NFM-T
Network Functions Manager - Transport

Release 22.6_FP1

OTN Guide

3KC73819QAAA

Issue 4

January 2023

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Warranty

Nokia provides a limited warranty for this product. For more information, consult your local Nokia customer support team.

Ordering information

The ordering number for this document is 3KC73819QAAA. To order Nokia NFM-T information products, contact your local Nokia customer support team.

Technical support

For technical support, contact your local customer support team. You can reach them via the Web at the Nokia Customer Support web site (http://www.nokia.com/support) or the customer support telephone number listed at the Nokia Contact Us web site (http://www.nokia.com/contact-us).

Information product support

For questions or concerns about this or any other Nokia information product, please contact us at one of the following numbers: (888) 727-3615 (for the continental United States), +1 (630) 713-5000 (for all countries).

Contents

List of tables

List of figures

About this document

Purpose

The purpose of the *OTN Guide* is to provide a detailed information of the NFM-T OTN application and to help the user to provision the system.

New Features in NFM-T Release 22.6_FP1

Following features are supported in Release 22.6_FP1.

Table 1 Platform: Release 22.6_FP1 Features

Feature	Description
Release 22.6 FP1, Issue 1, August 2022	
NFM-T deployment regression on RHEL 8.6	NFM-T introduces the support of RHEL 8.6 There is no documentation update for this feature.
NFM-T WaveLite - Enhanced Autostate feature	NFM-T introduces autostate feature on WaveLite See Set CIT Access Control in the *NFM-T NE Management Guide*.
[Sec-Cust] Scheduled Jobs visible and executable by owners and admin	NFM-T introduces the option that scheduled jobs (i.e. SW Download, Backup etc.) can be seen and executed only by the users having created them (owners) and admin users. This feature is not backward compatible and thus there is a preference to enable/disable (default is enabled) See the following in the *NFM-T Administration Guide*: • Preference Settings • Schedule a backup job
Release 22.6, Issue 1, June 2022	
NFM-T R22.6 Installation and Upgrade	The only supported distribution model is “Application Only” where NFM-T is installed over a RHEL Guest OS provided by the customer. Installation from scratch is supported. The supported direct upgrades on separate instances (migrations) are: • R20.11 to R22.6 Upgrade • R21.4 to R22.6 Upgrade • R21.12 to R22.6 Upgrade All deployment options are supported: Bare Metal, Classic, Distributed. See *NFM-T Installation_Migration Guide*.

Table 1 Platform: Release 22.6_FP1 Features (continued)

Feature	Description
Radius and TACACS+ transparent authentication for NE WebUI cut-through Completion	The NE WebUI User ID used by NFM-T for authentication on NE WebUI, in case of NE remote authentication, is extended to a maximum length of 64 characters. There is no documentation update for this feature.
Enhanced Autostate feature	A new NMS initiated Autostate feature such that NE Local CIT port is disabled when NFM-T is connected and enabled when disconnected is introduced for 1830 PSS R14.0.8, 1830 PSI-M R6.0.8, 1830 PSD R4.0, and 1830 ONE R4.2. **Note:** Both 1830 PSS-4 NEs and Classic EC 1830 PSS NEs, addressed with IPv6, do not support the NE-initiated auto-state. See Set CIT Access Control in the *NFM-T NE Management Guide*.
Restrict the account used for NFM-T to NE communication to NFM-T use only.	This feature is implemented to restrict the User ID used for NFM-T to NE communication for NFM-T use only (there is no direct access to NE using that User ID). This applies to HTTPS (NE WebUI) and NetConf (GMRE) interfaces. The NFM-T User ID is tied to the NFM-T IP addresses, and checked by NE, to verify that this User ID is exclusively used by NFM-T. This ensures that all actions performed on the NE can be accounted to individual (NFM-T or NE) users. The feature is available on 1830 PSS R14.0.8, 1830 PSI-M R6.0.8, and 1830 PSD 4.0. See Restrict the user for NFM-T-NE communication in the *NFM-T Administration Guide*.
Web UI Accessibility (Barrier Freeness) requirements	Accessibility (Barrier Freeness) to the NFM-T GUIs has been improved, focusing on the following areas: • Access at high zoom level (200% on browser). • Ability to operate the system without a mouse. • Logical progression of cursor (tab) movement and visible focus. See Accessibility Enhancements in the *NFM-T Getting Started Guide*.
MnC overall License Control policy	NFM-T system administrators (only) can do the following: • View the display in the NFM-T GUI for both Network and License Points (LPs). • Check whether the network growth is approaching the limit set by purchased LPs. • Export the license calculation information via *.csv and RestNBI. See the following in the *NFM-T Administration Guide*: • MnC Licence Management • License Threshold • Licence

Table 1 Platform: Release 22.6_FP1 Features (continued)

Feature	Description
CLOG support for 1830 PSD	NFM-T supports CLOG function introduced by 1830 PSD R4.0. See User Activity Log Description in the *NFM-T Administration Guide*
Security	
[Security Audit] Configurable password for SFTP/FTP swdl1 user	The user for all sFTP connections between NFM-T and NE (CPB, SW Download, MIB Backup/Restore, PM) is changed to eftp1 only (the swdl1 user has been removed). The eftp1 password can be changed, as documented in the *Administration Guide*. See Configure password for eftp1 user in the *NFM-T Administration Guide*.
[Sec-Cust] Support deny SSH root directive	NFM-T R22.6 does not need root user access during installation and post-installation operations. These can be performed by an independent user or maintenance user. See *NFM-T Installation_Migration Guide*.
[Sec-Cust] Proteus findings: Sudoedit instead of VI	VI is removed from a predefined list of sudoers command of the maintenance user. See *NFM-T Installation_Migration Guide*.
[Security] Mnc: Remove completely the world write permission to all application files and directories	The world write permission to all application files and directories except */nfmt/data/eml/eml_ft_data* directory,files and sub-directories is removed completely. See *NFM-T Installation_Migration Guide*.

Table 2 OTN: Release 22.6_FP1 Features

Feature	Description
Release 22.6 FP1, Issue 1, August 2022	
1830 PSS R14.0.9 support	NFM-T introduces the support of 1830 PSS R14.0.9 maintenance release There is no documentation update for this feature.
1830 PSD R4.0.1 support	NFM-T introduces the support of 1830 PSD R4.0.1 maintenance release There is no documentation update for this feature.
Support of nxOTU4 and mxOTUTC1 for 500G with SFM6 and S6AD600	NFM-T extends support for 500G profile for SFM6 and S6AD600 adding line structure composed by 5x OTU4 or 5x OTUTC1 (100G clients) See, Deploy a new service or infrastructure connection with template in the *NFM-T OTN Guide*

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
NFM-T Control Plane activation Procedure: L0 MP -> L0 GMPLS with L1 GMPLS active, with 1830 PSS-24x and OTSiG traffic	NFM-T validates L0 GMPLS activation procedure in networks with L1 GMPLS already active (on 1830 PSS-8x/1830 PSS-12x/1830 PSS-24x and 1830 OCS). In addition, NFM-T introduces the support of OTSIg as foreign connection to allow inclusion in L0 GMPLS activation procedure for all cards supporting OTSig. The unsupported configurations are as follows: • No support of 3R if 3R OTs are in a “secondary” NE in cluster with the NE crossed by the OTUk channel • No L0 GMPLs activation for network scenarios in which a 100G B&W I/O card (1AN100 on OCS and 4AN400/10AN400 in 24x) is connected to a OT/muxponder (for example D5X500). For 1830 PSS-24x, this is a not supported configuration in NFM-T • 1AN100 to 1AN100 (two separated NEs), to cross another vendor network, is not impacting by L0 GMPLS activation procedure There is no documentation update for this feature.
WaveLite NTW scenario: Cascade Access 200 w/ DD2M4	NFM-T supports the cascade configuration between WaveLite Access and 1830 PSI-M for 10G services. The configuration is made by: 1. Symmetric configuration (WaveLite Access 200 cascaded to PSI-M on both sides) with DD2M4 2. 10G clients ports on WaveLite Access 200 3. WaveLite Access 200 B&W port configured at OTU4 connected to PSI-M clients port configured at OTU4 as well See Interworking Scenarios in the *NFM-T NE Management Guide*.
Link Allocation cost - user value extension	NFM-T extends link allocation cost (both physical and logical) from 100 to 100,000. See the following in the *NFM-T OTN Guide*: • Physical Connections • Working in ASON • Network Profiles
OpenSNCP with hairpin configuration in a leg	NFM-T supports new scenario mixed-plane (with L1 GMPLS). In such a scenario, the SNCP protection is on one side in a managed-plane NE and the other in control-plane NE (OpenSNCP config). In addition, one leg of the protected service is a fully managed plane, a hair pinning configuration (managed-plane leg is looped on two clients ports on control-plane NE). See, Create ASON hairpin service in the *NFM-T OTN Guide*
500G QAM32, 67Gbaud, SD-FEC-G2, abs coding, Flex DFC12E	NFM-T introduces new line mode for 500G QAM32 @67 GBaud for DFC12E See, Profile and Supported Cards in the *NFM-T OTN Guide*

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Release 22.6, Issue 1, June 2022	
NE List	
1830 PSS R14.0.x and PSI-M R6.0.x Introduction and PSS release compatibility	NFM-T supports: • 1830 PSS-4, 1830 PSS-8. 1830 PSS-16, 1830 PSS16II, 1830 PSS-32, 1830 PSS-8x, 1830 PSS-12x, 1830 PSS-24x, 1830 PSS-64, 1830 PSS-36 R14.0.8 • 1830 PSI-M R6.0.8 • 1830 PSI-8L R14.0.8 See the following in the *NFM-T NE Management Guide*: • Add a Node • Add an 1830 PSI-M NE
1830 ONE R4.2 introduction	NFM-T introduces the support for 1830 ONE R4.2. For an upgrade to R4.2 from R4.1 there are two options according to the cards installed: • “SW+FW” download/activation command which works for any card • "SW only” option which is supported for following cards only: OC2O10MS-CBR, OC4S10MS, CC5S02MS, CCVS02MS, CC4S10MS. In this case, user has to active FW in a second moment. In case the user runs “SW only” on unsupported card, no preventive check is provided by NFM-T. The operation is concluded successfully but no upgrade is done. The user has to redo the operation using “SW+FW” only. For upgrade to R4.2 from previous releases (R3.1, R4.0) the only supported option is “SW+FW” download/activation command. There is no “SW only” option in UI menu since, such a command is not supported by the NE. See the following in the *NFM-T NE Management Guide*: • Add a Node • Add and view 1830 ONE node/NE
TPS R2.1 no break support (parity with R2.0.2)	NFM-T supports R2.1 for TPS-12 and TPS-24. See the following in the *NFM-T NE-Management Guide*: • Add 1830 TPS Node for Advanced Node. • Add a Node. • Introduction to 1830 TPS NE. See Introduction to 1830 TPS NE in the *NFM-T OTN Ethernet Services Manager Guide*.
Node Management	

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
NFM-T: 1830 PSS Shelf RI data editing and reporting	NFM-T supports editing of Shelf RI data and reporting through GRI , Hardware Inventory and REST API. There is no documentation update for this feature.
Reports: Shelf attributes added to the GRI report	Additional attributes pertaining to the shelf are now available in the GRI file where shelf details are provided. The attributes are: • part number • serial number • manufacturing date • quantity • shelf type • NE software release There is no documentation update for this feature.
NE SW Upgrade and Card FW administration	NFM-T enhances the software upgrade procedure, performing a set of operations automatically (NE SW download, NE MIB backup, NE SW activation). Additional improvements are introduced in the software and firmware management workflows. See Software Management in the *NFM-T Administration Guide*.
NTP sync enhancement for 1830 PSD and 1830 ONE	NFM-T extends NTP management for 1830 PSD and 1830 ONE adding the following features (to align 1830 PSD and 1830 ONE behavior to 1830 PSS): • NTP sync status reporting in node list. • Time zone reporting in node list. See the following in the *NFM-T NE Management Guide*. • NTP Description • NEs Table Columns See Network Time Protocol in the *NFM-T OTN Guide*.
Network Management	
S6AD600H and SFM6 400G Client - no transcoded ETH	NFM-T introduces the 400 GBe client on no-transcoded ETH model (OTUC4). It also provides the following: • Mix of Nx OTUC4 + MxOTU4 on a single carrier OTSiG in managed-plane and Control Plane. • Mix of NxOTUTC4 + MxOTUTC1 on a single carrier OTSiG in control-plane (managed plane in NFM-T R21.12). See the following in the: • New service/infrastructure connection in the *NFM-T OTN Guide* • 1830 PSI-M NE in the *NFM-T NE Management Guide*

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
S6AD600H OPSUM (Control Plane)	NFM-T extends OPSUM protection to S6Ad600H in Control Plane configuration as per 1830 PSS R14.0.8 feature set. See the following in the: • OPS protection in the *NFM-T OTN Guide* • S6AD600H in the *NFM-T NE Management Guide*
S6AD600H - New Carrier Profile for PSE-Vs	NFM-T supports new modulations and profiles introduced by 1830 PSS R14.0.8 for: • 300G SQAM16, 86.36 GBaud • 500G QAM16, 87.36 GBaud • 400G SQAM16, 85.82 GBaud Note: 500G modulation RRC 1.0 is supported for MP only (no Control Plane support), but NFM-T GUI has no logic to block the selection for Control Plane connections. See the following in the: • New service/infrastructure connection in the *NFM-T OTN Guide* • S6AD600H in the *NFM-T NE Management Guide*
S6AD600H 3R management	NFM-T supports S6AD600H for regeneration for unprotected and protected configuration (OLP, OPSUM, OMSP) for Managed Plane and Control Plane applications **Note:** In case of 3R and a mix of unprotected and protected OMSP segments, a specific provisioning sequence is to be followed (refer to documentation). • See S6AD600H in the *NFM-T NE Management Guide*. • See Manage 3Rs in the *NFM-T OTN Guide*.
S6AD600H OPSB5	NFM-T supports OPSB5 on S6AD600H introduced by 1830 PSS R14.0. • See S6AD600H in the *NFM-T NE Management Guide*. • See OPS protection in the *NFM-T OTN Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
SFM6 - New Carrier Profile for PSE-Vs	NFM-T supports new carrier profiles in SFM6 for Managed plane and Control-plane network. The carrier profiles are: • 300G SQAM16, 86.36GBaud, SD-FEC-G3, abs coding, Flex • 400G SQAM16, 85.82GBaud, SD-FEC-G3, abs coding, Flex • 500G QAM16, 87.36GBaud, SD-FEC-G3, abs coding, Flex TcGEnOTUFlex is a new mapping for transcoded GEthernet (ODUTCx): • 300G QAM16, 84.23GBaud, SD-FEC-G3, abs coding, TcGEnOTUFlex • 300G SQAM16, 84.23GBaud, SD-FEC-G3, abs coding, TcGEnOTUFlex • 500G QAM16, 87.16GBaud, SD-FEC-G3, abs coding, TcGEnOTUFlex For the carrier profile requiring 100GHz channel width as default value, @ 112.5 GHz remains a compatible channel width value for 300G, 400G and 500G. See the following in the: • See New service/infrastructure connection in the *NFM-T OTN Guide*. • See 1830 PSI-M NE in the *NFM-T NE Management Guide*.
SFM6 - OPSUM protection management	NFM-T introduces OPSUM support for 1830 PSI-M SFM6. • See PSI-M Interworking Scenario in the *NFM-T NE Management Guide*. • See OPS protection in the *NFM-T OTN Guide*.
SFM6 OPSB/5 Protection	NFM-T introduces OPSB protection on SFM6. See OPSB and OPSB5 protection in the *NFM-T OTN Guide*.
SFM6 cascade with MUX48W in 1830 PSI-CL	NFM-T supports a cascade configuration with SFM6 - 1830 PSI-CL for symmetric service with MUX48W. SFM6 configuration is supported with the following scenarios • Unprotected SFM6 - 1830 PSI-CL • Protected with OMSP/OLP with SFM6 - 1830 PSI-CL • Protected with 3-legs with SFM6 - 1830 PSI-CL • Cascade with WaveLite, WLA200 - SFM6 - 1830 PSI-CL To use SFM6 with PSI-CL, MUX48W is needed. See 1830 PSI-CL 3-fiber configuration support in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
2UC1T - Basic introduction	NFM-T R22.6 introduces the support of 2UC1T, a new 2 carrier PSE-Vs uplink card for 1830 PSS-24x with the following features: • Support of flexible carrier/port configuration facilitating PSE-Vs DSP module capabilities • Support of a Line Structure: Nx OTU4. In line with the carrier rate, the line is logically represented as mutiples of OTU4. • Support of a Line Structure: OTUC4 for client @ 400G in single ODUFlex. • OTSiG Tunnel can be regenerated with S6AD600H (flat mode). **Carrier Profiles** • Support of 400G SQAM16, 100GHz, (85.82GBaud), SD-FEC-G3, abs coding, Flex as carrier profile. • Target of the Baudrate is to be compatible with 32xWR20 filtering functions 100-GHz wide The list of spacings requested: • Default channel spacing: 100 GHz • Tight channel spacing: 100 GHz • ODUk/ODUflex (GFP, CBR) mappings • ODUflex (BMP, BGMP, IMP) Support of delay measurement DMi (latency) for not terminated infrastructure via tandem connection delay of HO TCM connections. The latency value is measured on demand like the other packs where DMi is already supported (i.e 4UC1T), stored and accessible in Infrastructure Connections list page. **Protections** OLP/OMPS based on OPSA. It is line protection (for Managed Plane and L1 GMPLS/MRN). This includes iOMSP protection as well. The current features set is supported for Managed Plane and Control Plane applications. See 2UC1T in the *NFM-T NE Management Guide*.
400Gbe service/ODUc4 management for PSS-x uplinks, I/O cards - 2UC1T, 4UC1T	NFM-T extends 400Gbe service management across the following 1830 PSS-x cards: 4UC1T, 10AN1T, 2UC1T for managed-plane and for control-plane configurations (in previous releases only managed-plane on 4UC1T/10AN1T was supported). See the following in the *NFM-T NE Management Guide*: • 10AN1T • 4UC1T • 2UC1T See Deploy a new service or infrastructure connection with template in the *NFM-T OTN Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
S5AD400H latency measurement	NFM-T extends On-demand Service Latency measurement support for S5AD400H. See S5AD400H in the *NFM-T NE Management Guide*.
S5AD400H 3R	NFM-T supports 3R with S5AD400H, with and without OCH protection with OPSUM, introduced by 1830 PSS R14.0 • See S5AD400H in the *NFM-T NE Management Guide*. • See Manage 3Rs in the *NFM-T OTN Guide*.
S5AD400H OPSB 100Gbe/OTU4	NFM-T supports OPSB5 protection introduced by 1830 PSS R14.0 on S5AD400H for 100Gbe, OTU4 and 400Gbe clients. • See S5AD400H in the *NFM-T NE Management Guide*. • See OPS protection in the *NFM-T OTN Guide*.
DD2M4 - OTU4 and 200G QPSK, 62Gbaud, SD-FEC-G2, abs coding, and Flex recovery	NFM-T supports 200G QPSK, 62Gbaud, SD-FEC-G2, Flex for DD2M4, and abs coding. See the following in the *NFM-T OTN Guide*: • Deploy a new service or infrastructure connection with template • CPB Application 1830 PSI-M Management in the *NFM-T NE Management Guide*
200G QAM16 33 Gbaud Carrier Profile	NFM-T extends the set of profiles for 2UX500 and 4UC1T adding 200G 16QAM at 33Gbaud. See the following in the *NFM-T NE Management Guide*: • 1830 PSS-12x • 4UC1T See New service/infrastructure connection in the *NFM-T OTN Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
OTSiG Interop	NFM-T introduces OTSiG model for: • D5X500Q (only Managed Plane). • 2UC400 (Managed Plane and Control Plane L1 and MRN). • 4UC400 (Managed Plane and Control Plane L1 and MRN). NFM-T provides support of 200G QAM08, 45Gbaud, SD-FEC-G2, abs coding, OTU4 for 4UC1T, 2UX500 for Managed Plane and Control Plane. NFM-T supports the following interworking scenarios based on OTSiG Model: • 10AN1T: SFM6 (with and without 3R in Managed plane and in GMPLS L1 and MRN. • S6AD600H: SFM6 (without 3R based on S6Ad600H) @ 400G-/86.20GBaud, 600G-/90Gbaud and new carrier profiled added in NFM-T R22.6. • 8UC1T: 4UC400 (with and without 3R based on S2AD200H)@ 100G 33Gbaud in Managed Plane, in GMPLS L1 CP and MRN. • 4UC1T: 4UC1T (with 3R based on S5AD400H) @200G/62Gbaud, @300G/62Gbaud, @400G/62Gbaud in Managed Plane, in GMPLS L1 CP and MRN. • 4UC1T - 2UC400: (without 3R based on S5AD400H) @ 200G 45GBaud in Managed Plane, in GMPLS L1 CP and MRN. • 2UX500 - 2UC400 (without 3R based on S5AD400H) @ 200G 45GBaud in Managed Plane, in GMPLS L1 CP and MRN 2UX500. • 2UX500 (with 3R based on S5AD400H) @ 200G/62Gbaud, 300G/62Gbaud, 400G/62Gbaud in Managed Plane, in GMPLS L1 CP and MRN. • 2UX500 - 4UC1T (with 3R based on S5AD400H) @ 200G/62Gbaud, 300G/62Gbaud, 400G/62Gbaud in Managed Plane, in GMPLS L1 CP and MRN. • D5X500 - 4UC1T (without 3R based on S5AD400H) 200G 45GBaud in Managed Plane. • S5AD400H - 4UC1T (with 3R based on S5AD400H) @ 200G/62Gbaud, 300G/62Gbaud, 400G/62Gbaud in Managed Plane. • D5X500Q - 2UX500 (without 3R based on S5AD400H) 200G 45GBaud in Managed Plane. • S5AD400H - 2UX500 (with and without 3R based on S5AD400H) @ 200G/62Gbaud, 300G/62Gbaud, 400G/62Gbaud-67Gbaud in Managed Plane. • DD2M4 - DD2M4 (w/o 3R based on S5AD400H) @ 200G/62Gbaud, 300G/62Gbaud, 400G/62Gbaud in Managed Plane. S5AD400H - DD2M4 (with and without 3R based on S5AD400H) @ 200G/62Gbaud, 300G/62Gbaud, 400G/62Gbaud in Managed Plane. More information is available in OTSiG Interop package delivered with BluePrint Package. See Manage an OTSig Tunnel in the *NFM-T OTN Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
PSE-Vs Path Delay Measurement	The On-Demand Service latency Measurement covers all rates for terminated services, which rely on either ODU4 or ODUFlex as LO ODUk connection layer where actually the measurement is implemented. The On-Demand Service latency Measurement is not supported for ODUk/OTUk unterminated services, which have TCM setting as a pre-requisite. See the following in the *NFM-T NE Management Guide*: • 1830 PSI-M NE • S6AD600H

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
ASG consolidation	NFM-T extends ASG support for the following nodal configurations for Managed Plane and Control Plane applications. **WR8-88A/AF (MP/CP)** ASG/ASGLP supports the full function of legacy amps in the ROADM node configurations: • **Protection**: OMSP/OLP protection • **Raman amplification (RA2P-96)**: RA4P is not supported in ROADM node. RA2P is not certified in 1830 PSS validation program • **OCM**: WTOCM/WTOCMA/WTOCM-F should be supported. • **TPIOC**: PTPIOC should be supported in ROADM config with ASG/ASGLP amp. **WR20TF/WR20TFM (MP/CP)** ASG/ASGLP supports the full function of legacy amps in the WR20-TF/WR20-TFM node configurations: • **Protection**: OLP protection. OMSP is not supported in WR20-TF/WR20-TFM node. • **OCM**: WTOCM/WTOCMA/WTOCM-F is supported. • **PTPIOC**: PTPIOC is supported in WR20-TF/WR20-TFM configuration with ASG/ASGLP amp. • **DCM**: support is transparent for NFM-T. **FOADM without WTOCM (auto power management)** ASG/ASGLP shall support the full function of legacy amps in the FOADM node configurations: • **Protection**: OLP/OMSP protection. • **Raman amplification (RA2P-96)**. RA4P is not supported in FOADM . RA2P is not certified in 1830 PSS validation program • **OCM**: No WTOCM/WTOCMA/WTOCMF • **PTPIOC**: PTPIOC is supported in FOADM configuraion with ASG/ASGLP amp. Supported shelf types are: 1830 PSS32, 1830 PSS 16II, 1830 PSS 8, 1830 PSI-8L, 1830 PSS-4 ASG support is independent from add/drop structure and from signal types. ASG is certified for all add/drop configurations and for all signal types (unkeyed, keyed, alien). See ASG and ASGLP in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
1.25GHz Central Frequency Granularity for S6AD600H and SFM6	Subsea applications require the ability to manage 70 GHz channel width in the spectrum, and the option to tune the central frequency of a given carrier (optical channel) with 1.25 Ghz granularity. NFM-T R22.6 extends the 1.25GHz tuning feature to S6AD600H and SFM6 as well. It was already introduced for S4X400H in NFM-T R21.4, with the same features set for all supported carrier profiles. No changes to Provisioning workflow and OAM flow with respect to NFM-T R21.4. 70 Ghz and 1.25 GHz tuning for submarine can be used in scenarios such as: • 1830 PSS Line System and 1830 PSS OTs • 1830 PSS Line System and 1830 PSS dangling OTs • 3R Regen between Subsea and Terrestrial DWDM networks See the following in the *NFM-T NE Management Guide*: • S6AD600H • 1830 PSI-M NE See 33.75 GHz and 70 GHz central frequency granularity for subsea application in the *NFM-T OTN Guide*.
16P200 new configurations and OTU2	NFM-T extends support of 16P200 card to include the following: • Stand-alone mode • Cascading with S4X400H for the Managed Plane application • OTU2 clients See 16P200 in the *NFM-T NE Management Guide*.
S13X100R/E and Client to Client (hairpin) Connections	NFM-T supports hairpin configuration on S13X100 (all variants) in order to "groom" the 10G client into OTU4 B&W client via port C32. The hairpin configurations are supported via top-down approach (via provisioning) or in discovery mode with network operation mode. The supported configurations are based on: • Symmetric configuration S13X100 - S13X100 B&W OPS link • Cascade configuration with 8P20 or 11DPM8 The Hairpin configuration is independent of 1830 PSS photonic architecture and it is independent of server protection (OLP/OMSP are supported). See S13X100 in the *NFM-T NE Management Guide*.
S13X100L OTU4 client and ADM function	NFM-T extends S13X100L support adding OTU4 client and ADM function. See S13X100 in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
WR20-TFM & IRDM32 Heterogeneous node in C-band for L0 GMPLS network	NFM-T R22.6 introduces the support of heterogeneous node based on WR20-TFM & IRDM32 for C-band network with L0 GMPLS only or with L1 GMPLS enabled as well. NFM-T does not provides any procedure to define the heterogeneous NE. It provides only the management and monitoring of this type of NE with the following capabilities: • Support of discovery for mixed degree configuration. • Support of mixed degree configuration for service/infrastructure connection deployment terminated in that node or in pass-through. • No break respect to all other functions supported on WR20 NE and IRDM32. **Note:** There is no improvement on the automatic routing for heterogeneous node management. Therefore the service creation via automatic routing is provided in the best-effort mode. In case of failure due to unavailability of routes, a re-provisioning of service/connection with manual routing (with constraints) is required. See the following in the *NFM-T NE Management Guide*: • Mesh Cards • MSH8A
Control Plane	

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Alien Restoration (read-only)	NFM-T introduces Alien wavelengths restoration in the photonic Control Plane network. The Alien Wavelength restoration service is defined via a template as an OCH service in the Managed plane network and it requires the ENE (Virtual NE) as termination point. The Alien wavelengths restoration service is supported with the following nodal configuration: • **C-F (iROADM9R, IR9)** IR9-(PSC) iROADM9R-PSC iROADM9r-SFD44/B (no ITLB) • **CDC-F 2.0 (iROADM20/32)** iRDM20/32 - AAR8x/AAR2x8A- MCS816/MCS1615 • **C-F (iROADM20/32)** iROADM20/32 - MLFSB - (PSC) • **CDC-F 1.0 (WR20-TFM)** WR20-TFM - AAR8x/AAR2x8A- MCS816/MCS1615 • **C-F (WR20-TF)** WR20-TF-PSC No discovery of alien restoration is available in the release. Alien Network Management (Alien wavelength support on Control Plane) in the *NFM-T OTN Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
2UX500 - Generalized support in GMPLS domain (GA)	NFM-T supports new uplink 2UX500 (with 2 multi-rate ports) in 1830 PSS-8x/12X with the following carrier profiles for Control Plane application: • 200G QPSK, 64Gbaud, SD-FEC-G2, abs coding, Flex • 300G QAM08, 64Gbaud, SD-FEC-G2, abs coding, Flex • 400G QAM16, 62Gbaud, SD-FEC-CE, abs coding, Flex • 400G via 67Gbaud 16QAM, SDFEC-G2 for FLEX OTU @87.5GHz (profile #5) Both line ports can be configured @100G, @200G. Or only one line port can be configured @300G or @400G. Support of NxOTU4 line structure. Support of multiplexing, switching and protection for ODUFlex (GFP-F) and ODUFlex (CBR) in Managed Plane and Control Plane applications. For CBR mapping, the following rates are supported: • FC-400, FC-800, FC-1600 • 3G-SDI Support of TCM in alignment to other uplink (8UC1T,4UC1T) and allowing the Delay Measurement based on TCM for HO TCM connection. The following scenarios are applicable to Control Plane and applicable to all OTN I/O packs like 5MX500, 20MX80, 20AX200 (for 1830 PSS-12x) or 30AN80, 30AN300 or 10AN1T for 1830 PSS-24x: • 2UX500 - 2UX500 with and without 3R based on S5AD400 • 2UX500 - 4UC1T @ 200G/300G/400G with and without 3R based on S5AD400H See 1830 PSS-12x in the *NFM-T NE Management Guide*.
Foreign Connection for OTSiG Tunnel	NFM-T R22.6 introduces the foreign connection concept for OTSiG Tunnel defined with: • S4X400H, S5AD400H, S6AD600H • SFM6, DFC12, DFM6 • 4UC1T, 8UC1T • 2UX500, 10AN1T See Foreign Connections in the *NFM-T OTN Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Qualify Automated Network Transformation use cases with L1 CP traffic	Extension of Automated Network Transformation to L1 GMPLS. In NFM-T R22.6 the Add & Remove NE on OTS (basically a Spilt/Join OTS) and Bulk Traffic Move is available for L1 GMPLS and for L0 GMPLS network with the same behavior. Automated Network Transformation is supported for a network with: • Pure L1 GMPLS • L0 GMPLS and L1 GMPLS (overlay mode) • MRN configuration with OTSiG Tunnel defined with new generation packs (S4X400H, DFC12, S5AD400H, S6AD600H, 8UC1T, 4UC1T and so on. **Add & Remove NE on OTS** The same Transformation template is available for L0 GMPLS transformation. It is not required to move the traffic to free the OTS resources. The traffic impacted during the transformation will be reconciled automatically by the system. **Bulk Traffic Move** The same command is available for Bulk Traffic Move for L0 GMPLS network. There is automatic rerouting of traffic, no constraint can be specified by the user. Stored rerouting log and export to external tools options are available. Both operations are available via REST call as well. See Insert and Remove a Node in an OTS link in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Path Alarm based restoration	NFM-T supports Path Alarm based restoration setup on SNC for L0 GMPLS and MRN network. NFM-T provides a new form on SNC to enable the path alarm based restoration. By default, this function is disabled. The user can specify the following: • **maximum number of movements:** 0 indicates disabled and this is the default. The max number is 5. • **path-alarm hold-down timer**: The range is 30 seconds to 1 hour. The default is 5 minutes. • **New state (RestorationLimit)**: Reported on the SNC if the maximum number of movements is reached. Two new alarms are reported if the path alarm based restoration is enabled. They are: • **ReversionBlocked-due-to-movement**: On detection of this alarm, the automatic reversion is blocked and the traffic has to be moved manually (via manual reversion) by the user. • **MovementBlocked**: Indicates that no more movements are performed as the maximum number of movements is reached. See Descriptions of Alarm Probable Causes for ASON in the *NFM-T Service Assurance Guide*. See the following in the *NFM-T OTN Guide*: • Path alarm based restoration movements • Field descriptions for Best Practices templates • New service/infrastructure connection • Deploy connection- ASON specific parameters • Modify the attributes of an SNC • Switch SNC routes
L0 GMPLS support on IR9	NFM-T introduces IR9 at feature parity with respect to iROADM9R for L0 GMPLS. See IR9 and IR9LP in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Information on Disjointness state in ASON SNC list	A new attribute is added in the ASON SNC GUI list to report the disjoint relationship of the selected SNC towards the other ASON SNCs available in the network. The new attribute also reports the type of disjoint relationship: • **Normal**: no diversity relationship • **Telink**: with TELink Diversity • **SNC Diversity**: with SNC Diversity • **TeLink and SNC Diversity**: TElink and SNC diversity See ASON SNC table columns in the *NFM-T OTN Guide*.
MRN support of OCS and 1830 PSS-x interworking - 1830 PSS 8x/12x	MRN support on 1830 PSS-8x /12x, with for 2UX100, covering symmetric configuration and interworking with 1830 PSS-36/64 (130SCUP) and 1830 PSS-24x (2UC400/4UC400). See Interworking of legacy cards of 1830 PSS-64, 1830 PSS-32, 1830 PSS-24x in the *NFM-T OTN Guide*.
UI and Usability	
New Topology Map Enhancements	NFM-T enhances MAP, adding the following new features: • Map Subnetwork Tree with a global NE search (also available in NFM-T R21.12 without the tree) • Expand or collapse single bundle • Manage X/Y Link shapes • Popup extensions • Rates updates • Save zoom level and position See Network Map in the *NFM-T Getting Started Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
GUI List improvements - propagate to more screens	NFM-T extends the filtering capabilities (per the configurable views shown at the top of the list) on the following lists: • NEs • Nodes • Looped back connections • Protected Connections view • SNCs • NPAs The same feature was introduced in R21.12 for Service, Infrastructure, and Physical connections. See the following in the *NFM-T NE Management Guide*: • View NE List • View Nodes and Subnetworks and Related Equipment • MSH8A See the following in the *NFM-T OTN Guide*: • Looped back connections • Protected Connections
GUI Screen conversion to REACT	NFM-T aligns additional pages to the new UI look and feel. See the following in the *NFM-T NE Management Guide*: • Activate/Deactivate Auto Restoration of the Control Plane • Move NE • Synchronize a Node with its NEs • Node Templates and New Nodes - Further Actions • Import CSV Template file to Create a Node(s) • Configure NTP for a Selected NE • Perform Trap Based Discovery • Perform Network Scan • Best Practice Node Templates • Access and View a Node Template • Perform Trap Based Discovery • Modify a Node Template

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Add ability to see discrepancies from the Inconsistencies screen	NFM-T introduces the following UI enhancements: From the **Parameter Mismatches** tab on the Inconsistencies page, a new menu item “Show Discrepancies” added to show discrepancies. See WebUI Enhancements in the *NFM-T Getting Started Guide*. See Parameter Mismatches in the *NFM-T OTN Guide*.
WaveLite	
Release 22.6 FP1, Issue 1, August 2022	
[WaveLite] EQM : Support GCC0 configuration for WaveLite Access-200 Uplink#1 and Uplink#2 ports	NFM-T extends GCC0 configuration on WaveLite Access-200 to Uplink #2 in addition to available Uplink #1 See the following in the *NFM-T NE Management Guide* • WaveLite Display and Operations on EQM • Protection in WaveLite
[WaveLite] WEB UI - with cookies	NFM-T introduces support for WaveLite WEBUI cut-through navigation with SSO and ZIC proxy integration. There is no need for WEBUI user credentials to be provided. Access to WaveLite WEBUI will be through NFM-T proxy and no direct access between user PC and WaveLite WEBUI is required. There is no documentation update for this feature.
[WaveLite] R2.1 management	NFM-T introduces the support of WaveLite R2.1 See Access NE WebUI for a Selected NE in theNFM-T *NE Management Guide*.
[WaveLite] ALS validation	ALS is the WaveLite 2.1 feature. NFM-T tested alarm correlations on WaveLite with ALS (generating a LOS in the opposite direction of the fault and related consequent alarms). See the following in the *NFM-T NE Management Guide* • View and Modify Ports on WLM200 and WLM200B • View and Modify Ports on WLA200 • View and Modify Ports on WLMux 16/WLAMP • Create and Manage Connections for WaveLite
[WaveLite] NTP sync enhancement for WaveLite	NFM-T improves the WaveLite NTP Sync status handling based on the trap notifications from the WaveLite NE. Equipment synchronization is no longer required to update the WaveLite NTP sync status to NFM-T. See NTP Description in theNFM-T *NE Management Guide*.
[WaveLite] Intrusion alarm	NFM-T manages WaveLite intrusion alarm (security alarms from NE alerting about the block of NE WebUI account due to three consecutive wrong login credentials insertion). See Alarm Management in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Release 22.6, Issue 1, June 2022	
[WaveLite] Bidirectional Power graph for WaveLite	NFM-T extends power monitoring graph to WaveLite NE for B&W cascading to 1830 PSS and for WaveLite to WaveLite colored scenarios. The power monitoring graph is available only for WaveLite R2.0 or later. See Manage Optical Power in the *NFM-T OTN Guide*.
[WaveLite] Cascade configuration WLA200-SFM6-OPSUM -GA	NFM-T supports symmetric cascade configuration based on WaveLite Access 200 connected to SFM6 with OPSUM protection (WLA200-- SFM6---OPSUM) for Managed Plane network. There is no documentation update for this feature.
1830 PSI-CL	
1830 PSI-CL Line protection scheme over 3 fibers	NFM-T R22.6 recovers the management of 3-legs protection schema supported by 1830 PSI-CL R1.2 only for DFC12 and SFM6. 3-legs protection is managed according to the following behaviours: • OMSP creation is based via discovery or path synchronization only. This is due to the fact that the connectivity in the NE is fixed. • Transformation from 2-legs to 3-legs can be done only via DB remove. The 2-legs configuration has to be removed from the NFM-T DB and the new 3-legs protection configuration is discovered via path synchronization. This operation does not maintain the old service user label of 2-legs configuration because the user label is not stored on the NE • NFM-T does not provide any offline procedure to perform the transformation from 3-legs to 2-legs. In case the NE is configured with the OMSP cascade, this configuration is automatically managed like a 3-legs configuration by the system. • Power monitoring for 3-legs is managed like 2-legs with an additional tab for the 3rd leg. • The 3-legs protection is reported in with separated OMSP protection entries in the list, since the protection switch command can be applied on the single OMSP protection block. See the following in the *NFM-T NE Management Guide*: • 1830 PSI-CL 3-fiber configuration support • Optical power display for 1830 PSI-CL 3-fiber connectivity • 1830 PSI-CL Service Assurance

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Recovery of OSNR, Fiber Characteristics and OTDR for 1830 PSI-CL	NFM-T R22.6 introduces the support of: • **OTDR scan**: Supported on LINEIN port for all PSI-CL amplifiers packs • **Fiber Characteristics**: Supported parameters are: Amplifier Current Gain, Target Gain, Egress, and Ingress Powers. Other typical parameters supported for 1830 PSS in Fiber Characteristics are not supported since 1830 PSI-CL does not need automatic power management and does not use planning and commissioning. Hence the parameters tied to these domains are not available. They are: - Max Planned Span Loss - Min Planned Span Loss - Commissioned Span Loss - Measured Span Loss - Max Planned Gain - Min Planned Gain • **OSNR and Optical Channel Power**: Supported only for OA-H/LINEOUT and SIGOUT ports. Hence, P2P terminal configurations are fully supported. For configurations with ILA, the power monitoring is not properly reported for the channels because no optical channel power is provided by ILA. The OSNR value is approximately computed using total power / Nchannels like the AA2DONWB. See the following in the *NFM-T NE Management Guide*: • OSNR Support for 1830 PSI-CL • Fiber Characteristics Support for 1830 PSI-CL Physical Connection • OTDR Scan Support for 1830 PSI-CL Physical Connection
1830 ONE	
1830 ONEm - Single Fiber Working (SFW)	NFM-T supports single fiber solution introduced by 1830 ONE R4.1 for 4/16 channels. **Notes** • There is no alien over single fiber - only point to point and FOADM only. • There is no optical pass-through between single fiber MUX and not 3R on transponder. • There is no mix single/dual fiber on same OTS - scenarios. • There is no single fiber in PSS-ONE interworking. See 1830 ONE Single Fiber Working (SFW) in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
1830 ONEh - MSP 1+1 protection support for SDH UNI IFs - CBR mapping	NFM-T supports new MSP 1+1 **line side** as per existing mOTN MSP fetaure set. See Configuring MSP 1+1 Protection in the *NFM-T NE Management Guide*.
1830 ONEm - CFP2 Amplifier	NFM-T supports new CFP2 amplifier introduced by 1830 ONE R4.1. See 1830 ONE - WDM Card in the *NFM-T NE Management Guide*.
1830 ONEm - 4 channels and 16 channels fixed Mux/Demux with PTP coupling filters	NFM-T introduces new 1830 ONE DWDM 4/16 Channel MUX: D4MDM-OT and D16MDM-OT See 1830 ONE NE in the *NFM-T NE Management Guide*.
1830 ONE support of Jabil CFP2-DCO module and OTU4 IW with 1830 PSS	NFM-T introduces new pluggable CFP2-DCO on the CCVS02MS card. The 1830 ONE-PSS interworking network scenarios supported are: • CC4S10MS - 2UX200 • CCVS02MS - 2UX200 • CCVS02MS - S2AD200H All above scenarios are at 100G line rate only, through OTU4, with SD-FEC. The photonic line is mROADM or a direct link (OPS link). 1830 PSS photonic line is not supported in this release. See CFP2-DCO module support and ONE-PSS interworking in the *NFM-T NE Management Guide*.
1830 ONE HUB - L2 features enhancement (on 10G PKT card only)	NFM-T extends OC2O10MS L2 functions adding: • LAG with 4 Member Ports • WTR on LAG A/A single card See Configure 1830 ONE Packet in the *NFM-T NE Management Guide*.
1830 ONE HUB - Enhanced packet card	NFM-T introduces a new 1830 ONE packet card OC2E10PK at same feature level of existing ones. See the following in the *NFM-T NE Management Guide*: • 1830 ONE NE • 1830 ONE - 1830 PSS Interworking Example • Introduction to 1830 ONE OTN cards • Configure 1830 ONE WDM • Packet cards management
[1830 ONE] Add/remove leaf	NFM-T introduces the add/remove leaf for EVP-tree L2 service type. See Evp Tree service in the *NFM-T NE Management Guide*.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
[1830 ONE] Procedure to reconfigure in-field services with LAG-O instead of LAG-V	NFM-T introduces a procedure to re-configure 1830 ONE services from LAG-V to LAG-O. See Create LAG-O configuration in the *NFM-T NE Management Guide*.
[1830 ONE] In Line Amplifier (ILA) for Single Fiber Working (SFW) solution and OSC	NFM-T extends single working fiber solution for 1830 ONE mROADM adding ILA NE type. Notes: • There is no alien over single fiber • There is only point to point • There is only FOADM • There is no optical pass-through between single fiber MUX and not 3R on transponder • There is no mix single/dual fiber on same OTS • There is no single fiber in 1830 PSS ONE interworking scenarios See 1830 ONE Single Fiber Working (SFW) in the *NFM-T NE Management Guide*.
[1830 ONE] ONEm - WDM functional configuration for OSC.	NFM-T supports the procedure to seamlessly swap OSC modules and amplifiers in 1830 ONE R4.2 (This feature is limited to the HW for which such change is supported in 1830 ONE R4.2) See Add Logical Blocks in the *NFM-T NE Management Guide*.
[1830 ONE] ONE Hub-10GE ports reconfigurable as 1GE ports on OC2O10MS PKT card	NFM-T supports 1830 ONE R4.2 to reconfigure 10GBE ports as 1GBE ports and vice-versa on the OC2O10MS card. See Reconfigure ports as 1GBE ports on OC2O10MS PKT card in the *NFM-T NE Management Guide*.
[1830 ONE] Transmission parameters (TTI, TX shutdown, port mode)	NFM-T extends the range of parameters controlled from the GUI for 1830 ONE connection provisioning: The parameters are: • TX Shutdown • Trace identifier (OTU, ODU) • Port Mode setting See Create a service in OTN in the *NFM-T NE Management Guide*.
[1830 ONE] ONE hub - alarm name alignment to 1830 PSS	NFM-T aligns 1830 ONE alarm name attribute to 1830 PSS naming (this is applicable to some alarms. Some others remain as per existing 1830 ONE value because there is no equivalent alarm in 1830 PSS). There is no documentation update for this feature.

Table 2 OTN: Release 22.6_FP1 Features (continued)

Feature	Description
Management of Live PM for 1830 ONE	NFM-T extends live PM function to 1830 ONE R4.2. See PM Counters in the *NFM-T Service Assurance Guide*.

Table 3 EML and Equipment Manager: Release 22.6_FP1 Features

Feature	Description
Release 22.6, Issue 1, June 2022	
NTP sync enhancement for 1830 PSD and 1830 ONE	NFM-T extends NTP management for 1830 PSD and 1830 ONE adding the following features (to align 1830 PSD and 1830 ONE behavior to 1830 PSS): • NTP sync status reporting in node list. • Time zone reporting in node list. See the following in the *NFM-T NE Management Guide*. • NTP Description • NEs Table Columns See Network Time Protocol in the *NFM-T OTN Guide*.

Table 4 Ethernet Service Manager: R22.6 Features

Feature	Description
Navigation options and actions from L2 Routing Display	The L2 routing display for asymmetric services supports the following new menu items: • **Port Properties**: A new menu option **Properties** is added for port and on clicking the navigation shall bring to port details in EQM. • **Show Elementary Alarms**: Gets access to EQM Alarm list. • **Show NE WEBUI**: Navigates to NE WEBUI, where WEBUI gets launched in separate tab. • **Show Equipment Manager**: Supported for NE and Port. Navigates to EQM. • **Show DSR Connection**: Supported on DSR links. navigates to 360 Degrees view of the DSR connection service in OTN associated to the L2 service. See View the Graphical Display in the *NFM-T OTN Ethernet Services Manager Guide*.
Support for Service SAP Type "Any" and C-VLAN value different from "0"	NFM-T supports EVPL asymmetric service having Service SAP Type "Any" and C-VLAN value different from "0". See Deploy a Provider Bridge Service - EVPL in the *NFM-T OTN Ethernet Services Manager Guide*.

Table 4 Ethernet Service Manager: R22.6 Features (continued)

Feature	Description
Dot1q-range scenario support	ESM provides the capability to use dot1q-range service with dot1q VLAN range SAP only to support the C-Tagged P2MP with QinQ. See Deploy a Provider Bridge Service - EVPL in the *NFM-T OTN Ethernet Services Manager Guide*.

Table 5 North Bound Interface: R22.6 Features

Feature	Description
NFM-T NBI: SNMP-AH alarm clear trap configurability	In NFM-T R21.12, with the **includeAlarmDetailsOnChangeEvent** flag set to TRUE, the CLEAR trap reported all the fields reported by the RAISE trap. In NFM-T R22.6, it is now possible for the operator to configure the fields that are to be reported in the CLEAR trap. This is being enhanced because setting the **includeAlarmDetailsOnChangeEvent** flag to TRUE would enable all the fields to be reported in the CLEAR trap. This might lead to performance issues since all customers would not require all the fields to be reported. See the following in the *NFM-T SNMP Alarm Handoff External Interface Specification for NSP Fault Management Guide*: • Change Log • Set/Modify user credentials • SNMP Alarm Handoff Primitives • Filter Configuration file

Table 6 Service Assurance: R22.6 Features

Features	Description
Enhance OCH PM counters (Qmargin, CSR)	NFM-T extends PM management adding the following counters: • [S2AD200H/R] Qmargin • [S4X400] Qmargin, CSR • [S4X400L] Qmargin, CSR • [4UC1T] Qmargin, CSR • [S5AD400] Qmargin, CSR • [2UX500] Qmargin, CSR • [SFM6] Qmargin, CSR See the following in the *NFM-T Service Assurance Guide*: • Performance Monitoring Description • OA&M Diagnostics • PM Counters (On Demand /Live PM) • Mapping PM Values for 1830 PSS • Create a TCA Profile • Manage PM for a Connection
New 1830 PSS-X Equipment alarm - Redundancy Impaired (REDIMPAIRED)	The Redundancy Impaired (EPS-IMPAIRED) alarm is a newly introduced Equipment alarm on the 1830 PSS-X Shelf type and reported in NFM-T. The alarm is raised on following conditions: • When the clock DNR Led is in Solid Amber color • When EC (Equipment controller) "ready to protect" state is different than yes • When SWC (Switch fabric) status is different than "redundancy available" The new alarms are raised against CEC (Clock & Equipment Control) and SWC (Switch Fabric) with Minor severity they are tagged as Root Alarm for NFM-T. See Alarm List in the *NFM-T Service Assurance Guide*.

Table 7 WaveSuite Synchronizer: R22.6 Features

Feature	Description
WStS: Sync Service operations (for PTP services)	On the Commissioned services, the output timing interfaces, BITS-OUT, 1PPS+ToD will be configurable. Sync service de-activation for maintenance reasons is supported. Modification of the service that includes addition or removal of clocks and ports and modification of their sync parameters is supported. There is no documentation update for this feature.

Table 7 WaveSuite Synchronizer: R22.6 Features (continued)

Feature	Description
WStS: SyncE FM	WStS will provide a summary view of sync alarms on the dashboard, with a navigable link to the NSP FM-App for a detailed view. See WStS Alarms in the *WaveSuite Synchronizer User Guide*.
WStS: Data export	The sync data (sync domain and services) can be exported as JSON and CSV. See WStS Service operations for time distribution in the *WaveSuite Synchronizer User Guide*.
WStS: PTP-PM	WStS supports PM monitoring/collection for PTP (time-distribution) services. This includes: • Automatic 15min/24hr PM data collection and storage from NE Sync Monitoring Points. An option to enable PM is provided during sync service creation itself. No other start/stop action will be required (from UI or via ReST API). • WStS has an option to navigate from a Sync Service to the M&C PM Reporting tool, where the involved Monitoring Points are selected. Live reporting and Data Queries will apply as well to Sync PM. • WStS supports Clear bin option on a per Sync Service basis. See the following in the *WaveSuite Synchronizer User Guide*: • WStS Performance Management • TCA profile summary • PM TCA Profile • Modify a TCA profile
WStS: Sync Service discovery (for Sync-E)	WaveSuite Synchronizer supports discovery of SyncE services (frequency distribution) from the deployed network. See WStS Service Discovery in the *WaveSuite Synchronizer User Guide*.
WStS: Sync Service Deploy (for Sync-E)	WaveSuite Synchronizer supports deployment of SyncE services (frequency distribution) See the following in the *WaveSuite Synchronizer User Guide*: • Create a new service for frequency distribution • View service summary details for frequency distribution • WStS Service operations for time distribution • WStS Service operations for frequency distribution
WStS: Map view enhancements	The synchronization layer of the NFM-T Map is enhanced to support rendering of SyncE services. See WStS network map for frequency distribution

What's new in OTN Guide

This is Issue 4 of *NFM-T OTN Guide, Release 22.6_FP1*.

The new features introduced in previous releases are available in Appendix E, "NFM-T Feature History".

The following table shows the document changes.

Table 8 Release 22.6_FP1 Document changes in Issue 4, February 2023

Unable to create an OPS connection between and External Network Element and a 1830PSS-16II	A note is added in Create an OTN OPS physical connection for packet switch. See • 7.19.8 "Task: Create an OTN OPS physical connection for packet switch" (p. 801)

Table 9 Release 22.6_FP1 Document changes in Issue 3, December 2022

Inconsistency while performing ASON synchronization	A note is added in ASON synchronization. See • 10.47 "Introduction" (p. 1569).
Removed the information on **Delete from NFM-T**.	A note which reads *The user can perform Delete from NFM-T in the OPERATE > Infrastructure Connections page on commissioned L0 and L1 ASON connections and perform ASON SNC discovery.* is removed. See • 10.47 "Introduction" (p. 1569).
Added a note in Routing Display	A note is added in *View Protected Connections* for managed plane and control plane Routing Display. See • 7.86 "View Protected Connections" (p. 1091).

Table 10 Release 22.6_FP1 Document changes in Issue 2, November 2022

Wavekey assignment show some assigned keys as available	A note is added in wave key and wave key assignments description to track the wave key usage. See • 17.2 "Wave key and wave key assignments description" (p. 1716).

Table 11 Release 22.6_FP1 Document changes in Issue 1, August 2022

Link Allocation cost - user value extension	NFM-T extends link allocation cost (both physical and logical) from 100 to 100,000. See • "Physical Connections " (p. 784) • Chapter 10, "Working in ASON" • Chapter 6, "Network Profiles"
Physical connection creation is success for 13.1 NEs after passing cost value more than 100	There is no NE version check for Allocation Cost value during physical link creation. See • "Physical Connections " (p. 784)
Config-13 -Transformation - Structure and ASON Paymap occupied 18 slots instead of 16 slots for 100 CW 2UC1T foreign tunnel	A note is added in Structure Overview for WR8-88AF support. See 24.12 "View and Manage Structure" (p. 2022) for more information.
Issues in Max Character Limit in Connection Name of OPS/Infra/Service	Changed the maximum character limit for Connection Name, Alias, and Alias 2 in Connection Aliases. See 2.26 "Connection names and aliases" (p. 260). Changed the maximum character limit in System Generated User Label. See 7.19.9 "Physical connection User Label" (p. 804).
Non 3R ports are listing to create 3R in NPA	Higher order (HO) ODU 3R regeneration data is added in NPAs, TE Links, and 3Rs. See 10.6 "ASON NPA" (p. 1438) for more information.
Support of nxOTU4 and mxOTUTC1 for 500G with SFM6 and S6AD600	NFM-T extends support for 500G profile for SFM6 and S6AD600 adding line structure composed by 5x OTU4 or 5x OTUTC1 (100G clients) See: Table 8-3, "OPTICAL LINE CHARACTERISTICS Tab Parameters" (p. 1234)
OpenSNCP with hairpin configuration in a leg	NFM-T supports new scenario mixed-plane (with L1 GMPLS). In such a scenario, the SNCP protection is on one side in a managed-plane NE and the other in control-plane NE (OpenSNCP config). In addition, one leg of the protected service is a fully managed plane, a hair pinning configuration (managed-plane leg is looped on two clients ports on control-plane NE). See: 8.13 "Create ASON hairpin service" (p. 1351)
500G QAM32, 67Gbaud, SD-FEC-G2, abs coding, Flex DFC12E	NFM-T introduces new line mode for 500G QAM32 @67 GBaud for DFC12E. See : Table 8-15, "Profile and Card Mapping" (p. 1267)

Table 11 Release 22.6_FP1 Document changes in Issue 1, August 2022 (continued)

NFM-T Control Plane Activation Procedure: L0 MP -> L0 GMPLS with L1 GMPLS active, with PSS-24x and OTSiG traffic Support of Control Plan Acitivation Procedure	NFM-T supports Control Plane Activation Procedure. There is no documentation update for this feature.

Table 12 Document changes in 22.6 Issue 1, June 2022

Features/Enhancements	Description
Removal of MWSVC from containers other than otncore, adapter-x, sdh, motn	Removal of MWSVC from containers other than otn core, adapter-a See • 12.2 “System Administration functionality for CPB application” (p. 1614) • 12.3 “Start or stop mnc-cpb container ” (p. 1615)
CPB Support for 14.0.8	CPB is enhanced to support 4-digit release for 1830 PSS R14.0.8/ 1830 PSI-M R6.0.8 and supports backward compatibility See • 11.3 “Network planning using EPT” (p. 1599) • 11.5 “Configurations and stages supported on CPB” (p. 1605)

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
Path Alarm based restoration	Support of Path Alarm based restoration setup on SNC for L0 GMPLS and MRN network. NFM-T provides a new form on SNC to enable the path alarm based restoration, by default this function is disabled, where the user can specify: • maximum number of movements: 0 = disabled, max number 5, default 0. • path-alarm hold-down timer: 30sec to 1hour - default 5 min. New state (RestorationLimit) is reported on SNC if the maximum number of movements has been reached New two alarms are reported if the path alarm based restoration is enabled: • ReversionBlocked-due-to-movement - At detection of this alarm the automatic reversion is blocked and the traffic has to be moved manually (through manual reversion) by the user. • MovementBlocked See • 10.5 “Path alarm based restoration movements” (p. 1433) • 7.3 “Field descriptions for Best Practices templates” (p. 675) • 8.4 “New service/infrastructure connection” (p. 1219) • 10.2 “Deploy connection- ASON specific parameters” (p. 1424) • 10.43 “ Modify the attributes of an SNC” (p. 1557) • 10.44 “Switch SNC routes” (p. 1560)

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
SFM6 - New Carrier Profile for PSE-Vs	NFM-T supports new carrier profiles in SFM6 for Managed plane and Control-plane network. The carrier profiles are: • 300G SQAM16, 86.36GBaud, SD-FEC-G3, abs coding, Flex • 400G SQAM16, 85.82GBaud, SD-FEC-G3, abs coding, Flex • 500G QAM16, 87.36GBaud, SD-FEC-G3, abs coding, Flex TcGEnOTUFlex is a new mapping for transcoded GEthernet (ODUTCx): • 300G QAM16, 84.23GBaud, SD-FEC-G3, abs coding, TcGEnOTUFlex • 300G SQAM16, 84.23GBaud, SD-FEC-G3, abs coding, TcGEnOTUFlex • 500G QAM16, 87.16GBaud, SD-FEC-G3, abs coding, TcGEnOTUFlex For the carrier profile requiring 100GHz channel width as default value, @ 112.5 GHz remains a compatible channel width value for 300G, 400G and 500G. See 8.4 "New service/infrastructure connection" (p. 1219).
Foreign Connection for OTSiG Tunnel	NFM-T R22.6 introduces the foreign connection concept for OTSiG Tunnel defined with: • S4X400H, S5AD400H, S6AD600H • SFM6, DFC12, DFM6 • 4UC1T, 8UC1T • 2UX500, 10AN1T See "Foreign Connections" (p. 1413).
PSE-Vs Path Delay Measurement	The On-Demand Service latency Measurement covers all rates for terminated services, which rely on either ODU4 or ODUFlex as LO ODUk connection layer where actually the measurement is implemented. The On-Demand Service latency Measurement is not supported for ODUk/OTUk unterminated services, which have TCM setting as a pre-requisite. See 7.82 " Services list further actions" (p. 1067).
S5AD400H latency measurement	NFM-T extends On-demand Service Latency measurement support for S5AD400H. See 7.82 " Services list further actions" (p. 1067).

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
S5AD400H 3R	NFM-T supports 3R with S5AD400H, with and without OCH protection with OPSUM, introduced by 1830 PSS R14.0 . See “Task: Create a 3R” (p. 1486).
S5AD400H OPSB 100Gbe/OTU4	NFM-T supports OPSB5 protection introduced by 1830 PSS R14.0 on S5AD400H for 100Gbe, OTU4 and 400Gbe clients. See “Multi-port OPSB5 or OPSB protection for S4X400H, S5AD400H, and S6AD600H card” (p. 473).
S6AD600H OPSB5	NFM-T supports OPSB5 on S6AD600H introduced by 1830 PSS R14.0. See “Multi-port OPSB5 or OPSB protection for S4X400H, S5AD400H, and S6AD600H card” (p. 473).
S6AD600H 3R management	NFM-T supports S6AD600H for regeneration for unprotected and protected configuration (OLP, OPSUM, OMSP) for Managed Plane and Control Plane applications **Note:** In case of 3R and a mix of unprotected and protected OMSP segments, a specific provisioning sequence is to be followed (refer to documentation). See the following topics: • 2.31 “Provisioning connections for ADD4 cards” (p. 286) • “Task: Create a 3R” (p. 1486)
S6AD600H and SFM6 400G Client - no transcoded ETH	NFM-T introduces the 400 GBe client on no-transcoded ETH model (OTUC4). It also provides the following: • Mix of Nx OTUC4 + MxOTU4 on a single carrier OTSiG in managed-plane and Control Plane. • Mix of NxOTUTC4 + MxOTUTC1 on a single carrier OTSiG in control-plane (managed plane in NFM-T R21.12). See 8.4 “New service/infrastructure connection” (p. 1219).
S6AD600H OPSUM (Control Plane)	NFM-T extends OPSUM protection to S6Ad600H in Control Plane configuration as per 1830 PSS R14.0.8 feature set. See “OPSUM (Optical Protection Switch Universal Multi Carrier) ” (p. 514).

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
1.25GHz Central Frequency Granularity for S6AD600H and SFM6	Subsea applications require the ability to manage 70 GHz channel width in the spectrum, and the option to tune the central frequency of a given carrier (optical channel) with 1.25 Ghz granularity. NFM-T R22.6 extends the 1.25GHz tuning feature to S6AD600H and SFM6 as well. It was already introduced for S4X400H in NFM-T R21.4, with the same features set for all supported carrier profiles. No changes to Provisioning workflow and OAM flow with respect to NFM-T R21.4. 70 Ghz and 1.25 GHz tuning for submarine can be used in scenarios such as: • 1830 PSS Line System and 1830 PSS OTs • 1830 PSS Line System and 1830 PSS dangling OTs • 3R Regen between Subsea and Terrestrial DWDM networks 5.7 "33.75 GHz and 70 GHz central frequency granularity for subsea application" (p. 537).
S6AD600H - New Carrier Profile for PSE-Vs	NFM-T supports new modulations and profiles introduced by 1830 PSS R14.0.8 for: • 300G SQAM16, 86.36 GBaud • 500G QAM16, 87.36 GBaud • 400G SQAM16, 85.82 GBaud Note: 500G modulation RRC 1.0 is supported for MP only (no Control Plane support), but NFM-T GUI has no logic to block the selection for Control Plane connections. See 8.4 "New service/infrastructure connection" (p. 1219).
Information on Disjointness state in ASON SNC list	A new attribute is added in the ASON SNC GUI list to report the disjoint relationship of the selected SNC towards the other ASON SNCs available in the network. The new attribute also reports the type of disjoint relationship: • **Normal**: no diversity relationship • **Telink**: with TELink Diversity • **SNC Diversity**: with SNC Diversity • **TeLink and SNC Diversity**: TElink and SNC diversity See 10.34 "ASON SNC table columns" (p. 1527).
SFM6 - OPSUM protection management	NFM-T introduces OPSUM support for 1830 PSI-M SFM6. See "OPSUM (Optical Protection Switch Universal Multi Carrier) " (p. 514).

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
SFM6 OPSB/5 Protection	NFM-T introduces OPSB protection on SFM6. See “OPSB or OPSB5 protection for DFC12 or DFC12E and SFM6 card ” (p. 475).
Bidirectional power graph for Wavelite	NFM-T extends power graph to Wavelite NE for B&W cascading to PSS and for WL to WL colored scenarios. See 17.13 “Optical power visualization” (p. 1818).
NTP sync enhancement for PSD, WL, ONE	NFM-T extends NTP management for PSD, WL and ONE adding the following features (to align PSD, WL and ONE behavior to PSS) • NTP sync status reporting in node list • Time zone reporting in node list • NTP sync alarm in FM app See “Network Time Protocol (NTP)” (p. 356).
OTSiG Interop	NFM-T introduces OTSiG model for: • D5X500Q (only Managed Plane). • 2UC400 (Managed Plane and Control Plane L1 and MRN). • 4UC400 (Managed Plane and Control Plane L1 and MRN). NFM-T provides support of 200G QAM08, 45Gbaud, SD-FEC-G2, abs coding, OTU4 for 4UC1T, 2UX500 for Managed Plane and Control Plane. See 8.11 “Manage an OTSig Tunnel ” (p. 1314)

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
Alien Restoration (read-only)	NFM-T introduces Alien wavelengths restoration in the photonic Control Plane network. The Alien Wavelength restoration service is defined via a template as an OCH service in the Managed plane network and it requires the ENE (Virtual NE) as termination point. The Alien wavelengths restoration service is supported with the following nodal configuration: • **C-F (iROADM9R, IR9)** IR9-(PSC) iROADM9R-PSC iROADM9r-SFD44/B (no ITLB) • **CDC-F 2.0 (iROADM20/32)** iRDM20/32 - AAR8x/AAR2x8A- MCS816/MCS1615 • **C-F (iROADM20/32)** iROADM20/32 - MLFSB - (PSC) • **CDC-F 1.0 (WR20-TFM)** WR20-TFM - AAR8x/AAR2x8A- MCS816/MCS1615 • **C-F (WR20-TF)** WR20-TF-PSC No discovery of alien restoration is available in the release. See “Alien Network Management” (p. 346)
Customer Name and Alias2 missing for Discovered Connections	A note has been added for Customer Name and Alias2 Name for Discovered Connections. See “CONNECTION CHARACTERISTICS tab” (p. 1223)
SVT_ASON_20.11_L1CP_ System Generated Name does not show the Flex Client Rate for the connection.	A note has been added for when *Use system-generated name?* option is selected, service Rate is included as part of the connection. See 7.64 “Rename Connection and Customer Name” (p. 997)
A or Z prefix is not present for most of the attributes in Physical Connection Page.	Physical connection page has attributes labels with A or Z as prefix. See “Physical Connections ” (p. 784).
400Gbe service/ODUc4 management for PSS-x uplinks, I/O cards - 2UC1T, 4UC1T	NFM-T extends 400Gbe service management across the following 1830 PSS-x cards: 4UC1T, 10AN1T, 2UC1T for managed-plane and for control-plane configurations (in previous releases only managed-plane on 4UC1T/10AN1T was supported). See “Deploy a new service or infrastructure connection with template” (p. 1216).

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
GUI List improvements - propagate to more screens	NFM-T extends the filtering capabilities (per the configurable views shown at the top of the list) on the following lists: • NEs • Nodes • Looped back connections. See “Physical, Logical, and Link Connections” (p. 219) • Protected Connections view. See “Protected Connections ” (p. 1088) • SNCs. See Chapter 10, “Working in ASON” • NPAs. See 10.9 “View the list of NPAs” (p. 1447) The same feature was introduced in R21.12 for Service, Infrastructure, and Physical connections.
200G QAM16 33 Gbaud Carrier Profile	NFM-T extends the set of profiles for 2UX500 and 4UC1T adding 200G 16QAM at 33Gbaud. See 8.4 “New service/infrastructure connection” (p. 1219).
MRN support of OCS and PSS-x interworking - 1830 PSS 8X/12x	MRN support on 1830 PSS-8x /12x, with for 2UX100, covering symmetric configuration and interworking with 1830 PSS-36/64 (130SCUP) and 1830 PSS-24x (2UC400/4UC400). See 2.51 “Interworking of legacy cards of 1830 PSS-64, 1830 PSS-32, 1830 PSS-24x” (p. 338).
GUI Screen conversion to REACT	NFM-T aligns additional pages to the new UI look and feel. See the following: • 9.9 “Schedule the Revertive Switching for ASON Routed Connection” (p. 1386) • 17.6 “Manage an OTDR Scan for an OTN OTS Physical Connection” (p. 1734) • 17.8 “Manage fiber cut localization” (p. 1781) • “Schedule Path Synchronization” (p. 1198) • 2.59 “Add or delete an NTP Server” (p. 358) • 10.55 “Manage and schedule the jobs for Reversion Control Group” (p. 1588)
DD2M4 - OTU4 and 200G QPSK, 62Gbaud, SD-FEC-G2, abs coding, and Flex recovery	NFM-T supports 200G QPSK, 62Gbaud, SD-FEC-G2, Flex for DD2M4, and abs coding. See • 8.11 “Manage an OTSig Tunnel ” (p. 1314)

Table 12 Document changes in 22.6 Issue 1, June 2022 (continued)

Features/Enhancements	Description
OTN Enhancements - 22.Tiber.1H	This epic will track OTN internal improvements for 22.H1 Planned items : Dev sanity enhancements and TTI related transmission parameter support gaps There is no documentation update for this feature
Enhancements to Card Capability module and associated references	Use CCS for LCGen involving new Gen cards Use CCS for PA Tables involving new Gen cards Use CCS for Port Selection involving new Gen cards Remove TransParams from RA and use CCS for new Gen cards Remove all references from RA for cards using /defined in CCS For cards I/W with new Gen cards, use CCS All components (SNA, NPR, ASON, OTN, EPT, FM, PM, ASAP, GUI) should use CCS and not RA wherever applicable There is no documentation update for this feature
Add ability to see discrepancies from the Inconsistencies screen	NFM-T introduces the following UI enhancement: A new popup menu item Show Mismatches is added in the PARAMETER MISMATCHES tab on the OPERATE > Network Inconsistencies screen. "Network Inconsistencies " (p. 1157)

Safety information

This document does not contain any safety information (cautions or warnings) because the NFM-T is a software product.

Important! When working with any hardware that is associated with any piece of software, always refer to the safety information that the hardware manufacturer provides for that particular piece of hardware. For example, when working with a server, refer to safety information that is provided in the documentation for that server. When working with any Nokia network element, refer to safety information that is provided in the Nokia documentation for that particular NE.

Intended audience

The *OTN Guide* is written primarily for network planners, engineers, or operators. This document can be used by anyone who needs specific provisioning information about the features of the NFM-T OTN and its NFM-T GUI. These people are you, its users.

Getting Started with NFM-T

The **Network Functions Manager - Transport** is a part of inter-operating network management modules and uses modular design and a common resource base to efficiently deliver a set of network management services.

The **Network Functions Manager (NFM)** performs comprehensive network management for network infrastructure.

Please refer to the *Getting Started Guide* for details on the product architecture. This documentation set describes the NFM-T features and functions as a complete suite.

Technical content

In general, the technical content in this document can be augmented by the technical content that is provided in other documents in this documentation set and/or in the document set of the particular network element (NE) or piece of hardware in the network configuration. It is the user's responsibility to have these documents on hand and to read all pertinent material in all documentation sets in order to understand a particular concept or procedure and/or to implement the procedure in his or her working environment.

Important!

The NFM-T GUI main menu enables users to perform **Design**, **Deploy**, **Operate**, and **Administer** functions. The majority of these functions are documented in the *OTN Guide*; however, the *OTN Guide* does refer users to the *OTN Ethernet Service Manager Guide* (which is the companion document of the *OTN Guide*), the *Administration Guide*, and the *Service Assurance Guide* for information and task details.

Each release of the NFM-T and its applications supports certain NEs within the Nokia family of optical NEs. Mention of NEs or specific NE features in the text of this document, or any document in the NFM-T documentation set, that are not supported in this particular product release can apply to prior or future product releases. Such material may not be currently visible or operable on the GUI and/or the server and has been added only as a convenience for our customers. Once again, it is the user's responsibility to have current copies these documents on hand and to read all pertinent material in all documentation sets in order to understand a particular concept or procedure and/or to implement the procedure in his or her working environment. This material is subject to change. For a list of NEs that are supported in the NFM-T Release 22.6_FP1, contact your Nokia local customer service support team.

This document, or any document in the NFM-T documentation set, may contain information that is related to features, service packs (SPs), maintenance releases, or other updates that our product and its applications supported in prior releases or is to support in the near future. This material may not be visible or operable on the supported servers and/or GUI, and has been added only as a convenience for our customers. This material is subject to change. For a list of all supported features for a particular release, contact your Nokia local customer service support team.

Document parts

The *OTN Guide* is a document that contains the following *parts*.

- **Part I: Understanding the Product and Provisioning**
- **Part II: Connections and Services**
- **Part III: ASON**
- **Part IV: Commissioning and Maintenance**
- **Part V: Tools**
- **Part VI: WebUI Quick HELP, TAB HELP and Data Tables**

Each document part can contain *chapters*, which can contain *sections*.

In addition, the *OTN Guide* contains appendices and an index.

Conceptual and task content

In the broadest sense, each chapter or section in this document contains the following types of content:

- *Conceptual* content, which is background information, is provided so users can better understand the tasks that must be performed. The presentation of conceptual information varies according to the topic being explained—sections, subsections, tables, figures, and screen captures can be commonly found.
- *Task* content, which includes step-by-step instructions, is provided so users can provision the system. The task information is typically presented as series of tasks that follows the conceptual information.

The conceptual information complements and enhances the step-by-step instructions that are found in each task. To optimize the use of the conceptual and task content, users should consider the following:

- The conceptual information should be used to broaden your general knowledge of the network management system. It is best if you read all conceptual information and have a good understanding of the concepts being presented before undertaking the step-by-step instructions given in any task.
- The conceptual and task portions of the document have extensive hyperlinks. Use these links to toggle between the two types of information presented so you can access all pertinent information related to particular concepts and tasks.
- The task information is based on a user-needs analysis that has been performed for each management system user job; therefore, use the task information to get the job at hand done quickly and with minimal system impact.

Organization and preparation of NFM-T GUI content

From the **Administration** main menu of the NFM-T GUI, users can specify **Preferences** to customize their views of the window arrangement, screen size, default page, and main menu configuration of the NFM-T GUI.

We used the following NFM-T GUI **Preferences** when we organized and prepared this document:

- The **Window Arrangement** field was set to **horizontal**.
- The **Main Screen Size (%)** field was set to **55**%.
- The **Initial Page** field was set to **Dashboard**.
- The **Main Menu Configuration** field was set to **Classic (cascading)**.
- The **Map Titles** field was set to **Open Street Maps**.
- The **PTN NM Launched At Login** field was left unchecked so the NFM-T GUI launched at login.
- The **Dashboard Charts** field was set to display **Elementary Alarms**, **Alarmed Physical Connections**, **Alarmed Connections**, **Pending Connections**, **Alarmed ASON SNCs**, and **Unavailable ASON Links**.

Note to our NFM-T OTN Release 22.6_FP1 users of this document!

Users can select a variety of preferences to customize the NFM-T GUI. We have retained part of former releasesNFM-T GUI defaults in this document so our existing customers, who migrate to Release 22.6_FP1, have continuity in their documentation.

Format of task content

Each task consists of sections that are called *When to use, Related information, Before you begin*, and *Task*. The intent of these sections is self-explanatory—they explain when you should use the task, any related information that you would need to know while doing the task, and what you need to consider or do before you start the task.

When a task does not have any related information that must be considered before it is started, the *Related information* section for that task states the following:

This task does not have any related information.

When a task does not have any conditions that must be considered before it is started, the *Before you begin section* for that task states the following:

This task does not have any preconditions.

Each *Task* section consists of steps. The completion of all steps, which are sequentially numbered, is required for the entire task to be completed successfully. In some instances, a step might be prefaced with the wording *Optional*, which indicates that the step can be skipped and the task can still be completed successfully. A task is considered to be completed when all of its steps are completed and when the wording *End of steps* is displayed.

Many times, the management system affords users with multiple ways to accomplish the same task. In these instances, this type of task gives the user several *Methods* of how to accomplish the same set of steps successfully.

Typographical conventions used

This document uses the following typographical conventions:

- **User input or path navigation on the NFM-T GUI is identified with this type. NFM-T GUI fields/parameters and their options are also identified with this type.**
- `System output is identified with this type.`
- **Examples, Notes, and Important considerations are identified with this type.**
- *Document titles or words that are being defined or emphasized are identified with this type.*

Marking conventions used for content

The following convention is used to indicate navigation paths from the NFM-T GUI, which are the mouse and/or button menu selections that users must make to arrive at a destination on the NFM-T GUI:

Operate > Nodes

All mouse selections are presumed to be left clicks. Right click mouse selections are indicated as the following:

Right-click the highlighted item and follow the path: **Synchronize > Full**.

Occasionally, a set of NFM-T features is not supported for all NEs or for all operating components and/or environments. This set of features is clearly marked to show these exceptions.

Treatment and definition of a term

A term that is presented in the text of this document, along with any used abbreviation for the term, is typically defined where the term is initially introduced. For a list of all of the terms that are defined in this document, users should look up the word *Definitions* in the Index of this document. A list of all of the terms that are defined along with their page numbers is under the word *Definitions*.

NFM-T Release 22.6_FP1 documentation

Documentation for the NFM-T Release 22.6_FP1 library consists of a set of technical manuals that help the user to navigate the system user interface of the NFM-T and to use these interfaces to provision the system. Installation and administration operations are also described to fulfill administrative tasks on the system.

The NFM-T Release 22.6_FP1 supports the following documents:

1. The *Installation and Migration Guide* (3KC73819NAAA) explains how to perform the installation of the NFM-T and its applications.
2. The *Administration Guide* (3KC73819MAAA) explains how to administer and maintain the element management layer, network management layer, and service management layer of the NFM-T.

   The document explains how to administer and maintain the common administration menus that are associated with the NFM-T and with its applications; it explains also how to administer and maintain the common tools and processes that are associated with the NFM-T and with its applications.
3. The *Troubleshooting Guide* (3KC73819LAAA) explains to network planners, engineers, users how to troubleshoot issues that occur during installation of the NFM-T application.
4. The *Getting Started Guide* (3KC73819AAAA) explains the product with an overview, the look-and-feel and the use of the WebUI, deeper described in the OTN Guide for new users. This document also contains a glossary of terms.
5. The *NE Management Guide* (3KC73819BAAA) explains how to manage the NEs supported by the NFM-T. A description of the operations and data for the NE management is available in this guide and also the equipment Manager application is widely described. In addition dedicated chapters for PSS, PSD, PSI, ONE 1830 NEs are available to consult.
6. The *OTN Guide* (3KC73819QAAA) explains how to provision the NFM-T OTN on the NFM-T GUI. The NFM-T OTN provides the Wavelength Division Multiplexing (WDM) and Dense Wavelength Division Multiplexing (DWDM) network management layer for the NFM-T. The *OTN Guide* includes EML and Service Assurance information for the NFM-T OTN application along with explanations of how to use the NFM-T GUI. The *OTN Ethernet Service Manager Guide* is the companion document to the *OTN Guide*.

   The *OTN Guide* describes also ASON management in the NFM-T providing users with the conceptual information that is needed to enhance their understanding of the technology involved in ASON management of the NFM-T.

   The Commissioning and Power Balancing (CPB) Tool, which is a software tool for automated provisioning, commissioning and power balancing functions of photonic networks based on the

Nokia 1830 PSS portfolio of WDM products is also described. In addition, the OTN Guide explains how to use the WebUI user interface.

7. The *OTN Ethernet Service Manager Guide* (3KC73819VAAA) explains how to provision the Ethernet services on the NFM-T GUI. The Ethernet Service Manager is a feature of the NFM-T OTN application of the NFM-T management system. The *OTN Ethernet Service Manager Guide* is the companion document to the *OTN Guide*.
8. The *Service Assurance Guide* (3KC73819FAAA) explains fault management and performance monitoring for the NFM-T and its different applications. Service Assurance information for the NFM-T OTN application are included in this guide.
9. The *SNMP Alarm Handoff External Interface Specification for NSP Fault Management* (3KC73819ZAAA) specifies the external interface to the SNMP Alarm Data Handoff Subsystem of the NSP Fault Management applicable for the Nokia OS system.

The NFM-T Release 22.6_FP1 also supports application for system resiliency. This application is explained in the following documents:

- *HA Guide* (3KC73819GAAA) explains how to install, administer, and use the High Availability feature.
- *Virtual Access to HA Enabled system - User Guide* (3KC73819JAAA) explains the steps to manage virtual access to the HA system.

The NFM-T Release 22.6_FP1 supports WaveSuite Synchronizer (WStS) application. This application are explained in the following document:

- *WStS User Guide* (3KC73819DAAA) explains how to install, administer, and use the WaveSuite Synchronizer feature.

Document formats

This document is available for use in PDF, HTML, EPUB, and MOBI formats.

Video Tutorials

The NFM-T Video Tutorials is a consolidated Help experience that allows the user to access NFM-T videos from the link in the Online Help package.

The Video Tutorial link from the Online Help directs the users to Nokia's Documentation Support Portal (https://infoproducts.nokia.com/aces/cgi-bin/chk_access.cgi/3KC73819TAAA.html).

Note: Access is available only to authorized users.

On-line Help

The main help icon is located on the top right corner of the title bar for the **Nokia Network Functions Manager - Transport**. This help icon, which is a **?** mark, enables you to access the library of customer documents for the Nokia Network Functions Manager - Transport for Release 22.6_FP1.

Help is also provided for the more complicated NFM-T GUI pages. For example, for infrastructure connection and service provisioning, the help icon, which is a **?** mark, is located on the bottom right corner of the Create Connection pop-up window. This help icon enables you to access information that explains the window, the provisioning fields, and any important provisioning considerations

How to order

The ordering number for this document is 3KC73819QAAA. Contact your Nokia local customer service support team for details.

In addition, to order the NFM-T and/or any of its applications, add-on features, or upgrades, contact your Nokia local customer service support team.

How to comment

To comment on this document, go to the Online Comment Form (https://documentation.nokia.com/comments/) or e-mail your comments to the Comments Hotline (mailto:comments@nokia.com).

Part I: Understanding the Product and Provisioning

Overview

Purpose

This part of the *OTN Guide* provides users with the conceptual information that is needed to enhance their understanding of the technology and the provisioning of the NFM-T OTN application of the NFM-T.

Contents

1 Product and Technology Concepts

1.1 Overview

Purpose

This chapter contains the conceptual material that users need to understand the NFM-T product and its applications and an overview on managed Network Elements families.

Contents

Understanding the NFM-T

1.2 NFM-T Overview

NFM-T definition

The NFM-T, Network Functions Manager - Transport, is the Nokia converged and unified network management system that manages the complete portfolio of the Nokia family of WDM photonic and OCS switching NEs. To accommodate the world of transmission standards, these NEs operate using different transport structures and support different native command languages.

NFM-T and its supported management layers

The NFM-T, is a network management system that supports several management layers. It accommodates and grows with a customer's optical network.

The Element Management Layer (EML), provides the functionality required to access any Nokia supported NEs that are deployed in a customer network. The EML provides a single access point for communication with an NE and the physical resources of a network.

The Network Management Layer (NML), provides the functionality required to commission, provision, and supervise the network that is deployed by a customer.

The Service Management Layer (SML), provides the functionality required to commission, provision, and supervise network services that a Nokia customer deploys to its end users or to its customers.

NFM-T software and access to its licensed applications

The NFM-T Release 22.6_FP1 is run through an Internet browser-based user interface that supports standard web features. The NFM-T Web application provides a central access point for user authentication. The NFM-T is launched through an Internet browser connecting directly to the application, users log in to the NFM-T. It is from the Web browser directly that users gain access to the NFM-T, and the user interface that supports the application:

- The Web User Interface (WebUI) supports the “NFM-T OTN” (p. 127) application and its Ethernet Service Manager, along with the NFM-T Element Management Level (EML), Equipment Manager (EQM), Performance Monitoring, and Alarm Management.

NFM-T and its Applications

The NFM-T is the Nokia converged and unified network management system. It manages the complete portfolio of Nokia's active NEs and it maintains the complete portfolio of Nokia legacy NEs.

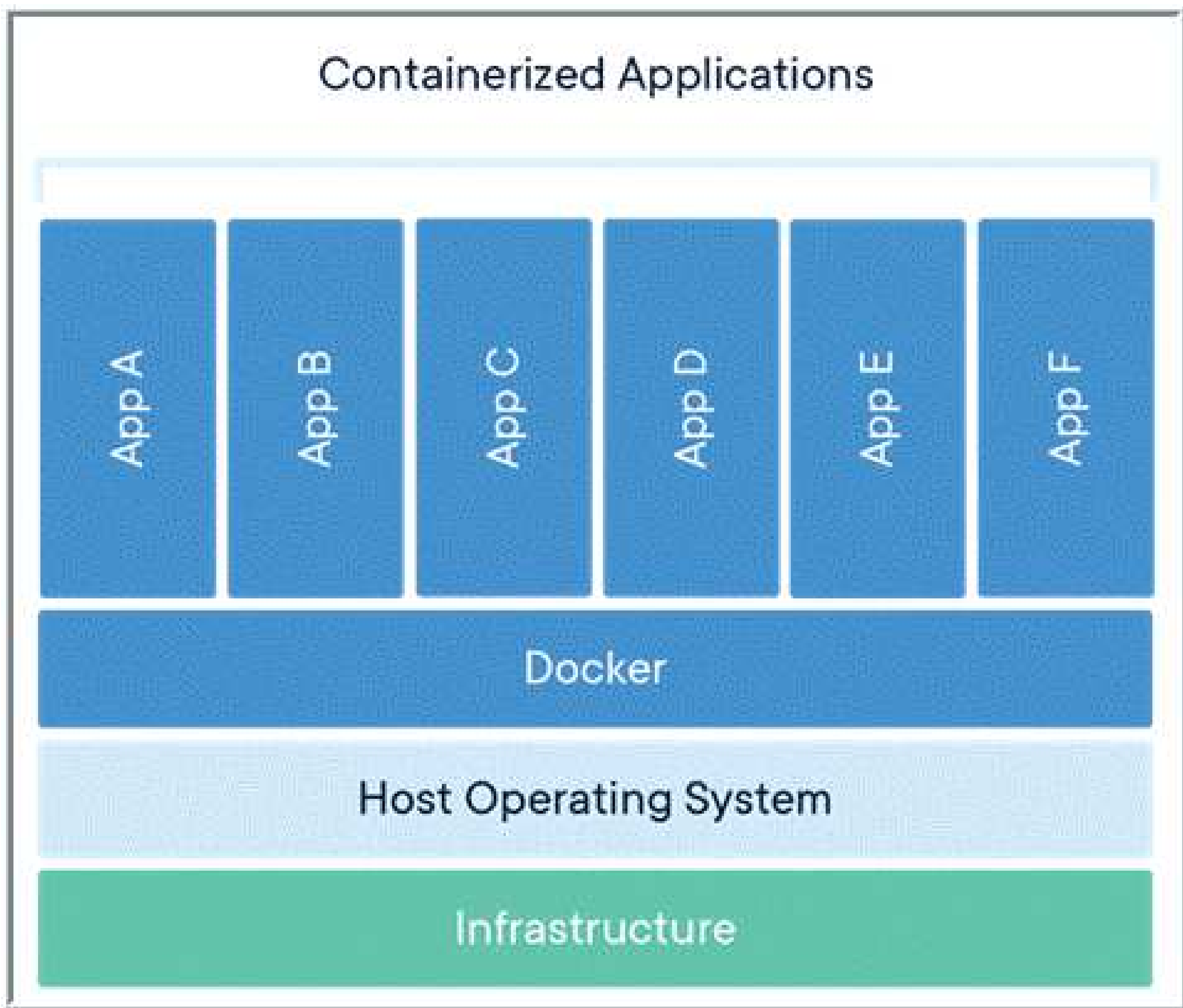
The user is encouraged to refer to the *Getting Started User Guide* volume for any further information about the applications and architectures that make up the NFM-T platform. The *NFM-T Product Overview* chapter in the User Guide provides the reader with an overview of the NFM-T platform. It helps the reader get acquainted with the different Network Elements, Networks, and Services that are managed with NFM-T. This chapter also describes the architecture and software components of NFM-T.

Platform Definitions

A **Container** is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

A **Docker** container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.

Figure 1-1 Platform - Container Applications

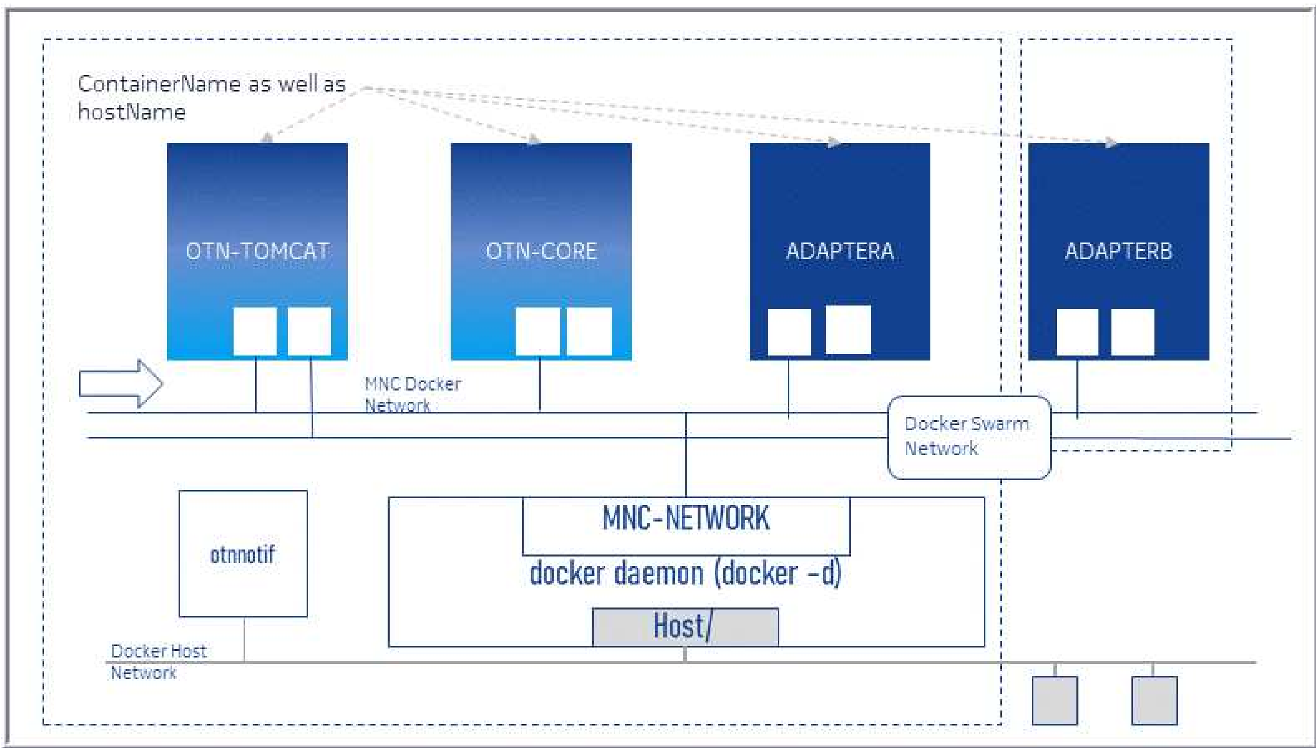


Docker Networking

The Docker Daemon creates a Docker network and a bridge between External Host Network and private container network. In this private network, each container is a *host* and is known by its name. All containers are in the private network. When specific ports need to be exposed external to the host to the public networks, containers provide a configuration via *Ports.cfg*

This mapping is used to map the ports between containers and external mapping. Docker Swarm Network is enabled for external EMLs, they all appear to the system as a single network, using container names.

Figure 1-2 Docker Networking



Only Specific ports are exposed to the outside world. When a container needs to expose its ports to the outside world, it is managed through the IPTables in the docker daemon and the port mapping is done there and then exposed to the outside world. For example 8081, 8443 port of Tomcat can be exposed to the outside world with a port mapping on the docker daemon. Some ports, for example in spring remoting between processes, are entirely within the containers and are not exposed to the outside world. These ports are in the NFM-T Network.

Microservices Concept

The microservices concept is intended to design software applications as suites of independently deployable **Services**, so the software architecture can structure applications as a set of loosely coupled, collaborating *Services*.

The NFM-T components are split into microservices deployed in Docker containers.

NFM-T Installation

The NFM-T install and package does not include RHEL OS distribution nor the deployment of the VM instance hosting the Application software.

Note: AID VM used for VMWARE deployment is no more present

The NFM-T Application Install embeds a tool executing the required pre-checks on the compliance of the VM environment. Warning messages alert in case any pre-check fails.

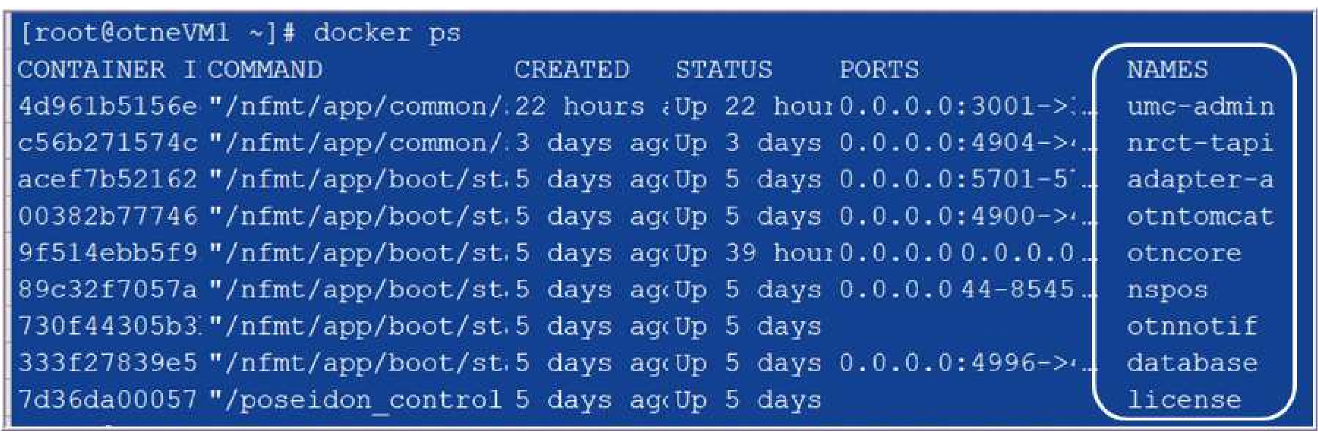
NFM-T Application Install is a tarball including the Docker images plus setup rpms. It includes ORACLE and all other 3rd party SW. The 3rd party components used by applications are deployed into Containers. The docker deployment and configuration is based on *Kubespray* open-source tool and Ansible rules. The Install exploits Ansible models for deployment automation.

Target system configuration is described by Templates, the system customization step is no more required.

Figure 1-3 Installation Commands Example

```
/NFMT-MS-Download/NFMT-MS-Download.pl R20.7 BA /DEPOT rpm
rpm -U /DEPOT/mnc-setup-20.7.0-81.noarch.rpm
/NFMT-MS-Download/NFMT-MS-Download.pl R20.7 BA /DEPOT iso
/nfmt/os/enableSSH.sh 135.250.206.162
vi /DEPOT/nfmt_desc.yml
/nfmt/setup/setup.sh
```

Figure 1-4 Containers Example

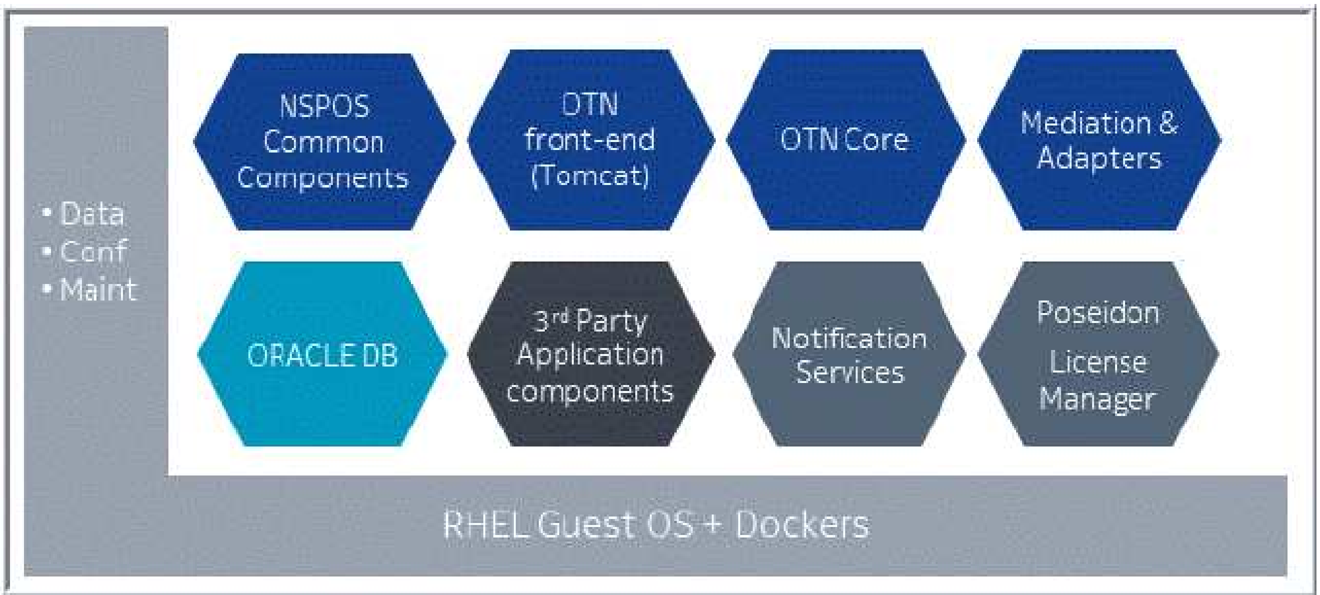


NFM-T architecture

The NFM-T platform architecture is moving from virtual machine environment to containers to manage system splitting in multiple services.

Both Network and Element Layer data are stored in a single Oracle instance, into a dedicated container. The containers are based on Docker technology and all NFM-T containers are still deployed in a single Virtual Machine.

Figure 1-5 NFM-T Architecture - Container



The architecture evolves to an *application-only* schema, that is only NFM-T applications are delivered, the operating system environment is a prerequisite to be compatible to run the NFM-T applications installed.

A single database instance is deployed across distributed EMLs.

In order to reduce the complexity of this architecture, a new architecture has been introduced, focused, and optimized for 1830 PSS networks.

The current configuration is split in different containers: OTN Core, OTN Tomcat, Database, NspOS and the Adapters that can be a maximum of four. The EML is one of the adapters. The containers are collapsed into a *single Virtual Machine* and the EML is one adapter and is located on a different Virtual Machine.

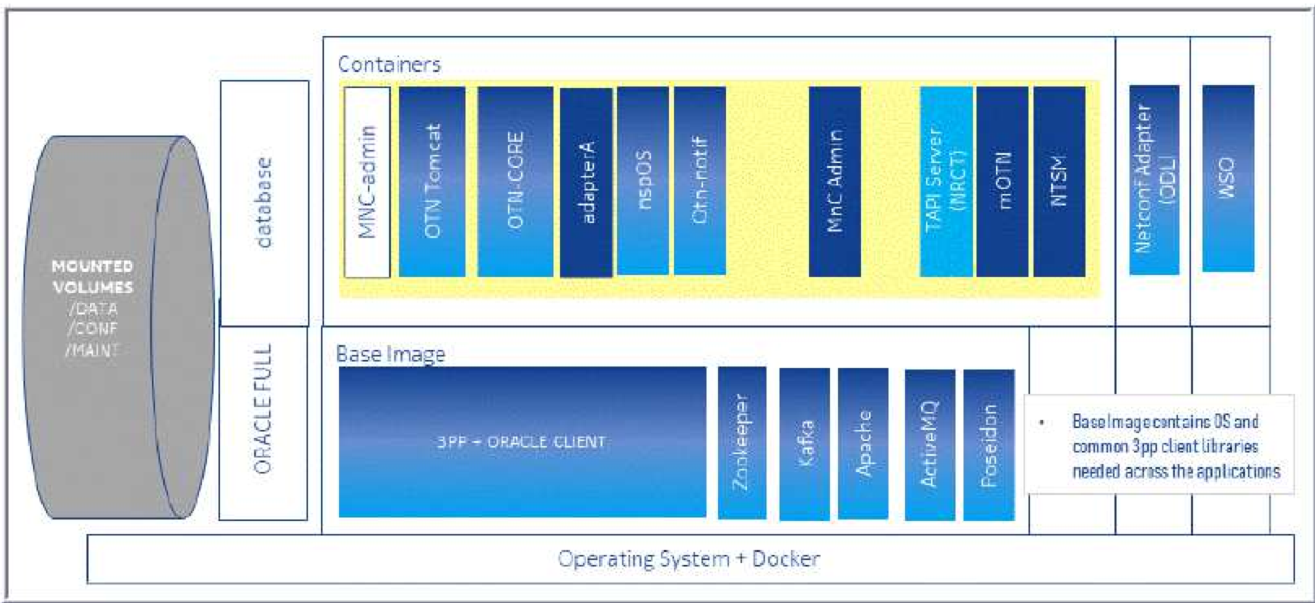
Management and Control (MnC) is a consolidated solution for NFM-T, NRC-T, WSO, and WStS components

Containers in NFM-T

- DATABASE: Oracle processes in this container. Contains all data from NML and external EMLs
- OTNTOMCAT: Main entry point to All User driven functions, Physical Resource Management and Control Plane Management.
- OTNCORE: Managed Plane connection management, Alarm Management, SDH Applications, Performance Management, Log Management, Messaging (Kafka, ActiveMQ, CORBA)

- adapterA,B,C,D: SNMP Adapters, Zic Manager
- nspOS: NSP Core Model, FaultManager, CAS
- mncAdmin: PMC, System Health Monitoring
- WSO
- NRC-T
- SystemPreferences

Figure 1-6 NFM-T Platform Evolution



Optional components

The optional components are installed in additional VMs, according to the following network needs:

EML is required for large or extra large networks, including 1830 PSS NEs, and for PTN networks.

NFM-T OTN

The NFM-T OTN application provides a single network manager for optical GMRE Layer (L0) and electrical GMRE Layer 1 (L1) switching, along with a single database and one provisioning workflow that enables end-to-end connection setup across WDM/photonic and OCS/switching nodes. The integrated Ethernet Service Manager feature of the NFM-T OTN application supports the provisioning of Ethernet switched traffic for the 1830 PSS NEs and provides integrated L0, L1, and L2 transport management.

To support these technical services, the NFM-T OTN application provides users with its own user interface, which is the OTN WebUI. Through the OTN WebUI users can accomplish all element level and network level functions along with performance monitoring and alarm management.

NFM-T supported NEs

The NFM-T supports the Nokia family of optical NEs. To accommodate the world of optical transmission standards, these NEs operate using different transport structures and they support different native command languages.

Contact your local customer support team for a list of NEs that are supported by the NFM-T and its particular applications.

Important! Each release of the NFM-T and its applications supports certain NEs within the Nokia family of optical NEs. Mention of NEs or specific NE features in the text of this document, or any document in the NFM-T documentation set, that are not supported in this particular product release, can apply to prior or future product releases. Such material may not be currently visible or operable on the GUI and/or the server and has been added only as a convenience for our customers. This material is subject to change. For a list of NEs that are supported in the NFM-T Release 22.6_FP1, contact your Nokia local customer service support team.

NFM-T EML

The NFM-T EML application provides capabilities for both Nokia ANSI and ETSI NEs that are under the management of the application. Its set of protocol adapters support basic NE functions such as NE MIB backup/restore and software downloads.

1.3 NFM-T Modules for System Resiliency

NFM-T HA

The NFM-T supports High Availability (HA) as an added value module, which is referred to as the *NFM-T HA*.

As its name suggests, the NFM-T HA provides *high availability* to these applications whose main task is to manage transport networks. It protects the NFM-T applications and its server platform against hardware and software failures that could be caused by system failures (such as the failure of the system power supply or a system component), a site failure (such as a natural disaster or fire), a backplane failure, a processor failure, or any unplanned outage.

High Availability is typically geographic, so the servers are located in different sites called NOC (Network Operation Centers) and DRC (Disaster Recovery Center).

NFM-T HA is supported on both KVM and VMWARE virtualization.

A Fast switch, that is less than 5 minutes, is possible having the protecting unit in warm standby and real time replication of data.

The NFM-T HA is explained in detail in the *HA Guide* (3KC73819GAAA). This document includes installation, administration, and user information for the NFM-T HA feature.

Contact your Nokia local customer service support team for additional details.

Understanding the Technologies

1.4 WDM Overview

WDM definition

WDM, which is *Wavelength Division Multiplexing*, is a multiplexing technique that is used to increase the bandwidth of a single mode optical fiber, which enables the simultaneous transport of several different signals on one fiber. The optical multiplexing technique that is used in WDM is formatted as well as protocol independent, which enables the transport of different signal formats on different wavelengths at the same time.

The WDM signal

The WDM signal is composed of client signals that are multiplexed onto the same optical fiber. Each client signal is transported into a well-defined wavelength, usually identified as a *lambda*.

For example: Up to 80 channels (+ 1 supervisory channel, when its supported) are transported on the same optical fiber.

The digital client signal that is transported at the WDM layer is identified in the OTN by the client endpoints of the paths that are managed at the WDM level. These paths are referred to as *client paths*.

A client path maps a logical physical connection in the network in the WDM layer. Typically, the client path supports several paths crossing the OTN network.

The client path can also represent the transport end-service that is delivered by an operator, only if the OTN network is managed by the NML OS or only if the specific terminating non-DWDM NEs are managed by another NML OS.

The client path concept is a way to define the generic *server provided by the optical transport network*.

When *a network is the client of the OTN network*, the WDM client path is the service that is provided by the OTN to the network, which looks at it as a physical connection that joins two NEs at the extremities of the WDM section.

Digital client signals and WDM layering

The digital client signal must be *colored*, which means that it must be transmitted with the wavelength that has been assigned to its channel. This transmission operation is performed by specific boards called *transponders* or *Wave Length Adapters (WLAs)*. If the signal source is already colored in the client equipment through colored interfaces (specific transmission boards) this transmission operation might not be necessary.

When a digital client signal is transported through the WDM layer, the following occurs:

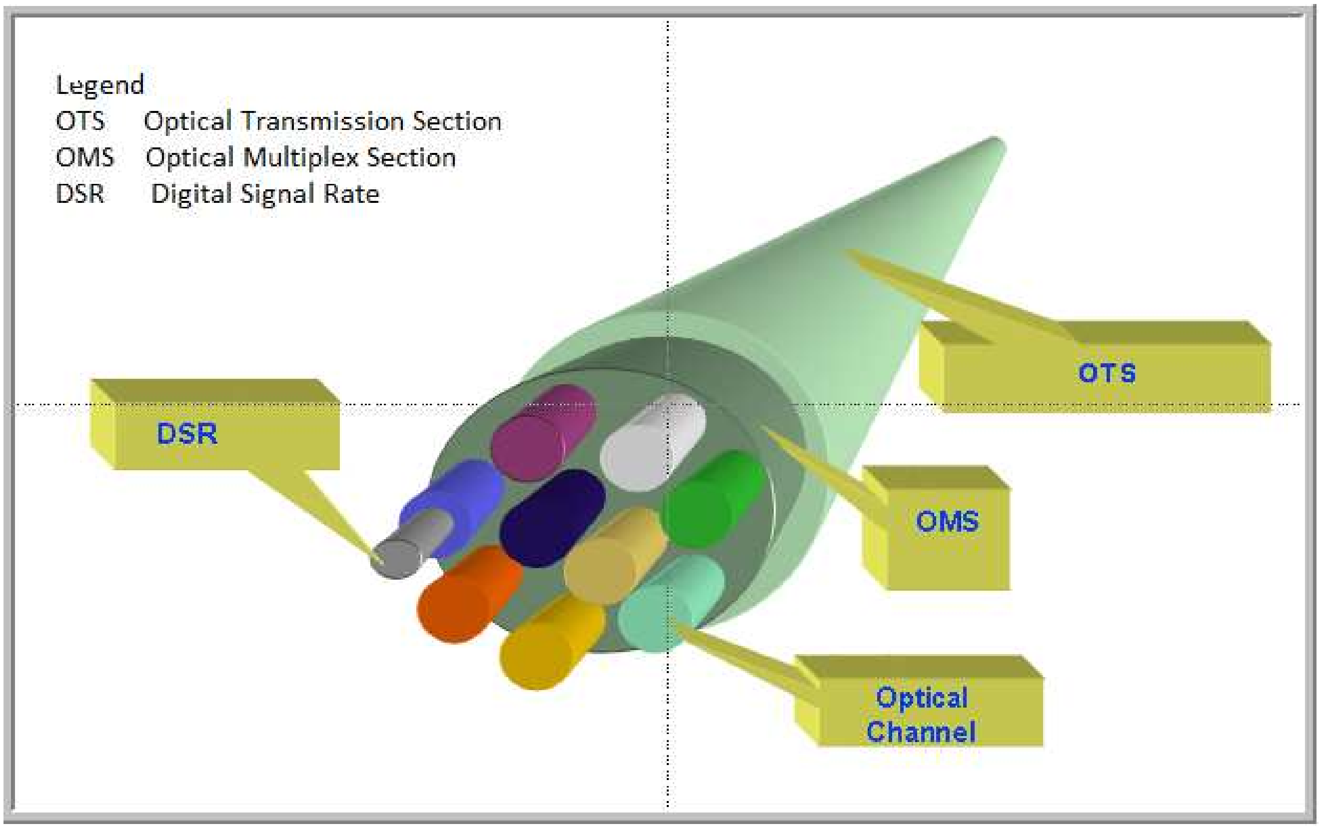
- The colored signal belongs to the optical channel (OCH) layer.
- The optical channels that compose the WDM signals are multiplexed into the WDM signal.
- The multiplexed signal belongs to the Optical Multiplex Section (OMS) layer.
- The signal is transported along the optical fiber until it is extracted to upper layers.

- The signal interfaced with the optical medium belongs to the Optical Transmission Section (OTS) layer.

When a single optical channel (without a supervisory channel) is transported along the optical fiber, the OMS layer is skipped and the OTS layer is named the Optical Physical Section (OPS) or the Optical Section (OS).

By extension of this concept, related to mono-lambda signals, in a WDM layer, the ports of WLA boards are identified as OPS ports and the physical connections connecting the NEs are identified as OPS physical connections.

Figure 1-7 WDM Overview – WDM Layering



Topological components

A *network* is the highest level of partitioning that the NFM-T manages.

A *subnetwork* is the second highest level of partitioning that the NFM-T manages. A network can consist of more than one subnetwork.

A *node* represents a *network element* or a group of network elements.

A *physical connection* is the logical representation of fibers and coaxial cables that exists between network ports. For example: The physical connection that is delimited by two network ports, such as two OTS physical ports.

An *end point* is a port, physical connection, link connection, infrastructure connection, or service.

Add/Drop Multiplexer

An Add/Drop multiplexer is a device installed at an intermediate point on a transmission line that enables new signals to come in and existing signals to go out. In a typical example, most signals pass through the device, but some would be *dropped* by splitting them from the line. Signals originating at that point can be *added* into the line and directed to another destination. Add/Drop multiplexing can be done with optical or electronic signals. The device may deal only with wavelengths, or it may convert between wavelengths and electronic TDM signals. The setup in an Add/Drop multiplexer is generally static, and the device is not reprogrammed very often.

Note that the new signal being added can use the same optical channel (wavelength) as the dropped signal.

The optical Add/Drop multiplexer (OADM) is a device used to insert (add) or extract (drop) a specific wavelength, for example a channel, in wavelength division multiplexing (WDM) communication systems. Being a key component of all-optical nodes, its functionality has been obtained in many ways.

Reconfigurable Optical Add/Drop Multiplexer

Regardless of the context, a ROADM is a subsystem, large or small, that allows for the dynamic configuration of how wavelengths add, drop or pass through the subsystem.

Reconfigurable optical Add/Drop multiplexers (ROADMs) are crucial to wavelength division multiplexing (WDM) networks because they support dynamic photonic layer switching without manual intervention. The next generation ROADM requires three main features: colorless, directionless and contention-less (CDC).

The photonic switching configuration supports colorless, directionless, contentionless with Flexgrid (CDC-F) wavelength routing.

Colorless means that any wavelength channel on an express fiber may be directed to any transponder associated with that fiber. A colorless transponder includes a pair of transmitter and receiver to Add/Drop traffic without any color limitation.

Directionless means that all transponder banks be shared among all wavelength channels from any nodal degree (where N denotes the number of input/output fibers). Contention-less means that the setup of the cross-connects between input and output fibers and Add/Drop ports does not prevent other cross-connects from being setup.

1.5 Understanding the OTN

Overview

OTN is a set of optical network elements connected by optical fiber links capable of providing optical channel transport, multiplexing, routing, management, supervision, and survivability.

Introduction

Before any of the provisioning concepts that are used in the management of an Optical Transport Network (OTN) can be fully understood, the layered architecture that is implemented in an OTN must be examined, considered, and understood.

How we evolved to OTN

The evolution from PDH to Optical Transport Network (OTN) has progressively grown from the 90s up today as a natural path to provide a converged transport solution for TDM and packet based services (Ethernet, IP, ATM) and further to offer the required greater flexibility for new services and transport technology.

If PDH is absolutely not able to sustain and manage the huge traffic demand requested today and in the nearest future as well, SONET/SDH was designed with only two levels of switching at 1.5/2 Mbps and 50/150 Mbps providing a restricted level of scalability and transparency.

On the contrary, OTN, primarily designed to transport SONET/SDH, also supports a number of other clients including ATM (Asynchronous Transfer Mode), Ethernet, Fiber Channel (FC), IP, MPLS, and GFP (Generic Framing Procedure).

The OTN network if compared with the SONET/SDH network, offers several advantages: the transparent transport of the client signal, the switching capabilities and more effective tools for management and supervision.

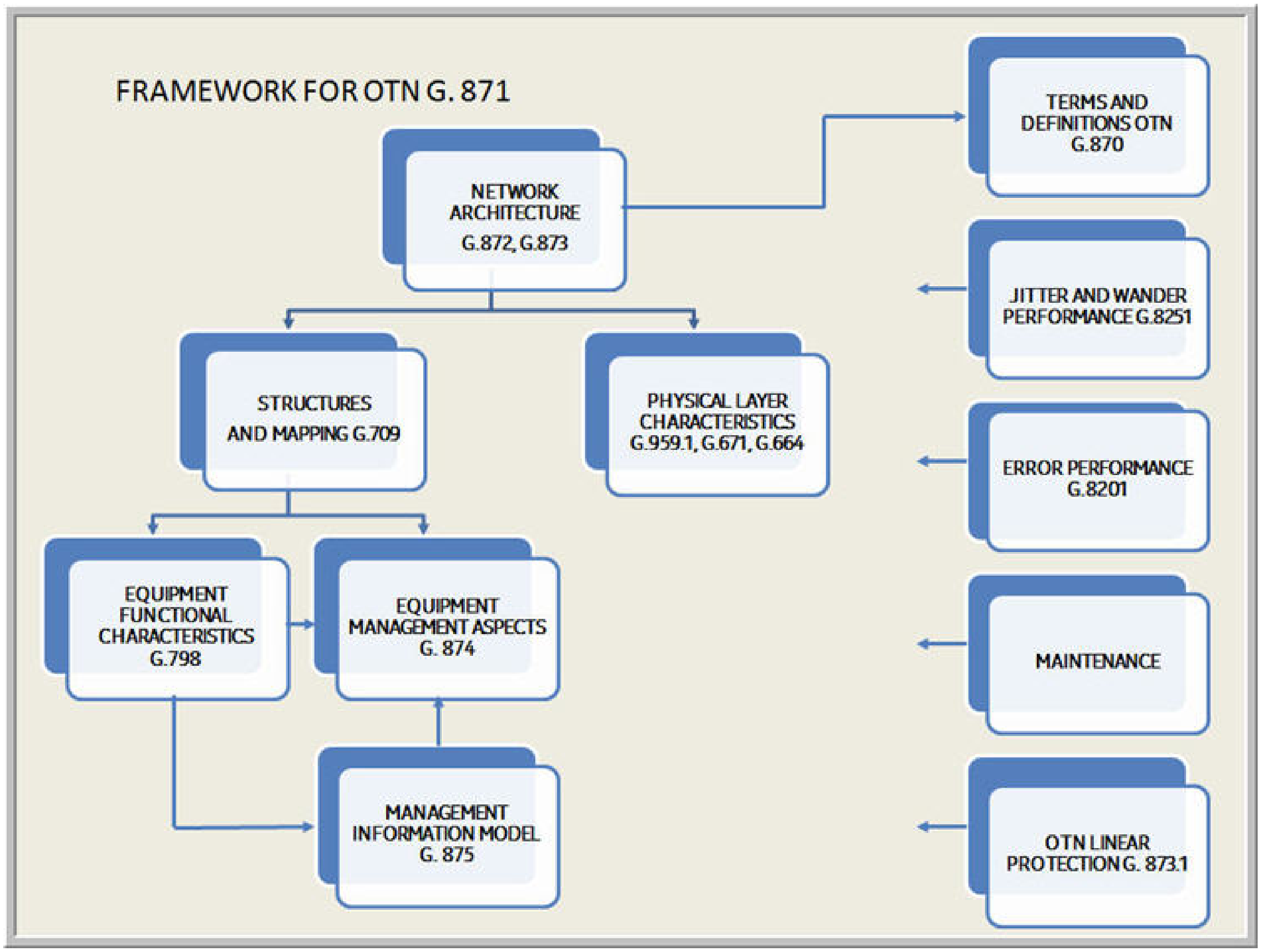
The ITU-T conceived and implemented a set of recommendations to establish, define and set up all the parameters involved in the OTN. The framework of OTN encompasses the series of standards created to combine the benefits of SONET/SDH with the bandwidth-expanding capabilities of DWDM in order to build more network functionality into Next Generation optical networks.

ITU-T framework for OTN recommendations

The OTN environment, is structured according to a framework of specifications.

The ITU-T G.871 defines the *Framework for Optical Transport Network* and provides an overview of the different recommendations. Figure 1-8, “OTN specifications” (p. 134) highlights how this framework is composed of as well as a short description of each ITU-T recommendation.

Figure 1-8 OTN specifications



The ITU-T G.872 and ITU-T G.873, describe the architectural aspects of an OTN. The former describes the *layered network structure* including client/server associations, network topology, signal transmission multiplexing and routing, the latter defines OTN applications including interconnection with other networks. While, the ITU-T G.870 provides an overview about OTN terms and definitions.

Based on the signal structures and mappings, the ITU-T G.709 describes the *network node interfaces* necessary to enable the interconnections of OTN network elements and to transport the client signals in the OTN. Mainly there are two interfaces used in OTN:

- The user-to-network interfaces (UNI), which are the demarcation points between the responsibility of the service provider and the responsibility of the subscriber.

- The network-to-network interfaces (NNI), which are interfaces that specify the signaling and management functions between two networks.

The ITU-T G.709 Recommendation defines these interfaces of the OTN that are to be used within and between the subnetworks of the optical network, in terms of the following components:

- the optical transport hierarchy (OTH), which supports the operation and management aspects of optical networks of various architectures such as point-to-point, ring, and mesh architectures
- the functionality of the overhead to support of multi-wavelength optical networks
- frame structures
- bit rates
- formats for the mapping client signals.

Several recommendations cover the physical layer:

- ITU-T G.959.1 provides *Interface Specifications*
- ITU-T G.671 describes the *Transmission Aspects* related to components for OTN equipment
- ITU-T G.664 describes *Optical Safety Procedures* and requirements

Based on the ITU-T G.709, ITU-T G.798 describes the *Functional Characteristics* of the equipment containing OTN layers.

Complementing ITU-T G.798, the recommendation ITU-T G.875 describes the *Management Information Models* for the network elements belonging to OTN.

In addition, ITU-T G.874 defines the Management Aspects of Optical Network Elements (ONE), specifying: management functions for fault management, configuration management and performance monitoring, regardless of the client.

The scope of the other recommendations is to describe: Jitter and Wonder performance, Error performance parameter and Maintenance and OTN Linear protection schemes.

OTN structure

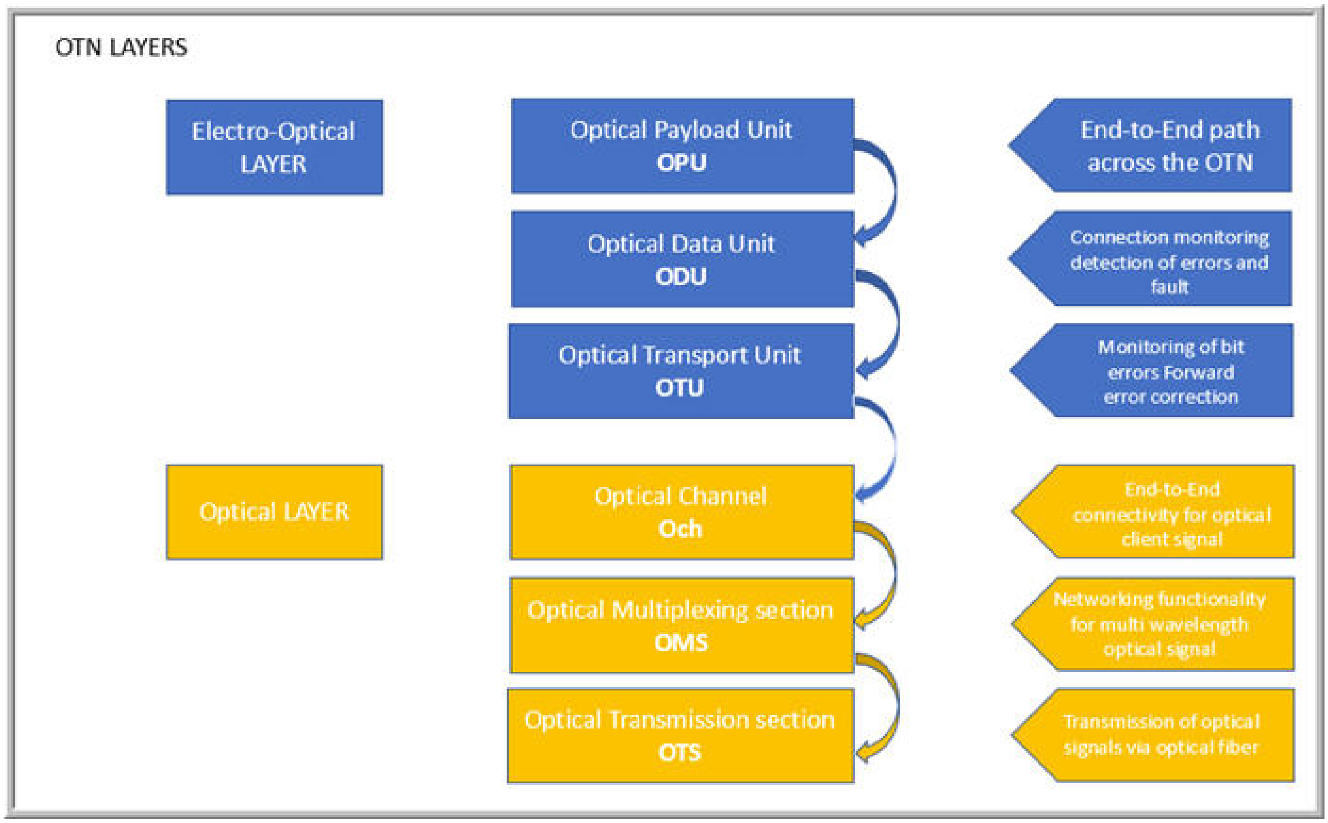
The OTN structure as defined in the ITU.T G.709, is based on layers. Mainly the structure is composed of two layers named *Electro-Optical Layer* and *Optical Layer*.

The Electro-Optical Layer contains overhead for managing end-to-end paths across the OTN, monitoring connections and monitoring faults and bit errors. The Forward Error Correction mechanism is implemented in the Electro-Optical Layer.

The Optical Layer represent the complete optical network consisting of optical network elements such as optical cross connects, optical add/drop multiplexers, optical amplifiers and wavelength division multiplexers. The Optical Layer expands the WDM functionalities to provide end-to-end network management capabilities for the optical signal. It transports signals using optical channels. Overhead information for reporting defects in the optical signal and to enable management is transmitted as well.

The following figure details the OTN structure.

Figure 1-9 OTN Structure



Electro-Optical Layer

The *Electro-Optical* Layer is composed of three functional layers:

The client signal is mapped into the *Optical Payload Unit (OPU)* layer. The OPU path connects the client equipment in an end-to-end manner and is not changed inside the OTN. The OPU overhead specifies the structure of the payload signal.

The *Optical Data Unit (ODU)* layer adds optical path-level monitoring of the end-to-end OPU paths. It enables detection of faults and bit errors and Tandem Connection Monitoring (TCM). TCM enables the transmission of bytes for connection monitoring, this information can be used for protection switching purpose.

The *Optical Transport Unit (OTU)* layer monitors bit error and faults and adds additional information for the Forward Error Connection (FEC).

Optical Layer

The *Optical Layer* is composed of following functional layers:

- Optical Channel (OCh) layer
- Optical multiplex section (OMS) layer

- Optical Transmission Section (OTS) layer

The *Optical Channel (OCh)* layer establish end-to-end connectivity for the transparent transmission of the different optical client signals. The OCh layer corresponds with the OTU layer of the Electro Optical layer, practically it covers the same network parts of the OTU layer. The OCh layer uses a single wavelength also referred as “λ” to transport the OTU layer. The OCh layer includes overhead information which is transmitted in a separated optical channel called *Optical Supervisory Channel (OSC)*.

Multiplexing several optical channels creates the optical multiplex section (OMS) layer. It provides networking functionality for the transmission of a multi-wavelength optical signal. The OMS layer includes overhead information for operation and management. This overhead is transmitted in the OSC as well.

The *Optical Transmission Section (OTS)* layer provides transport function for the OMS layer signal. There is a one-to-one mapping between both layers.

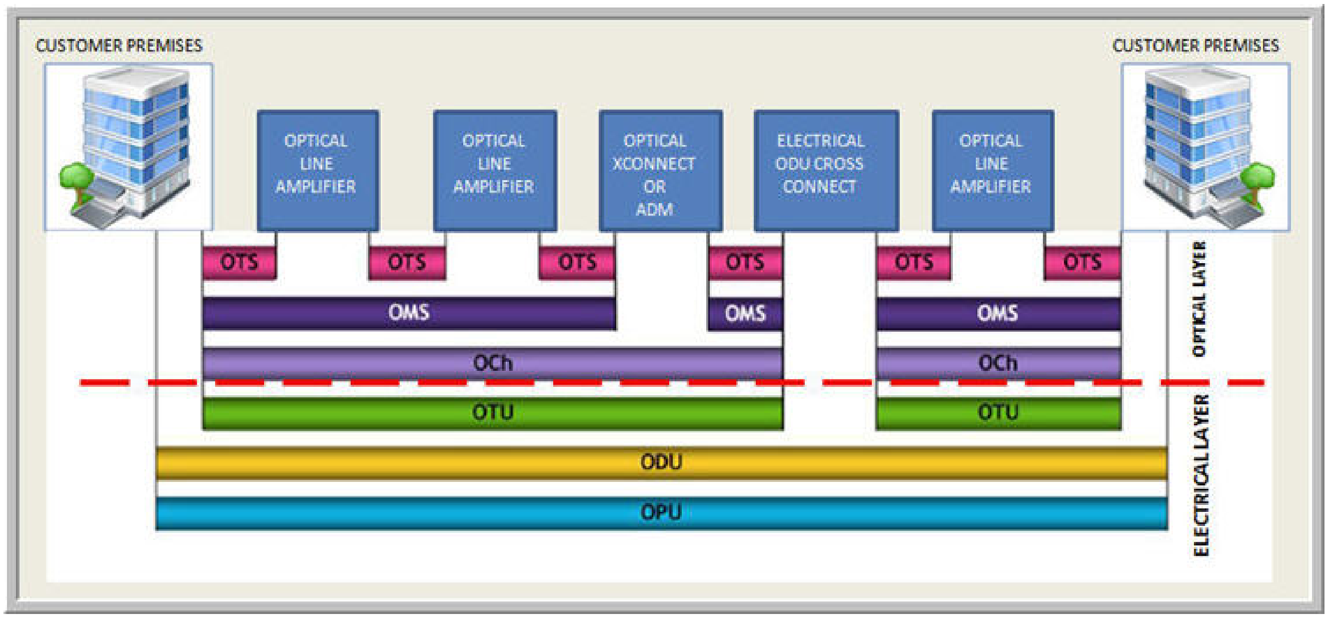
The OTS defines the optical parameter of the physical interface such as frequency and power level. The optical transmission section layer includes overhead bytes for maintenance and management purposes, which are transmitted in the optical supervisory channel together with the overhead of the optical channel layer and optical multiplex layer.

OTN layers interaction

The Figure 1-10, “OTN Layers Interaction” (p. 138) and the below explanation is a theoretical example of how the OTN layer is applied to an OTN network. For some configurations this scheme does not represent the normal way of operating of NFM-T.

For example, in NFM-T the OMS connection does not cover the OTS connection of external NEs, with the exception for the OLP configuration. Moreover, NFM-T does not model the OPU layer and merge that with the ODU; it does the same for OTU and OCh.

Figure 1-10 OTN Layers Interaction



The client access (CA) equipment, at the customer premises, maps the client signal, similar to an STM-N signal, into the OPU and creates the OTH signal. This signal is transmitted through the OTN and terminated at opposite client access equipment.

To cover long distances optical line amplifiers (OLA) are used to amplify the optical signal.

Optical cross-connects or optical add/drop multiplexers are used to switch the optical channels between different ports.

To switch a single ODU signal, which is an electrical layer, it's necessary to terminate higher levels of the signal. This requires optical-electrical conversion, including 3R regeneration. For this operation an electrical ODU cross connect can be used. After switching the ODU, an electrical-to-optical conversion is performed to build the optical OTS signal.

The Optical Transmission Section (OTS) layer with its associated overhead is terminated at each network element and provides transport function for the OMS layer signal. The OTS defines the optical parameters of the physical interface such as frequency and power level.

Optical cross connects or optical add-drop multiplexers switch on optical level only.

They do not perform optical-electrical-optical conversion. Therefore, only the OMS is terminated. If an optical-electrical conversion must be performed, the complete optical section has to be terminated, including the optical channel and OTU path.

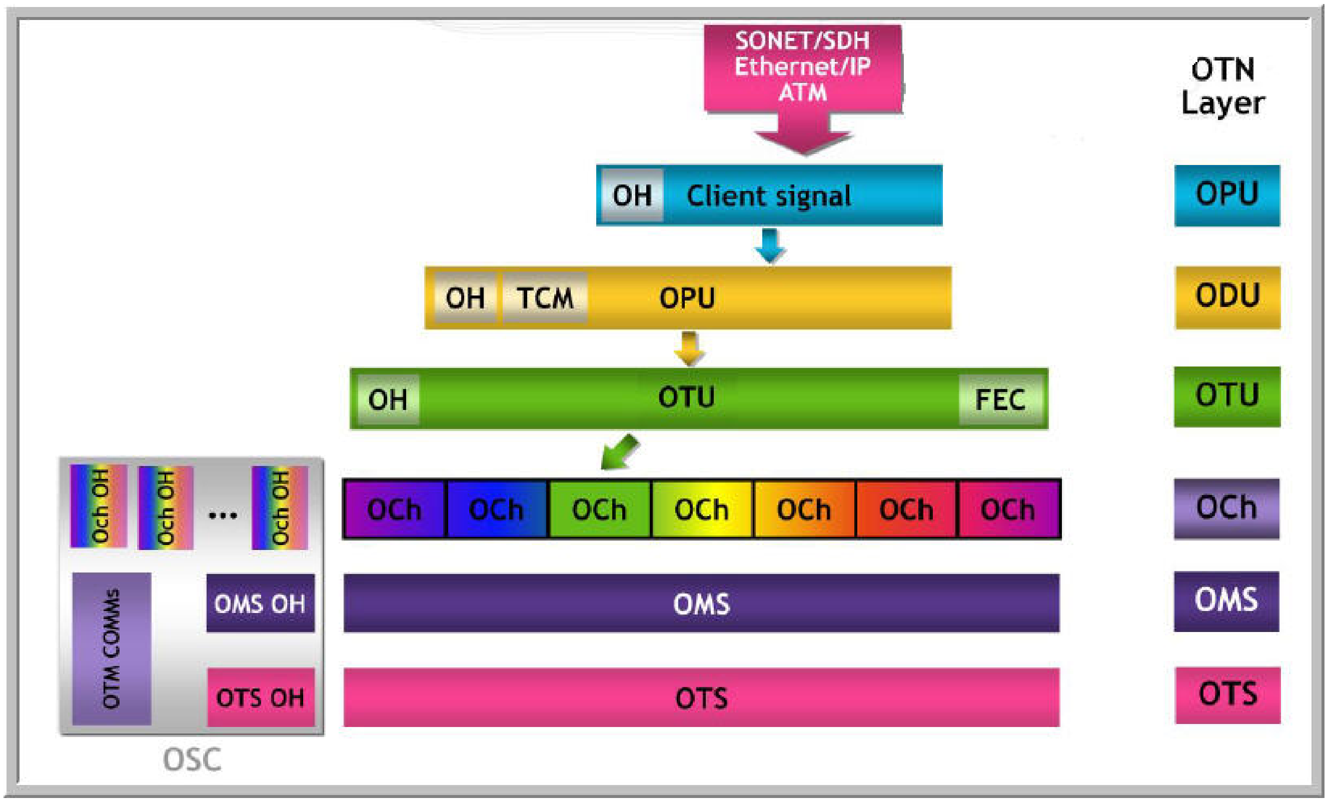
In this example, the ODU and OPU layers are terminated at the client access equipment and not terminated inside the OTN.

OTH multiplexing and mapping

With a mechanism similar to the Synchronous Digital Hierarchy (SDH), signal is multiplexed and mapped within a more complex structure with a prearranged bit-rate. This structure is called *Optical Transport Hierarchy (OTH).*

Refer to the Figure 1-11, “OTH Multiplexing and Structure” (p. 138) for a better understanding of the OTH multiplexing and mapping.

Figure 1-11 OTH Multiplexing and Structure



The client traffic is mapped into the payload area and the overhead bytes are added to form the Optical Payload Unit (OPU).

In the next layer, the OPU is added with overhead bytes and bytes for Tandem Connection Monitoring (TCM) to build the Optical Data Unit (ODU). The ODU, together with overhead bytes and bytes for Forward Error Correction (FEC), represents the Optical Transmission Unit (OTU) that is the last electrical layer. The OTU is then converted into an optical channel of a specific wavelength. Several wavelengths are multiplexed.

Additional overhead bytes for each optical channel are also transmitted on a dedicated channel called Optical Supervisory Channel (OSC).

The Optical Supervisory Channel is also used to host:

- The overhead bytes for the Optical Multiplex Section (OMS).
- The overhead bytes for the Optical Transmission Section (OTS).
- The OTM communication channels for management purposes.

In case of colorless OTN signal, only one optical channel is mapped into an Optical Physical Section (OPS) without any OSC creation. This case is referred to as *Reduced Functionality* compared with the *Full Functionality* where the OSC channel is transmitted.

Going through the layers, the OTU is the last one to expand the description with addition details.

The OTU appears in different levels given in the number “K” which can assume values from 1 to 4 depending on the capacity transported. Refer to Figure 1-12, “Different levels of OTU” (p. 139) for details.

Figure 1-12 Different levels of OTU

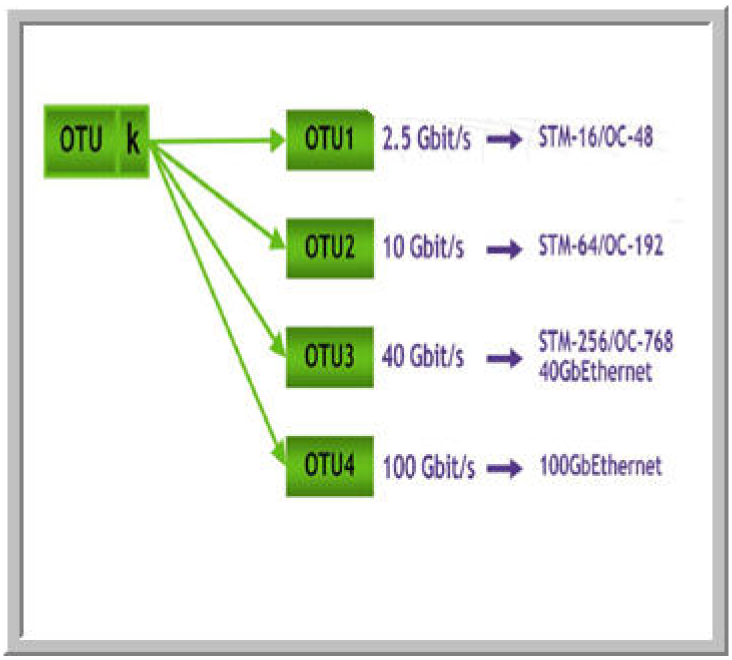
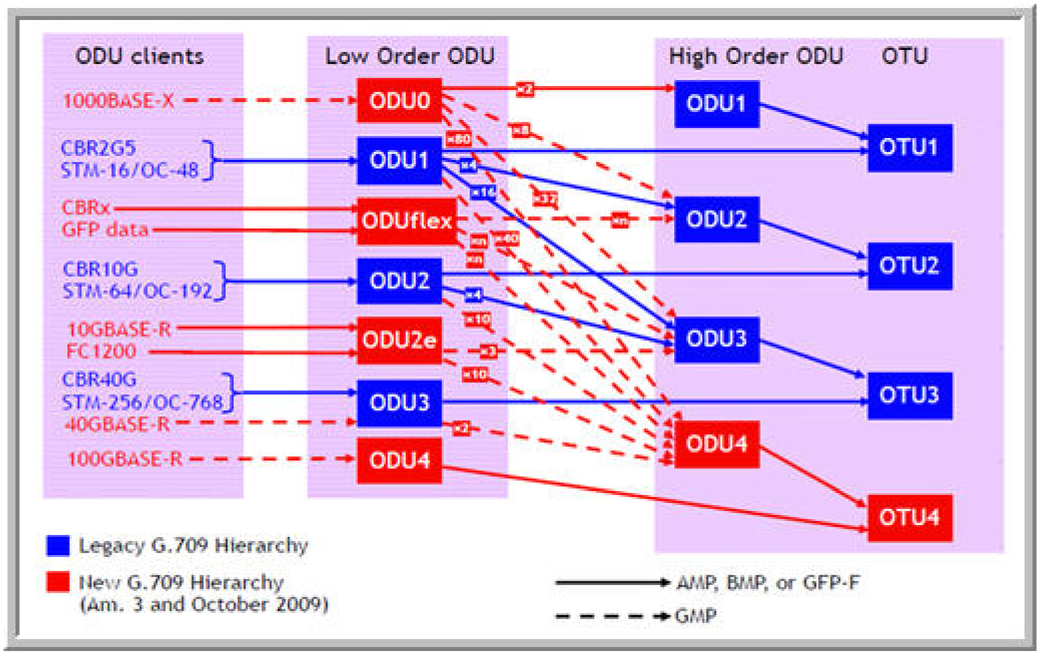


Figure 1-13, “OTU Multiplexing Structure” (p. 141) describes the OTU multiplexing structure. It highlights how the different OTU levels are obtained starting from the ODU client signals.

Figure 1-13 OTU Multiplexing Structure



OTN Photonic and electrical transport layers in short

The OTN and/or the WDM transport network provides the end-to-end services that are required for the high speed transmission of data. The two main layers in the OTN/WDM transport network are the following:

1. The *photonic layer* of OTN is provided through Wavelength Division Multiplexing (WDM) NEs. Using ITU-standard optical WDM wavelengths, these NEs enable the provisioning of wavelength transport services, which are known as *OCH/OTUk trails*.
2. The *electrical layer* of OTN is provided through both WDM and Optical Cross-connect System (OCS) NEs or only through a network of OCS NEs that carry either the same data rate level as the photonic layer or a lower data rate level that is multiplexed and transported through the photonic layer. At this electrical layer, the Optical Data Unit (ODU) provides the needed infrastructure and adaptation for end-to-end *DSR paths* to carry customer traffic. The ODU is known in OTN layered hierarchy as the following:

   ODUk (k=0 (~1 Gb), 1 (~2.5Gb), 2(~10Gb), 3 (~40Gb), 4 (~100Gb))

The Table 1-1, “ODUk Rates and the Signals/Packets Typically Transported” (p. 142) lists the ODU rate and the signals or packets that are typically transported at a particular rate.

Table 1-1 ODUk Rates and the Signals/Packets Typically Transported

Rate	Data Rate (~Gb)	Typically Transports one of the following...
ODU0	~1 Gb	• A timing transparent transcoded (compressed) 1000BASE-X signal • A stream of packets (such as Ethernet, MPLS or IP) using GFP
ODU1	~ 2.5 Gb	• Two ODU0 signals • A SONET OC-48 signal • A SDH STM-16 signal • A stream of packets (such as Ethernet, MPLS or IP) using GFP
ODU2	~ 10 Gb	• Up to 8 ODU0 signals • Up to 4 ODU1 signals • A SONET OC-192 signal • A SDH STM-64 signal • A WAN PHY (10GBASE-W) • A stream of packets (such as Ethernet, MPLS or IP) using GFP
ODU2e	~ 10 Gb	• A 10GBase-R Ethernet signal • A timing transparent transcoded (compressed) Fibre Channel 10 GFC signal
ODU3	~ 40 Gb	• Up to 32 ODU0 signals • Up to 16 ODU1 signals • Up to 4 ODU2 signals • A SONET OC-768 signal • A SDH STM-256 signal • A timing transparent transcoded 40GBASE-R Ethernet signal • A stream of packets (such as Ethernet, MPLS or IP) using GFP
ODU3e2	~ 40 Gb	• Up to 4 ODU2e signals • Up to 4 10GBase-R Ethernet signals
ODU4	~ 100 Gb	• Up to 80 ODU0 signals • Up to 40 ODU1 signals • Up to 10 ODU2 signals • Up to 2 ODU3 signals • A 100GBASE-R Ethernet signal
ODUflex (CBR)	Any Configured Rate	• A constant bit rate signal such as Fibre Channel 8GFC, InfiniBand, or Common Public Radio Interface

Table 1-1 ODUk Rates and the Signals/Packets Typically Transported (continued)

Rate	Data Rate (~Gb)	Typically Transports one of the following...
ODUflex (GFP)	Any Configured Rate	• A stream of packets (such as Ethernet, MPLS or IP) using GFP
Generic Framing Procedure (GFP) is a multiplexing technique defined by ITU-T G.7041 that allows the mapping of variable length, higher-layer client signals over a circuit switched transport network like OTN, SDH/SONET, or PDH.		

OTUCn

In G.709 [ITU-T_G709_2012], the standard mechanism for transporting a client signal is to first map it into an ODU signal (of the appropriate rate), and then switch the resulting ODU signal through the OTN network.

In the course of its traversal through the OTN network, the ODU signal generated by the mapper is either:

(a) multiplexed into higher-order ODU, and then encapsulated to form an OTU or

(b) directly encapsulated into an OTU signal that defines the section layer.

Option (b) is only possible for ODU1/ODU2/ODU3/ODU4. ODU signals with other rates, such as ODUflex, must first be processed using option (a). The term "client signal" is generic in the sense that it encompasses both Constant Bit rate (CBR) clients (e.g. 10GBASE-R, SONET OC-768), or packet traffic -- where the goal is to transfer the payload from end-to-end (without regard for bit transparency at the PCS layer). Given that OTU4 was the highest rate section layer signal supported in [ITU-T_G709_2012], the client signal rates were limited to be less than 100G (if ODU-VCAT was not used).

In order to carry client signals with rates greater than 100 Gbps, [ITU-T_G709_2016] takes a general and scalable approach that decouples the rates of OTU signals from the client rate evolution. The new OTU signal is called **OTUCn**; this signal is defined to have a rate of (approximately) n*100G.

The following are the key characteristics of the OTUCn signal:

- The OTUCn signal contains one ODUCn, which in turn contains one OPUCn signal. The OTUCn and ODUCn signals perform digital section roles only (see [ITU-T_G709_2016]:Section 6.1.1). The OTUCn and ODUCn are seen as being analogous to the regenerator section, and multiplex section in SDH respectively.
- The OTUCn signals can be viewed as being formed by interleaving n OTUC signals (where are labeled 1, 2, ..., n), each of which has the format of a standard OTUk signal without the FEC columns (per [ITU-T_G709_2016]). The ODUCn, and OPUCn have a similar structure, they can be seen as being formed by interleaving n instances of ODUC, OPUC signals (respectively) The OTUC signal contains the ODUC, and OPUC signals, just as in the case of fixed rate OTUs defined in G.709 [ITU-T_G709_2016].
- Each of the OTUC *slices* have the same overhead (OH) as the standard OTUk signal in G.709 [ITU-T_G709_2016]. The combined signal OTUCn has n instances of OTUC OH, ODUC OH, and OPUC OH.

- The OTUC signal has a slightly higher rate compared to the OTU4 signal (without FEC); this is to ensure that the OPUC payload area can carry an ODU4 signal.

ODUCn

The ODUCn signal [ITU-T_G709_2016] can be viewed as being formed by the appropriate interleaving of content from n ODUC signal instances. The ODUC frames have the same structure as a standard ODU -- in the sense that it has the same Overhead (OH) area, and the payload area -- but has a higher rate since its payload area can embed an ODU4 signal. The ODUCn signal can be formed in one of the following ways:

- By multiplexing lower-rate (i.e. both low-order and high-order) ODUk signals.
- Each of the n instances of ODUC can carry the NULL signal (as specified in [ITU-T_G709_2016]: Section 17.5.1)
- Each of the n instances of ODUC can carry the PN-11 PRBS test sequence (as specified in [ITU-T_G709_2016]: Section 17.5.2)
- It is conceivable that vendors might implement proprietary mappings (Payload Type values of 0x80-x8F) of non-OTN client signals. An interoperable control plane cannot make use of these proprietary ODUCn signals.

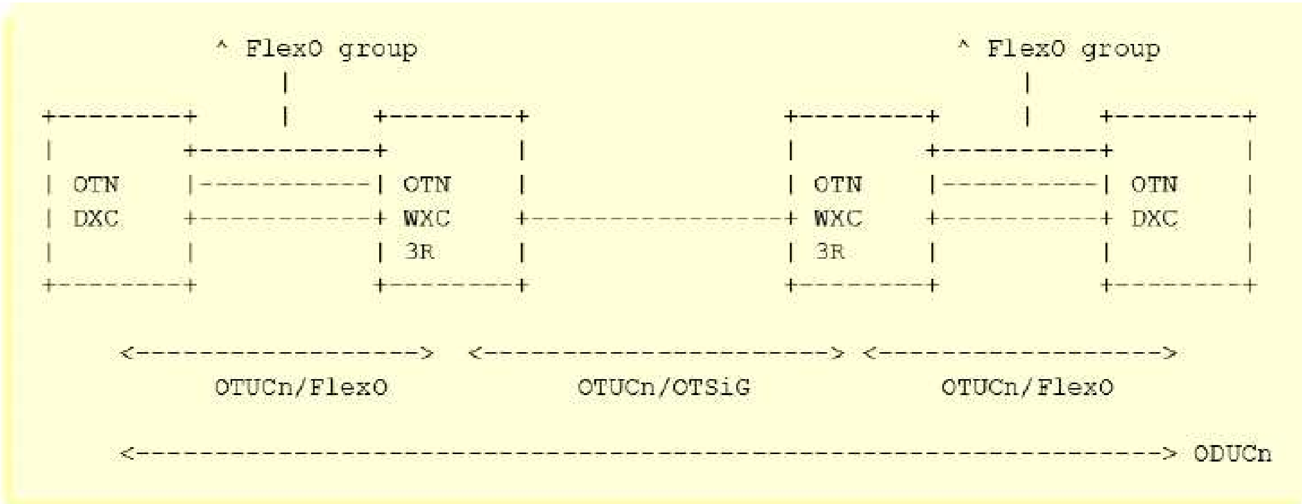
Table 1-2 ODUCn rates

ODU Type	ODU Bit Rate
ODUCn	n x 239/226 x 99,532,800 kbit/s = n x 105,258,138.053 kbit/s

The ODUCn is a multiplex section ODU signal, and is mapped into an OTUCn signal which provides the regenerator section layer. In some scenarios, the ODUCn, and OTUCn signals will be co-terminous, i.e. they will have identical source/sink locations. [ITU-T_G709_2016] and [ITU-T_G872] allow for the ODUCn signal to pass through a digital regenerator node which will terminate the OTUCn layer, but will pass the regenerated (but otherwise untouched) ODUCn towards a different OTUCn interface where a fresh OTUCn layer will be initiated (see Figure 3). In this case, an ODUCn LSP needs to be set up to traverse the three OTUCn segments.

Specifically, the OPUCn signal flows through these regenerators unchanged. That is, the set of client signals, their TPNs, trib-slot allocation remains unchanged. Note however that the ODUCn Overhead (OH) might be modified if TCM sub-layers are instantiated in order to monitor the performance of the repeater hops. In this sense, the ODUCn should not be seen as a general ODU which is switched using an ODUk cross-connect.

Figure 1-14 Multi-hop ODUCn signal



ITU G.709 is amended and ODUflex is introduced

In the Optical Transport Network (OTN), the *Optical Data Unit*, or *ODU*, is the transport container defined to carry client signals from network ingress to egress. The ODU provides a payload area for client data along with overhead for performance monitoring and fault management. The payload area of an ODU may contain a single non-OTN signal as a client or may contain multiple lower rate ODUs as clients.

The existing ODU rates were not efficient to transport these new clients non-OTN client signals like STM-16/64/256 and GbE,10GbE or 100GbE; then, the concept of a flexible rate ODU, or *ODUflex* was devised to fill in the gaps of the fixed rate hierarchy and included in the third version of G.709.

The current, new OTN hierarchy and the mapping between hierarchy levels are illustrated in Figure 1-13, “OTU Multiplexing Structure” (p. 141).

1.6 NFM-T OTN Overview

The NFM-T OTN as a NML management system

The NFM-T OTN, an application of the NFM-T, is an MNL system that manages Nokia NEs. It is fully compliant with the ITU-T Recommendation G.709, which is the Optical Transport Hierarchy (OTH) standard for the transparent transport of services over optical wavelengths in DWDM systems.

The NFM-T OTN is based on the functional modeling concepts of Multi-Technology Network Management (MTNM), which is an NML-EML interface that is heavily based on ITU-T Recommendations G.805 and G.852.2 from the TeleManagement Forum (TMF).

The NFM-T OTN application provides a single network manager for optical GMRE Layer (L0) and electrical GMRE Layer 1 (L1) switching. It has a single database, one connection inventory list, and one fault correlation engine.

Its provisioning workflow enables end-to-end connection setup across WDM and OCS nodes. The NFM-T OTN functions in the managed plane, the GMPLS/ASON control plane, and mixed planes.

NE management

The NFM-T OTN application supports all Nokia 1830 PSS Network Elements (NEs), which include the families of WDM/Photonic (PHN) NEs, the electrical/OCS NEs, and the access/edge NEs.

The NFM-T OTN application provides an end-to-end connection management solution for these NEs. NE provisioning is a simple process of creating an NE, inserting its OS address, and *starting supervision* to establish communication between the NE and the network management system.

EPT support

The NFM-T OTN application supports the use of the Engineering and Planning Tool (EPT) to design and plan the user's network. Use of the EPT enables users to define the equipment that will be required to meet the demands of the current network and to support future demands that are not required during the first phase of deployment.

The EPT produces separate commissioning files for each system in the network. The data in these commissioning files, which are called *EPT Plan files*, provides minimum and maximum values for span losses, port-to-port losses between Wavelength Tracker detection points, and amplifier gains. Users can export the EPT Plan file to be used during the Commissioning and Power Balancing phase of their installation.

Layer support

When all physical connectivity is completed, the graphical map of the NFM-T OTN GUI affords users with an end-to-end view of all layers.

The NFM-T OTN supports logical connectivity at the following rates:

- OCH, which is an Optical Channel, is an optical logical connection without a specific rate. An OCH typically carries alien wavelengths.
- For an Alien Wavelength Bank connection the default signal rate is OTS and the connection is

created on the same OTS rate. However, for the Alien Wavelength connections, we change the signal rate from OTS to OCH.

- For an Alien Wavelength Bank connection, only Unkeyed + Manual wavekey type is supported. Before creating Alien Wavelength Bank connections, external topological link should be created on ADT ports for IROADM9R/IROADM32LP/IR9/IR9LP packs.
- Incase of Control Plane Scenarios, Alien Wavelength Bank connections should be created by making the **ASON Routed** field unchecked and **Allow ASON Resources** field checked. It is a foreign connection for ASON.
- OTUk, which is an Optical channel Transport Unit-k, translates the incoming signals to the appropriate wavelengths for multiplexing and performs signal regeneration and functions such as performance monitoring. An OTUk typically terminates on the line ports of OT packs.
- ODUk, which is an Optical Data Unit, where *k* represents the layer rate being carried and k=2 (10G), 3 (40G), 4 (100G).
- OMS, which is an Optical Multiplex Section, is a logical connection that rides on an OTS connection. The NFM-T OTN automatically creates OMS link connections based on the creation or discovery of an OTS connection.
- OMSBand refers to a subset of wavelengths (lambdas) that are multiplexed and are carried within an NE like in the 1626LM NE.
- DSR is a Digital Signal Rate that carries data services.

Optical power

Specific NEs set up the initial targeted optical power at each monitoring point, and then the NFM-T OTN receives the optical power set-up data and implements the routes at the network. Wavelength Tracker, which is only available on supported NEs, allows an optical power display at the optical channel level.

The NFM-T OTN supports the following:

- Per span (OTS) optical channel power display
- Per channel connection (OCH) power display

Common PM and FM

The common performance monitoring of the NFM-T provides for performance-related data collection from NEs, automatic or manual stopping/starting of performance monitoring, and TCA profile settings.

The common alarm correlation of the NFM-T provides alarm enabling/disabling, collection, correlation and root cause analysis to the NFM-T OTN application, along with setting ASAPs and TCA alarm/alert monitoring.

2 OTN Network Provisioning

2.1 Overview

Purpose

This chapter contains the conceptual content that users need to understand how to provision the NFM-T OTN network on the NFM-T system.

Contents

Understanding Provisioning

2.2 NFM-T OTN Provisioning overview

Provisioning definition

Provisioning is the act of making services available, or *providing* services, to end users through optical networking equipment such as NEs and controlling the particular services that are available to these users.

Provisioning the NFM-T OTN requires knowledge of preset installation parameters and involves both automatic and manual methods that include adding network equipment, connecting network equipment, and associating the network equipment and the network connection with an endpoint.

In addition, NFM-T OTN provisioning requires both the initial creation of services and the ongoing operational maintenance of those services.

Installation parameters and provisioning

Installation parameters are the variables that control the behavior of the NFM-T OTN and are set during the installation of the system. Some installation parameters control the provisioning parameters and the parameter values that are displayed to users as *fields* on the NFM-T OTN NFM-T GUI.

Installation parameters are explained in the *Administration Guide: System Maintenance and Troubleshooting*.

Auto Discovery and manual provisioning

Provisioning the NFM-T OTN application involves the following types of provisioning methods:

- With *automatic provisioning*, the NFM-T OTN system initiates the provisioning of system components such as NEs and certain types of connections through its Auto Discovery feature. In addition, the NFM-T OTN system initiates the routing of a connection if users specify automatic routing during connection provisioning.
- With *manual provisioning*, the NFM-T OTN user accesses the NFM-T GUI to provision the NFM-T OTN system.

Consideration: The NFM-T OTN system automatically discovers connections during certain system events, and users manually provision certain connections using the NFM-T GUI.

Initial and operational provisioning

Provisioning the NFM-T OTN system requires both the initial creation of services and the continual operation of those services.

- The *initial provisioning* of the NFM-T OTN system requires the addition of NEs to the network, the power balancing of those NEs, and the creation of connections. Some of this initial provisioning is automatic; the remainder of this provisioning is manual.
- The *ongoing continual operation* of the NFM-T OTN system involves viewing and modification of

the parameters set during the initial provisioning of the NFM-T OTN. In addition, NEs and their associated connections are added to the initial configurations.

Provisioning is a combination of initial provisioning activities and continual operational activities. For example: when you search for NFM-T OTN components and entities to determine their existence before their creation; and after creation, based on further requirements you modify them. The search activity is operational in nature; the creation activity is an initial task; and the modification activity is operational.

Refer to 2.3 "The initial provisioning of the NFM-T OTN" (p. 154) and 2.4 "The continual operation of the NFM-T OTN" (p. 156) for details.

Configuration restriction

Provisioning of end-to-end service through auto routing, in a back to back configuration with falcon packs in the same quadrant of PSS-8 or PSS16II network elements, requires that the corresponding back to back OS connection is inserted as User constraints in the auto routing scenario manually by the user.

2.3 The initial provisioning of the NFM-T OTN

Preliminaries

Ensure and make note of the following to provision the NFM-T OTN :

- *The hardware platform on which their network is built.*

  In particular, for provisioning, familiarize with the NEs that are to be managed in the network and the features that are supported for the NE release that is being managed. Also, about the feature sets of the various packs.

  For information about a particular NE or NE release, refer to the documentation that accompanies the NE.
- *Activities that must be performed at the Topological level and the Element Management Level of the NFM-T*.

  For information on Element Management for other NFM-T applications, refer to the *EML Guide for Specific Networks*.
- *Initial NFM-T OTN log in information*.

  For information on how to log into the NFM-T OTN, see *Administration Guide*.
- *The passwords to their system and the available instances that have been created for each NFM-T application*.

  Information about passwords and the available instances that have been created for the applications can typically be obtained from the local system administrator.
- *The NFM-T OTN installation parameters* that have been configured for their system.

  For information about the NFM-T OTN installation parameters, see *Administration Guide: System Maintenance and Troubleshooting*. In addition, the local system administrator is often knowledgeable about the installation parameters that have been configured for the system.
- *The NFM-T NFM-T GUI and the terminology* that describes the NFM-T and optical networking.

Create NEs

Users can manually add an NE to the system. When an NE is added to the NFM-T, the system performs an automatic syncronization that finds all of the internal links and all of the ports. When an NE is created in the system, the NFM-T OTN system automatically discovers neighboring NEs.

Understand deployment

Before creating network connections, users must completely understand the NFM-T OTN deployment feature for physical connections, infrastructure connections, and services.

The deployment feature consists of all of the administrative data that is associated with a customer service order, and it enables users to track a customer service request through its life cycle and to move the task that is associated with the request forward or backward depending on the state of the request.

Create connections

A *connection* is a generic term that is used to define any electrical or optical connectivity between NEs. Once the NEs have been successfully added to the system and the optical domain is commissioned and power balanced, users can begin to connect endpoints using the NFM-T GUI.

The NFM-T OTN supports different types of connections depending on basic function and the endpoints being connected. For example, physical connections are internal or external connections that use wires, cables, or optical fibers to connect two physical ports; whereas, logical connections, such as infrastructure connections and services, are typically connections between DWDM NEs that span more than one DWDM NE. Different transmission rates, and, for infrastructure connections, services, and link connections, different service types, connection shapes, and protection types define each supported connection.

The NFM-T follows the G.709 standards model and models all appropriate layers in the network according to that standard. After the system automatically discovers some connection types during certain system events, users can then begin to provision one layer at a time starting from the physical layer.

2.4 The continual operation of the NFM-T OTN

Operations overview

Once the initial end-to-end provisioning of the NFM-T OTN system has been completed, the continual operation of the network that has been created begins. Users must monitor optical power, search for and deal with cross connections and inconsistent connections, and make any provisioning adjustments by modifying parameters.

Monitor and measure optical power

Ensuring that the optical power for each wavelength in the transmission is maintained within the required limits is part of the continual operation of the NFM-T OTN system. Users whose NEs support Wavelength Tracker and Optical Power Visualization and who have made Wave Key assignments during the initial provisioning of their networks, can monitor and measure the optical power of their provisioned connections through the NFM-T GUI.

View cross connections and remove uncorrelated cross connections

A cross-connection is an connection within an NE that internally connects one logical port on an NE to one or more logical ports on the same NE. Cross-connections can be correlated, which means that they are associated with a connection that is provisioned in the NFM-T OTN or they are uncorrelated, which means that they are not associated with a connection that is provisioned in the NFM-T OTN. Users can view both types of cross connections and remove those that are uncorrelated.

View, acknowledge, and restore inconsistent connections

Part of the continual operation of the NFM-T OTN involves the user viewing, acknowledging, and restoring those connections that the management systems views to be inconsistent with the NE level view of the connection. These connections, which occur for infrastructure connections and services, are attributed to SNC, Parameter, Download Disabled, or ASAP mismatches that occur when a Commissioned or Implemented Complete connection contains a cross-connection that has been disconnected or rearranged outside of the NFM-T OTN.

View and modify parameters

Change is an inevitable action in any network. Users can view all of the parameter values that have initially been provisioned and they can modify many of those parameters.

Respond to alarms

The continual operation of the management system requires users to create, maintain user defined alarm profiles, as well as respond and troubleshoot alarms.

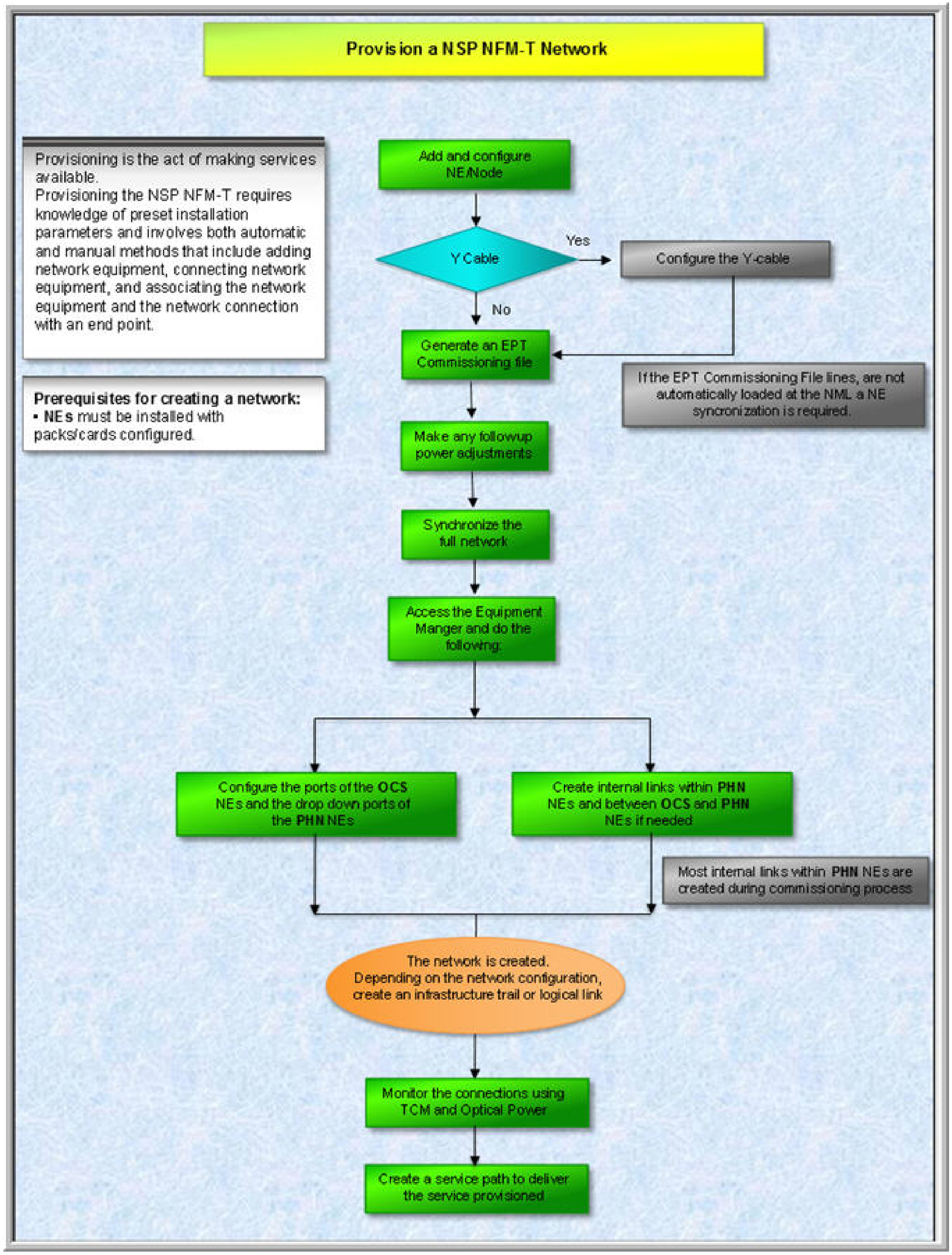
OTN Network Provisioning Sequence

2.5 OTN Network Provision Flowchart

Overview

The following flowchart provides you a graphical view of all of the steps that are needed to provision a network.

Figure 2-1 Flowchart for provisioning a network



2.6 Provision a NFM-T OTN network

When to use

Use this task to provision a NFM-T OTN network.

Related information

See the following topics in this document:

- Node Management
- Operate Equipment Manager
- “TCM on Infrastructure Connections and Services” (p. 1117)
- 2.8 “Determine the Infrastructure to be created” (p. 168)
- 2.38 “Transponder configurations” (p. 311)
- 2.39 “Muxponder UNI/NNI configurations” (p. 312)
- 2.40 “Muxponder/Switchponder cascaded configurations” (p. 313)
- 2.41 “Muxponder extended to OCS configuration” (p. 314)
- 2.42 “Uplink configurations” (p. 315)
- 2.43 “L1 ASON configuration” (p. 316)
- 7.12 “Deploy a template to make a connection” (p. 754)

Before you begin

The NE must be installed, which includes adding the NE and the partner NE, and configuring the packs/cards.

This task requires knowledge of NE installations, partnering, and packs/cards. In addition, this task requires knowledge of the Engineering and Planning Tool (EPT).

It is helpful to have the NE and EPT documentation handy.

Be knowledgeable about the guidelines concerning the **Auto Server Creation** field, which determines if you must create or if the NFM-T system automatically creates the server layer for the infrastructure connection or service. Refer to the “Auto Server Creation” (p. 708) section for provisioning guidelines.

Task

Complete the following steps to provision a NFM-T OTN network.

1

Install the NE, which includes adding the NE and the partner NE, and configuring the packs/cards.

Refer to Add Node/NE in the *NFM-T NE Management Guide* for detailed steps.

2

If you have a Y-Cable configuration in the network, go to the 2.7 "Provision an NFM-T OTN network with Y-Cable configurations" (p. 163) task and, depending on your particular configuration, complete the steps provided.

If you do not have a Y-Cable configuration in the network, go to and continue with Step 3.

3

Generate an EPT Commissioning File and commission the lines.

If the lines are not automatically loaded on the NML, do a full synchronization on the NE. Refer to Synchronize Nodes for detailed steps.

Make any follow-up power adjustments. Refer to "Task: View and Refresh Optical Power for an OTUk Infrastructure Connection" (p. 1868) for details.

4

Perform an initial full network synchronization; or perform a full network synchronization after a communication loss with the NE has occurred.

Refer to Synchronize Nodes for detailed steps.

5

Use the Equipment Manager to configure 1830 PSS-64 ports (signal types) and the drop ports on the photonic NE.

Use the Equipment Manager to create internal links within the photonic NE and between the 1830 PSS-64 and 1830 PSS-32 as needed (which is usually an uplink to SFDs and an uplink to MCS cards).

For configurations with D5X500 circuit packs, use the Equipment Manager to configure the pack and the signaltypes of the clients *before* proceeding with any photonic commissioning. (The D5X500 pack default setting is 100GBE. All clients must have same signaltype.)

Refer to the *Equipment Management* section of the NFM-T NE Management Guide for all Equipment Manager related tasks.

Note: Typically, most internal links within the photonic NE are created in the commissioning process.

Result: The network is now ready for infrastructure logical link/trail and service path creation.

6

Depending on the network configuration, create an infrastructure trail or logical link. Refer to the 2.8 "Determine the Infrastructure to be created" (p. 168) task for an explanation on whether you must create a trail or a logical link. Use task 7.12 "Deploy a template to make a connection" (p. 754) to create the infrastructure trail or logical link; or, use task 7.8 "Design and publish a template for a connection" (p. 741) to create a connection to suit the needs of your site.

Important! When you access a template to create (deploy) an infrastructure connection, the system defaults to a trail. To create a logical link, you must check the **Logical Link** box in the **Service Definition**.

Note: Occasionally, in Muxponder and cascaded configurations, an additional step might be needed if signal types are not provisioned in the previous step. Refer to 2.40 "Muxponder/ Switchponder cascaded configurations" (p. 313) for illustrations of cascaded configurations.

7

Monitor the connections made using Tandem Connection Monitoring (TCM) and Optical Power Visualization. Refer to "TCM on Infrastructure Connections and Services" (p. 1117) for detailed tasks on TCM and "Task: View and Refresh Optical Power for an OTUk Infrastructure Connection" (p. 1868) for a detailed task on optical power.

8

Create a service path with a container to deliver the service being provisioned. Use the 7.12 "Deploy a template to make a connection" (p. 754) task to create the service; or, use the 7.8 "Design and publish a template for a connection" (p. 741) task to create a service to suit the needs of your site.

END OF STEPS

2.7 Provision an NFM-T OTN network with Y-Cable configurations

When to use

Use this task to provision a NFM-T OTN network with Y-cable configurations.

Related information

See the following topics in this document:

- 7.12 "Deploy a template to make a connection" (p. 754)
- 7.8 "Design and publish a template for a connection" (p. 741)
- "Auto Server Creation" (p. 708)
- Synchronize Nodes in the NE Management Guide
- 7.42 "View the 360° tabs for a physical connection" (p. 890)

Before you begin

This task requires knowledge of NE installations, partnering, and packs/cards. In addition, this task requires you to use the ZIC. It would be helpful to have the NE documentation handy.

This task requires the NE to be installed, which includes adding the NE and the partner NE, and configuring the packs/cards.

In addition, based on the guidelines concerning the **Auto Server Creation** field, determine if you must create or if the NFM-T system automatically creates the server layer for the infrastructure connection or service. Refer to the "Auto Server Creation" (p. 708) section for provisioning guidelines.

Task: Provision Y-Cable configurations with transponders at the DSR layers

Example: With 11QPA4 and/or 112SCA1 circuit packs...

Complete the following steps to provision NFM-T OTN Y-cable configurations with transponders at the DSR layers.

1

From the NE ZIC, configure the **Client Signal Type** for both the main pair of ports and the spare pair of ports.

2

From the NE ZIC, configure the **Protection Groups**.

3

From the NFM-T GUI, perform a full synchronization on the both A node and the Z node. Refer to Synchronize Nodes for detailed steps.

Result: The system automatically creates the required internal OS connections (now known as *link connections*), which are the physical fiber connections that are provisioned within the NE and are established as a bidirectional connection.

4

From the NFM-T GUI, after the synchronization of the A node and the Z node, verify if the required link connections have been made. Refer to the 7.42 “View the 360° tabs for a physical connection” (p. 890) task for detailed steps; click on the **Link Connections** tab.

5

From the NFM-T GUI, create two sets of ODU/OTU connections. One set for the main set of ports and the other set for the spare set of ports in Step 1.

Important! When creating both sets of ODU/OTU connections, check the box in the **Auto Server Creation** field.

Use the 7.12 “Deploy a template to make a connection” (p. 754) task to create the ODU/OTU connections; or, use the 7.8 “Design and publish a template for a connection” (p. 741) task to create the ODU/OTU connections to suit the needs of your site.

Result: The system automatically creates the protected DSR connections.

6

For additional Y-Cable protected clients on the 11QPA4 and/or 11QPEN4 circuit packs, repeat all of the previous steps.

End of steps

Task: Provision Y-Cable configuration with muxponders at the DSR layers

Example: With 112SCX10 and/or 432CX4 circuit packs...

Complete the following steps to provision a NFM-T OTN network with Y-cable configurations with muxponders at the DSR layers.

1

From the NE ZIC, configure the **Client Signal Type** for both the main pair of ports and the spare pair of ports.

2

From the NE ZIC, configure the **Protection Groups**.

3

From the NFM-T GUI, perform a full network synchronization on both the A node and the Z node. Refer to Synchronize Nodes for detailed steps.

Result: The system automatically creates the required internal OS connections (now known as *link connections*), which are the physical fiber connections that are provisioned within the NE and are established as a bidirectional connection.

4

After the synchronization of the A node and the Z node, verify if the required link connections have been made. Refer to the 7.42 “View the 360° tabs for a physical connection” (p. 890) task for detailed steps and click on the **Link Connections** tab to view the connections.

5

From the NFM-T GUI, create two sets of ODU/OTU connections. One set for the main set of ports and the other set for the spare set of ports in Step 1.

Important! When creating both sets of ODU/OTU connections, check the box in the **Auto Server Creation** field.

Use the 7.12 “Deploy a template to make a connection” (p. 754) task to create the ODU/OTU connections; or, use the 7.8 “Design and publish a template for a connection” (p. 741) task to create ODU/OTU connections to suit the needs of your site.

Result: The system automatically creates the protected DSR and ODUj connections

6

For additional Y-Cable protected clients on the 112SCX10 and/or 43SCX4 circuit packs, repeat Step 1 to Step 3.

End of steps

Task: Provision Y-Cable configuration with G709 switchponders

Example: G709 11DPM12 circuit pack...

Complete the following steps to provision a NFM-T OTN network with Y-cable configurations with switchponders.

1

From the NFM-T GUI, create an ODU2/OTU2 connection. For service with an OPTSG container, create an ODU1 infrastructure trail.

Important! When creating the ODU2/OTU2 connection, check the box in the **Auto Server Creation** field.

Use the 7.12 “Deploy a template to make a connection” (p. 754) task to create the ODU2/OTU2 connection; or, use the 7.8 “Design and publish a template for a connection” (p. 741) task to create an ODU2/OTU2 connection to suit the needs of your site.

2

From the NE ZIC, configure the **Client Signal Type/Container**.

3

From the NE ZIC, configure the **Protection Groups** on all of the involved clients.

4

From the NFM-T GUI, perform a full network synchronization on the both A node and the Z node. Refer to Synchronize Nodes for detailed steps.

Result: The system automatically creates the required internal OS connections (now known as *link connections*), which are the physical fiber connections that are provisioned within the NE and are established as a bidirectional connection.

5

From the NFM-T GUI, after the synchronization of the A node and the Z node, verify if the required link connections have been made. Refer to the 7.42 “View the 360° tabs for a physical connection” (p. 890) task for detailed steps and click on the **Link Connections** tab.

6

From the NFM-T GUI, create two separate ODUj infrastructure trails using the ODUk infrastructure template.

Important! When creating the two separate ODUj infrastructure trails, UNCHECK the box in the **Auto Server Creation** field and DO NOT CHECK the box for **Logical Link**.

For an OPTSG container, create a protected DSR connection with DSR ports on the Y-Cable.

Use the 7.12 “Deploy a template to make a connection” (p. 754) task to create the separate ODUj infrastructure trails; or, use the 7.8 “Design and publish a template for a connection” (p. 741) task to create the separate ODUj infrastructure trails to suit the needs of your site.

Result: The system automatically creates the protected DSR services upon completion of the two ODUj infrastructure trails.

End of steps

Task: Provision Y-Cable configuration with non-G709 switchponders

Example: non-G709 11STMM10, 11DPE12E/A circuit pack, full/subrate/QinQ...

Complete the following steps to provision a NFM-T OTN network with Y-cable configurations with switchponders.

1

From the NFM-T GUI, create an ODU2/OTU2 connection.

Important! When creating the ODU2/OTU2 connection, check the box in the **Auto Server Creation** field.

Use the 7.12 “Deploy a template to make a connection” (p. 754) task to create the ODU2/OTU2 connection; or, use the 7.8 “Design and publish a template for a connection” (p. 741) task to create an ODU2/OTU2 connection to suit the needs of your site.

2

From the NE ZIC, configure the **Client Signal Type/Container**.

3

From the NE ZIC, configure the **Protection Groups** on all of the involved clients.

4

From the NFM-T GUI, perform a full network synchronization on the both A node and the Z node. Refer to Synchronize Nodes for detailed steps.

Result: The system automatically creates the required internal OS connections (now known as *link connections*), which are the physical fiber connections that are provisioned within the NE and are established as a bidirectional connection.

5

After the synchronization of the A node and the Z node, verify if the required link connections have been made. Refer to the 7.42 "View the 360° tabs for a physical connection" (p. 890) task for detailed steps and click on the **Link Connections** tab to view the connections.

6

From the NFM-T GUI, create a protected DSR service that terminates on the Y-Cable.

Use the 7.12 "Deploy a template to make a connection" (p. 754) task to create the protected DSR service; or, use the 7.8 "Design and publish a template for a connection" (p. 741) task to create a protected DSR service to suit the needs of your site.

Result: The system automatically creates the VTSs or the DSR cross connections.

END OF STEPS

2.8 Determine the Infrastructure to be created

When to use

Use this task to determine the infrastructure that must be created for the NFM-T OTN network.

General provisioning rules

The aim of this paragraph is furnishing some general guidelines defining provisioning rules to help the user in understanding the provisioning flow.

Definitions

Integrated Provisioning is a scenario where the user creates the Service/Logical Link/Infrastructure and the associated server for this request is auto created. An example is the ODU4 Infrastructure between 130SCX10 where the OTU4 is created as part of same request.

Non Integrated Provisioning is the scenario where provisioning of the Service/Logical Link/ Infrastructure does not require the auto creation of a server. The auto creation of the server is done checking the Auto Server creation check box in the create connection wizard. This type of provisioning is required for cascading configurations.

Infrastructure or Logical Link?

General rules:

- Create an *Infrastructure* on line interfaces if both end ports are on Transponders muxponders or on legacy switchponders.
- Create a *Logical Link* if one or both end ports are I/O ports or line ports on 8x/12x/24x/OCS/ Falcon packs.
- Create an *integrated Logical Link* when you have a PSD Symmetric scenario with transponders on PHN catering to the OTUK termination.
- For some cases logical link on client interfaces are defined by how the ODUj grooming capability is being utilized.

Exceptions to general rules to be considered:

- 4QPA8 pack requires the creation of a logical link followed by the creation of an infrastructure, depending on the container type.
- 11DPM12/8 OTU1 client interface needs terminated or unterminated trail depending on client to be carried.
- Black and white links between 8x/12x/24x/OCS/Falcon packs do not require any logical link creation.
- If we need ODU grooming on PSD then we need to create a logical link on the line interface of the PSD NE.
- When creating NNI Paths on PSD, the creation of logical link is not required.

Workflow

Integrated or mix of integrated and non-integrated work flow:

- Create a non-integrated OTUK when we have a frequency conversion from CWDM to DWDM.

- A combination of non-integrated workflow is required for scenarios where we have interworking between two different network scenarios.
- A non-Integrated workflow is required when we need to create OCH path or trails on PSI2T R1.0 NEs.
- A non-Integrated workflow is required for Single fiber trails when only manual routing is allowed.
- When we have cascaded configurations, the higher speed card's line is typically connected to a Filter/Photonic switch (SFD/CWR/WR/PSC/MCS) and the lower speed card is connected to the higher speed card. In such cases, the card connected to the Photonic layer has ODU and OTU/OCH created together and hence requires an integrated connection. The connection originated on the Line side of the lower speed card does not create photonic cross-connection and therefore creates only one layer and is a non-integrated connection.
- In general use non-integrated service creation if the server is already present.

Related information

See the following topics in this document:

- 2.6 "Provision a NFM-T OTN network" (p. 160)
- 2.38 "Transponder configurations" (p. 311)
- 2.39 "Muxponder UNI/NNI configurations" (p. 312)
- 2.40 "Muxponder/Switchponder cascaded configurations" (p. 313)
- 2.41 "Muxponder extended to OCS configuration" (p. 314)
- 2.42 "Uplink configurations" (p. 315)
- 2.43 "L1 ASON configuration" (p. 316)
- 7.12 "Deploy a template to make a connection" (p. 754)

Before you begin

An *infrastructure* is typically a user-created or auto discovered entity, such as a trail or a logical link, that is constructed in the network before services are delivered.

Infrastructures are unterminated or terminated. An *unterminated entity* is one in which G.709 transmission overhead is not processed; for example, in Optical Core Switching (OCS), the OTU/ODU termination point on an uplink card would be an unterminated entity. A *terminated entity* is one in which overhead is processed.

A *logical link* is an unterminated entity that provides contiguous fixed connectivity to the far end, which can be terminated or unterminated. The connectivity can be over regenerators; but note that an OTUk through a photonic node without any regenerators is also considered a logical link. Having a logical link infrastructure implies flexibility at the endpoint; meaning, it can provide the ability to terminate or to create a flexible cross-connection to a client port or to another network port.

A *trail* is a terminated entity that can multiplex or demultiplex client signals. Strictly speaking, the client side adapting entity (a GbE ODU0, for example) is also a trail.

Important! Be aware of the following points:

- Determine if you must create an infrastructure trail or a logical link, and use the 7.12 "Deploy a template to make a connection" (p. 754) task to create the connection.
- Access a template to create (deploy) an infrastructure connection, the system defaults to the option trail. To create a logical link, you must check the **Logical Link** box in the **Service Definition**.
- The **Auto Server Creation** field determines whether the NFM-T system must automatically create the server layer for the infrastructure connection or service or the user must perform it manually. Refer to the "Auto Server Creation" (p. 708) section for provisioning guidelines.
- The 2.32 "Auto Payload" (p. 295) feature enables an HO-ODUk infrastructure trail, along with a LO-ODUk infrastructure trail, to be provisioned in a single step when you provision a DSR service. The Auto Payload feature relies on the system's automatic creation of virtual servers, which are ODU2POOL ports on the 1830 PSS OCS NEs that are used for internal routing. Refer to 2.32 "Auto Payload" (p. 295) for an more detailed explanation of Auto Payload and refer to "Auto Payload supported configurations" (p. 295) for configuration information.
- After creating the infrastructure trail or a logical link, use the 7.12 "Deploy a template to make a connection" (p. 754) to create any service paths.

Task

Complete the following steps to determine the infrastructure to be created for the NFM-T OTN network.

1

For transponders (11STA*, 11QPA4, 43STAP1, 43SCA1, 43SNA1, 112S[CN]A1, 130S[CN]A1), perform the following:

If both ends are transponders, create an ODUk trail. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Result: The system automatically creates the OTUks, on the server side and discovers DSRs if signalTypes are set to non-OTU* (UNI) on the client side. If regenerators exist in the configuration, the system creates more than one OTUk.

If one end is a uplink card (43SCUP, 11QCUPC, 130SCUP[BC]), create a logical link. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Refer to 2.38 "Transponder configurations" (p. 311) for illustrations of transponder configurations.

2

For muxponders (43SCX4, 112S[CN]X10, 130S[CN]X10), perform the following:

If both ends are Muxponders, create an ODUk trail. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Result: The system automatically creates the OTUks on the server side, discovers and creates the ODUj+DSR if the client signal type is already set, and discovers the ODUj logical links if the client signal type is set and is extended to an OCS (10XANY10G). If regenerators exist in the configuration, the system creates more than one OTUk. Refer to 2.39 "Muxponder UNI/NNI configurations" (p. 312) and 2.41 "Muxponder extended to OCS configuration" (p. 314) for illustrations.

If one end is a uplink card (43SCUP, 130SCUP), create a logical link.

Refer to for 2.42 "Uplink configurations" (p. 315) illustrations of uplink configurations.

3

From an 1830 PSS OCS NE to an 1830 PSS OCS NE (with an uplink card or with a 10XANY10G connected to a Muxponder), create a logical link. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Refer to 2.42 "Uplink configurations" (p. 315) and 2.41 "Muxponder extended to OCS configuration" (p. 314) for illustrations of uplink and Muxponder configurations.

4

From an 1830 PSS OCS NE, if more than one hop on a logical link needs to be made or for a HO-SNCP, create a ODUk trail using the ODU Pool endpoint. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Important! Refer to the "Auto Server Creation" (p. 708) section for provisioning guidelines.

5

For Switchponders (11DPM12, 11DPE12), perform the following:

If both ends are Switchponders create an ODUk trail. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Result: The system automatically creates the OTUks on the server side. If regenerators exist in the configuration, the system creates more than one OTUk.

If one end is a uplink card (11QCUPC), create a logical link. Go to the 7.12 "Deploy a template to make a connection" (p. 754) task.

Refer to 2.40 "Muxponder/Switchponder cascaded configurations" (p. 313) for illustrations of Muxponder/Switchponder configurations and 2.42 "Uplink configurations" (p. 315) for illustrations of uplink configurations.

6

For 4UC1T, 2UX500, 8UC1T, 2UC1T, DFC12, DFC12E, DFM6, DFM6E, DD2M4, SFM6, S4X400H, S4X400L, S5AD400H and S6AD600H perform the following:

Create an unprotected infrastructure tunnel with 8UC1T, DFC12, DFC12E, DFM6, DFM6E,, SFM6, 2UX500, S5AD400H, S6AD600H, or S4X400H with rate as OTSig Tunnel. Ensure both the sides of a tunnel have the same type of cards for Symmetric.

OTSig Tunnel provisioning is a new provisioning with user input variable called Optical Line Mode Profile, which is an integer enum that identifies a specific set of universally defined configuration parameters.

Both Managed Plane and Control Plane connections are supported. For Control Plane, only

MRN Terminated Tunnel is supported.

Note: In NFM-T R20.11, Control Plane connections are not supported on cards DFM6 and DFM6E.

For more information on OTSig Tunnel, see “OTSiG tunnel” (p. 258).

For more information on Optical Line Characteristics, see “Optical line characteristics” (p. 706).

To manage an OTSig Tunnel creation, see 8.11 “Manage an OTSig Tunnel ” (p. 1314).

7

Create the service path. Go to the 7.12 “Deploy a template to make a connection” (p. 754) task.

END OF STEPS

NEs, Subnetworks, Nodes, Ports, and Cross-connections

2.9 Nokia NE configurations

NE, node, compound node, and Multi-NE clusters definitions

A Network Element *(NE)* is a unit of equipment within a network that performs specific transport and/or switching functions such amplification, regeneration, cross-connection, multiplexing, and packet switching. Refer to 2.11 "Nodes" (p. 190) for details.

A *node* is any NE or non-managed NE or a group of NEs or non-managed NEs. A node can contain a single NE or two NEs that are linked together and are treated as a single unit.

A *compound node* is a configuration that includes the user partnering of 1830 PSS OCS NEs and 1830 PSS PHN/WDM NEs through the use of uplink cards. Refer to "Compound node scenarios" (p. 181) for details.

A *Multi-NE Cluster* is a user association of 1830 PSS R9.0 and later NEs that include multi-slot 100 G Optical Transmitters (OTs) located at a single site; the individual NEs, which contain the OTs, continue to perform general management functions; however, NEs with optical line resources perform auto power management for OT line ports on other NEs. Refer to "Multi-NE Clusters" (p. 183) for details.

1830 PSS OCS cross-connect fabric and TDM switching and grooming

The 1830 PSS-64 and 1830 PSS-36 OCS NEs support different types of I/O circuit packs that are used to adapt a customer signal of varying data formats and rates into the standard ODUk data rate or to transport an incoming ODUk signal across the network.

The 1830 PSS OCS NE architecture provides two cross-connect fabrics to transport these signals:

- One for a high order ODUk (HO-ODUk) that terminates on a ODUPOOL virtual port in the backplane.
- One for a low order ODUk (LO-ODUk) that supports a low order ODUk cross-connect.

For HO-ODUk level signals that enter the 1830 PSS OCS NE from other networks or from customer premises equipment, the HO-ODUk cross-connect provides a direct connection without going through the low order cross-connect fabric. The termination of the HO-ODUk signal at the ODUPOOL virtual port inside the NE provides the grooming of the low order ODUk signals that come from the low-order cross-connect fabric. The NE supports either ODU0 (~1 Gb) or ODU1 (~2.5G) cross-connects through the low order cross-connect fabric. The low order cross-connect level (ODU0 or ODU1) has to be predetermined and set for the NE ahead of time.

Both HO-ODUk and LO-ODUk cross-connect fabrics support unprotected or protected signals with SNC-I (inherent) or SNC-N (non-intrusive) protection types. In addition, client signals that enter the 1830 PSS OCS NE can also be protected with the SNC-Nc protection type, which chooses the better of two client signals that are entering in the 1830 PSS OCS NE at two I/O ports.

A schematic representation of HO-ODUk and LO-ODUk trails through the two cross-connect fabrics is illustrated in the figures that follow.

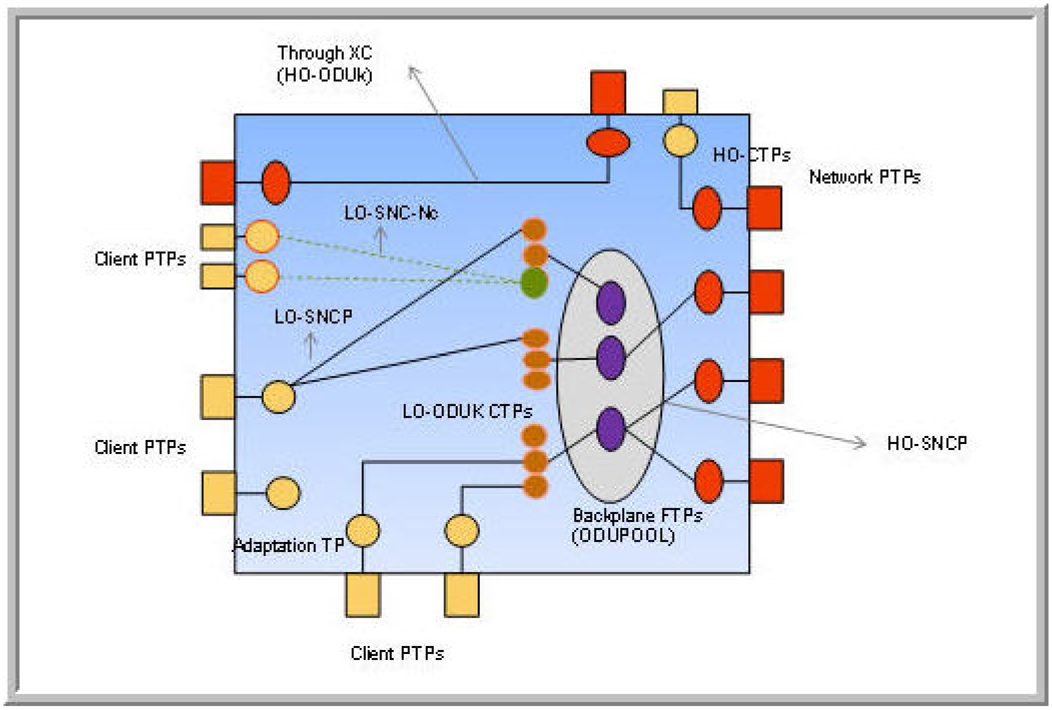


Figure 2-2 Nokia NE Configurations – Abstract View of an 1830 PSS OCS NE with Two Cross-Connect Fabrics

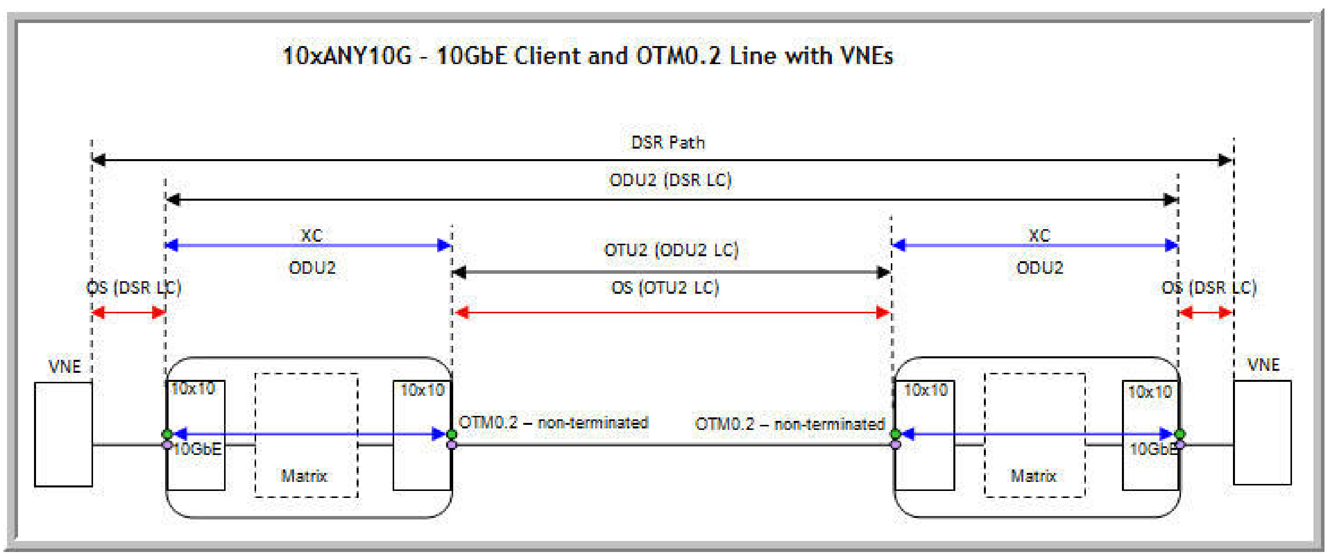
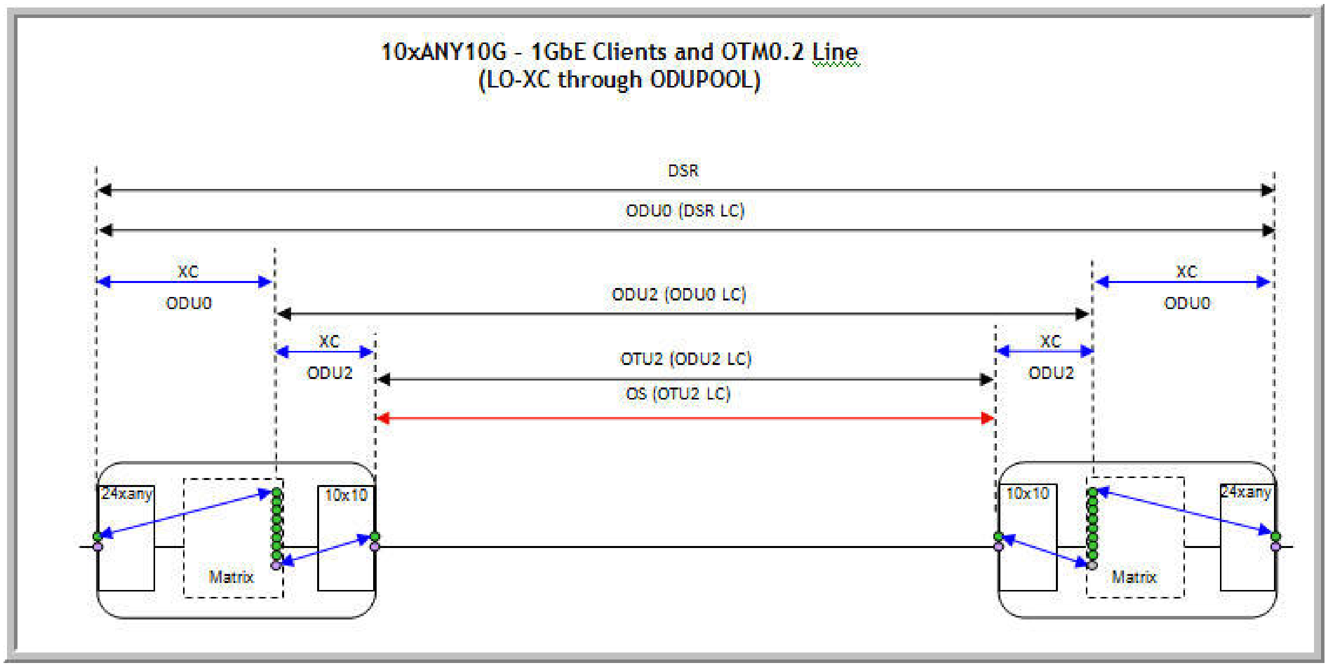


Figure 2-3 Nokia NE Configurations – 10xANY10G – 10GbE Client and OTM0.2 Line with VNEs

Figure 2-4 Nokia NE Configurations – 10xANY10G – 1GbE Clients and OTM0.2 Line (LO-XC through ODUPOOL)

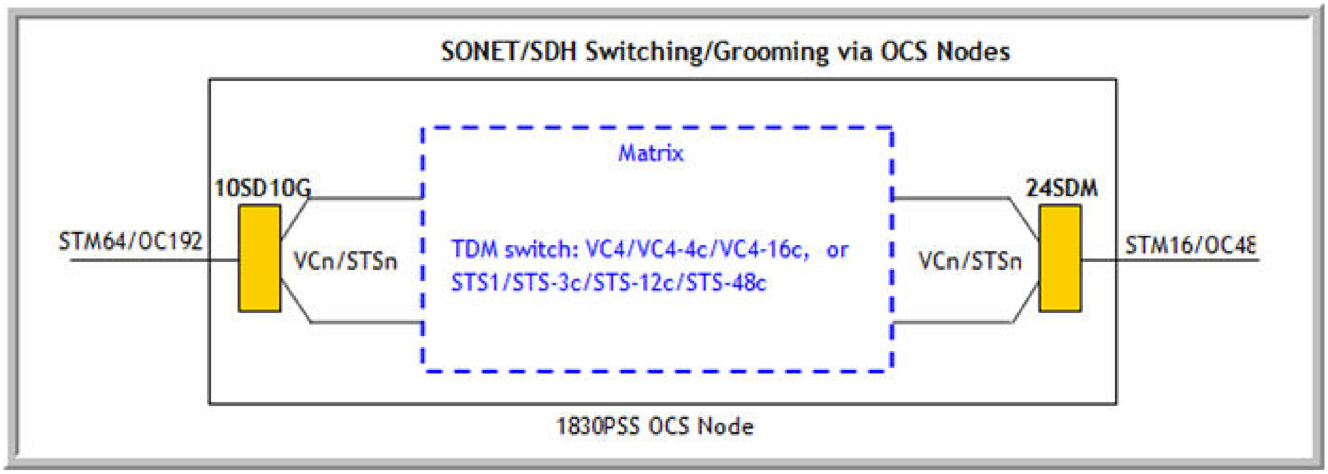


Since the 1830 PSS OCS NEs support the 10XSTH10G (10SD10G) and 24XSTHMR (24SDM) packs, the NFM-T OTN supports their TDM switching and grooming related functions:

SONET/SDH Networking via 1830 PSS OCS Nodes

A client signal rate of STM-64 or OC-192 uses 1830 PSS OCS TDM Input/Output Modules (IOMs) to perform VCn/STSn level switching/grooming through the network in order to produce a client signal rate of STM-16 or OC-48. The following Figure 2-5, “Nokia NE Configurations – 1830 PSS OCS Nodes – SONET/SDH Switching/Grooming” (p. 176) illustrates this grooming.

Figure 2-5 Nokia NE Configurations – 1830 PSS OCS Nodes – SONET/SDH Switching/Grooming

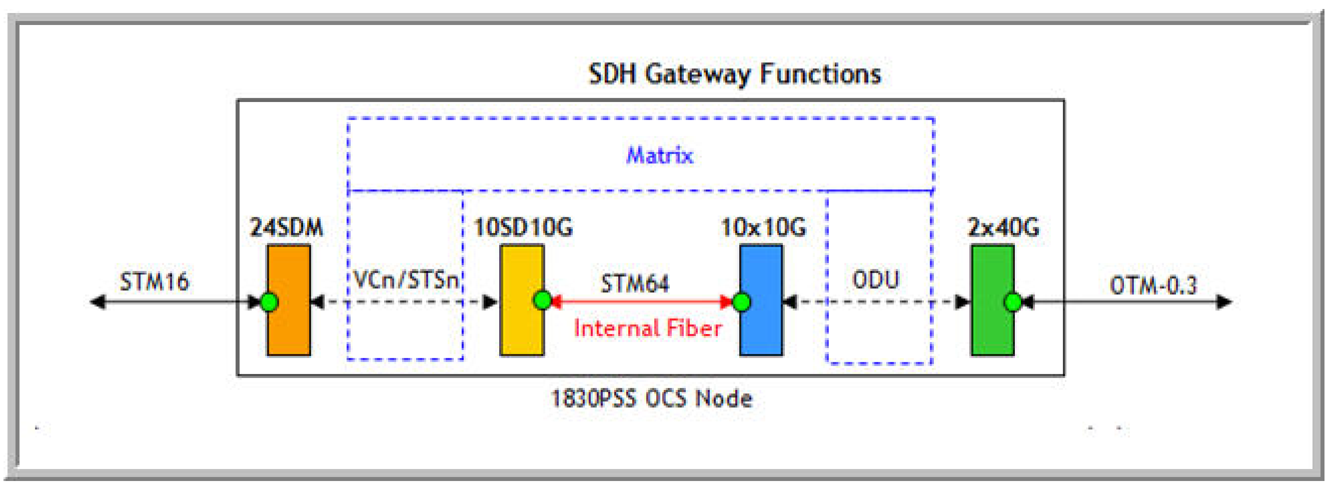


The SDH Gateway

In general, an *SDH Gateway*, or an *SDH GW*, is a set of 1830 PSS-36 and 1830 PSS-64 TDM switch cards and other TDM/OTN Input or Output Modules (IOMs) that enable the 1830 PSS-36 or 1830 PSS-64 to be used as SDH equipment, which thereby enables the 1830 PSS-36 and 1830 PSS-64 to be deployed in an NFM-T OTN network.

When an 1830 PSS OCS NE, which is equipped with the appropriate TDM switch cards and other TDM/OTN IOMs, receives a client signal of STM-n or OC-n, this client signal can be transported through the OTN/WDM network.

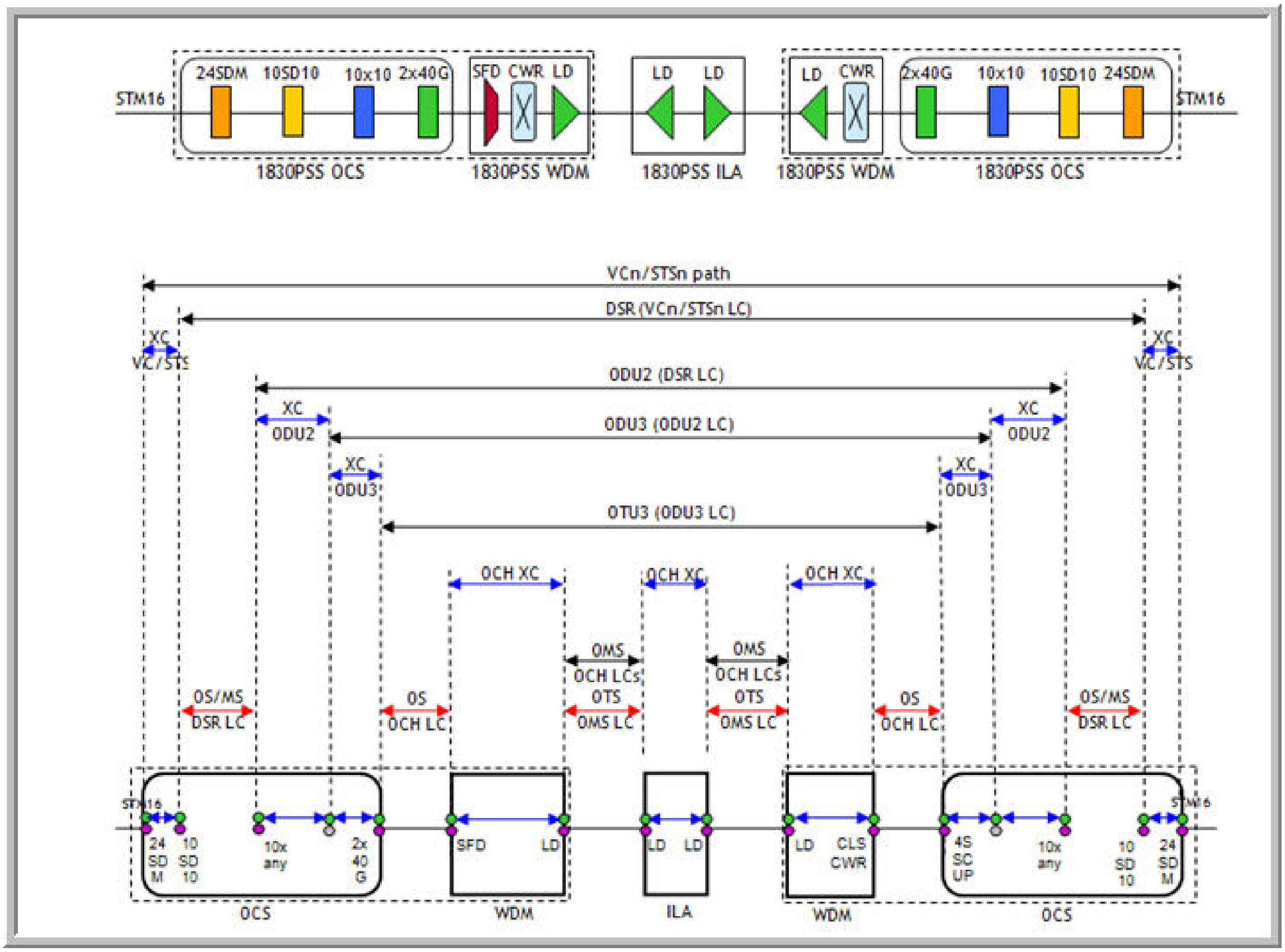
Figure 2-6 Nokia NE Configurations – 1830 PSS OCS Nodes – SDH Gateway



Within the NFM-T environment, many examples of SDH Gateways exists. One example, which is illustrated in Figure 2-7, "Nokia NE Configurations– 1830 PSS OCS Nodes – SDH Gateway Example – STM-16 Client" (p. 176), involves an STM-16 client signal passing through an 1830 PSS OCS NE, to an 1830 PSS WDM NE, to an 1830 PSS ILA, to an 1830 PSS WDM NE, and lastly through an 1830 PSS OCS NE. Each NE is equipped with the appropriate switch cards or IOMs. As the signal traverses each node/NE, the needed cross-connections (XCs) and internal link connections (LC) are created until a VCn/STSn service path is created.

For other supported configurations of SDH Gateways, contact your Nokia local customer service support team.

Figure 2-7 Nokia NE Configurations– 1830 PSS OCS Nodes – SDH Gateway Example – STM-16 Client



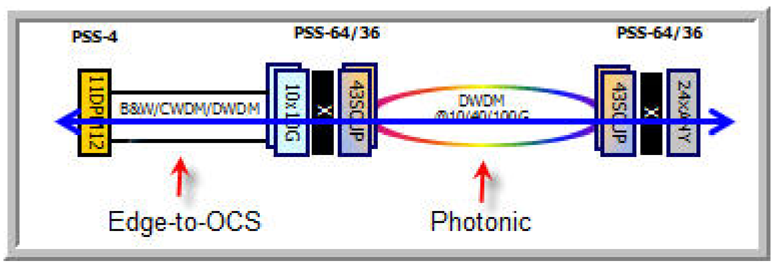
1830 PSS OCS and 1830 PSS PHN interworking

Some of the transponders used in 1830 PSS WDM/PHN network of NEs, such as the 11QCUP, 130SCUP, 43SCUP circuit packs, which are known as *uplink* cards, also directly interwork with 1830 PSS-32 NEs. These uplink cards provide a photonic layer infrastructure connection that terminates on an 1830 PSS OCS NE with optical power management capabilities. The 1830 PSS OCS NEs in the configurations that include the 1830 PSS-32 NEs will then partner to form *compound nodes*.

The NFM-T OTN application manages the 1830 PSS PHN/WDM and electrical switching, which includes GMPLS L0 (PHN/WDM) and GMPLS L1 (OCS/switching) support. Users can partner an 1830 PSS OCS NE and an 1830 PSS PHN/WDM NE as a compound node. The management system provides a single node inventory that is used to retrieve the 1830 PSS data, and it also offers the ability to expand the compound node with additional 1830 PSS OCS and 1830 PSS PHN/WDM NEs.

Example: The following figure illustrates the interworking of 1830 PSS NEs.

Figure 2-8 Nokia NE Configurations – 1830 PSS OCS and 1830 PSS PHN Interworking



Any interworking of NEs and the NEs that form compound nodes is achieved through physical connections. In NFM-T, physical connections are automatically discovered or they are provisioned by users. Once physical connections are automatically discovered or created, they are listed on a single connection list, which also contains the links between any OCS-PHN components. These links, which are known as *intra-nodal* or *OPS links*, represent how OCS and PHN/WDM are connected. For example, the links 43SCUP (40G uplink) connected to the PHN MUX/WSS, the 10X10ANY card connected to an 112SCX10 client, or the colored XFP connected to an SVAC/MVAC/MVAC8B, as illustrated in Figure 2-8, “Nokia NE Configurations – 1830 PSS OCS and 1830 PSS PHN Interworking” (p. 178). In addition, these links can be the 1830 PSS-4 connections to OCS or PHN NEs.

The following are the ways to configure and connect 1830 PSS OCS and 1830 PSS PHN/WDM NEs:

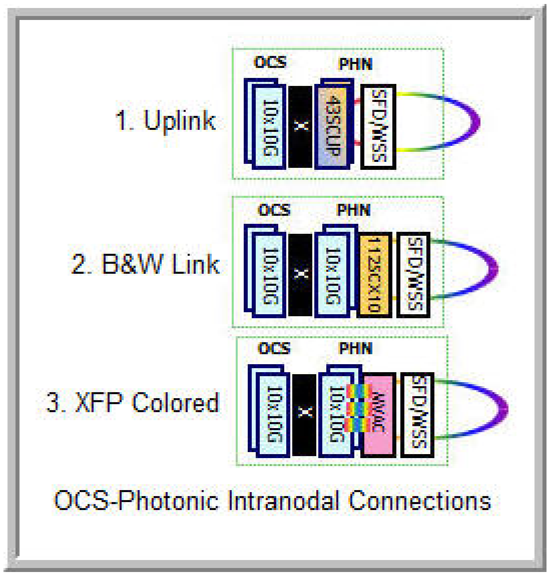
1. As 1830 PSS compound nodes

It is possible to connect an 1830 PSS-32/1830 PSS-16 II WDM/PHN to an 1830 PSS-36/1830 PSS-64 OCS) in these different ways, as illustrated in Figure 2-9, “Nokia NE Configurations – OCS-to-Photonic Intranodal Connections” (p. 179):

- An 1830 PSS OCS **uplink** card, such as the 43SCUP, to the 1830 PSS PHN via a MUX (SFD)/WSS.

- An 1830 PSS OCS with a **B&W** port to the OT port in an 1830 PSS PHN NE, which could be done with an 10X10ANY card connected to an 112SCX10 client.
- An 1830 PSS OCS with a colored **XFP** to an SVAC/MVAC/MVAC8B.

Figure 2-9 Nokia NE Configurations – OCS-to-Photonic Intranodal Connections

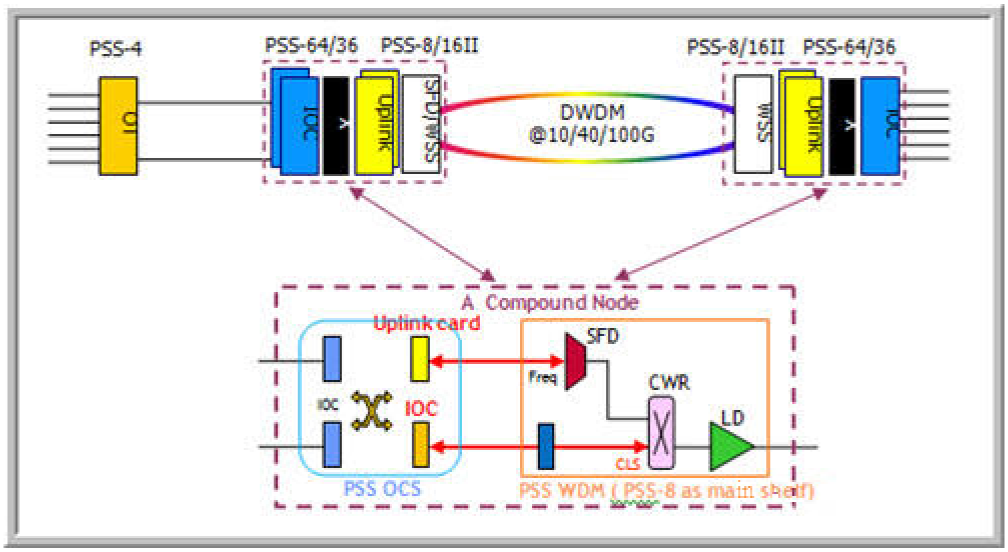


As an 1830 PSS compound node with the 1830 PSS-8 as the main shelf and the 1830 PSS-32 as the extended shelf

Besides having one 1830 PSS OCS NE (PSS-64/PSS-36) and one 1830 PSS PHN NE (PSS-32/ PSS-16 II/PSS-8/PSS-16II) forming one OTN compound node with either an 1830 PSS-32 or 1830 PSS-16 II as the main shelf and all of the other shelves as extension shelves, the 1830 PSS-8 or the 1830 PSS_16II can be used as a main shelf within the PHN NE, and this PHN NE can be used to combine with an OCS NE to form a compound OTN node.

The OTN compound node includes the OCS uplink, along with input or output cards (IOCs) that are used to connect to the PHN NE.

Figure 2-10 Nokia NE Configurations – 1830 PSS-8/1830 PSS-16II as a PHN Main Shelf in an OTN Compound Node



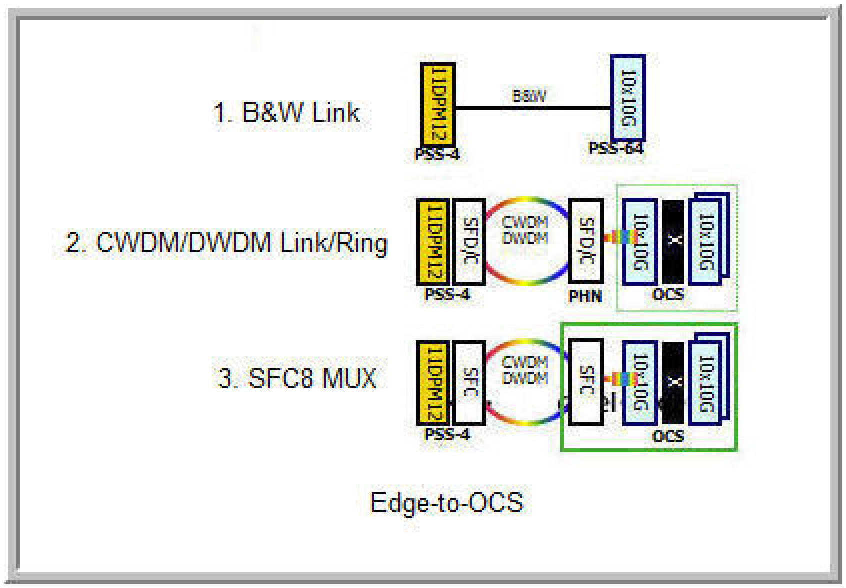
The "Compound node scenarios" (p. 181) section provides two compound node scenarios along with set up details.

2. The 1830 PSS-4 as an access/edge devices connected to an 1830 PSS OCS or 1830 PSS PHN/WDM NE

It is possible to connect in one of the following three ways as illustrated in Figure 2-11, "Nokia NE Configurations – Edge-to-OCS Connections" (p. 181):

- An 1830 PSS-4 OT **B&W** port can to an 1830 PSS OCS NE 10X10ANY circuit pack or to a PHN client OT.
- An 1830 PSS-4 OT colored port (**CWDM**) to an 1830 PSS OCS NE with an 10X10ANY circuit pack with a colored XFP CWDM or PHN client OT through a MUX.
- An **SFC8 MUX** can reside in an 1830 PSS-36 or 1830 PSS-64 NE.

Figure 2-11 Nokia NE Configurations – Edge-to-OCS Connections



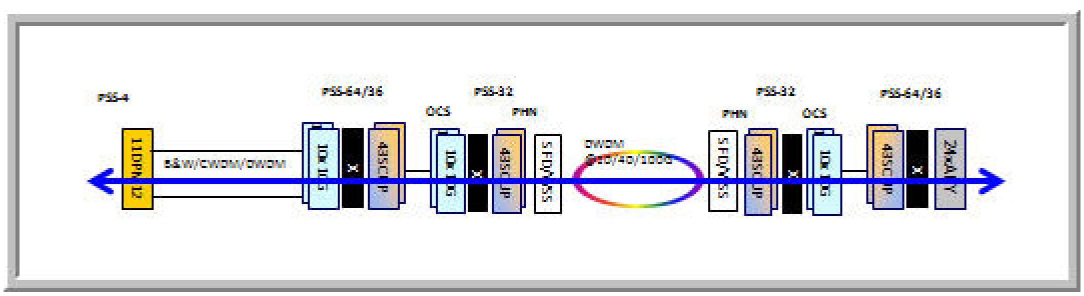
Compound node scenarios

Users can partner 1830 PSS OCS NEs and an 1830 PSS PHN/WDM NEs through the use of uplink cards to create compound nodes. Two common scenarios follow.

Scenario One:

This compound node scenario consists of an 1830 PSS-32 PHN NE configured with an 1830 PSS-36 OCS NE and an 1830 PSS-4 edge NE. It is an unprotected, end-to-end service from the 1830 PSS-4 11DPM12 to the other 1830 PSS-4 11DPM12.

Figure 2-12 Nokia NE Configurations – Compound Node – Colorless/Directionless Configuration



Explanation:

- The physical network must be set up, which includes the OTS and internal 1830 PSS-32/1830

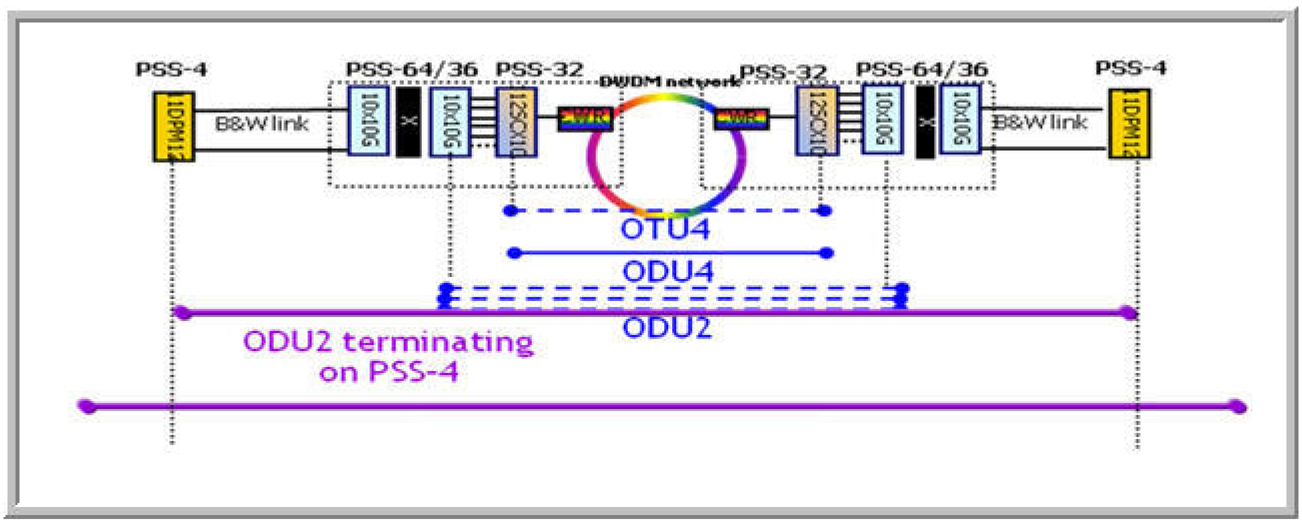
PSS-4 cabling that must be created or uploaded and any links between the 1830 PSS-36 and the 1830 PSS-32 that must be created. In this example, an OTS link is between the 10X10ANY and 43SCUP.

- The 1830 PSS-32 is configured for colorless/directionless transmission.
- The 1830 PSS-4 is connected with a B&W link from the 11DPM12 line to an 10X10ANY port in the 1830 PSS-36 NE.
- The 1830 PSS-36 OCS NE is connected to the OSC of the 1830 PSS-32 PHN NE.

Scenario Two:

This compound node, end-to-end 1 Gb OTN service is from an 1830 PSS-4 to an 1830 PSS OCS NE.

Figure 2-13 Nokia NE Configurations – Compound Node – End-to-End 1 Gb Service



Explanation:

- 1830 PSS-4 edge NEs are connected to 1830 PSS-64/1830 PSS-36 NEs using a B&W link on either end of the connection.

  An ODU2 connection is created to connect to the 1830 PSS-4 edge NEs.

  The 1830 PSS OCS NEs are crossed using an ODU2 connection that terminates on an 10X10ANY card, which is automatically created by an ODU4 set up.
- 1830 PSS-64/1830 PSS-36 NEs are connected to an 1830 PSS-32 NE.

  To complete this end-to-end service, a 1Gb DSR path connection is created on an ODU-0. (The ODU0 grooms the ODU2 in the 11DPM12 on the 1830 PSS-4 NE.)

  A LO-ODU-k connection is automatically created with the DSR connection.

Multi-NE Clusters

With configurations such as those that include multi-slot 100 G optical transmitters (OTs), a 24-shelf NE might not have enough room for OTs to fill 8 degrees. To promote scalability and flexibility in such configurations, the NFM-T supports the Multi-NE Cluster feature for 1830 PSS 9.0 and later NEs.

With Multi-NE Clusters, multiple 1830 NEs at a single site are associated in a cluster. Each NE in the cluster has its own 24-shelf maximum size. Each NE in the cluster is independent and is managed separately through its own management interface. Individual NEs, which contain the OTs, continue to perform general management functions; however, NEs with optical line resources perform auto power management for OT line ports on other NEs.

In a Multi-NE Cluster, an NE assumes one of two role types; and, all currently supported shelf types can assume both role types:

1. An *Optical-Line NE* has resources that automatically manage power settings, wave keys, and channel assignments for connected OT line ports that are located on add-drop NEs. An Optical-Line NE does not perform other aspects of management, such as general provisioning and alarm notification, for OTs that are located in the Add/Drop NEs.

   An Optical-Line NE can also contain its own local OTs, which are managed in a legacy manner. The most common configuration is an Optical-Line NE with its own local OTs.

2. An *Add/Drop NE* contains OTs whose line ports are connected to an Optical-Line NE. The Add/Drop NE performs most aspects of OT management, such as general provisioning and alarm notification locally. Alarms from the Add/Drop NEs are not notified to the managing Optical-Line NE. The Optical-Line NE manages the port power settings, wave keys, and channel assignments.

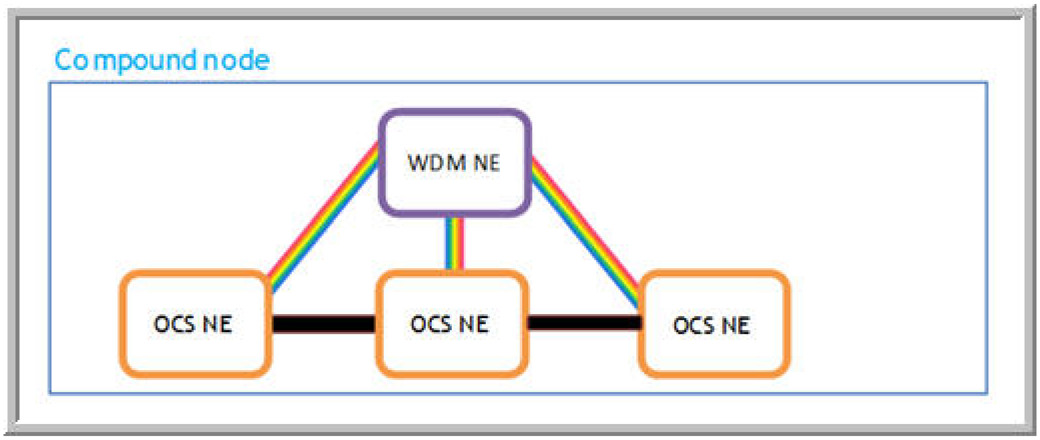
   An Add/Drop NE must only contain OTs or include local LDs and CWRs that are connected to local OTs and managed in a legacy manner. The most common configuration is an Add/Drop NE with only OTs.

UCM Support for Three 1830 PSS OCS NEs

Uplink Card Management, or *UCM*, allows the 1830 PSS NE to directly control optical characteristics (frequency, wave keys, dynamic power levels) of 1830 PSS OCS uplink ports as needed in order to integrate uplink channels into WDM lines on three 1830 PSS OCS NEs.

Note: 1830 PSS Release 9.0 NEs limit UCM support to up to three 1830 PSS OCS NEs.

Figure 2-14 Nokia NE Configurations – Multi-NE Clusters – UCM Support for Three 1830 PSS OCS NEs

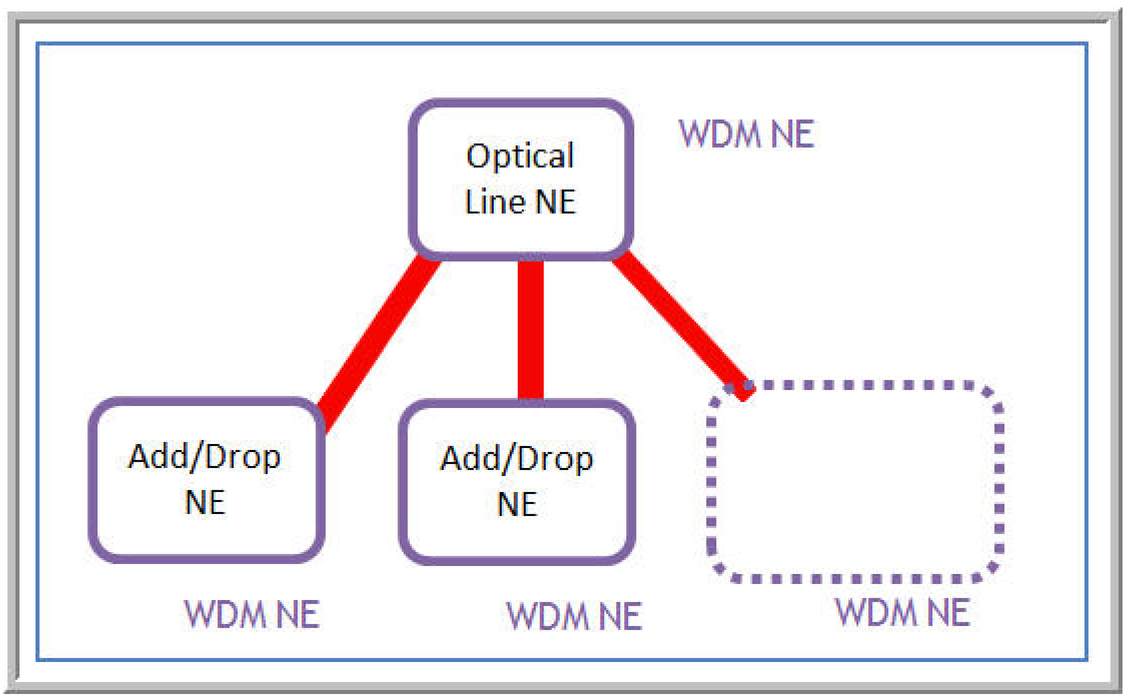


1:N Configuration

In a *1:N configuration*, the cluster contains *1* Optical-Line NE and *N* Add/Drop NEs where: *N >=1*, but not greater than *3*. Each NE assumes only one role.

Important! In the 1:N configuration, *N being not greater than 3* is the NE recommendation; not a NFM-T limitation or validation.

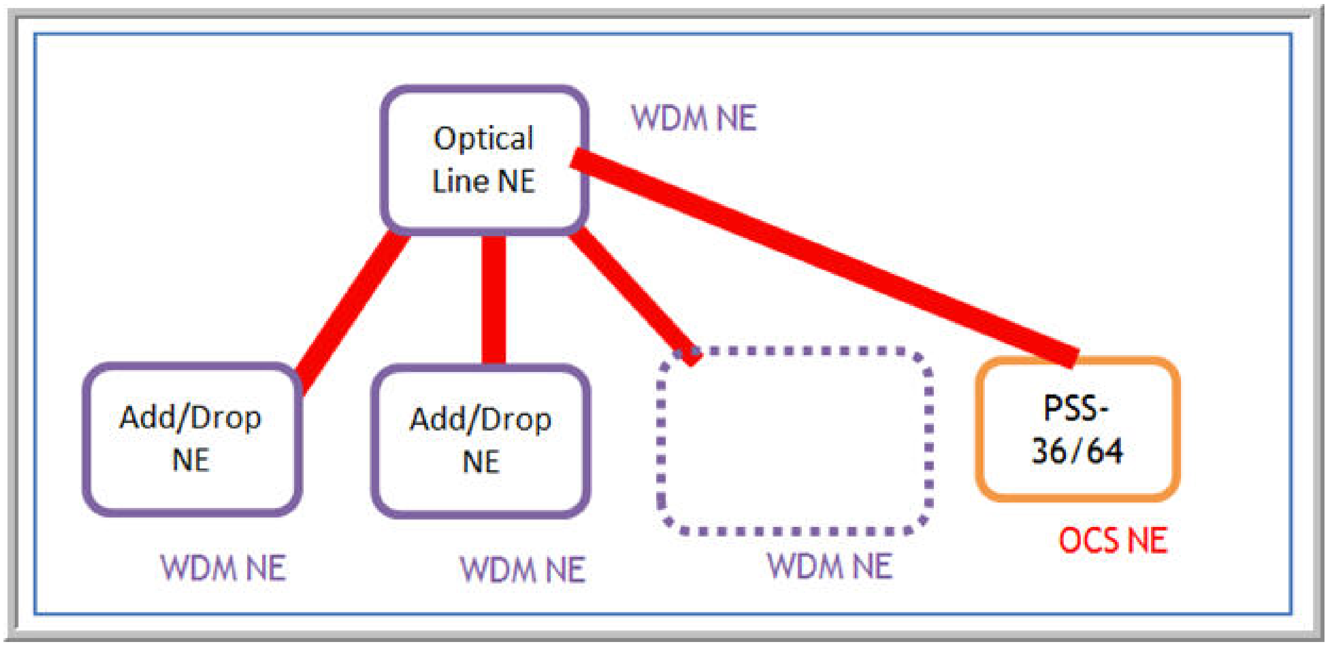
Figure 2-15 Nokia NE Configurations – Multi-NE Clusters – 1:N Configuration



1:N Configuration and UCM Support

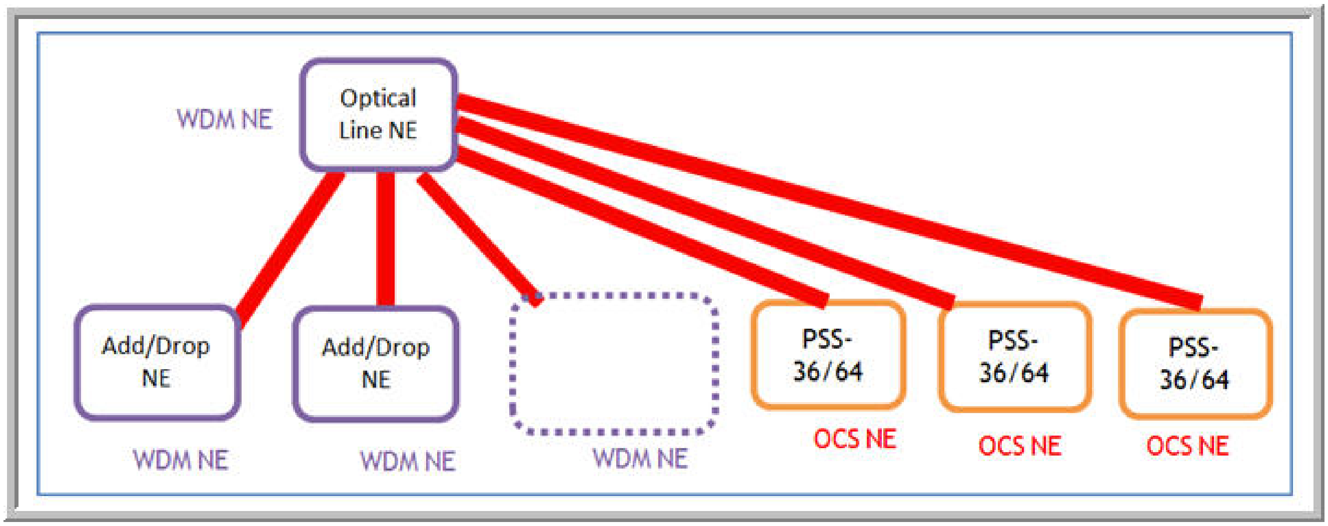
In another version of the *1:N configuration*, the Multi-NE Cluster contains 1830 PSS NEs with *Uplink Card Management support* (DWDM-OCS uplink management). *UCM support* enables 1830 PSS NEs to directly control, as needed, the optical characteristics of OCS ports, such as frequency, wave keys, dynamic power levels, in order to integrate uplink channels into WDM lines.

Figure 2-16 Nokia NE Configurations – Multi-NE Clusters – 1:N Configuration – UCM Support



With UCM support, an NE can be configured in a Multi-NE Cluster and it can be linked to 1830 PSS-OCS NEs.

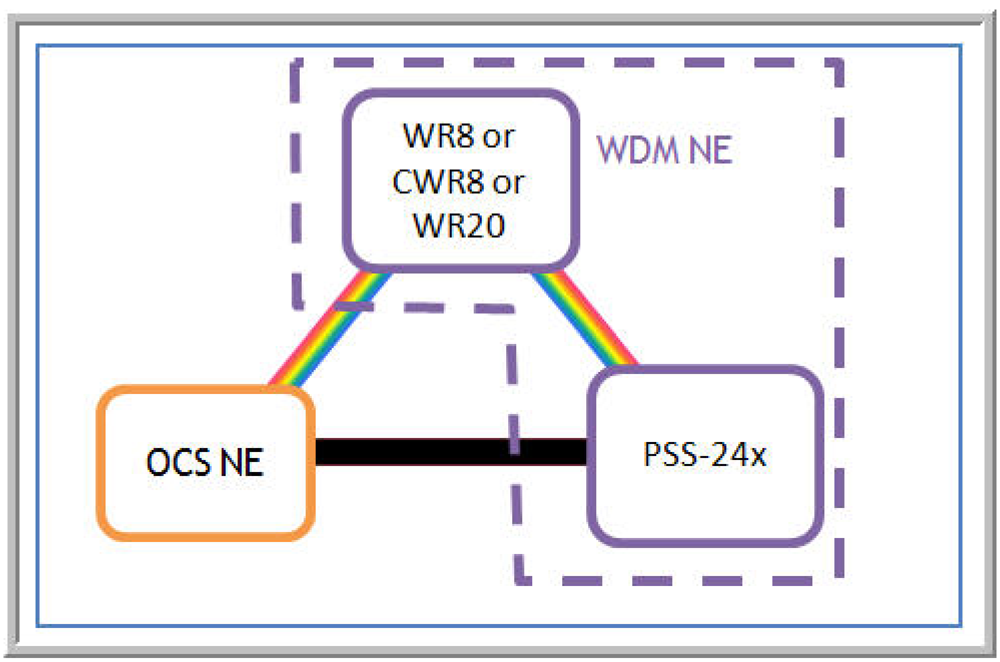
Figure 2-17 Nokia NE Configurations – Multi-NE Clusters – 1:N Configuration – UCM Support – Three 1830 PSS-OCS NEs



1830-PSS 24x Configuration

The 1830 PSS-24x can be a main-shelf with an 1830 PSS-32 in a single NE configuration or it can be the extension-shelf in an 1830 PSS-32 in a single NE configuration.

Figure 2-18 Nokia NE Configurations – Multi-NE Clusters – 1830-PSS 24x Configuration



Cluster configuration with 1830 PSS-24x

An NxM cluster configuration is obtained by combining the 1830 PSS-24x with an 1830 PSS SDWM NE. According to the number of the NEs, the following configurations are available:

- an NxM configuration where N is limited to two 1830 PSS SWDM and M to three 1830 PSS 24X (stand-alone).
- an NxM configuration where N is limited to one 1830 PSS 24X SWDM NE and M to one or two SWDM NE.

  Note:

  - 1830 PSS SWDM can be in compound configuration with an 1830 PSS OCS.

  - Managed plane is supported only for L0. L1 GMPLS supported on 1830 PSS-24x and 1830 PSS OCS if in compound with 1830 PSS SWDM, is already supported from previous releases.

  - NxM configuration with 1830 PSS R9.1, is limited to 2x2, meaning two 1830 PSS-24X SWDM NE and two SWDM NE.

Multiple 1830 PSS PHN and Multiple 1830 PSS OCS NE Connection Considerations

In general, if 1830 PSS PHN and 1830 PSS OCS NE configurations allow Multi-NE Clusters, that configuration is supported in the NFM-T.

2.10 NEs

NE definition

An *NE*, or a *Network Element*, is a unit of equipment within a network that performs specific transport and switching functions. Examples of transport and switching functions are amplification, regeneration, cross-connection, multiplexing, and packet switching.

Refer to "NE types" (p. 188) and "User interaction with NEs" (p. 188) for additional information.

NE types

The NEs that the NFM-T OTN system manages are of two types:

- A *directly managed NE* is a WDM NE that the NFM-T OTN application manages directly.
- An *indirectly managed NE* is a WDM NE that is managed directly by the NFM-T SDH application and indirectly by the NFM-T OTN application. Indirectly managed NEs are also referred to as *black boxes* or *virtual NEs* (*VNEs*).

User interaction with NEs

The management system enables users to discover an NE and to create an NE. Users can ping the NE, get NE information, and get the current NE status.

Users can perform MIB backups, download NE software, resynchronize the NE, start and stop supervision of the NE, and other NE-related tasks.

Users can also view lists of NE equipment, NE alarms, PM data, and remote inventories. Refer to the NE Operations section for detailed steps.

In addition, users can create subnetworks of NEs. Refer to "Subnetworks" (p. 189) for details.

NEs list

The NEs defined for a node, with the associated attributes and statuses is listed in the tabbed topics of a selected node from the **Operate > Nodes** navigation option. All the NEs in a network is also available from the **Operate > NEs** navigation option. Both lists provide the operations that are possible on a selected NE. See NE Operations in the *NFM-T NE Management Guide* for related information.

Columns represent the NE attributes and could be dragged to move towards left or right. Filtering and sorting could be applied to each column or attribute. Rows are representing NE instances; single and multiple selections are available. Actions or commands are applicable on the selected NEs according to the dynamic definition of the popup menu (right mouse click) or the icons displayed and enabled on the top right corner of the list. Attribute values displayed in this window are automatically updated when AVC notifications are received.

See the task View Nodes for accessing the list.

NE time configuration - important time setup

Network Elements and system components work internally in UTC/GMT0 and time stamps of data exchanged between NE and the Network Management System are in UTC/GMT0. The time stamps comes from Alarms, Events, PM Data, Command Logs: the GUI applications have the task to show time stamps in Local Time.

Open Interfaces also follow the same approach: IOO exports Alarms and PM Data with time stamp GMT0 and it will be up to OSS to show time stamp in Local Time.

For this reason to have a correct behavior on the collection of data that is time sensitive, it is mandatory to set the local time zone of each NE to UTC before supervising it with NFM-T. However, from Release 17.9, the NFM-T supports local time zone setting on NEs that support local time zone setting for PM and FM functions.

See also "Network Time Protocol (NTP)" (p. 356)

Subnetworks

A *subnetwork* is a user-defined group of NEs, VNEs, or other child subnetworks that helps the user to minimize network map crowding and to provision infrastructure connections (trails and logical links) and services within and between subnetworks.

A subnetwork is created from the physical connections view of the Network Map. Subnetwork names must be unique. Each subnetwork must be created with a minimum of one NE or one subnetwork. The creation of an empty subnetwork is prohibited. Any empty subnetwork is not displayed on the Network Map.

Users can modify and delete subnetworks. Modifications include the ability to add and remove NEs and to rename the subnetwork.

Guidelines and considerations for subnetworks include the following:

- A subnetwork is not a node.
- Any NE or NEs that forms a node cannot belong to different subnetworks; meaning, any NE or NEs that forms a node must be in the same subnetwork.
  Example: An 1830 PSS OCS NE and an 1830 PSS Photonic (PHN) NE that form a compound node through an uplink card must belong to the same subnetwork.
- A subnetwork can include other subnetworks.
- The members of a subnetwork can include NEs, VNEs, or other subnetworks.
- An NE or a VNE can only belong to one subnetwork.
- The number of NEs or VNEs that belong to one subnetwork is unlimited.
- NEs that reside in the staging area of the Network Map cannot be included in a subnetwork.

Refer to the **Network Maps** chapter in the *Getting Started Guide* for detailed steps regarding subnetworks.

2.11 Nodes

Node definition

A *node* is any NE or non-managed NE or a group of NEs or non-managed NEs.

A node can contain a single NE or two NEs that are linked together and are treated as a single unit.

Example: An 1830 PSS OCS and an 1830 PSS WDM NE form a single node when they communicate through an uplink card. Users can provision or view details of the NE pair from the NFM-T GUI menus.

Refer to "Nokia 1830 PSS nodes" (p. 190) and "User interaction with nodes" (p. 190) for additional information.

User interaction with nodes

From the node level, the management system enables users to create a port, modify a port, delete a port, and view all physical ports for a selected node, and view all contained ports for a selected node. In addition, users can create physical connections, along with OTN infrastructure connections (trails and logical links) and services from a selected node.

Users can perform OTN synchronizations of all information, alarms and events, system parameters, port parameters, protection groups, subnetwork connections, cross connections, optical connections, external topological links, transmission parameters, optical client connections, and ASAP audit configurations from a selected node. Configuration downloads can also be enabled and disabled from the node level.

For detailed procedures regarding NEs, refer to the Operate Equipment Manager and Node Operations sections.

Nokia 1830 PSS nodes

The Nokia 1830 PSS NEs support both WDM functions and OCS switching functions in one node, which is referred to as a *1830 PSS WDM/OCS* or a *compound* node.

- The *photonic compound* supports WDM functions with TOADM, ROADM, FOADM, and ILA configurations. It is often referred to as *WDM/photonic* or *WDM/PHN*.
- The *switching compound* supports mainly OCS or optical cross-connect system switching functions. It is often referred to as *OCS/switching*.

Uplink cards, such as the 11QCUP (10G), the 43SCUP (40G), and the 130SCUP (100G) in the switching compound, and the single variable (SVAC) and multiple variable (MVAC) attenuator cards in the photonic compound, are used to support the interworking of WDM and OCS.

Important! The 43SCUP configurations can also be made using the 130SCUP uplink card. For the 130SCUP uplink card, a 100G connection on an ODU4 can be provisioned.

1830 PSS-64 - 1830 PSS-36

The 1830 PSS-64 and the 1830 PSS-36 family of NEs are electrical or *OCS/switching NEs*. Refer to "1830 PSS OCS cross-connect fabric and TDM switching and grooming" (p. 173) and "1830 PSS OCS and 1830 PSS PHN interworking" (p. 178) for details.

1830 PSS-16 II - 1830 PSS-32

The 1830 PSS-16 II and the 1830 PSS-32 family of NEs are *WDM/Photonic (PHN) NEs*. Refer to "1830 PSS OCS and 1830 PSS PHN interworking" (p. 178) for details.

Nokia 1830 PSS-4 nodes

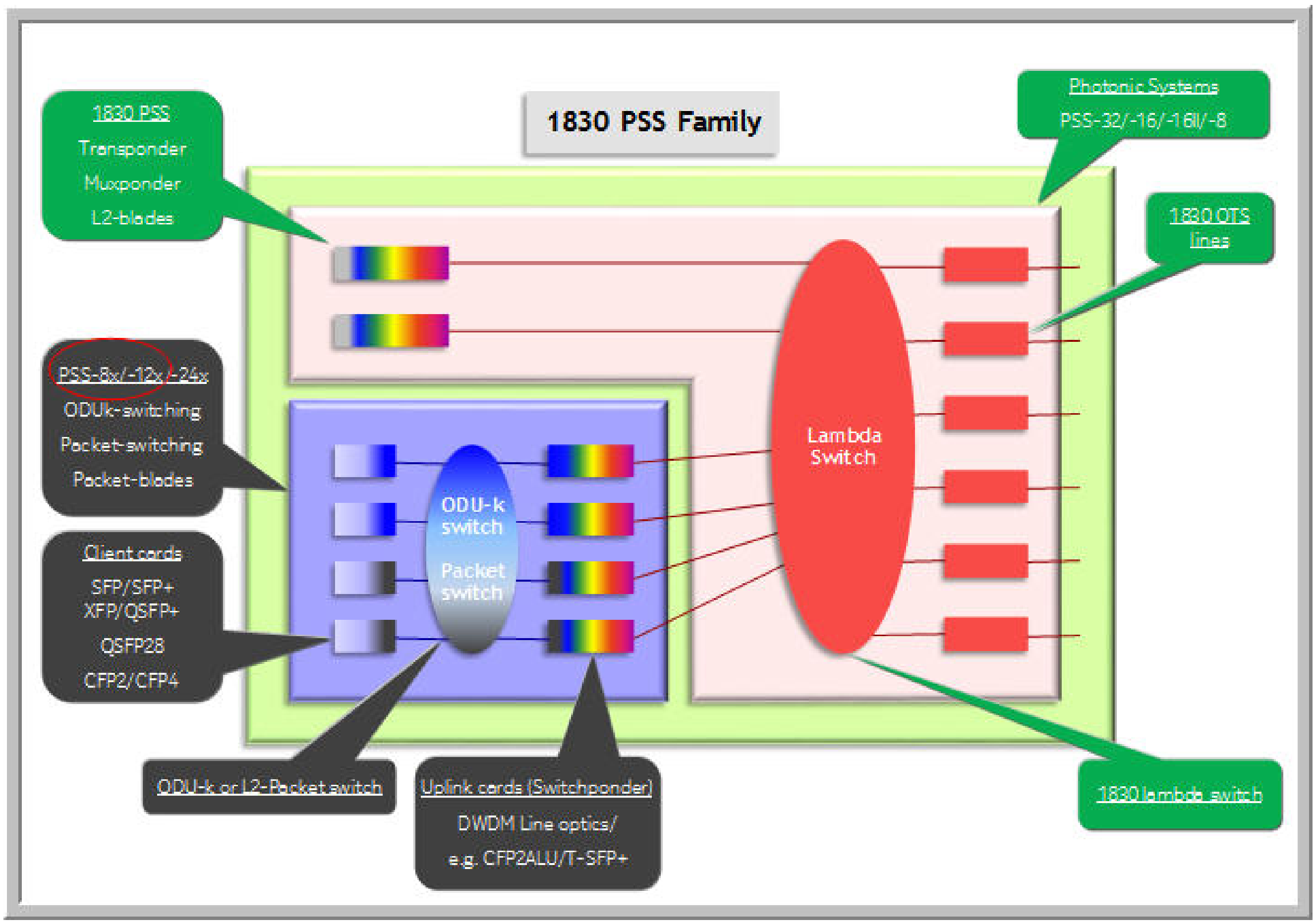
The 1830 PSS-4 NE is considered an *access NE* or *edge NE*. The 1830 PSS-4 NE can be connected directly to the 1830 PSS-36/1830 PSS-64 OCS NEs or to the 1830 PSS-16 II/1830 PSS-32 WDM/PHN NEs. Refer to "1830 PSS OCS and 1830 PSS PHN interworking" (p. 178) for details.

Nokia 1830 PSS-8x nodes

The 1830 PSS-8x is optimized for metro OTN switching applications. 1830 PSS- 8x is managed as stand-alone NE or as shelf of photonics NE.

The PSS-8X shelf supports a switch fabric card that provides non-blocking switch for all client and line cards inside the shelf, with ODU-0 switching granularity.

Figure 2-19 Nokia NE Configurations – 1830 PSS-32 NE with an 1830 PSS-8x Shelf



The 1830 PSS-8x functional block is highlighted in blue in the above figure.

1830 PSS-8x shelf can play the role of *Main* in a cluster configuration, or set as extension in case of SWDM main shelf with 1830 PSS-32 and 1830 PSS-16 II.

For 1830 PSS-8x R11.1 and onwards, NFM-T supports GMPLS management with L0 and L1 configurations with 2UX200 supporting 200G as an uplink card and 20AX200, 4MX200 as I/O cards.

Note: 1830 PSS-12x interworks with 1830 PSS-8x for L0 Control Plane connections and L0 L1 overlay connections.

Figure 2-20 1830 PSS-12X or 1830 PSS-8X with OTU4x2 Line in CDC-F – 100GbE Client, L0 CP

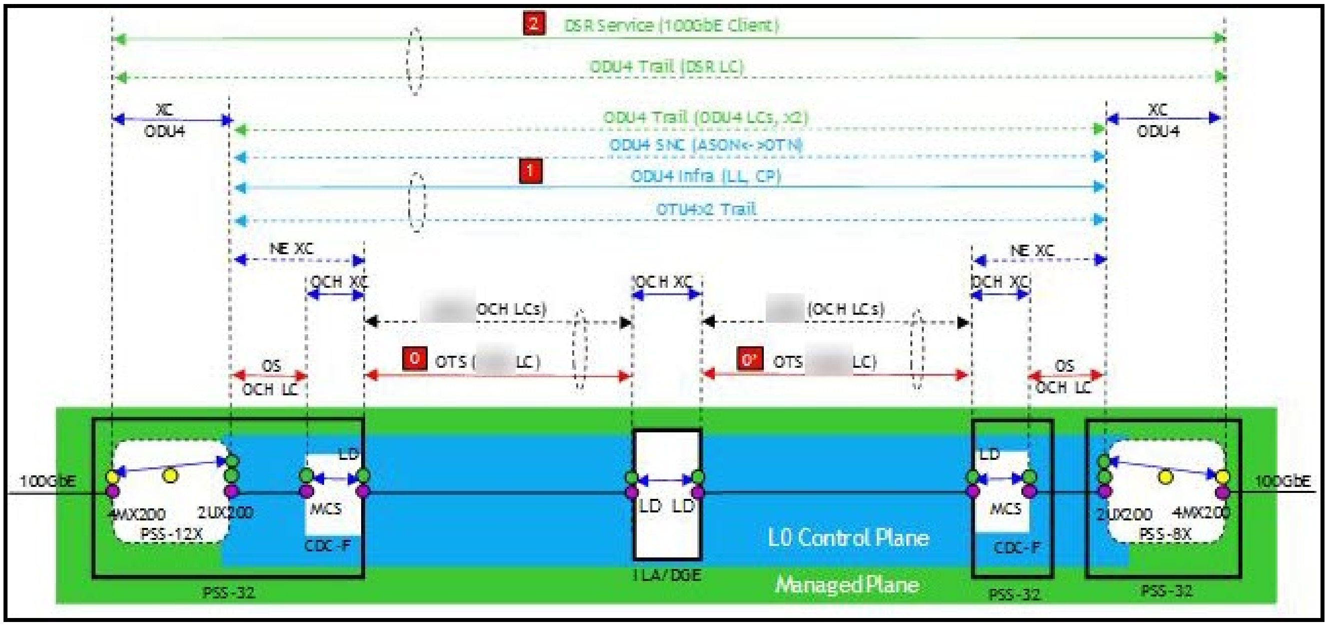
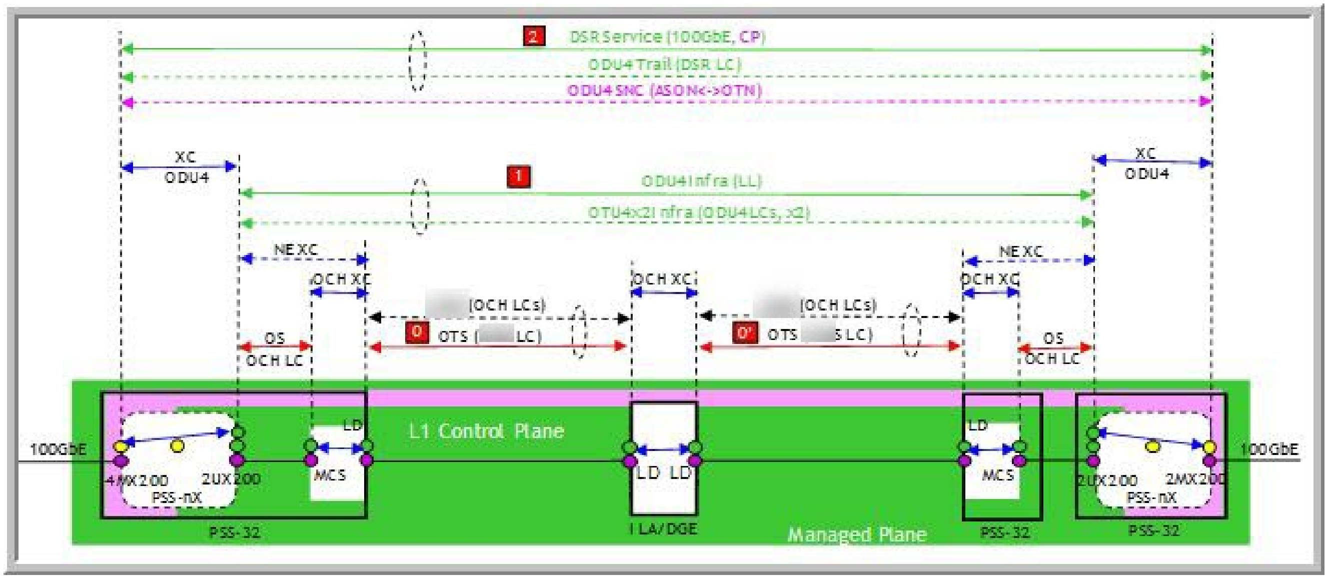


Figure 2-21 1830 PSS-12X or 1830 PSS-8X with OTU4x2 Line in CDC-F – 100GbE Client, L1 CP



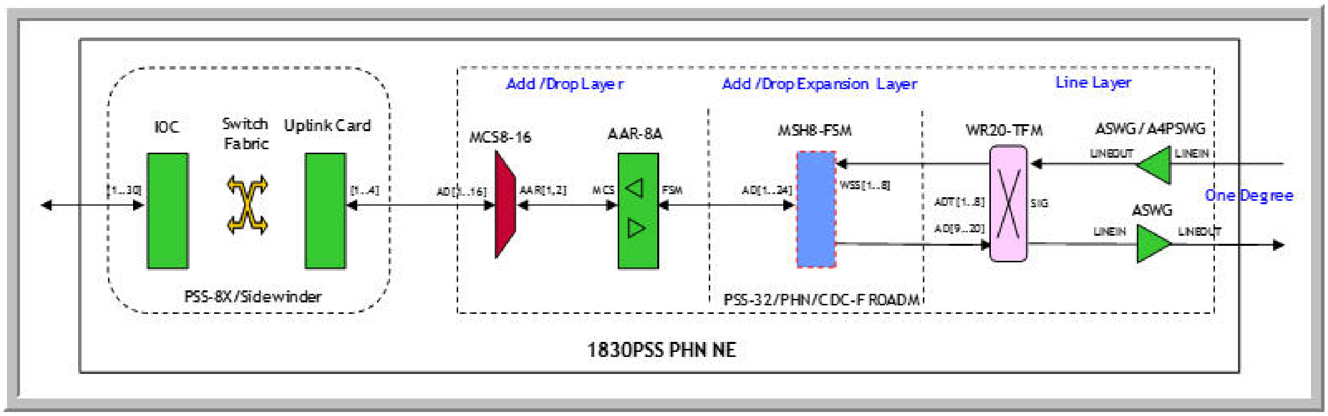
Circuit Packs	Specification	Pluggable Support
20MX80	I/O Card which supports 4x10G (SFP+) and 16 x sub-10G (SFP) interfaces	For a 10GbE port, the pluggables SL64TU and SL64TUW are supported on port 17 to port 20. For a 10GbE port, the pluggable SL64TU is supported on port 17 to port 20 as Client card.
20AX200	Uplink/Client card capable to support 20 x 10G (SFP+) interfaces Managed as IO card only in L1 Control Plane.	For a 10GbE port, the pluggables SL64TU and SL64TUW are supported on port 13 to port 20 as Uplink card. For a 10GbE port from 1830 PSS R13.0.4, the pluggable SL64TU is supported on port 1 to port 20 as Client card.
1Ux100	Coherent Uplink Card that supports 100G PDM-QPSK with HDFEC and SDFEC-G2 feature	-
2UX200	200G Uplink Card	-

Circuit Packs	Specification	Pluggable Support
4MX200	I/O Card which supports 2 x 100G mode with 2 x 100G QSFP28 pluggables as client pack on 1830 PSS-12x and 1830 PSS-8x in L1 and L0 GMPLS network.	-

Note: When provisioning a client signal of 10GbE using the DWDM interface pluggables, the A-end and Z-end can use different pluggables (DWDM or non-DWDM, with or without keys on DWDM), however the pluggables at both the ends must be for 10GbE client.

The next figure outlines a schema to provide an example of the 1830 PSS-8x transmission connectivity.

Figure 2-22 1830 PSS-32 NE with an 1830 PSS-8x Shelf in CDC-F ROADM – Pack View



The 1830 PSS-8x is equipped within the 1830 PSS-32 NE, and the fiber connections between 1830 PSS-8x Uplink cards to the PSS PHN MUX/DeMUX packs are considered as internal topological links.

Network configurations

The PSS-8x card supports the following network configurations:

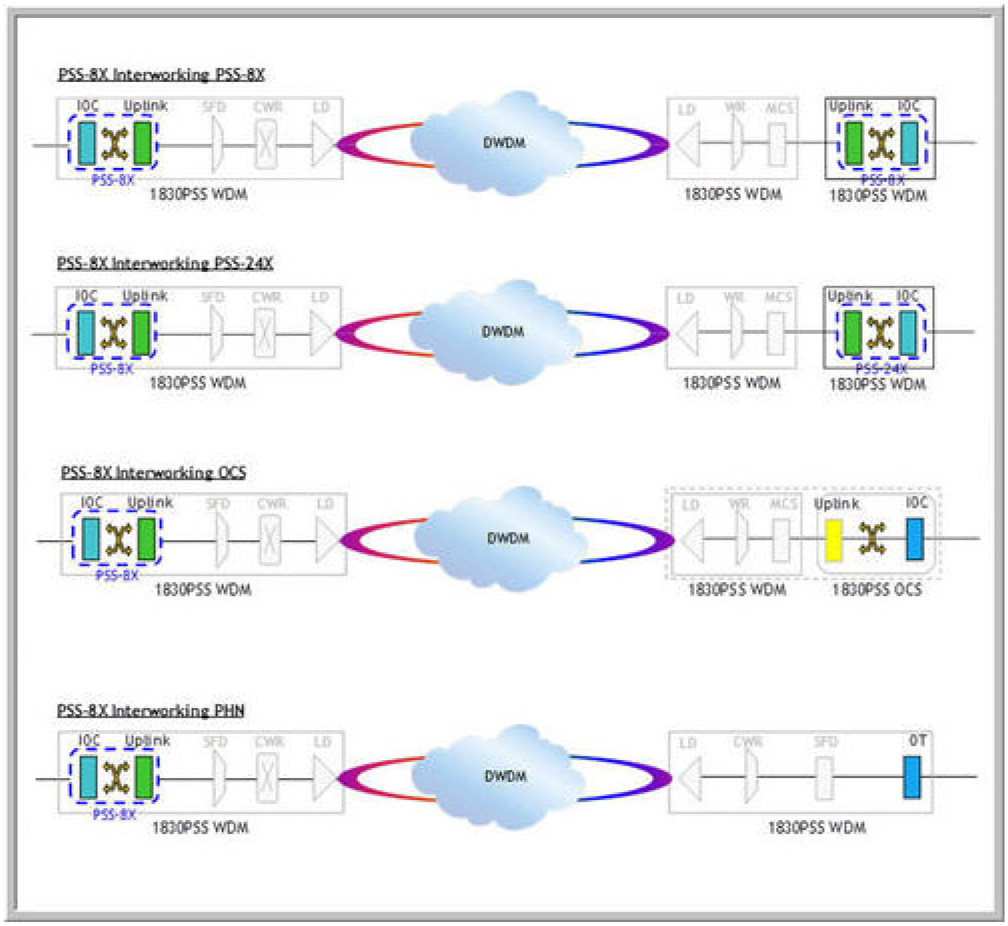
- CDC-F with Flexgrid Phase I support.
- AC-DC with Flex Grid Phase I support.
- WR8-88AF ROADM with Flex Grid Phase I support.

The supported network interworking scenarios are those summarized below and outlined in the next figure:

- PSS-8x interworking with another PSS-8x.
- PSS-8x interworking with PSS-24x.
- PSS-8x interworking with PSS OCS.

- PSS-8x interworking with PSS PHN.

Figure 2-23 PSS-32 with PSS-8X – Network View



SFDC8 support

SFDC8 is a Compact 8ch Static Filter DWDM – DWDM optical channel filter (MUX and DeMUX) pack. There are five variants of this card, each variant is able to Add/Drop 8 100GHz spaced channel and provide an additional expression port for through connection in Multi-degree FOADM, or Filter cascading. The pack is made for low cost 8-channel SFD in ½ height and single slot.

The SFDC8 card is supported by 1830 PSS-32 NEs, starting from R10.0 with 1830 PSS-8 and 1830 PSS16II shelves.

Main Functions for this card are:

- 8-channel SFD.
- Supporting Add/Drop and THRU OCH channels.
- Add/Drop and THRU 100G spaced channels, 192.1THz to 196.0THz (Exp port support channel

plan from [1970..9600]) – 40 continuous channel frequency support (different from the existing SFD8), THRU port support full 44 DWDM channels.

- Total input/output Optical Performance Monitoring.
- Cascading between SFDC8 is allowed, but not recommended.
- Interwork with legacy filters/SFDs.
- EPT support.

Nokia 1830 PSS-12x nodes

The 1830 PSS-12x provides a higher capacity OTN switch function within the existing 1830 PSS-32 NE. The 1830 PSS-12x shelf supports switch fabric cards that provide non-blocking switch for all clients and line cards inside the shelf, with an ODU-0 switching granularity.

The 1830 PSS-12x is managed as an extend shelf of the 1830 PSS-32 photonic NE, or as a stand-alone NE. The client packs (IOC) and uplink cards are used on both 1830 PSS-12x and 1830 PSS-8x shelves.

The 1830 PSS-12x switching capacity is of 4.8 Tb/s, and requires the ODUk switch fabric packs to allow ODUk cross-connects among a group of 1830 PSS-12x packs.

The 1830 PSS-12x with L1 GMPLS is compatible with overlay configuration with photonic L0 GMPLS active in 1830 PSS SWDM. The 1830 PSS-12x supports L0 GMPLS with overlay configuration (@200G & @100G). L0 GMPLS applies to all 1830 PSS-12x photonic nodal configurations (C-F, CD-F, CDC-F, Config D, D', D"), and all supported circuit packs. L1 GMPLS on 1830 PSS-12x supports the “intra-node” links, that are links internal to 1830 PSS SWDM NE connecting the 1830 PSS-12x.

1830 PSS-12x supports the following Control Plane configurations:

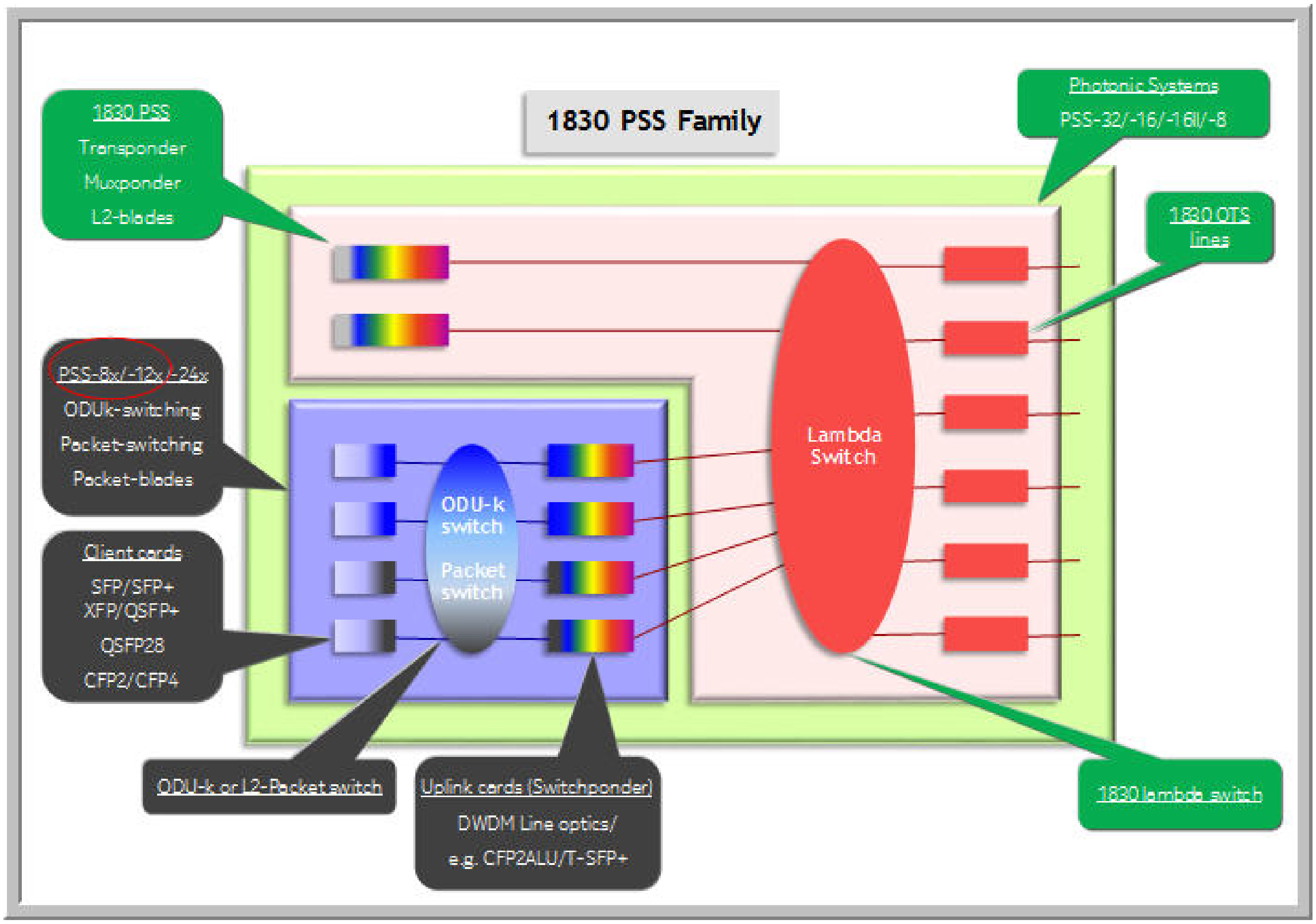
- L0 GMPLS Control Plane
- L1 GMPLS Control Plane
- L0-L1 overlay

1830 PSS-12x interworks with 1830 PSS-8x for L0 Control Plane connections and L0-L1 overlay connections. For more information, see Figure 2-21, “1830 PSS-12X or 1830 PSS-8X with OTU4x2 Line in CDC-F – 100GbE Client, L1 CP” (p. 193) and Figure 2-20, “1830 PSS-12X or 1830 PSS-8X with OTU4x2 Line in CDC-F – 100GbE Client, L0 CP” (p. 192).

For information on OTU4 scenarios for 1830 PSS-12x interworking with 1830 PSS-8x, see Figure 2-25, “1830 PSS-12x/1830 PSS-8x with OTU4 Line in CDC-F – 100GbE/ODU4 Client, L0 CP” (p. 199) and Figure 2-26, “1830 PSS-12x/1830 PSS-8x with OTU4 Line in CDC-F – 100GbE/ODU4 Client, L1 CP” (p. 200).

MRN configuration and Cluster configurations are not supported.

Figure 2-24 Nokia NE Configurations – 1830 PSS-12x shelf equipped within 1830 PSS-32 NE



The 1830 PSS-12x functional block is highlighted in blue.

The 1830 PSS-12x shelf along with its circuit packs is equipped within a 1830 PSS-32 NE.

Figure 2-25 1830 PSS-12x/1830 PSS-8x with OTU4 Line in CDC-F – 100GbE/ODU4 Client, L0 CP

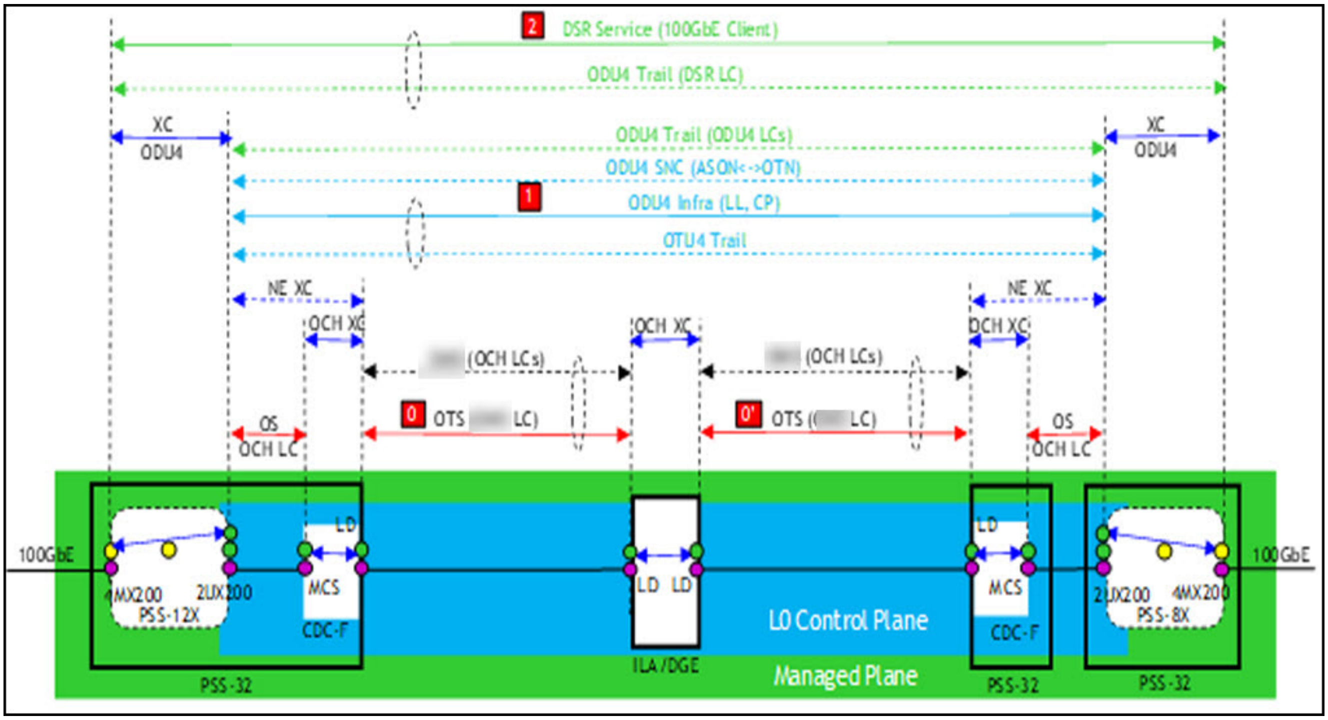
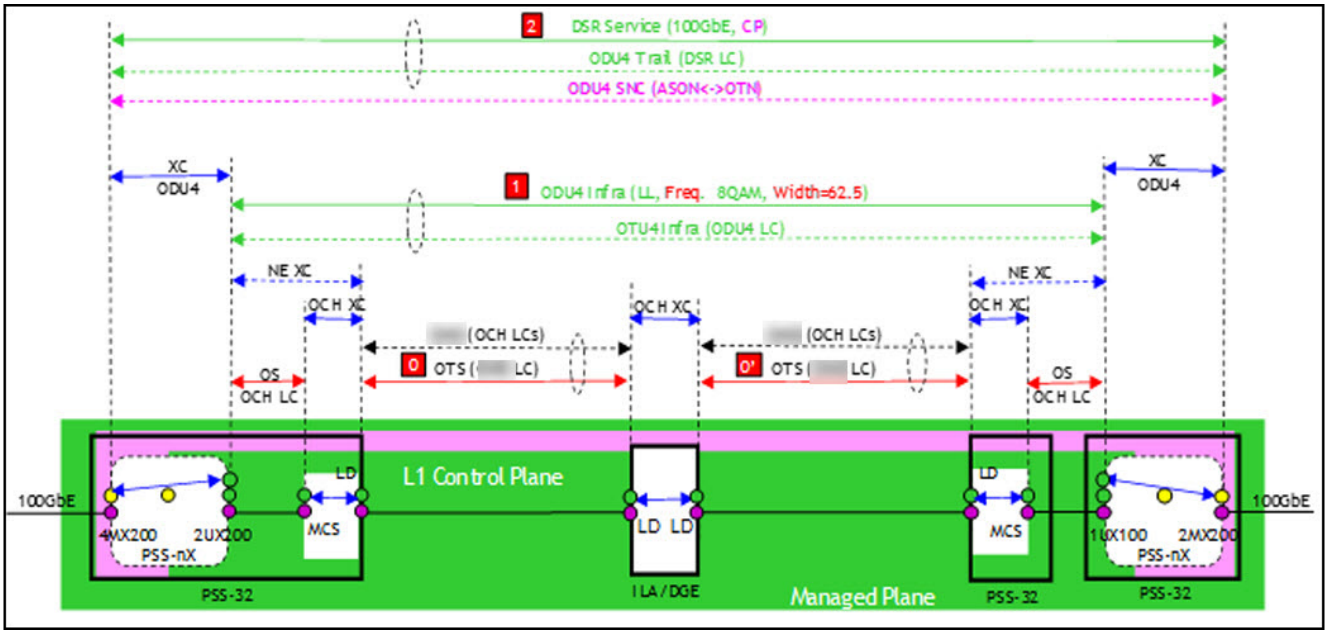


Figure 2-26 1830 PSS-12x/1830 PSS-8x with OTU4 Line in CDC-F – 100GbE/ODU4 Client, L1 CP



1830 PSS-12x shelf play the role of *Main* as standalone or in a cluster configuration, or set as extension in case of SWDM main shelf with 1830 PSS-32 and 1830 PSS-16 II.

The following circuit packs can be equipped on the 1830 PSS-12x shelf:

Circuit Packs	Specification
20MX80	MultiRate switch card (20 ports), IOC, 16 ports sub-10G rates, 4 ports 10G with or without WT
20AX200	20x10G I/O or uplink card, AnyRate switch card (20 ports), IOC, 8 ports WT capable
1UX100	1x100G uplink card (1 port)
2UX200	2x100G, 1x200G uplink cards (2 ports)
4MX200	2x100G/4x40G Client IO card (4 ports)

In the circuit pack 20MX80, the pluggables SL64TU and SL64TUW are supported on port 17 to port 20. For 20MX80, the pluggable SL64TU is supported on port 17 to port 20 as Client card.

In the circuit pack 20AX200, the pluggables SL64TU and SL64TUW are supported on port 13 to port 20. For 20AX200, from 1830 PSS R13.0.4, the pluggable SL64TU is supported on port 1 to port 20 as Client card.

These pluggables are used to create logical links.

Note: When provisioning a client signal of 10GbE using the DWDM interface pluggables, the A-end and Z-end can use different pluggables (DWDM or non-DWDM, with or without keys on DWDM), however the pluggables at both the ends must be for 10GbE client.

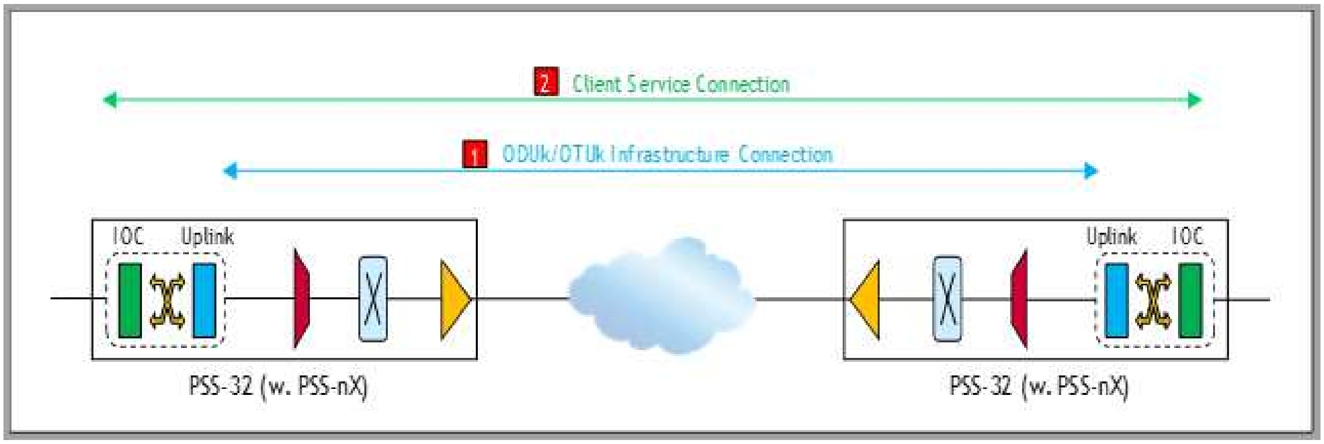
2UX200 as uplink and 20AX200 as IO are supported for L0 CP, L1 CP, and L0-L1 CP overlay scenarios for 1830 PSS-12x shelf in PHN NE.

End-to-End Connection

The following integrated connection provisioning are supported in 1830 PSS-12x:

- HO-ODUk/OTUk Infrastructure connection provisioning (Protected and Unprotected)
- Client service connection provisioning (Protected and Unprotected)

Figure 2-27 1830 PSS-12x End-to-End Connection



1830 PSS-12x Node Management

The maximum number of 1830 PSS-12x shelves is 8 and following 1830 PSS-12x related shelf configurations are supported:

- 1830 PSS-12x as standalone main shelf.
- 1830 PSS-12x as main shelf, with up to 8 shelves per NE (a mix of shelf types are allowed).
- Any combination of 1830 PSS-8, 1830 PSS-8x, 1830 PSS-12x, 1830 PSS 24x, 1830 PSS 16, 1830 PSS 16II, and 1830 PSS 32 shelves is supported by the 1830 PSS-32 NE, where the maximum number of 1830 PSS 8 +1830 PSS 8x +1830 PSS 12x + 1830 PSS 16 + 1830 PSS 16II + 1830 PSS-24x + 1830 PSS-32 shelves is 24 (including the main shelf, 1830 PSS-8 cannot be a main shelf for 1830 PSS-12x).

The NFM-T supports different node types, including:

- Cluster configurations. For example, one 1830 PSS-12x standalone NE and one 1830 PSS PHN NE.
- Dangling OT configuration (1830 PSS-12x using a 3rd party line system)

- Compound node (including all the supported shelf combinations on the PHN NE).
- PHN and OCS NEs formed multi-node clusters.

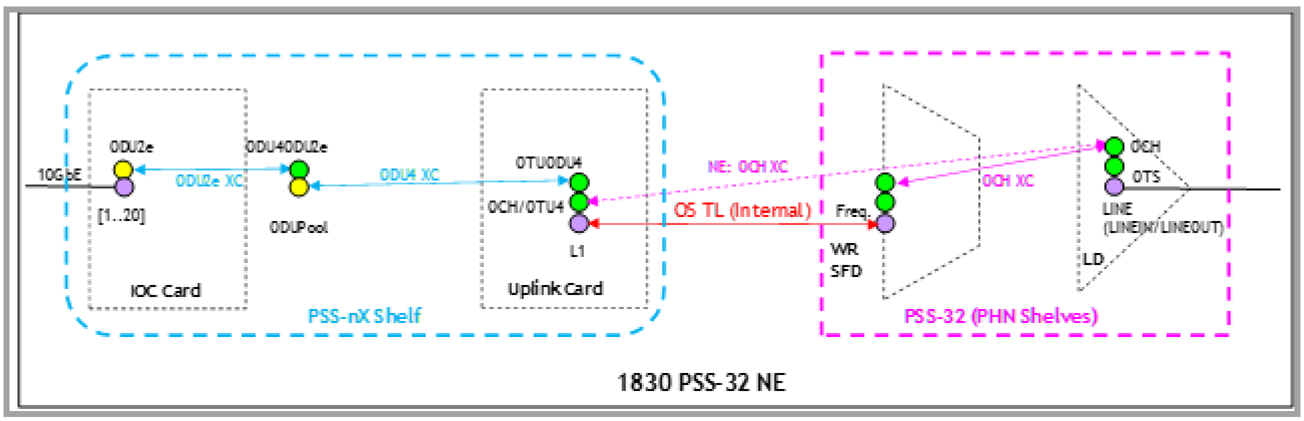
The 1830 PSS 12x shelves are used in the following optical architectures:

- ROADM (legacy ROADMs, including Config. D, D', D").
- FOADM
- TOADM
- CDC-F ROADM
- C-F or AC-DC ROADM
- iROADM ROADM

The 1830 PSS-12x supports the following types of cross connections:

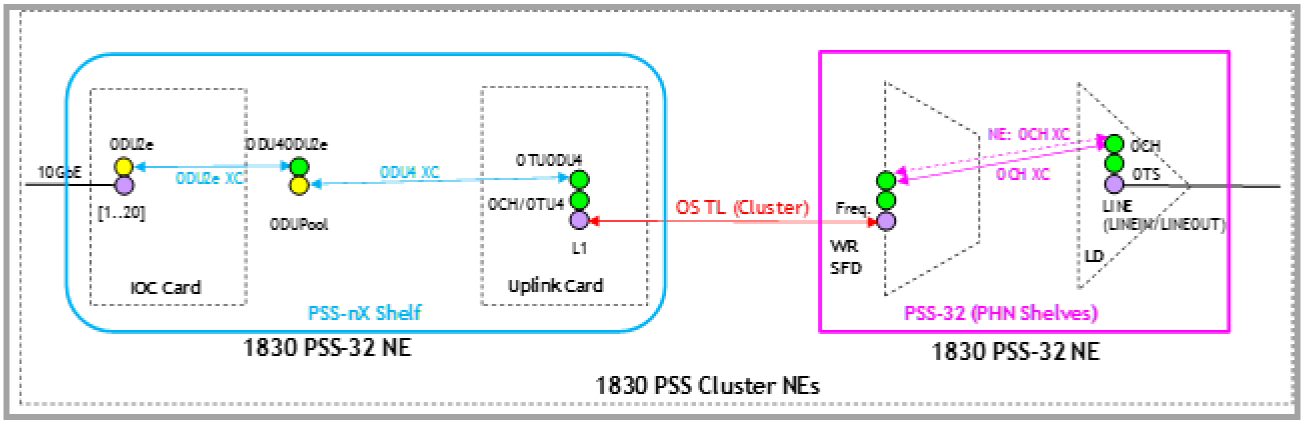
1. ODUk XC: within the 1830 PSS 12x shelf (in Blue)
2. OCH XC: between 1830 PSS 12x uplink card and WDM MUX/DeMUX pack (in Pink)

Figure 2-28 Cross connects supported by 1830 PSS-nX and 1830 PSS PHN – within One NE



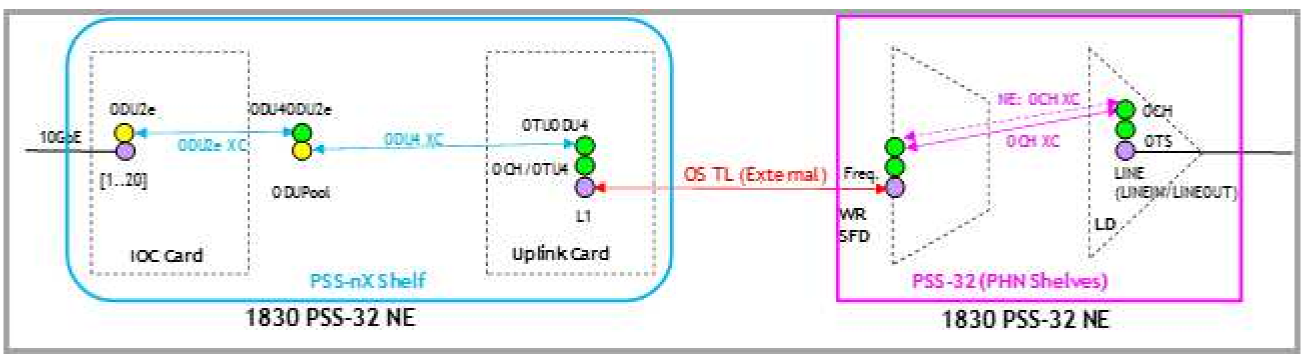
When an 1830 PSS-nX shelf and PHN shelves are within one NE, the OS topological link (TL) is Internal. The NE OCH XC (Dashed Pink line) is between Uplink line port and LDs.

Figure 2-29 Cross connects supported by 1830 PSS-nX and 1830 PSS PHN – with Cluster Configuration



When an 1830 PSS-nX shelf and PHN shelves are two different NEs within one Cluster, the OS topological link (TL) in Cluster. The NE OCH XC (Dashed Pink line) is only within the PHN NE, between SFD/MCS/PSC/Frequency Add/Drop ports and LDs.

Figure 2-30 Cross connects supported by 1830 PSS-nX and 1830 PSS PHN with Dangling OT Configuration



When an 1830 PSS-nX shelf is a Drop shelf, and Line system is a 3rd party (or 1830 PSS PHN), the OS topological link (TL) is External. The NE OCH XC (Dashed Pink line) is between Uplink line port and LDs. 1830 PSS-nX Uplink line port needs to be manually provisioned (frequency tuning, power level setting, and so on.)

Network Configurations

The 1830 PSS-12x card supports the following network configurations:

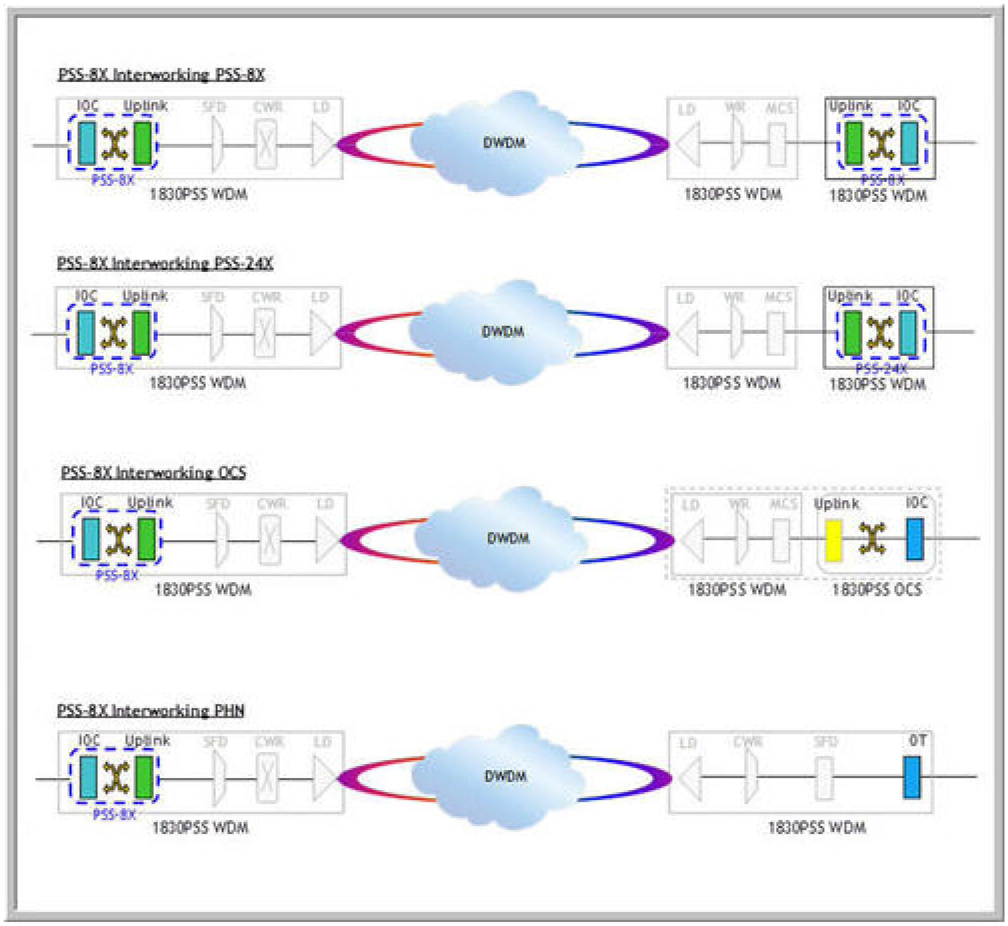
- CDC-F, C-F, WR8-88AF ROADMs with fixed grip or Flexgrid support
- Legacy ROADMs, TOADMs, FOADMs with fixed grid support

- Existing configurations supported by 1830 PSS-8x (1830 PSS-24x)

The supported network interworking scenarios are those summarized below and outlined in the following figure:

- 1830 PSS-12x interworking with 1830 PSS-8x.
- 1830 PSS-12x interworking with 1830 PSS-24x.
- 1830 PSS-12x interworking with Falcon (N/A).
- 1830 PSS-12x interworking with 1830 PSS OCS.
- 1830 PSS-12x interworking with 1830 PSS PHN.

Figure 2-31 1830 PSS-32 with 1830 PSS-12x – Network View



2UX200

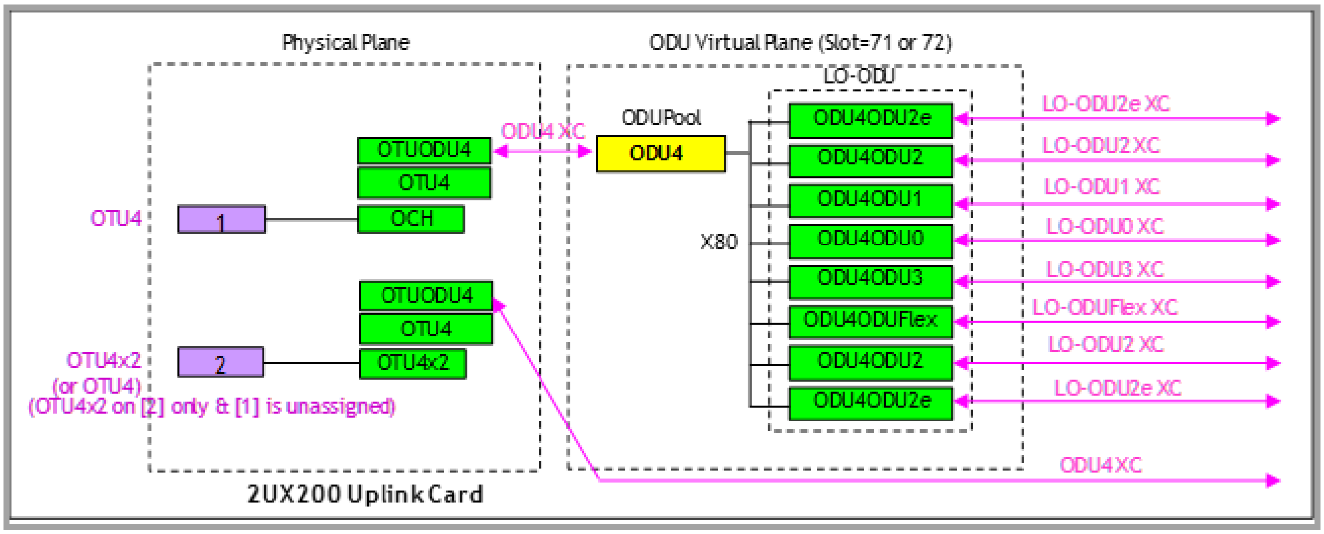
2UX200 is an Uplink card for the 1830 PSS-12x and 1830 PSS-8x shelves. It is a 100G/200G two port coherent Uplink card, using C4ACO pluggables (CFP4, PSE 3c, up to 2), with single slot and full height, supporting Uplink card configurable for 100G QPSK and 200G 16QAM. 2UX200 will support both Control Plane and Manage Plane. 2UX200G @200G supports L0 L1 Control Plane and Manage Plane.

2UX200 supports either 100G line (OTU4) on ports 1 and 2, or 200G line (OTU4x2) on port 2. It also supports both unprotected and protected cross connects (SNCP).

NFM-T provides support for 20MX200 port 17-20 and 20AX200 all ports (1-20) with 10GbE/ODUFLEX.

Example: During connection provisioning, the user can create a unprotected connection with 20AX200 on one end and 20MX80 on the another end with the **Service Rate** as **Flexible Rate Client** and **Container** field set to **ODUFlex**. The **ODUFlex Bandwidth** field must be set to 10.

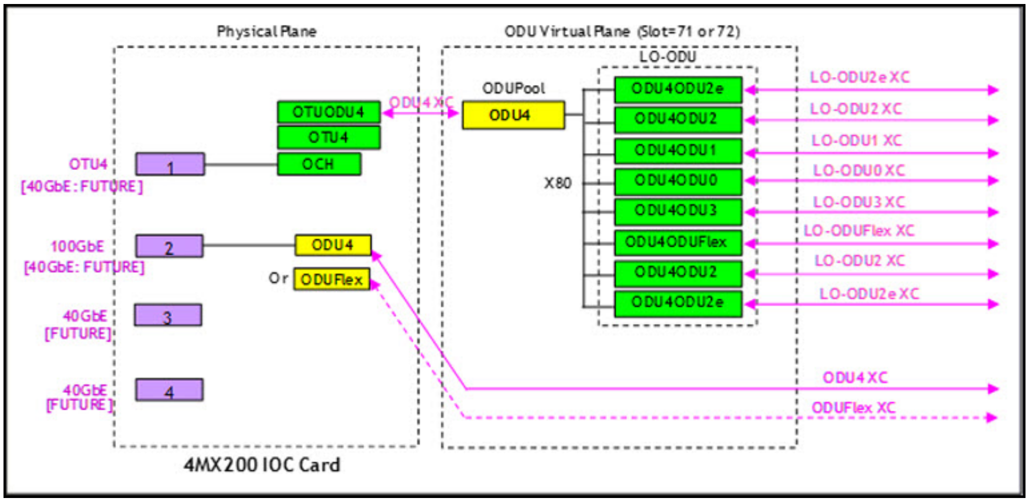
Figure 2-32 Optical Model for 2UX200 – Ports and Crossconnects



4MX200

4MX200 is a 100G multirate Input/Output (IO) card for 1830 PSS-12x and 1830 PSS-8x shelves, with a total capacity of 200G ODUk. The pack can have up to 2x 100GbE/OTU4 Optical Module (QSFP28) in 1830 PSS R11.1 and NFM-T R19.2. This card is supported only for managed plane connections.

Figure 2-33 Optical Model for 4MX200 – Ports and Crossconnects



4MX200 supports the following:

- 100GbE and OTU4 clients on ports 1 and 2.
  Port 3 and port 4 is not supported in NE Release 11.1
- Client signals of 100GbE with the **Container** set to ODU4 with GFP-F, and OTU4.
- Client-to-client connection, which means a connection can be established from an 4MX200 card to another 4MX200 card with SNCP protection. 4MX200 interworks with 2UX200 uplink card or any transponders.
- Colored optical module without wavelength tracker encoder. This must be supported for interworking with other 1830 PSS NEs.

Nokia 1830 PSS-24x nodes

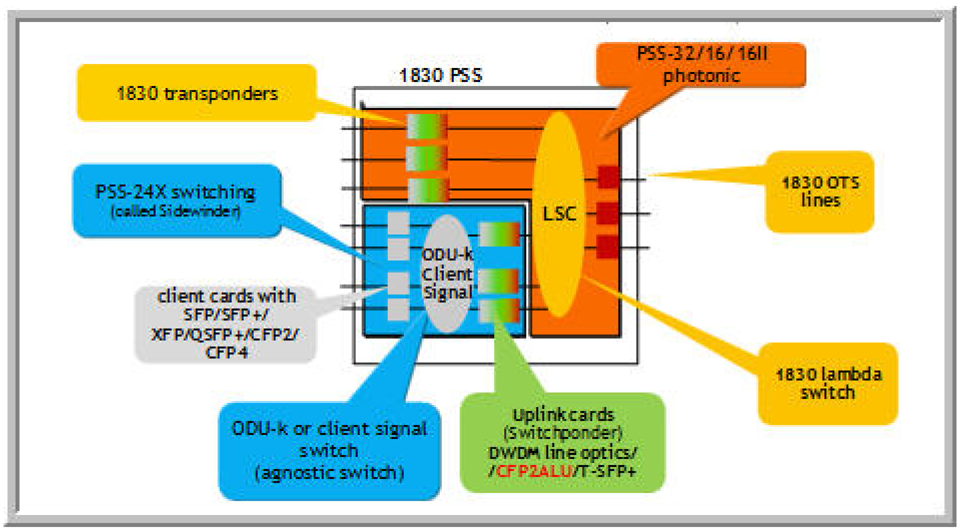
The 1830 PSS-24x is used to optimize 1830 PSS NE configurations for core packet and/or optical transport network (OTN) switching applications. It can be used in 1830 PSS PHN NEs (1830 PSS-32/1830 PSS-16 II NE) configurations as a main shelf or as the extension shelves. It provides L1 switching features and can also be used as a standalone 1830 PSS PHN NE. The 1830 PSS-24X can be included in compound 1830 PSS PHN/1830 PSS OCS node configuration.

GMRE supports interworking L1 with Uplink in PSS24X shelf and MUX in PSS32 main shelf in case of single NE, along with L0 GMPLS.

Supported interface circuit packs include the 2UC400 (uplink card that supports tunable frequency, optical power, and wave keys), 4UC400 (4x100G regional/long-haul transport), 4AN400 (an IOC pack and its supported client signal rates are 100GbE and OTU4), and the 30AN300 (an IOC pack that supports 10GbE, OC-192, STM-64, OTU2, OTU2e as possible client signal rates).

1830 PSS-24x supports 30SE300 and 6SE300 cards. 30SE300 can be configured on 1 to 20 card slots and 6SE300 can be configured on 1 to 24 card slots on the 1830 PSS-24x shelves in Packet Switch configuration.

Figure 2-34 Nokia NE Configurations – 1830 PSS-32 NE with an 1830 PSS-24x Shelf



1830 PSS-24x cards (30SE300 and 6SE300) support Managed Plane connections, L1 Control Plane connections, and MRN tunnels. For more information, see "MRN and L1 Control Plane support for L2 cards" (p. 1391).

1830 ONE family of nodes

The NFM-T supports the management of the 1830 Optical Network Extender (ONE). The platform family includes the Aggregator (1830 ONE-a) version and the Hub (1830 ONE-h) version. Each version can be installed separately or mixed according to the network needs and the type of service to be transported.

The 1830 ONE provides efficient migration of PDH and SDH traffic to an OTN network. The 1830 ONE Aggregator primarily aggregates E1 services over an OTU1 signal while the 1830 ONE Hub is used to close aggregation rings and aggregate STM-N traffic over an OTU1 or an OTU2 signal.

Both platforms manage Micro OTN (µOTN) traffic, mapping the E1 signal into an ODUε (epsilon) container.

1830 LX nodes

The 1830 LX, which can be thought of as the *1830 Link eXtender*, is a standalone NE that functions as a repeater. The 1830 LX can be provisioned in Managed Plane and Control Plane configurations for submarine or for long haul terrestrial applications in conjunction with 1830 PSS-32 NEs in DWDM networks.

The 1830 LX is one of four types: Booster, CO-RAMAN, RAMAN, or ROPA. The 1830 LX NE is a two rack unit that functions in one direction, either transmit or receive. For bi-directional applications, on one OTS link, different 1830 LXs can function in two directions, one as transmitter and the other as receiver. In addition, the 1830 LX can be installed at different at termination points; for example: one side can be a booster; the other side can be a RAMAN.

The 1830 LX is managed as stand alone NE. Refer to the procedure *Add 1830 LX Information* for provisioning details and refer to 7.35 “Manage repeaters for an OTN OTS physical connection” (p. 850) for details on how to associate a repeater with an OTN physical connection.

NFM-T supports 1830 LX single span and multispan configurations. NFM-T supports 1830 LX single span with Control Plane L0 GMPLS, where as multispan is supported with both Managed Plane and Control Plane. The 1830 LX supports subsea or super long-haul application, with a set of amplifiers, and 1830 LX OSC-WC boxes.

External OTS link is created between the amplifiers of the 1830 PSS NE. The user has to manually associate 1830 LX to the OTS. With this configuration, the OTS link is not created as long span links.

NFM-T supports flex-grid channels over OTS physical connection with all the configuration types of 1830 LX and 1830 LX OSC-WC NEs.

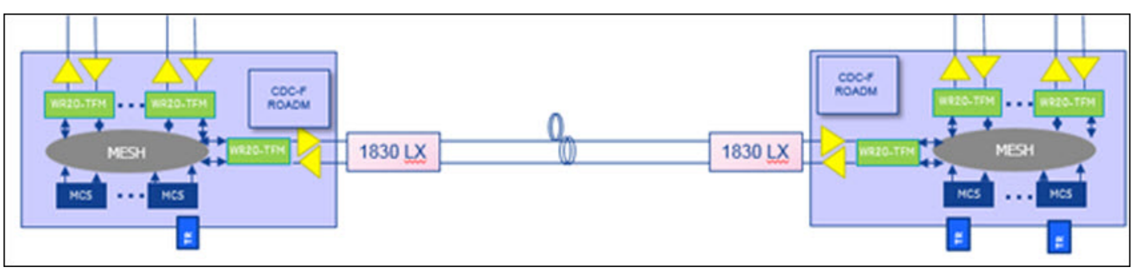
NFM-T supports MRN Terminated OTSig tunnel creation that are correlated to 1830 LX. MRN Terminated OTSig tunnel is supported for ADD4 cards such as S4X400H, DFC12, and DFC12E, S5AD400H.

Single Span Configuration

In single span configurations, the connections pass through single OTS with 1830 LX NEs, that is, supports the association of an 1830 LX box to its ROADM or ILA degree (or OTS) port. Multiple 1830 LX boxes can be associated to one ROADM degree. Each 1830 LX NE is associated to 1830 PSS NE.

The supported Grid Spacing on the OTS link is 100 GHz.

Figure 2-35 1830 LX Single Span Configuration



Multispan configuration

In multispan configurations, the connections pass through multiple OTS links with multiple 1830 LX NEs and multiple 1830 PSS NEs.

Note: 1830 LX multi span in GMPLS network is supported only for CDC-F configuration.

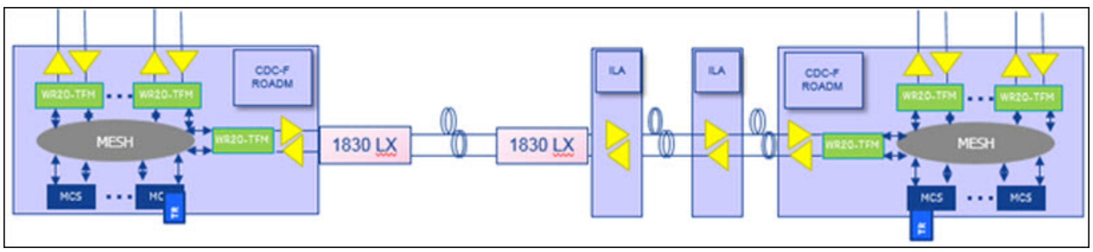
Note: NFM-T supports 1830 LX multispan support on a ROADM standard degree for L0 Control Plane and Managed Plane connections (without the need of an extra FOADM). Following WSS/ROADM configurations are supported:

- iROADM9R - C-F configuration
- iROADM20 - CDC-F configuration

The minimum allowed frequency on the OTS is 9190.000, which is specified in channel mask of wavelength parameters related to the OTS ports.

Note: Ensure that the Grid Spacing is set to 50 GHz or 100 GHz in the EPT and uploaded to NFM-T. When the 1830 LX is associated with OTS, the frequency range is reduced from 88 channels (9170-9605) to 84 channels (9190-9605).

Figure 2-36 1830 LX Multispan Configuration



Manage 1830 LX configuration

Complete the following steps to manage 1830 LX multispan configurations:

1

From the NFM-T GUI, navigate to **Operate > Physical Connections** page and check that the OTS connection is created.

Ensure that the OTS connection is created with the same type of amplifier card.

2

Associate the OTS physical connection to the Repeater. To manage repeaters, see 7.35 “Manage repeaters for an OTN OTS physical connection” (p. 850).

3

Configure the following infrastructure connection:

1. Create an ASON Routed Logical Link infrastructure connection with Trail/Link as the Routing Constraint.
2. Select the OTS physical connection that is associated to the repeater as the Routing Constraints.
3. Deploy the connection.
4. Check the **Current Route** and the **Nominal Route** of the connection in the **Operate > ASON > SNCs** page.

4

Create a service with 1830 PSS NEs and an amplifier or muxponder cards on the **From/To NEs** and **From/To ports**.

Some of the supported cards for this configuration are:

- 2UC400 (QPSK/OTU4)
- 130SNX10, 260SCX2 (QPSK/OTU4)
- 130SCA1, 130SCX10 (QPSK/OTU4)
- 4UC400 (2AC100H) (QPSK/OTU4)
- 4UC400 (2AC100) (QPSK/OTU4)

Result: The configuration is established.

END OF STEPS

1830 LX flex grid support

The 1830 LX supports flex-grid network to support channel spacing used in ADD4 cards. 1830 LX supports all the configuration types supported by Flex Grid such as CDC-F, C-F, iROADM20, iROADM9R, ROADM, 100GbE client support for D5X500, and config D with amplifier cards. This support is extended to Managed Plane and L0 Control Plane connections.

Complete the following steps to enable Flex Grid and create an end-to-end connectivity for the same:

1. In the GMRE data bearer, set the following parameters:
   - **Fiber Type**
   - **Maximum Allowed Channels**
   - **Chromatic Dispersion**
   - **Flex Grid Granularity**
   - **Polarization Mode Dispersion**
   - **Submarine Grid Type**

   Ensure the number of channels supported is 84, that is the wavelength is 9190 to 9605.

   The **Flex Grid Granularity** supported is 100 GHz.

2. From the NFM-T GUI, navigate to **OPERATE > Physical Connections**.
3. In the **Physical Connection** page, ensure the **Flex Grid Capable** column is enabled.
4. If the **Flex Grid Capable** column is **Yes**, associate the OTS physical connection to 1830 LX by adding the repeaters. See 7.35 "Manage repeaters for an OTN OTS physical connection" (p. 850)
5. Create an infrastructure connection on the OTS physical connection associated to 1830 LX. For Control Plane connection, reduced channel that is supported is included automatically for automatic routing. For more information on infrastructure connection, see 8.4 "New service/ infrastructure connection" (p. 1219).
6. Create an service on the infrastructure connection to manage the end-to-end network. For more information on service connection creation, see 8.4 "New service/infrastructure connection" (p. 1219).

Nokia 1830 LX OSC WC nodes

The 1830 LX OSC-WC (Optical Supervisory Channel Wavelength Converter), is a new 1830 LX box that is used to extend the reach of 1830 PSS OSC in 1830 LX applications. 1830 LX OSC-WC has its own IP address.and is a bi-directional box. The box has no transmitter or receiver.

Since 1830 LX OSC-WC is used in conjunction with 1830 LX, the 1830 LX OSC-WC added to an OTS is listed in 360 tab, only if the OTS is also associated with 1830 LX.

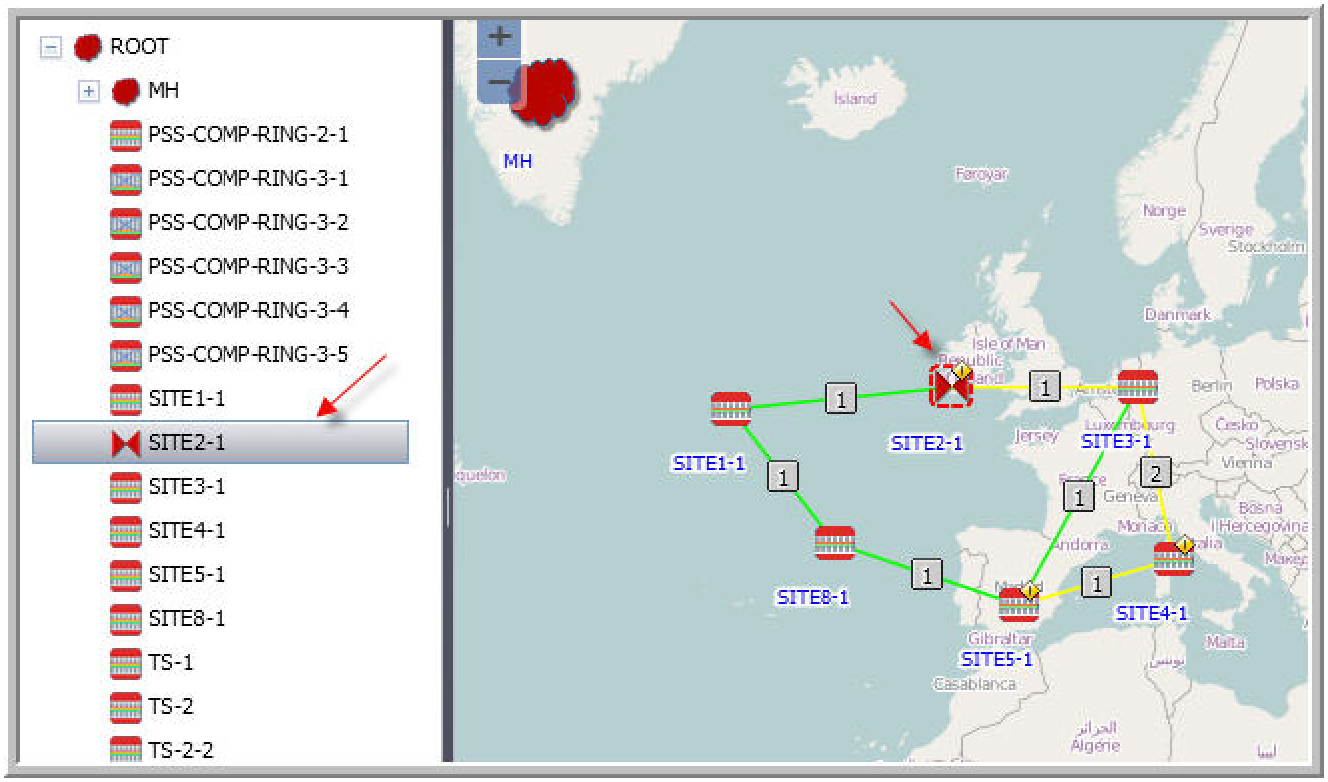
Nokia 1830 SLTE nodes

In submarine applications, the 1830 SLTE, which is an external, stand-alone NE, is used to maintain constant output power for subsea repeaters, regardless of the incoming channel number on the submarine cable.

The 1830 SLTE, which can be connected to 1830 PSS-32 and 1830 PSS-16 II NEs, is placed between the 1830 PSS line (after the amplifiers) and the submarine section. The 1830 PSS SLTE can connect multiple 1830 PSS nodes to the same submarine section. Unlike other NEs, the NFM-T does not auto discover the 1830 SLTE; however, it is treated as a managed node with limited capabilities.

Users can add 1830 SLTEs using the procedure *Add a Node/N*E, explained in the *NFM-T NE Management Guide*. They can manually associate the 1830 STLE NE to an amplifier port and to a transmit/receive direction through OTS physical connection ports using the in the 7.35 "Manage repeaters for an OTN OTS physical connection" (p. 850) procedure. Users can readily identify 1830 SLTEs on the Physical Connections data table by customizing the data table to list the **SLTE** column. From the Physical Connections data table, users can then navigate to the 1830 SLTE Craft Interface Terminal (CIT). A unique double triangle icon on the Network Map and the Routing Display makes the OTS physical connections to 1830 SLTEs readily visible.

Figure 2-37 Nokia NE Configurations – 1830 SLTE NEs – Identified on the Network Map



Because the 1830 SLTE does not have an SNMP interface, features such as Stop/Start supervision along with FM and PM, are not supported; however, since the 1830 SLTE can be pinged, the NFM-T raises an NE isolation alarm if the 1830 SLTE is unreachable.

Nokia 1830 VWM nodes

The NFM-T supports a semi-passive solution of the front-haul architecture based on Cloud-RAN (CRAN) and a Common Protocol Radio Interface (CPRI) using the 1830 VWM NE.

The 1830 VWM provides a management interface through an Optical Service Unit (OSU). The NFM-T supports 1830 VWM as a new NE with central and remote objects.

Nokia 1830 WaveLite nodes

The WaveLite optical transport product family provides enterprise, purpose-built DCI solutions that are highly economical, scalable, as well as easy to deploy and operate.

WaveLite is a family of service aggregation and transport components. There are multiplexing transponders (muxponders) for aggregating a wide range of client services onto higher rate optical lines using commonly available pluggable optical modules. The WaveLite NE also includes optical amplifier and wavelength multiplexer or demultiplexer modules. Together, these modules meet the needs of enterprise networks and service provider networks built to specifically support enterprises. All WaveLite products are compact, have a 1RU-high chassis with low power consumption, and AC or DC power.

Nokia 1830 PSI-2T nodes

The NFM-T supports 1830 PSI-2T management. The 1830 Photonic Service Interconnect-2T (1830 PSI-2T) is a combination of a virtual equipment controller card (PSIEC2), a virtual muxponder card (LCI2000), a power filter card (PF), and a fan (FAN).

Nokia 1830 PSI-M nodes

The NFM-T supports 1830 PSI-M management. The 1830 Photonic Service Interconnect-Modular (1830 PSI-M) NE is a combination of a virtual equipment controller card (MEC2), up to four transponder/muxponder cards (DA2C4), a power filter card (PF), and a fan (FAN).

Nokia 1830 PSD nodes

The NFM-T supports auto-discovery and management of the 1830 PSD (Photonic Service Demarcation) node/NE. The 1830 PSD can carry OTN or Ethernet traffic.

The 1830 PSD is a low-latency, compact, and versatile Network Interface Device (NID) designed for customer premises. It extends the reach of the optical network in support of 10G Ethernet or wave services and provides interfaces in support of Ethernet and wave services as well as OAM related ports. The client and line ports of the 1830 PSD feature pluggable optics.

Nokia 1626 LM nodes

The NFM-T supports auto-discovery and management of the 1626 LM (Light Manager) node/NE.

The 1626 LM is the platform of DWDM Multi-reach systems for Regional, National, and Pan-continental Networks. The 1626 LM addresses terrestrial applications from Metro-Core to Ultra Long-Haul and unrepeatered submarine applications, from average capacity for regional networks up to large capacity for pan-continental networks.

The 1626 LM is designed to efficiently address greenfield applications for new networks and links as well as to upgrade legacy platforms without traffic interruption. Carriers can keep their installed DWDM base and increase its capacity by loading new wavelengths from the 1626 LM.

Nokia 7210 SAS family of nodes

The NFM-T supports auto-discovery and management of 7210 SAS (Service Access Switch) node/NE.

The 7210 SAS is a family of next generation, small footprint, Carrier Ethernet customer edge devices. The 7210 SAS optimizes the business case for providing innovative Ethernet services to multiple locations, enables the cost effective addition of new sites to a Carrier Ethernet VPN network, and delivers multiple services per port. With SR OS deployed end-to-end, the 7210 SAS extends Service Level Agreements (SLAs) of more enhanced multipoint services such as Ethernet LAN (ELAN) and point-to-point services such as Ethernet Line (ELINE) along with Ethernet access to Internet Enhanced Services (IES) and Internet Protocol Virtual Private Network (IP-VPN) services into the customer edge.

2.12 Ports

Port definition

A *port* is a connectable endpoint that can terminate a physical or logical network connection.

There are two types of ports:

1. A *physical port* is an actual hardware connection point, which is specific place for being physically connected to some other device. Transmission lines connect to physical ports.
2. A *logical port* is a connection point within a physical connection point, which is a number assignment that is made in a certain format to let network applications differentiate services. Logical ports are contained within physical ports. Logical ports can contain other logical ports.

Refer to "User Interaction with ports" (p. 215) for additional information.

User Interaction with ports

The management system enables users to create ports and delete ports, and to modify existing parameters for ports.

In addition, the management system enables users to view the contained OTU2, ODU2, DSR Connection Termination Points (CTPs) for the line port and the DSR CTP for the client port. The user can also modify the parameters for these ports. The circuit packs for which this type of manual provisioning applies are the following:

- 11DPGE12
- 11DPE12
- 11DPE12E
- PSS1GBE

Users can view Used Ports, which lists all NFM-T OTN connections that terminate or pass through a selected NE; that is, connections that have at least one port of their layout that belongs to the selected NE.

For detailed procedures regarding ports, refer to the Operate Equipment Manager and Operate Nodes sections.

2.13 Cross Connections

Cross connection definition

A *cross connection* is a connection within an NE that internally connects one logical port on an NE to one or more logical ports on the same NE.

When a cross connection is automatically created, the system assigns a label for all cross connections in the connection. This label indicates the multiple cross connections that belong to the same connection.

Cross connection shape definition

A *cross connection shape* is a grouping of one or more cross connections into a pattern that the NFM-T OTN supports.

The connection shapes for NFM-T OTN cross connections include bidirectional (bi) shapes of simple and add-drop, along with unidirectional (uni) shapes of simple, add-drop A, add-drop Z, and double simple. The bidirectional shapes of simple (bi) and Add/Drop (bi) are the same connection shape.

The following figures illustrate the valid connection shapes for NFM-T OTN cross connections:

Figure 2-38 NFM-T NFM-T OTN Provisioning – Simple (uni) Connection Shape

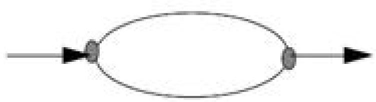


Figure 2-39 NFM-T NFM-T OTN Provisioning – Simple (bi) Connection Shape

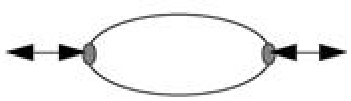


Figure 2-40 NFM-T NFM-T OTN Provisioning – Double-Simple (uni) Connection Shape

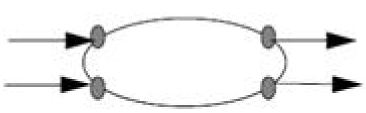


Figure 2-41 NFM-T NFM-T OTN Provisioning – Add-Drop A (uni) Connection Shape

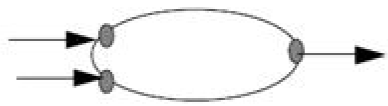


Figure 2-42 NFM-T NFM-T OTN Provisioning – Add-Drop Z (uni) Connection Shape

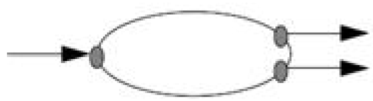
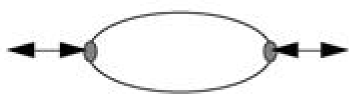


Figure 2-43 NFM-T NFM-T OTN Provisining – Add/Drop (Bi)



Correlated and uncorrelated cross connection definitions

A *correlated cross connection* is a cross connection that is associated with a connection that is provisioned in the NFM-T OTN. Correlated cross connections cannot be deleted using the NFM-T OTN.

An *uncorrelated cross connection* is a cross connection that is not associated with a connection that is provisioned in NFM-T OTN. Uncorrelated cross connections exist on the NE and are created outside NFM-T OTN, for example, by using the ZIC. Uncorrelated cross connections can be deleted using the NFM-T OTN. An uncorrelated cross connection can occur in any of the following scenarios:

- The cross connection shape that the NE reports and that the NFM-T OTN reports do not agree.
- At least one end port of the cross connection that the NE reports and that the NFM-T OTN reports do not agree. (The order of the ports is not significant.)
- The cross connection in the NE is not in use by a connection order.

Note: When an uncorrelated cross connection becomes a part of a connection that is either **Implemented**/**Completed** or **Commissioned**, the management system automatically reclassifies the uncorrelated cross connection as a correlated cross connection.

User interaction with cross connections

The following guidelines apply to user interaction with cross connections:

- Users cannot create cross connections.

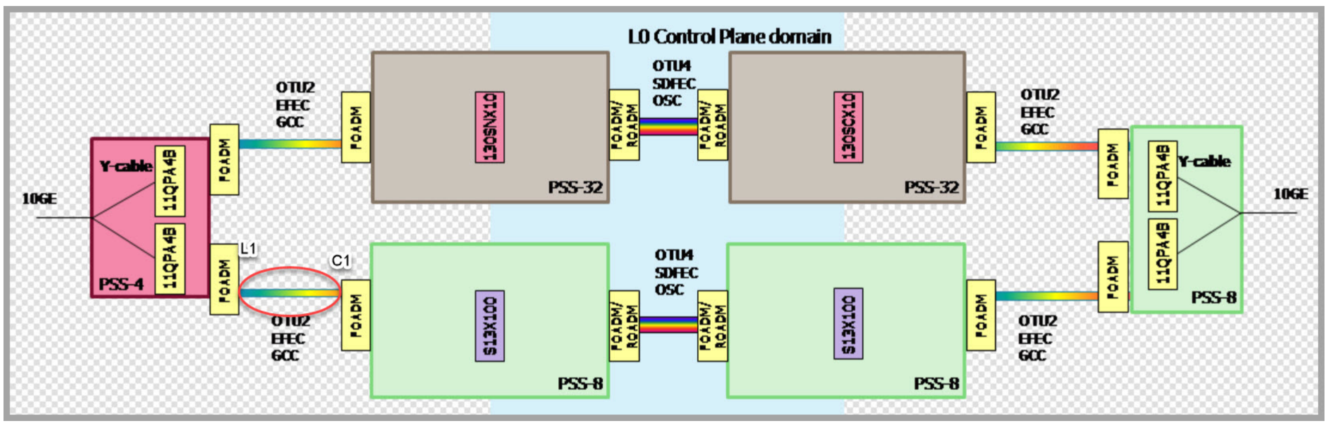
- Users can delete uncorrelated cross connections.

OCH cross connection creation support for S13X100, 20P200 and 11QPA4 cards

The following additional support has been added for S13X100R, S13X100E, 20P200 and 11QPA4 cards.

- For an 1830 PSS NE, OCH cross connection creation from the client port of S13X100R, S13X100E, 20P200 and 11QPA cards to the SFD/SFC packs is supported.
- The client port of these cards supports the creation of an OCH cross connection towards the SFD or SFC pack, which serves as a logical connection OPS between the line and the client ports of two cards.
- Supports the monitoring of fault management and performance management data between the line and client port over the logical connection.

Figure 2-44 Client OCH Cross Connection on S13X100E/R with 11QPA4



In the Figure 2-44, “Client OCH Cross Connection on S13X100E/R with 11QPA4” (p. 218), there is a logical connection created between the line port of 11QPA4 card and the client port of S13X100 card.

This is possible due to the support of OCH cross connection creation between the client port to SFD or SFC pack.

Note:

1. For the 11QPA4 card, creation of OCH cross connection is possible only towards the SFC pack and for S13X100R, S13X100E and 20P200 cards, OCH cross connection creation towards both SFD and SFC packs is supported.
2. The port role for the client port must be changed to **Line** (portRole=Line) for S13X100R, S13X100E and 20P200 cards.

Physical, Logical, and Link Connections

2.14 Connection definition, creation, and categorization

Connection definition

Connection is a generic term that is used to define any electrical or optical connectivity between NEs.

Methods of connection creation in the system

Connections can be created in, or added to, the management system in the following ways, depending on the nature of the connection:

- Without any user intervention, the management system can automatically add connections to the system during certain system events; these connections are said to be *automatically added* or *discovered*.
- Users can provision certain connections in the management system on the GUI; these connections are *manually provisioned*; and the parameters that describe these connections are *user-defined*.

Connection categories

Connections in the NFM-T OTN environment can be categorized as the following:

- *Physical connections* are connections that use wires, cables, or optical fibers to connect two physical ports in a network. Physical connections are automatically discovered or user-defined connections that users manually provision. Refer to 2.15 "Physical connections" (p. 220) for details.
- *Logical connections* are client connections that ride on any other server, including physical connections. A logical connection is typically created between DWDM NEs. It spans more than one DWDM NE that is carrying one or more (that is, Mux OTs) client signals that are converted into a single wavelength (or frequency) or multiple wavelengths, with each carrying one or more client signals. These logical connections, which are also referred to as *optical logical layers*, are established logically by the receipt and the acknowledgment of commands to the optical devices to connect the ports internally.

  Logical connections, which can be automatically discovered connections or user-defined connections, are either infrastructure connections or services. Refer to 2.17 "Infrastructure connections and services" (p. 224) for details.
- *Link connections* are connections that transport a client signal between the end ports of its serving connection. Link connections are connections that the system automatically adds or deletes during certain system events. Refer to 2.22 "Link connections" (p. 244) for details.

2.15 Physical connections

Physical connection definition

A *physical connection* is a connection that uses wires, cables, or optical fibers to connect two physical ports in a network.

Physical connection types

Physical connections are one of the following types:

- *External physical connections* are connections that are made between NEs.
- *Internal link connections* are connections that are made within an NE. These connections are also be created from the Equipment Manager application window.

External physical connections

The NFM-T automatically discovers two types of external physical connections during its subnetwork discovery process. Users can manually create by selecting the **+** sign on the icon bar at the top of the physical connection list window.

The following types of physical connections are automatically discovered:

- An *External Optical Section (OS)* is a physical connection that involves two different NEs. It is a physical connection between the a TDM NE OC-n port and an NFM-T OTN port.
- An *External Optical Transmission Section (OTS)* is a physical fiber bidirectional connection between two high speed lines of DWDM NEs, which consists of two unidirectional fibers making up a bidirectional connection.

Internal link connections

An *internal link* is a physical fiber connection that is provisioned within the NE and is established as a bidirectional connection either automatically by the NE when it detects a valid signal, or explicitly through a TL1 command.

These internal links either can be discovered or they can be user-defined; meaning, if they are not automatically discovered, users can explicitly provision them or create them during OTU infrastructure/service connection provisioning by checking the **Auto Server Creation** check box in the template.

When creating an internal link, the following signal type parameters apply:

Table 2-1 Signal Type Parameters

Signal Type Group	Signal Types
Optical (the default)	**OTU1**, **OTU2** (the default), **OTU2e**, **OTU3**, **OTU4**

Table 2-1 Signal Type Parameters (continued)

Signal Type Group	Signal Types
Ethernet	**100 GbE**, **40 GbE**, **10 GbE** (the default), **1 GbE**, or **Fast Ethernet**
SDH	**STM-256**, **STM-64** (the default), **STM-64MS**, **STM-16**, **STM-16MS**, **STM-4**, or **STM-1**
SONET	**OC-768**, **OC-192** (the default), **OC-48**, **OC-12**, or **OC-3**
CBR	**CBR 2G5** or **CBR 10G3**
Data	**FC 100** (the default), **FC 200**, **FC 400**, **FC 800**, **FC 1200**, **HDSDI**, **SDSDI**, **DVBASI**, **DDR**, or **3GSDI**

During the creation of an internal link, the NFM-T OTN application uses the signal type value as follows:

- The signal type value is used as the initial value for the signal type in the **Transmission Parameters** panel.
- The signal type value is used to filter the list of ports that are displayed in the **From/To...** fields in the **Service Definition** panel. Only ports with the particular signal type or ports that are unassigned and can be assigned with the particular signal type are displayed for selection in the **From/To...** fields in the **Service Definition** panel.
- For OTU2 and OTU2e signal types, OS PTPs on SFC8 cards on the 1830 PSS OCS NEs are displayed.

User interaction with Physical connections

From the physical connection level, the management system enables users to create a physical connection, modify a physical connection, delete a physical connection, and view all physical connections, insert a node and correlate a physical connection to ASAP or SRG. The user can also manage OTDR scan, manage Optical Power. In addition the user can also manage PM on the physical connection.

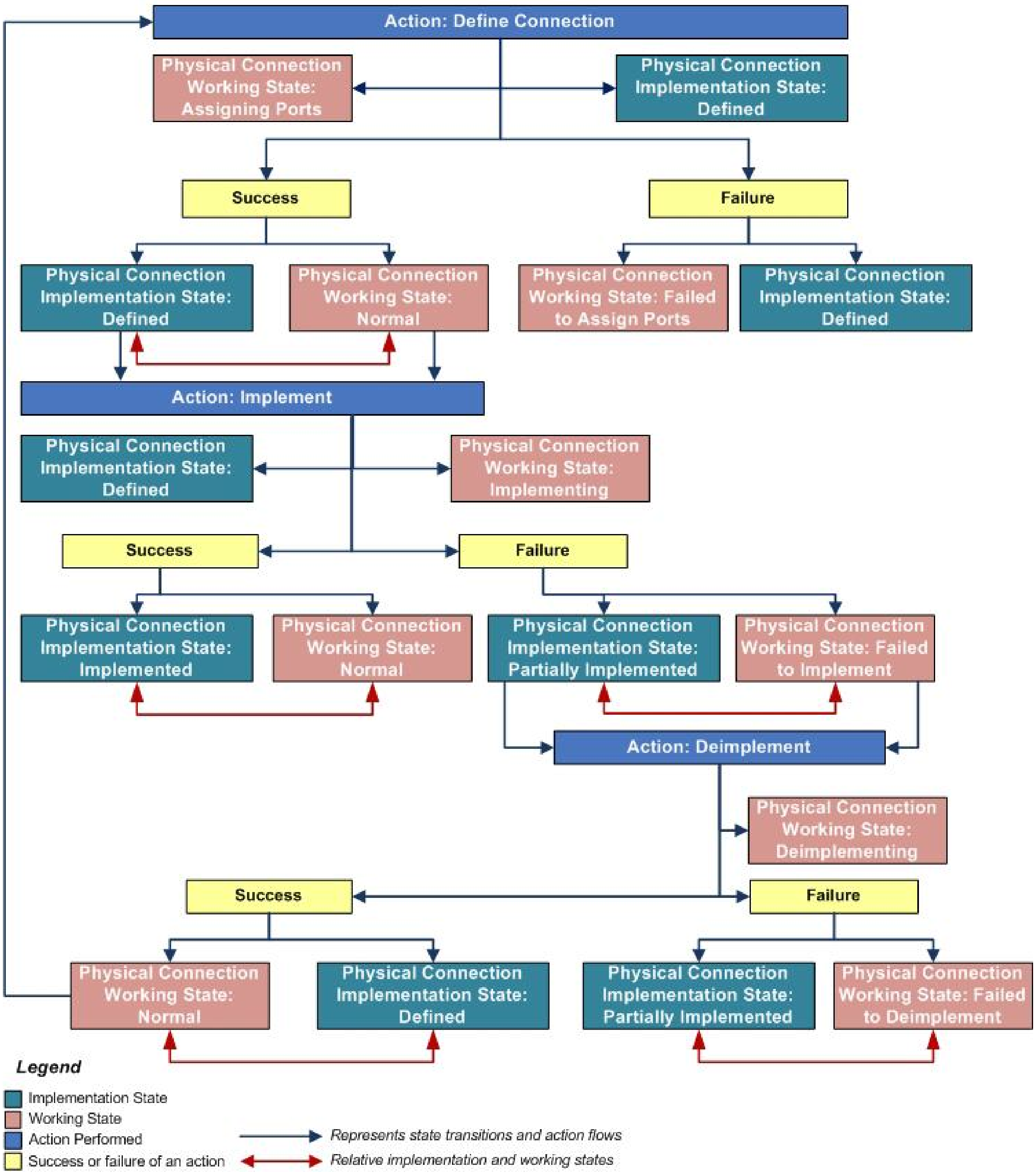
For detailed procedures regarding physical connections, refer to the "Physical Connections " (p. 784)section.

2.16 Physical connection state transition diagram

Overview

The following diagram provides information about the state transitions that applies to a physical connection during its creation and implementation.

Figure 2-45 Flow Chat for State Transitions



2.17 Infrastructure connections and services

Infrastructure connections

An *infrastructure* is a connection that acts as a hierarchical server layer to carry customer services. Infrastructure connections, which can be unterminated or terminated connections, are categorized on the NFM-T GUI as *trails* and *logical links*.

Provisioning Note: During template-based infrastructure provisioning, users must specify whether the infrastructure connection is a trail or a logical link. For guidance and more information, refer to 2.8 “Determine the Infrastructure to be created” (p. 168).

Infrastructure connections — trails

An *infrastructure trail* is a terminated entity that can multiplex or demultiplex client signals. An infrastructure trail connects the interior, logical network ports that are adapted connections with one or more types of link connections.

An infrastructure trail can consist of a hierarchy of trails according to the OTN layered model per ITU-T G.709 standard. It is used as a server connection for other connections (either service paths or other infrastructure trails).

Infrastructure connections — Logical links

A *logical link* is an unterminated entity that provides contiguous, fixed connectivity to the far end, which can be terminated or unterminated.

Services

Services are also known as *paths*. A *service* is a connection between the boundary ports of a service provider network that provides service to an end-user/customer of the network. A service is an end-to-end connection that carries the customer's service as a container in Low Order (LO) or High Order (HO) trail. A service connects the logical ports that are entirely used to carry a unique service.

The following parameters apply to the creation of a service:

Table 2-2 Parameters for a Service Creation

Service Rate Type	Service Rate
Ethernet	**100 GbE**, **40 GbE**, **10 GbE** (the default), **1 GbE**, or **Fast Ethernet**
Optical	**ODU1, ODU2** (the default), **ODU2E, ODU3, ODU4, OCH,** or **OMS**.
SDH	**STM-256**, **STM-64** (the default), **STM-64MS**, **STM-16**, **STM-16MS**, **STM-4**, or **STM-1**
SONET	**OC-768**, **OC-192** (the default), **OC-48**, **OC-12**, or **OC-3**
CBR	**CBR 2G5** or **CBR 10G3**

Table 2-2 Parameters for a Service Creation (continued)

Service Rate Type	Service Rate
Data	**FC 100** (the default), **FC 200**, **FC 400**, **FC 800**, **FC 1200**, **HDSDI**, **SDSDI**, **DVBASI**, **DDR**, or **3GSDI**

During the creation of a service, the NFM-T OTN application uses the service rate value as follows:

- For DSR connection rates, the service rate value is the initial value of the signal type in the **Transmission Parameters** panel. **Note:** Digital Service Rate (DSR) is a term that is used generically to represent the service rate of a connection that is being provisioned. When provisioning the service path, users must select the actual **Service Rate** of the connection in order for the connection to be implemented.
- The particular service rate value is used to filter the list of ports that are displayed in the **From/ To...** fields in the **Service Definition** panel. Only ports that have a signal type that is equal to the service rate or ports that are unassigned and can be assigned with the signal type that is equal to the service rate are displayed for selection in the **From/To...** fields in the **Service Definition** panel.

For a service, the NFM-T OTN application automatically assigns a service type based on the a connection rate and a service rate.

Table 2-3 Connection Rate, Service Rate, and Service Type

Connection Rate	Service Rate	Service Type
ODUk, OCH, OC-nRS, STM-nRS	Not applicable	**Undetermined**
DSR	**100 GbE**, **40 GbE**, **10 GbE** (the default), **1 GbE**, or **Fast Ethernet**	**Ethernet**
DSR	Any value except **100 GbE**, **40 GbE**, **10 GbE** (the default), **1 GbE**, or **Fast Ethernet**	**Undetermined**

The Category of a connection

When users create or modify a connection, the system automatically determines and names the **Category** of the connection based on the route of the connection, which is determined by the user selection in the **ASON Routed** field in the Service Definition of the connection. The **Category** of a connection is not user-selectable; meaning, it does not appear on any template; the **Category** field appears on the data table for an infrastructure connection or service.

The system-assigned **Category** of a connection can be one of the following:

- A **Managed Plane** connection is a connection in which the user has not checked the **ASON Routed** field and the connection is not a logical drop link connection. Managed Plane connections can be infrastructure connections or services.

- A **Control Plane** connection is an infrastructure connection in which the user has checked the **ASON Routed** field, has unchecked the **MRN Tunnel** box, and the entire route of the connection is in the Control Plane.

  Note: A *Drop Link*, which is an external OS connection that is assigned to a Network Protection Architecture (NPA) in ASON, is the link between the Managed Plane and the Control Plane.
- A **Mixed Plane** connection is a connection in which the user has checked the **ASON Routed** field and the route of the connection is in both the Managed Plane and the Control Plane. Mixed Plane connections can be infrastructure connections or services.
- An **ASON Logical Edge Drop Link** is an ODUk connection with at least one connection endpoint on an ODUPOOL where the ODUPOOL is in the Control Plane and the route of the connection contains at least one link connection that belongs to an external OS connection that is a Drop Link. For these connections, the HO-ODUk cross connection in the NE in the Control Plane must be created via the ASON manager. Therefore, if the HO-ODUk cross connection in the NE in the Control Plane does not already exist when the Logical Drop Link connection is created, the HO- ODUk cross connection must be created as part of the order for the Logical Drop Link. Logical Drop Links can only be deleted if all Control Plane clients are deleted. (Note: when all Control Plane clients are deleted, the HO-ODUk cross connection in the NE in the Control Plane is deleted via ASON manager.)
- An **ASON Logical Link** is a managed plane infrastructure connection or a managed plane logical link connection that is created in OTN and is assigned to an NPA in ASON. These connections, which are reserved by the ASON manager, are locked in OTN and cannot be modified, deleted, or rearranged. ASON Logical Links and link connections of ASON Logical Links are not available for use by routing when **ASON Routed** is not selected for the connection. When users select **ASON Routed** for the connection and the connection will be a Control Plane or Mixed Plane connection, ASON Logical Links and link connections of ASON Logical Links are not available to be used in any portion of the connection in the Managed Plane and can only be used in the portion of the connection in the Control Plane.
- An **ASON Implicit Server** is the server of another ASON connection. An ASON Implicit Server is automatically created by GMRE and OTN; and, as such, it cannot be modified, deleted, or rearranged in OTN. ASON Implicit Servers and link connections of ASON Implicit Servers are not available for use by routing when ASON routing is not selected for the connection. When users select **ASON Routed** for the connection and the connection will be a Control Plane or Mixed Plane connection, ASON Implicit Servers and the link connections of ASON Implicit Servers are not available to be used in any portion of the connection in the Managed Plane and can only be used in the portion of the connection in the Control Plane. ASON Implicit Servers only appear on the infrastructure connection data table for Layer 0 GMRE.
- An **ASON MRN Unterminated Tunnel** is a connection in which the user has checked the **ASON Routed** field and the tunnel type is **Unterminated**.
- An **ASON MRN Terminated Tunnel** is a connection in which the user has checked the **ASON Routed** field and the tunnel type is **Terminated**.

How infrastructures and services differ

Services and infrastructures have many of the same characteristics. However, when users view infrastructure connections or services in their respective data tables, some differing characteristics become apparent. The following table summarizes these different characteristics.

Table 2-4 Infrastructure Connections and Services — Different Characteristics

Characteristic	Infrastructures	Services
Category	ASON Implicit Server ASON Logical Edge Drop Link ASON Logical Link ASON MRN Unterminated Tunnel ASON MRN Terminated Tunnel Control Plane Managed Plane Mixed Plane	Managed Plane Mixed Plane
Clients*	—	✓
Created by	N/A SDH/GMRE System System Notify User	—
Deploy Type	Add Delete Discover	Add Discover
Implementation State	Commissioned Defined Implemented	Commissioned Defined Implemented Partially Allocated
Protection	OMSP Protected Unprotected	Protected Segment Protected Unprotected
Provisionable Wave Key	Keyed N/A Unkeyed	Keyed N/A
Servers*	✓	✓

* A client is an object that uses a service of another object; whereas a server is an object that provides a service to another object. Services do not have client connections. Infrastructure trails can create client link connections; meaning, they can carry clients. Refer to 2.23 “Client or server relationships” (p. 247) for details.

Infrastructure connections and services user interaction

Users can view and operate in different modes on Infrastructure Connections and Services. Refer to “ Infrastructure Connections and Services” (p. 913) for detailed explanations and steps.

Before creating a connection

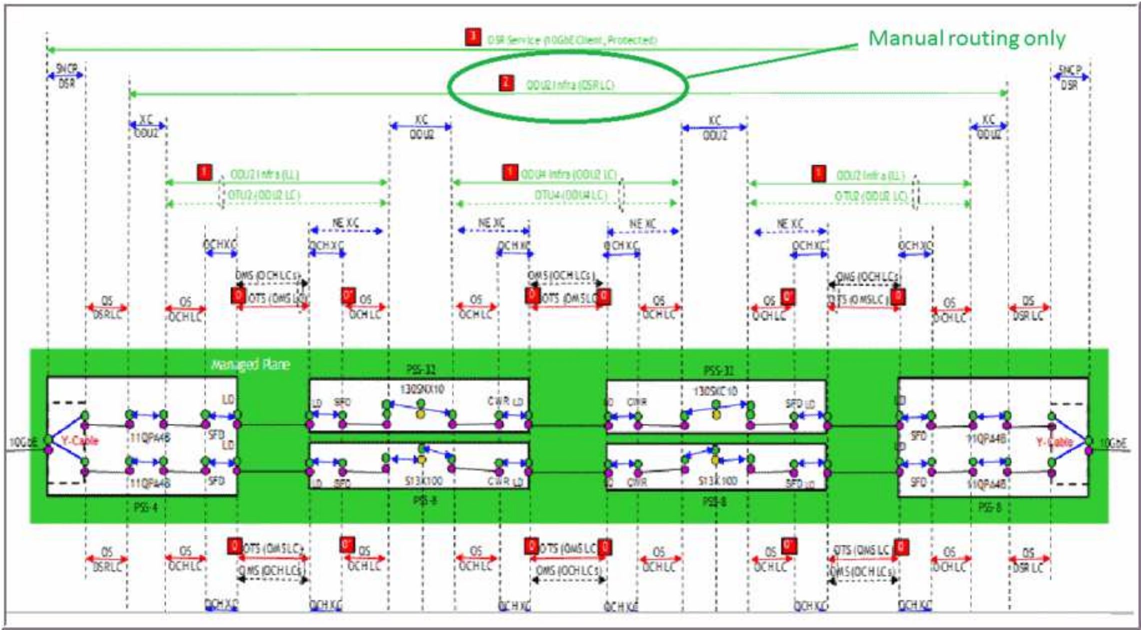
Be aware of the following guidelines when creating connections:

- When you create one particular type of connection, the 2.30 “Single Step Provisioning” (p. 275) feature will automatically create the appropriate server connection. For more details refer to 2.30 “Single Step Provisioning” (p. 275).
- When you provision a DSR service, the *Auto Payload* feature enables an HO-ODUk infrastructure trail, along with a LO-ODUk infrastructure trail, to be provisioned in a single step. The Auto Payload feature relies on the system's automatic creation of virtual servers, which are ODU2POOL ports on the 1830 PSS OCS NEs that are used for internal routing. Refer to 2.32 “Auto Payload” (p. 295) for a more detailed explanation and configuration information on Auto Payload.
- If you directly create an LO-ODUk infrastructure connection, the DSR and the LO-ODUk connections will not be linked and they will remain independent connections. In addition, if you directly create an OTUk infrastructure connection, the ODUk and OTUk connections will not be linked and they will remain independent connections.
- When you create an HO ODU4 connection that terminates on an 112SDX11 circuit pack, the system automatically creates the server OTU4 and four server OTL4.4 connections. So when you select the route of the HO ODU4 connection, choose link connections or trails to constrain the OTL4.4 connections. You will only have to select the route for the first server OTL4.4 connection, which is the server connection that terminates on the L1 port. The system will automatically determine the route for the three remaining OTL4.4 connections, which are the server connections that terminate on the L2, L3, and L4 ports. You can only select the frequency of the L1 port. Once you select the frequency for the L1 port, the system automatically selects the frequencies of the L2, L3 and L4 ports with 100G spacing and continuous channels. Therefore, once you specify the route of the first OTL4.4, the route of the three remaining OTL4.4 connections, which are L2, L3, and L4, is fixed.
- When creating a connection and NFM-T needs to send command to Network Element, the NE reachability is checked. But it can happen that along the provisioning intermediate nodes are present also as constraint, in this case the connection can go through also if the node is not reachable from NFM-T side.

  Let us consider the different cases:
  - For Managed Plane, NFM-T checks the NE reachability for each NE before deploying commands along the route, this include 3R node too.
  - For Control Plane, NFM-T checks the NE reachability only at A Node and Z node, not on intermediate nodes because the commands are deployed only to A Nodes and Z Nodes.
  - For Mixed Plane, on Managed Plane entity, if commands are sent, the NE reachability is checked. For the ASON boundary, the NE reachability is checked for A Nodes and Z nodes.
- For SNCP protected connections involving auto routing, the behavior is on best effort basis. The protection type is not enforced. The behavior can be described as: Select the Link Connections from unprotected servers between the same two nodes. Internal Link Connections can be

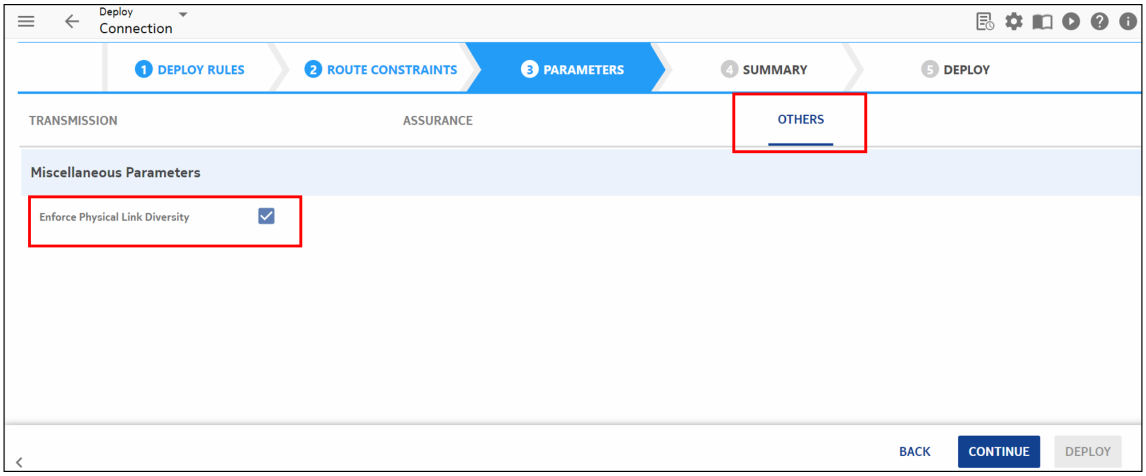
unprotected. If the appropriate Link Connections cannot be found, select Link Connections from unprotected servers and update the protection type to *segment protected* or *unprotected* as appropriate. See 2.22 “Link connections” (p. 244) for further information.

- If a connection uses auto routing, this implies that all the resources are available to use for auto routing. In case there is a cross connection set up in the path provisioning route, the link connections associated with this connection are unavailable for auto routing. This connection must be setup manually as indicated in the figure.



- For an auto routed network of L1 Managed Plane connections, a single OTS link can be reused between two subsequent unique infrastructure trails.

From **PARAMETERS > OTHERS** tab, disable the **Enforce Physical Link Diversity** parameter. By default, this field is enabled.



Enforce Physical Link Diversity parameter is used for both protected and unprotected services.

Following are important considerations for the OTS link reuse -

- Disable the **Enforce Physical Link Diversity** parameter to allow reuse of OTS link(s).
- If the **Enforce Physical Link Diversity** parameter is disabled, the routing engine finds the shortest path to create a connection. The physical link, node, and trail constraints must be provided if OTS link is reused.

  See Route Constraints 7.5 “Advanced Settings field descriptions for deploy Best Practices templates” (p. 708) for more details.
- For ODUk infrastructure connection, an error message is displayed if user tries to set the **Enforce Physical Link Diversity** parameter to false.
- To allow reuse of the OTS link is applicable only for auto routing of the service.
- For protected connections, **Enforce Physical Link Diversity** can be applied on different OTS links separately on the service and protection paths.

  During creation of protected connection, disable the **Enforce Physical Link Diversity** parameter to reuse the OTS link and to allow maximal physical diversity rather than strict diversity.
- Add protection carries forward the same physical diversity policy that was used during create operation.
- Remove protection operation retains the existing physical diversity of the working path.
- For Modify route, **Enforce Physical Link Diversity** is applicable only on ODUj infrastructure connection.

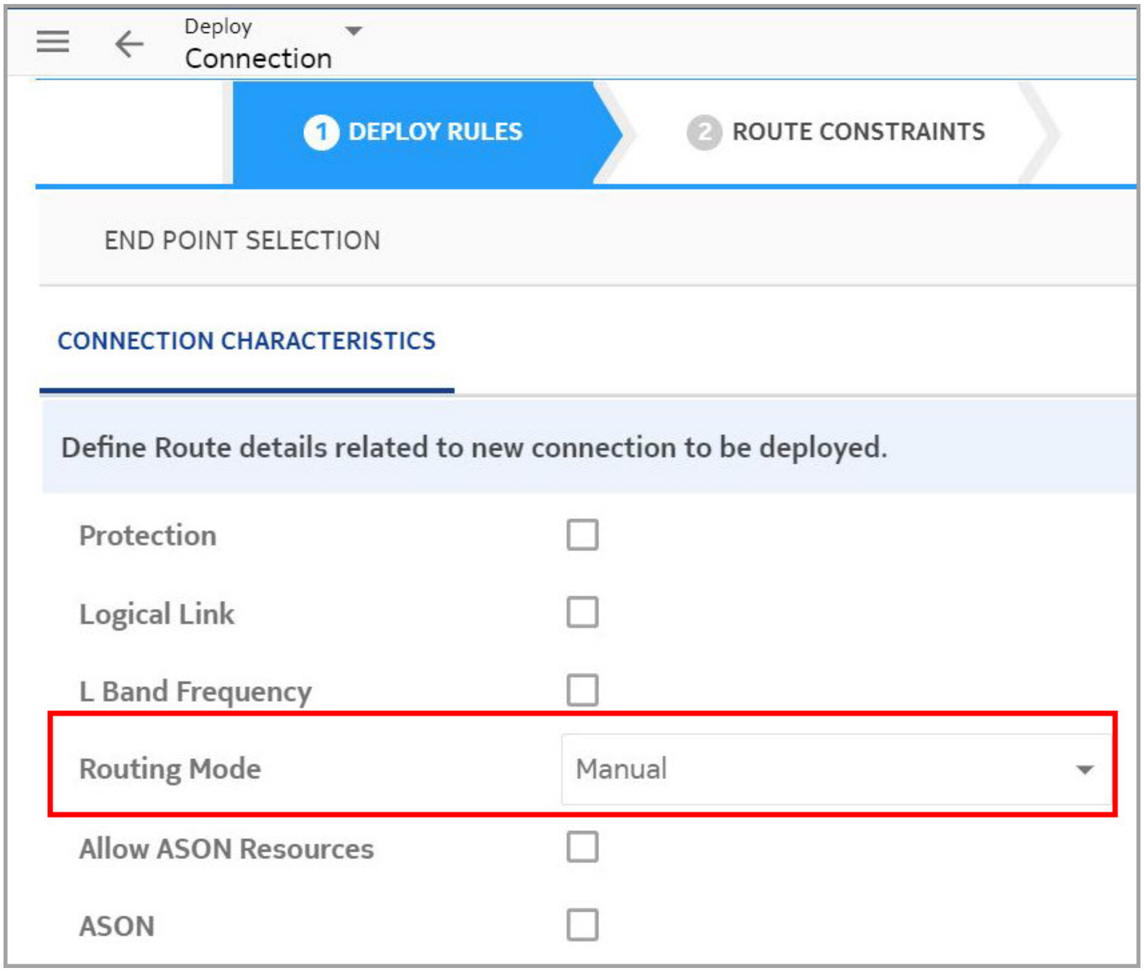
• When you create a protected connection, for example an OPSA protected connection, if you have OTU4/ODU4/DSR connections or OTU4x2/ODU4/DSR connections, the connections lists 7.72 “View Infrastructure Connections or Services” (p. 1019) displays the following:

Rate	Protection
OTU4 or OTU4X2	Protected
ODU4	Server Protected
DSR	Unprotected

Only the immediate client of a protected connection shows **Server Protected** and not all of the subsequent clients. The exception is an HO ODUk SNCP protection. When an HO ODUk connection has SNCP protection, both the LO ODUk and DSR client connections show **Server Protected**.

- When you create a connection or service that involves D5X500Q card that interwork with another D5X500Q card or with 2UC400/4UC400 cards, ensure to configure the interworking mode appropriately. For more information, see *Equipment Management* section of the NFM-T NE Management Guide .
- Using the pluggable *T-XFP zero-chirp* the user has to provision only unkeyed channels. The pluggable is applicable to any configuration and scenario supported by 11DPM8/12P120 cards in managed-plane and in L0 GMPLS control plane. The Pluggable Module Type is XL-64TC.
- **Important!**: If there are fixed cross-connections or uncorrelated cross-connections in place on the NE, that are used in the connection path, ensure to select **Routing Mode** as **Manual** under the **CONNECTION CHARACTERISTICS** pane of **DEPLOY RULES** section and check the **Fully Specified** check box under **Infrastructure** tab of **ROUTE CONSTRAINTS** section. See 7.6 “Routing Constraints” (p. 731) for details.

Figure 2-46 Manual Routing Selection



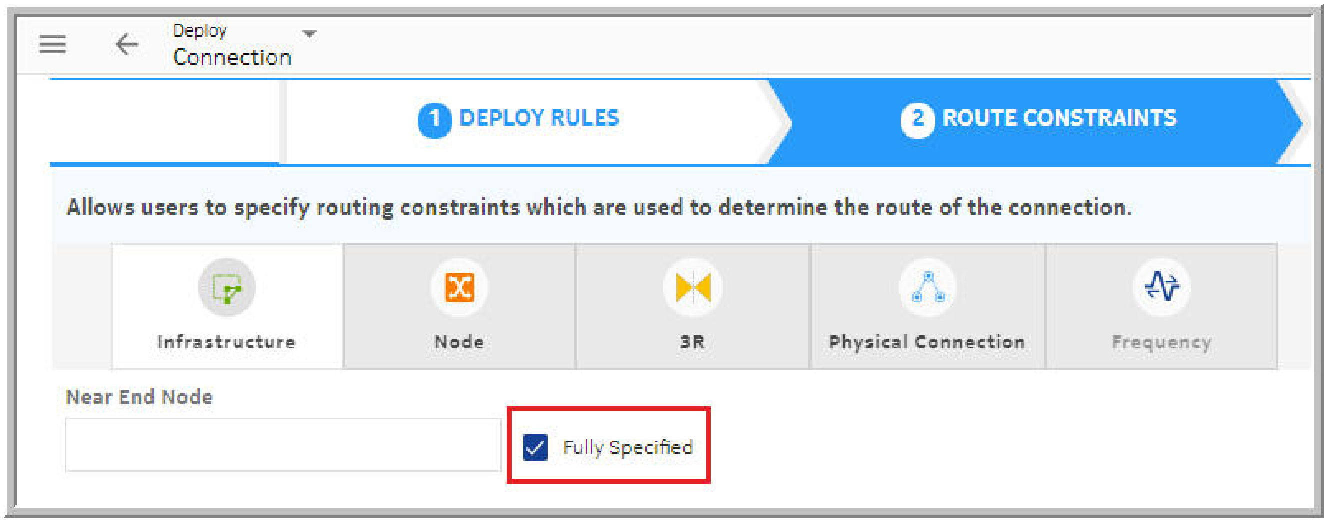


Figure 2-47 Fully Specified Selection

2.18 Infrastructure connections state transition diagram

Overview

The following diagram provides information about the state transitions that applies to an infrastructure connection during its creation.

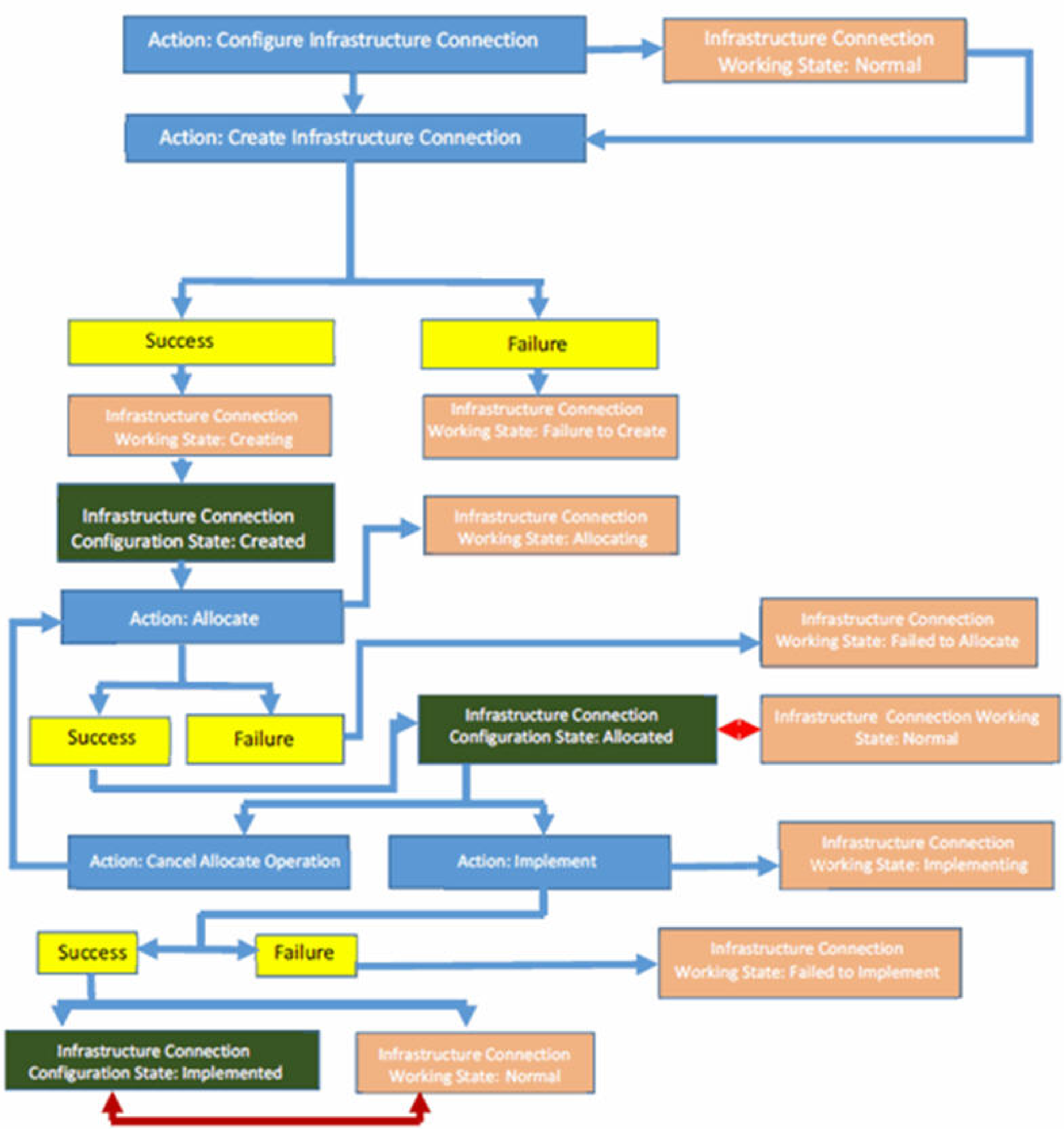
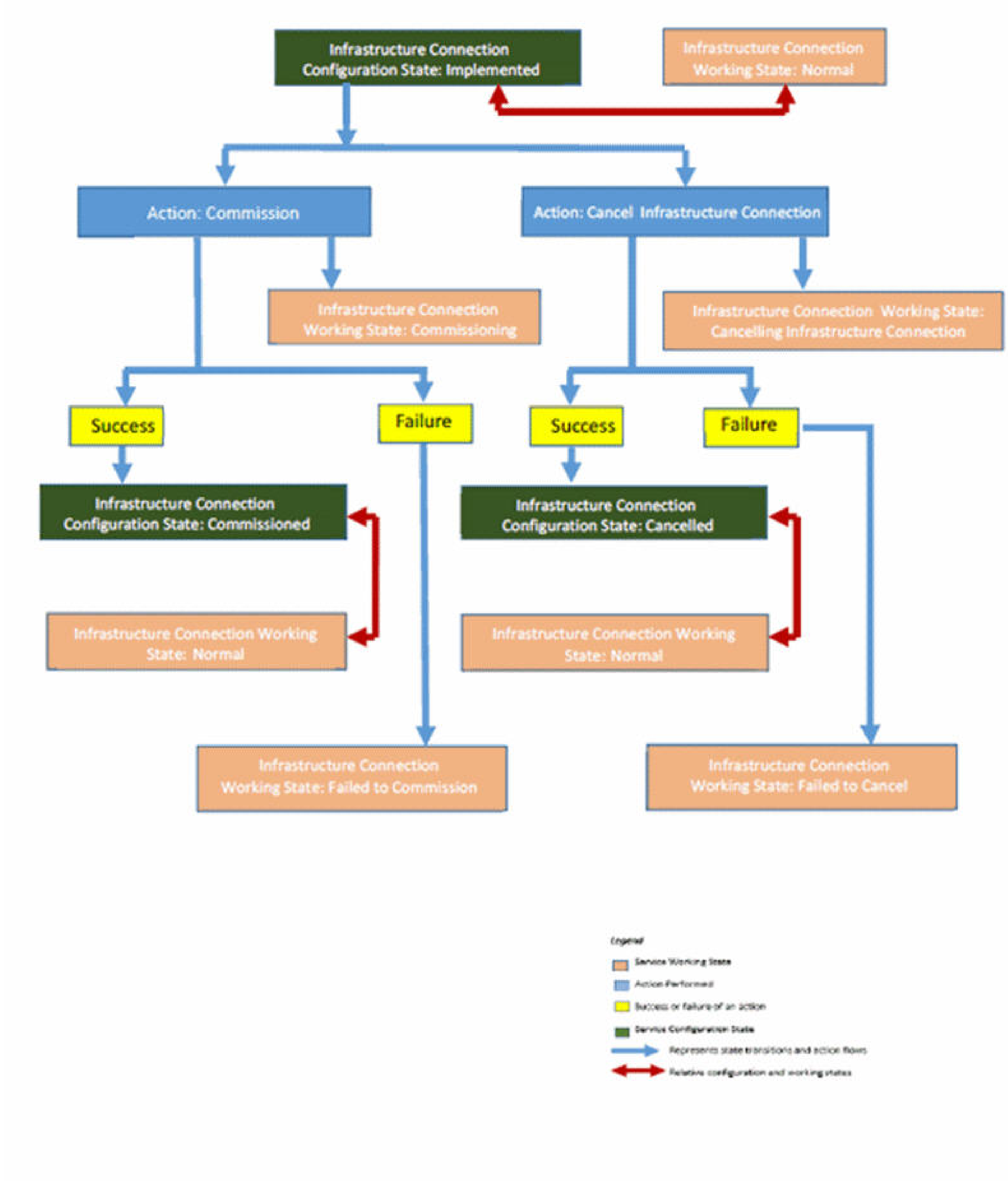


Figure 2-48 State Transitions of an Infrastructure Connection

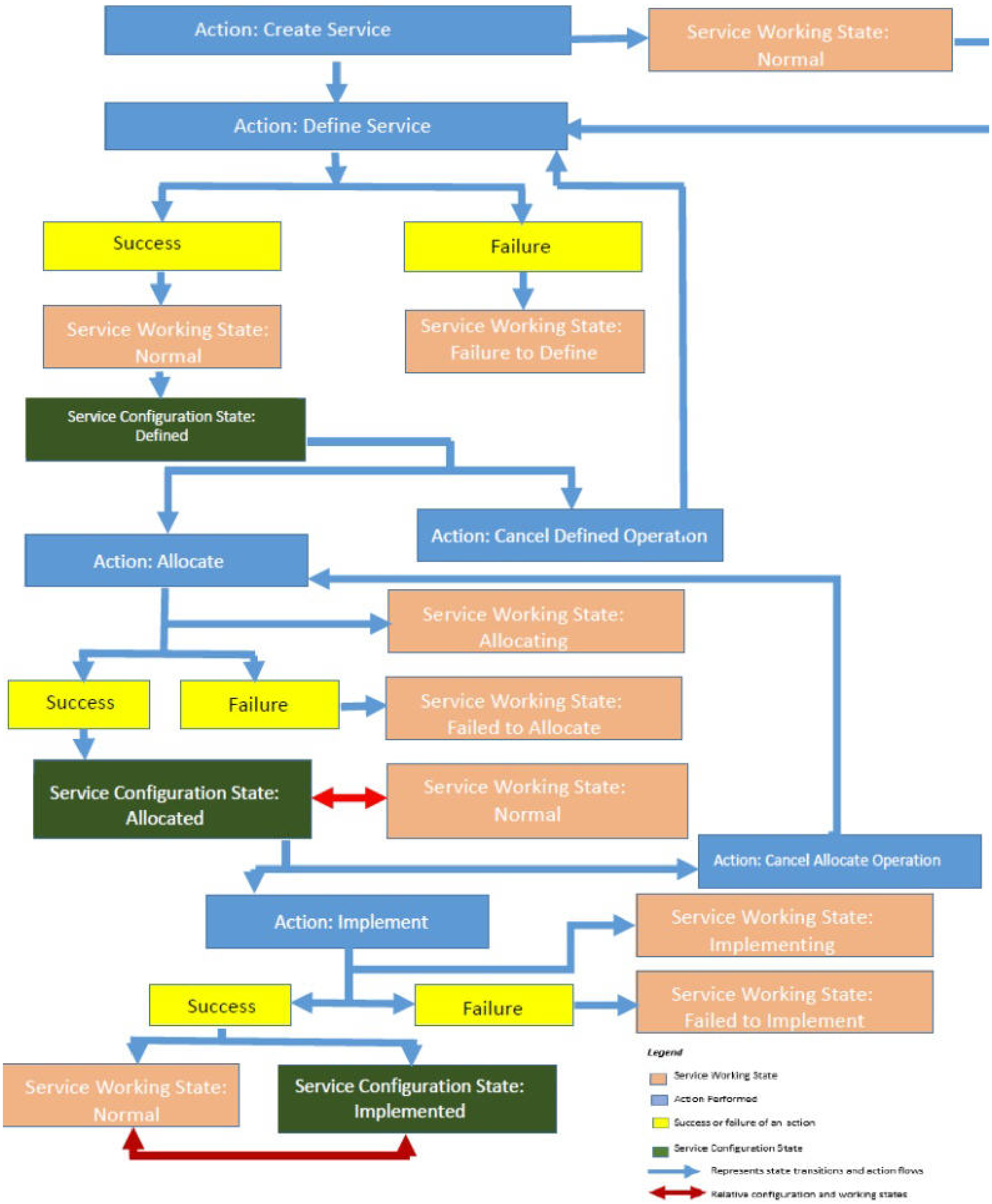

Infrastructure Connection Configuration State: Implemented
Infrastructure Connection Working State: Normal
Action: Commission
Action: Cancel Infrastructure Connection
Infrastructure Connection Working State: Commissioning
Infrastructure Connection Working State: Cancelling Infrastructure Connection
Success
Failure
Success
Failure
Infrastructure Connection Configuration State: Commissioned
Infrastructure Connection Configuration State: Cancelled
Infrastructure Connection Working State: Normal
Infrastructure Connection Working State: Normal
Infrastructure Connection Working State: Failed to Commission
Infrastructure Connection Working State: Failed to Cancel

2.19 Services state transition diagram

Overview

The following diagram provides information about the state transitions that applies to a service connection during its creation.

Figure 2-49 State Transitions of a Service Connection during its Creation



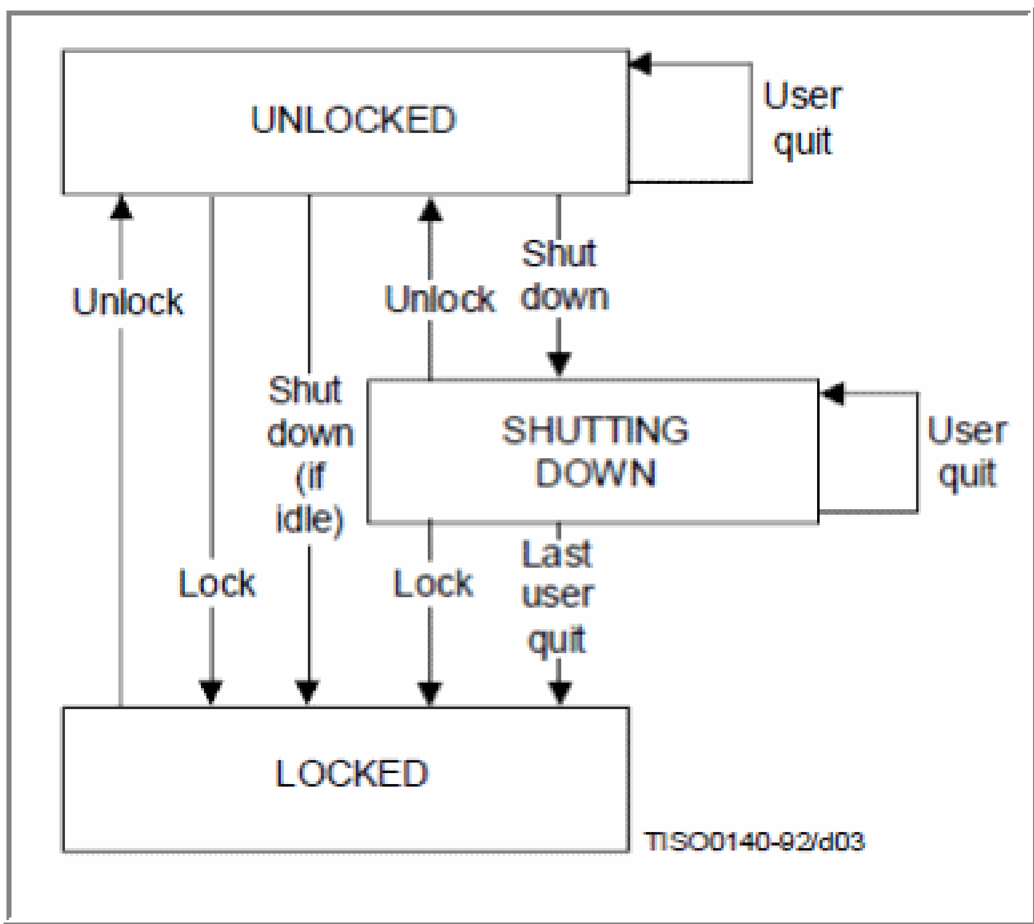
2.20 State definitions

Administrative State

The administration of managed objects operates independently of the operability and usage of the managed objects is described by the administrative state attribute, which has three values locked, unlocked and shutting down. These are represented in Figure 2-50, “Administrative State Diagram” (p. 240).

Specific events associated with the managed object cause specific transitions from one administrative state value to another, depending upon the original value of the administrative state, the specific event, and also upon the number of users of the resource.

Figure 2-50 Administrative State Diagram



Unlock

This event consists of an operation being performed at the managed object boundary to unlock the managed object’s corresponding resource. It can occur only if the managed object’s administrative state is locked or shutting down. It causes a transition to the unlocked administrative state.

Lock

This event consists of an operation being performed at the managed object boundary to lock the managed object’s corresponding resource. It can occur only if the managed object’s administrative state is unlocked or shutting down. It causes a transition to the locked administrative state.

Shut down

This event consists of an operation being performed at the managed object boundary to shut down the managed object’s corresponding resource. It can occur only if the managed object’s administrative state is unlocked. It causes a state transition as follows:

- if, at the time of the event, the resource has existing users, the administrative state becomes shutting down;
- if, at the time of the event, the resource has no users, the administrative state becomes locked

Administrative state attribute

The administrative state attribute is single valued and read-write. It can have one of the following values, not all of which are applicable to every class of managed object:

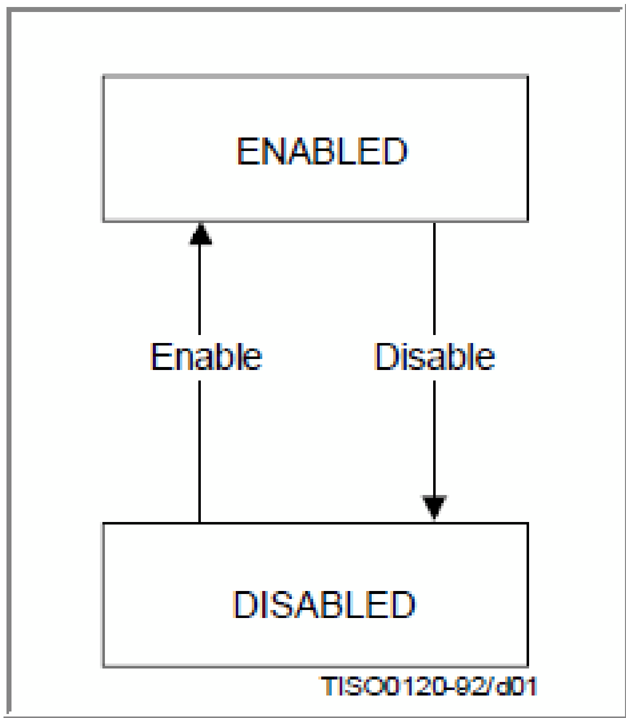
- **locked**: The resource is administratively prohibited from performing services for its users.
- **shutting down**: Use of the resource is administratively permitted to existing instances of use only. While the system remains in the shutting down state the manager may at any time cause the managed object to revert to the unlocked state.
- **unlocked**: The resource is administratively permitted to perform services for its users. This is independent of its inherent operability.

Operational state

The operability of a resource is described by the operational state attribute, which has two possible values: disabled and enabled.

When a managed object is unable to reflect the operational state of its associated resource and the unknown status attribute defined in “Unknown status attribute ” (p. 242) is supported, the unknown status attribute value will be true. It is the natural operation of the resource that causes operational state transitions to occur, and therefore, management cannot request a managed object to change from one operational state to another. Management can only gather information about the operational state of a managed object, that is, the operational state is read-only in nature. Specific events associated with the resource cause specific transitions from one operational state value to the other. These events and transitions are summarized in Figure 2-51, “Operational State Diagram” (p. 242), and are described below.

Figure 2-51 Operational State Diagram



Unknown status attribute

The unknown status attribute is used to indicate that the state of the resource represented by the managed object is unknown. When the unknown status attribute value is true, the value of the state attributes may not reflect the actual state of the resource.

Operational state attribute

The operational state attribute is single-valued and read-only. It can have one of the following values.

- **disabled**: The resource is totally inoperable and unable to provide service to the user(s).
- **enabled**: The resource is partially or fully operable and available for use.

2.21 Object Life Cycle (OLC) state

OLC state

Maintenance activities on an NE can evoke many alarms. The Object Life Cycle (OLC) state of an object indicates whether the object is in service or in maintenance. The user can filter out alarms based on the OLC state of an object. When an object is in **Maintenance** OLC state, the alarms that are raised on these objects are dynamically updated in the Fault Management application. The alarms are also listed in the **Alarms** tab from the 360 degree view hover icon of the corresponding object. These are applicable only for current alarms. By default, the OLC state of each object is **In Service**. The OLC state for an object is modifiable only on NFM-T, and is propagated from the NE level. If OLC state is changed at NE level, then the OLC state is propagated to the child objects such as all shelves, cards, and ports. In EQM, the OLC state is in alignment with the NE.

Important! OLC state feature is enabled for all user profiles except for the Viewer profile.

The objects that support OLC state include the following:

- NEs
- Shelves
- Cards/Packs
- Ports
- Physical connections
- Infrastructure connections
- Services

Useful links

See the following for more information on OLC State configuration for various objects:

- 7.27 “Configure OLC State for connections and services” (p. 823) to configure OLC state on connections and NEs from the NFM-T GUI.
- See the *NE Management Guide* to configure OLC state on an NE from the NFM-T EQM GUI, to configure OLC state on an NE from the NFM-T GUI, to configure OLC state on ports, cards, and shelves and to view all objects in **Maintenance** OLC state and to reset the state to **In Service** for multiple objects.

2.22 Link connections

Link connections

A *link connection*, which is sometimes abbreviated as an *LC*, is a connection that transports a client signal between the end ports of its serving connection. Link connections are also known as *channels*.

Two types of link connections

The NFM-T OTN network supports two types of link connections:

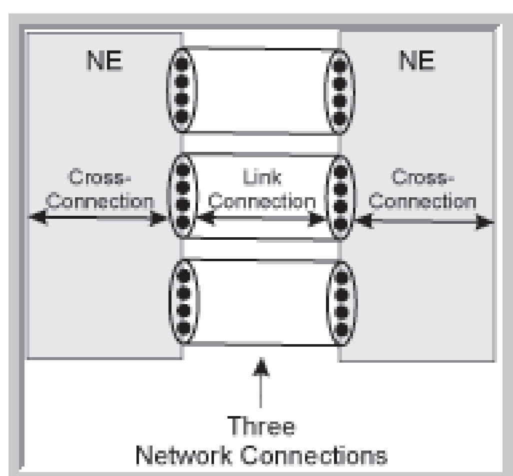
1. *External link connections* are link connections from servers between two NEs.
2. *Internal link connections* are link connections from servers (OS) that are internal to an NE (link connection of an internal OS).

Link connection example

When finding a route for a NFM-T OTN connection, the system finds a route through all external link connections and builds the complete layout with the internal link connections before it successfully completes finding the route.

The following figure illustrates a link connection.

Figure 2-52 NFM-T NFM-T OTN Provisioning – Link Connection Example



Link connections automatically and added and deleted

Link connections are automatically added to the management system when a service or a physical connection moves to the **Commissioned** state. When either event occurs, a link connection is automatically created and added to the database without any user intervention. Users cannot manually add any link connections.

Link connections are automatically deleted from the management system when their server connection is deleted. When this event occurs, the management system automatically deletes the link connection and deletes it from the database without any user intervention. Users cannot manually delete a link connection.

Creation of link connection terminations

When an Optical Transmission Section (OTS) link is discovered by the NFM-T and moves to the **Commissioned** state, the management system automatically creates an OMS link connection. The connection rate field value for OTS displays **OTS**. The value of the service type for OTS is **Not Applicable**.

When an internal Optical Transmission Section (OTS) connection is created and moves to the **Commissioned** state, the management system automatically creates an OMS link connection. The connection rate field value for OTS displays **OTS**. The value of the service type for OTS is **Not Applicable**.

The type and rate of OS link connections depends on the terminations of the OS. The connection rate field value for OS displays **OS**. The value of the service type for OS is **Not Applicable**.

Link Connections tab and data table

Link connections are a tabbed topic, which means that users can access the link connections data table by selecting the **Link Connections** tab from the physical connections, infrastructure connections, or looped back connections data tables.

Users can also access the link connections data table from the NFM-T GUI graphical displays (the Routing Display and the network map).

The link connections data table enables users to view the main parameters that are associated with a link connection. These parameters can help users to assess the bandwidth usage of the network. The link connections data table displays the following:

- Simple link connections that are derived from a unique server (for example, a VT1.5 link connection of an STS-1 infrastructure connection).
- Link connections that are derived from virtual concatenated servers (for example, a VCG link connection derived from a VCn/STSn).

Two additional columns are available in the **LINK CONNECTIONS** tab for **Infrastructure Connections** involving a configuration where 10AN1T is used as client card along with 8UC1T card. The following table provides the column name and description for the additional columns.

Table 2-5 LINK CONNECTIONS – Additional column and description

Column	Description
Group Number	The **Group Number** column displays the ODU4 slice to which the LCs belong.

Table 2-5 LINK CONNECTIONS – Additional column and description (continued)

Column	Description
Resource Restriction	The **Resource Restriction** column displays the corresponding trail capacity restriction and consists of the following values: • NA: Default value. • Capacity Restricted: If the trail has restriction value. **Note: Resource Restriction** is also added to the **LINK CONNECTIONS** list under Routing constraints.

See Table 25-7, "LINK CONNECTIONS tab – Column and description" (p. 2117) for the complete list of columns and descriptions that are available under **LINK CONNECTIONS** tab.

By default, the columns shown in Table 2-5, "LINK CONNECTIONS – Additional column and description" (p. 245) are hidden for the **LINK CONNECTIONS** tab for an **Infrastructure Connection** involving a configuration where 10AN1T is used as client card along with 8UC1T card.

Complete the following steps to view the **Group Number** and **Resource Restriction** columns.

1. From the NFM-T GUI, navigate to **OPERATE > Infrastructure Connections**. The **Infrastructure Connections** page is displayed.
2. Select the required **Infrastructure Connection** from the list and click the corresponding **360^0 View** icon.
3. Click **LINK CONNECTIONS** tab.
4. Click **More** icon at the top right corner of the table header and select **Manage Columns...**. The **Manage Columns** window is displayed.
5. Scroll down to select the **Group Number** and **Resource Restriction**.
6. Click **APPLY** to save the selection. Alternatively, click **CANCEL** to terminate the operation.

Link Connections state

Link Connection data have a state called *Invalid as Center Frequency*. This state during the provisioning operations identifies the *Available* Link Connections that are invalid for use in the current provisioning operation. The associated Link Connections are invalid because the channel/ spectrum width required for the connection is too small for that LC.

For a provisioning operation on a flexgrid trail, the user must select a center frequency that can accommodate the required channel/spectrum width. For example, if the spectrum width is 62.5, this value requires ten of the 6.25 grid slices to implement. When the user chooses a LC frequency, the chosen LC needs four available grid slices to the left of the selection and five to the right. At the bottom/lowest frequency range, the first four LCs are invalid as a center frequencies and at the top/ upper frequency range, the last five are invalid frequencies.

The operation formula to support a 62.5 spectrum width is: n(10) * m(6.25) = 62.5.

Note: This checking is only performed for Flexgrid Link Connections.

2.23 Client or server relationships

Connections linked by client/server relationships

A transmission network is layered; and, as such, the connections within a transmission network are linked to one another through client/server relationships.

A *client* is an object that uses a service of another object.

A *server* is an object that provides a service to another object.

Client/Server relationship of various connection types

The client/server relationship of the various connection types is as follows:

- Infrastructure trails can have other infrastructure trails or services (paths) as clients, and infrastructure trails can also have other infrastructure trails or physical connections as servers.

  When users access an infrastructure trail (either from a Connection list or from other windows, such as the Routing Display), the system provides users with access to the following:
  - To the list of infrastructure trail server connections; that is, the connections that are serving this connection (infrastructure trails or physical connections depending on the selected infrastructure trail position in the hierarchy.)
  - To the list of clients that are served by the infrastructure trail (infrastructure trails and services).
  - To the list of services that are served by the infrastructure trail (both direct clients and indirect clients).
- Services never have clients. Services always have servers.

  When accessing a service, the system provides users with access to the servers of the selected service, which are its infrastructure trails.
- Physical connections never have servers; they only have clients.

  When accessing a physical network connection, the system provides users with access to the clients of the selected connection, which are its infrastructure trails.

2.24 Auto Discovery

Auto Discovery definition

Auto Discovery feature in NFM-T automatically finds various types of connections during certain system events.

Auto Discovery of connections

The automatic discovery of physical connections occurs during the subnetwork discovery process.

Whenever an OTS connection is provisioned or notified, the automatic discovery of OMS connections occurs. When an OS connection is successfully provisioned or a notification is received, the NFM-T OTN automatically attempts to discover if the connection completes new OCH, OTUk, or ODUk rate connections. Automatic discovery is also attempted if the new rate is either OC-n or STM-n for specific NEs. If a new valid connection is discovered, it is added to the database.

Whenever an OTS connection is provisioned or notified from NFM-T, the automatic discovery of OMS connections occurs. When an OS connection is successfully provisioned or a notification is received, the NFM-T OTN automatically attempts to discover if the connection completes a new OMS rate connection. If a new valid connection is discovered, it is added to the database.

The process is illustrated in Figure 2-53, “NFM-T OTN Provisioning – Example – Supported Connection Layer Rates” (p. 251).

Auto Discovery of clients

The system automatically attempts to discover client connections whenever a new OS rate physical connection is provisioned in the system. When an OS connection is successfully provisioned, the system automatically attempts to discover if that connection completes any new OCH, OTUk, OTL4.4 , and/or ODUk rate connections. If the system successfully discovers a new valid connection at any of these rates, it adds it to the database.

When an ODU2 infrastructure connection that terminates on an 11QPE24, 11OPE8, or 11QCE12X circuit pack is successfully **Implemented**in the network, the system automatically attempts to discover if that connection completes any new DSR rate connections; and, if it does, that connection is automatically added to the connection list.

Auto Discovery of OS connections and OPSB protection

When a DSR or ODUk service is created with OPSB protection, the system automatically creates the OS connections between the following:

- The working ports on the OPSB circuit packs and the OTU client ports.
- The OS connections between the Protected Ports on the OPSB circuit packs and the OTU client ports.

The DSR or the ODUk connection remains in the **Defined** order step until all OS connections reach the **Commissioned** Deploy State.

Auto Discovery of DSR/ODUk service connections

The system automatically discovers DSR connections that terminate on ENEs and ODUk service connections that terminate on ENEs.

In addition, the system automatically discovers DSR/ODUk connections that reside on the client ports of a transponder, regardless if Alarm Reporting is enabled for the connection end points, if following conditions are met:

- The connections whose end points are on 1830 PSS OCS, 1830 PSS, 1830 PSS-1 MD4H, 1830PSS-4 or 1830 PSS-1 GBE/GBEH NEs.
- The connection end ports have a valid signal type and the signal type is the same for all connection endpoints.
- The connection end ports have a valid signal type and the signal types of all connection endpoints are equivalent, but are not necessarily the same for all connection endpoints.

  Example of asymmetric service connections:

  The system discovers a connection with one endpoint with signal type of 10GbE and one endpoint with signal type of OTU2.
- The connection end ports have valid signal type and the signal types of all connection endpoints are compatible, but are not necessarily the same, for all connection endpoints.

  Example of asymmetric service connections with channelized endpoints:

  The system automatically discovers a connection with one endpoint with signal type of 10GbE and one endpoint with signal type of OTU2 and a connection with one endpoint with signal type of OTU4 and one endpoint with signal type of OTU2.

Important!

The system does not automatically discover a DSR connection if the DSR connection consists of just one link connection and the server of the link connection is an external OS.

Auto Discovery of HO-ODUk connections

When users create a DSR service, the system can automatically create all point-to-point HO-ODUk infrastructures along with any accompanying LO-ODUk infrastructures. However, for any HO-ODUk infrastructures that involve pass-through HO cross connections or protected HO-ODUk infrastructures, users must provision these connections in separate steps.

Auto Discovery of edge HO infrastructure trail connections

The system discovers edge HO infrastructure trail connections that consist of an HO ODU cross connection between an OTUk port on an 1830 PSS OCS I/O card and a TTP on an ODUPOOL regardless if Alarm Reporting is enabled for the connection end points and regardless of if NIM is enabled for the connection endpoints. When an edge HO infrastructure trail connection is discovered, the system attempts to discover any client connections of the edge HO infrastructure trail connection.

When the system discovers an edge HO infrastructure trail connection, it automatically assigns it a connection name, changes the port type of the edge PTP port to eNNI, removes the edge PTP from the Free Port list, and sets the connection category to **Edge HO Trail** if the connection is in the Managed Plane or sets the connection category to **ASON Edge HO Trail** if the connection is in the Control Plane.

Auto Discovery and the D5X500 circuit packs

Auto Discovery, OTU4x2/OTU4 connections, and and D5X500 circuit packs

For the D5X500 pack, when an OTU4x2 connection is discovered, the system also discovers the two client ODU4 logical links. When an OTU4 connection is discovered, the system also discovers the client ODU4 logical link.

Auto Discovery, ODU4 and DSR client connections, and D5X500 circuit packs

When a new ODU4 logical link connection terminates on a D5X500 circuit pack is successfully provisioned in the system (meaning, it is in the **Implemented** state), the system discovers the corresponding ODU4 and DSR client connections if an ODU4 compound cross connection exists between a client port and the line port. If the system successfully creates new valid connections at the ODU4 and DSR rates, these connections are added to the database.

Auto Discovery and the 260SCX2, 1UD200, 2UC400 circuit packs

For the 260SCX2 pack in 260g mode, when an OTU4x2 connection is discovered, the system also discovers the two client ODU4 connections. If the pack is in Add/Drop Mode, the system also discovers the two client DSR connections.

For the 1UD200 pack in 260g mode, when an OTU4x2 connection is discovered, the system also discovers the two client ODU4 connections.

For the 2UC400 pack, when an OTU4x2 connection is discovered, the system shall discovers the two client ODU4 logical links.

2.25 Connection rates and layers

Connection rate

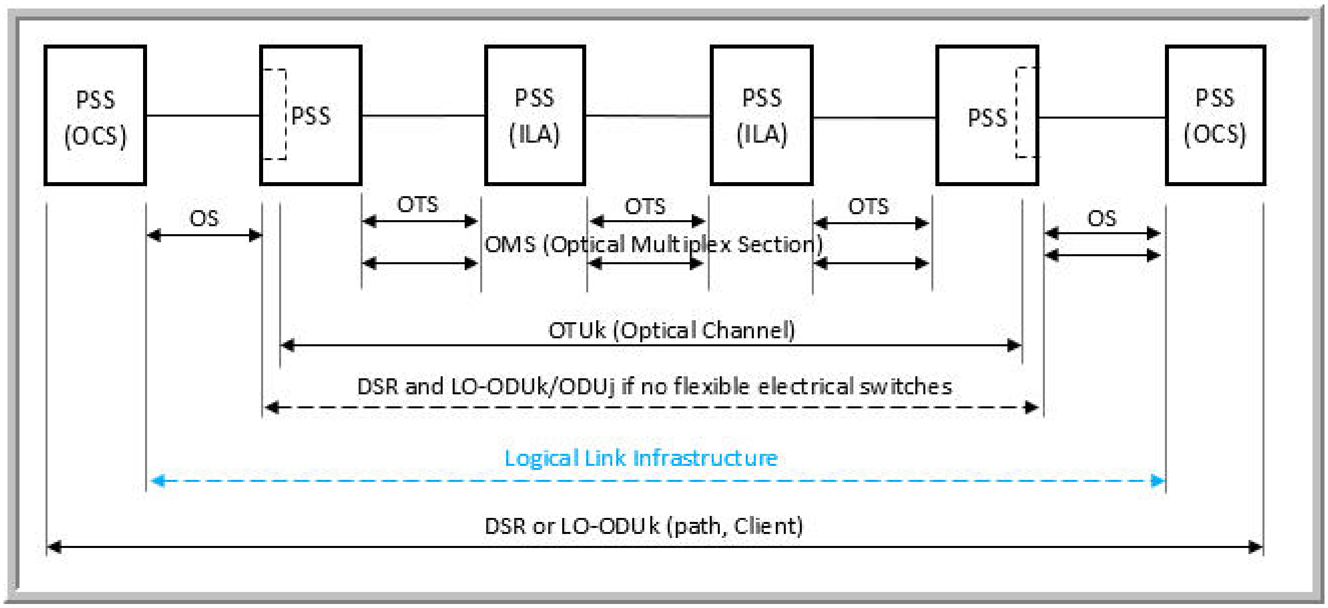
A *connection rate* represents a single layer or a merged layer described in 1.5 "Understanding the OTN" (p. 133) carrying a signal of a specified bitrate.

Connection layer rates

The NFM-T follows the G.709 standards model and models all appropriate layers in the network according to that standard. After the system automatically discovers some connection types during certain system events, users can then begin to provision one layer at a time starting from the physical layer.

For the management of an end-to-end connection, the following figure illustrates an example of the supported connection layer rates.

Figure 2-53 NFM-T OTN Provisioning – Example – Supported Connection Layer Rates



At the innermost layer, the OTS internal links are typically used for the external line connection of optical amplifiers between two NEs. The OS internal links are used for the fiber connections that carry one optical channel (for example, the OT line to SFD).

The OMS infrastructure connection is terminated on the first multiplexing points. For WDM, it is carried by OTS and terminated on LDs. Refer to section "OMS connections" (p. 254) for additional information.

The OTUk infrastructure connection typically terminates on the line ports of OT packs. WDM merges OCH and OTUk; so, the OTUk carries the frequency information for an optical channel. Refer to section "OTUk connection" (p. 255) for additional information.

Depending on the client mode, the HO-ODUk infrastructure connection for UNI typically terminates on OT line ports; for NNI, it can reach OT client ports and can be extended further and terminated on other NEs. Refer to "ODUk connections" (p. 255) for additional information.

The logical link connection (which is an infrastructure connection) serves to separate the WDM and OTN layers.

The DSR service serves as a client to carry transparent TDM, Ethernet signals, and terminates on OT client ports. The LO-ODUk is a service or an infrastructure. Refer to "OC-nRS/STM-nRS and DSR connections" (p. 258) and "ODUk connections" (p. 255) for additional information.

Note: Digital Service Rate (DSR) is a generic representation of the payload carried through the OTN network of different rates. For example these could be 1GBE, STM16 or 10GBE service.

Connection rate summary

The following table summarizes the available connection rates for infrastructures, services, and link connections.

Table 2-6 Connection Rate Summary for Logical Connections

	OCH	ODUk	OTUk	OMS	OC-nRS/STM-nRS and DSR
Name	Optical Channel	Optical Data Unit k	Optical channel Transport Unit-k	Optical Multiplex Section	Synchronous Transport Module Digital Service Rate

Table 2-6 Connection Rate Summary for Logical Connections (continued)

	OCH	ODUk	OTUk	OMS	OC-nRS/STM-nRS and DSR
Behavior	An OCH is a logical optical connection without a specific rate. Carries a single wavelength Spans multiple NEs.	An ODUk is a logical optical connection in which *k* is the specific rate. Spans multiple NEs. Becomes a server connection that creates link connections.	An OTUk is a logical optical connection in which *k* is the specific data rate. Translates the incoming signals to the appropriate wavelengths for multiplexing. Carried over a single wavelength. Performs signal regeneration and functions like PM. Spans multiple NEs. Is a server connection for an ODUk, which creates link connections.	Rides on the OTS. Between high speed lines of 2+ NEs. Carries multiplexed wavelengths with or without ILAs. Without ILAs, multiple OCH/ODUk link connections exist. The NFM-T OTN automatically creates OMS link connections based on the creation or discovery of an OTS connection.	Service connections supported for some NEs.
Provisioning			Discovery and user manual provisioning.	Discovery and user manual provisioning.	
Routing Modes		Automatic and Manual routing modes.	Automatic and Manual routing modes.	Automatic and Manual routing modes.	Automatic and Manual routing modes.

Table 2-6 Connection Rate Summary for Logical Connections (continued)

	OCH	ODUk	OTUk	OMS	OC-nRS/STM-nRS and DSR
Service Rates	OCH	ODU1 ODU1f ODU2 ODU2E* ODU3 ODU3E2 ODU4 ODUk		OMS	DSR** OC-3RS OC-12RS STM-4 OC-48 OC-192 FC 200 FC 400 FC 800 FC 1200 1GbE 10GbE 40GbE 100GbE
Infra-structure (Trail) Rates	OCH (default)	ODU0 ODU1 ODU2 ODU2E* ODU3 ODU3E2* ODU4 ODUflex OTSig Tunnel	OTL4.4 OTU OTU1 OTU2 OTU2E** OTU3 OTU3E2** OTU4 OTU4X2	OMS OMSBAND	OC-48RS OC-192RS STM-16 RS STM-64 RS
Link Connection Rates	OCH	ODUk	OTUk	OMS	OC-n RS DSR STM-n RS

OMS connections

An Optical Multiplex Section (OMS) is a connection that rides on an OTS connection. The NFM-T OTN automatically creates OMS link connections based on the creation or discovery of an OTS connection.

An OMS logical connection can exist between the high speed lines of two more DWDM NEs carrying multiplexed wavelengths with or without In-Line Amplifiers (ILAs). ILAs are sometimes referred to as *repeaters*. If ILAs do not exist between two DWDM NEs, then the Optical Multiplex Section has the same connection layout as the physical OTS connection. This type of OMS connection has multiple OCH/ODUk link connections. The number of link connections depends on the type and capacity of the NE that multiplexes many wavelengths.

With the manual based routing of OMS connection, both discovery and manual provisioning is supported. You can create OMS connections as infrastructure connections. Refer to 2.24 “Auto Discovery” (p. 248) for details on the Auto Discovery of OMS connections.

For Manual Routing, if the connection rate is **OMS** and the template type is OMS-P Protected, users can specify the OMS Protection to be **OPS Port A** or **OPS Port B**. By these user-defined designations for the **From Port**, **OPS Port A**, and **OPS Port B**, the system traverses the infrastructure connection to determine the route. No additional routing information is displayed or needed.

OTUk connection

OTUk is an *Optical channel Transport Unit-k* as defined in the G.709 model, where *k* represents the data rate of the connection. This unit translates the incoming signals to the appropriate wavelengths for multiplexing. It also performs signal regeneration and performs functions such as performance monitoring.

Table 2-7 G.709 OTUk Rates and Alternate Designations

G.709 Rate	Alternate Designation	Rate
OTU1	OTU2.5G	2.5 Gps
OTU2	OTU10G	10 Gps
OTU3	OTU40G	40 Gps
OTU4	OTU100G	100 Gps

An Optical channel Transport Unit-k connection typically is a infrastructure trail connection that spans multiple DWDM NEs and carries a single wavelength. An OTUk connection is a server connection for a ODUk connection, which creates one ODUk link connection (or more than one in the case of Mux OTs) in the NFM-T OTN. The OTUk connections can be discovered or provisioned explicitly by the user. OTUk provisioning is supported in the **Automatic** or **Manual** routing mode.

ODUk connections

ODUk is an *Optical Data Unit* as defined in the G.709 model, where *k* represents the data rate of the connection. This unit provides one of the transport structures that is needed to carry a signal across an optical network. An ODUk is carried by one or more OTUk connections in the network.

Table 2-8 G.709 ODUk Rates and Alternate Designations

G.709 Rate	Alternate Designation	Rate
ODU1	ODU2.5G	2.5 Gps
ODU2	ODU10G	10 Gps
ODU3	ODU40G	40 Gps
ODU4	ODU100G	100 Gps

In the NFM-T OTN, an ODUk connection typically spans multiple DWDM NEs and carries a single wavelength. Depending on the use of compatible optics ports on TDM NEs or using OTs in DWDM NEs, each ODUk connection can originate at either the TDM NE port or at the line side of the OT port.

ODUflex

The *ODUflex* is based on the *Flexible Rate Adaptation* mechanisms that enable users to configure capacities for containers based on the effective service traffic volume.

ODUflex envisages only the transport of the ODUflex payload into n*ODU-0 timeslots of a terminated ODUk.

ODUflex is a single networking entity, the n*ODU0s that carry an ODUflex container must be switched together as a bundle, and is managed and monitored as a bundle. The individual time slots are not visible for management. This implies that all OTN nodes that an ODUflex container can cross, must be ODUflex capable.

In addition, the n*ODU-0s are protected as a bundle using standard ODU SNCP protections.

GFP-F and CBR are supported by ODUflex: CBR supports fixed mapping, while GFP-F supports configurable size of mapping.

NFM-T manages ODUflex technology for *Managed Plane*, *L1, L0 and L1 overlay, and MRN* overlay network.

ODUflex is managed by 1830 PSS-24x, 1830 PSS-8x, 1830 PSS-12x, and 1830 PSS OCS shelves with the following cards:

- 1830PSS-24x shelf with 8UC1T, 10AN1T, 2UC400, 4UC400, 30AN300, 4AN400 , 20UC200 (THRU only), 6SE300 , 30SE300 cards.
- 1830 PSS-8x shelf with 1UX100, 20AX200, 20MX80 (THRU only) cards.
- 1830 PSS-12x shelf with 20MX80, 20AX200, 1UX100, 2UX200, and 4MX200.
- 1830 PSS-64, 1830 PSS-36 (OCS) shelves with 130SCUPC, 130SCUPB, 130SCUPH, 10AN10GC, 103SCEC, 11OCEC, and 1AN100G cards.

Note: ODUflex is supported by 1830 PSD Network Elements using 10GbE/1GbE Client OTU2 Network with ODUflex system mode.
When the NE is provisioned using 10GbE/1GbE client OTU2 network with ODUflex system mode, by default the client ports have 10 GbE client port rate. When a service connection is created, NFM-T automatically provisions the client port with the required rate.

- From the NFM-T GUI, navigate to **OPERATE** > **Equipment Manager**.
- From the navigation tree, browse to the 1830 PSD client port and click the **Configure** tab.
- Under the **Port Details** tab, change the **Signal Rate** to the required value. The available values are **TENGIGE** and **GIGE**.
  Note: If more than one timeslot is assigned, then the modification of the client port signal type from 1 GbE to 10 GbE is not allowed.

Note: With the 6SE300 and 30SE300 cards, the ODUPTF (ODU2e/ODUFlex) ports are not displayed in the EQM view. While, when a DSR or ODUPTF service is created (including

ODUflex) or ODUPTF ports are manually created on the NE, only WANIF ports are displayed. Being 30SE300 and 6S300 packet switch cards, packet switch needs to be created with EQM before creating a service. For details on packet switch provisioning see 1830 PSS Card Management in NE Management Guide.

1830PSS OCS shelves (1830PSS-64, 1830PSS-36) supports ODUflex with 6SE300, 30SE300, 103SCEC, 10AN10GC, and 11OCEC cards only for ODUFlex Add/Drop, GFP terminated and not-terminated service (channelized service) connection for both Control and Managed Plane connections.

From release 19.2, 1830 PSS-OCS supports Add/Drop configuration with 10AN10GC (R11.0/11.1) card. Moreover, ODUflex is supported by 20AX200 (R1.1) in the 1830 PSS-8x, by 20AN80 (R.11.1) and 30AN300 (R.11.1) cards housed in the 1830 PSS-24x shelf. These cards are handled similarly to the 20AX200 and 20MX80 cards when housed in the 1830 PSS12x shelf. For their provisioning refer to "2UX200" (p. 204).

Provisioning Note: Service creation with *Flexible Rate Client* is supported by:

- 20AN80 pack, only from 17 to 20 ports
- 30AN300 pack, from all ports
- 20AX200 pack, from all ports

Configurations

For Packet Switch cards, the ODUflex is used as an ethernet link to transport ethernet signals of different bandwidth towards the far-end for different packet topologies like E-LINE, E-TREE, etc.

Only pass-thru ODUflex crossconnects are supported for 1830 PSS-24X and 1830 PSS8-X cards. Only FC400 and 3GSDI services are supported with ODUflex with 11DPM12 card and 1830 PSS-24X and 1830 PSS-8X in cascaded configuration.

The OCS 1830 PSS node supports the add / drop configuration. The service can be terminated at the nodes for 103SCEC card. The switching card allows the client signal mapping in a ODUflex exploiting the GFP-F protocol.

Provisioning notes

To provision an ODUflex, select a *Service* template for *Ethernet* from **DEPLOY > New Service/ Infrastructure Connection** page.

In the **DEPLOY RULES** section select **Flexible Rate Client** as **Service Rate**. In the *Connection Characteristics* enter the bandwidth value in the **ODUflex Bandwidth(Gps)** field.

The **Container** parameter is set to `ODUflex` automatically in the **TRANSMISSION** tab of **PARAMETERS** section. (for more information, see "ODUflex Bandwidth (Gps)" (p. 700)). Complete the other fields and deploy the connection. Once Service is created, the ports involved in the connection, will be automatically created and provisioned by the system.

The information related to the Service created with **Flexible Rate Client**, like the ODUflex Bandwith (Gps), visualized when selecting the *Additional Attribute* of the Service.

ODUflex support for Control Plane network

From NFM-T R20.11, ODUflex is supported on Control Plane network for the following network elements:

- 1830 PSS-64
- 1830 PSS-36
- 1830 PSS 8
- 1830 PSS 32
- 1830 PSS 16 Type II
- 1830 PSS-24x
- 1830 PSS-12x
- 1830 PSS-8x (Uplink cards only)

GMRE support for ODUflex connectivity are ODU types that have flexible ODUk rate to determine the number of 1.25 GHz slices per interface.

NFM-T supports the following for the ODUflex Control Plane connections:

- ODUflex uses a user defined end-end fixed number of ODU0 slices irrespective of the interface type.
- GMRE Syntax is "odu0-Xf“, where "x" can be any number between 1 and interface maximum number (80 for ODU4; 8 for ODU2).
- Input/Output client supporting ODUflex signal [Support of multiplexing, switching and protection of ODUflex] 1AN100G, 10AN10GC, 4MX200, 4AN400, 20UC200, 30AN300.
- Uplink cards supporting ODUflex signal [Support of multiplexing, switching and protection of ODUflex] 130SCUPC, 130SCUPH, 4UC400, 2UC400, 2UC200E, 8UC1T, 1UX100, 2UX200.
- IO Cards/Ethernet client supporting ODUflex signal [Support GFP-F mapping of Ethernet client signal into ODUflex] 1AN100G, 10AN10GC, 4AN400, 30AN300.

OTSiG tunnel

OTSiG tunnel provisioning as a signal rate is available under */Best Practices/Infrastructure Trail/ Unprotected* with *ODUk or OTSiG Tunnel* template. OTSiG Tunnel provides end-to-end infrastructure connectivity between transponders / uplinks. The OTSiG Tunnel groups the individual carriers (wavelengths), which are referred to “OTS-iG” objects. When the user selects **OTSiG Tunnel** as the **Rate**, the **OPTICAL LINE CHARACTERISTICS** pane is enabled.

OTSiG Tunnel is supported for Managed Plane and Control Plane MRN Tunnel.

OC-nRS/STM-nRS and DSR connections

Service connections are supported at the OC-nRS/STM-nRS and DSR rates. DSR and OC-nRS/ STM-nRS infrastructure trail connections are supported for some NEs. Provisioning is supported in the **Automatic** and **Manual** routing modes.

Note: Digital Service Rate (DSR) is a term that is used generically to represent the service rate of a connection that is being provisioned. When provisioning the service path, users must select the actual **Service Rate** of the connection in order for the connection to be implemented.

For the successful interworking of the 1830 PSS OCS and 1830 PSS WDM NEs, users must select compatible and consistent values for the **Mapping Mode** and **Payload Type** parameters when creating a DSR connection. The following values are not compatible or consistent values:

- **Mapping Mode** of **Async** and **Payload Type** of **BSCBR**
- **Mapping Mode** of **BitSync** and **Payload Type** of **ASCBR**

When creating a DSR connection with Signal Type of OC-192 or STM-64, if at least one connection endpoint is on an 1830 PSS OCS NE and at least one connection endpoint is on an 43SCX4 or 43SCX4E circuit pack on an 1830 PSS or 1830 PSS-4 NE, the following guidelines apply:

- If the user selects the value of **Async** for the Mapping Mode parameter and the value of **Use NE Values** for the Payload Type, for all endpoints on 1830 PSS OCS NEs with which the ODU2 FTP is associated, the OC-192/STM-64 PTP has the Payload Type set to **ASCBR**.
- If the user selects the value of **BitSync** for the Mapping Mode parameter and the value of **Use NE Values** for the Payload Type, for all endpoints on 1830 PSS OCS NEs with which the ODU2 FTP is associated, the OC-192/STM-64 PTP has the Payload Type set to **BSCBR**.
- If the user selects the value **ASCBR** for the Payload Type parameter and **Use NE Values** for the Mapping Mode, for all endpoints on the 43SCX4 and/or 43SCX4E circuit packs, the DSR CTP has the Mapping Mode set to **Async**.

  If the user selects the value **BSCBR** for the Payload Type parameter and **Use NE Values** for the Mapping Mode, for all endpoints on the 43SCX4 and/or 43SCX4E circuit packs, the DSR CTP has the Mapping Mode set to **BitSync**.

  For all endpoints to have compatible values either of the following can occur:

  - All 1830 PSS OCS endpoints must have the Payload Type of **ASCBR** and all 43SCX4/ 43SCX4E circuit packs must have the Mapping Mode of **Async**.
  - All 1830 PSS OCS endpoints must have the Payload Type of **BSCBR** and all 43SCX4/ 43SCX4E circuit packs must have the Mapping Mode of **BitSync**.

2.26 Connection names and aliases

Connection name formats

Users can name internal link, service, and infrastructure trail connections during the initial creation of the connection in the **Connection Name** field. In addition, users can subsequently modify the name that they have given to the connection.

The format of a **Connection Name** on the NFM-T GUI is based on one of the following three name formats:

1. **M1400**, which has a fixed **Name Format** of:

   A central office <separator> Z central office <separator> connection rate <separator> ID
2. **Telcordia**, which has a fixed **Name Format** of:

   ID <separator> connection rate <separator> A location <separator> Z location
3. **Free format**

The type of separator used is controlled by the **Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR)** and the **Port based Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR2)** system parameters. Refer to the *Administration Guide: System Maintenance and Troubleshooting* for details on these system parameters.

Note: If the user leaves the **Connection Name** blank, the system automatically generates a connection name according to the values that are specified in the **Connection Name Format (NWC.CONNECTION_NAME_FORMAT)** and **Auto Discovery Connection Name Format (AUTO_CONN_NAME_FORMAT)** system parameters; and, for the separator, the system uses the values specified in the **Port based Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR2)** system parameter.

With **Free format**, the format for the automatically populated portion of the connection name using a system parameter is also selected. The choices are **M1400** or **Telcordia**; meaning, the auto-population part of the service or infrastructure connection name follows either **M1400** or **Telcordia** format, and users can change any of the populated strings to whatever they prefer. With one of the fixed formats (**M1400** or **Telcordia**), the auto-populated strings such as A or Z location, and connection rate cannot be changed. Users must only enter the ID part of the service or infrastructure connection name.

The names that users give to their connections must be unique. If users select one of the fixed formats, they can have two different connections with the same IDs or qualifiers, the same A and Z locations, but with different connection rates; or they can have two different connections with the same IDs or qualifiers, the same connection rate, but with different A or Z locations.

For PSS-4 and PHN (starting from R11.0) NEs, **Connection Name** supports UTF-8 encoding.

UTF-8 allows the use of ideograms, supporting compatibility for example with Chinese and Japanese languages. In such cases:

- Node/NE label length is 32 characters

- Service/Connection label length is 15 characters

In addition, some cards/configurations have specific behavior with UTF-8, such as:

- UTF-8 cannot be used for Y-cable protected services (this is valid for all PSS SWDM NE types: 32/16 II/16/8/4 and any card supporting Y-cable).
- UTF-8 is not supported for all services based on 11DPE12E/A card (old generation L2 cards).
- UTF-8 cannot be used for OPTSG function (11DPM12), discovery operations (Create from NE and Discover into NFM-T) but if provisioning is performed from NFM-T, then the name associated with the XC on the NE is blank.
- UTF-8 cannot be used for ODUJ XC protected (ODU0/1/2 and so on, SNCP ODUj protection). XC name is shown correctly on the NE but the protection group description (a string attribute) does not support UTF-8.
- TID field should always be with non-UTF-8 characters.

Automatic generation of a connection name

The **Connection Name** field on the NFM-T GUI is optional; meaning users do not have to specify a connection name because the NFM-T OTN automatically generates a connection name if one is not specified.

If a user leaves the **Connection Name** blank, the system automatically generates a connection name according to the values that are specified in the **Connection Name Format (NWC.CONNECTION_NAME_FORMAT)** and **Auto Discovery Connection Name Format (AUTO_CONN_NAME_FORMAT)** system parameters; and, for the separator, the system uses the values specified in the **Port based Connection Name Separator (NWC.CONNECTION_NAME_ SEPARATOR2)** system parameter.

The system generates a connection name automatically according to one of the following formats:

- **M1400**, which has a fixed format of:

  A central office <separator> Z central office <separator> connection rate <separator> qualifier

  Where:

  qualifier is a 4 digit number from 1 to 9999.

  For a new **A central office <separator> Z central office <separator>** connection rate, the NFM-T sets the first qualifier to 1 and then increments it by 1 for each new connection. When auto generating a service or infrastructure connection name, the system always uses the smallest free qualifier. For example, if the used qualifiers are {1, 2, 3} and if a user enters 500, the system generates 4 for the next qualifier.

  The type of separator that can be used is controlled by the **Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR)** system parameter. Refer to the *Administration Guide: System Maintenance and Troubleshooting* for details on this system parameter.

- **Telcordia**, which has a fixed format of:

  qualifier <separator> connection rate <separator> A location <separator> Z location

  Where:

  qualifier is a 4 digit number from 0001 to 9999.

The type of separator that can be used is controlled by the **Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR)** system parameter. Refer to the *Administration Guide: System Maintenance and Troubleshooting* for details on this system parameter.

- **Free format**, which depends on the format selected by the system parameter. Refer to "Connection name formats" (p. 260) for details.
- **Port Based**, which is the default value.

  The **Port based** format for internal links (internal OS/OTS physical link connections) is the following:

  NE name <separator> port1 <separator> port2 <separtor>

  The Port Based format for ODUk/OTUk trail and ODUk service connections is the following:

  NE1name <separator1> port1 <separator2> NE2name <separator1> port2 <separtor2> Stringed version of Layer Rate

  The Port Based format for DSR service connections is the following:

  NE1name <separator1> port1 <separator2> NE2name <separator1> port2 <separtor2> Signal Type from End Port

  The Port Based format for OCH service connections is the following:

  NE1name <separator1> port1 <separator2> NE2name <separator1> port2 <separtor2> OCH

  Note: For the **Port Based** format, users can select two separators. The separators are defined according to the values set in the **Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR)** and **Port based Connection Name Separator (NWC.CONNECTION_NAME_SEPARATOR2)** system parameters.

  For connections that span more than one NE, the A1/Z1 port is used when generating the connection name for the end points. Once a connection name is generated, the user must rename the connection if the NE or ports change. Automatic renaming does not occur.

When the creation of a DSR connection results in the automatic creation of an ODUk connection, the system generates a connection name for all system created server connections using these rules. The connection name format is based on the settings of the **Connection Name Format (NWC.CONNECTION_NAME_FORMAT)** and the **Auto Discovery Connection Name Format (AUTO_CONN_NAME_FORMAT)** system parameters. Refer to the *Administration Guide: System Maintenance and Troubleshooting* for details on these system parameters.

If the user enters a connection name that contains German characters, the system also generates a connection name using these rules.

Connection aliases

The **Connection Alias** field on the OTN WebUI is also optional and its display on the NFM-T GUI is determined by the setting of the **Connection Alias (NWC.CONNECTION_ALIAS)** system parameter. Refer to the *Administration Guide: System Maintenance and Troubleshooting* for details on this system parameter.

When creating/modifying a connection the user can enter 178 characters in **Connection Name** and the user can enter 256 characters when creating/modifying **Alias** and **Alias 2**.

Note: Special character `%` (percentage) is not supported, all other characters are supported.

Infrastructure connection or service names also support the international character set (for example, circumflex and accents) and UTF-8 encoding.

The infrastructure connection or service name is used to generate the cross connection user label when creating cross connections on 1830 PSS, 1830 PSS-1, and 1830 PSS-4 NEs.

When the infrastructure connection or service name is less than or equal to 60 characters, the infrastructure connection or service name is used as the cross connection user label.

When the infrastructure connection or service name is greater than 60 characters, the infrastructure connection or service name is truncated to ensure the length of the cross connection user label is exactly 60 characters.

2.27 Protected connections

Protected connection definition

A *protected connection* is an infrastructure connection or service connection that is assigned the Protection Level of protected or segment protected.

Protected connections protection types and parameters

Protection types include the following:

- *Optical Protection Switch Advanced* (OPSA)

  OPSA is a type of enhanced network protection afforded by the OPSA board that supports *server-side* OPS protection. It provides 1+1 OCh, OMSP, or OLP protection over DWDM lines.

  Note: The OPS packs (OPSA and OPSB) are implemented as half-height modules. The OPS packs provide photonic protection switching in DWDM configurations for channels supporting the C-band, which enables users to provide 1+1 APS protection.
- *Optical Protection Switch Board* (OPSB)

  OPSB, which is a type of protection that is afforded by an OPSB pack, which is an 1830 PSS NE circuit pack that supports *client-side* OPS protection. The OPSB pack uses a non-latching switch, which means that upon power failure, the OPSB automatically switches back to the default path of the connection. It provides 1+1 protection with shelf diversity.
- *Subnetwork Connection Protection* (SNCP)

  SNCP is specified for infrastructure connections (trails) or services to create protected cross connections. Managed Plane SNCP (MP SNCP) where the protection group is in the managed plane domain. Control Plane SNCP (CP SNCP) where the protection group is in the control plane domain. A mixed plane connection is one that has MP SNCP, CP SNCP or both.
- Y-Cable

  A *Y-cable*, also called a *splitter* or *signal splitter*, is a type of cable that contains three ends. One end of the cable is common; the other end splits into two leads. The Y-Cable Protection feature is available for SONET and SDH service connections.

The following table identifies the parameters that apply to a specific protection type and those parameters that are displayed in the **Protection** tab.

Table 2-9 Protection Type and Parameters

Field	OPSA	OPSB	Y-Cable	MP SNCP	CP SNCP
Switch Mode	No	No	Yes	No	No
Hold Off Time	No	No	No	Yes	No
Protected Protection Method	No	No	No	Yes	No

Table 2-9 Protection Type and Parameters (continued)

Field	OPSA	OPSB	Y-Cable	MP SNCP	CP SNCP
Protecting Protection Method	No	No	No	Yes	No
Signal Degrade for Protection Switching	No	Yes	No	Yes	No
Revertive Mode	Yes(1)	Yes	Yes	Yes	No
Wait to Restore Time	Yes(1)	Yes	Yes	Yes	No

Note: Because a connection can consist of multiple SNCP protected control plane segments and each can have a different value for the same parameter, there is no connection level value for these fields and all the fields have N/A as the value. To view the values for a control plane segment use the ASON SNC tab in the 360 degree view.

(1) This feature is supported only for specific types of shelves and packs. See 7.92 “Manage OPSA protection with revertive mode” (p. 1114)

Protected connection inclusions and exclusions

The Protected Connections data table list includes all protected service connections and protected infrastructure connections, regardless of the protection type, which include the following:

- Managed Plane connections
- L1 Control Plane connections
- Mixed Plane connections in which the Control Plane section of the Mixed Plane connection is a L1 Control Plane connection

For managed plane network SNCP Protection the value of Protection Type is the Network Protection Type such as SNC-N, SNC-I, and so on.

For Control Plane SNCP protection the value of Protection Type shall be SNCP-N.

For Client SNCP Protection the value of Protection Type is the value of Client Protection Type such as SNC-N, SNC-Nc, and so on.

The Protected Connections List does not include server protected connections:

- It lists the **Defined**, **Allocated**, **Implemented**, and **Commissioned** Connections. Refer to 7.86 “View Protected Connections” (p. 1091) and 7.87 “View tabbed topics for a protected connection” (p. 1095) for details.
- The **From End Active Route** indicates if the **Working** or **Protection** Route is the **Active Route**

of the first protection group on the **From End** of the connection. This is the first network protection group found in the route starting from the **From End** of the connection and may not be on the end node.

- The **To End Active Route** indicates if the **Working** or **Protection Route** is the **Active Route** of the first protection group on the **To End** of the connection. This is the first network protection group found in the route starting from the **To End** of the connection and may not be on the end node.
- The **Active Route** indicates if either the **From End** or **To End** of the connection has the Protection Route as the **Active Route**. By sorting on this field a user can find all connections which have the **Protection Route** as **Active**.
- For connections with more than one protected segment the value of the **Active Route** field is calculated using only the **From End** and **To End** Network Protection groups. All intermediate protection groups are ignored.

A value of NA can appear for the **Active Route**, **From End Active Route**, **To End Active Route**, **From End Switch Reason** and **To End Switch Reason** for the following reasons:

- the connection is not in Commissioned state
- the network element is not Communicating
- the connection is an Inconsistent connection
- the connection has been created or rearranged and the switch data has not yet been synchronized with the Network Element
- the connection has been discovered and the switch data has not yet been synchronized with the Network Element
- an inconsistent connection has been restored and the switch data has not yet been synchronized with the Network Element
- asymmetric three ended connections with protection at only one end of the connection

The Synchronized Switch Data with Network column in the Protected connection list indicates that the values displayed for the **Active Route**, **From End Active Route**, **To End Active Route**, **From End Switch Reason** and **To End Switch Reason** are up to date or they may be out of synchronization with the network element. In such a scenario, a value of out of synchronization is displayed because of the following reasons:

- the network element is not communicating
- the connection is an inconsistent connection
- the switch data for the connection has not yet been synchronized with the Network Element

If the user believes the protection switch data is not synchronized with the network element the user can choose to synchronize the data with the Network Element by choosing a connection and the Synchronize Switch Position action. The **Synchronize Switch Position** action retrieves the current protection switch data from the network element. See 7.89 “Perform Synchronize Switch Position” (p. 1103).

The user can also synchronize protection switch data for an entire network element using database synchronization

User interaction with protected connections

When an infrastructure connection is selected in the Protected Connection List the NFM-T GUI enables users to perform the same actions from the **Operate > Protected Connections** navigation path as it does from the **Operate > Infrastructure Connections** path, refer to 7.85 “Manage Protected Connections” (p. 1088) for details.

When a service connection is selected in the Protected Connection List the NFM-T GUI enables users to perform the same actions from the **Operate > Protected Connections** navigation path as it does from the **Operate > Service Connections** path; refer to 7.85 “Manage Protected Connections” (p. 1088) for details.

To synchronize switch position, see 7.90 “Perform protection switching” (p. 1106), 7.91 “Perform Force Switch Operation” (p. 1112) and 7.91 “Perform Force Switch Operation” (p. 1112).

2.28 TCM connections

TCM definition

Tandem Connection Monitoring (TCM) is a network management feature for 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, and 1830 PSS 8X shelves, and for Managed Plane connection on 1830 PSS 32 for 260SCX2 service pack, that facilitates the monitoring of the transport path of a client signal as it passes through the network at the ODUk (HO/LO) layer.

TCM is the overhead part of the monitoring, which supports monitoring of arbitrary subnetwork connections. These monitoring functions may be used to monitor segments of an end-to-end OTN trail (path) and can be used to support unprotected or protected connections.

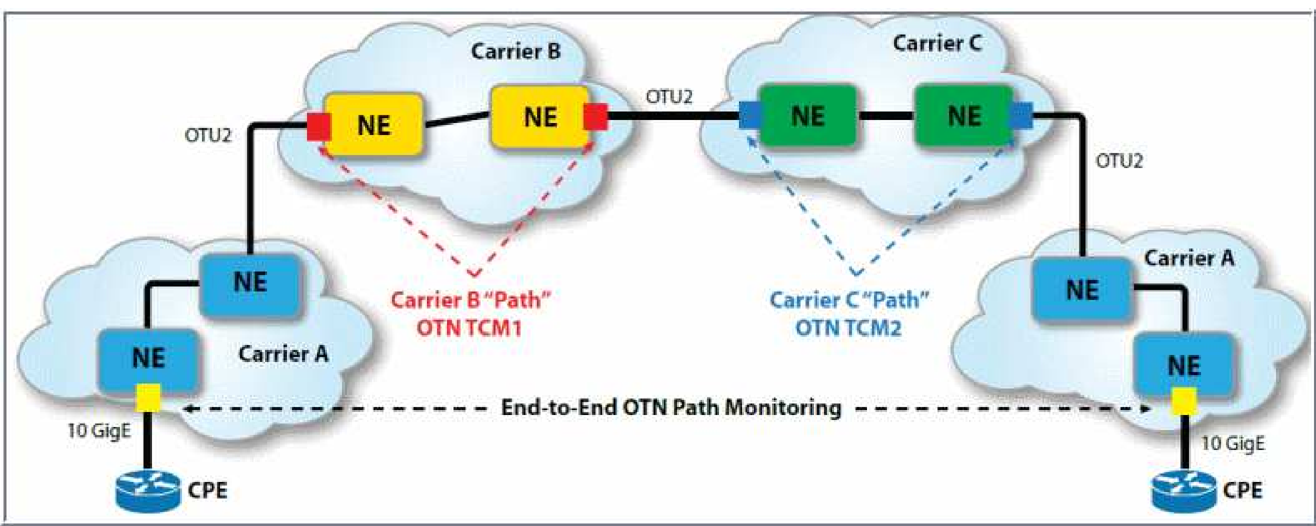
TCM can be viewed as a sublayer connection that lies between the client layer connections and server layer connections.

OTN enables path-layer monitoring at multiple, user-defined endpoints, and it is one of the more powerful features of OTN.

Six levels of TCM, each with various modes of operation, are provided to allow for simultaneous use for different monitoring applications along any each and every individual ODU trail. These applications include: segment protection, administrative domain monitoring, service monitoring, fault localization, verification of delivered quality of service, delay/latency measurements and adjacency discovery. It is important to note that for any given hierarchy of ODU trails, each independent ODU trail within that hierarchy is supported by an end to end path monitor and also by all six levels of tandem connection monitors. TCMs for one particular ODU layer trail within the hierarchy do not interfere with TCMs assigned for another ODU layer trail within the hierarchy.

TCM provide this user-defined path monitoring function. There are up to six different levels of TCM available in the OTN overhead, labeled TCM1 through TCM6. These bytes allow carriers to define their own path layers.

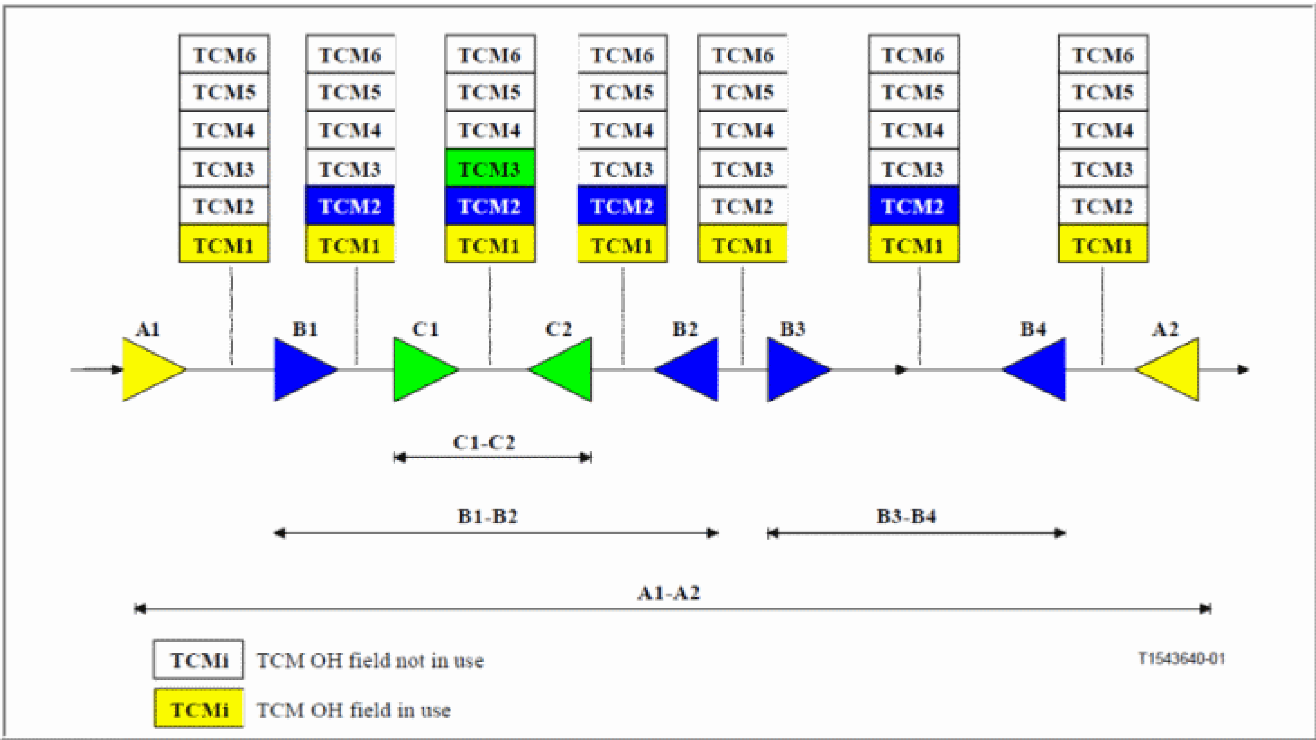
Figure 2-54 OTN Tandem Monitoring



Monitored connections A1-A2/B1-B2/C1-C2 and A1-A2/B3-B4 are nested, while monitored connections B1-B2/B3-B4 are cascaded. Overlapping monitored connections are also supported.

A TCM field is assigned to a monitored connection. The number of monitored connections along an ODUk trail may vary between 0 and 6. The types of monitored connections are nested, overlapping, and cascaded.

Figure 2-55 ODUk monitored connections



TCM Types

Depending on what is supported on the 1830 PSS OCS NE, the management system automatically enables one of the following types of TCM:

- *LC*, or *link connection based TCM*, for logical optical physical connection (LOPCs) or OTUk connections.

  The link connections or OTUk connection rates that are supported are OTU2, OTU2e, OTU3, OTU3e2, and ODUk (with connection type = L-OPC) where k = 0, 1, 2, 2e, 3, 3e2, 4 for any OTUk or link connection regardless of whether one or both endpoints are on an 1830 PSS OCS NE or whether one or both end points are on circuit packs on an 1830 PSS-24X shelf.
- *XC*, or *cross connection based TCM*, for LO-ODUk or HO-ODUk connections.

  The ODUk connection rates that are supported are ODU4, ODU3e2, ODU3, ODU2e, ODU2, ODU1, and ODU0 for any LO-ODUk or HO-ODUk connection regardless of whether one or both endpoints are on an 1830 PSS OCS NE or whether one or both end points are on circuit packs on an 1830 PSS-24X shelf. For 1830 PSS-32 and the 1830 PSS-24X, the applicable **k** values are 0, 1 ,2, 2e, and 4.

Note: If the selected connection does not have one or both endpoints on the particular 1830 PSS OCS NE or 1830 PSS-24X shelf, the first ingress and egress OCS NE/port is used to provision TCM.

TCM ASAP

An Alarm Severity Assignment Profile (ASAP) can be set on TCM endpoints in one of two ways:

- When users enable TCM on a connection, the management system enables ASAP by default.
- Users can set ASAP on TCM endpoints using the Assurance panel during connection provisioning.

TCM support

TCM is supported on Control Plane, Mixed Plane, and Managed Plane connections.

In Control Plane and Mixed Plane connections, TCM is supported for unterminated ports.

During the deployment of the connection (see 7.12 “Deploy a template to make a connection” (p. 754)), the **TCM** field is set by default to **No Tcm**. The modification of the **TCM level** for all ASON routed connections is currently disabled.

The TCM level flag for MRN tunnel (FA-Unterm) is fixed on level 6 because it is the GMRE default.

TCM support for 260SCX2

TCM is supported for three levels on the Managed Plane connection in 1830 PSS 32 shelf only for the 260SCX2 service pack, when the client signal type is OTU4. The TCM provisioning is not allowed on any other pack on the 1830 PSS 32 shelf.

The OT card supports TCM on both 100G and 200G modes of 260SCX2. TCM is applicable to HO and LO ODU.

TCM Alarms and TCM PM are supported as currently supported for 1830 PSS-24x nodes.

Managing TCM on 260SCX2

To manage the three levels of TCM on the 260SCX2 service pack follow the steps:

• During the deployment of the connection (see 7.12 “Deploy a template to make a connection” (p. 754)), the **TCM** field is set by default to **No Tcm**.

• Create Level 1 TCM. After this operation, **Create TCM** item is enabled on the right click menu of the connection, allowing the user to create remaining levels, two and three.

• Click on the PM Enabled Points tab for the selected connection on the Infrastructure connections page.

• The TCM Termination Points for the NE can be retrieved starting from the NE list for the TCM involved NE.

2.29 Looped back connections

Loopback definition

Loopbacks are tests that users can initiate to test a circuit or to isolate a failure by connecting test equipment to the system interface and to create the loopback at different points in the transmission path.

Loopbacks supported

The NFM-T OTN supports the following types of loopback operations, which include testing and returning status, for directly managed NEs.

- *Facility Loopbacks*, which are also referred to as *local tests*.
- *Terminal Loopbacks*, which are also referred to as *remote tests*.

Loopback support

Loopbacks are an installation, system maintenance, or troubleshooting function that the NEs offer and the NFM-T OTN supports.

The NFM-T OTN supports loopbacks only for the optical transponder circuit packs (OT packs) of directly managed NEs.

Important! Both loopback operations and loopback status are not provided for indirectly managed NEs. The NFM-T SDH application supports loopback operations and status for these NEs.

Loopback options available from the Routing Display

From the Routing Display, the **Loopback** options that are available to users are the following:

- The **Synchronize** option is available to synchronize the loopback status on an NE.
- The **Terminal Loopback** option is available when the port is capable of performing a Terminal Loopback and the loopback has not been set yet. Terminal Loopback can be executed only when the port is not already looped back in **normal** or **forced** mode (when supported by the NE).

  For the NFM-T OTN, the**Terminal Loopback** is applicable to the physical port at the client side and at the line side of an appropriate transponder.
- The **Facility Loopback** option is available when the port is capable of performing a Facility Loopback and the loopback has not been set yet. Facility Loopback can be executed only when the port is not already looped back in **normal** or **forced** mode (when supported by the NE).

  For the NFM-T OTN, the **Facility Loopback** is applicable to the physical port at the client side and at the line side of an appropriate transponder.
- The **Release** option is used to release the existing loopback on the port.

Loopback icon and Loopback tool tip

When the user's cursor is pointed to the **Loopback** icon on the Routing Display, a tool tip is displayed that indicates the loopback type that has been initiated on the port.

Figure 2-56 Looped Back Connections – Examples – Loopback Icon Location – Loopback Tool Tip Moused Over

Note the following about loopback status:

- When the Routing Display is initially displayed, the tool tip shows the loopback type as it is known in the application database. Refer to Figure 2-57, "Looped Back Connections – Example – Terminal Loopback Set on the Routing Display" (p. 272) and Figure 2-58, "Looped Back Connections – Example – Facility Loopback Set on the Routing Display" (p. 273).

Figure 2-57 Looped Back Connections – Example – Terminal Loopback Set on the Routing Display

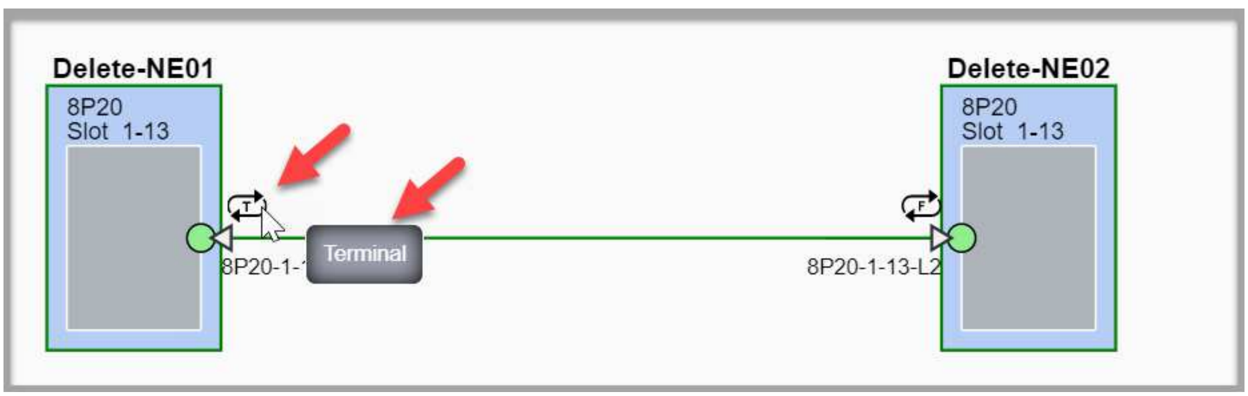


Figure 2-58 Looped Back Connections – Example – Facility Loopback Set on the Routing Display

Loopback disruptions

Loopbacks impact service operation. Before initiating loopbacks, the intended port or the related/associated ports must be set to out-of-service (OOS). Once loopback testing concludes, any OOS ports must be returned to their previous state.

The following general guidelines apply to client and line ports:

- For loopback testing on a client port, the client port needs to be put OOS before loopback testing begins. There is no need to put its line port OOS.
  For OT packs with multiple client ports, loopback testing on the client ports is independent.
- For loopback testing on a line port, the port, along with its associated client ports, must be put in OOS.
  For OT packs with more than one line port, loopbacks on each line port are independent.

Additional validations apply for each type of NE that supports loopbacks. Refer "Loopbacks for the Nokia 1830 PSS family of NEs " (p. 273).

When users initiate loopback testing, the system cautions and queries the user:

```
All services on this port will be impacted. Do you wish to continue?
```

Loopbacks for the Nokia 1830 PSS family of NEs

For the 1830 PSS family of NEs, **Terminal Loopback** and **Facility Loopback** are supported on all OT line and client ports; however, loopbacks are not supported for the following:

- 43STA1P client ports (no terminal and facility loopback)
- All VA ports
- On SVAC
- All OTs with Mode = Regen (no terminal and facility loopback)

The NE supports loopback testing when the OT pack is in a protected line configuration using OPS, Y-cable, or E-SNCP, where the loopback occurs at a physical port level such as not at a flow level in

E-SNCP. Users can only enable a loopback when the port is clear of being in a loopback state and is in a certain state OOS-MA (MT).

Important! When a port is in a loopback state, the NE does not allow the port to be deleted. In addition, its primary port state to set to IS. If the port is involved in an NE cross connection (LD to OT line), the loopback fails. The NFM-T OTN does not remove the cross connection so the loopback can go through. The user must use other methods to remove the cross-connection first, and then apply the loopback.

User Interactions with looped back connections

From the looped back connection level, the management system enables users to release the looped connection, and view the routing display. Refer to the following tasks:

- 7.103 “Initiate Facility Loopback Testing on an NE” (p. 1143)
- 7.104 “Initiate Terminal Loopback testing on an NE” (p. 1146)
- 7.105 “Release the loopback on a connection” (p. 1149)
- 7.106 “Synchronize loopback status on an NE” (p. 1152)
- 7.107 “View Looped Back Connections” (p. 1153)
- 7.108 “View tabbed topics for a Looped Back Connection” (p. 1155)

Provisioning Features

2.30 Single Step Provisioning

Single Step Provisioning definition

Single Step Provisioning is a method of connection provisioning in which the user creates one particular type of connection and the system automatically creates the appropriate server connection. In addition, when users modify the route of the connection, the system automatically modifies the route of the server connection.

Single Step Provisioning and LO-ODUk/DSR connections

With Single Step Provisioning, when users create a payload service known as the Digital Signal Rate (DSR) service, the system automatically creates the LO-ODUk server connection. Transmission parameters can be set for the DSR service that the user created and the ODUk server connection that the system created. One order is created for each connection and both orders transition through the order steps in tandem.

The user can only modify the route of the DSR. However, the user can modify parameters on both the DSR and LO-ODUk to change transmission parameters. During the creation, the TX parameters are set for both the DSR and LO-ODUk but to modify the TX parameters of the LO-ODUK the user must perform the action on the LO-ODUk. When users modify the route of the DSR service, the system automatically modifies the route of the LO-ODUk server connection. One order is created for each connection and both orders transition through the order steps in tandem.

Connection type, group name, and group order

All automatically created servers have the connection type of *Managed Plane Implicit Server*.

When servers are automatically created, the primary connection (the DSR connection) and the automatically created servers have an automatically assigned group name, which has the format:

g-[connection name]

Where: The connection name is the name of the primary connection.

When servers are automatically created, the primary connection (the DSR connection) and the automatically created servers have a group order status that reflects the status of all connections in the group. Meaning, if any connection is in a failed state, the group order status is *failed*.

Single Step Provisioning and auto creation of LO-ODUk with DSR

For 1830 PSS, 1830 PSS-4, and 1830 PSS OCS NEs, the following circuit packs support DSR connections that have supported server layers at the ODUj rate. The ODUj server is automatically provisioned along with the requested DSR connection:

- 11DPM12
- 11DPM8
- 11DPM4M
- 112SDX11

- 11QPE24
- 11OPE8
- 11QCE12X
- 20P200 (for 1830 PSS-32)
- 30AN400
- 4AN400

Restrictions

Restrictions include the following:

- Users can continue to create the immediate LO-ODUk connection; however, the DSR and LO-ODUk connections will not be linked.
- For DSR connections on 11DPM12 packs with OPTSG container type, the system does not automatically create the ODU1 server connection when the first DSR connection is created.
- When a DSR service has two or more LO-ODUk server connections, the system only creates the immediate LO-ODUk server connection. Users must create the second LO-ODUk.

Single Step Provisioning and HO-ODUk/OTUk connections

With Single Step Provisioning, when users create a HO-ODUk infrastructure connection (trail) or service, the system automatically creates the OTUk server connection. Users cannot create OTUk connections directly. One order is created for each connection and both orders transition through the order steps in tandem.

Transmission parameters can be set for the HO-ODUk connection that the user creates and the OTUk server connection that the system created.

Wave Key parameters can be set for the OTUk server connection that the system created.

Users can modify only the HO-ODUk connection that they created.

When users modify the route of the HO-ODUk infrastructure connection (trail) or service, the system automatically modifies the route of the respective LO-ODUk server connection. One order is created for each connection and both orders transition through the order steps in tandem.

When users delete or database delete an HO-ODUk connection, the system automatically deletes the OTUk server connections.

Supported circuit packs

When an ODUk service or infrastructure connection is created, the OTUk server connections are automatically created for the following circuit packs that support an NNI client port rate that is equal to the line port rate:

- 11STAR1
- 11STAR1A
- 43STA1P
- 43SCA1
- 11QPA4

- 11QPEN4
- 112SCA1
- 112SNA1
- 130SCA1

For the 260SCX2 pack, the following guidelines apply:

- In 130 mode, when an ODU4 service connection is created, the server OTU4 connection is created.
- In 130G or 260G mode, when an ODU4 (for 130G) or OTU4x2 (for 260G) infrastructure connection is created, the server OTU4 connection is created. If either 260SCX2 130G or 260G mode pack is in Add/Drop mode, the DSR client connection is created.

For a configuration where 260SCX2 card is used on both ends, single step provisioning is not supported. Ensure a connection is created using the following two-step process:

1. Create a Logical link.
2. Create a DSR or NNI client on C1 port.

The following are the guidelines to be adhered to while creating an ASON connection using the 260SCX2 cards:

1. A Logical Link must be created with ASON routed between the OTUODU4 ports.
2. A Managed Plane service must be created on C1 port.
3. If client ports are pre-provisioned, then the client ports are discovered.

Note:

For 100G service, user must create an ODU4 service from client to client ports. DSR service is automatically discovered by the system.

For 200G service, user must create an ODU4 service using C2 ports.

For the D5X500 pack, when an ODU4 logical link connection is created, the server OTU4x2 connection is created if it does not already exist.

For the 2UC400 pack, the following guidelines apply:

- In 100Gmode, when an ODU4 logical link connection is created, the server OTU4 connection is created.
- In 200G mode, when an ODU4 logical link connection is created, the server OTU4x2 is created if it does not already exist. Alarm monitoring is set to **On** for the two child OTU4 CTPs of each OTU4x2 connection end point.
- In 200G mode, when an ODU4 logical link connection is created, the second ODU4 logical link client of the server OTU4x2 is created if it does not already exist. Alarm monitoring is set to **On** for the connection end points. Ingress NIM, Egress NIM, and Transmission Parameters are not set.

For the 1UD200 pack, the following guidelines apply:

- In 130G mode, when an ODU4 infrastructure connection is created, the server OTU4 connection is created.

- In 260G mode, when an ODU4 infrastructure connection is created, the server OTU4x2 connection is created, providing it does not already exist.
- In 260G mode, when an ODU4 logical link connection is created, the second ODU4 logical link client of the server OTU4x2 is created if it does not already exist. Alarm monitoring is set to **On** for the connection end points. Ingress NIM, Egress NIM, and Transmission Parameters are not set.

For the 20P200 pack, when an ODU2/ODU2e infrastructure connection is created, the server OTU2/OTU2e connection is created.

For the 112SDX11 pack, if the signal type of the line port is OTU4, when an ODU4 infrastructure connection is created, the OTU4 server connection is automatically created. If the signal type of the line port is OTL4.4, when an ODU4 infrastructure connection is created, the OTU4 server connection and four OTL4.4 server connections are automatically created.

When the ODUk connection contains one or more regenerators (which users select via the Routing Constraints tab during connection creation and modification), multiple OTUk server connections are created. Example: For an unprotected ODUk connection, if the connection contains one regenerator, two OTUk server connections are created; and, if the connection contains two regenerators, three OTUk server connections are created. For a protected ODUk connection, if the service and protection paths each contain one regenerator, four OTUk server connections are created.

ODUk connections with regenerators

When the ODUk connection contains one or more regenerators (which are selected via the Routing Constraints tab), multiple OTUk server connections are created. Some examples follow:

- For an unprotected ODUk connection, if the connection contains one regenerator, two OTUk server connections are created.
- For an unprotected ODUk connection, if the connection contains two regenerators, three OTUk server connections are created.
- For a protected ODUk connection, if the service and protection paths each contain one regenerator four OTUk server connections are created.

Connection type, group name, and group order

All automatically created servers have the connection type of *Managed Plane Implicit Server*.

When servers are automatically created, the primary connection (the ODUk connection) and the automatically created servers have an automatically assigned group name, which has the format:

g-[connection name]

Where: The connection name is the name of the primary connection.

When servers are automatically created, the primary connection (the ODUk connection) and the automatically created servers have a group order status that reflects the status of all connections in the group. Meaning, if any connection is in a failed state, the group order status is *failed*.

For the 260SCX2 pack in 260g mode, when the second ODU4 client is created, the group name of the existing OTU4x2 server connection is used as the group name of the ODU4 connection.

Single Step Provisioning and DSR/ODU4 connections for D5X500 circuit packs

For the D5X500 pack, when users create a DSR connection, the system automatically creates the server ODU4 connection if it does not already exist.

When the server connection is automatically created, the primary connection, which is the DSR connection, and the automatically created server connection have an automatically assigned group name in the format of the following:

g-[connection name]

Where: The connection name is the name of the primary connection.

When the server connection is automatically created, the primary connection, which is the DSR connection, and the automatically created server connection, have a group order status. This status reflects the status of all connections in the group; meaning, if any connection is in a failed state, the group order status is failed.

ODU4 infrastructure connection creation:

When an ODU4 infrastructure connection is created either automatically with a DSR connection or directly by the user, the following port parameters are set for the connection end points:

- Alarm monitoring is **Enabled**.
- Ingress NIM and Egress NIM are **Enabled**.
- Transmission parameters are set by the user.

In addition, when an ODU4 infrastructure connection is created either automatically with a DSR connection or directly by the user, the following port parameters are set for the intermediate ports on the D5X500 pack in the connection:

- Alarm monitoring is **Enabled** for OTU4 FTPs and ODU CTPs on D5X500 packs.
- Ingress NIM and Egress NIM are **Enabled** for ODU CTPs on D5X500 packs.
- Trail trace parameters are set for the OTU4 ports on D5X500 packs.
- Burst Threshold and Burst Interval are set for OTU4 and ODU4 ports on D5X500 packs.
- For protected connections, Alarm Monitoring, NIM and Transmission Parameters are set for both the working and protected ODU4 connections.

ODU4 service creation:

When an ODU4 service is created connection with connection end points on client ports on D5X500 packs is created, the following port parameters, the following port parameters are set for the connection end points:

- Alarm monitoring is **Enabled**.
- Ingress NIM and Egress NIM are **Enabled**.
- Transmission parameters are set by the user.

In addition, when an ODU4 service is created, the following port parameters are set for the intermediate ports on D5X500 packs in the connection:

- Alarm monitoring is **Enabled** for OTU4 FTPs and ODU4 CTPs on the D5X500 packs

- Ingress NIM and Egress NIM are **Enabled** for the ODU4 CTPs on the D5X500 packs
- Trail trace parameters are set for the ODU4 CTPs and OTU4 ports on D5X500 packs
- Burst Threshold and Burst Interval are set for OTU4 and ODU4 ports on D5X500 packs
- For protected connections, Alarm Monitoring, NIM and Transmission Parameters are set for both the working and protected services. The Transmission Parameters are based on the OT ports and not the connection end points

Note: The system supports OPSB client protection and OPSA protection support for D5X500. OPSB is managed in 100Gbe and OTU4 client types and for managed-plane and L0 GMPLS network configurations:

- OPSB is supported for all D5X500 supported modulation (being a client protection and independent by the modulation). OPSB client protection with line rate OTU4Half (modulation-BPSK) and OTU4HalfX5 (modulation- 16QAM_250G) is not supported.
- OPSB is supported in any PSS photonic architecture: FOADM, ROADM WR8-88/CWR8, D/D'/D'' configuration (colored/colorless), CDC-F, CD-F and C-F.

OPSA must be supported for all D5X500 modulations:

- OPSA on D5X500 is uni-directional, non-revertive.
- Conventional ROADM with filtered optical drop ports - MUX (e.g. ROADM, TOADM, FOADM including D/D'/D'' config with D5X500 connected to MUX/colored)
- For OPSA OCH line protection, we only support it for OTU4, and OTU4x2 line

Figure 2-59 D5X500 (100G Mode) with OPSB – 100GbE Client, Managed Plane

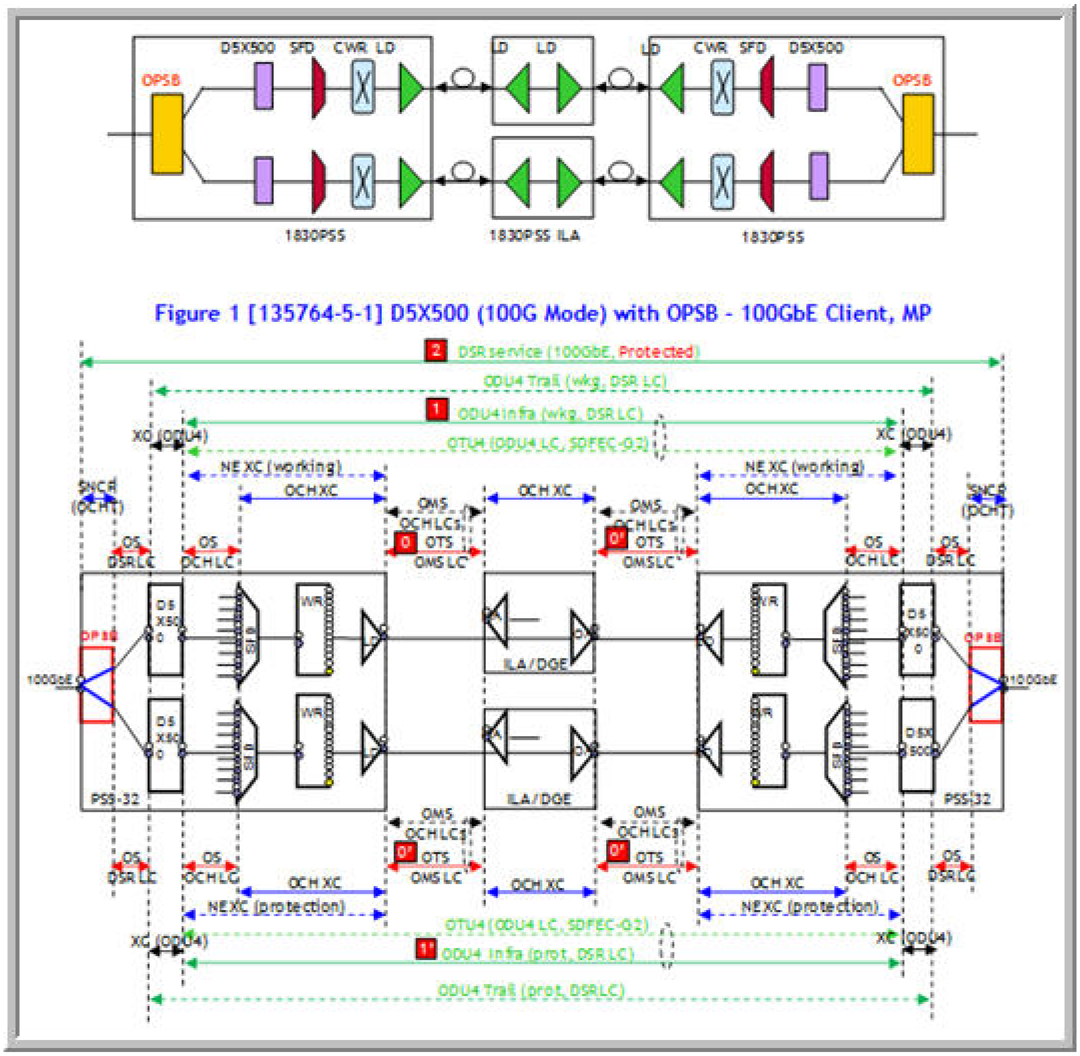


Figure 2-60 D5X500 (100G Mode) with OPSB – 100GbE Client, L0 Control Plane

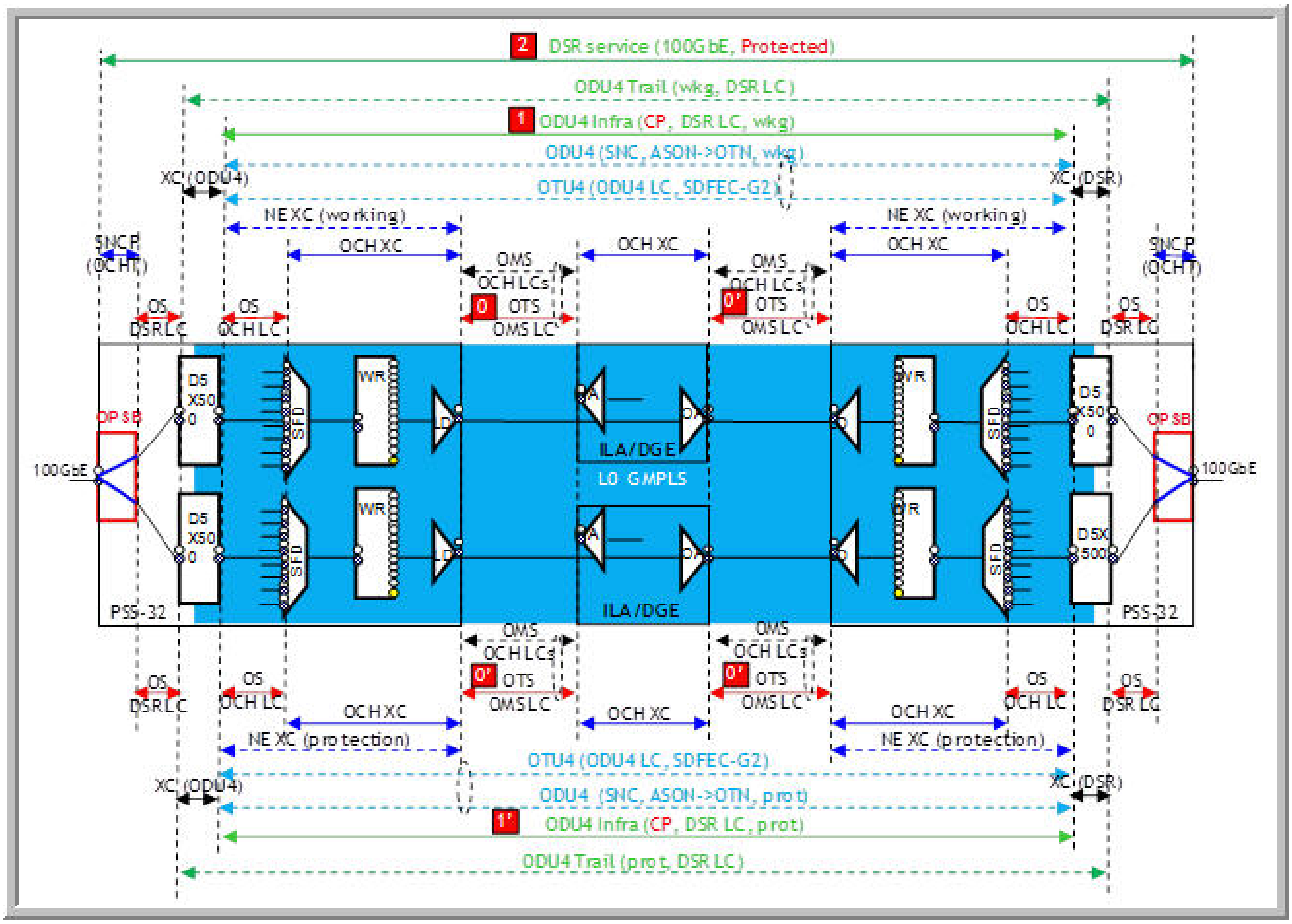


Figure 2-61 D5X500 (100G Mode) with OPSB – OTU4 Client, Managed Plane

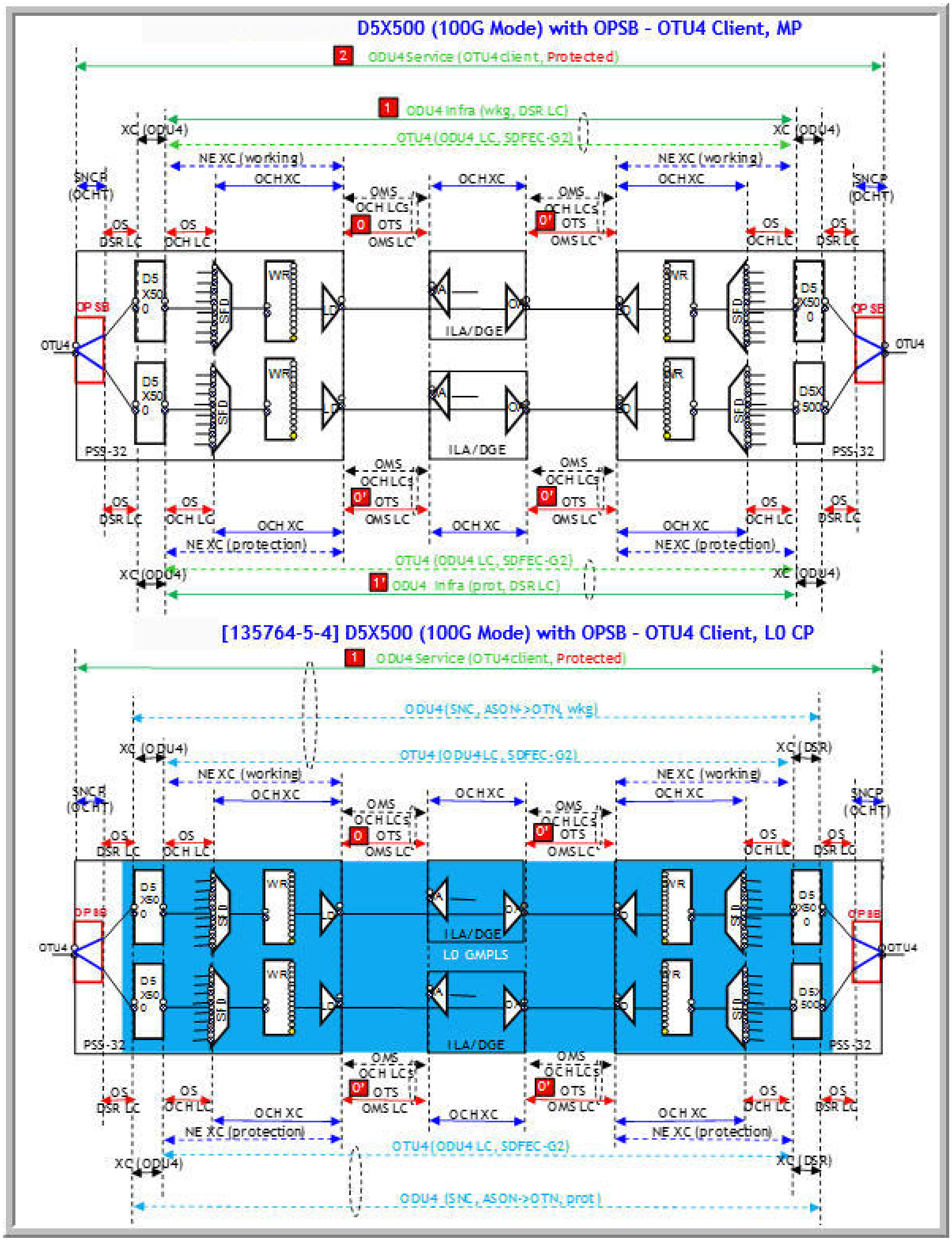


Figure 2-62 D5X500 (200G Mode) with OPSB – OTU4 Client, L0 Control Plane

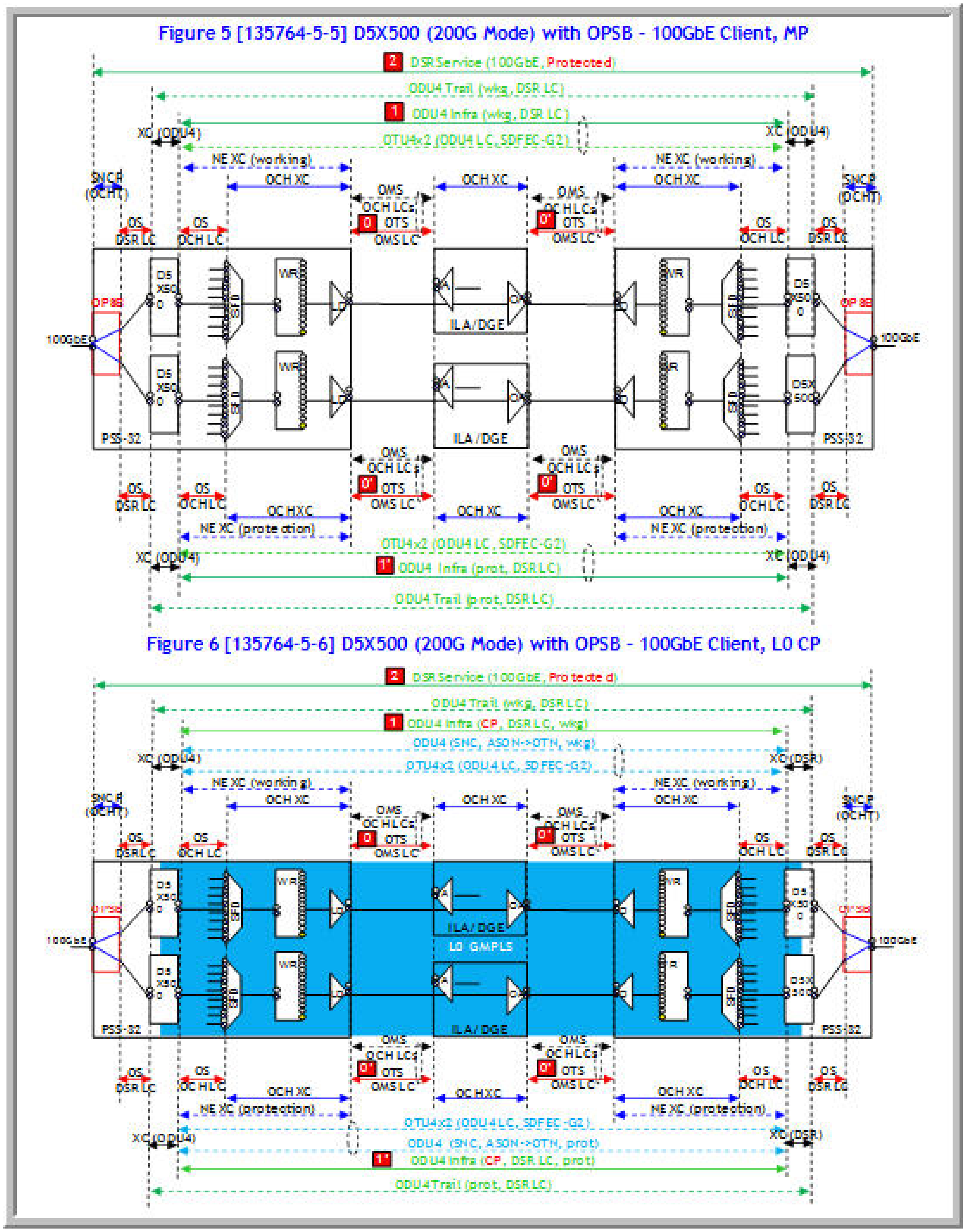
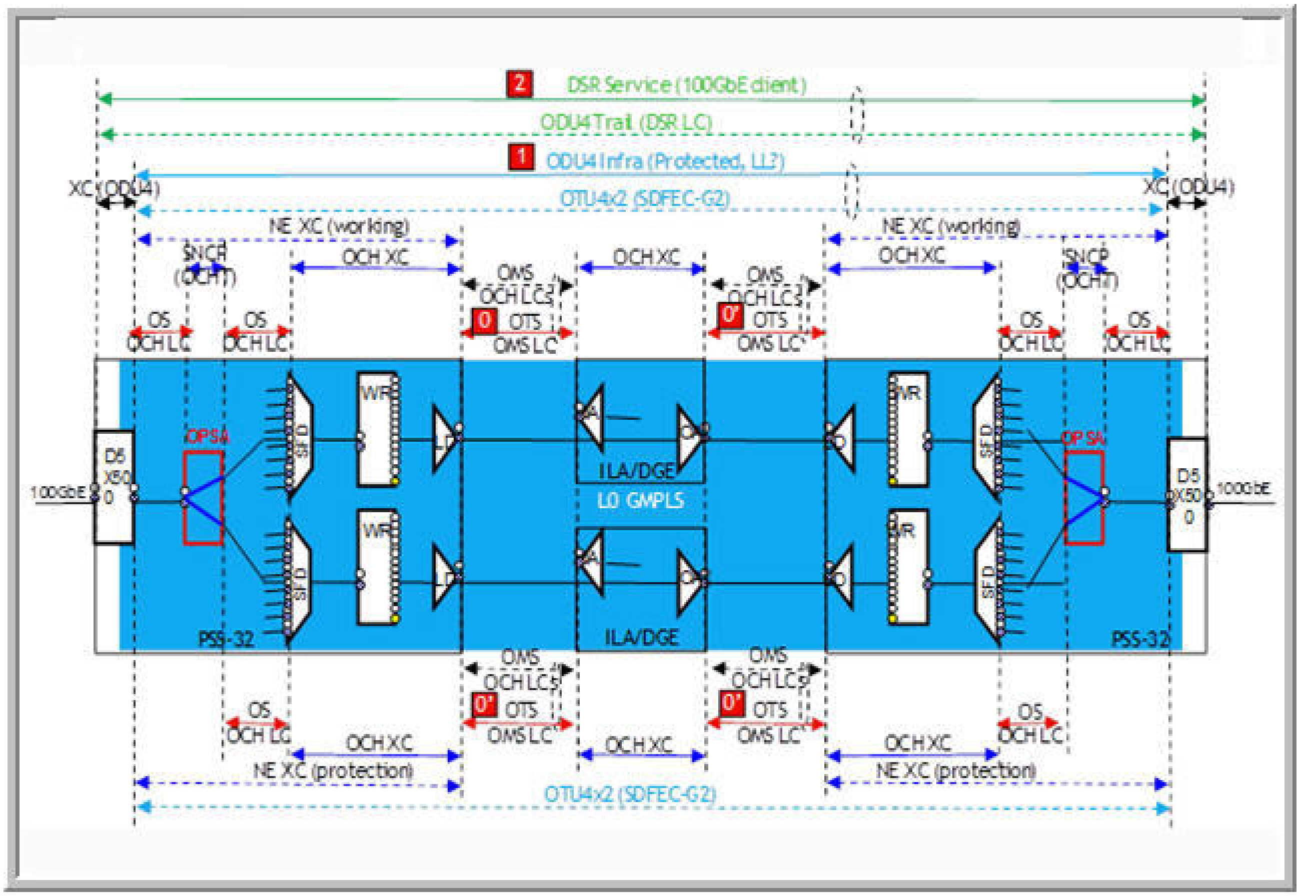


Figure 2-63 OPSA OCH Protection - 100 G Line L0 Control Plane



2.31 Provisioning connections for ADD4 cards

Overview

The OTSiG Tunnel is the object modeling the end-to-end infrastructure connectivity between transponders or uplinks. It is a multi-carrier object, embedding 3R points, when they are present along the route. The OTSig Tunnel groups the individual carriers (wavelengths), which are referred to “OTS-iG” objects.

OTSig Tunnel provisioning is a new provisioning with user input variable called **Optical Line Mode Profile**, which is an integer enum that identifies a specific set of universally defined configuration parameters.

The OTSig Tunnel takes the place of traditional ODUk (for example, ODU4) Infrastructure connection provisioning for the new ADD3 and ADD4 ASIC cards. When OTSig Tunnels are created, the OTSig trail is automatically created by the system (taking the place of the traditional OTUk connection) and can be seen on the server list for each OTSig Tunnel.

When OTSig Tunnel is created using DFM6, DFM6E, SFM6, 2UX500, S5AD400H or S6AD600H card the NFM-T system auto creates an OTSig Trail. If the OTUStruct assigned on the NE is OTUC4, then an ODUC4 trail is auto created by the system. Further you can create a 400GbE service over the OTSig Tunnel using the ODUFlex container.

NFM-T supports DB Delete and integrated OTSig Tunnel and OTSig Trail discovery for ADD4 cards.

The OTSig Tunnel is supported for both Managed Plane and Control Plane MRN tunnel. L1 Control Plane and L0 Control Plane are not supported. For Control Plane, only MRN Terminated Tunnel is supported.

Note: In NFM-T R20.11, Control Plane connections are not supported on cards DFM6 and DFM6E.

NFM-T supports Link Span parameter for OT to OT and FOADM configurations in ADD4 cards. Link Span parameter is for short-haul communications where the user has a setup without amplifiers and the line side receiver's optical power must be adjusted accordingly. Link Span parameter is applicable only for Managed Plane connections.

Note: EPT support is applicable with bulk upload only. Partial upload for Direct and FOADM configurations is not supported in R19.9.2 release.

NFM-T supports rerouting of OTSig tunnels for Managed Plane and Control Plane connections with ADD3 and ADD4 cards. After rerouting, NFM-T also allows the conversion of current route to nominal route for Control Plane connections.

OTSig Tunnel is supported for the following cards:

- DFC12, DFC12E, DFM6, DFM6E, SFM6 (1830 PSI-M),
- 2UX500 (1830 PSS 8x and 1830 PSS12x) and
- S6AD600H, S5AD400H , S4X400H, 8UC1T (1830 PSS PHN)

Note:
The port names are appended with `\WDM` for the following:

- **OPERATE > NPAs > 360° View > 3R**
- **OPERATE > NPAs > 360° View > LINKS**. Filter for *termTunnel* in the **Category** column.

For more information, see

- 2.8 “Determine the Infrastructure to be created” (p. 168)
- “Best Practices templates” (p. 669)
- “Optical line characteristics” (p. 706)
- 8.11 “Manage an OTSig Tunnel ” (p. 1314)
- “OTSiG tunnel” (p. 258)
- Step 5
- Table 2-10, “Layer Rate and corresponding Signal Type” (p. 286)

Layer Rate - Signal Type

Table 2-10 Layer Rate and corresponding Signal Type

Profile Type	Layer Rates	Signal Types
Digital	OTU1	OTU1
Digital	OTS	OTS
Digital	OTU2	OTU2 NA
Digital	OTU2E	OTU2E OTU2eETH OTU2EWANETH NA
Digital	OTU3	OTU3 NA
Digital	OTU3E2	NA
Digital	OTU4	OTU4 OTU4WANETH NA
Digital	ODU0	NA
Digital	ODU1	OTU1 NA
Digital	ODU2	OTU2 NA
Digital	ODU2E	OTU2E OTU2eETH NA

Table 2-10 Layer Rate and corresponding Signal Type (continued)

Profile Type	Layer Rates	Signal Types
Digital	ODU3	OTU3 NA
Digital	ODU3E2	NA
Digital	ODU4	OTU4 NA
Digital	ODU0TCM	NA
Digital	ODU1TCM	NA
Digital	ODU2TCM	NA
Digital	ODU2ETCM	NA
Digital	ODU3TCM	NA
Digital	ODU3E2TCM	NA
Digital	ODU4TCM	NA
Digital	OTU1F	OTU1F
Digital	ODU1F	ODU1F

Table 2-10 Layer Rate and corresponding Signal Type (continued)

Profile Type	Layer Rates	Signal Types
Digital	DSR	OC3 NA DVBASI FC100 FC200 FC400 FC800 FC1200 GBE400 GBE100 GBE40 GBE10 GBE1 FASTETH OC768 OC192 OC48 OC12 STM256 STM64 STM16 STM4 STM1 CBR2G5 SDSDI HDSDI SDR 40GBEMLD FC1600 GIGECONV TENGIGELANETH
Digital	ODU3E1TCM	NA
Digital	ODUFTCM	NA
Digital	OCH	OTU1 OTU2 OTU2E OTU3 OTU3E2 OTU4 OTU4x2 OTU4Half OTU4HalfX5 OTU1F

Table 2-10 Layer Rate and corresponding Signal Type (continued)

Profile Type	Layer Rates	Signal Types
Digital	OTU4x2	OTU4x2
Digital	OTU4Half	OTU4Half
Digital	OTU4HalfX5	OTU4HalfX5
Digital	OTU4_OCH	OTU4 NA
Digital	ODUFlex	FC400 FC800 FC1600 G3SDI18 IBSDR IBDDR IBQDR G3SDI19
Digital	OTUTC1	OTUTC1
Digital	OTUTC4	OTUTC4
Digital	ODUTC1	ODUTC1
Digital	ODUTC4	ODUTC4

Table 2-10 Layer Rate and corresponding Signal Type (continued)

Profile Type	Layer Rates	Signal Types
Analog	OS	OC3 NA OTU1 OTU2 OTU2E OTU3 OTU3E2 OTU4 OTU4x2 DVBASI FC100 FC200 FC400 FC800 FC1200 GBE100 GBE40 GBE10 GBE1 FASTETH OC768 OC192 OC48 OC12 STM256 STM64 STM16 STM4 STM1 CBR2G5 SDSDI HDSDI G3SDI3 DDR SDR OTU1F OTL4.4 40GBEMLD FC1600 CBR10G3 OTU4Half OTU4HalfX5 HUNDREDGIGELANETH OTU2eETH OTU2EWANETH OTU4WANETH TENGIGELANETH

Table 2-10 Layer Rate and corresponding Signal Type (continued)

Profile Type	Layer Rates	Signal Types
Analog	OTS	OTS
Analog	OCH	OCH
Both	OTS	OTS

OTSiG tunnel with protected connection

To configure an OTSiG tunnel consisting a mix of protected and unprotected segments (OMS +3R + OMSP), perform the following steps:

- Create the tunnel as protection enabled, with routing mode as either Auto or Manual.
- If there is more than one OMS link connecting two nodes include the unprotected OMS link as a constraint in both the service and protection leg. If the OMSP contains multiple links, then include any one link or leg as a constraint
- The constraint can be fully or partially applied, however all the unprotected OMS links must be included as a constraint

When re-routing an OTSiG tunnel consisting a mix of protected and unprotected segments (OMS +3R + OMSP), the unprotected links are displayed as only service, even though it was included as both service and protection during creation. Hence ensure the tunnel is protection enabled and manually re-add all the new and existing OMS links with constraint type as **Protection** along with the service.

To achieve a pass through between an OMSP protected span and unprotected span, use a 3R configuration or back to back configuration on the OMSP ending node.

20P200 and S4X400H or S4X400L cards interwork configuration

NFM-T supports interwork configuration for S4X400H or S4X400L and 20P200 cards on Lower Order (LO) service mapping of less than 100 GbE on the managed plane network. Backplane (BP) ports are used for LO provisioning on these cards.

When provisioning the Infrastructure connection, ensure to select **Rate** as `OTSig Tunnel`. From NFM-T R20.7 onwards, **Profiles** `16` and `17` are not supported for interwork configuration.

For more information on 20P200 and S4X400H or S4X400L cards interwork configuration, see *S4X400H and S4X400L* and *20P200* sections of *NE Management Guide*.

The table shows the S4X400H or S4X400L and 20P200 pack Backplance (BP) mating slot rules for mating support.

Table 2-11 S4X400H or S4X400L and 20P200 pack BP mating

1830 PSS8 Slot	2	3	4	5

Table 2-11 S4X400H or S4X400L and 20P200 pack BP mating (continued)

1830 PSS16II Slot	3	4	5	6
1830 PSS16II Slot	7	8	9	10
1	S4X400H or S4X400L	20P200	NA	NA
2	NA	NA	20P200	S4X400H or S4X400L
3	20P200	S4X400H or S4X400L	NA	NA
4	NA	NA	S4X400H or S4X400L	20P200

Perform the following steps for configuring 20P200 and S4X400H or S4X400L card to interwork:

1. Provision the S4X400H or S4X400L card and 20P200 card as per mating slots rules mentioned in the table.
2. Assign Backplane (BP) ports on S4X400H or S4X400L and 20P200 cards with OTL4.10 signal type.

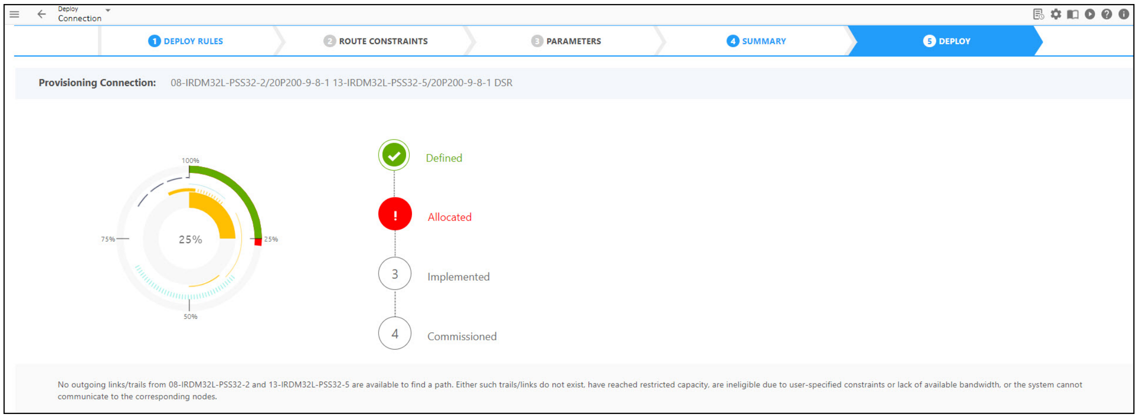
   BP port connections between S4X400H or S4X400L and 20P200 cards:

   - If BP1N1 (Backplane) port of S4X400H or S4X400L card is assigned with OTL4.10, ensure BP1 port of 20P200 card is assigned to OTL4.10 (that is, BP1N1 port of S4X400H or S4X400L card can only be paired with BP1 port of 20P200 card and not with BP2 port).
   - If BP2N1 port of S4X400H or S4X400L card assigned with OTL4.10, ensure BP2 port of 20P200 card is assigned to OTL4.10 (that is, BP2N1 port of S4X400H or S4X400L card can only be paired with BP2 port of 20P200 card and not with BP1 port).

   If any other combination of BP ports is selected between S4X400H or S4X400L and 20P200 cards such as BP1N1=OTL4.10 on S4X400H or S4X400L card and BP2=OTL4.10 on 20P200 card, service creation on 20P200 card fails with the following error message as shown in the figure, You must reassign the BP ports on both the cards appropriately.

   ```
   No outgoing links/trails from <From Node> and <To Node> are available
   to find a path. Either such trails/links do not exist, have reached
   restricted capacity, are ineligible due to user-specified constraints
   or lack of available bandwidth, or the system cannot communicate to
   ```

`the corresponding nodes.`



3. Create OTSig Tunnel from S4X400H or S4X400L to S4X400H or S4X400L line ports. For more information, see *Deploy a Template to Make a Connection* section.
4. Create a Service from 20P200 to 20P200 ports.

Functionalities not supported for ADD4

NFM-T does not support the following functionalities for ADD4 (cards equipped with ADD4 ASIC) Management:

- Delete with clients.
- For ADD4 cards, the NE does not support TCA correlation for FEC and Pre-FEC PM groups. Hence TCA correlation is disabled OTSi rate PM TPs on OTSig Tunnel and OTSi trail connections.
- Interworking between S4X400H and DFC12/DFC12E is supported.
- Modify Parameters of OTSig Tunnel and OTSig trail. Any modification of Tx parameters for OTU4 and OTUC4 layer from the OTSig tunnel, will not be reflected in the **Equipment Manager** page.
- Modify PM OTSig trail.
- For ADD4 cards, only MRN Terminated is supported. L1 and L0 Control Plane is not supported.
- 3R recoloring is not supported for DFC12 and DFC12E cards.

2.32 Auto Payload

Auto Payload definition

Auto Payload is a NFM-T OTN provisioning feature that enables an HO-ODUk infrastructure trail, along with a LO-ODUk infrastructure trail, to be provisioned in a single step when users provision a DSR service.

Auto Payload functional description

When users provision DSR services, the system automatically creates all point-to-point HO-ODUk trails along with any accompanying LO-ODUk trails. However, for any HO-ODUk trails that involve pass-through HO cross connections or protected HO-ODUk trails, users must provision these connections in separate steps.

Auto Payload routing mode considerations

The Auto Payload feature supports the provisioning of DSR services and LO-ODUk infrastructure connections in the **Automatic** and **Manual** routing modes.

When users specify the **Automatic** routing mode during the creation of a DSR service or a LO-ODUk infrastructure connection (trail), the system automatically determines the route of the connection. When the LO-ODUk infrastructure trails are implemented, the system creates the HO-ODUk infrastructure trails and makes the appropriate cross connections to the NEs.

During the provisioning of LO-ODUk infrastructure trails in the **Manual** routing mode, users can select the LO-ODUk link connections from the HO-ODUk trails as well as the appropriate OTUk trails. When users select the OTUk trails, the system uses those link connections to create the HO-ODUk trails and it makes the appropriate cross connections to the NEs during implementation of the LO-ODUk.

Auto Payload supported configurations

The Auto Payload feature relies on the system's automatic creation of *virtual servers*, which are ODU2 pool ports on the 1830 PSS OCS NEs that are used for internal routing. Virtual servers are not visible to our users; the system uses the virtual servers internally for routing.

The system creates a virtual server at the HO-ODUk layer during the following events:

- When a logical link is created with an endpoint on a 2UC400 I/O port on an 1830 PSS PHN NE.
- When a logical link is created with an endpoint on a 4UC400 I/O port on an 1830 PSS PHN NE.
- When a logical link is created between two 1UD200 I/O ports of two photonic NEs.
- When a logical link is created between two 1830 PSS OCS I/O ports that have a photonic core in the middle.
- When a logical link is created between two 1830 PSS OCS uplink ports that have a photonic core in the middle.
- When an OTUk infrastructure connection is created between two 1830 PSS OCS I/O ports in an electric switch.
- When an OTUk infrastructure connection is created between an 1830 PSS OCS NE and an 11DPM12 circuit pack in an edge switch such as the 1830 PSS-4.

- When an OTUk infrastructure connection is created between two 1830 PSS OCS NE and a black box.

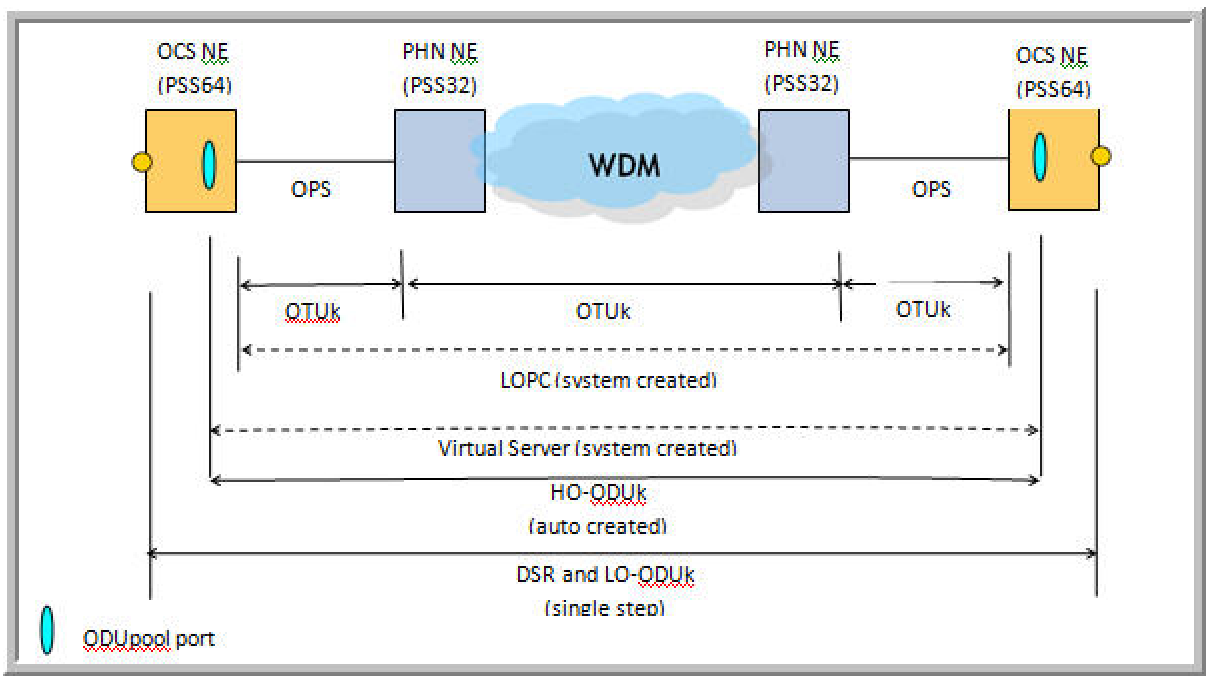
When an HO-ODUk infrastructure connection is automatically created, the system enables alarm monitoring, along with ingress and egress NIM, on the connection endpoints. The endpoints of virtual servers on the 1830 PSS OCS NEs are the ODU2 pool ports.

When an HO-ODUk infrastructure connection is automatically created using a logical link between two 1UD200 I/O ports, the system enables alarm monitoring for OS PTPs on 1UD200 BP ports, ODU4 CTPs on 1UD200 line ports, OS PTPs on 20P200 BP ports, and ODU4 FTP on 20P200 BP ports. In addition, the system enables ingress NIM and egress NIM for ODU4 CTPs on 1UD200 line ports.

Auto Payload configuration examples

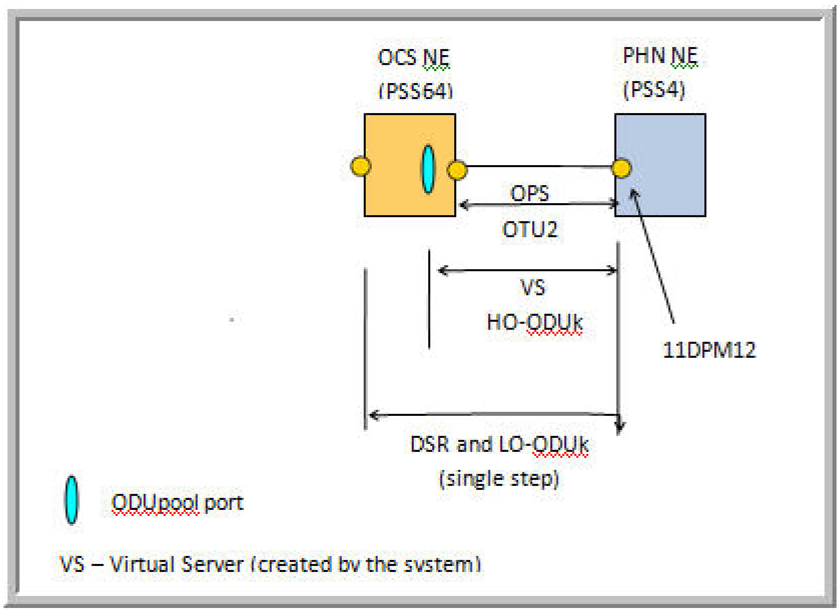
The **first configuration example** consists of two 1830 PSS-64 OCS NEs that pass through a photonic core of 1830 PSS-32 NEs. In a single step, users create a DSR and LO-ODUk connection that connects the two 1830 PSS-64 OCS NEs. The system automatically creates the HO-ODUk infrastructure connection (trail) and virtual servers on the 1830 PSS-64 OCS NEs, the endpoints of which are ODUPOOL ports. The remaining L-OPC and OTUk connections are then automatically created among the 1830 PSS-64 OCS and 1830 PSS-32 NEs.

Figure 2-64 NFM-T NFM-T OTN Provisioning – DSR Service Creation between Two 1830 PSS-64 OCS NEs Passing Through a 1830 PSS Photonic Core



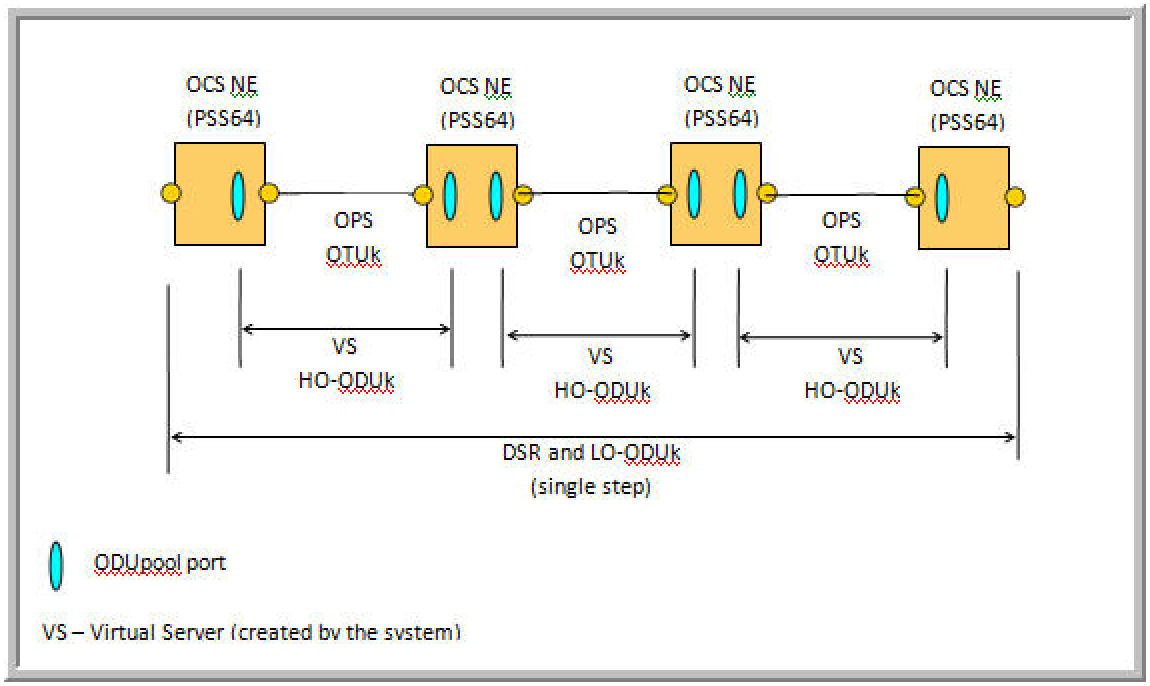
The **second configuration example** consists of an 1830 PSS-64 OCS NE asymmetrically connected to an 1830 PSS-4 Photonic NE that is configured with an 11DPM12 pack. In a single step, users create a DSR and LO-ODUk connection that connects the OCS and photonic NEs. The system automatically creates the HO-ODUk infrastructure connection (trail) and a virtual server on the 1830 PSS-64 OCS NE, the endpoint of which is an ODUPOOL port. The remaining OTUk connection is then automatically created between the 1830 PSS-64 OCS and 1830 PSS-4 Photonic NE.

Figure 2-65 NFM-T NFM-T OTN Provisioning – DSR Service Creation between One 1830 PSS-64 OCS NE and One 1830 PSS-4 Photonic NE



The **third configuration example** consists of the connection of four 1830 PSS-64 OCS NEs. In a single step, users create a DSR and LO-ODUk connection that connects the four 1830 PSS-64 OCS NEs. The system automatically creates the HO-ODUk infrastructure connections (trails) and virtual servers on the 1830 PSS OCS NEs, the endpoints of which are ODUPOOL ports. The remaining OTUk connections are then automatically created among the four 1830 PSS OCS NEs.

Figure 2-66 NFM-T NFM-T OTN Provisioning – DSR Service Creation between Four 1830 PSS-64 OCS NEs



Auto Payload and delete or DB delete

Whenever users delete or DB delete HO-ODUk infrastructure connections (trails) that use the link connection of an L-OPC or link connections from an OTUk trail that is between two 1830 PSS OCS NEs, the system recreates the ODUPOOL ports that are between the two end 1830 PSS OCS NEs or are on the L-OPC.

When users delete or DB delete DSR services, the system automatically deletes the corresponding LO-ODUk infrastructure connection (trail). The system also deletes the HO-ODUk if the LO-ODUk is the only client of the HO-ODUk infrastructure connection (trail).

2.33 Auto creation of edge connections

Auto creation of edge HO ODUk connections

When users create an asymmetric service connection with one endpoint on a black box and the other endpoint on a managed NE, the system automatically creates an edge HO ODUk connection between the black box and the adjacent managed NE when the connection is required. The edge HO ODUk server connection is created as part of the service connection order.

Example:

If one connection endpoint is a 10GbE client port on a 10X10ANYG card and the second endpoint is a black box connected to an OTU4 port on a 1XAN100G card, an HO ODU4 connection must exist or must be created between the black box and the OTU4 port.

Auto creation of edge HO trail connections

If users create a DSR or LO-ODUj connection and if the connection is the first connection using a channelized endpoint, the system automatically creates an edge HO infrastructure trail connection. If the DSR or LO-ODUj connection has multiple channelized endpoints, the system automatically creates an edge HO infrastructure trail connection for each channelized endpoint.

The system automatically provisions these edge HO trail connections for DSR or LO-ODUj connections that are created using automatic, trail based, and link connection based routing. In addition, the system automatically provisions these edge HO trail connections regardless if users select **Auto Server Creation**.

After users submit the DSR/LO-ODUj connection request, the system determines if one or more edge HO trail connections need to be created:

- If one or more edge HO trails need to be created, the system creates an order for each edge HO trail connection.
- If an edge HO trail connection exists without an associated order, the system create an order for the edge HO trail connection.
- If an edge HO trail connection order exists and the order is not in **Commissioned** state, the system moves the order to **Commissioned**.

In each instance, the system creates an order for each connection and all orders transition through the order steps in tandem. If any order fails, the group state for the connections is **Failed**. If the auto-creation of the edge HO trails connection is successful, the system names the connection (*ENNI:[PTP Name]:[rate]<num>*) and the system generate link connections.

For the automatically created edge HO trail, the following applies:

- The connection is **Created by** the **System**.
- The connection category is **Edge HO Trail** if the connection is in the Managed Plane.
- The connection category is **ASON Edge HO Trail** if the connection is in the Control Plane.
- The port parameters for the connection endpoints have alarm monitoring set to **On**; ingress and egress NIM **Enabled**; and the LO ODU structure set.
- All other transmission parameters are not set. Users can change any required transmission parameters through **Modify Parameters**.

- The port type of the edge PTP port is changed to **eNN** and is removed from the **Free Port** list.
- The timeslot map for the TTP on the ODUPOOL displays whether the timeslot is available or assigned. When assigned, the timeslot displays the connection name using the timeslot or if it is used by an uncorrelated cross connection.

2.34 Unterminated OTUk/ODUk infrastructures without virtual termination management

Terminated/Unterminated and channelized/unchannelized connections

In a Multi-Regional Network, (MRN), connections can be labeled as *forward adjacency-terminated* (*FA_TERM*) and *forward adjacency-unterminated* (*UNTERM*).

A *terminated connection* is a connection that occurs when a particular layer comes to a logical end and a client (technology) layer payload is mapped or several clients of the same layer are multiplexed, and overhead bytes are inserted or removed. A terminated connection can be asymmetric; meaning, one end of the connection can be terminated and the other end can be unterminated.

An *unterminated connection* is a connection that occurs when a transmission frame passes through a particular connection endpoint (TP) and overhead is not inserted or not removed. The management system does not have any knowledge of the internal payload structure. Both logical links and ODUk paths are unterminated.

A *channelized connection* occurs when, at the edge of the network, the hand-off port is unterminated at a layer higher (lower bit rate) than the hand-off layer. The hand-off layer is then referred to as *channelized* because it multiplexes several unterminated lower order connections and leaves the managed domain as a singular entity.

For a channelized endpoint, an HO-ODU cross connection is required between the ODUk CTP of the edge port and a TTP on the ODUPOOL. The route of the *edge HO trail* consists of the HO ODU cross connection. The edge HO trail has x number of link connections at the ODUj rate.

An *unchannelized connection* is a connection that is unterminated on one end and is carrying an invisible payload (no multiplexing, only one-to-one mapping). When a connection is unchannalized on both ends, it is typically referred to as a *path*.

Control Plane connections can be terminated or unterminated:

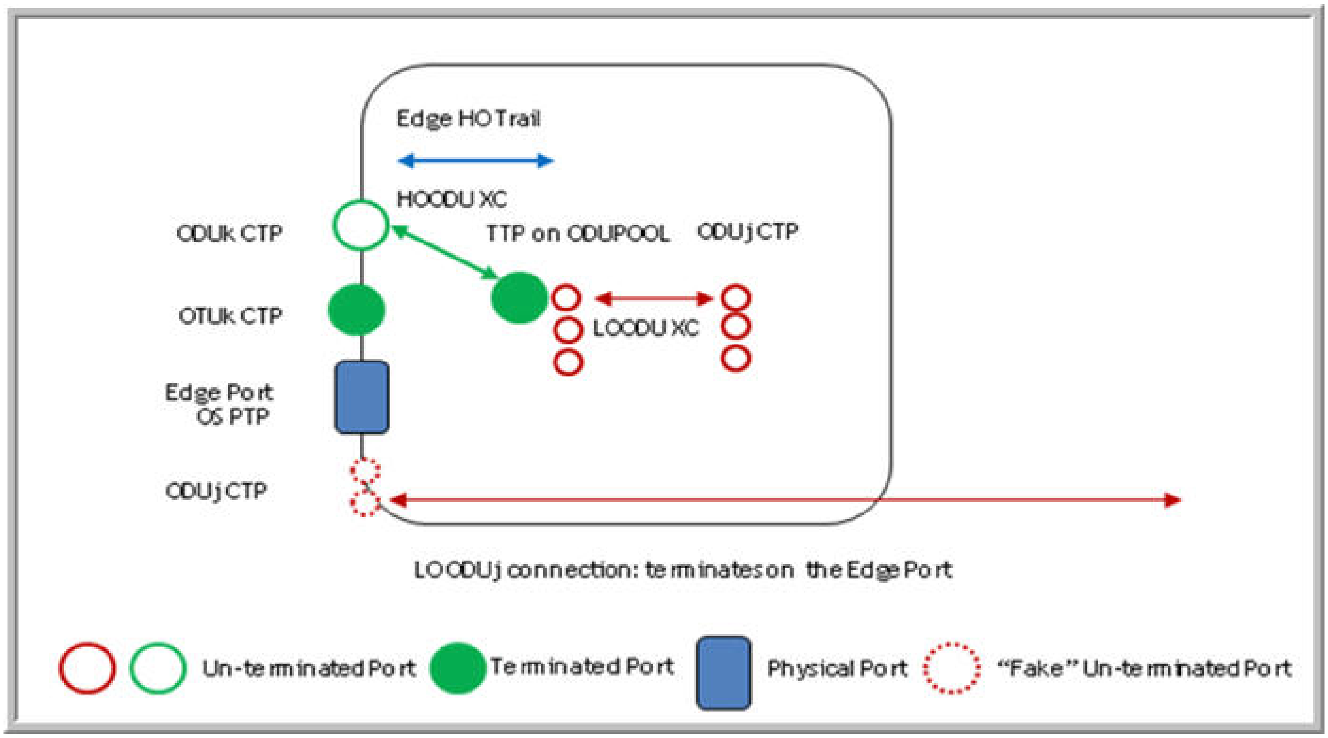
- The terminated ASON connections are those that are terminated on a UNI port.
- The unterminated ASON connections are those that have the endpoints on an NNI port.

Managed Plane connections can be terminated, unterminated, or channelized:

- The terminated connections are one-to-one with the client and server and terminated on UNI port.
- The unterminated connections have endpoints on an NNI port and are one-to-one with the client and server.
- The channelized connections are those in which the server rates are higher than the client rate (such as a ODU2 client riding on a OUT4/ODU4 on a 260SCX2 port).

The following figure illustrates connections for channelized and/or unterminated endpoints.

Figure 2-67 NFM-T NFM-T OTN Provisioning – Connections for Channelized or Unterminated Endpoints



Unterminated OTUk/ODUk infrastructures without virtual termination

To support both terminated and unterminated connections, the NFM-T OTN manages unterminated ODUk connections in the Managed Plane, Control Plane, and Mixed Plane environments without having to create an external topological link and an edge NE (ENE). Users can continue to create unterminated ODUk connections using topological links and ENEs; and, within the network, users can create unterminated connections that do not use topological links and endpoint NEs (ENEs) along with other unterminated connections that use topological links and ENEs.

Asymmetric connections, in which one connection endpoint is a transponder/muxponder/ switchponder and the other connection endpoint is an MVAC/SVAC, are not supported.

Supported connection types

The following connection types are supported:

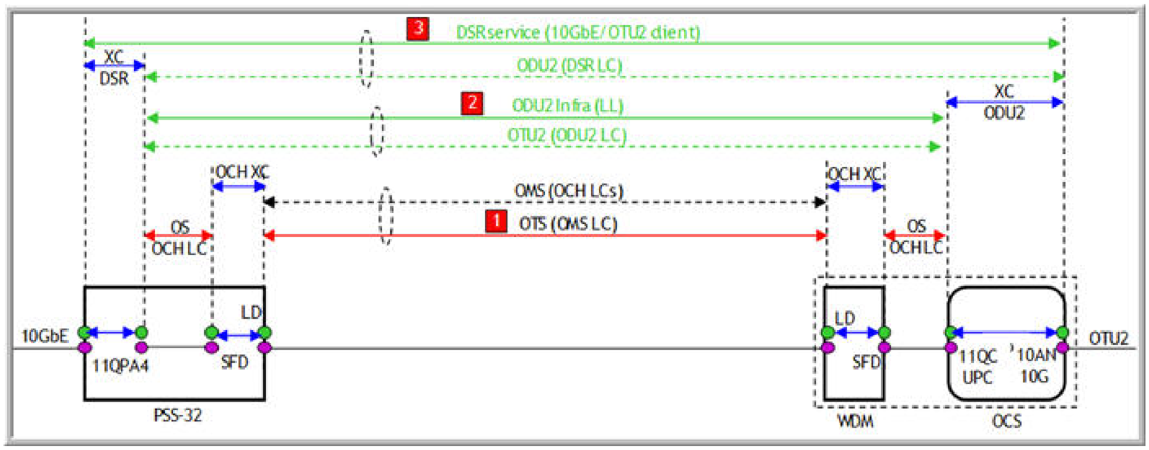
- Channelized and unchannelized ODUk service connections are supported.
- Channelized connections with one or more endpoints on an ENE are supported.
- Configurations that require three-ended HO-ODU cross connections and subsequent three-ended edge HO trails are supported.

- Both HO-ODUk and LO-ODU (at the point where each exists the network) connections are supported.
- Connections in which all connection endpoints have the same signal type (symmetric) and connections in which the endpoints have different, but compatible, signal types (asymmetric) are supported.
- DSR service connections in which the DSR LO-ODU connections are created in a single step using Auto Server Creation are supported.
- DSR connections are supported in which one connection endpoint is an NNI port, the other connection endpoint is a UNI port, and the rate of the NNI port is equivalent to the container rate of the UNI port is asymmetric and is not channelized at either connection endpoint.

  Example:

  One connection endpoint is an OTU2 port and the second endpoint is a 10GbE port and the connection rate is a 10GbE DSR.

  Example – Asymmetric DSR Connection Not Channelized at Either End



- An ODUk service connection in which the connection endpoints are all at the same rate, but the rate of the ports is greater than the rate of the connection is symmetric and channelized at both connection endpoints.

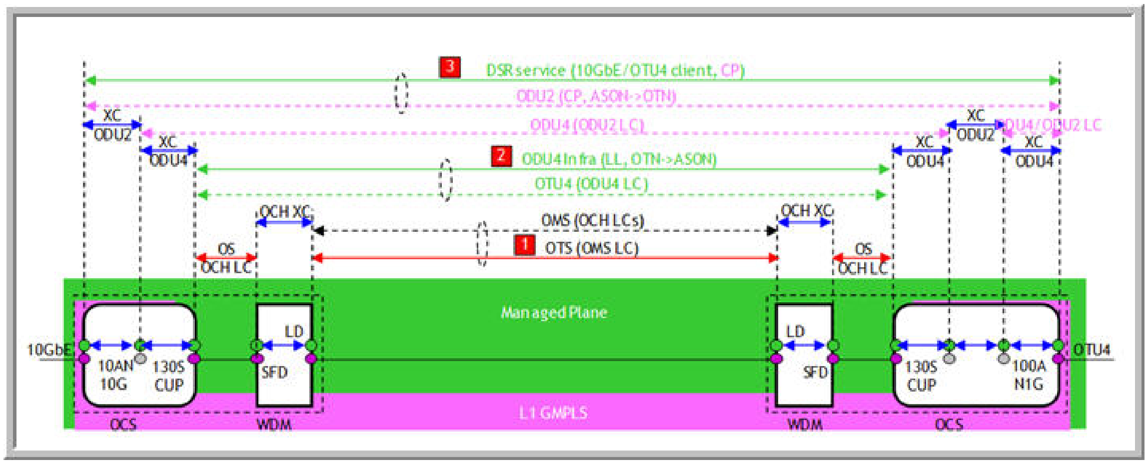
  Example:

  The endpoints are OTU4 ports; but, the connection rate is ODU2.
- A connection in which the connection endpoints are at different rates and the rate of at least one port is greater than the rate of the connection is asymmetric and channelized at one or both connection endpoints.
- A DSR connection that is asymmetric and channelized at one of the connection endpoints.

  Example:

  One connection endpoint is an OTU4 port; the second endpoint is a 10GbE port; and the connection rate is 10GbE DSR.

Example – Asymmetric DSR Connection Channelized at One End – L1 Control Plane



- An ODUk service connection can be asymmetric and channelized at one or both connection endpoints.

  Examples:

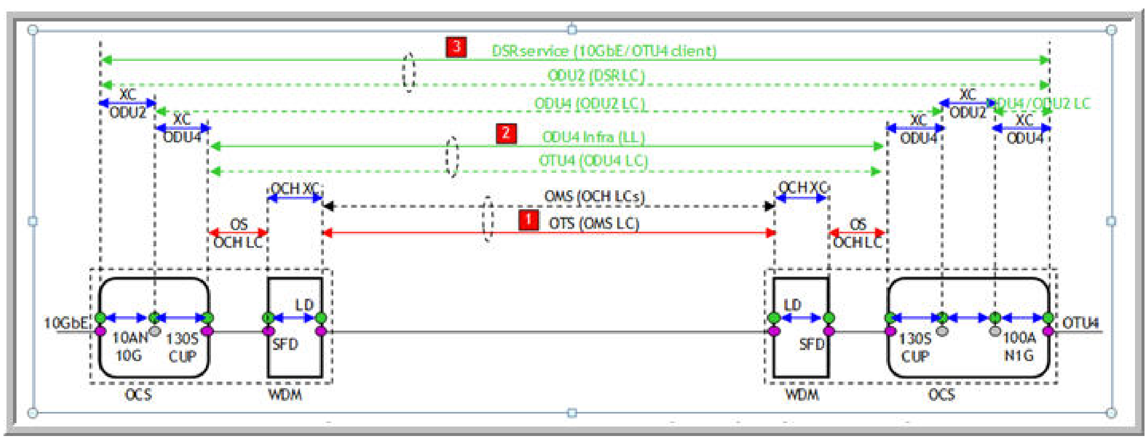
  A channelized connection at one endpoint is one in which one connection endpoint is an OTU4 port, the second endpoint is an OTU2 port, and the connection rate is ODU2.

  A channelized connection at both endpoints is one in which one connection endpoint is an OTU4 port, the second endpoint is an OTU3 port, and the connection rate is ODU2.

- Channelized configurations where the aggregation is at the end node of the connection are supported with two step provisioning. In the first step, the user creates the HO ODU logical link and OTUk connection. In the second step, the user creates the service connection and LO ODUj connection.

  The following figure illustrates an asymmetric DSR connection that is channelized at one end.

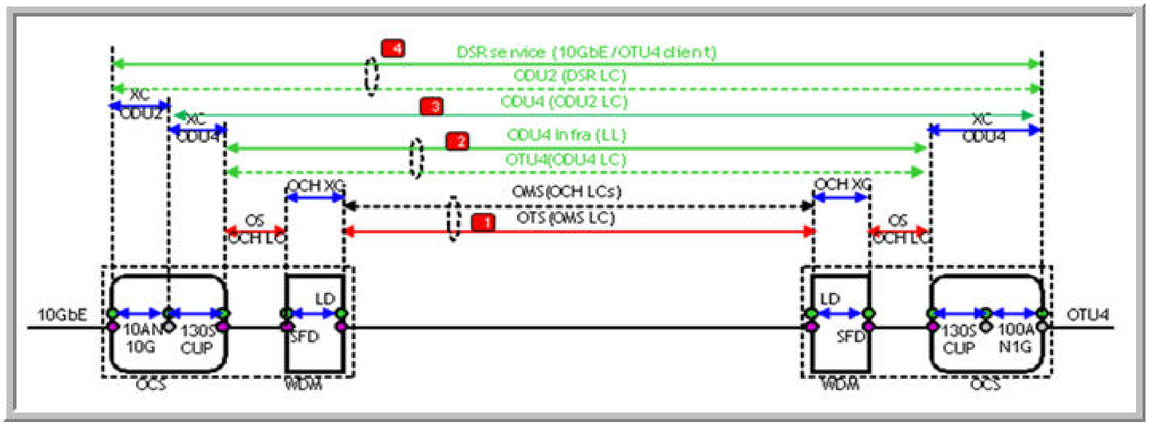
  Example – Asymmetric DSR Connection Channelized at One End



- A service connection where an endpoint is channelized and the aggregation of the connection is in the non-managed portion of the network supported; however, users must complete an additional step when creating the service connection.

For this configuration, a single HO ODU cross connection is on a node that contains a channelized endpoint. To create this type of service connection, users must first create the OTS connection(s), and then create the HO ODU logical link. Next, for the additional step, users must create the HO ODU trail. One endpoint is on an ODUPTF on the ODUPOOL (the left hand node in the following figure) and the other endpoint is the edge port. Lastly, users must create DSR/ODUj connection.

Example – Asymmetric DSR Connection Channelized Multi Hop at Edge



Channelized ports

For HO ODU service connections, connection termination points (CTPs) on ports (including black box ports) with a **Signal Type** of OTUK are supported on 1830 PSS OCS I/O cards and uplink cards.

Channelized LO ODU CPTs on unassigned and assigned ports are supported on 1830 PSS OCS I/O cards and uplink cards. Channelized LO ODU CTPs on black boxes are also supported.

2.35 Auto Discovery support

Introduction

The OTN is able to discover all connections based on notifications from the network element.

Currently, when a topological link is created on the network element and a notification is received, the OTN create an internal OS connection and attempts to discover all client connections.

When a notification of a cross connection creation is received no discovery is attempted.

In this scenario, if there are some discrepancies between the two mode, the user is notified of the inconsistencies in order to make the necessary modifications.

It is possible, via some changes to the usual connection method, to operate the network making the network element always the main for both element and network layers.

In this mode, changes in the network element are reflected in the network layer so if the user creates, modifies or deletes a connection in the network, these actions are reflected in the management system.

The scope of this feature, is mainly to address connection discovery from the network.

Any cross connect changes on the network element will be reported to or discovered by the NFM-T and the network layer connection is stitched end to end by the OTN.

The network becomes essentially the database and the management system needs to align to the network view.

Network connection discovery

The network connection discovery can be carried out according to two case scenarios:

- **Scenario 1**: Manual or automatic synchronization
- **Scenario 2**: Network triggers notifications

Manual or automatic synchronization

This scenario considers that network is already managed by the NFM-T.

The deployed network and the NFM-T database may drift out of alignment due to communication problems, lost events or notifications or any other reason.

This scenario, considers the operations to align the NFM-T database with the network assuming the network is the main.

The NFM-T user can either use the NFM-T GUI to trigger the synchronization of the network entities or can set up a scheduled task to perform the synchronization manually.

The preconditions are:

- The network is available and recognized in the NFM-T database.
- The alignment issues, also known as inconsistencies, are identified by the user.
- Events loss are identified by the system.

The synchronization rediscovers the network entities and compares them to the NFM-T database.

This comparison allows to identify discrepancies and proceed to update the database.

The update can be manual or not depending on network operation mode.

Network triggers notifications

This scenario considers that the network is already managed by the NFM-T.

Changes are made to this network directly by the operator.

Any modification in the network that is different from the NFM-T database will be handled based on network operation mode.

The NFM-T database may be automatically updated or user notified about inconsistencies based on operation mode.

The preconditions are:

- The network is available and recognized in the NFM-T database.
- Communication available between the NFM-T and network.
- Notification received from the network to be handled.

This scenario considers only the cross connect notifications.

The handling depends on the network operation mode.

The NFM-T database is updated and inconsistencies notified to user.

STMM10 cards

For discovery of services involving STMM10 card with time slot spanning multiple ODU1 group, the user has to provision all the ODU1 trails under the ODU2, then run a path synchronization to discover services that are crossing more than one ODU1 timeslot group.

PSI-2T

For PSI-2T NEs (R2.0 and R4.0) in cluster configurations involving 3R connections, external link discovery needs to be triggered on the PHN NE, not on the PSI-2T NE.

If external link discovery is triggered on the PSI-2T NE, then users need to complete the following recovery procedure:

1. If there are OTUk connections, then perform **Delete Connection and Clients from NFM-T** from the OTUk connection client of the OPS.

   Note: If the OTUk connections are not yet commissioned, then you need to cancel them.
2. Perform **Delete from NFM-T** for the OPS.
3. Perform **Discover External Physical Links** on the PHN NE that is connected to the PSI-2T NE.
4. Perform **Path Sync** on the PSI-2T NE to discover clients.

2.36 Regeneration

DWDM - DWDM regeneration

The NFM-T OTN supports connections with DWDM - DWDM regeneration via back-to-back OTs and connections with DWDM - DWDM regeneration via a single dual port pluggable OT.

In DWDM - DWDM regeneration via a single dual-port pluggable OT, the OT performs single channel OEO regeneration to translate the DWDM signal to an electrical signal and the electrical signal to a DWDM signal.

In DWDM-DWDM regeneration via back-to-back OTs, the pair of OTs performs single channel OEO regeneration where the first OT translates the DWDM signal to an electrical signal and the second OT translates the electrical signal to a DWDM signal.

Both types of DWDM-DWDM regeneration require two or more OTUk infrastructure connections for a single DSR/ODUk service connection. Separate OTUk connections are required for each DWDM portion of the connection. An OTUk connection must be terminated whenever the optical signal is translated to an electrical signal at a circuit pack or pair of circuit packs performing OEO regeneration.

The DWDM OTUk connections may be keyed or unkeyed. The OTUk connections composing the DSR/ODUk service connection do not have to have the same value of keyed or unkeyed.

DWDM -DWDM regeneration via back-to-back OTs also requires an internal link between the back-to-back OTs.

CWDM - DWDM regeneration using a Single OT

The NFM-T OTN supports connections with CWDM - DWDM regeneration using a single OT. The OT performs the single channel OEO regeneration to translate the CWDM signal to an electrical signal and the electrical signal to a DWDM signal. Connections where the CWDM portion of the connection is a dual fiber or single fiber are supported.

When a connection has CWDM - DWDM regeneration, multiple OTUk infrastructure connections are required for a single DSR/ODUk service connection. Separate OTUk connections are required for each CWDM and DWDM portion of the connection. An OTUk connection is terminated whenever the optical signal is translated to an electrical signal at a circuit pack performing the OEO regeneration.

If a connection performs CWDM - DWDM regeneration, two OTUk connections are required. If a connection performs DWDM-CWDM-DWDM or CWDM-DWDM-CWDM regeneration, three OTUk connections are required.

Each OTUk connection carries a single frequency, or a pair of transmit and receive frequencies for the Single Fiber CWDM case. CWDM and DWDM connections support different frequency ranges and the frequency of the connection must change during the CWDM-DWDM or DWDM-CWDM regeneration.

The table below summarizes the connection shapes that are required for the DWDM and CWDM connections.

Table 2-12 Connection Shapes Required for DWDM and CWDM Connections

Connection	Connection Shape
DWDM OTUk	**2 Ended Bi (I)**
Single Fiber CWDM OTUk	2 **Ended Split Bi (I)**
Dual Fiber CWDM OTUk	**2 Ended Bi (I)**

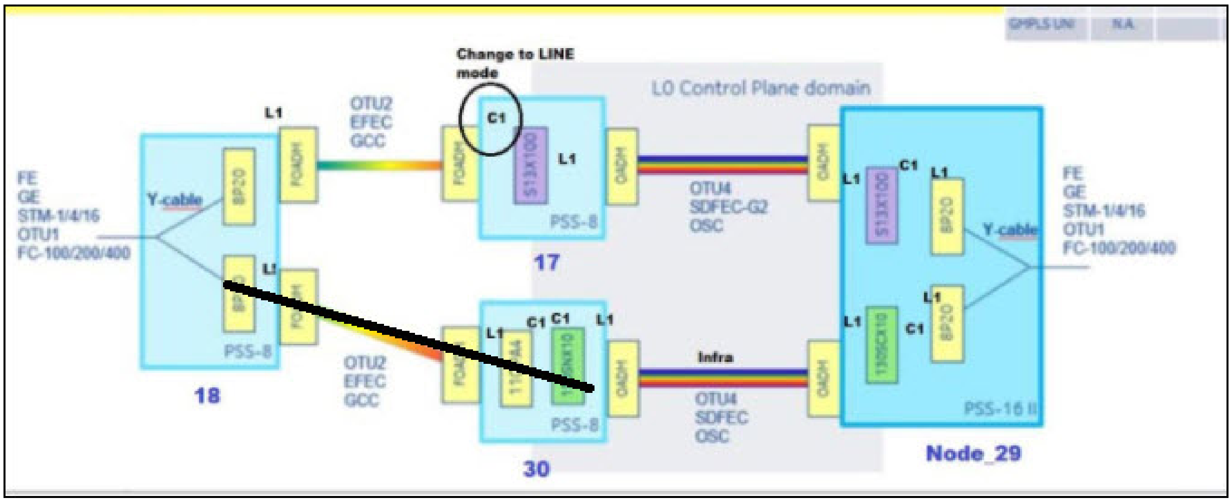
The DWDM OTUk connections can be keyed or Unkeyed. The CWDM connections must be Unkeyed. All OTUk connections composing the DSR/ODUk service connection need not have the same value of keyed or Unkeyed.

2.37 Auto-discovery of LOPC

Auto-discovery of LOPC between line ports

Create logical links and then create client-to-client interconnection between the fixed connecitvity cards, to avoid unwanted auto-discovery of connections. For example, create logical links between the two line ports. Because of fixed connectivity client assignment, the cross connections are created. Then the logical link is discovered between the line (L1 to L1) ports.

Figure 2-68 Logical Links between two line ports

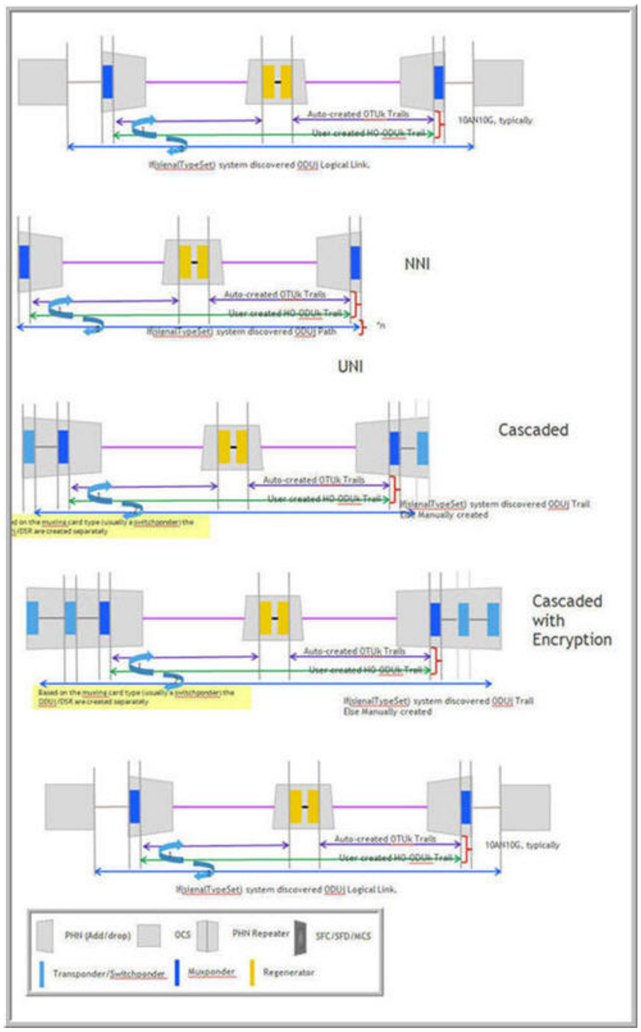


Common NFM-T OTN Network Configurations

2.38 Transponder configurations

Typical UNI and NNI transponder configurations

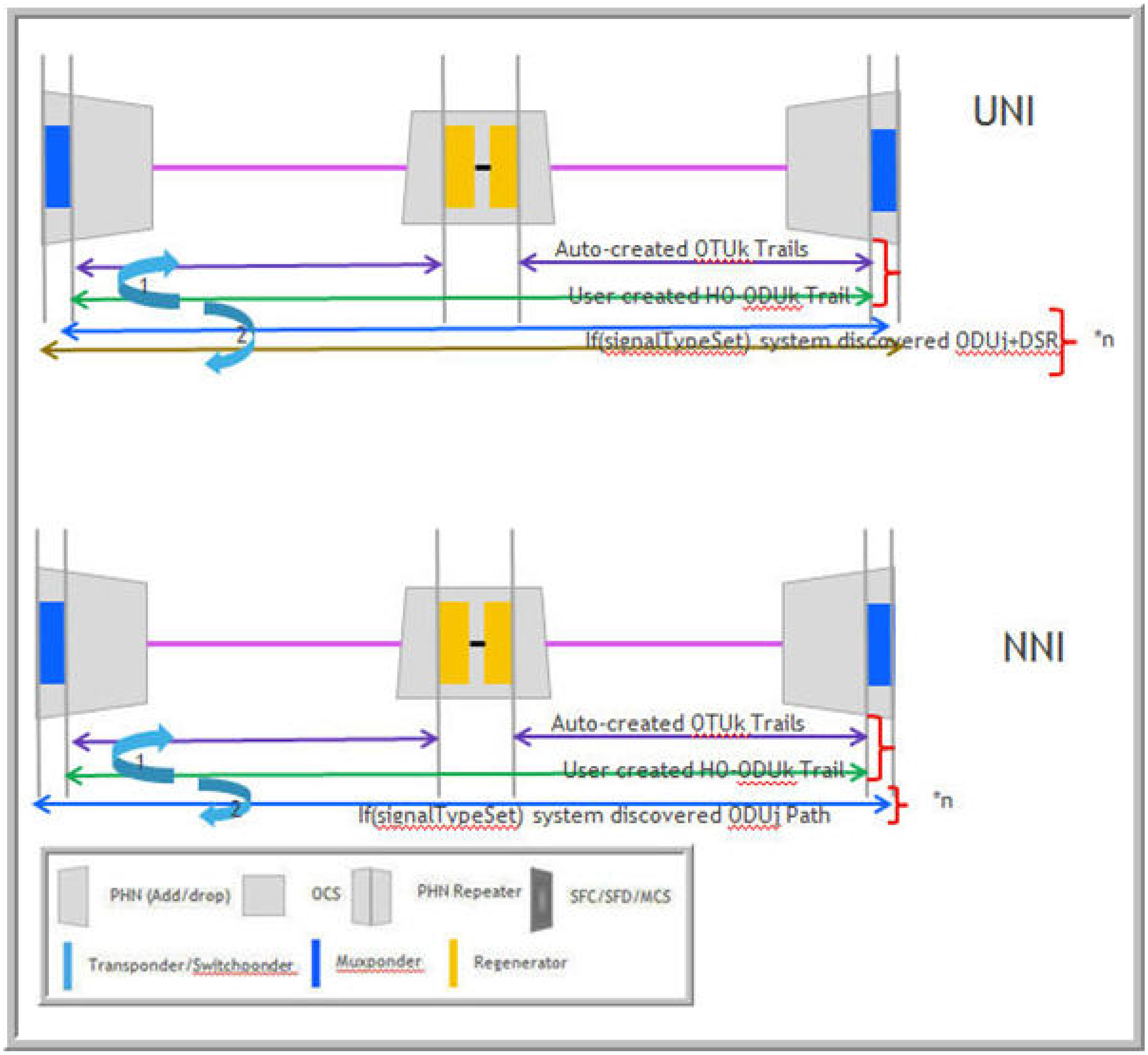
Figure 2-69 NFM-T OTN Network Provisioning – UNI and NNI Transponder Configurations



2.39 Muxponder UNI/NNI configurations

Typical muxponder UNI/NNI configurations

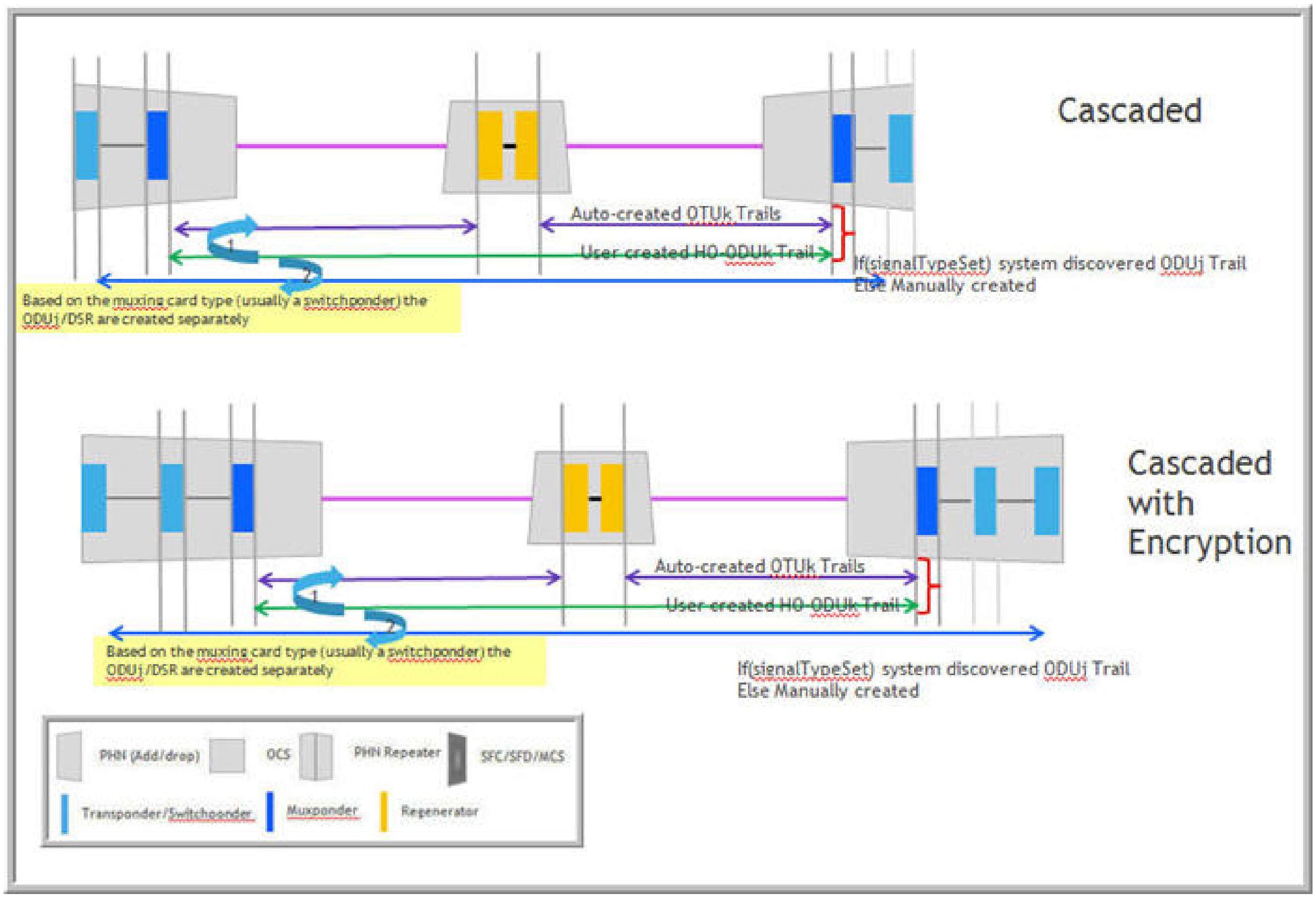
Figure 2-70 NFM-T OTN Network Provisioning – Muxponder UNI/NNI Configurations



2.40 Muxponder/Switchponder cascaded configurations

Typical Muxponder/Switchponder cascaded configurations

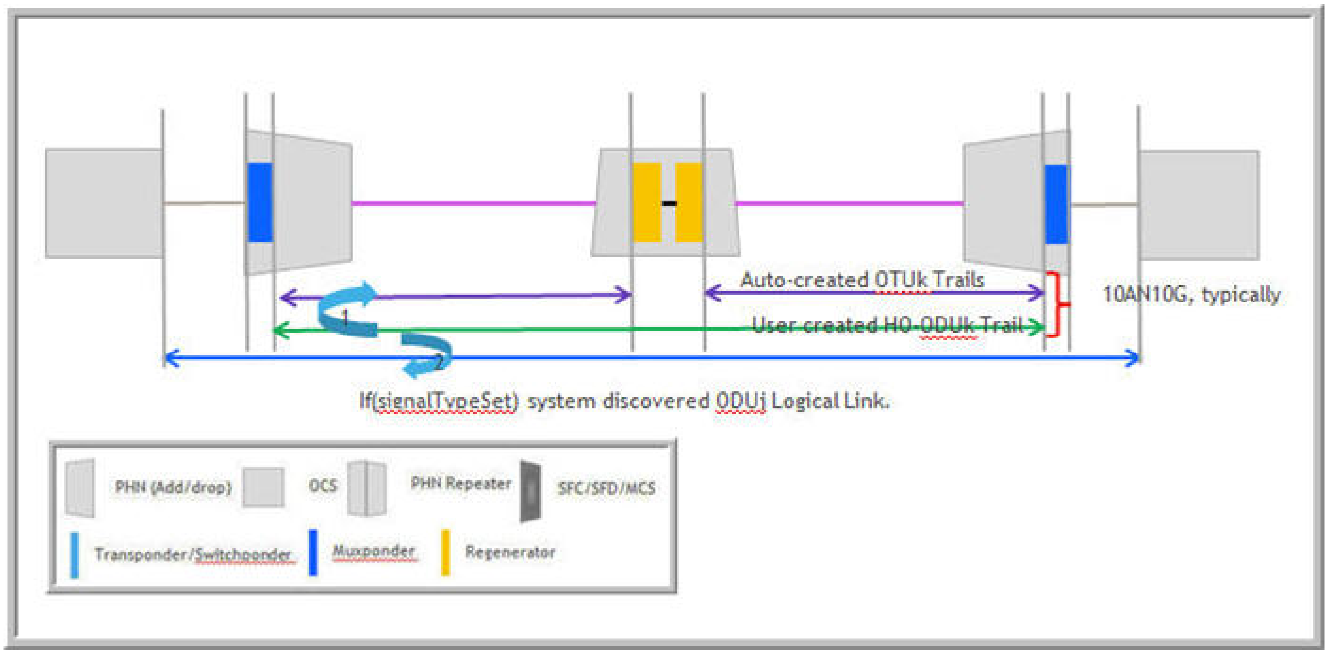
Figure 2-71 NFM-T OTN Network Provisioning – Muxponder/Switchponder Cascaded Configurations



2.41 Muxponder extended to OCS configuration

Typical muxponder extended to OCS (10XANY10G) configuration

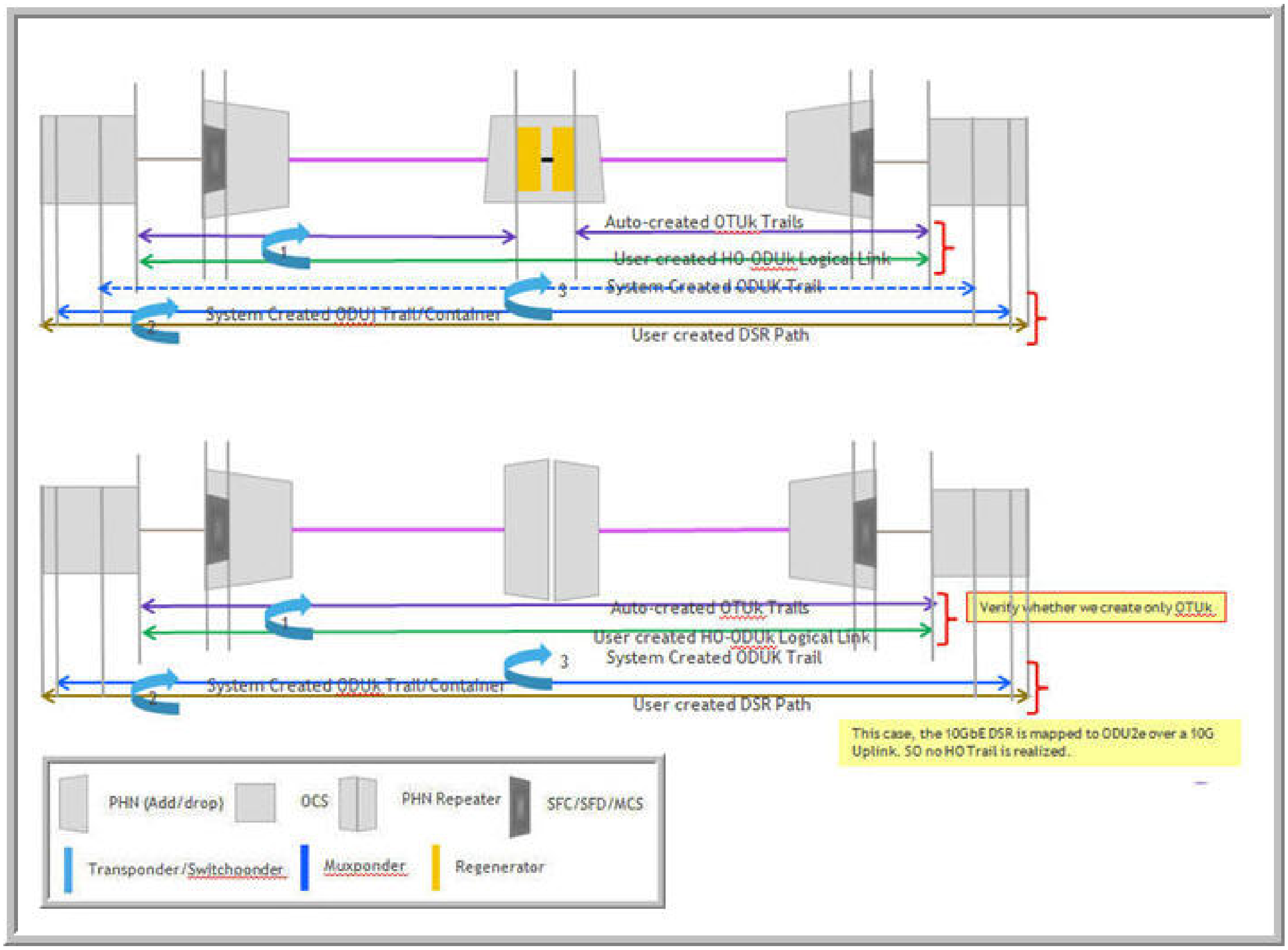
Figure 2-72 NFM-T OTN Network Provisioning – Muxponder Extended to OCS (10XANY10G) Configuration



2.42 Uplink configurations

Typical uplink configurations

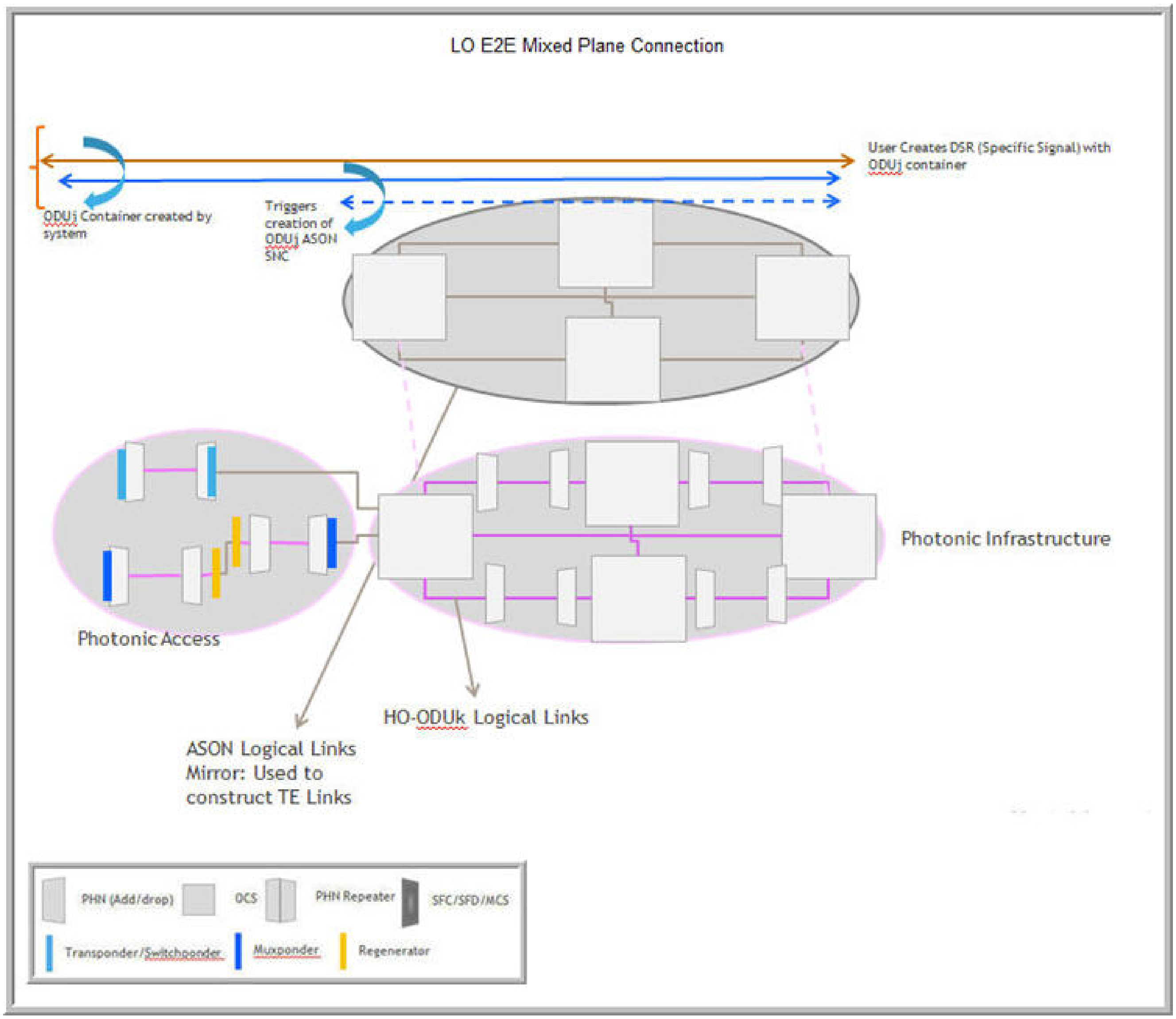
Figure 2-73 NFM-T OTN Network Provisioning – Uplink Configurations



2.43 L1 ASON configuration

Typical L1 ASON configuration

Figure 2-74 NFM-T OTN Network Provisioning – L1 ASON Configuration



2.44 Single node Hairpin service

Overview

Hairpin provides services between two clients of the same PSS-Nx node, that is, a service terminated on two ports of the same node, with no other nodes involved in the service route.

The service is client-to-client, requiring cross connection provisioning on the involved NE.

Supported shelf types: 1830 PSS-8x, 1830 PSS-12x, and PSS-24x

Supported Input/Output Circuit (IOC) cards:

- 1830 PSS-24x: 20AN80, 30AN300, 4AN400, 10AN400, 20UC200, and 10AN1T
- 1830 PSS-8x and 1830 PSS 12x: 20MX80, 4MX200, 20AX200, and 5MX500

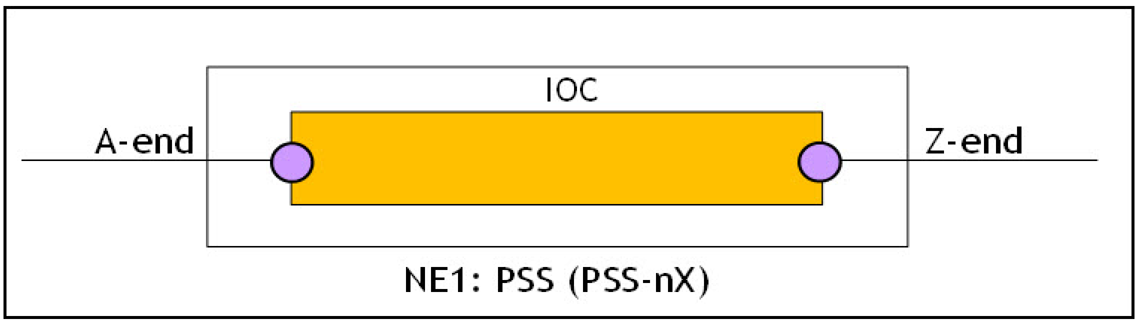
The interworking between these IOC cards is supported.

Supported Scenarios

The supported scenarios are as follows:

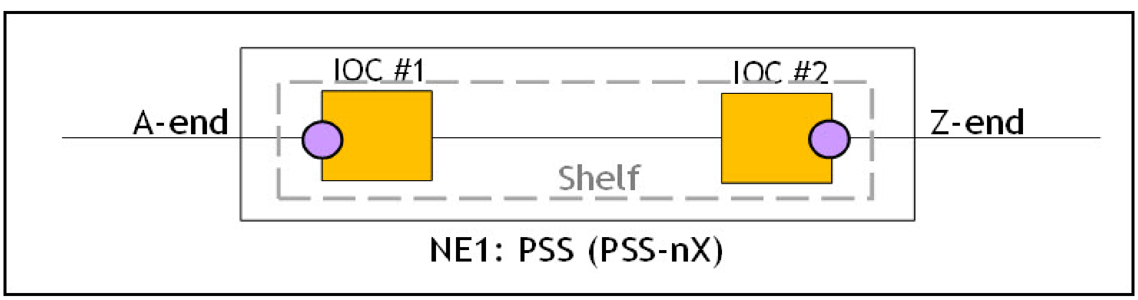
1. Same Input/Output Circuit (IOC) card

   The service termination points, that is, A and Z ends are within the same card.



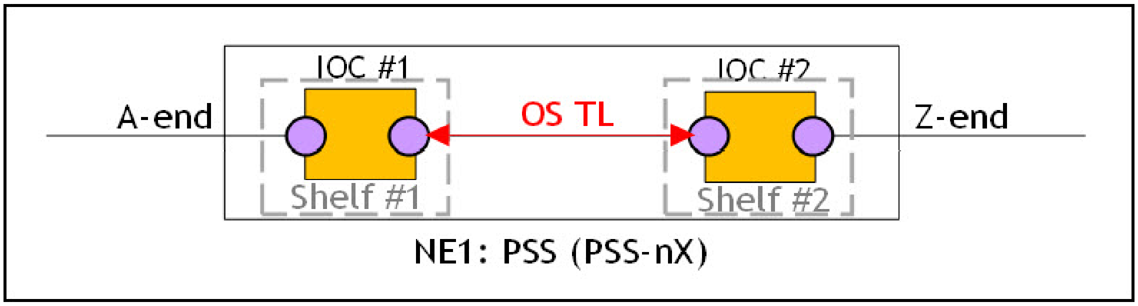
2. Two different Input/Output Circuit (IOC) cards positioned on the same shelf.

   The service termination points, that is, A and Z ends are on different IOC cards, whereas both the cards are on the same shelf.



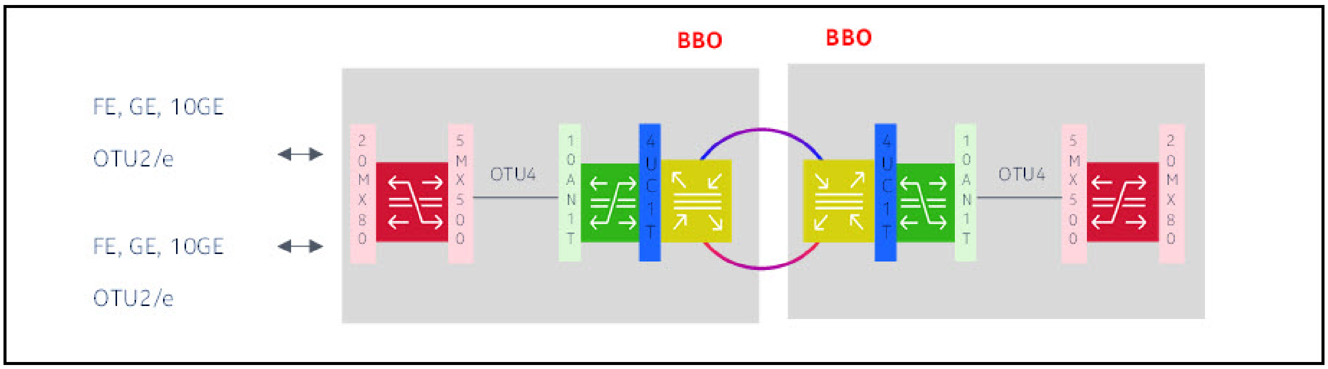
3. Two IOC cards positioned on different shelves

   The service termination points, that is, A and Z ends are on different cards that are on different shelves. There is an OS between two shelves.



The configuration is as follows:

Figure 2-75 Single Node Hairpin Service



Restrictions

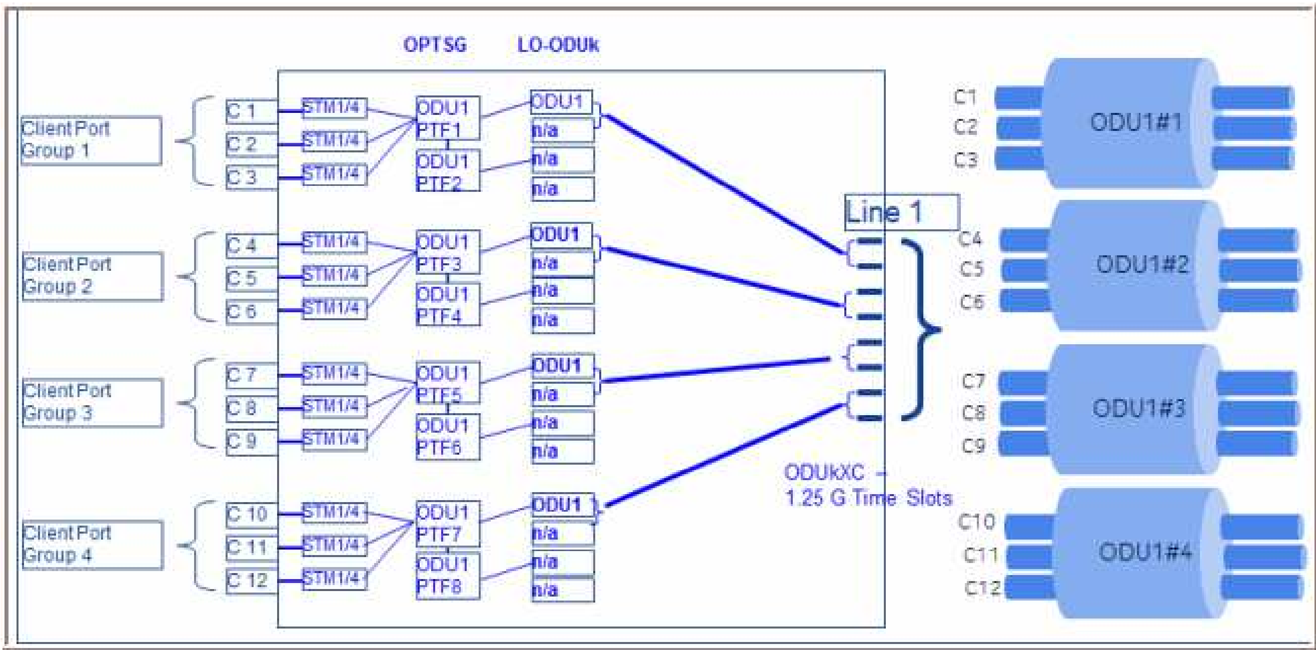
- In NFM-T Release 21.12, Hairpin service is supported for Managed Plane only.
- NNI discovery is not supported. A user can provision OTU2 Hairpin services, but discovery is not supported.
- Asymmetric OTU2-10Gbe services are not supported.
- The workflows for deployment, alarm, PM, OAM practice on such service types should not change with respect to the other existing services types.

Particular NFM-T OTN Network Configurations

2.45 Managed Plane scenarios

1830 PSS WDM NEs – 11DPM12 scenarios provision 1830 PSS WDM NEs – OPSTG cascading in 11DPM12

Figure 2-76 Scenario Example



The following provisioning steps must be performed for the 11DPM12 OPTSG cascading configuration.

- DSR connection must be provisioned between the 11DPM12 client ports that belong to the same port group using the deploy of infrastructure connection.

  Note: Digital Service Rate (DSR) is a term that is used generically to represent the service rate of a connection that is being provisioned. When you provision the service path, enter the actual Service Rate of the connection in order for the connection to be implemented.
- A cascaded cross connect (ODU1) must be created between the ODU1 PTFs using the 1830 PSS NE equipment view functionality that is accessible through the Equipment Manager window. This task requires you to access other tasks that are contained in this document.

  Refer to the *Equipment Manager (EQM)* chapter in the *NFM-T NE Management Guide*, for the creation of the cross connection procedures.

Network Scenario Examples

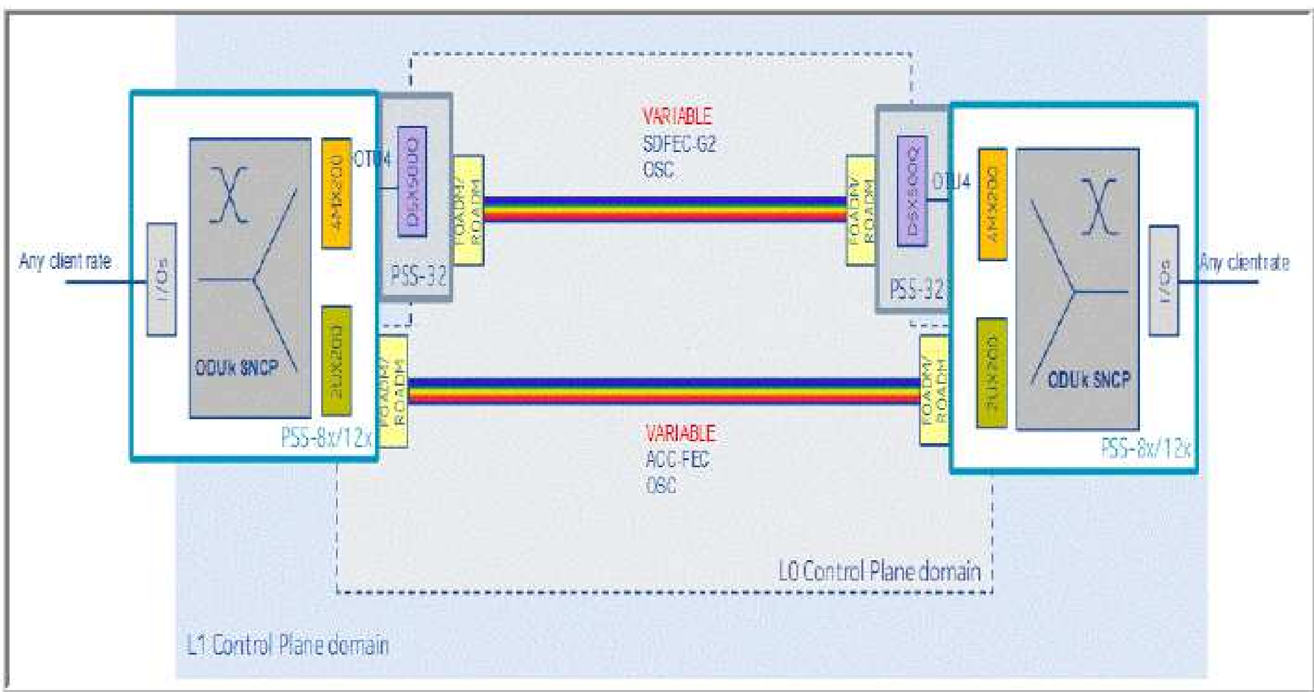
2.46 OTN packs cascading to D5X500/Q

Description

This network scenario example for OTN packs cascading to D5X500 and D5X500Q is composed by:

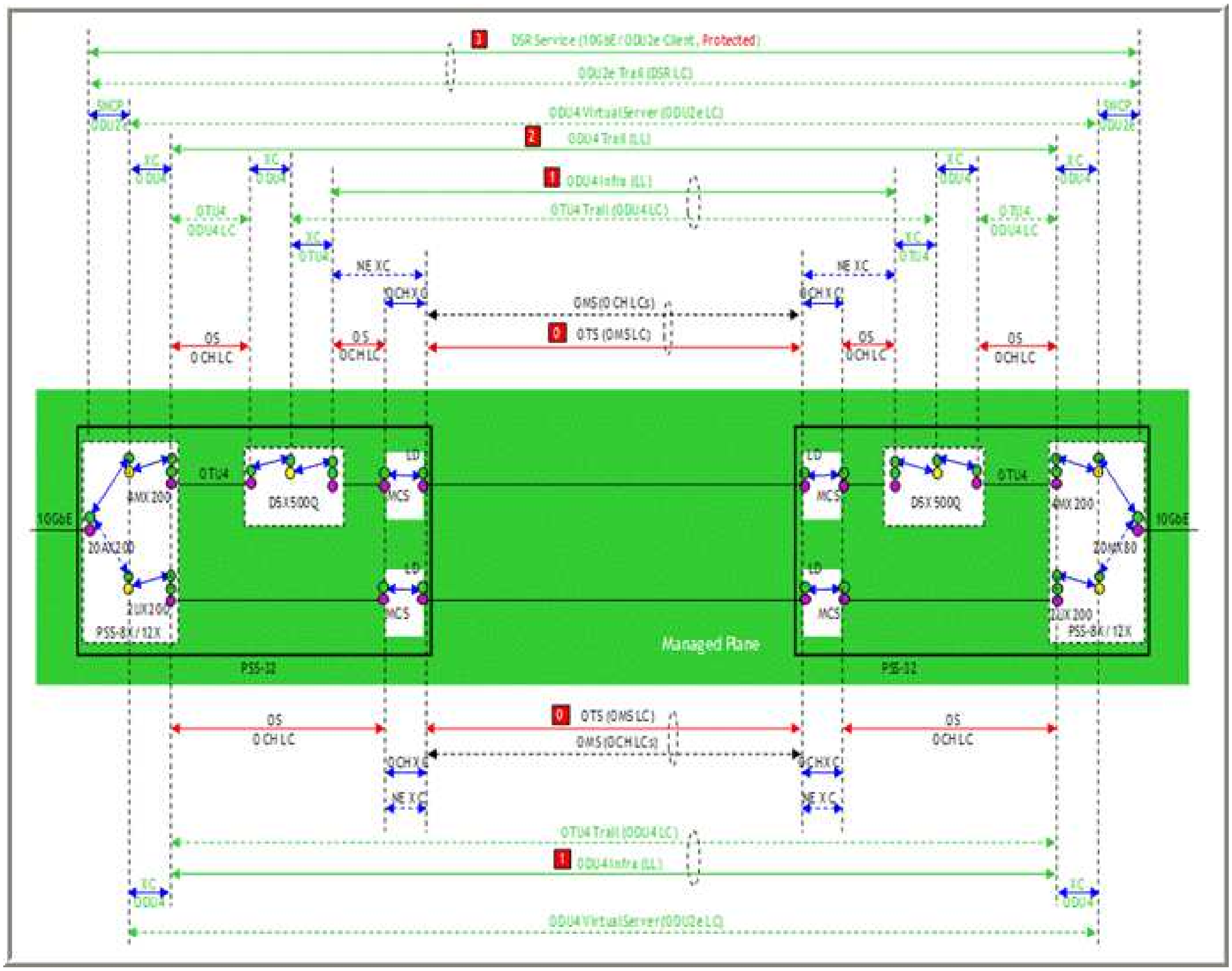
- A single PSS SWDM composed by a PSS-32 and a PSS-8x/12x interworking between D5X500/Q and 4MX200 (PSS8x/12X). Such interworking is a B&W OPS link.
- L1 GMPLS active on PSS-8x/12x. As consequence the ODU Logical Link terminated on 4MX200 need to be added to L1 GMPLS NPA as I-NNI.
- The scenario can be provisioned with D5X500 or D5X500Q packs.

Figure 2-77 OTN packs cascading to D5X500



Managed Plane scenario

Figure 2-78 Cascading to D5X500 - Managed Plane



Managed Plane scenario example

1

Create the ODU4 Logical Link between D5X00/Q and D5X00/Q

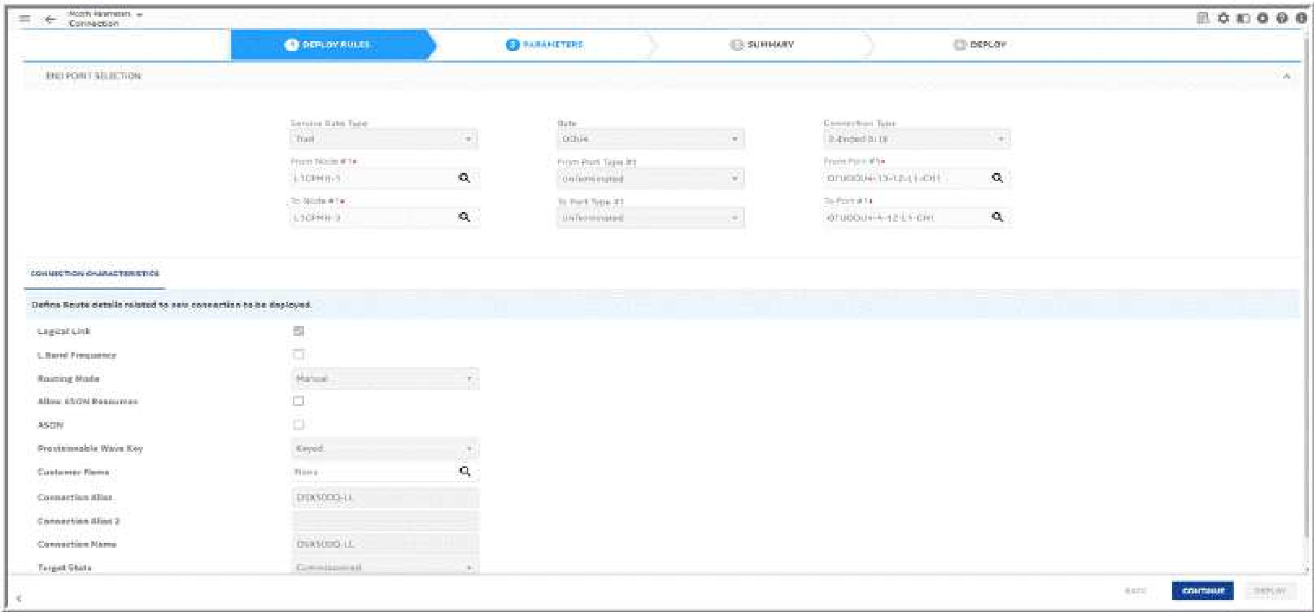
From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select the following parameters in the **DEPLOY RULES** panel:

- **Service Rate Type**: `Trail`

- **Rate**: `ODU4`
- Check the field **Logical Link**
- Insert the **Connection Name**

Figure 2-79 Cascading to D5X500 - Create ODU4 LL



2

Create ODU4 Long Logical Link between 4MX200 and 4MX200

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Trail`
- **Rate**: `ODU4`
- Check the field **Logical Link**
- Insert the **Connection Name**

In the **CONNECTION CHARACTERISTIC** panel the parameter **Auto Server Creation** must be unchecked which means that no auto server creation is requested.

3

Create ODU4 Logical Link between 20UX200 and 20UX200 Assign both the 4MX Long LL and the 20UX LL to NPA.

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Trail`
- **Rate**: `ODU4`
- Check the field **Logical Link**
- Insert the **Connection Name**

4

Create a 10G protected service between 20AX200 and 20AX200

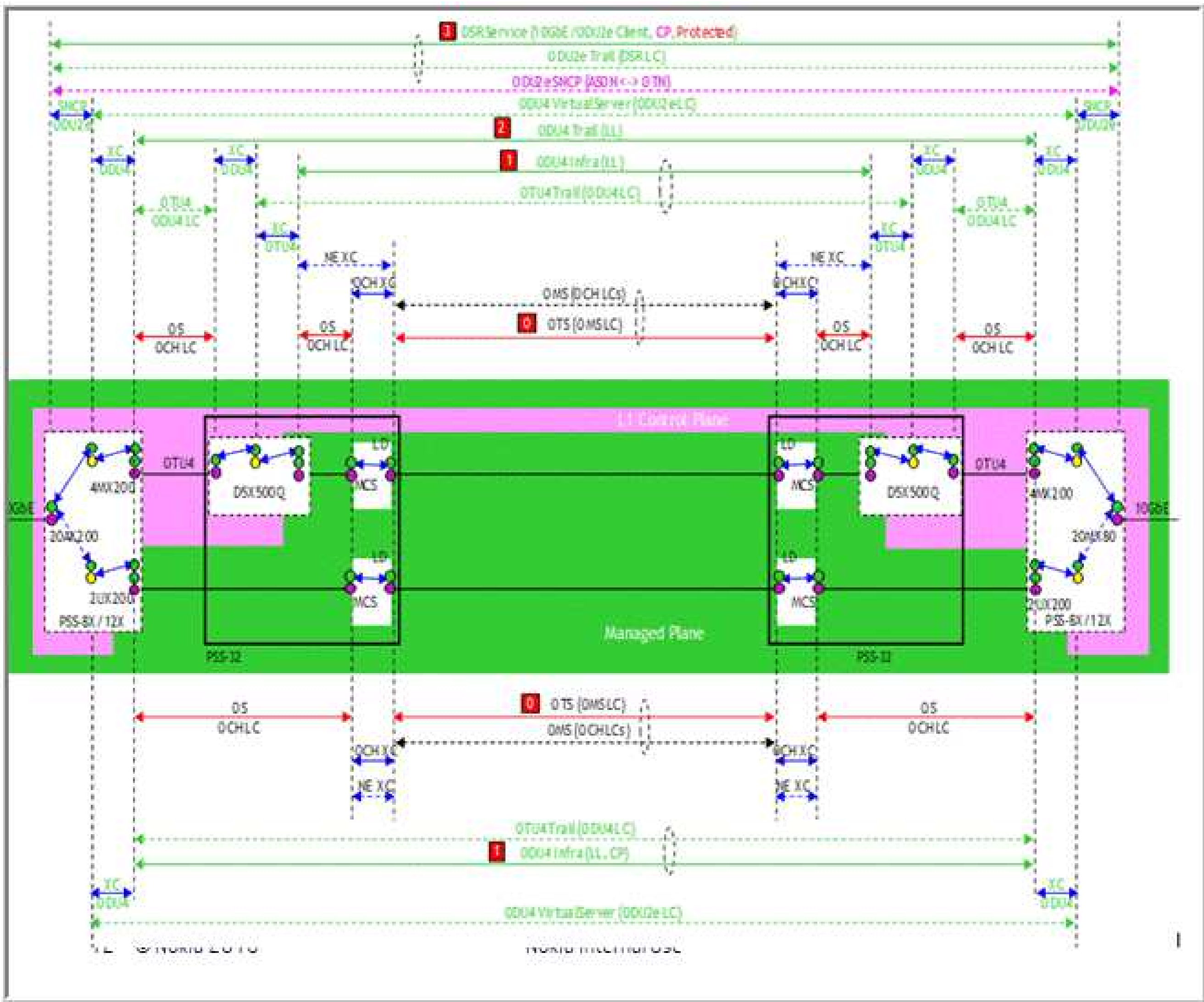
From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Ethernet`
- **Rate**: `10GbE`
- Check the field **Protection**
- Check the field **Auto Server Creation**
- Insert the **Connection Name**

Control Plane scenario

Figure 2-80 Cascading to D5X500 - Control Plane



Control Plane Scenario

1

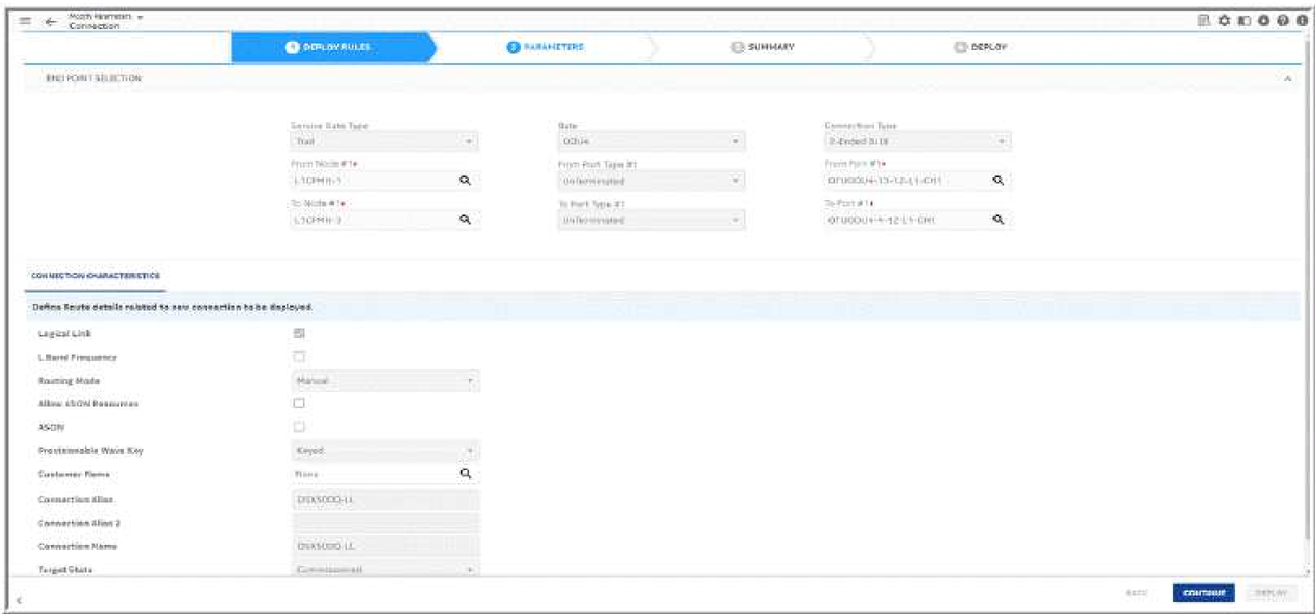
Create the ODU4 Logical Link between D5X00/Q and D5X00/Q (L1CP)

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Trail`
- **Rate**: `ODU4`
- Check the field **Logical Link**
- Insert the **Connection Name**

Figure 2-81 Cascading to D5X500 - Create ODU4 LL



2

Create ODU4 Long Logical Link between 4MX200 and 4MX200 (L1CP)

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Trail`
- **Rate**: `ODU4`
- Check the field **Logical Link**
- Insert the **Connection Name**

In the **CONNECTION CHARACTERISTIC** panel the parameter **Auto Server Creation** must be unchecked which means that no auto server creation is requested.

3

Create ODU4 Logical Link between 20UX200 and 20UX200 (L1CP)

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Trail`
- **Rate**: `ODU4`
- Check the field **Logical Link**
- Insert the **Connection Name**

4

Assign both the 4MX Long Logical Link and the 20UX Logical Link to NPA.

5

Create a 10G protected service between 20AX200 and 20AX200

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel

- **Service Rate Type**: `Ethernet`
- **Rate**: `10GbE`
- Check the field **Protection**
- Check the field **ASON**
- Check the field **Auto Server Creation**
- Insert the **Connection Name**

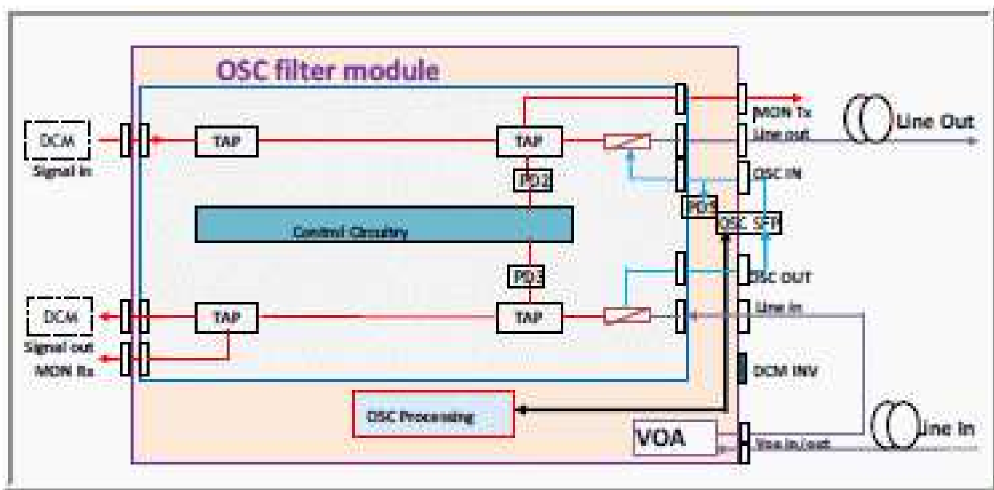
2.47 Network scenario example with OSCTAPR circuit pack

OSCTAPR description

The **OSCTAPR** is an upgraded version of the legacy OSCT card, it replaces the OA module inside AA2DONWB with an OSC filter module. This card is used to Add/Drop OSC channel into optical line when the amplifier is not equipped, and an open loop VOA is also integrated to adjust the link margin.

OSCTAPR-OSCT with APR support in half slot, and the pack diagram is shown the figure.

Figure 2-82 OSCTAPR Circuit Pack



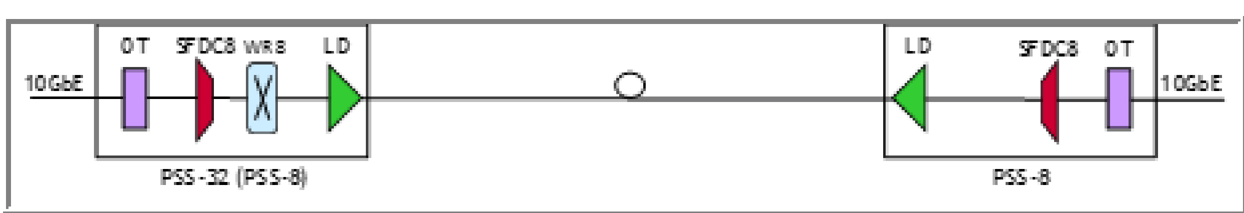
The NFM-T supports OSCTAPR at an optical model level, as for the other Line Driver circuit packs. The OCH crossconnect provisioning is supported, only with width=50GHz, and its frequency grid is 100GHz. OSCTAPR is supported in FOADM configuration, more specifically 100GHz spaced 1 degree FOADM terminal and 2 degree FOADM are required for OSCTAPR application with highest priority.

OSCTAPR APR interworks with AHPHG.

Supported network scenario example

Two example for OSCTAPR network configuration, in FOADM/ROADM or ILA/DGE.

Figure 2-83 OSCTAPR in Add/Drop FOADM/ROADM



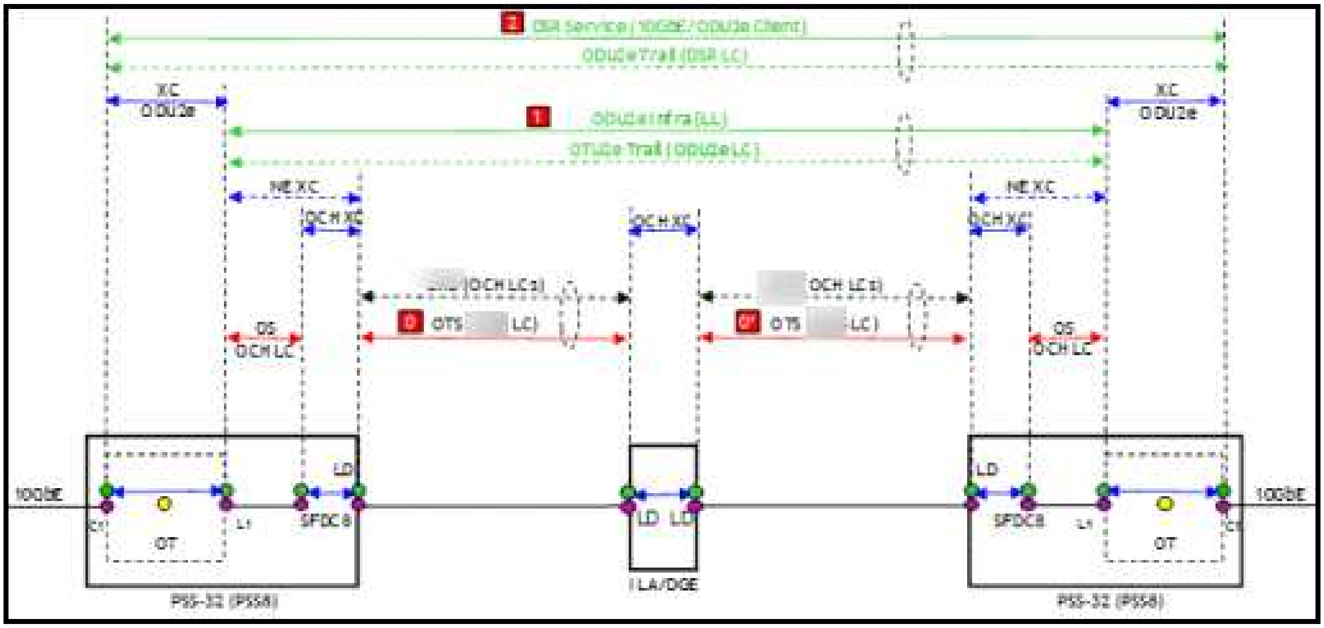
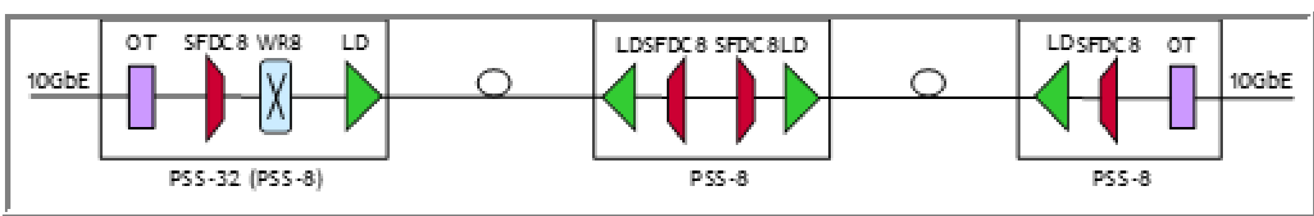
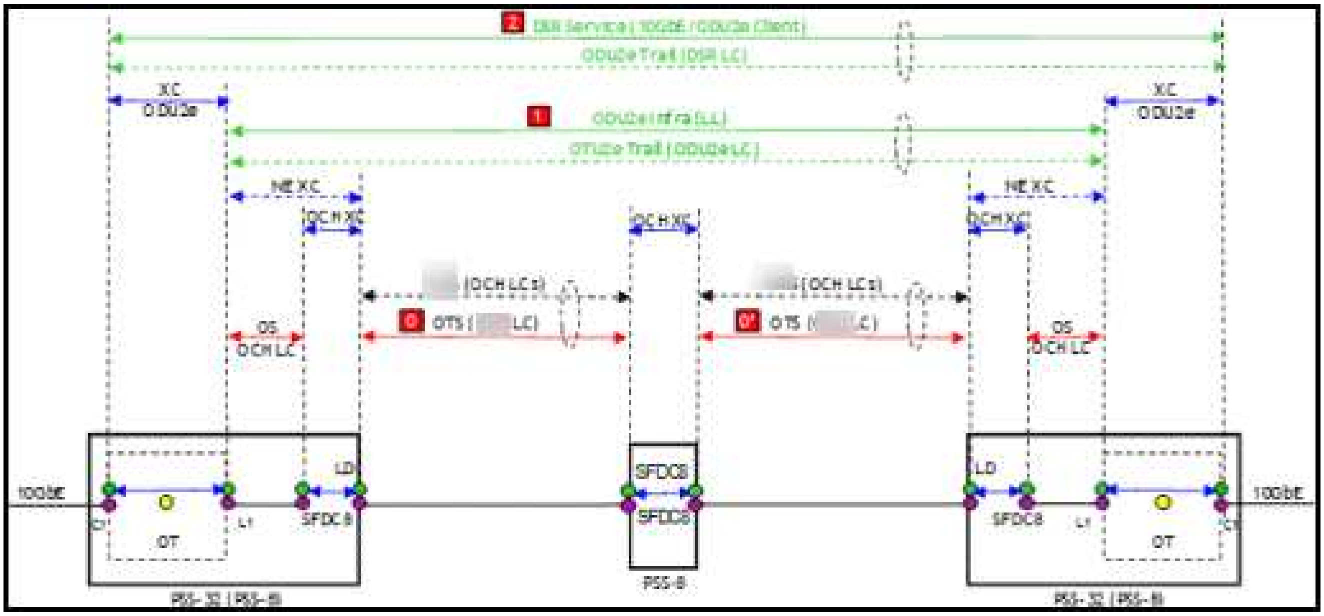


Figure 2-84 OSCTAPR in ILA/DGE




2
1
XC
ODU2e
XC
ODU2e
NE XC
OCH XC
OCH XC
NE XC
OCH XC
(OCH LCs)
(OCH LCs)
0
0'
OS
OCH LC
OS
OCH LC
10GbE
10GbE
LD
LD
SFDC8
SFDC8
SFDC8
SFDC8
OT
OT
L1
L1
C1
C1
PSS-32 / PSS-8
PSS-8
PSS-32 / PSS-8

2.48 Network scenario example with L2 and non-L2 circuit pack with ODUflex

Description

This network scenario shows an example of interworking between L2 packs (e.g. 6SE300/30SE300) and non L2 packs (such as 8x/12x/24x IO packs 20AN80/20MX80/30AN300/10AN400), involving an DSR/ODUflex connection.

Figure 2-85 Example of Interworking Scenario

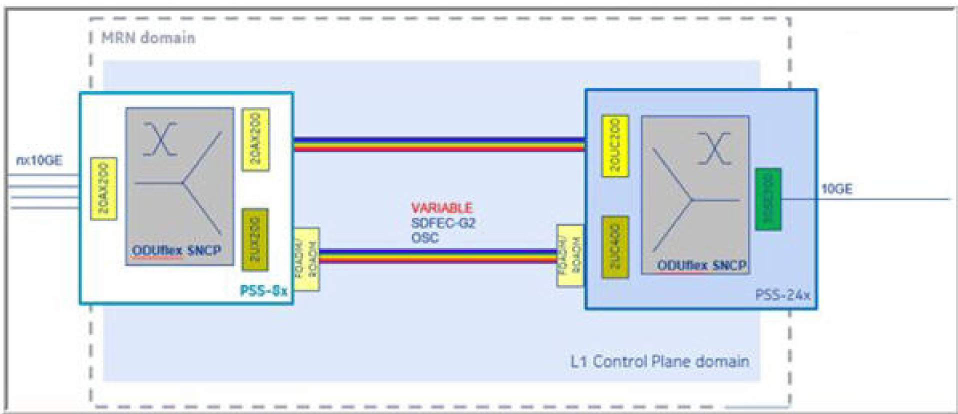
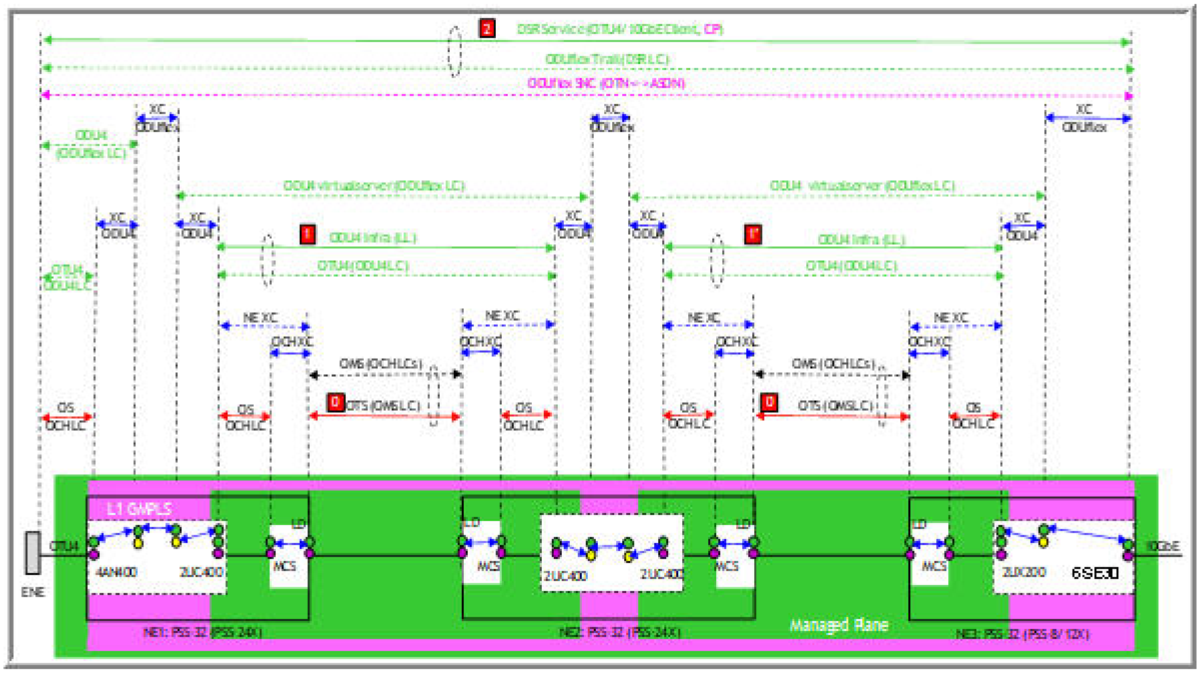


Figure 2-86 Supported Network Scenario Example



Provisioning steps

This scenario applies to: DFOADMs, ROADMs, including CDC-F, AC-DC ROADM. To provision the scenario perform the following:

1

Create the Internal OPS TLs and OTSs within the network.

From the NFM-T GUI, follow the path **OPERATE > Physical Connections**

2

Create the HO ODUk trails between the nodes.

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

Select following parameters in the **DEPLOY RULES** panel:

- **Service Rate Type:** `Ethernet`
- **Rate:** `Flexible Rate Client`

3

Create the ENE to be connected to the IO board.

From the NFM-T GUI, follow the path **OPERATE > Nodes**

4

Create the external NNI OPS between ENE and IO card with *OTUk* as signal Type.

From the NFM-T GUI, follow the path **OPERATE > Physical Connections**

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

5

Create a DSR / ODUFlex connection between the ends of the connection: the ENE on one end and the L2 cards on the other end, applying the following setting:

a) **L2 side:** terminated ports, use the L2 pack client ports

b) **ENE side:** unterminated ports, user need to choose ODUflex port and timeslots

From the NFM-T GUI follow the path **DEPLOY > New Service/Infrastructure**

The figures below show an example of the provisioning flow.

Figure 2-87 Example with provision template and ports selection

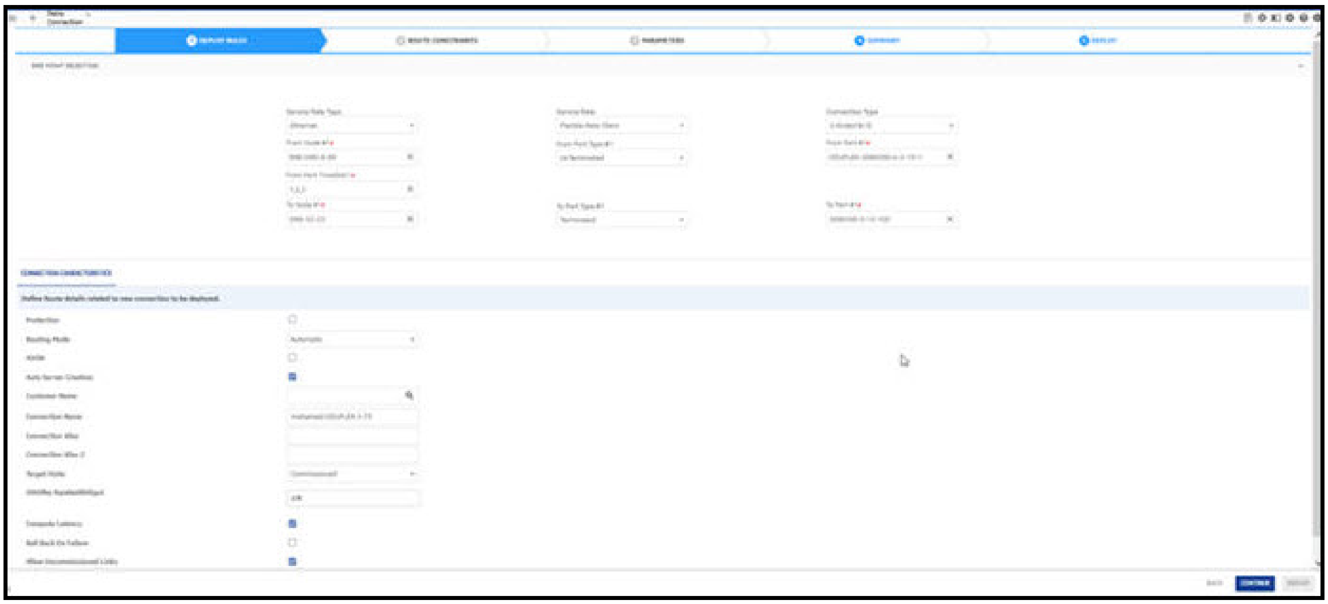


Figure 2-88 Example of E2E Routing Display with the created DSR/ODUFlex service.

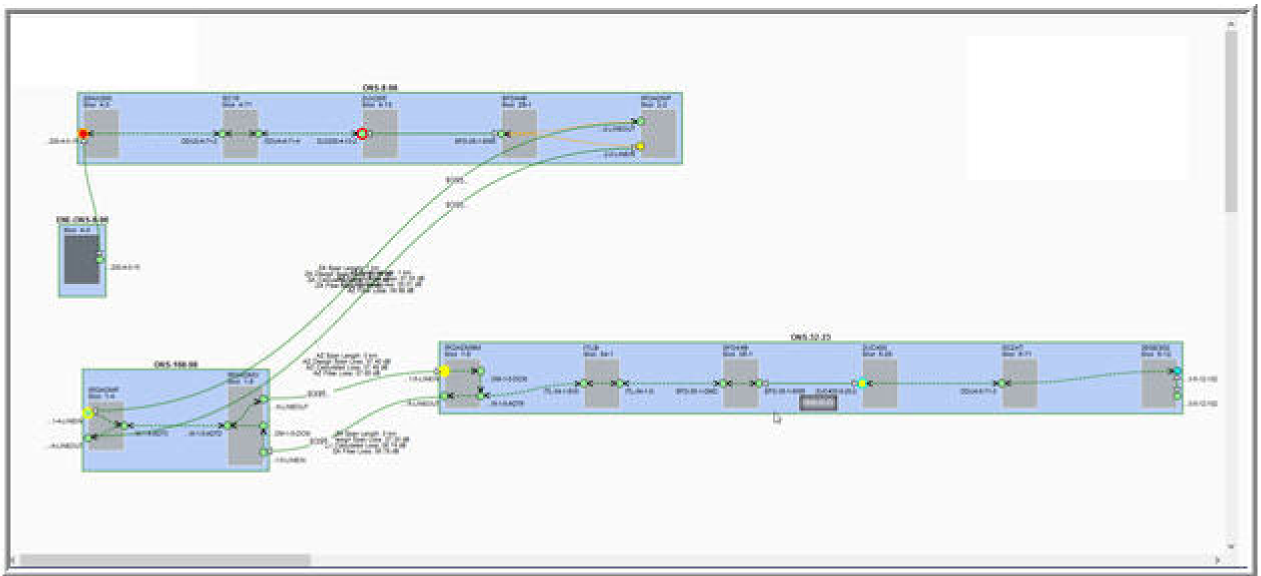
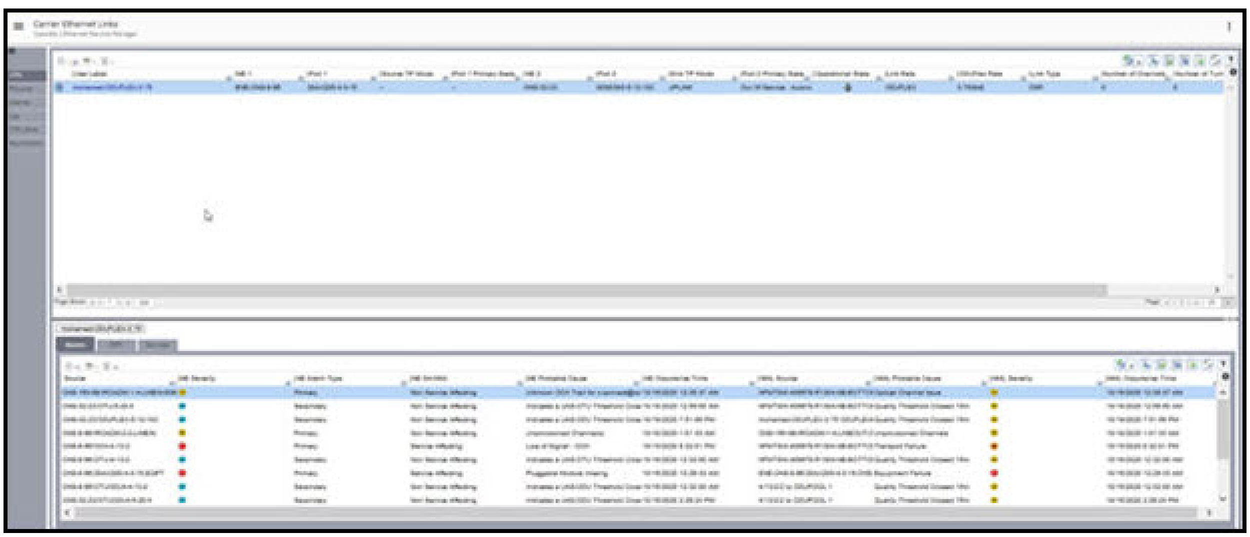


Figure 2-89 Example of DSR service exported to ESM subsystem



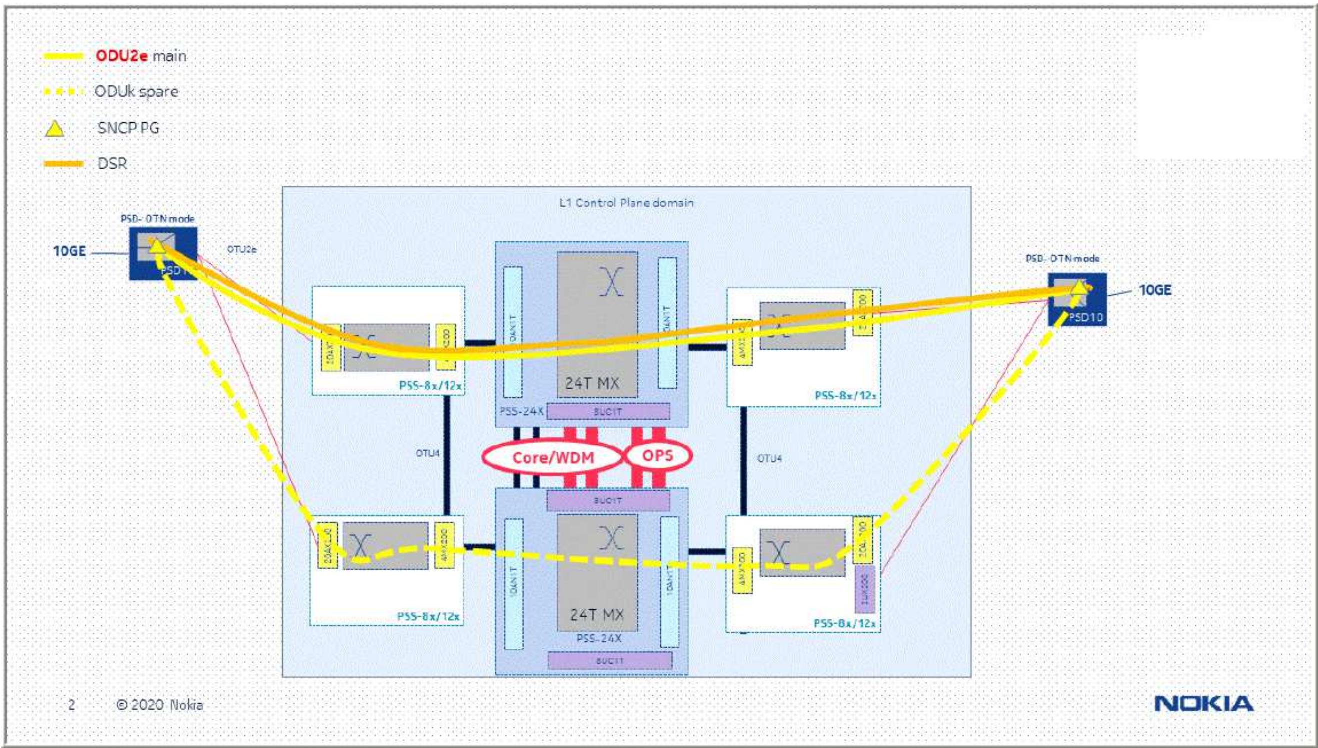
2.49 Add or remove protection for end-to-end 10G service

For a service starting and ending in MP and routed via L1 CP

Scenario description : A (SNCP and L1 Control Plane) 10G-Service starting and ending on PSD-Nodes is created. The SNCP is starting and ending on the PSD-End Nodes. So the end-to-end Service is SNCP-Protected with two separate ASON SNCs (Main and Spare).

1830 PSDs nodes are managed in Managed Plane and all other OTN NEs (OTN transit NEs) are managed in L1 Control Plane. To execute the Remove Protection command in this scenario, the user has to follow the procedure "To remove protection on service in MP routed via L1 CP" (p. 335)

Figure 2-90 Remove Protection Example



Note:

- Remove protection is not supported and cannot be performed for end-to-end protected Mixed Plane connection with two independent ASON SNCs.
- Add Protection cannot be performed for end to end protected Mixed Plane connection where new ASON SNC has to be created
- Reroute is not supported for 10 GbE service connection, where there are two ASON SNCs on the same service.

- Network 1 is always the working port and Network 2 is always the protection port, this is fixed behavior on the 1830 PSD NE.

To remove protection on service in MP routed via L1 CP

For detailed information to create connections and logical links see "Deploy a new service or infrastructure connection with template" (p. 1216). To setup the configuration in Figure 2-90, "Remove Protection Example" (p. 334) follow the steps:

1

Create L1 control Plane Network mix of PSS12x/PSS8X/PSS24X and provision OPS between L1 nodes.

2

Add all the OPS link to the NPA as NNI, then unlock all the Link. See 10.27 "Set the ASON administrative state of links" (p. 1504) and 10.15 "Add links and remove links from ASON" (p. 1462)

3

Create the OPS links between PSD (Network1) and PSS8x (20AX200) and between PSD (Network2) and the other PSS8x (20AX200) in A-end and Z-end node and add these OPSs as drop links to NPA.

4

Create the unprotected ODU2 ASON Logical Link from PSD (Network1) to PSD (Network1) in AUTO routing mode.

5

Create the unprotected ODU2 ASON Logical Link from PSD (Network2) to PSD (Network2) in AUTO routing mode.

6

The unprotected DSR path is discovered.

7

Execute the command **Add protection - System Routed** in the **Modify Connection** function on the ODUk infrastructures created between 71 port of PSD. See 7.58 "Manage protection for a connection in Managed Plane and Control Plane" (p. 960) for more details.

8

Automatically the unprotected service is converted in protected service

9

Execute the command **Remove Protection - Retain Main** in the **Modify Connection** on SNCP ODUk ending on 71 ports. See 7.58 “Manage protection for a connection in Managed Plane and Control Plane” (p. 960) for more details.

10

The DSR path is turned to unprotected path and can be displayed in the Routing Display function for the path.

2.50 OMS having OMSP as protection

- Create an OMSP connection.
- Create Tunnel using the same OMSP
- Navigate to **OPERATE > Infrastructure Connections** page.
- Select a connection and click **360° View** of that OMSP.

Note: The **CLIENTS** tab is disabled for OMS with OMSP Protection.

2.51 Interworking of legacy cards of 1830 PSS-64, 1830 PSS-32, 1830 PSS-24x

The legacy cards of 1830 PSS-64, 1830 PSS-32, 1830 PSS-24x interworks with each other in different scenarios Control Plane is already enabled at both L0 and L1.

Scenario 1: Interworking between two 2UX200 cards

1. Create a three node setup with 1830 PSS PHN NEs, where two nodes are in the Control Plane domain and one node is in the Managed Plane domain.

   The system automatically creates the OS connection.
2. Add the OS link to NPA as drop link.
3. Create a logical Link between 10AX200 (which is in the CP domain) and 8P20 (which is in MP domain) cards I
4. Create an OTSig tunnel with or without 3R between two 2UX200 cards on two NEs, where one NE from the three node setup is common and the other one is a different NE. The profile IDs supported for OTSig tunnel creation between two 2UX200 cards is 7. 9. 10. and 11.

   To view the 3Rs, navigate to **OPERATE > ASON SNCs > ROUTES** tab.
5. Create an end-to-end 10GbE protected service.

The end-to-end connectivity is established.

Scenario 2: Interworking between 2UX200 and 1830 PSS OCS

1. Create a two node setup with 1830 PSS PHN and 1830 PSS OCS NEs, where 1830 PSS OCS is connected to 1830 PSS PHN.
2. Create an MRN FA Unterm tunnel between 2UX200 and 130SCUP cards.
3. Create 1G ODUk SNCP protected service between 2ux200 and 130SCUP cards

   Create 10G ODUk SNCP protected service between 10XANY10G/10GC cards.

   Create 100G ODUk SNCP protected service between 24XANYMRB cards.

Scenario 3: Interworking between 4UC400/2UC400 and 2UX200

1. Create a multi-node setup with 1830 PSS PHN NEs.
2. Create an MRN FA Unterm tunnel between 2UC400/2UC400 and 2UX200 cards.
3. Create an 100G OTSig tunnel or FA-Unterm tunnel between 4UC400/2UC400 and 2UX200.

   The profile IDs supported for OTSig tunnel creation between two 4UC400/2UC400 and UX200 cards is 7.
4. Create an end-to-end service for all the rates.

Scenario 4: Interworking between 4UC400 and 2UX200

1. Create a multi-node setup with minimum four nodes, where two nodes are in Managed Plane and two nodes are in Control Plane.
2. On the Control Plane part of the setup, create an OTSig Tunnel between 4UC400 cards. The Profile IDs supported for OTSig tunnel creation between 4UC400 cards is 7 and 31.

On the Managed Plane part of the setup, create ASON routed ODU4 logical link between S13X100 and 2UX200.

An ODU2 infrastructure connection is automatically created.

3. Create a 10G end-to-end mixed plane protected service for all the rates.

ROADM

2.52 ROADM network configurations (iROADMF/V)

Additional ROADM network configurations (iROADMF/V) with 1830 PSS R9.0

1830 PSS R9.0 introduces a new set of 1830 PSS configuration interworking between iROADMF/V and other WSS.

Considering iROADMV, this interworks with OTS lines build as:

- **1D FOADM**.
- **WR20TF based C-F (former AC-D-C) architecture**.
- **WR2-88 base ROADM**.
- **WR20TFM based CDC-F based architecture**.

In addition, it is possible to have a 1830 PSS SWDM single NE with both iROADMV and CDC-F architectures together.

The pass through between these two architectures is possible using 3R.

This specific configuration considers L0 GMPLS, L1 GMPLS and managed-plane.

In case of L0 GMPLS, only CDC-F architecture is part of GMPLS domain/ASON NPA.

The iROADM architecture, and related degrees, is not in L0 GMPLS domain/ASON NPA and it must be managed-plane only.

In all of such interworking configurations, iROADMV NE must contains either SFDx or PSC1:6 for Add/Drop channels.

Considering iROADMF, this interworks with legacy OTS lines build as:

- **ILA**.
- **ROADM: WR2-88 or WR8-88 based including CONF D, D',D"**.
- **TOADM: CWR8B 100GHz based interoperability & CWR8-88 50GHz based interoperability**.
- **WR20TF based C-F (former AC-D-C) architecture**.
- **WR20TFM based CDC-F based architecture**.
- **1DFOADM Auto power manage**.

In addition, it is possible to have a 1830 PSS SWDM single NE with both iROADMF and CDC-F architectures together.

The pass through between these two architectures is possible using 3R.

This specific configuration considers L0 GMPLS, L1 GMPLS and managed-plane.

In case of L0 GMPLS, only CDC-F architecture is part of GMPLS domain/ASON NPA.

While iROADM architecture, and related degrees, is not in L0 GMPLS domain/ASON NPA and it must be managed-plane only.

In all of such interworking configurations, iROADMF NE must contains either SFDx or PSC1:6 for Add/Drop channels.

2.53 Unkeyed services in ROADM configurations

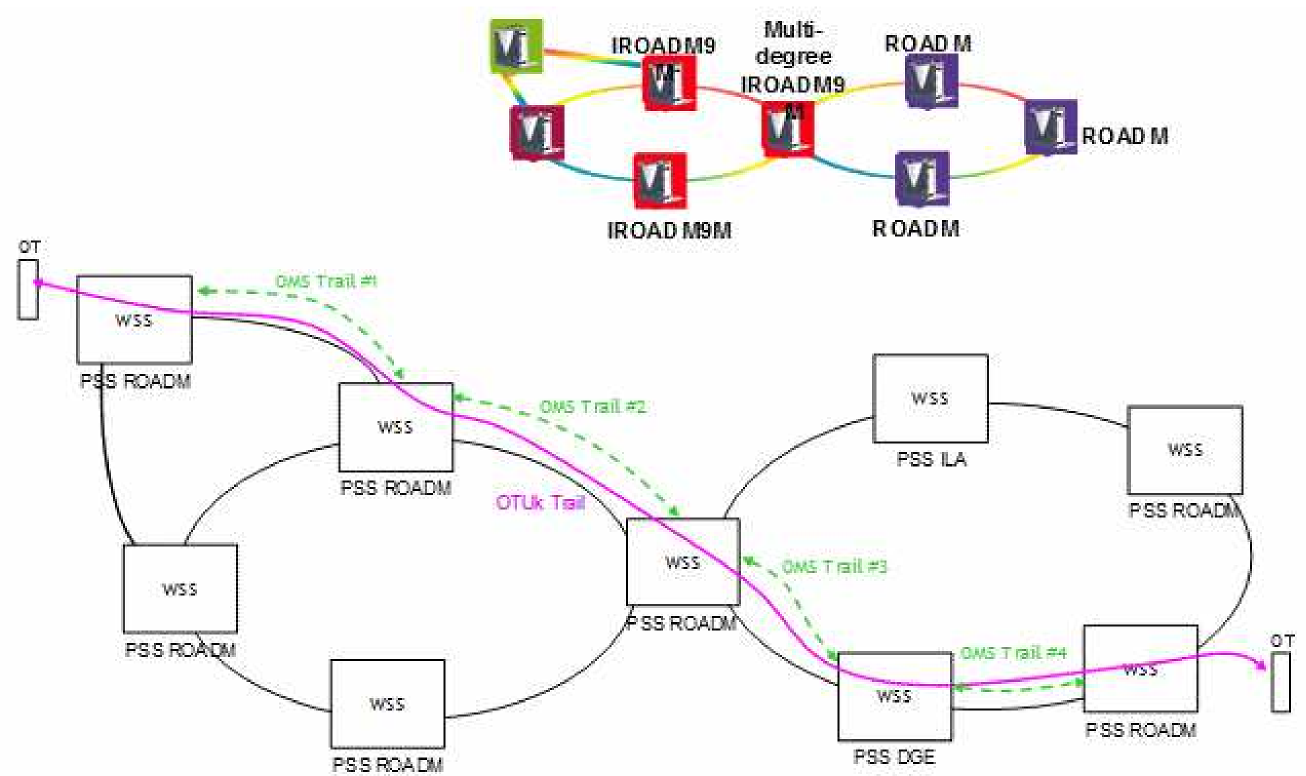
Description

The NFM-T supports an OCH optical channel without wavekeys, that is an unkeyed OTUk trail end-to-end. Unkeyed services (OCh trails) were previously supported with no auto optical power managed. This feature adds general support for unkeyed services by the PSS NE, allowing unkeyed services to be used in manual and auto power managed networks.

In addition to CDC-F, all other architectures are supported, including alien wavelength.

The configuration is applied in Managed Plane.

Figure 2-91 Unkeyed Services in ROADM – OTUk/OCH Trail Provisioning



All existing optical ROADMs types are supported:

- CDC-F (MCS) ROADM – high priority
- C+L ROADM – high priority from PSS R10.1 and NFM-T Release 22.6_FP1
- TOADM (CWR) from PSS R10.1 and NFM-T Release 22.6_FP1
- Legacy ROADMs from PSS R10.1 and NFM-T Release 22.6_FP1
- Config. D, D’, D” ROADM from PSS R10.1 and NFM-T Release 22.6_FP1

- C-F (AC-DC/PCS1-6) ROADM from PSS R10.1 and NFM-T Release 22.6_FP1
- iROADM from PSS R10.1 and NFM-T Release 22.6_FP1
- FOADM (including PSS-4) from PSS R10.1 and NFM-T Release 22.6_FP1
- ILAs/DGEs from PSS R10.1 and NFM-T Release 22.6_FP1

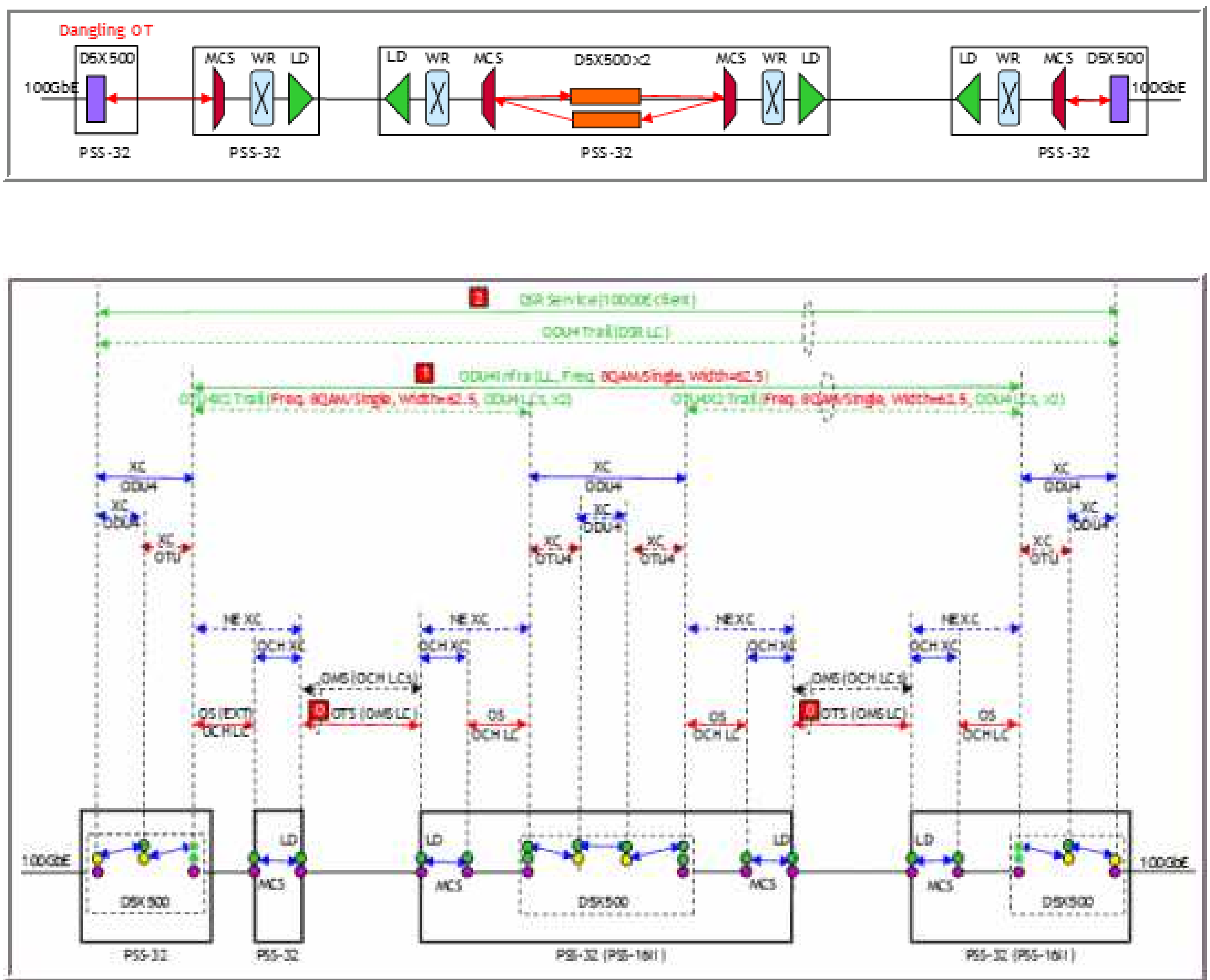
Network scenarios

The example of network scenario in the figure displays:

OTs: D5X500/D5X500L, 130SNX10, 260SCX2

Configurations: CDC-F, Add/Drop and THRU/3R Regen, Dangling OT, Managed Plane only

Figure 2-92 Unkeyed Services – D5X500 Add/Drop & THRU, 100GbE Client



Provisioning the configuration

The create connection window filters out the **Provisonable Wave Key** based on the end points type, that is a difference between DWDM and CWDM NE types as described in the table. See the procedure 7.12 "Deploy a template to make a connection" (p. 754) for the details on creating a connection.

Table 2-13 Provisionable Wave Key - DWDM and CWDM

	NE Release	Provisionable Wave Key	Wave Key Type	default Wave Key Type
DWDM	10.0, 10.1	Unkeyed	Manual	Manual
	10.0, 10.1	Unkeyed	Automatic	
	10.0, 10.1	Keyed	Manual	Automatic
	10.0, 10.1	Keyed	Automatic	
	10.0, 10.1	N/A		
CWDM	10.0, 10.1	Unkeyed	N/A	N/A
	10.0, 10.1	N/A		

2.54 Non CDC-F ROADM configurations support

Non CDC-F ROADM configurations support for ASWG and A4PSWG

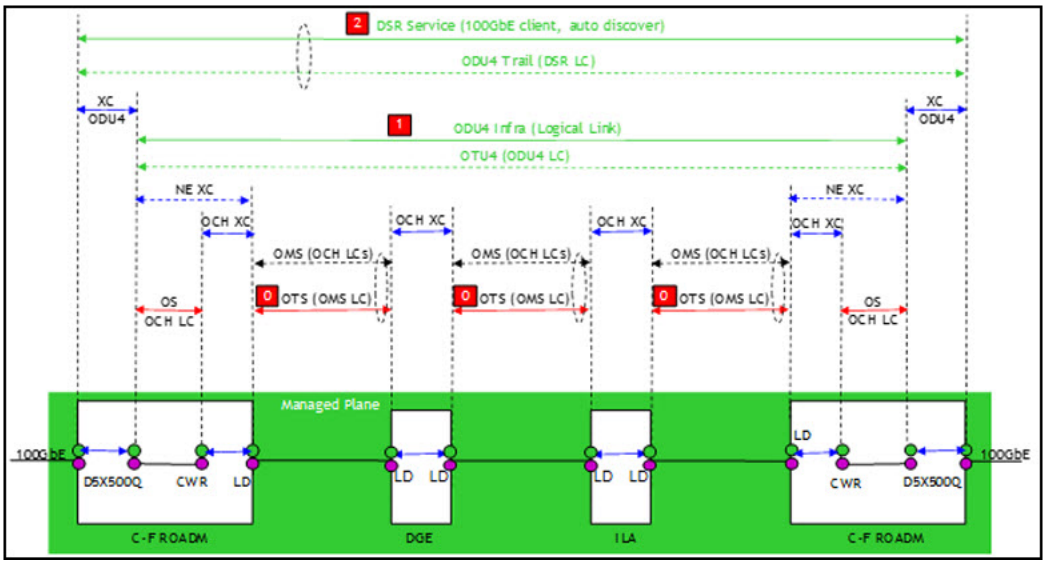
NFM-T supports non CDC-F ROADM configurations for ASWG and A4PSWG, which are the Line Driver (LD) packs. This configuration is supported for both Managed Plane and L0 Control Plane connections.

The following non CDC-F configurations are supported with ASWG and A4PSWG:

- Legacy ROADMs (Config. D, D’, D”)
- TOADM (with CWR packs)
- C-F Any Color - directional colorless (AC-DC) ROADMs

An example of ASWG/A4PSWG in TOADM/Legacy ROADM is depicted in Figure 2-93, “1.1.2. ASWG/A4PSWG in TOADM/Legacy ROADM” (p. 345).

Figure 2-93 1.1.2. ASWG/A4PSWG in TOADM/Legacy ROADM



Alien Network Management

2.55 Alien services

Description

NFM-T supports two different set of services to implement alien network management

- Alien service with MVACx, this function is supported with OCH service type and deploys a standard provisioning workflow. The MVACx cards have limited alarms, but PM have WT encoder/decoder points. MVAC and MVAC8B are not supporting the same set of photonic architectures.

  The MVACF (fixed grid) is introduced in NFM-T R19.9/PSS R12.0.
- An additional service type, unkeyed service, is introduced to allow the support of pure alien services.

  This type of service allows to create channels and related services without wavelength tracker keys. It is required for alien channel without MVACx. The channels are created without any OTs/MVACx card (terminated in ENE connected to MUX/WSS port).

  Alien wavelength (lightpath) service management extended to L0 GMPLS (as foreign connections), flex grids, support of Power Management charts.

Alien services with MVACx

sVAC/MVAC and MVAC8B management for alien wavelength is supported in *Managed Plane* configuration (MVACx).

- Equipment: Card and related cabling are defined in EQM (Equipment Manger). Card/cabling are then uploaded in NFM-T.
- Provisioning
  - Done by NFM-T through a dedicated template. Provisioning workflow is similar to other OTs.
  - Alien wavelength is modeled as a OCHs service/channel and this is specific to MVACx only.
  - OCH Service/channel is terminated on two virtual NE/Black box, that can be other vendor NEs.
  - OCH Service/channel is created as *keyed*. NFM-T can assign WT keys or let NE assign them.
  - NFM-T supports OPSB protection on MVACx.
- OA&M
  - Alarms generated by MVACx are correlated to OCH services. This includes either simply LOS or other photonic alarms, alarms related to WLT such as WLT keys alarms.
  - Only analog PM, optical Power Rx/Tx, generated by MVACx and collect/correlate by NFM-T to related points.
  - WLT graph (per lambda) supported as per any other channels.

NFM-T supports *managed-plane* alien wavelength through a GMPLS L0 domain using the foreign connection feature, see “Foreign Connections” (p. 1413)

- MVAC/MVAC8B are on PSS-32 with L0 GMPLS enabled.

- The user provisions a managed-plane connection through a L0 GMPLs domain using the foreign connection feature.

Figure 2-94 Alien Configuration - MVACx

Unkeyed service

Unkeyed service is introduced to support OTs with pluggables without Wavelength tracker and *pure* alien channels/services. This feature disables the wavelength tracker keys setting/generation in the NE, but still supports the *power tuning* for the channels (auto power mode).

Alien services without MVACx

To manage the connection without MVACx a *virtual NE/Black box* connection to PSC1:6/WSS/SFD modules (physical link management) is used, so the OCH service (Optical channels) can be provisioned E2E using the virtual NE/Black box as channel terminations.

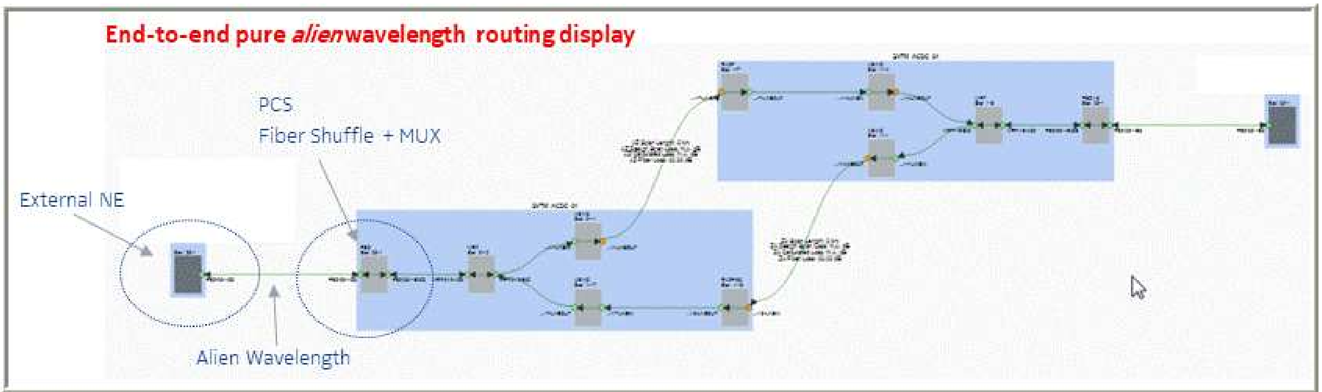
Equipment: Card and related cabling are defined in EQM (equipment manger).

Provisioning: Like the MVACx channels, the pure alien service is modeled as a OCHs service/ channel.

A lightpath service is an alien wavelength service that does not require an MVAC pack. An NE can be used for lightpath service configuration, if the NE is licensed with the feature.

An OCH service can be provisioned without VNE/BBOX, which allows to create LightPath service ending on Add/Drop ports directly (SFD/PSC1:6/MCS/CWR/WR...). It is possible to use VNE/BBOX as end points for LightPath service.

Figure 2-95 Alien Configuration - Service without MVACx



Alien wavelength support on Control Plane

Alien wavelength in GMRE L0 is supported on Control Plane from NFM-T R22.6 onwards and 1830 PSS NE (GMRE) R14.0.8 onwards.

GMRE restoration follows the normal scenario for line cuts and equipment failures. *Unprotected, SBR, and GR* restoration types are supported.

GMRE supports restoration of Alien services in read-only mode supporting a single service profile and single frequency.

A virtual Alien OT is used as demarcation point inside the 1830 PSS network.

- OT relevant parameters (Modulation, FEC) are configured on the virtual Alien OT, that is, a set of parameters on the MUX port describing the minimum information required by GMRE is set-up on the Alien channel.
- The manually defined virtual Alien OT parameters are used by the GMPLS for routing calculations.
- The configuration is static, that is, FEC cannot be modified on the virtual OT.
- The following are supported in 1830 PSS R14.0.8 onwards.
  - single channel access port - the port carries a single channel only
  - PSC
  - MCS
  - SFD
  - MLFSB

Supported configurations for Control Plane

When provisioning Alien service on Control Plane, for ENE only, it is mandatory to assign the OPS from ENE connecting to NOKIA Add/Drop port to NPA as droplink.

The following configurations are supported as Add/Drop devices with virtual Alien OT access ports (this excludes MVAC, OPSA, OPSFlex, and OPSUM).

- C-F (IROADM9R, IR9)
  - IR9 - PSC
  - IROADM9R - PSC
  - IROADM9R - SFD44/B (with ITLB is the only configuration supported and validated by EPT/ GMRE)
- CDC-F 2.0 (IRDM20/32)
  - IRDM20/32 - AAR8x/AAR2x8A - MCS816/MCS1615
- C-F (IRDM20/32)
  - IRDM20 - MLFSB
  - IRDM32 - MLFSB - PSC
- CDC-F 1.0 (WR20TFM)
  - WR20TFM - AAR8x/AAR2x8A - MCS816/MCS1615
- C-F (WR20TF)
  - WR20TF – PSC

Virtual Alien proxy OT configuration

The reference of the Alien proxy OT is the Alien OT identifier and the ingress/egress reference port, the frequency and slot width are defined with the default Alien profile. Set PCONN, to modify the parameters defined for the virtual Alien OT.

The proxy OT definition contains the following attributes:

- Proxy OT ID (Integer- reference index)
- Network access port
- Service profile (using given profiles, extended profiles and alien profiles)
  - NE uses for OTSiG service profiles from 1..99
  - For Alien profiles using default value 99999 - mapped to Alien type
- Module type (using given module types and alien module types)
  - GMRE uses a set of known modules for 10G/40G/100G
  - Add additional module type for Alien
- Frequency in 4:3 format
- Slot width for switching required in multiple of 12.5 GHz
- Descriptor (string)
- Add/Drop XC (integer representing the PCONN XC-ID (ID assigned to each PCONN within the PSS Node)

Relationships between PCONN(XC), port, and Alien OT port.

- Port type cannot be changed (from external) when Alien OT's are configured
- When a PCONN is created, the Alien OT, XC attribute is updated

- Port type is external when an Alien OT is created
- Reference port and index cannot be changed
- Frequency, profile, slot width and module type can be changed only when no PCONN XC is present

  PCONNs supports all cross connection slot width up to 125Ghz (that is, 50,62.5,75,87.5,100, 112.5,125 Ghz)
- Alien OT cannot be deleted when PCONN is present

Limitations

- Single default virtual Alien OT profile for alien wavelength (read-only mode).
- Alien OT's must be deployed in a separate Add/Drop block for managed OTs Add/Drop block (for example, MCS), that is, as there is no power control, to avoid Alien traffic impacting the managed OT traffic, it is recommended to configure Alien OT in their own Add/Drop block.

  No mixing with supported Nokia OTs. However the mixed configuration is not blocked by the NE nor NFM-T.
- DCM free networks only
- By default **System Assigned Frequency** is unchecked. Select **System Assigned Frequency** and assign a **Frequency**.
- No ADT port for IRDM card support
- No MVAC support
- One single profile (ID 99999)
- No 3R support for Alien LSP
- For Managed Plane, Alien wavelength is supported with or without an ENE connection.
- For Control Plane (from NFM-T R22.6 onwards), Alien wavelength is only supported with an ENE connection.
- Support for *Unprotected* and *Unkeyed* services only

  NOTE:

  − Before provisioning the OCH unkeyed service direct connection, from the NE WebUI, ensure the **Unkeyed Dangling Add/Drop Enabled** parameter is set to `Yes` for the NE.

  − For an OCH Alien service, connection is not valid if A-end is an ENE and Z-end is a non-ENE.

  − Protection on OPSA, OPSFLEX, and OPSUM requires wavekeys support.

NFM-T GUI Changes

- Support for *Unprotected* and *Unkeyed* services only. When *Unkeyed* is used, GMRE automatically enables **Use NE Value** on Nodes in a Control Plane connection.
- Enable **ASON** in the *Deploy* template for routing the connection in ASON.

  NFM-T provisions the Alien parameters on the NE and these values are used by GMRE to set-up the Alien channel.
- Default template for routing constraints will not have the **System Assigned Frequency** parameter flagged (current default option in Managed Plane) in Control Plane. Set the frequency according to the remote OT assigned frequency.

NFM-T provisions the alien parameters on the NE and these values are used by GMRE to set-up the alien channel.

- No need to provision any Virtual OT equipment on the NE, provision only the MIB parameters.
- Once the SNC is deployed, Alien parameter values cannot be changed.

2.56 MVACF

MVACF

MVACF is a variant of MVAC with flexgrid, which is a uni-directional 8 port Multiple-port Variable Attenuator Card, with Flexgrid support. Other VAC packs are fixed grid only. The pack is used for inserting and removing wavekeys (keyed/fVOA, unkeyed/sVOA). NFM-T provides the same level of support for MVACF as for MVAC, with addition of Flexgrid support for MVACF.

MVACF is the new MVAC card introduced in 1830 PSS R12.0 to handle *Alien* flex-grid channels.

MVACF is applicable to managed-plane configuration, instead for L0 GMPLS, it can be supported only as foreign connection. See "Foreign Connections" (p. 1413) for details.

New supported connectivities for MVACF configuration are:

- CDC-F 2.0 (IRDM20 and IRDM32) with MCS8-16 Add/Drop block
- CDC-F 2.0 (IRDM20 and IRDM32) with MCS1615 Add/Drop block
- IRDM20/32 MLFSB+MVACF
- IRDM20/32 MSH4FSB+MLFSB+MVACF
- IRDM20/32 MLFSB+PSC1-6+MVACF
- IRDM20/32 MSH4FSB+MLFSB+PSC1-6+MVACF

MVACF flex grid support

The Alien MVACF configuration supports new spectrum widths up to 100GHz. For alien wavelength support, MVACF only supports services terminated on the ENEs and can only interwork with MVAC configuration.

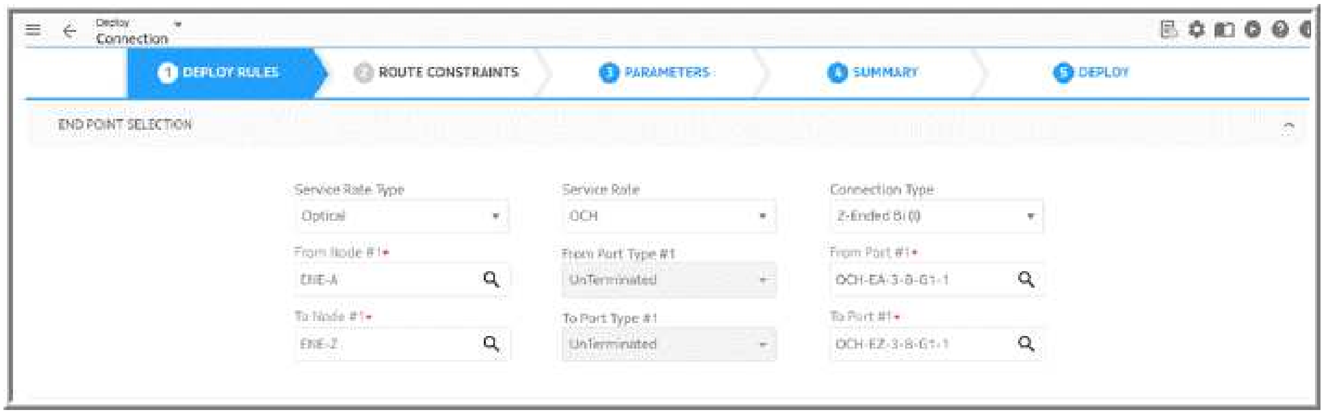
NFM-T supports, on MVACF, channel width at 37.5/50/62.5/75/87.5/100Ghz. This alien enhancement, for channel width setting and flex-grid support, is supported only by a new MVAC card called MVACF.

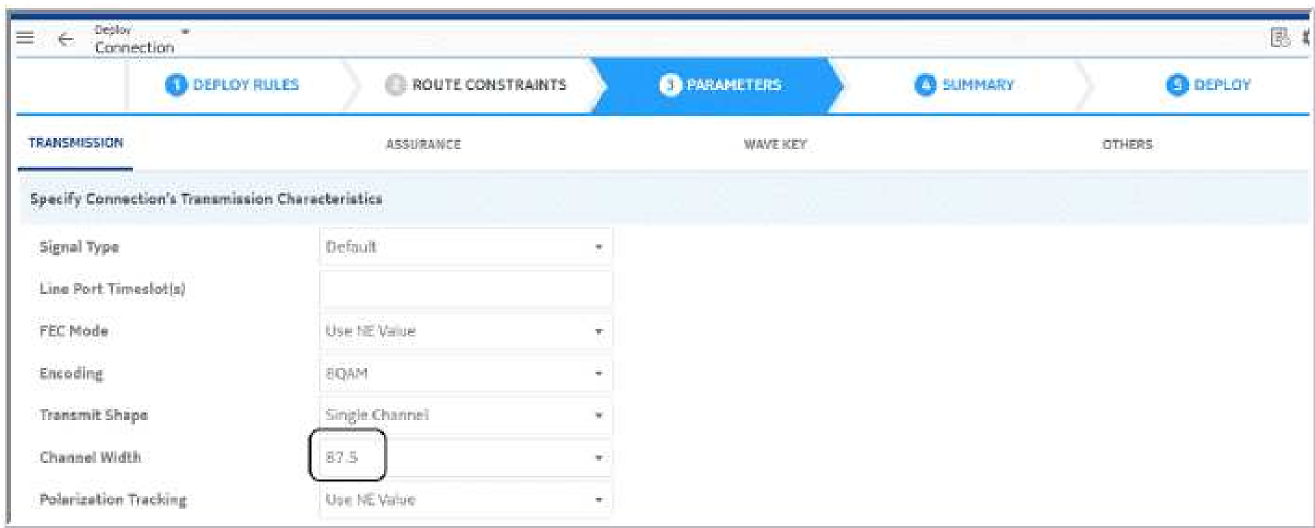
Note: 3R protected service (OPSA/OPSFlex OCHP), asymmetric service (one end ENE the other end managed NE) are NOT supported.

Provisioning flow

The flow to provision alien wavelength support with MVACF can be summarized in:

- Set up the core network (for example. CDC-F, C-F)
- Set up the add/Drop port from core network for MVAC to connect. For example the MLFSB MxDx port needs to be set up to OCH usage before being connected.
- Create the physical connection with **WDM Connection Type** set to `OPS` between ENE and MVACF pack (on both A and Z ends). See the procedure 7.19 "Create an OTN physical connection" (p. 784).
- Create the **OCH** Service terminated on the ENEs. See the procedure 8.4 "New service/ infrastructure connection" (p. 1219).





OCH infrastructure for alien/MVACF is supported in any photonic PSS architecture, in managed-plane and L0 GMPLS configurations. For L0 GMPLS alien over MVACF is a foreign connection. See "Foreign Connections" (p. 1413)

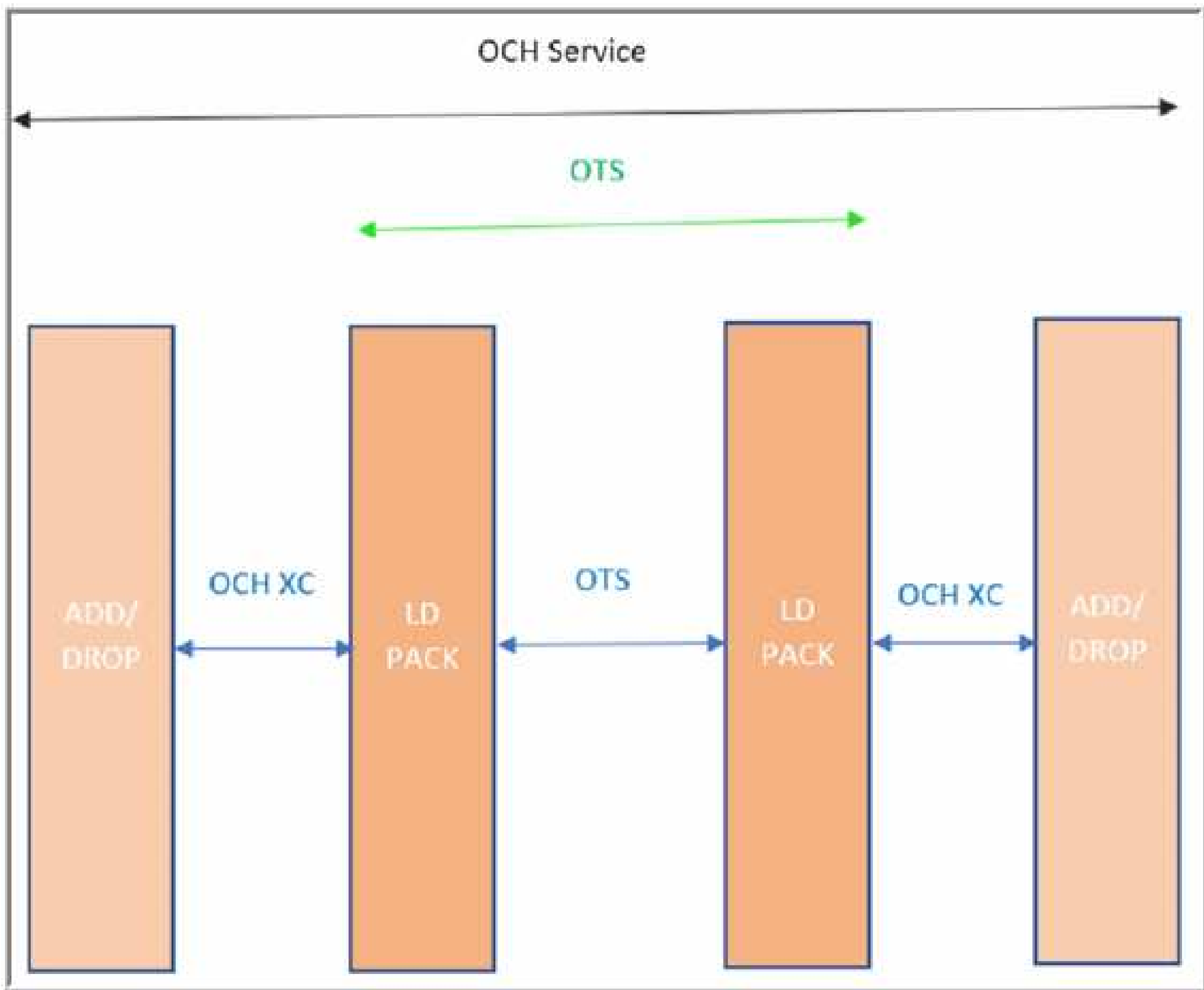
The provisioned services can be only symmetric, that is MVACF to MVACF.

2.57 Lightpath service

OCH service schema

The figure outlines the OCH service creation as lightpath for alien services.

Figure 2-96 Alien Management - OCH Service



Create an OCH service

The scope is to provision an OCH service without using Virtual NE or Black BOX. It is allowed to create a LightPath service ending on Add/Drop ports directly (SFD/PSC1:6/MCS/CWR/WR). It is still possible to use VNE/BBOX as endpoints for LightPath service.

To create the OCH connection follow the steps:

1

From the NFM-T GUI main menu follow the path **DEPLOY > New Service/Infrastructure Connection**.

2

Select the **/Best Practices/Infrastructure Trail/OCHP Protected** for **Alien Wavelength (OCH)** or **/Best Practices/Service/Transparent/Unprotected** for **Alien Wavelength (Unkeyed OCH)** template, and click **Deploy** to display the **Connection** template page.

3

Rate is automatically set to `OCH`.

Note: The following points are applicable for an OCH service:

- The possible endpoints are: SFD, MCS, PSC, CWR8, MLFSB, or IROADM9R.
- Only In-service service state is supported.
- PM is not supported.

4

From **Service Definition** tab, select **Channel Width** from the listed values, for example, *37.5, 50, 62.5, 75, 87.5* GHz. 50GHz is the default Channel width.

Note: Flex-grid is supported for the defined lightpath channel as 6.25 GHz slice.

Modify the route

Reroute for OCH services is not supported on SFD service pack. The end points are Add/Drop ports, so, to change the frequency user needs to change Add/Drop ports as well and this operation is not supported using the Modify Connection function. For the other service packs the function is supported.

Network Time Protocol (NTP)

2.58 NTP Description

NTP Definition

Network Time Protocol (NTP) is a networking protocol that is used to synchronize the clocks between computer systems over packet-switched, variable-latency data networks. NTP, which is an Internet protocol, is intended to synchronize all participating computers to within a few milliseconds of GMT.

NTP and NEs

The ability to configure NTP for an NE is available only if the NE and a particular release of the NE supports NTP.

When you set NE time, the system gives you the option of setting the NE time with current OS time. If the NE is associated with a NTP server, you cannot synchronize the NE time with the OS time. The time that is displayed in the Set NE Time window is converted according to the local terminal time zone. The time sent to the NE is GMT.

Table 2-14 NTP Sync Status

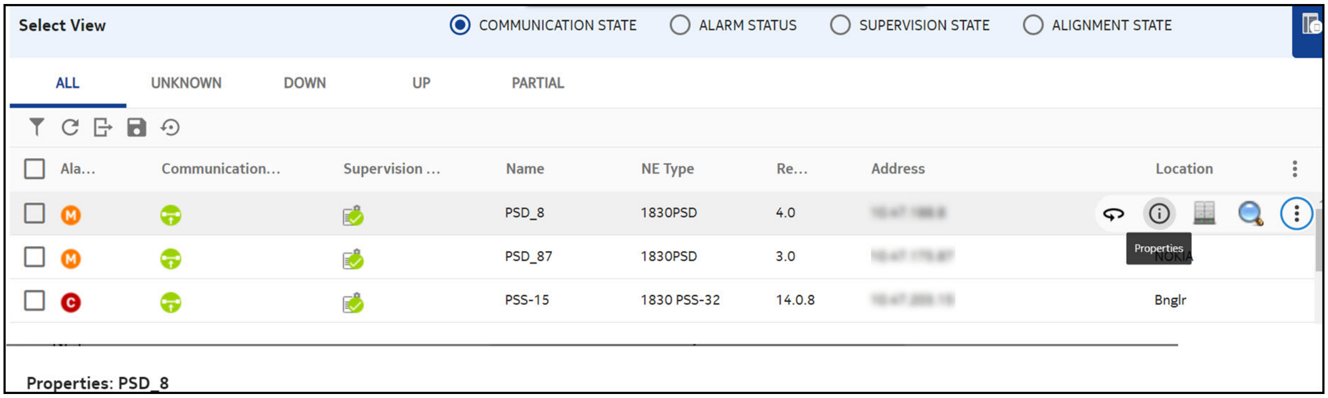
NTP server status	NFM-T reporting
Disconnected	Free running
Connected	SNTP sync
Unknown	Holdover

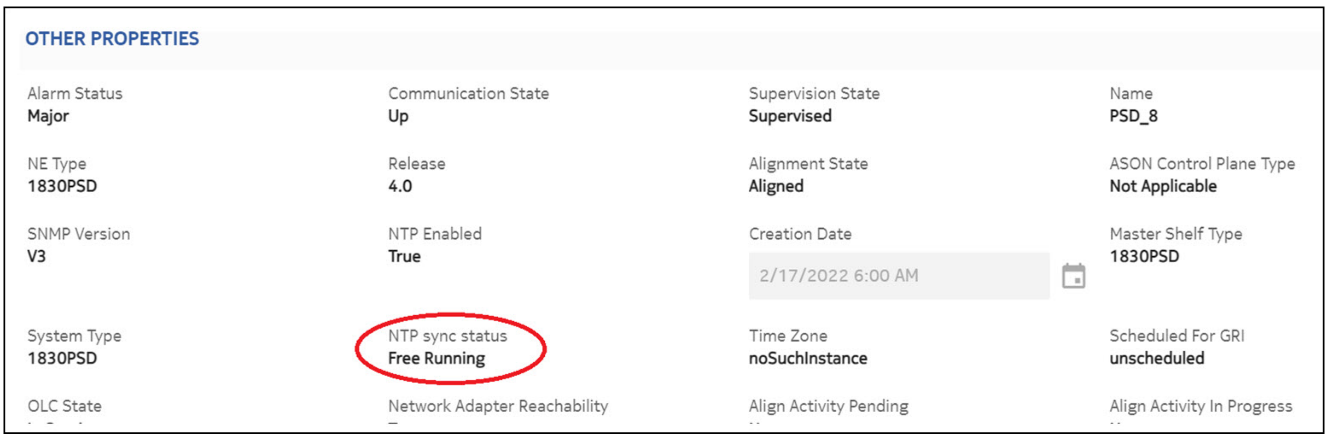
The user is allowed to view the *NTP Sync Status* for 1830 PSD, and 1830 ONE in the NE Properties. However, any change in the value of *NTP Sync Status* is not notified by the NE to NFM-T. The user is expected to do an NE Sync on equipment to get the updated value.

Table 2-15 NTP Sync Status - WaveLite

NTP Enabled	NTP Server Status	NTP Sync Status
Disabled	-	Free running
Enabled	All the available servers are disconnected.	Holdover
Enabled	One available server is connected.	SNTP sync
Enabled	More than one available server is connected.	NTP sync redundancy

Figure 2-97 NTP Sync Status - NE Properties





User Interaction with NTP Configuration

Users can perform following actions for the NTP configuration.

- 2.59 “Add or delete an NTP Server” (p. 358)
- 2.60 “Correlate the IP address of an NTP Server with an NE” (p. 360)

2.59 Add or delete an NTP Server

When to use

Use this task to add or delete an NTP server.

Related information

See the following topics in this document:

- 2.58 “NTP Description” (p. 356)
- See section Configure NTP on Nodes in the *NE Management Guide*

Before you begin

The ability to configure NTP for an NE is available only if the NE and a particular release of the NE supports NTP.

Task

Complete the following steps to add or delete an NTP server.

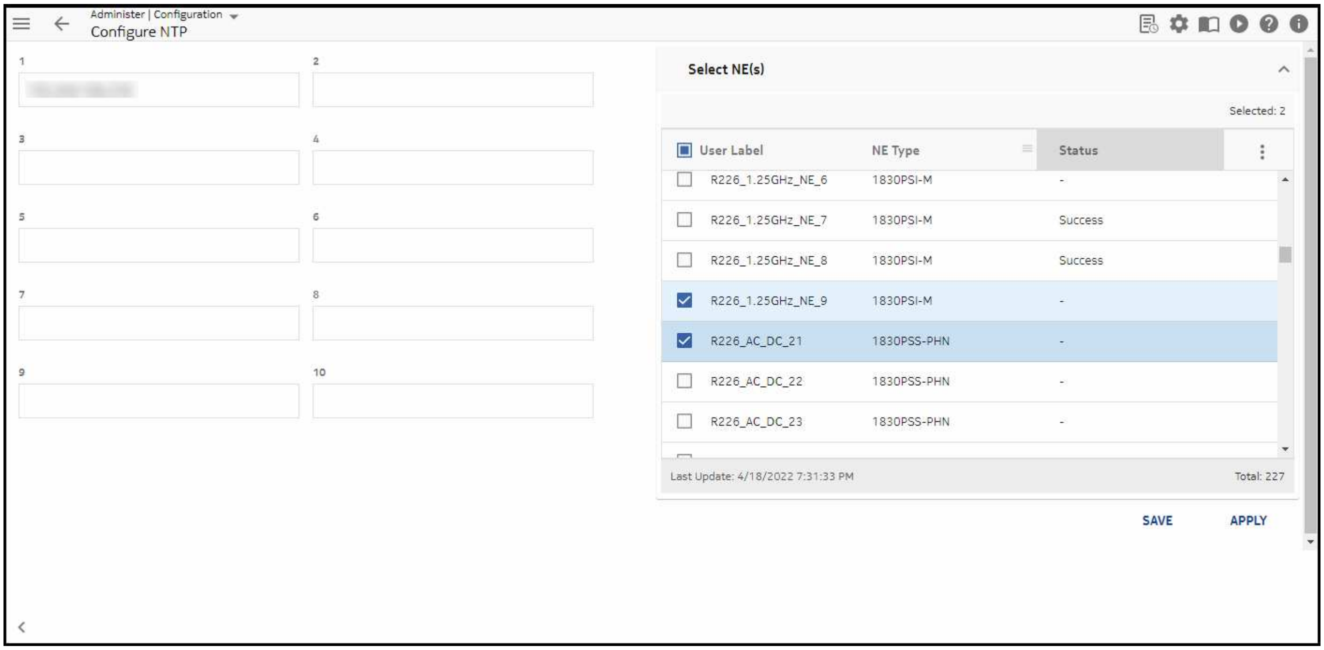
1

From the NFM-T GUI, follow this navigation path:

Administer > Configure NTP

Result: The system displays the Configure NTP page.

Figure 2-98 Configure NTP page



2

To add the IP address of a new NTP server, perform the following:

Enter the IP address of the server in the numbered field that is located in the left panel of the Configure NTP page and click **Save**.

Note: Maximum of three IPs can be configured for WaveLite NEs.

Result: The system outputs the following message in the lower right corner of the window:

`Success`

3

To delete the IP address of an existing NTP server, perform the following:

In the left panel of the Configure NTP page, click the IP address of the NTP server that is displayed in the numbered field, click the **X** that is displayed, and click **Save**.

Result: The system deletes the IP address of the selected NTP server.

END OF STEPS

2.60 Correlate the IP address of an NTP Server with an NE

When to use

Use this task to correlate the IP address of an NTP Server with an NE.

Related information

See the following topics in this document:

- 2.58 "NTP Description" (p. 356)
- See section Configure NTP on Nodes in the *NE Management Guide*

Before you begin

The ability to configure NTP for an NE is available only if the NE and a particular release of the NE supports NTP.

Task

Complete the following steps to correlate the IP address of an NTP Server with an NE.

1

From the NFM-T GUI, follow this navigation path:

Administer > Configure NTP

Result: The system displays the Configure NTP Settings window.

2

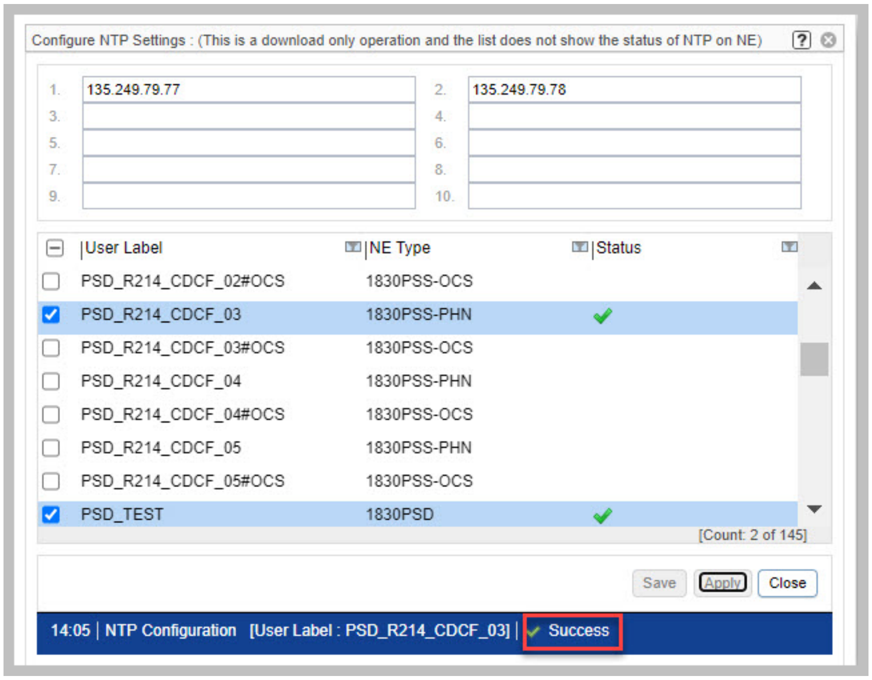
In the lower panel of the Configure NTP Settings window, perform the following:

• To correlate one NE or multiple NEs to an NTP server, click on the NE or NEs to which you want to correlate the NTP server and click **Apply**.

• To correlate all of the NEs to an NTP server, click the box next to the **User Label** field and click **Apply**.

Result: The system configures the selected NE or NEs to the NTP server and shows the success message in the lower panel.

Figure 2-99 Configure NTP – NTP Configuration Successful



Note: Configure NTP function has ten IP fields enabled, because it supports multi select option on NEs. If the user selects different types of NEs, that have different maximum number of NTP servers association possible, all the ten IP fields are enabled. If the user inserts ten IP addresses, the system assigns the servers for each NE until the maximum number of possible servers is reached for the different selected NEs

END OF STEPS

3 ASON Overview

3.1 Overview

Purpose

The purpose of this chapter is to introduce the fundamentals of ASON and GMPLS.

Contents

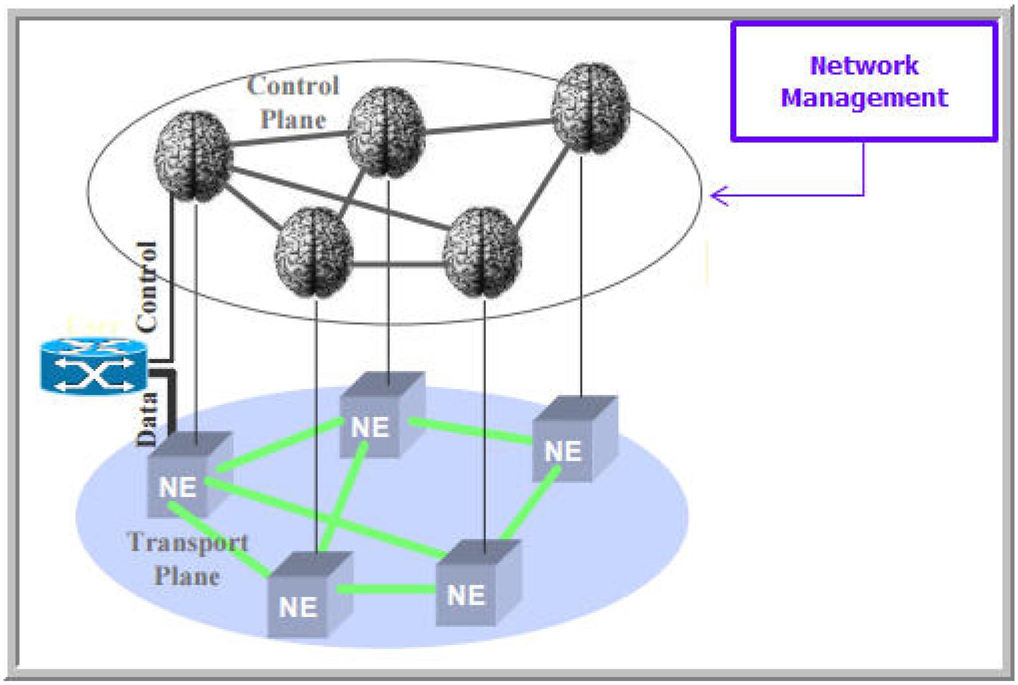
ASON Concepts

3.2 Introduction to ASON

Introduction

The Automatic Switched Optical Network (ASON) is both a framework and a technology. As a framework, ASON depicts a control and management architecture for an automatic switched optical transport network. As a technology, ASON refers to routing and signaling protocols applied to an optical network that enables dynamic connection creation and life cycle management.

Figure 3-1 ASON as a Smart Network



Traditional networks consist of two operating planes: the management plane and the transport or the data plane. In this architecture, the data plane carries the user data. The data plane consists of various network equipment, such as interface cards, switching equipment, and the fiber plant. Network operating information is managed by the management plane consisting of the Element Management System (EMS), the Network Management System (NMS), and the Operation Support System (OSS). With the advent of optical networks, a third operating plane was added. The optical control plane is located between the management plane and the data plane and helps to move some network intelligence down to the Network Elements (NEs). As a result of adding the optical control plane, the NEs have access to the overall topology of the network and the available resources allowing the NEs to participate in the planning, establishment, and maintenance of network services for the end user.

Figure 3-2 Operating planes for an optical transport network

The control plane offers several benefits to the carriers:

- Provides faster and less labor-intensive service provisioning.
- Provides efficient and cost-effective network restoration.
- Supports new dynamic service provisioning: Reduces time from a Service request to Service Delivery.
- Network efficiency and resilience – supports mesh topologies and dynamic service restoration: Network processing and distribution of restoration improves Time-To-Repair.
- Reduces OPEX cost - decreasing operator workload, reducing service turn-up fallout, and supporting multi-vendor inter-operability.

Network

An ASON is an *intelligent* optical network that can automatically manage the signaling and routing through the network. Traditionally, it was necessary to configure cross-connections in the NEs (such as an optical switch) to create a new traffic connection for a customer.

In an ASON framework, this process is automated. The user defines a new connection by its start and end point, the bandwidth needed, the Quality of Service, and so on. The Network Elements have the necessary processing functions built in to configure the new traffic connection. The connection itself is not specified by the user. The ASON network creates a light connection through the network for this customer. This traffic connection is changed if the network is changed.

ASON uses the Generalized MPLS (GMPLS) signaling protocol to set up and monitor edge-to-edge transport connections. ASON concentrates on the optical backbone network.

Switching technologies used in ASON ranges from simple fiber switching to wavelength (λ) switching to optical packet switching. The components required for the switching are optical cross connects (OXCs), wavelength converters, and optical Add/Drop Multiplexers (OADMs).

ASON is a control plane architecture allowing a policy driven control of an optical network using signaling between the NEs and between users and NEs of a network. Its objective is to provide automated control functions for network resources and connections. The main objectives of an ASON network are:

- Automated end-to-end provisioning

- Automated re-routing for protection and restoration
- Dynamic setup of connections
- Enable different levels of quality of services

Control Plane Applications

Most optical control plane applications focus mainly on the services that perform connection management for the transport plane for both the packet-based services and connection-based services. The main functions of a control plane are:

- Routing control
- Resources discovery
- Connection management
- Connection restoration
- Resource management

Routing Control

The routing control function is responsible for selecting the combination of links to be used for a given connection, based on the network topology and routing criteria that is provided. Common route selection criteria are shortest path, lowest cost, fewest hops, and least congested. This function is triggered by a connection management function request and utilizes the network topology populated by resource discovery function.

Resource Discovery

The resource discovery function keeps track of the system resource availability such as bandwidth, multiplexing capability, and ports. It is responsible for the discovery of neighboring nodes and the links connecting them, and the communication of this information to all relevant elements. It maintains the neighbor and link information and updates this in real time. This information enables all the elements of the control plane to have an accurate topology map of the network to be used for connection management and routing control functions.

Connection Management

Connection management functions provide end-to-end service provisioning for different services as requested by the end users. The services include connection creation, modification, status update, and tear down. Connection management functions perform connection computation based on parameters provided by the carriers. For example, connection computation could establish a requested connection based on the lowest cost. Other parameters could be bandwidth requirements, wavelength continuity, maximum allowable latency, and optical characteristic allowable for the bit rates to be carried. Connection computation is used to calculate diverse routes needed for restoration.

Connection Restoration

Connection restoration function provides an additional level of protection to the network by establishing for each connection one or more pre-assigned backup resources. This pre-assigned connection allows for quick restoration in case of a network failure.

Resource Management

Resource management is the function of controlling the utilization of resources based on network design parameters. It includes the formation of the Traffic Engineering (TE) database, based on the network topology and the real-time utilization of each link and node. The database makes it possible for the routing control function use the existing utilization of a link as criteria for routing. Resource management, in addition to maintaining an accurate record or utilization, typically includes the ability to reserve capacity for a particular purpose (such as capacity reserved for protection of active connections) or connection that is not yet active (such as a new customer circuit to be turned up at a certain time).

Control Plane Standards

When intelligent optical networks first arrived on the market, every implementation utilized different control plane architectures, to support varying functions, using proprietary protocols. Due to the fact that network operators typically included equipment from multiple suppliers (either by design or acquisition) and suppliers wanted to sell standards based products globally, work was started to standardize the optical control plane. There were parallel efforts in multiple standards development organizations and forums, but the International Telecommunication Union Telecommunications Sector (ITU-T) first defined a clear architecture and a standardized set of functions for an optical network.

The optical network with an active control plane between was labeled an ASON and the ASON architecture was defined in ITU-T Recommendation G.8080/Y.1304.

ASON is a standardized network architecture. The set of functions for automated resource and connection management within the network are driven by the dynamic signaling between the users and the ASON network elements. Although the acronym ASON implies applicability to optical networks, it is general enough for application to any network layer where connections (static or virtual) are used. Implementers of the ASON control planes chose to reuse existing protocols from the Internet Engineering Task Force (IETF) for the control plane messages and agreed to a protocol based on Multi-Protocol Label Switching (MPLS).

3.3 ASON/GMPLS control plane

Overview

GMPLS is the protocol defined to support a control plane based on the ASON architecture. Specific capabilities that fit under the ASON architecture are defined for GMPLS. The fundamental service provided by an ASON/GMPLS control plane is dynamic end-to-end connection provisioning. The user can specify the connection parameters and send them to the ingress node. The network control plane can then determine the best optical connections across the network according to the parameters, and signal the adjacent nodes to establish the connection. ASON/GMPLS functions in multi-layers optical networks. It is used for traffic grooming on edge nodes when applied across a two-layer network.

For example, consider an optical wavelength routed in an optical network and an *optoelectronic* multiplexed layer over it. When a transparent light connects in the optical layer (operating strictly at wavelength granularity) to physically adjacent or distant nodes, these nodes seem adjacent to the multiplexing layer. The multiplexing layer can then multiplex the different traffic streams into a single wavelength-based light connection. It can also demultiplex different traffic streams from a single light path. At a multiplexing node, some of the demultiplexed traffic can also be remultiplexed into different light paths using a GMPLS-based control plane.

GMPLS includes the definition of several forms of labels: the generalized labels suitable to be used with wavelength based optical networks. These objects include the generalized label request, the generalized label, the explicit label control, and the protection flag. The generalized label can be used to represent time slots, wavelengths, wave bands, or space-division multiplexed positions. To set up a light path, GMPLS uses a signaling protocol to exchange control information among the nodes in the network, to distribute labels, and to reserve resources along the connection. Signaling protocol to be used for the GMPLS control plane includes Resource Reservation Protocol (RSVP). RSVP can be used to reserve a single wavelength for a light path if the wavelength is known in advance. Open Shortest Path First (OSPF) can be used over GMPLS as a routing protocol to keep track of link states and select link as requested by users, management plane, or triggered by control plane functions. GMPLS also uses the Link Management Protocol (LMP) to communicate proper cross-connect information between the network elements. LMP runs between adjacent systems for link provisioning and fault isolation.

In addition to the service-related advantages of using a control plane, the most important function of a control plane is to provide efficient and cost effective restoration for optical networks. In view of the current implementation of 40G and 100G systems, restoration becomes critical for future optical networks. The efficient ASON/GMPLS based control plane incorporated with the management plane provides not only new and better network functions, it also helps the carriers explore new revenue streams as well as save network and operational costs.

Figure 3-3 GMPLS/ASON key features - 1

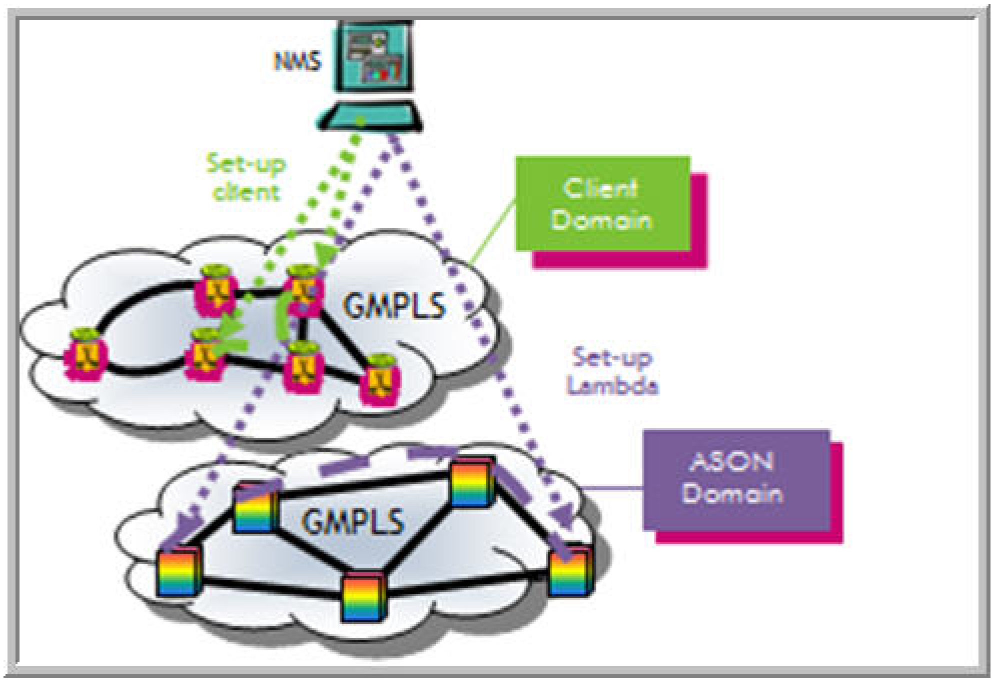
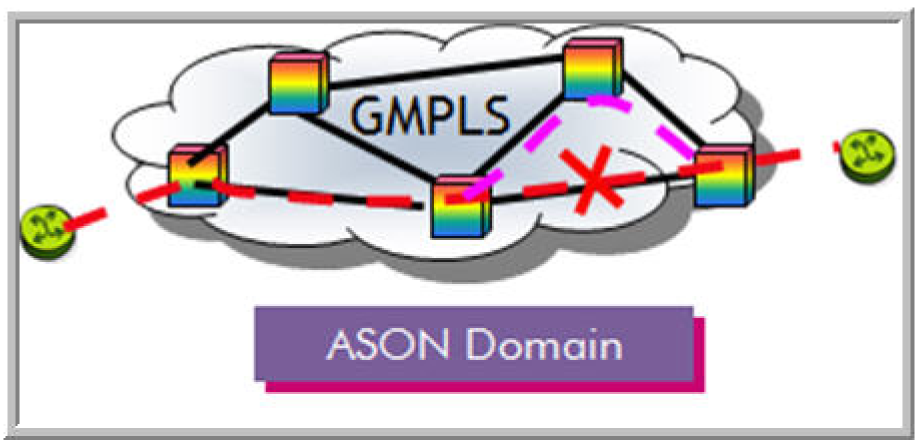


Figure 3-4 GMPLS/ASON key features - 2



The key features of GMPLS are:

- Network and Resource Discovery: Eases the installation and commissioning process

- Dynamic Provisioning: Supports bandwidth-on-demand services & end-to-end provisioning: Connection set-up triggered through the NMS (soft permanent connections)
- Distributed Automatic Restoration
  - Enables sharing of protection resources in the network
  - Differs from traditional protection schemes (MS-SPRING, SNCP or MSP) where protection resources are dedicated and already assigned, so that they cannot be used to protect other circuits or links
  - GMPLS alarming: Specific GMPLS alarms in case of restoration (reroute), reverse to nominal (ready to revert), APE in progress (for optical tuning)
- Maintenance features
  - Possibility to modify nominal routes
  - Possibility to move away traffic from a link in case necessary a maintenance on the link

The GMPLS protocol suite mainly consists of the following protocols:

- Routing protocols (OSPF-TE)
- Signaling protocols (RSVP-TE)
- Link Management Protocol (LMP)

Routing protocols

In general, routing protocols (OSPF-TE with GMPLS extensions) are used to exchange topology and reachability information between GMRE nodes to allow each node to build its own topology map of the entire network or subnetwork. A topology map basically consists of node-related information and link-related information which is then stored in a topology database.

Each node periodically disseminates node-related information describing the node itself (local state information). Furthermore, it disseminates link state information describing its local links (leading to one of its adjacent neighbors). The routing information, a node periodically receives from each of its neighbors, is used to update its local topology database, and is further advertised to all other adjacent neighbors. This mechanism implemented in routing protocols ensures, that each node in the network repeatedly obtains information describing all the nodes and links in the network so that it is able to build its own topology map of the entire network or subnetwork.

In the path establishment process, the GMRE node uses this information to calculate a route from a given source to a given destination or to determine the *next hop* leading into the direction of the given destination.

Signaling protocols

Signaling protocols (RSVP-TE with GMPLS extensions) are used to exchange information between neighboring nodes mainly for the purpose of establishing or releasing a path across the network or subnetwork. Thus, when a new path is being established, the signaling messages have to be processed in every node along that path.

Signaling protocols facilitate the establishment of a link connection over a particular transmission link between a pair of connection points. For this purpose, they convey the assigned labels between each pair of neighboring nodes to support the label allocation procedure.

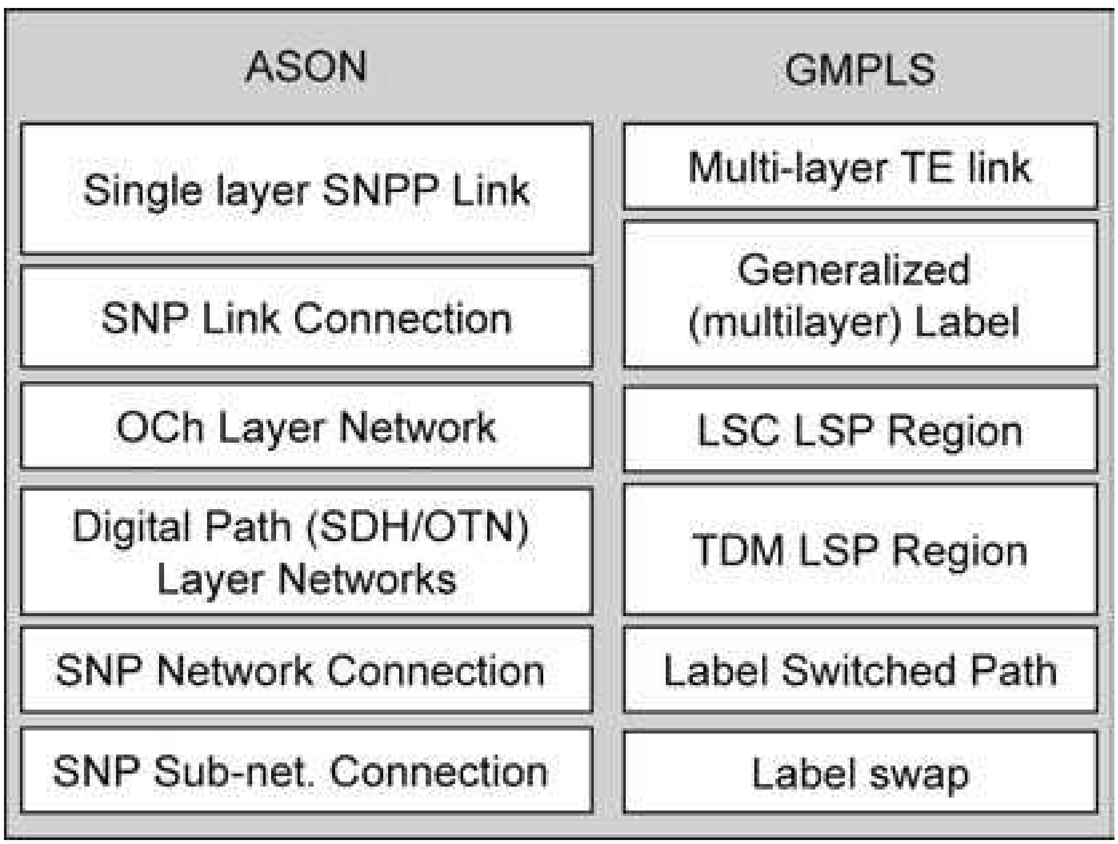
Link Management Protocol (LMP)

The Link Management Protocol (LMP) extends between the neighbor NEs and is used to manage the TE links. Furthermore, it supports the supervision of control channel connectivity and verification of the physical connectivity of the transmission links.

Control plane architecture

GMPLS makes no assumptions regarding the control plane architecture. It implicitly assumes the existence of the routing (OSPF, ISIS), the signaling (RSVP, CR-LDP), and the LMP controllers. These communicate with their peers and exchange the particular protocol information performing the tasks of connection control, call/connection control, and resource discovery. Network state information is contained in MIBs. This information is partially configured from the management system or updated as a result of automatic actions performed in the control plane. The architecture of a GMPLS control plane is inherently protocol-specific. On the other hand, the ASON control plane architecture is specified in a protocol neutral way. Control Plane functions are modeled by control components with generic functional interfaces organized in federations. Components are configured and monitored, and their behavior is changed by applying policies. ASON specifications introduce a set of control components responsible for call control, connection control, and resource discovery.

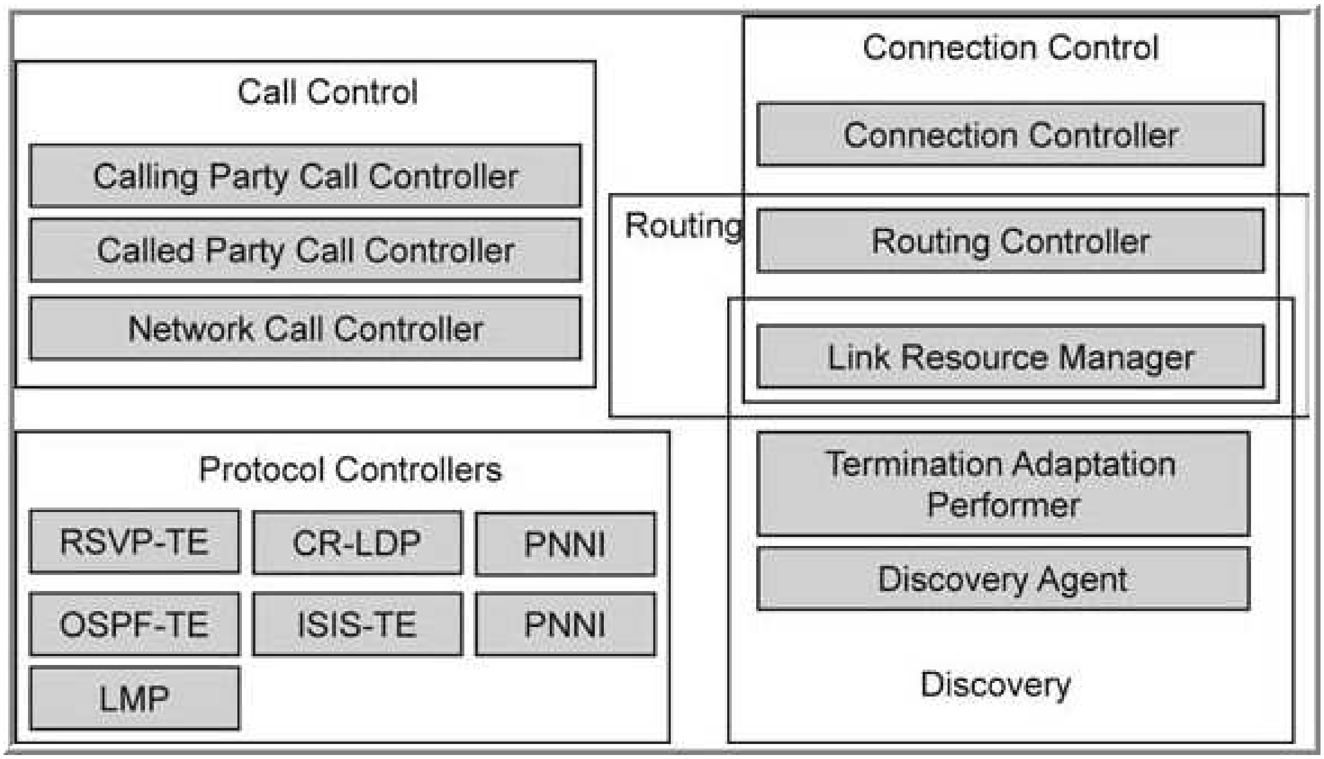
Figure 3-5 Mapping between GMPLS/ASON resource models



In addition, the ASON architecture includes specific Protocol Controller (PC) components responsible for translating functional primitives defined on the generic interfaces of control components, into protocol messages of a suitable protocol implementation. Protocol messages are transported in the control network over the control plane interfaces.

The ASON protocol neutral control plane architecture enables a generic approach for defining and understanding requirements and for validating potential solutions. However, the aim of ITU-T is not to define some new protocols but to incorporate the GMPLS protocols and other valid candidates in the ASON framework retaining the visibility of the generic requirements. GMPLS protocols are represented within the protocol control components as outlined in the Figure 3-6, “ASON control processes and components” (p. 371).

Figure 3-6 ASON control processes and components



Functional components and planes

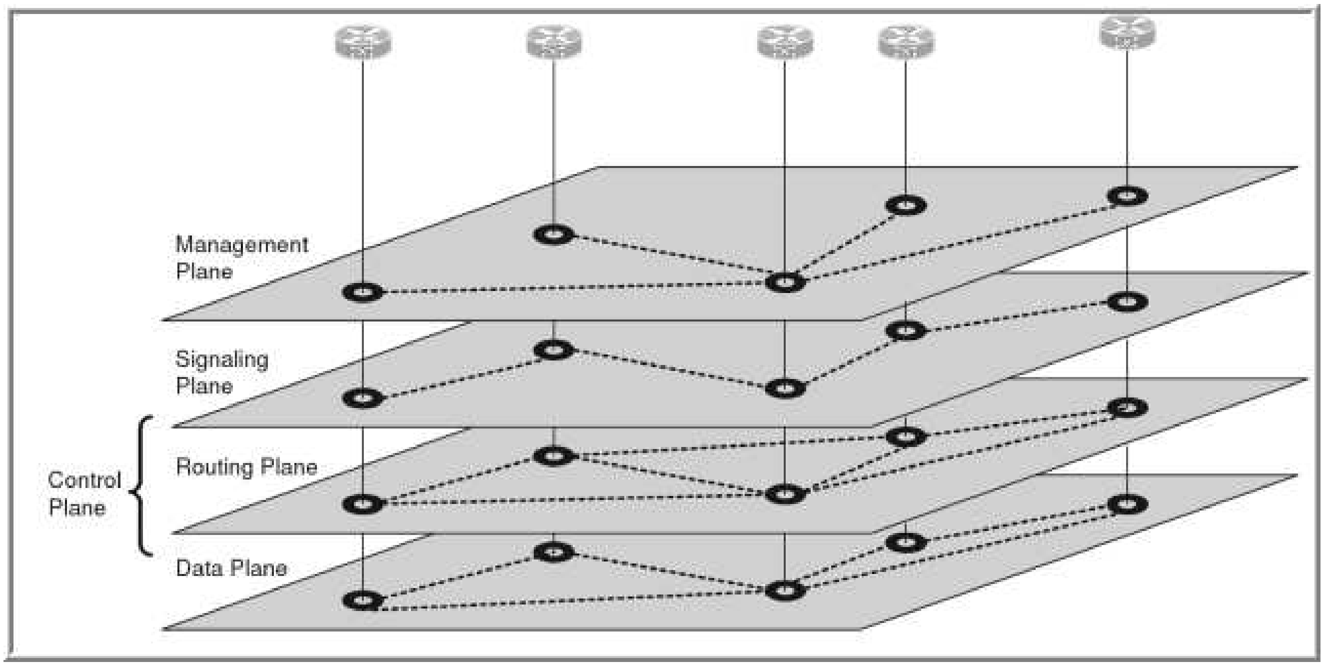
There are many functional components in the network nodes. This makes it possible to build a more coherent architectural model, but also makes it easy to understand the roles that particular networks nodes play and how they communicate.

For example, one functional component has the responsibility for managing network nodes, and another provides the management support within a network device such as a router. These components would possibly be positioned at remote sites within the network (the Network Management Station and the router itself) and communicate with each other across the network.

When a network is seen partitioned into these functional components, messages and information move around the network between components with the same, or related, functional responsibilities. The example of communications between management components cited in the previous paragraph is one illustration. Similarly, the data-switching components of network nodes process data and distribute it among themselves. If we follow up this idea, we see that the network may be sliced into sets of functional components that communicate with each other and all of which have related responsibilities. These slices are called *planes*.

The communication between the planes takes place only within a network node; communication between the network nodes take place only within a plane. For example, the management component on one node does not interact with the data processing component on another node.

Figure 3-7 Functional interaction between network nodes within a set of planes



The above Figure 3-7, “Functional interaction between network nodes within a set of planes” (p. 373) depicts a simple network divided into the four planes. Data is moved between the devices within the data plane, so the connectivity in this plane is a direct representation of the physical data links in the network. The management plane is responsible for all management activity, such as configuration requests, statistics gathering, diagnostics, and so forth. The signaling plane and the routing plane are sometimes grouped together and referred to as a control plane. The routing protocols dynamically distribute connectivity and reachability information. The TE resource attributes operate in the routing plane, where the signaling path exists.

The data plane is sometimes referred as the user plane or the transport plane, because it carries user traffic. The application plane facilitates communication between applications. The vertical lines represent the presence of each network node across all the planes. The dotted lines represent the communication relationship within each plane. In the data plane, the communication services map to the actual physical connection in the network, however, in the other planes the communications use logical connections to form associations between the network nodes. For example, the management relationship is shown with a single management controller, the routing relationship is shown as a mesh, and the signaling relationship is shown as linear.

Exchanges between the planes take place along the vertical nodes, that is, at the network nodes, which is as follows:

1. A management plane request is sent from a management station to an MPLS router through the management plane.
2. At the router it is converted to a signaling request that is sent hop by hop through the network in the signaling plane.
3. At each hop in the network, the MPLS router programs the data plane.
4. The end result is a data path through the data plane on which data can be sent.

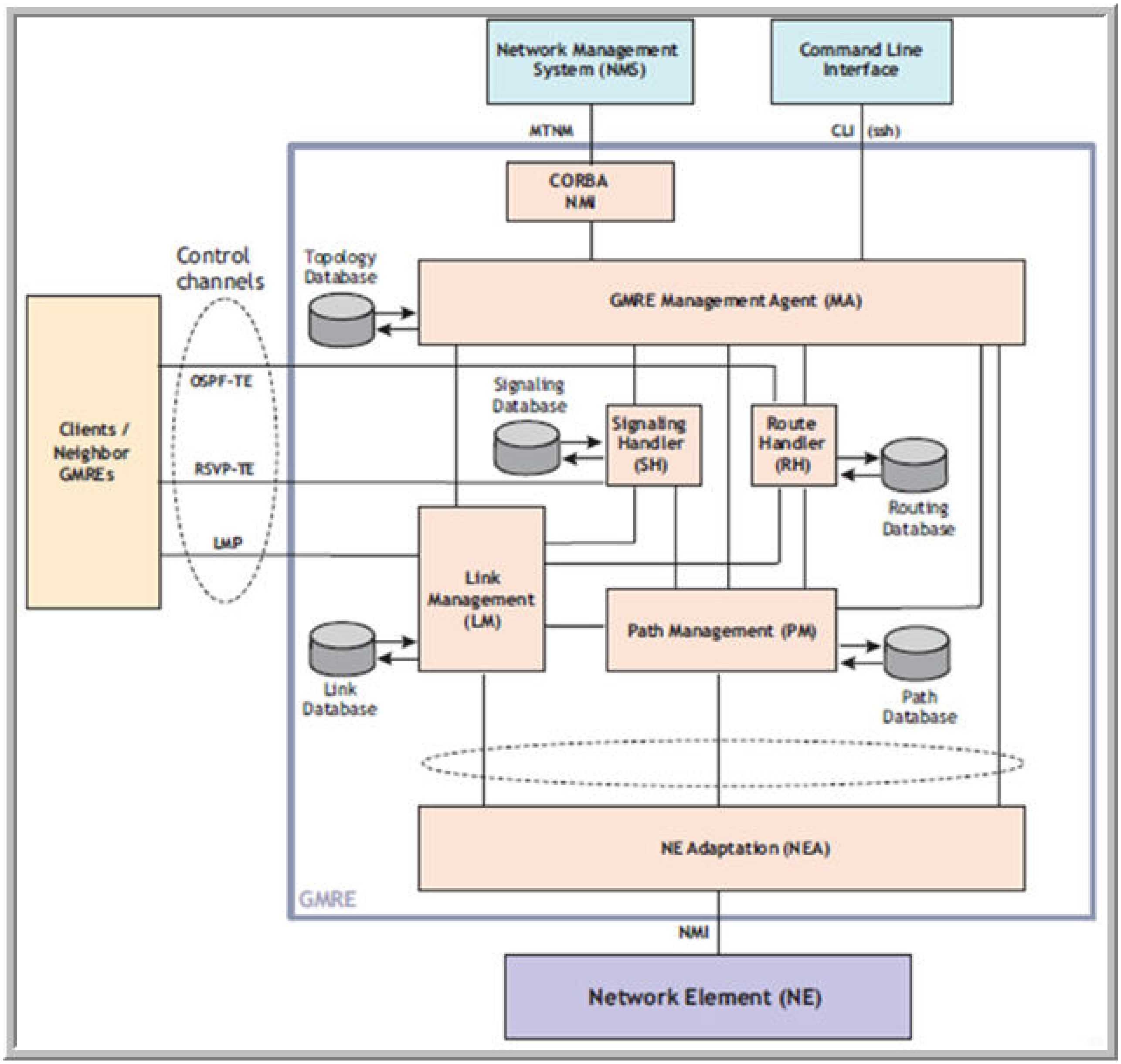
The GMPLS protocol family operates within the control plane. However, the interaction with the data management planes are also of fundamental importance to the way in which GMPLS works.

3.4 GMPLS Routing Engine

Introduction

Each transport NE (TNE) is equipped with a controller called GMRE which runs the GMPLS protocols. The GMRE is a software package that is activated on the basic NE software on the Controller card, First-Level Controller (FLC) in case of 1830 OCS, Equipment Controller (EC) in case of 1830 WDM. No additional hardware is required for the implementation of the GMRE.

Figure 3-8 GMRE top-level architecture



GMRE architecture

The basic elements of the ASON networks are the GMRE nodes. The GMRE nodes are designed to implement the GMPLS architecture.

In the GMRE nodes reside a set of processes implementing the control plane (Signaling, Routing, link and path management). Those processes interact with the NE MIB through a specific interface and with the Management Plane through a dedicated interface. The Management Plane is represented by the NMS or a simple user command line interface (CLI).

GMRE is capable of establishing as Soft Permanent Connections (SPCs) between TTPs.

For more information on GMRE architecture, see *1830 PSS GMPLS Control Plane Guide*.

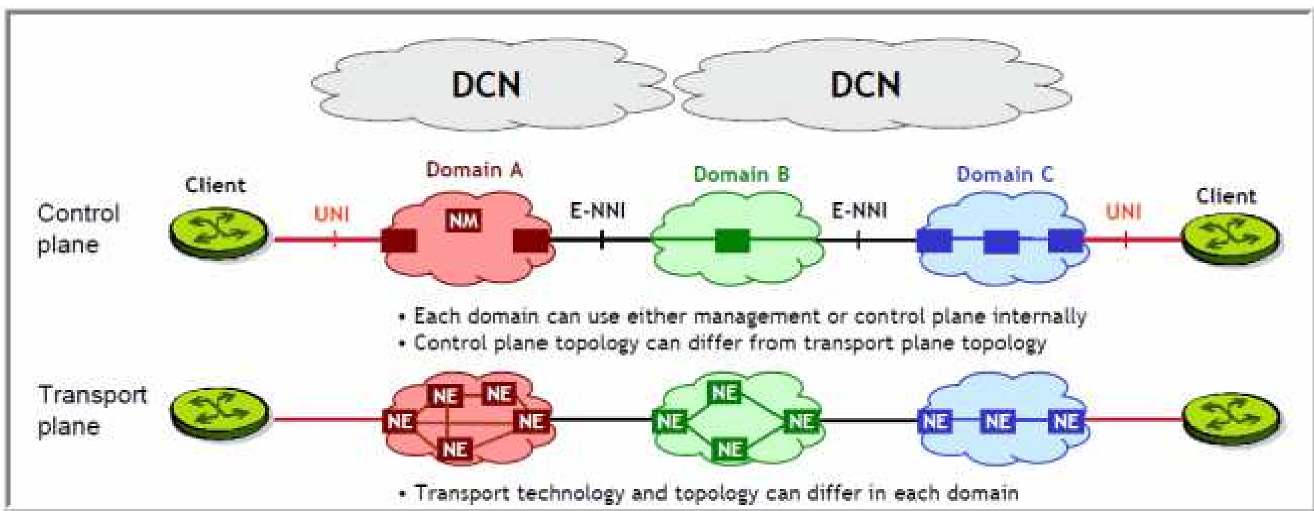
3.5 ASON architecture concepts

ITU key ASON architecture requirements

The ITU ASON requirements are:

- Supports heterogeneous network topologies, technologies, and applications.
- Supports control plane or management plane subnetworks.
- Provides boundaries of policy and information sharing.
- Supports varying trust relationships among users and providers.
- Provides functional independence between control plane, data plane, and the management plane.

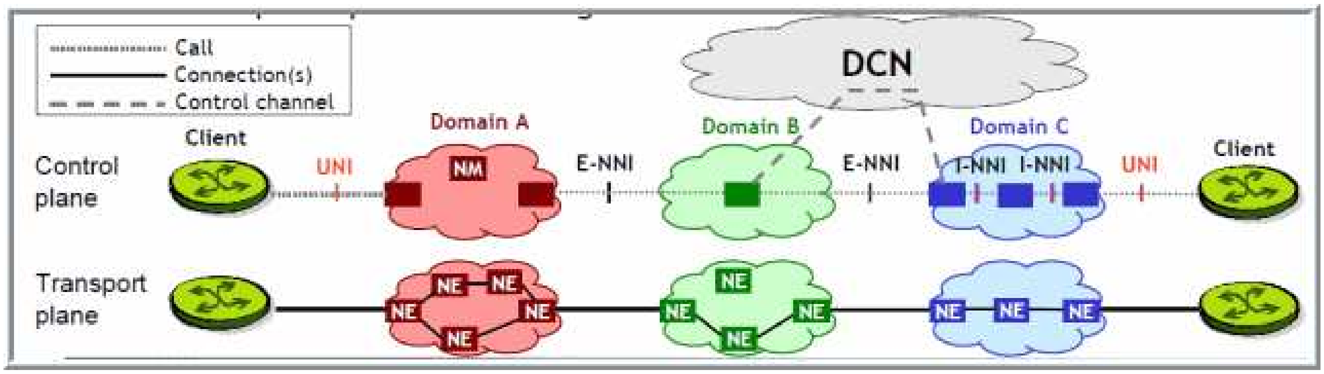
Figure 3-9 ASON Architecture Requirements



Key ASON architecture concepts

- Call/connection control: The call is a service activation mechanism in control plane and may be associated with 0, 1 or more connections in the transport plane. It states the level of service required (for example, QoS, protection, and so on). Calls does not provision any network resources to carry data for the service. The connections carry the requested services in the transport plane.
- Networks are partitioned into *domains* by network operator policies.
- Service demarcation and reference points are defined within and between the domains, and between a provider network and a user/client.
- A control channel (CC) is a communication connection in a DCN supporting exchange of control plane protocol messages.

Figure 3-10 Key ASON Architecture



ASON and the NFM-T

3.6 ASON concepts applied in NFM-T

ASON in NFM-T

ASON, which is an *Automatically Switched Optical Network*, is a network that can automatically manage the signalling and routing of a connection through an optical (for a GMRE Level 0 Control Plane) or electrical (for a GMRE Level 1 Control Plane) network without input from a user or a management system, which is an important function if a failure occurs within the network. If a failure does occur within the network, service is quickly restored by using the spare capacity that is already available in the network; therefore, minimizing the amount of protection capacity that is needed in the network.

ASON relies on *Generalized Multiprotocol Label Switching*, or the *GMPLS* protocol, to reroute traffic dynamically around a failure. Once the failure in the network is repaired, the connection is returned to its original route automatically or upon demand depending on the connection settings.

If the network is equipped with a *Generic MPLS (Multi-Protocol Label Switching) Routing Engine (GMRE)* module, the 1830 PSS NEs have the necessary processing functions to acknowledge the GMPLS protocols for the signalling, path management and the link management that are needed to create ASON.

The NFM-T is able to manage distributed restoration network defining a network protection architecture (NPA) of type ASON, the NE available with control plane are 1678Mcc, 1830 PSS 32, 1626LM R6.x, and 1830 PSS-64/36. All the NEs are not managed in the same way.

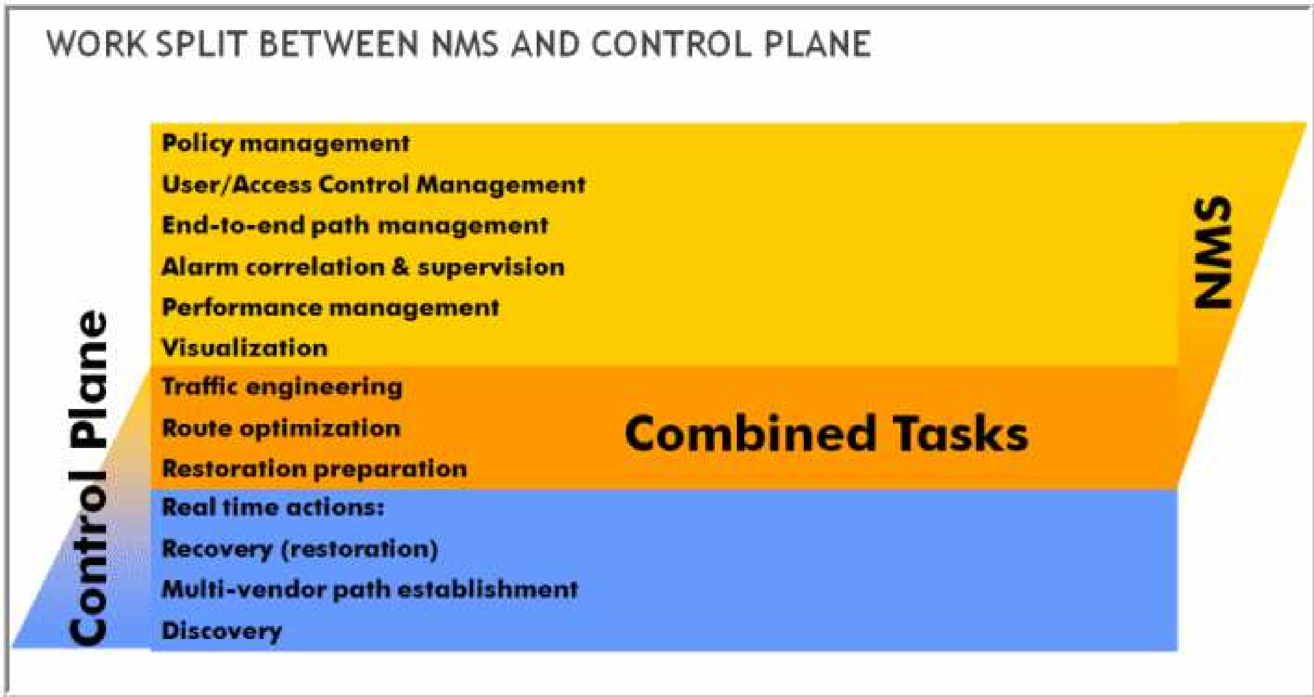
The Control Plane is discovered during the NE upload and a specific object, with a specific icon, is associated to the node. The status of reachability, management of control plane alarms, visible attributes in the proprieties, the navigation towards the Control Plane and the CLI are the salient features of ASON.

Control plane

ASON GMRE supports photonic switching (L0) and electrical (L1) switching. In NFM-T ASON domain is represented by the NPA.

The following figure summarizes the main concepts of the NMS/Control Plane cooperation in ASON, identifying the NMS and GMPLS functions, and the tasks where the two managers overlap and perform operations in a coordinated way.

Figure 3-11 Work Split between NFM-T and Control Plane



These physical links represent in NFM-T the links of inter-working between the two managers for the ASON SNC routed in ASON domain. The port at the end of the drop link and I-NNI link and belonging to the shared NE represents the *shared* port.

The TPs on a shared port can either be completely managed by the NFM-T or managed by both the NFM-T and the GMRE, according to the routing of the ASON SNC involving the TP.

Both managers operate on the TP: NFM-T is in charge of all the normal operations on the TP, apart from the set up of the cross-connection, set up by GMREs, and dynamically changed according to GMRE's restoration strategies.

Physical links and the NEs of the ASON network are represented in the NFM-T as ASON links and the nodes.

NFM-T provides to GMRE the description of the network belonging to the ASON domain and the links at the boundary of that domain (inter-working links). These links connect shared ports.

NFM-T, for maintenance purposes, manages the physical and the Multiplex Section layers (linear MSP included).

On the I-NNI links, NFM-T can apply the payload structure. In the ASON domain, the payload structure is defined by the GMRE as a consequence of a SPC (Soft Permanent Connection) set up by the NFM-T.

Important! NFM-T user must perform the payload structure on the internal links to allow connection allocation activities. However, the command is not propagated to GMRE.

On connection setup phase, NFM-T provides the setup of the SNC in the ASON domain with the help of GMRE, between the two TPs of the shared ports. GMRE is in charge of restoring that subnetwork connection in case of any failures.

While the TPs ends of the above subnetwork connection are chosen by NFM-T, the other TPs involved in the cross-connection inside the shared NE, are moved by GMRE as per the restoration purposes.

The setup of the single cross-connections inside the NEs belonging to the ASON domain (included the shared NEs) is done by GMREs. For all the other operations at path layer (POM, TCT, PM, path trace), NFM-T is the master for the TPs on the shared ports, while GMRE is the master for the TPs of the ASON domain.

As a consequence, ports dedicated to the inter-working between NFM-T and GMRE are marked as "shared". Each manager is able to distinguish between ports on which all the normal operations are allowed because completely "assigned" to it and ports on which only specific operations can be performed because "shared".

The NFM-T provides management for both of the following:

- An *optical GMRE Layer 0 (L0) network* at the optical OCH/OTU/ODU connection rate for 1830 PSS WDM/photonic NEs.
- An *electrical GMRE Layer 1 (L1) network* at the electrical ODUk connection rate for 1830 PSS Optical Cross Connect System (OCS/switching) NEs.
- A *Multi Rate Network – MRN* with coordination of coexisting L0/L1 GMPLS overlay network.

For the user provisioning of a GMRE L0 WDM/photonic connection or a GMRE L1 OCS/electrical switching connection in an 1830 PSS network, the NFM-T supports the following plane domains:

- The *Control Plane* is the operating plane in which pure ASON connections enable the network to reroute connections if a failure occurs, provided the NE has the necessary processing functions to acknowledge the GMPLS protocols for signalling, connection management, and link management.

  With the NFM-T, the Control Plane is a generalized term that is used to represent the portion of the network or a connection that uses ASON/GMPLS. The Pure Control Plane connections are infrastructure connections that originate and terminate in ASON.

  For GMRE L0 Control Plane provisioning on the 1830 PSS WDM/photonic NEs, the OTUk is provisioned in parallel by the network when the ODUk provisioning is done. For GMRE L1 Control Plane provisioning on the 1830 PSS OCS NEs, the base network is build up until the connectivity between the 1830 PSS OCS network is established at a rate that supports the ODUk Control Plane layer rate. Any optical connectivity that is present in the network via 1830 PSS WDM/photonic NEs is established first to provide connectivity between the 1830 PSS OCS NEs.

  For both GMRE L0 and GMRE L1, the overall process of establishing connections follow the G.709 standard. Each layer rate is established in the network starting with the physical network.

Both ASON layers cannot be active in the network at the same time; the network is designed to have either GMRE L0 or GMRE L1 active at any given time. Once the NFM-T network is provisioned, connections can be rerouted depending upon the occurrence of different failure conditions.

The role of NFM-T for ASON Networks are as follows:

- Network Setup and Topology configuration (NPA, TE-Links, SRGs)
- Network Configuration: Path Computation and deployment of SPC for the following:
  Connections terminating within the domain (I-NNI links)
  Interworking with non-Control Plane networks and seamless management
  MRN (Mixed L0/L1) Control plane Connection
- Manage life-cycle of SPC for Operation Maintenance and Bandwidth Management
  Modification of Nominal Route, Switching, and Reversion to Nominal Route
  Move traffic
- Planning and Maintenance of Network via Graphical and 360 degree Display of SPC
  Visualization of the Nominal and Current/Backup route on network maps (2D/3D Map)
  Determination of bandwidth usage with respect to Nominal And Current Route
- Fault Management analyzing the “root cause” of ASON alarm – view Control plane and Transmission Alarms Together

• The *Managed Plane* is the historically traditional operating plane technology where the NMS is used to set up the connections in the network along with any existing protection services. The network itself does not reroute any connections.

  Pure Managed Plane connections are infrastructure connections or services that are provisioned outside of ASON, which is the traditional method of managing connections within a network.

• The *Mixed Plane* is the operating plane in which its connections have a Managed Plane and a Control Plane portion.

  Mixed plane connections are the end-to-end infrastructure connections or services that reside partially in ASON and partially outside ASON network.

• A *drop link* is an external OS connection that is assigned to the NPA in ASON. A drop link connection is the link between the Managed Plane and the Control Plane.

ASON supports the following Network Reference Points:

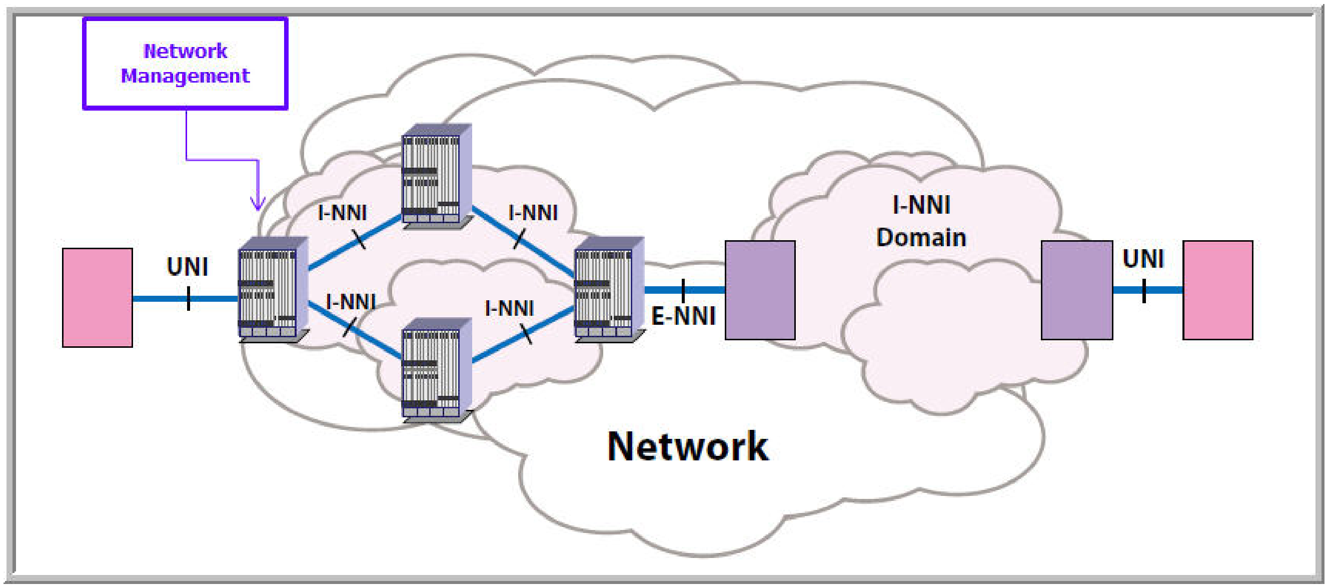
• User-Network Interface (UNI)
• Internal Network-Network Interface (I-NNI)
• External Network-Network Interface (E-NNI)

ASON supports the following Connection Types:

• Permanent Connection (PC) => NMS Designed and executed
• Soft Permanent Connection => NMS originated, executed on the NE by the Control Plane
• Switched Connection => Originated by Client Networks Executed by Control Plane

The following figure depicts the various connection types and the network reference points in ASON.

Figure 3-12 ASON: Network Reference Points and Connection Types



ASON domain

An ASON domain represents the set of instances of (distributed) GMPLS Control Planes (GMREs) working together to automate the resource and connection management, including the rerouting in case of failure.

In case the OTN is configured into GMPLS domains supporting distributed restoration capabilities, the connectivity related to the infrastructure needs to be configured by the Management Plane to the distributed GMPLS controllers.

As previously described the role of reference 1390NPT data does not change: the optimum infrastructure connectivity data determined by the Planning Tools could be used to implement such connectivity in the GMPLS domain.

NFM-T supports:

- Soft Permanent Connection provisioning: NOC users can associate in the provisioning window, as it is for the traditional management approach, the data available from 1390NPT determines the nominal route of the connection; in addition it decides the restoration type supported (The information is also available from the 1390NPT data). The nominal route for the Control Plane provides the reference to the network it considers to restore as soon as the failure conditions allows the current route to be reverted, to guarantee at the maximum extent the proximity to the optimal design.
- The distribution of the Virtual Network Topology information to all GMPLS controllers in the domain, to exploit the information of the available virtual adjacencies in the scope of restoration.
- The capability to request to GMPLS Control Plane the set-up of either a terminated ODU-x trail

as well as a portion of it, where the end-to-end exceeds the GMPLS domain and falls into NMS directly managed resources. Again that is an extension of the behavior already provided in SDH context.

- The capability to partition the network resources of the involved nodes between Control and Management Planes, to implement the specific restoration policy, giving the customers a flexibility to decide how they want to protect the traffic, and at the layers they want restoration to be triggered.

  Example referred to the OTN reference architecture layout: to set-up through GMPLS only the infrastructure closest to the client payload (e.g. ODU-2 connectivity) and avoid any restoration process to occur on higher rate ODU-x connections, such connections can be normally implemented through the Management Plane and then indicated as part of the (strict) nominal route of the client connectivity.

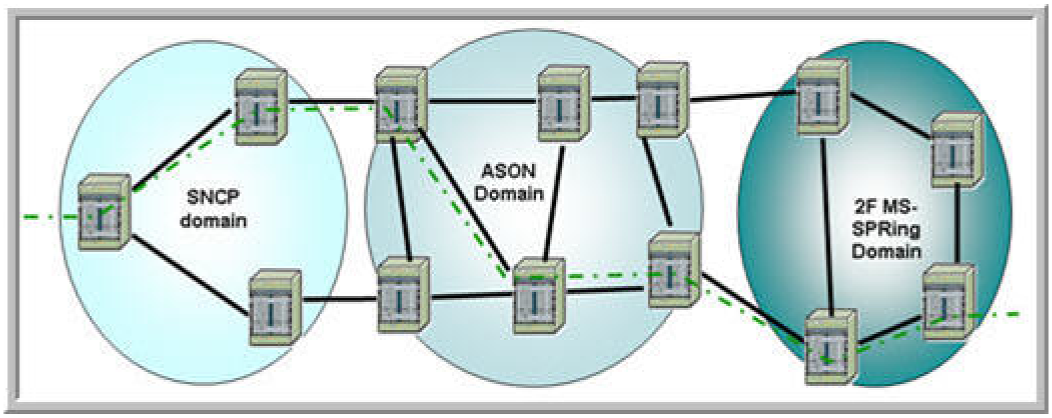
  The capability between non GMPLS and GMPLS to provide the partition of resources in the same node is possible solely in the electrical nodes because this feature is available only with PSS 36/64.
- In case the GMPLS domain sees restoration applicable to both electrical ODU and OCH, NFM-T is in charge to configure, on a per SPC basis, depending on the policy the GMPLS controller must consider when reacting to network failures, so that restoration at either electrical or optical layer is coordinated. The policy typically depends from the kind of traffic to be transported: example high priority traffic is indicated for electrical restoration to ensure the minimum restoration time; other type of traffic could have the policy set for optical restoration first, electrical as second attempt, and so on.

An ASON domain is composed of the following:

- Control plane instances (1 GMRE per NE, Two CPs in each PSS Node PHN+OCS)
- Links and aggregation of links = TE-LINKS (see later for details)
- Soft permanent Connectivity (SPC)(ASON SNC part of the e2e connection)

Nokia's management of GMPLS networks calculates on the NMS the Soft Permanent Connection (SPC) optimum route, which is the nominal route, and then shares this nominal route to the GMPLS and the Control Plane for implementation.

The rationale of this choice is that NFM-T span of control is larger than a single GMPLS domain instance and therefore has the ability to identify the global optimal route (not only the local optimum one) for a given service. The global optimal route can cross GMPLS and traditionally managed domains implementing other kinds of protection mechanisms. This end-to-end route can be then implemented with a single provisioning action and managed as a single entity which represents a key OPEX optimization for a network operator.



The nominal route concept and the strategy to have it decided by NMS have a number of implications, which have been validated by the Nokia experience in the ASON field deployments:

- NFM-T is able to autonomously calculate the nominal route
- NFM-T shares the nominal route with GMPLS engine, which is maintained in the GMPLS domain as the reference; GMPLS engines then plays autonomously for the calculation of the current/backup route when restoration is requested upon network failures
- NFM-T can exploit its own additional optimization criteria when calculating the nominal route.

ASON domain set-up

On top of all the mentioned functions supporting the operations involved in the construction and characterization of the OTN topology, NFM-T provides additional functions in support of the GMPLS domain set-up :

- Creation of the Network Protection Architecture (NPA)
- TE-link (= OMS section) cost and optical parameter assignment to GMPLS controllers

The NPA basically defines a domain in which a given protection architecture (SNCP, GMPLS restoration) applies. In the OTN environment, the concept does not change: NFM-T supports NOC users in defining the GMPLS NPA and managing the assignment of nodes and TE-links to it.

NFM-T is notified and tracks successful SC implementations, which are inventoried in the NML database.

ASON NPA

Network Protection Architecture (NPA), is a set of NEs, protections blocks, and physical links that work together to create a dedicated protection mechanism or are grouped together to establish service layer protection

The NFM-T uses NPA to associate resources that are part of the same protecting structure. By creating and implementing NPA, users can specify the role of a physical link and they can assign a reduction cost factor and a usage cost factor to the physical link.

The users can access the following related objects associated to the NPA from the NPA data table:

- *Traffic Engineered link*, or a TE link, is a unique application entity that is configured through grouping component links. The groupings can be based on different attributes such as SRGs, link metrics, or latency parameters.
- A *3R* is a user-selected optical regeneration group that consists of a node and two NNI transponder line ports that reshape, retime, and retransmit a signal.

ASON link

An ASON link represents the connectivity between the NEs that can be used for ASON routing. In an optical L0 ASON network, the ASON link is equivalent to the NFM-T layer rate. In an electrical L1 ASON network, the ASON link represents the OTU layer rate.

The following guidelines apply to ASON links:

- ASON links are established in the OTN and cannot be deleted or rearranged.
- ASON links and link connections of ASON links are not available for use by manual or automatic routing in OTN.

Users can view ASON links in the Connection list within the OTN Manager by filtering the Category Column for ASON Links.

Nominal route

Nokia's management of GMPLS networks is based on the NMS calculating the Soft Permanent Connection (SPC) optimum route, which is the nominal route, and then passing this nominal route to the GMPLS and the Control Plane for implementation. This end-to-end route can be then implemented with a single provisioning action and managed as a single entity.

In addition, NFM-T minimizes the probability of link saturation and server trail fragmentation of the available time-slots.

The NFM-T enables users to specify routing constraints or to strictly impose the complete route.

The concept of a nominal route ensures that the GMPLS network avoids states where a given level of traffic protection is not guaranteed. The revert-to-nominal command (which is either automatically implemented by the GMPLS or is configured to be triggered by NFM-T) brings traffic back to its nominal route as soon as the network has recovered.

For a guaranteed restoration, the GMPLS control plane pre-evaluates a backup route that can carry the traffic if a fault affecting the current route occurs (for example not sharing any SRG with the current route). The NFM-T raises an alarm if the backup route cannot be pre-defined due to a shortage of network resources.

NFM-T also supports Protection and Restoration Combined (PRC) where the restoration mechanism is invoked after SNCP protects the traffic within 50 ms.

Through the NFM-T, users can view the nominal, current, and backup routes of a connection. They can view, in real time, the traffic that is carried by a link and they can softly move the traffic away from a link to support maintenance activities.

The NFM-T distributes and keeps aligned the TE-link cost and optical parameter values on all the GMPLS controllers in the domain. Centralized parameter distribution ensures that all GMPLS controllers in the domain use the same information and keep a consistent behavior when re-routing is invoked by restoration events. The optical feasibility of a given OCH connection (in case of switching at the optical layer) needs to be calculated by GMPLS controllers as well.

ASON specific OAM

If the OTN network is implemented with GMPLS distributed restoration enabled, the network management must provide additional maintenance-related capabilities that are specifically oriented to the Control Plane environment.

For distributed restoration support against network failures, the NFM-T adds the management of dedicated Control Plane events that are with the restoration process. Assuming a given ODU-x sub-network connection (SNC) passes-through a GMPLS domain, the following events, for example, from the GMPLS controller are mapped into alarms that are forwarded to the Common Alarm repository, as associated to the SNC provisioned in the GMPLS domain:

- SNC Rerouted
- SNC Ready To Revert
- SNC Reversion Blocked
- SNC Backup Unavailable
- SNC Protection Degraded
- SNC Not Disjointed
- SNC Active Unavailable

Beyond restoration associated events, the GMPLS-related maintenance functions that are available from NFM-T are the following:

- **Return to nominal:** The concept of a nominal route in OTN technology, as well as in TDM, ensures that the network will not irreversibly degrade during a restoration to a point where the non-optimal use of network resources can no longer guarantee adequate traffic protection and serve new traffic requests. The NFM-T enables the GMPLS controller to be configured on a per-call basis to revert the current route to the nominal route when the overall failure conditions in the network allow the reversion. Differently, the automatic revertive behavior is disabled and soft rerouting can run instead.
- **Modify nominal or current route commands:** Nominal or current routes can be modified to impose traffic re-routing.
- **Control Plane maintenance commands:** NFM-T offers the capability to issue commands to the GMPLS controllers to do the following:
  - To perform a graceful shutdown and restart of the entire Control Plane in a given domain.
  - To request that a given set of TE-links are locked or shut-down in order to prevent new traffic from passing through.

- To initiate soft re-routing operations on the current routes (such as in-field maintenance tasks over that TE-link).

Multi-Region Network (MRN)

Networks are rarely composed of a single data plane technology hence the applicability of a control plane being in charge of multiple switching layers, as well as their combinations, within the scope of a single network is of interest for a wide range of carriers. Based on this concept, NFM-T support the *Multi-Region Networks/Multi-Layer Network (MRN/MLN)* .

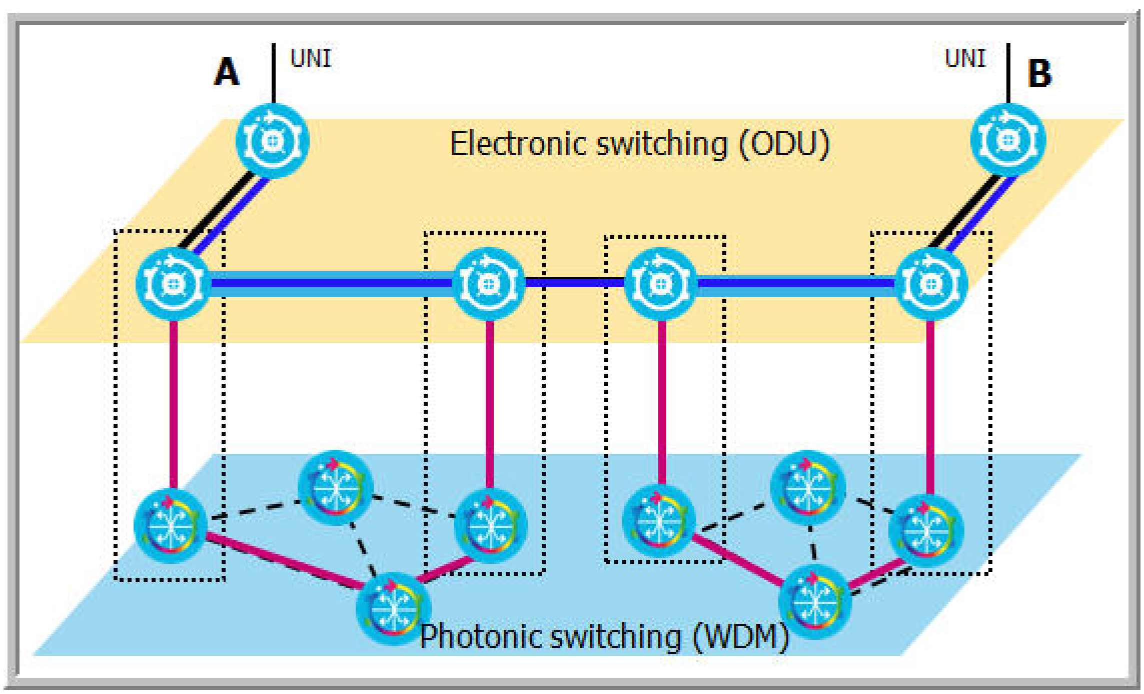
The MRN is a solution for the vertical integration of the networks, based on the GMPLS. MRN gives the possibility of operating domains hosting several technologies acting as a single network.

MRN control plane maximizes multi layer awareness and resource optimization of WDM and ODU layers.

MRN simplifies and harmonizes operations on multiple layers, providing cross-layer visibility and end-to-end service view across network layers. MRN increases the service availability by maintaining dis-jointness of primary and spare resources in multiple layers. MRN recovers quickly by coordinating response to failures, without mandating hold-off timers for layer decoupling. MRN avoids traffic hits through a coordinated sequenced reversion strategy.

The MRN architecture can be resumed as a Vertical Integration of the network, where nodes hosting multiple and inter-working Switching Capabilities (SC) are controlled by a single instance of the Control Plane.

Figure 3-13 Multi-Region Network



Connection setup

When the NFM-T user sets up a connection crossing (or terminating) in the ASON domain, the subnetwork connection at the ASON NPA level is created along with the related cross-connection inside the Nodes.

These cross-connections are marked in such a way that the NFM-T does not directly forward the cross-connection implementation to the NE, but they are provided to the GMRE with the provisioning of the SPC nominal route (the provisioning of the single cross-connections to the NE is in charge of GMRE).

Control Plane domain object

The controlPlaneDomain class represents the GMRE, that is, the Control Plane instance contained in the Network Element.

Some important attributes are:

- *reachable:* indicates the Control Plane communication status.
- *userLabel:* indicates the user label of the Control Plane
- *operationalState, alarmStatus*
- *emsFactoryAddress:* indicates the GMRE Factory IOR for addressing the GMRE/Control Plane using NMI Corba (not visible on the User Interface)
- nativeName: it indicates the name inside GMRE
- *ipAddress:* indicates the IP address of the GMRE (routing IP)
- *assignSt:* indicates if the Control Plane has been taken in charge by NFM-T or not
- *consistSt:* indicates the consistency state

Control Plane tandem connection

A Control Plane tandem connection is a connection that appears in the Control Plane tandem connection list. Control Plane tandem connections cannot be deleted or rearranged in OTN. You cannot terminate a Control Plane Tandem Connection, if it is also a service or trail connection that appears in both the Control Plane Tandem Connection List and the Service/Trail List in OTN. In the Service/Trail List, the connection has a category of control plane. Discovered connections/trail connections cannot be deleted or rearranged in OTN. An unterminated Control Plane tandem connection can be extended in OTN to create a mixed plane connection. When extended, the connection appears in both the Control Plane tandem connection List and the Service/ Trail List. In the Service/Trail List, the connection has a category of mixed plane if any NEs in the extended connection are in the managed domain. If none of the NEs in the extended connection are in the managed plane, the connection will have a category of control plane. Two-ended, three-ended, and four-ended control plane tandem connections are supported. For connections with category of Control Plane, two-ended, three-ended and four-ended control plane tandem connections are supported. For connections with category of Mixed Plane, only two ended control plane tandem connections are currently supported. Therefore, for protected Mixed Plane connections two control plane tandem connections are chosen, one for the working side and a second for the protection side.

Subnetwork connection

Subnetwork Connection (SNC) is a WDM ODU0, ODU1, or ODU4 layer that connects user-selected primary and spare endpoints. An SNC is further defined by its connection shape, its support of Tandem Connection Monitoring (TCM), and its sets of Control Plane restoration parameters and color parameters.

Some important attributes are:

- *userLabel*
- *sncActiveSt:* specifies if the subnetwork Connection has been implemented on the NEs by the GMRE (not visible on the User Interface).
- *rerouting:* specifies if the rerouting by the Control Plane is allowed or not.

Network Element

The following attributes are added to the Network Element:

- controlPlaneDomId: it is the Identifier of the Control Plane Domain (not visible on the User Interface)
- controlPlaneStatus: it identifies the Control Plane status.

Allowed values are:

- notPresent: the Control Plane is not present on the NE (default value).
- notManaged: the Control Plane is not managed by the NFM-T.
- reachable: the Control Plane is managed by the NFM-T and it is reachable.
- notReachable: the Control Plane is managed by the NFM-T but not reachable.

Port

The following attributes are added to the port class:

linkType: it identifies the port type inside NFM-T. Allowed values:

- *NFM-T-internal:* it is a port of an NE not involved in an ASON NPA (default value).
- *drop:* it is a port (without signaling) of an NE belonging to an ASON NPA, connected to a port of a client device.
- *uni-n:* it is a port (with signaling) of an NE belonging to an ASON NPA, connected to a port of a client device.
- *i-nni:* it is a port of an NE belonging to an ASON NPA, connected to an NNI port of a neighboring NE belonging to the same ASON NPA.
- *e-nni:* it is a port of an NE belonging to an ASON NPA, connected to an NNI port of a neighboring NE belonging to a different ASON NPA.

portNativeName: it identifies the port inside the Control Plane.

remotePort: it identifies the native name of the far-end port.

3.7 ASON connection setup

Connection setup using the nominal, optimal, and current routes

The initial set up of a connection in ASON involves the establishment of the *nominal route*, which is the initial route though the network. For optical connections, the user sets up the nominal route in conjunction with the Engineering and Planning Tool (EPT) to establish an *optimal route* through the network. The nominal route information is sent to the GMRE module on the 1830 PSS NE for implementation in the network.

The route that a connection takes through the network is known as the *current route*. In most cases, the current route and the nominal route are the same. If a failure occurs, ASON *reroutes* traffic around the failure automatically and restores service. The current route follows a path that differs from the nominal route. Once the failure is repaired, the traffic is switched back to the nominal route to ensure optimal routing through the network. The NFM-T system stores the details of the nominal route and retrieves the current route upon demand when needed.

The following figures illustrates how the traffic is rerouted.

Figure 3-14 ASON - ASON Nominal Route and Current Route - 1

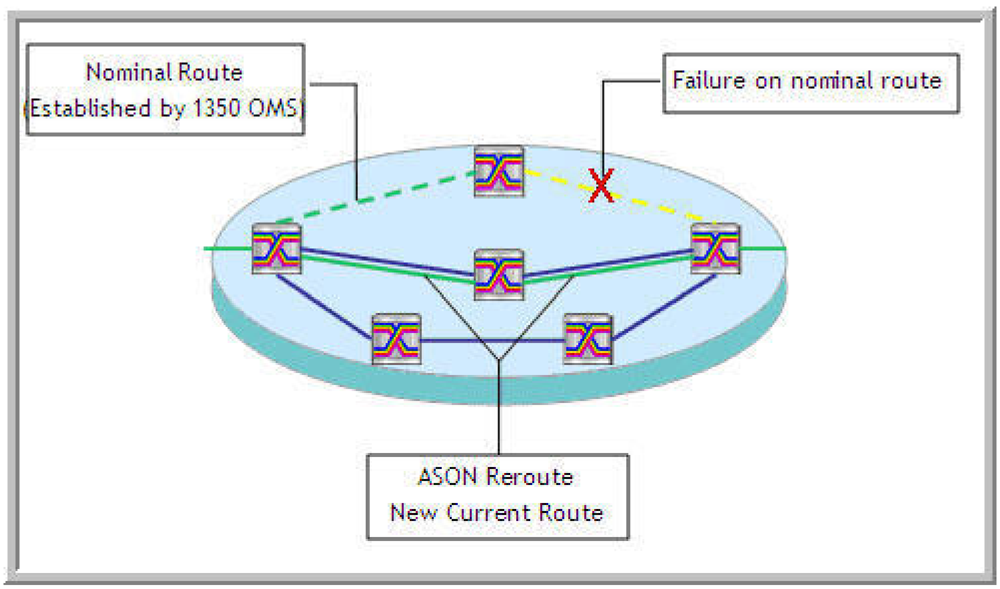
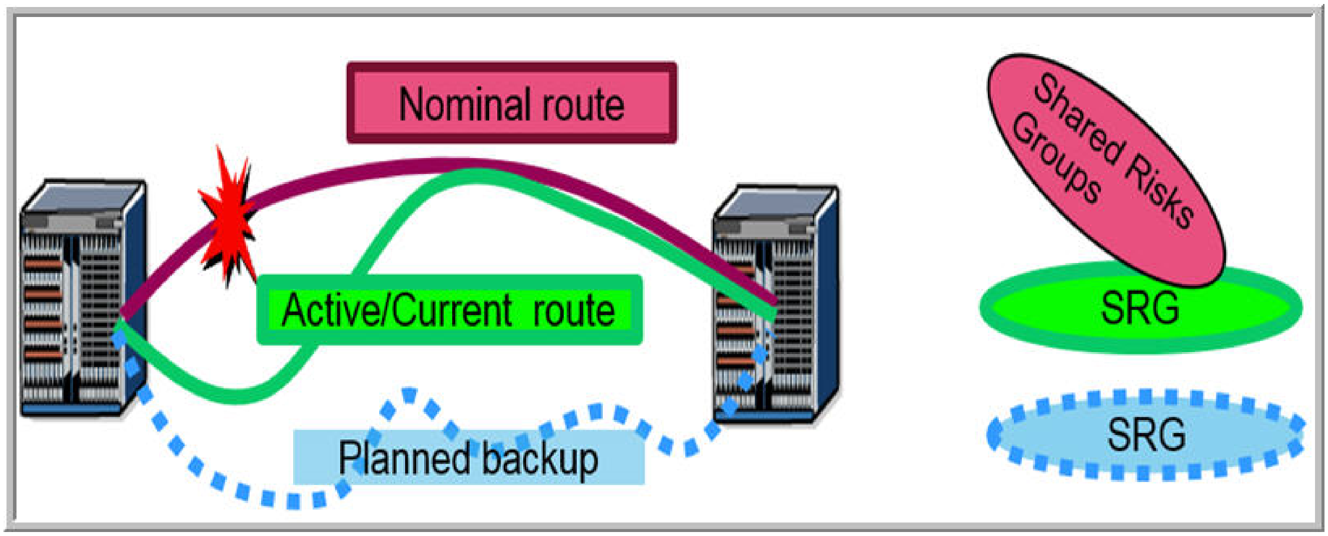
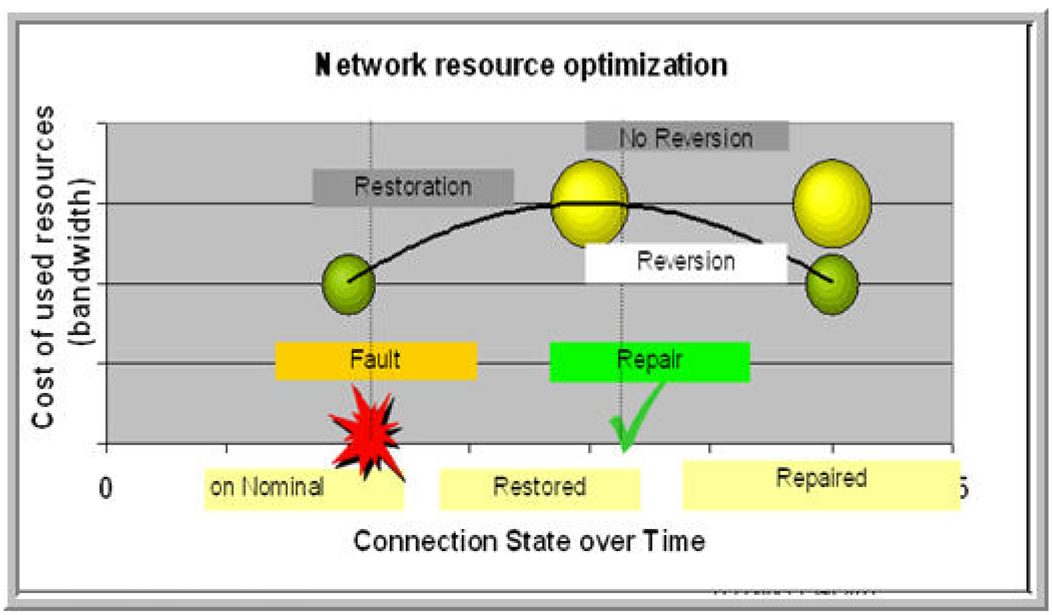


Figure 3-15   ASON Nominal Route and Current Route - 2



Note: The users can rearrange the nominal route of a Control Plane connection in ASON. When a control plane connection is rearranged, a service disruption on the connection might occur as cross connects are being taken down and are being re-established, which causes alarms to occur on both the given connection and the client connections.

Figure 3-16   Network resource optimization



The Nominal Route and Reversion concepts keeps control over the ASON network.

3.8 ASON protection and restoration

ASON protection

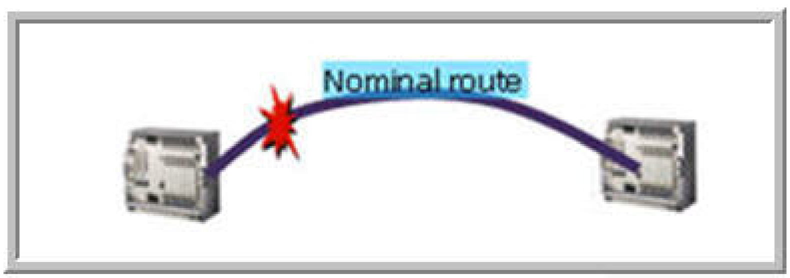
ASON generally uses fewer network resources than ring or other one-to-one protection schemes or it can be combined with ring protection methods to provide more robust protection if network survivability is critical to a site. The combine protection method provides fast recovery through ring protection and also restores the failed portion of the ring through ASON.

GMPLS protection services that can be established through ASON include unprotected service, SBR (upon failure), and PRC (through SNCP inside ASON for GMRE L1; through O-SNCP outside ASON in GMRE L0), and precalculated.

Unprotected service

With *unprotected service*, traffic is lost if a fail occurs.

Figure 3-17 ASON – GMPLS Unprotected Service



Network backbone setup

To reroute traffic successfully if a failure occurs, the network needs additional information, which is supplied by the user establishment of *Shared Risk Groups (SRGs)* and a *Network Protection Architecture (NPA)* for the network.

An *SRG* is a user-defined group of associated physical links and, in some cases, logical links that represent a common failure point, such as a conduit.

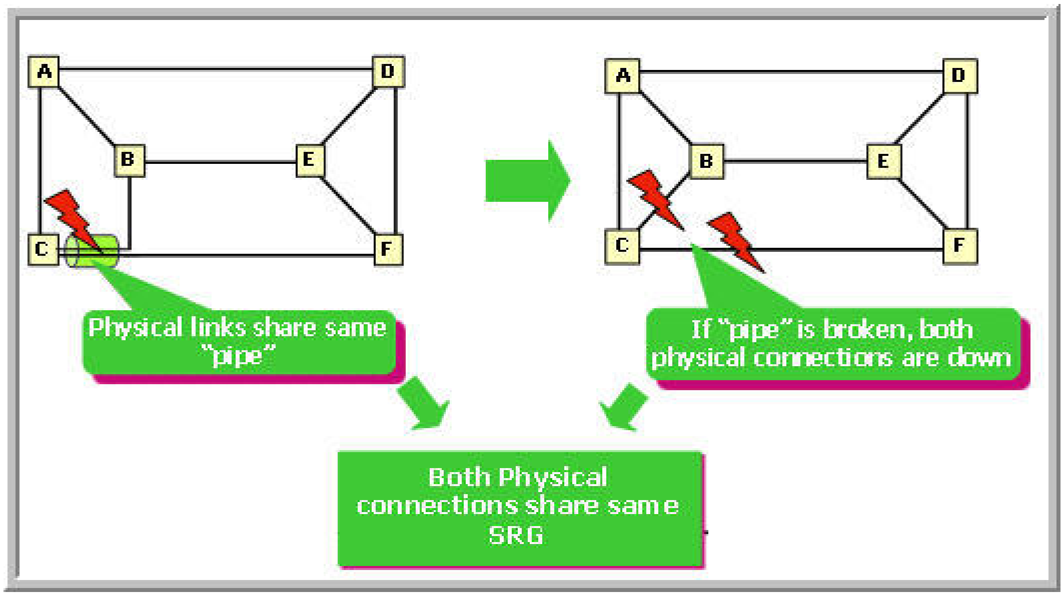
The establishment of proper SRGs in a network is important because a primary and backup connection should not be set up through the same failure points, even though they may be using different fibers. (A failure point can be a shared conduit or other such physical structure.) If multiple fibers share the same conduit, they can all share a common failure point and they can also all be affected if the conduit is damaged or destroyed. Because an SRG contains the physical connections that use the same physical plan, ASON uses SRG information to reroute traffic to ensure that the rerouted traffic avoids the failure point.

Example:

If two fibers pass through the same conduit, they would be grouped in the same SRG. If a failure occurs on the conduit, all traffic is rerouted around the fibers that are assigned to that SRG.

The following figure illustrates a physical depiction of a network on the left and a logical depiction of a network on the right. With the physical network (left), rerouting procedures require the knowledge of the physical aspects of the network to avoid shared risks and localized faults. The physical links share the same *pipe*. With the logical network (on the right), the network management system requires a logical view of the network to route traffic. If the pipe is broken, both physical connections are down. Both the physical and logical networks share the same SRG.

Figure 3-18 ASON – ASON SRGs



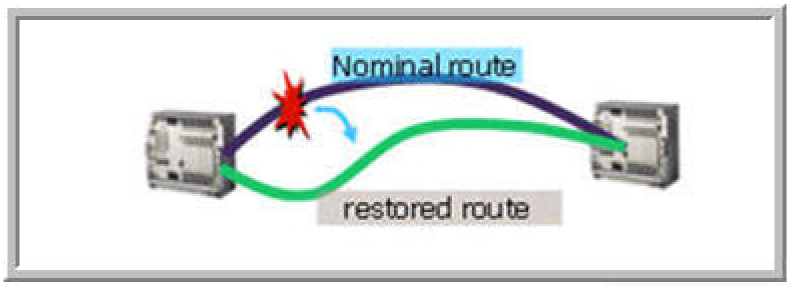
ASON also relies on the information supplied by the NPA. The NPA is a set of NEs, protections blocks, and physical connections that work together to create a dedicated protection mechanism or are grouped together to establish path layer protection. NPAs are used by the NFM-T to associate resources that are part of the same protecting structure. By creating and implementing an ASON NPA, users can specify the role of the physical connection and they can assign a reduction cost factor and a usage cost factor to the physical connection.

Source based restoration

With *SBR*, or *Source Base Restoration*, the Control Plane protects the traffic if a failure occurs by calculating a new route.

The following figure illustrates GMPLS SBR.

Figure 3-19 GMPLS Source Based Restoration



In Provisioning, the Nominal Route is computed by NMS.

For Restoration, Backup route is computed after failure. SBR uses failure information to identify diverse link(s).

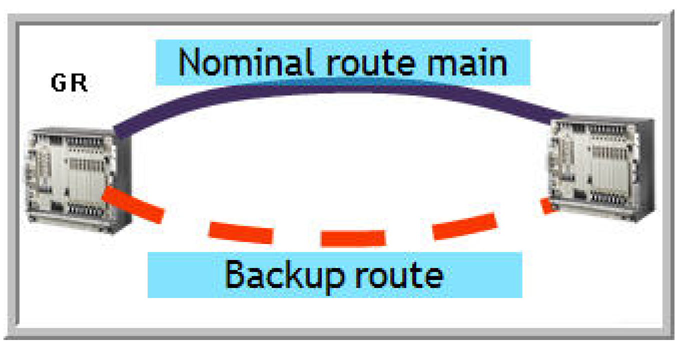
When the restoration occurs, intact resources are preserved whenever possible without additional intermediate switching.

Guaranteed restoration

In guaranteed restoration, the restoration route is calculated in the same time of implementation of nominal route.

With guaranteed restoration, protection and restoration are used together to optimize recovery time and to maximize service quality. The Control Plane calculates a restored route as an alternative to the nominal route (main).

Figure 3-20 Guaranteed Restoration



In provisioning, the Nominal Route is computed by NMS. The backup path that is calculated and reserved is shared among several active nominal routes.

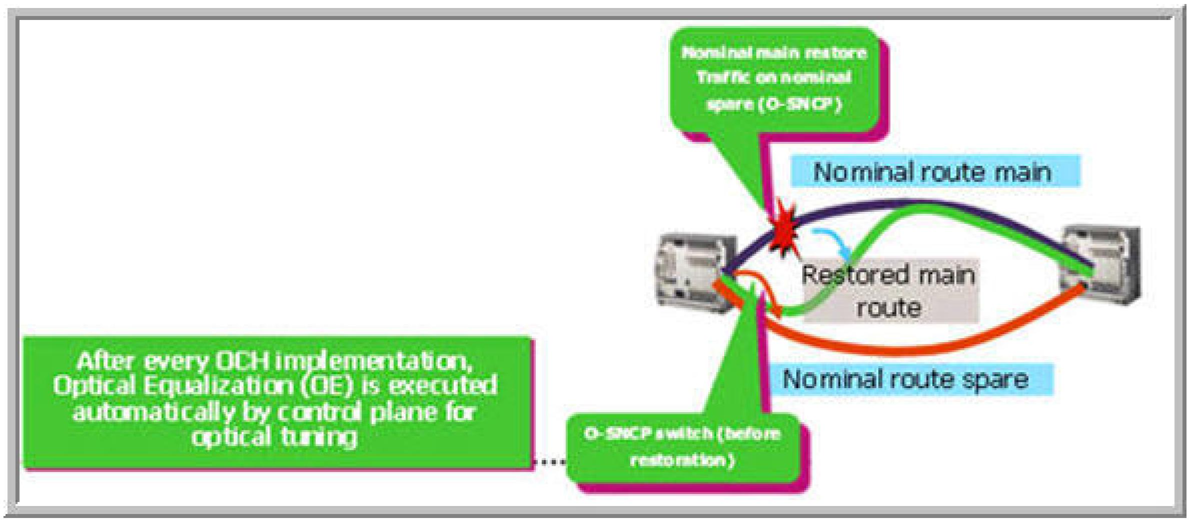
In restoration, the Backup path is implemented upon failure detection. The backup path is reserved subsequently.

Protection and restoration combined

With *PRC*, or *Protection and Restoration Combined*, protection and restoration are used together to optimize recovery time and to maximize service quality. The Control Plane calculates a *restored route* as an alternative to the *nominal route* (main).

The following figure illustrates GMPLS PRC in an optical network. Note that after the first failure, an Optical-Subnetwork Connection Protection (O-SNCP) switch occurs in less than 50ms. The network then calculates a restored route as an alternative to the nominal route.

Figure 3-21 ASON – GMPLS Protection and Restoration Combined



In Provisioning, the Nominal Route and fully-diverse backup path is computed by the NMS.

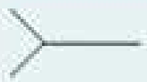
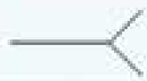
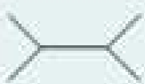
For restoration, the following functionalities are supported:

- On first failure detection, backup path becomes active (tail-end path selection).
- A new, diverse backup path is then computed and activated.
- After subsequent failure(s), new services are computed and activated.
- Applies to failures on either/both active and backup services.
- When available, original nominal route and/or backup path is reinstated by means of bridge and roll.

Protection and restoration parameters

The table summarizes the interaction of the parameters in ASON connection deployment: type of protection, type of connection, client protection type, network protection type and restoration.

Figure 3-22 ASON Protection and Restoration

	Prot Type	Connect. Type	Client Prot Type	Ntw Prot Type	Ason Restor. Type
	Prot.	3- ended A Bid	SNC-NC or SNC-N	None	SBR/GR/ Unpro
	Prot.	3- ended Z Bid	SNC-NC	None	SBR/GR/ Unpro
	Prot.	3- ended A Bid	SNC-NC or SNC-N	SNC-N ESNCP	SBR => PRC
	Prot.	3- ended Z Bid	SNC-NC or SNC-N	SNC-N ESNCP	SBR=> PRC
	Prot.	4- ended	SNC-NC or SNC-N	None	SBR/GR/ Unpro
	Prot.	4- ended	SNC-NC or SNC-N	SNC-N ESNCP	SBR => PRC

Guaranteed Restoration and Protection

Guaranteed Restoration is allowed for protected service, ASON routed but not protected in ASON, that is ASON Sub-network protection type is *None*. In the following figures you vcan see the difference betwwen GR allowed and not allowed, depending on the parameters set and the ASON subnetwork.

Figure 3-23 Guaranteed Restoration not allowed

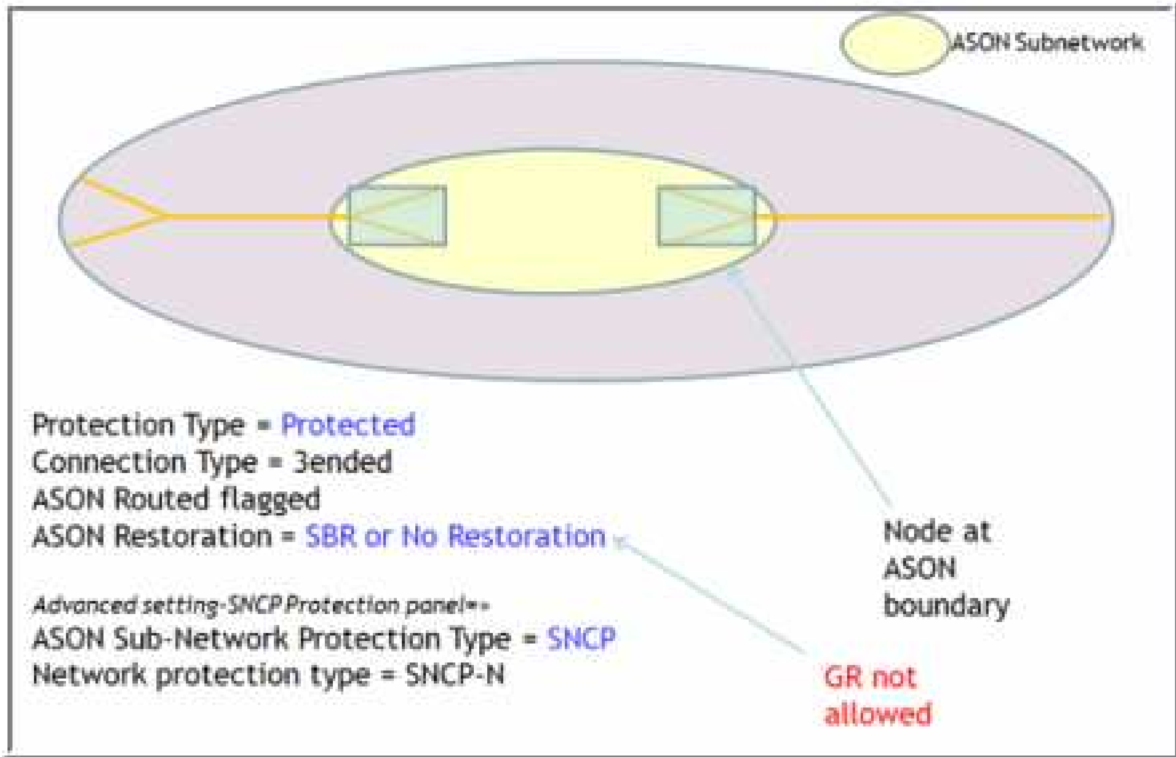
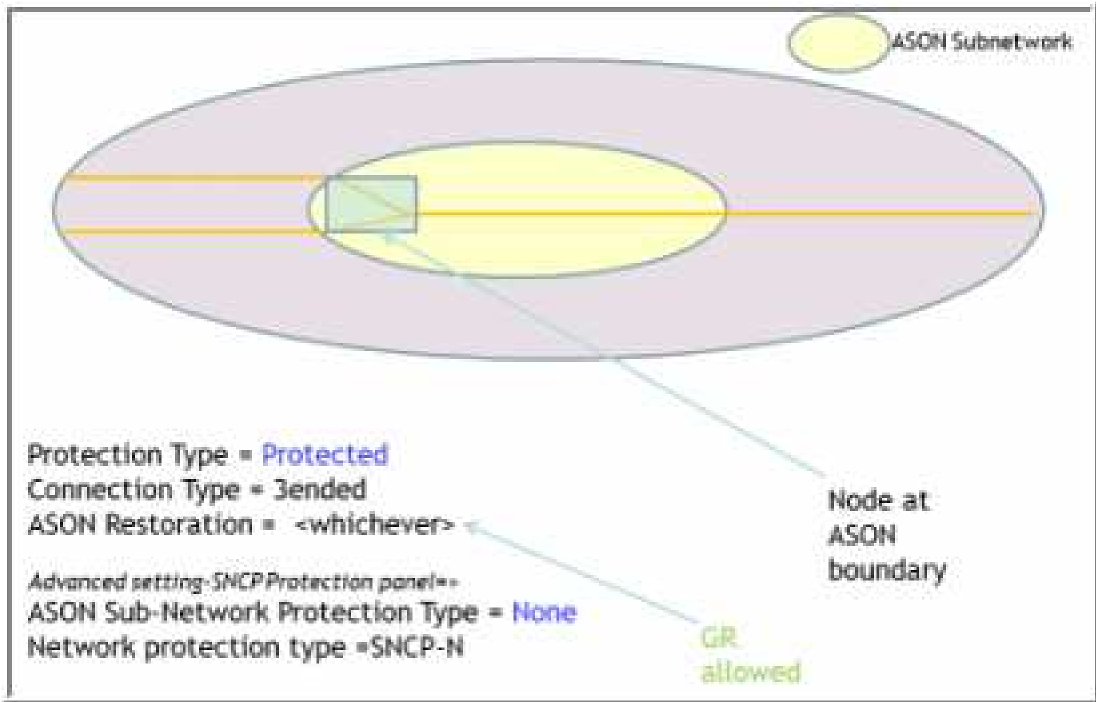
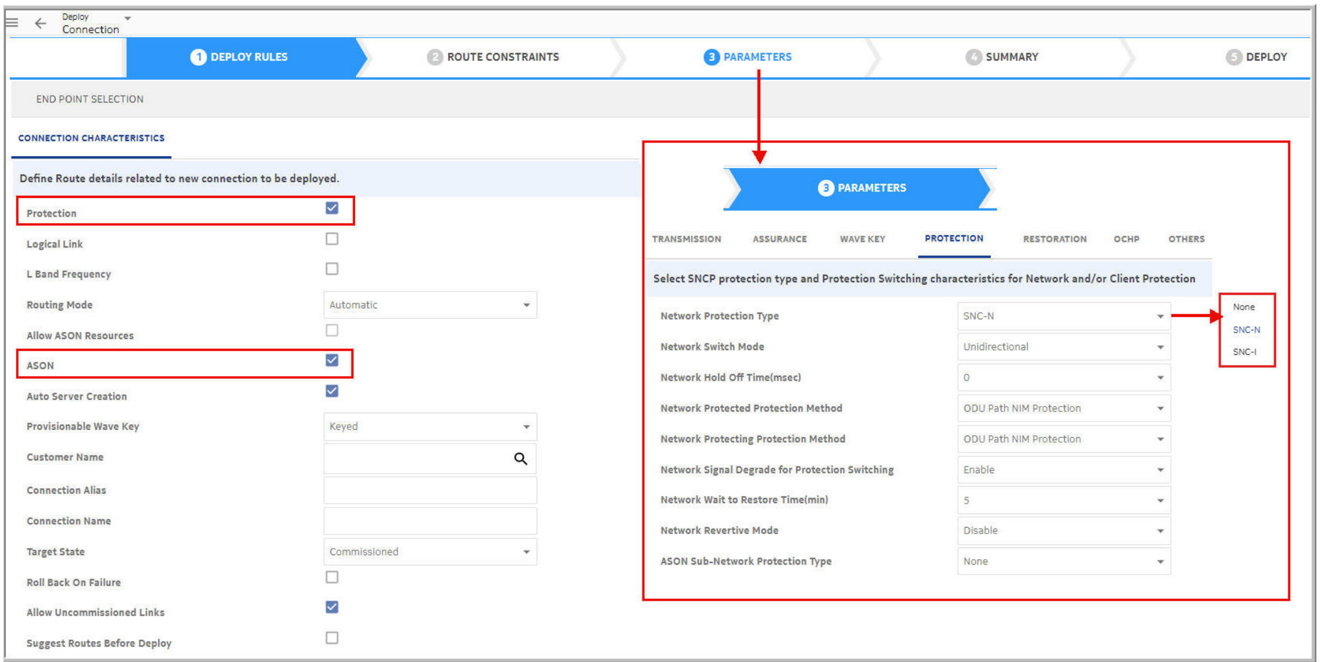


Figure 3-24 Guaranteed Restoration allowed



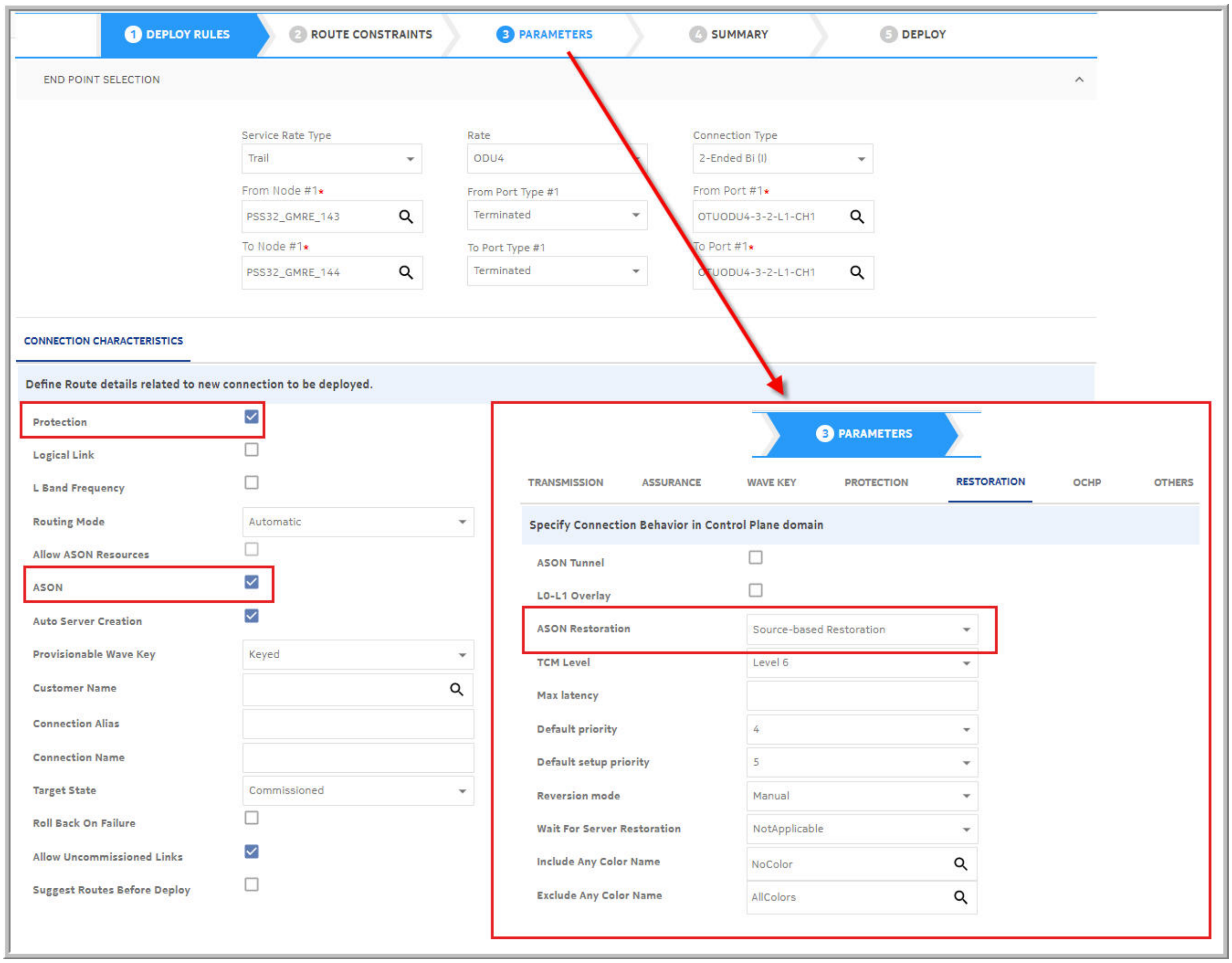
The user is allowed to select in the creation template both ODU Protected (end to end), ASON routed and unprotected with Guaranteed Restoration (alternative to SBR) in ASON domain.

Figure 3-25 Parameter Setting in Deploy Connection



In case Guaranteed Restoration does not apply per defined route, for example OPSA protection is present on the route, the system automatically changes the ASON SNC restoration method from **GR** to **SBR** before provisioning to GMRE and both restoration methods, the preferred, that is the user request, and current, selected by the system, are shown as parameters of ASON SNC, in the SNC list.

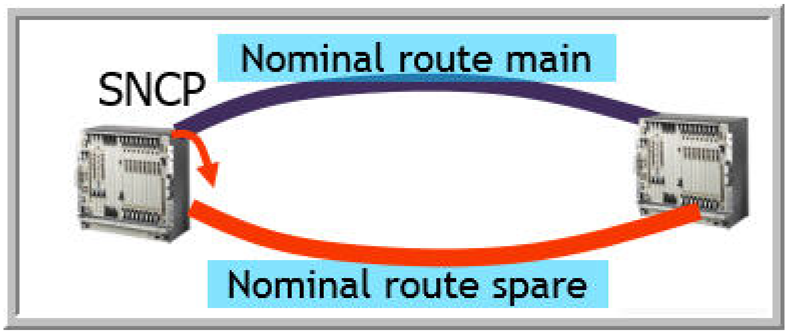
Figure 3-26 Template GR and SNC List



Sub Network Connection

Sub Network Connection (SNC) specifies if the subnetwork Connection has been implemented on the NEs by the GMRE

During provisioning, Nominal Route and fully-diverse backup path is computed by NMS.



During restoration, following functions are available:

- On failure detection, backup path becomes active (via tail-end path selection)
- Reversion to original nominal route upon failure resolution
- Backup path remains implemented and active

3.9 Network setup in ASON

Overview

To reroute traffic successfully if a failure occurs, the network needs additional information that is supplied by the establishment of *Shared Risk Groups (SRGs)* and a *Network Protection Architecture (NPA)* for the network.

An *SRG* is a user-defined group of associated physical links and, in some cases, logical links that represent a common failure point, such as a conduit.

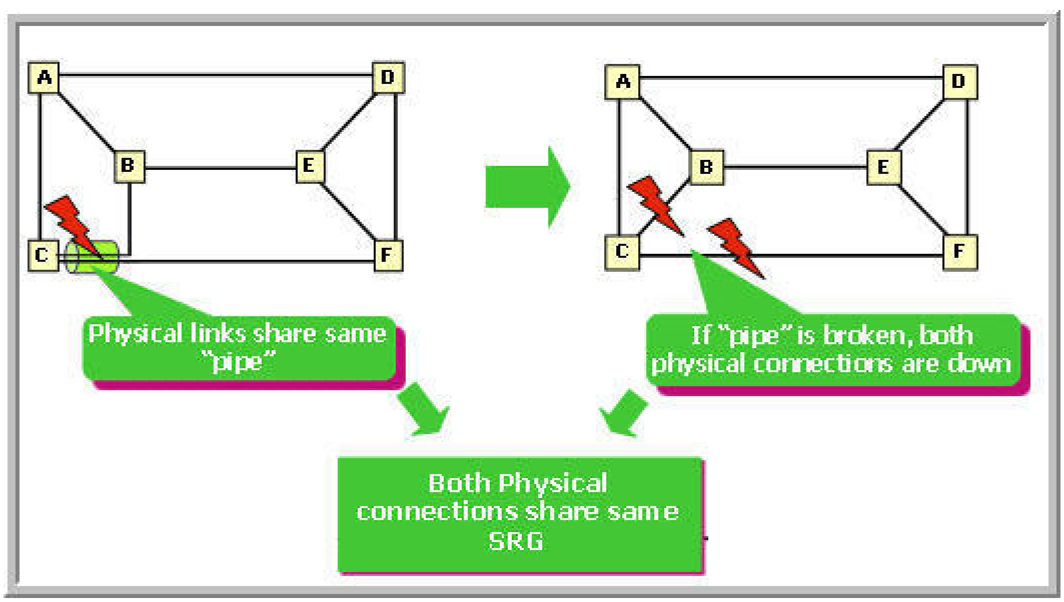
The establishment of proper SRGs in a network is important because a primary and backup connection is not set up through the same failure points, even though they may be using different fibers. (A failure point can be a shared conduit or other such physical structure.) If multiple fibers share the same conduit, they can all share a common failure point and they can also all be affected if the conduit is damaged or destroyed. Because an SRG contains the physical connections that use the same physical plan, ASON uses SRG information to reroute traffic to ensure that the rerouted traffic avoids the failure point.

Example:

If two fibers pass through the same conduit, they would be grouped in the same SRG. If a failure occurs on the conduit, all the traffic is rerouted around the fibers that are assigned to that SRG.

The following figure illustrates a physical depiction of a network on the left and a logical depiction of a network on the right. With the physical network (left), rerouting procedures require the knowledge of the physical aspects of the network to avoid shared risks and localized faults. The physical links share the same *pipe*. With the logical network (on the right), the network management system requires a logical view of the network to route traffic. If the pipe is broken, both the physical connections are down. Both the physical and logical networks share the same SRG.

Figure 3-27 ASON SRGs



ASON also relies on the information supplied by the NPA. The NPA is a set of NEs, protections blocks, and physical connections that work together to create a dedicated protection mechanism or are grouped together to establish path layer protection. The NPAs are used by the NFM-T to associate resources that are part of the same protecting structure. By creating and implementing an ASON NPA, the users can specify the role of the physical connection and they can assign a reduction cost factor and a usage cost factor to the physical connection.

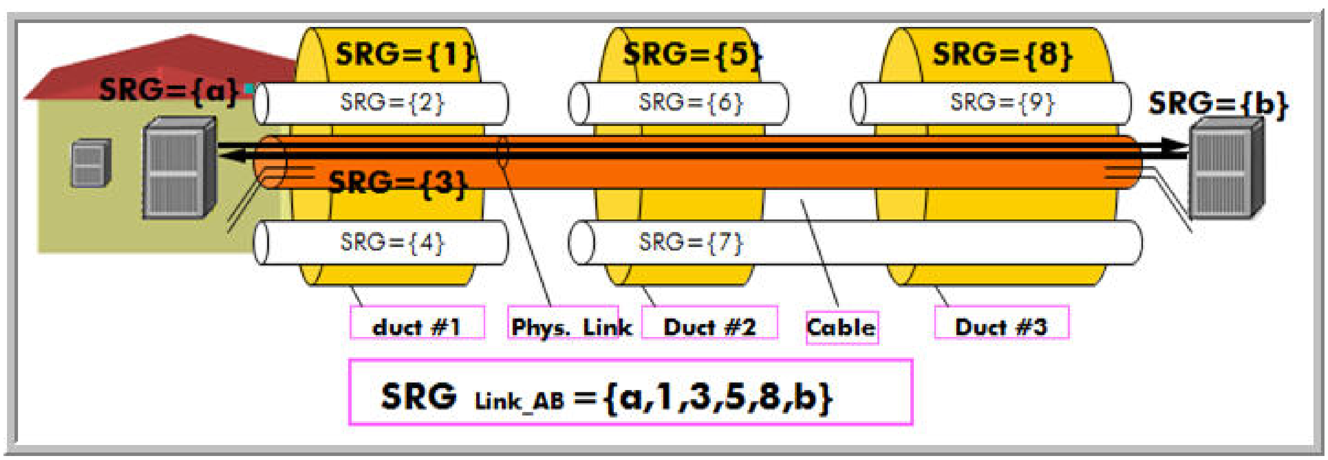
Shared Risk Group (SRG)

Shared Risk Group (SRG) is a group of elements that share a common risk, and whose failure can cause the failure of all the elements in the group. The purpose of SRG is to provide a redundant route through the network for an existing route avoiding that the same problem, for example a link failure, disturbs both the routes.

SRGs are identified by means of SRG values that need to be unique within a GMRE domain One or more SRG identifiers have to be assigned to the TE links in the GMRE domain network that share at least one risk. An SRG attribute can be empty, can comprise a single SRG identifier, or comprises a list of multiple SRG identifiers in case the entity is vulnerable to a number of different failures. Two or more connections are fully SRG diverse, if the intersection of their SRG attributes is empty, that is, if the respective connections do not have any SRG values in common.

A single Optical Physical link may belong to several SRGs in different sections. Routing algorithms for nominal and pre-planned restoration avoids common risks between main, spare, or planned backup.

Figure 3-28 Shared Risk Group



Latency

Latency is a configurable attribute for constraint-based routing.

Latency must be configured manually and is not measured automatically.

End-to-end latency threshold

The source node of a control plane service maintains a configurable latency constraint per service, which specifies an end-to-end latency threshold in microseconds that is not exceeded by any of the actual paths of the service and, in case of a GR service, is not exceeded by the backup path. An end-to-end latency threshold of 0 means that the latency is not used for constraint-based routing.

TE link latency

The TE link latency is a configurable attribute that specifies the latency costs in microseconds associated to a TE link.

Access link latency

If an end-to-end latency threshold is specified, then the source node of a control plane service maintains an access link latency value in microseconds representing the latency caused by the drop ports at the source and destination node.

Calculated latency

The source node of a control plane service maintains a calculated latency per actual path, which is the sum of the TE link latency plus the access link latency of the service.

Color

The color values associated to a logical I-NNI link are the union of a propagated set of color values and a user-defined set of color values.

The propagated set of color values is inherited from the include color constraints of the underlying tunnel service.

The user-defined set of color values is initially empty but can be modified without constraints.

The propagated set of color values cannot be modified.

Cost

The cost value of a logical I-NNI link is propagated (inherited) from the underlying physical I-NNI links as the sum of all cost values of the underlying physical I-NNI links minus 1, according to the actual route of the LSP.

In addition, there are the following configuration options

- The propagated cost value can be overwritten by a manually provisioned value. The manually provisioned value is valid for the link irrespective of any route changes occurring on the underlying tunnel service.
- A manually provisioned cost value can be invalidated. Then, the propagated value becomes valid and is updated based on any route changes occurring on the underlying tunnel service.

ASON Configuration and Provisioning

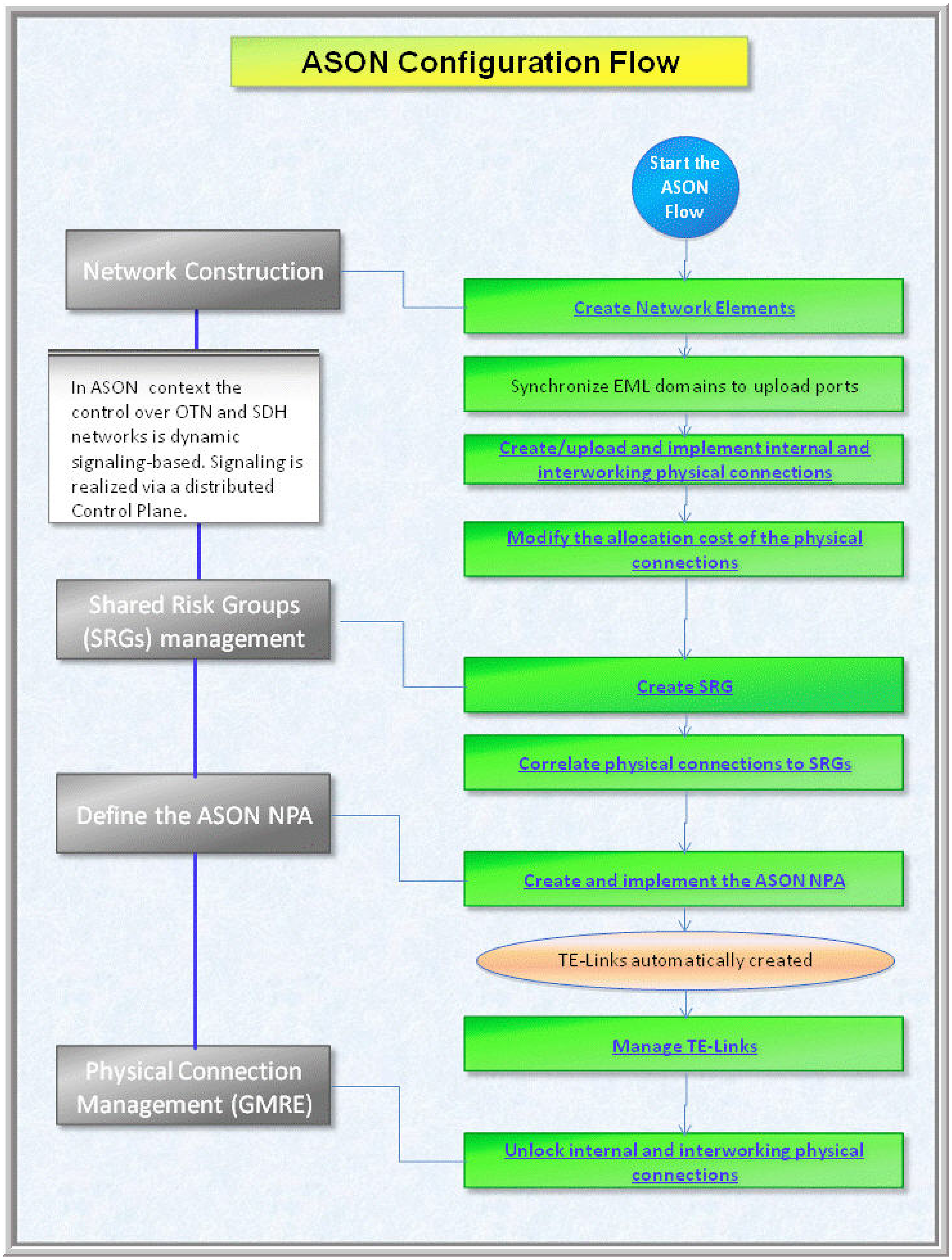
3.10 ASON configuration flow

Overview

ASON has been represented in electrical or Photonic environment as a specific Network Protection Architecture that offers GMPLS restoration.

In traditional networks, services are provided connecting a chain of subnetwork connections. In ASON, the control over OTN is signal-based. Signal is distributed through a distributed Control Plane.

Figure 3-29 ASON configuration flow

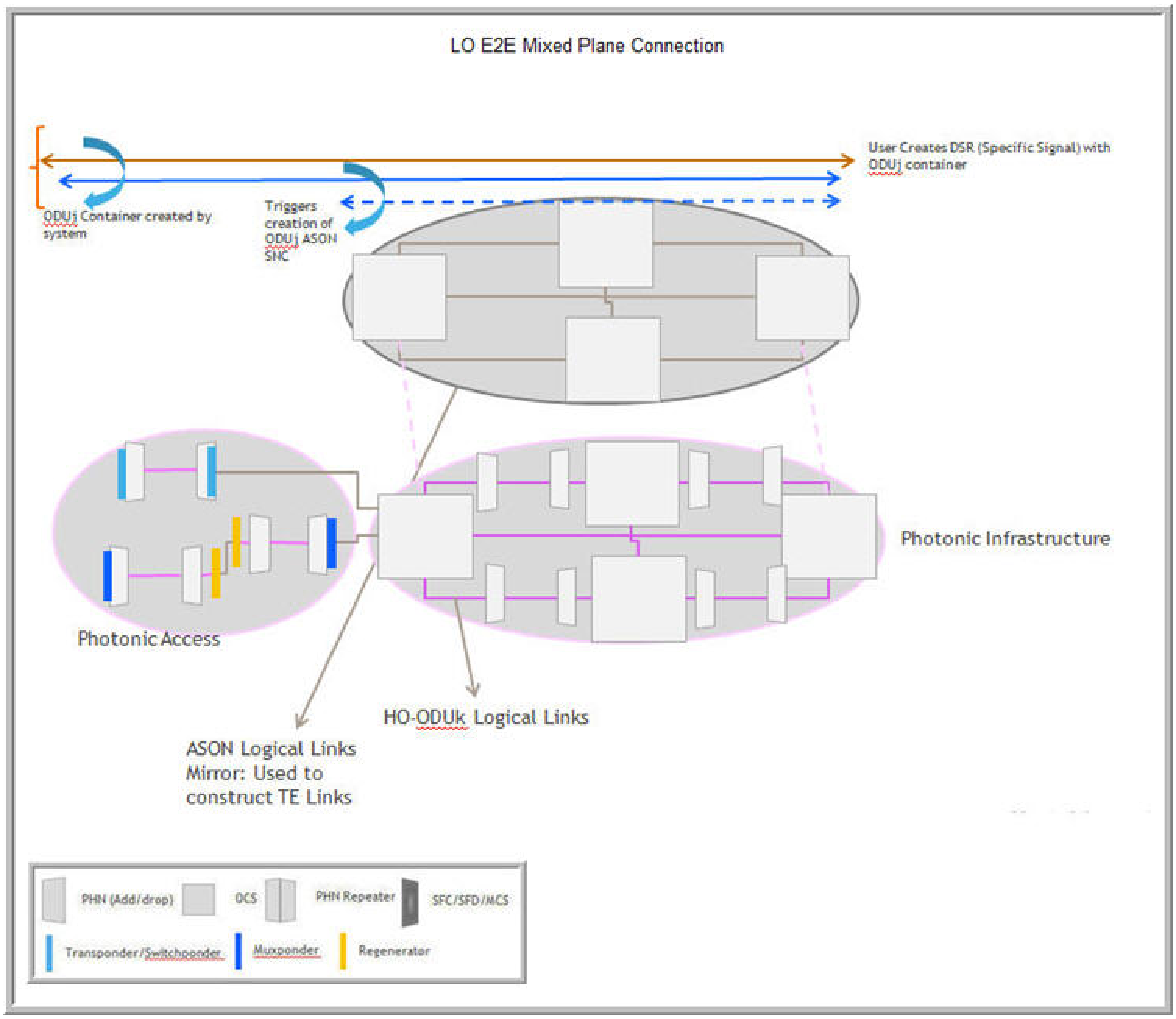


3.11 L1 ASON configuration

OTN Network Provisioning - ASON Configuration

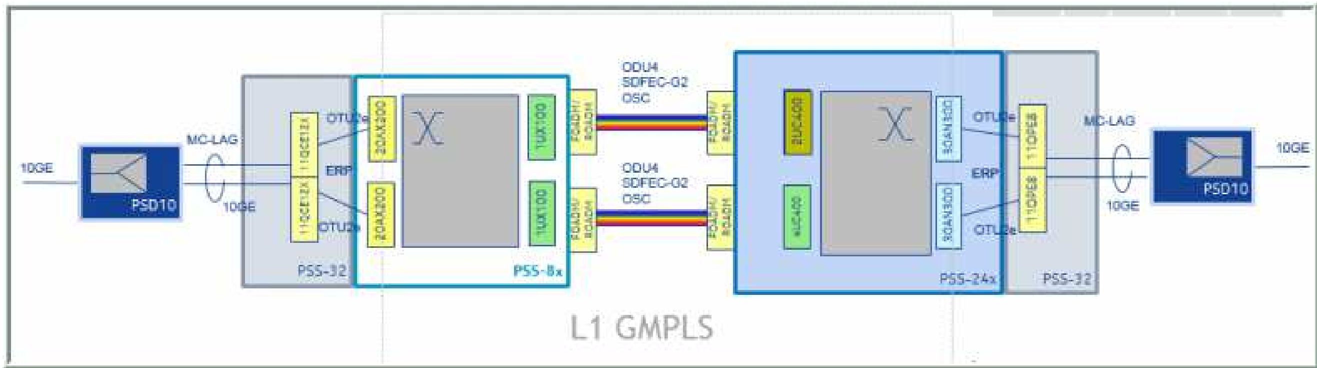
The figure shows an example of L1 ASON network.

Figure 3-30 OTN Network Provisioning – L1 ASON Configuration



If the configuration is L1 GMPLS configuration and the end points are L2 cards, an integrated DSR connection has to be created.

Figure 3-31 L1 ASON Configuration Example



3.12 Macro-steps for ASON configuration

Purpose

To manage a restoration network, the NPA is defined and the links of GMPLS domain must be assigned to the NPA so that the NEs are inserted in the GMPLS domain in an automatic way. The NEs and the links have been uploaded automatically by NPR module and the commissioning has been done on the NE (for only WDM NE). The NPA can be defined or implemented. During the implementation phase, the TE-Link, data-bearers, SRGs, and costs are automatically created on the NE.

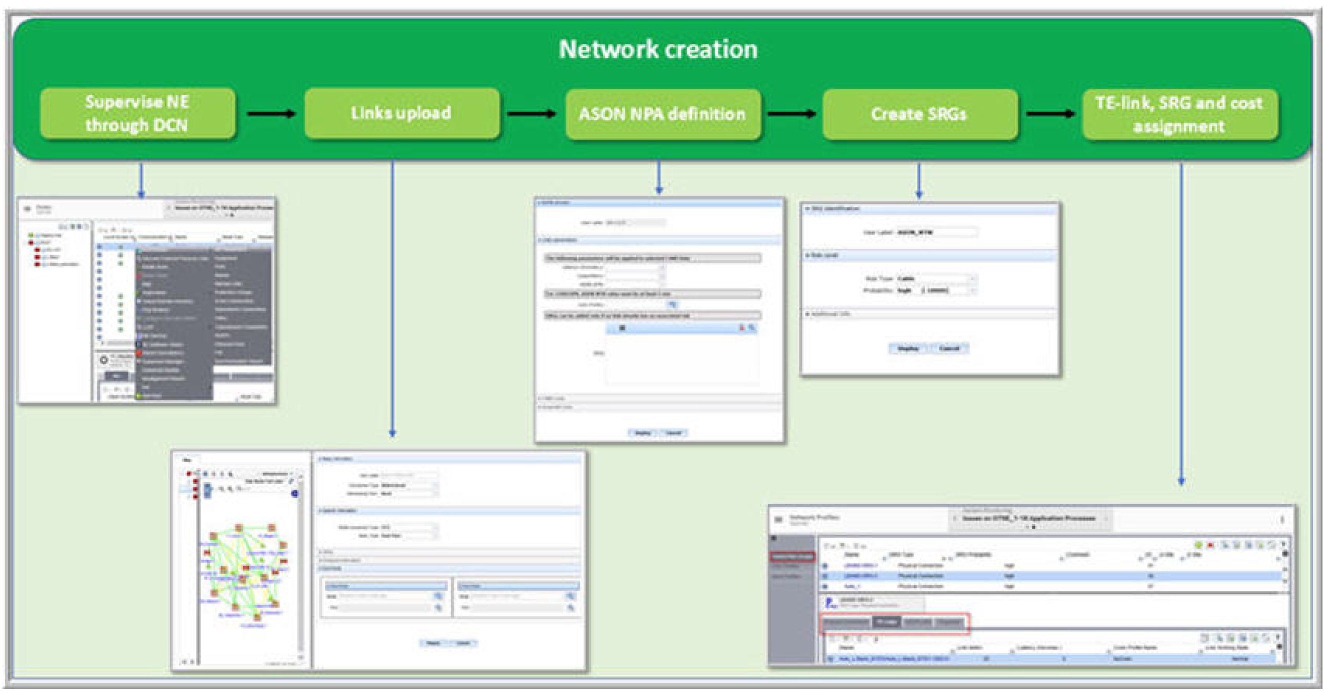
The TE-Links are the links in the GMPLS domain, In a electrical restoration network, the TE-Link represents one or more physical links with the same extremities and same rate; whereas in photonic GMPLS the TE-Link is in relation with the trail (ASON link).

The SRG defines the risk linked to the connectivity. The NFM-T provides a specific wizard to create or remove the SRG and different types of SRGs are managed by the system.

Using the modification wizard of the TE-Link, the SRG and cost can be assigned to TE-Link. The SRG and cost are needed to do the routing.

After the NPA implementation, the TE-Links are in **Locked** state. In this state, the links cannot be used by the GMRE and the traffic does not flow in **Locked** state. To activate all the links in the NPA, all the TE-Links have to be changed to **Unlocked** state. The **Lock** state can be used for maintenance purpose.

Figure 3-32 Network Creation



Task

Complete the following steps to configure ASON.

1

Network construction. Create the physical network in NFM-T System:

- Create the Network Elements.
- Synchronize EML domains to upload ports.
- Create, upload, and implement drop link and I-NNI physical connections.
- Modify the allocation cost of the physical connections.

2

Shared Risk Groups (SRGs) management. Assign dependencies relevant for routing in NFM-T:

- Create SRGs.
- Correlate physical connections to SRGs.

3

ASON NPA (Network Protection Architecture) management. Define the ASON NPA. Implement ASON NPA:

- Create and implement ASON NPA.
- TE-Links are automatically created.

4

Physical connection management. Make the physical connections usable for GMRE:

- Unlock drop link and I-NNI physical connections
  Subsequently, the connections crossing the ASON are created from NFM-T.

END OF STEPS

3.13 Construct a network

Purpose

Use this task to create all network topological objects.

Task

Complete the following steps to create all network topological objects.

1

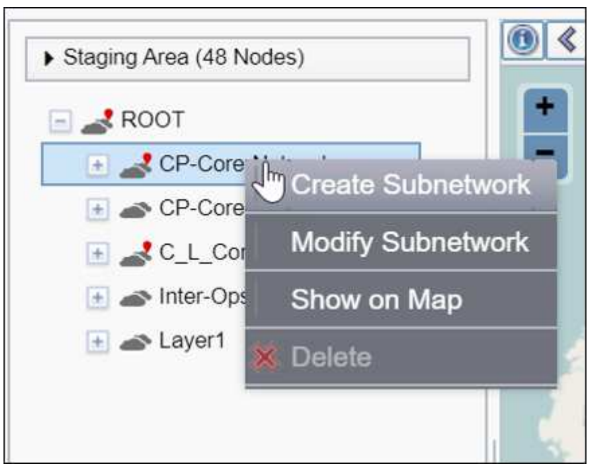
From the NFM-T GUI, select **Operate > Network Map**.

Result: The system displays the OTN Network Map window.

2

Select the root map in the left tree, right click, and select **Create Subnetwork**.

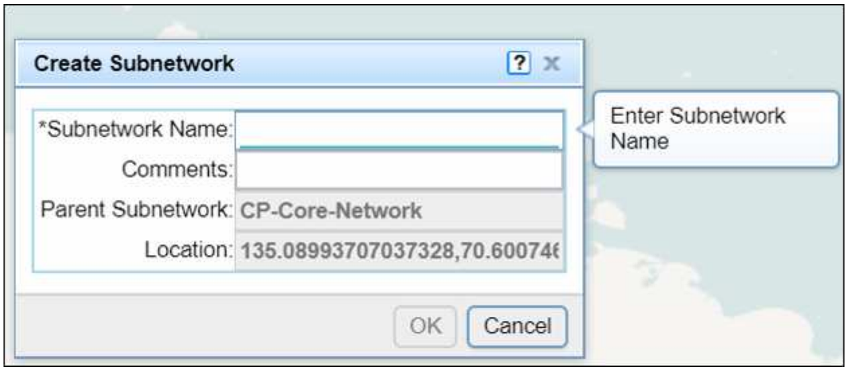
Figure 3-33 Create subnetwork menu



3

In the **Subnetwork Name** field, enter the value and click **OK**.

Figure 3-34 Create subnetwork window



4

Create all the required NEs. From the NFM-T GUI menu, follow the path **Operate > Nodes**.

Result: The system displays a data table that lists all of the nodes.

5

Mouse over the icons on the top right and click the **Add Node** icon.

Result: The **Add Node/NE** window is displayed.

6

Enter the relevant attributes and click the **Create** button.

7

To assign the NE to the Subnetwork from the Subnetwork issue, select **Operate > Network Map**.

8

Open the subnetwork to which you want to add the node or NE.

In the Staging Area of the **Network Map**, identify the node or NE that you add to the opened subnetwork and drag the node or NE into the subnetwork.

Result: The node or NE is added to the subnetwork.

9

From the NFM-T GUI menu bar, follow the path **Operate > Physical Connection**.

Result: The system displays a data table that lists the OTN physical connections.

10

Mouse over the icons on the top right and click the **Create** icon.

11

Create a OTN physical connection and **Deploy**.

END OF STEPS

3.14 Bundling rule

Bundling rule definition

When an ASON NPA is built, the related TE-Links are automatically created in the NFM-T and in the involved GMREs.

The creation of the TE-Links is based on the following:

- Defined SRGs
- Bundling rule with the same risks and cost: The physical connections having the same type, cost, protection, and belonging to the same Shared Risk Groups are grouped in the same TE-Link.

The user labels of the TE-Links are automatically created by NFM-T and forwarded to the GMREs.

3.15 High-level provisioning flow for Layer 0 GMRE

Layer 0 GMRE provisioning flow

The Layer 0 GMRE is a Control Plane network at the ODUk layer rate supported by the 1830 PSS WDM/photonic NEs. The overall process of establishing connections follows the G.709 standard. Each layer rate is established in the network starting with the physical network.

Prerequisite

The high-level provisioning flow for Level 0 GMRE is as follows

- Physical connection creation occurs within the optical network.

  All required external or internal OTS or OS physical connections are typically auto discovered by the system. If they are not auto discovered, they are created by the user. The physical connections are both external (between NEs) and internal (within an NE). Typically, both are automatically discovered through notifications from the NE or when a synchronization is initiated with the NE.
- The OMS layer is created.

  The OMS layer rate is automatically discovered by the system.

  Once the physical connections are created, the OTN Manager automatically discovers the OMS layer rate and makes this connection layer available to the ASON Manager. For L0 optical connections, the ASON Manager uses the OMS layer rate to provision the OTU or ODU Control Plane connections.
- ASON Manager takes control of the OMS layer rate.

  The ASON Manager takes control of the OMS layer rate when the user assigns the OMS to an NPA. The ASON Manager creates a separate connection, called an ASON link, once the NPA assignment is made. The ASON links carry the ASON connections.

  User provisioning includes the following steps:
  - Users must assign the OMS connection to the NPA in the ASON Manager.

    For optical provisioning, the OMS layer rate is shared with the ASON Manger to ensure that the ASON Manager has knowledge of the connectivity between the NEs. When the user assigns the OMS to an NPA, the ASON Manager notifies the OTN Manager so that the OMS layer is not used to support Managed Plane connections, which reserves the OMS for Control Plane connections. In the OTN Manager, the connection is changed to a category of ASON link, indicating that it is in use by the ASON Manager.
  - Users must make SRG assignments and associate connections with TE links within the ASON Manager.

    An SRG represents a group of connections that all pass through the same physical failure points in the network. The establishment of proper SRGs in the network is important to ensure that a primary and backup connection are not set up through the same failure points, even though they may be utilizing different fibers. A failure point may be a shared conduit or other such physical structure.
- **Provisioning the Control Plane ODUk connection**

  Users can provision the ODUk nominal route through the network using the ASON links (OMS layer rate) as servers. When implemented in the network, the ODUk and the OTUk connections are set up in tandem. The OTN Manager tracks the OTUk nominal route.

When the ODUk is provisioned, GMRE automatically creates OTUk connections. As the ODUk is created in the ASON network, the OTUk servers are created in parallel. Both layer rates are therefore created at the same time. The ASON Manager establishes a nominal route in the network. The OTN Manager maintains the OTUk nominal route information and provides access to the current route on demand.

This nominal route through the 1830 PSS OCS NE network contains one of the following ODUk connection types:

- For an HO-ODUk terminated connection, an HO-ODUk connection is created and the DSR client of the connection is automatically discovered and inventoried in the OTN Manager.
- For a LO-ODUk terminated connection, an LO-ODUk connection is created and the ODUk is terminated within the Control Plane (entirely in the ASON domain). The three connections that are generated, which are LO-ODUk, HOODUk, and OTUk, are all shared with and inventoried by the OTN Manager
- For a LO-ODUk un-terminated connection, an LO-ODUk connection is created and is it not terminated; meaning, it extends beyond the Control Plane into the Managed Plane. If the extension is to an NE that is managed by the NFM-T, the OTN Manager then extends the connection to the next managed object. This connection is then classified as a mixed plane connection and is locked so the ASON Manager cannot delete the connection until the connection is free. When the LO-ODUk mixed plane connection is created, the system automatically discovers the DSR client on the LO-ODUk

  Because the OTN Manager maintains the OTUk nominal route information, the OTUk/ODUk connections are now visible to the user on the OTN connection list, which is accessible through the OTN path. In addition, the OTUk/ODUk connections are now visible to the user on the Control Plane Tandem Connections list.

• **The Managed Plane connection is established**

Digital Service Rate (DSR) is a term that is used generically to represent the service rate of a connection that is being provisioned. When provisioning the service path, users must select the actual Service Rate of the connection in order for the connection to be implemented.

The LO-ODUk/DSR connection is provisioned in the network as a Managed Plane connection that uses an optical ODUk Control Plane connection

When the DSR connection is discovered, users can then use the OTN path to make any needed changes to the LO-ODUk/DSR path connection in the Managed Plane using the optical ODUk Control Plane connection.

If, for some reason, the DSR connection is not discovered, users can use the OTN path to create the LO-ODUk/DSR path connection in the Managed Plane using the optical ODUk Control Plane connection. Refer to the “Create a New Trail or Path in OTN” task in the OTN Guide.

Figure 3-35 High level provisioning flow for Layer 0 GMRE

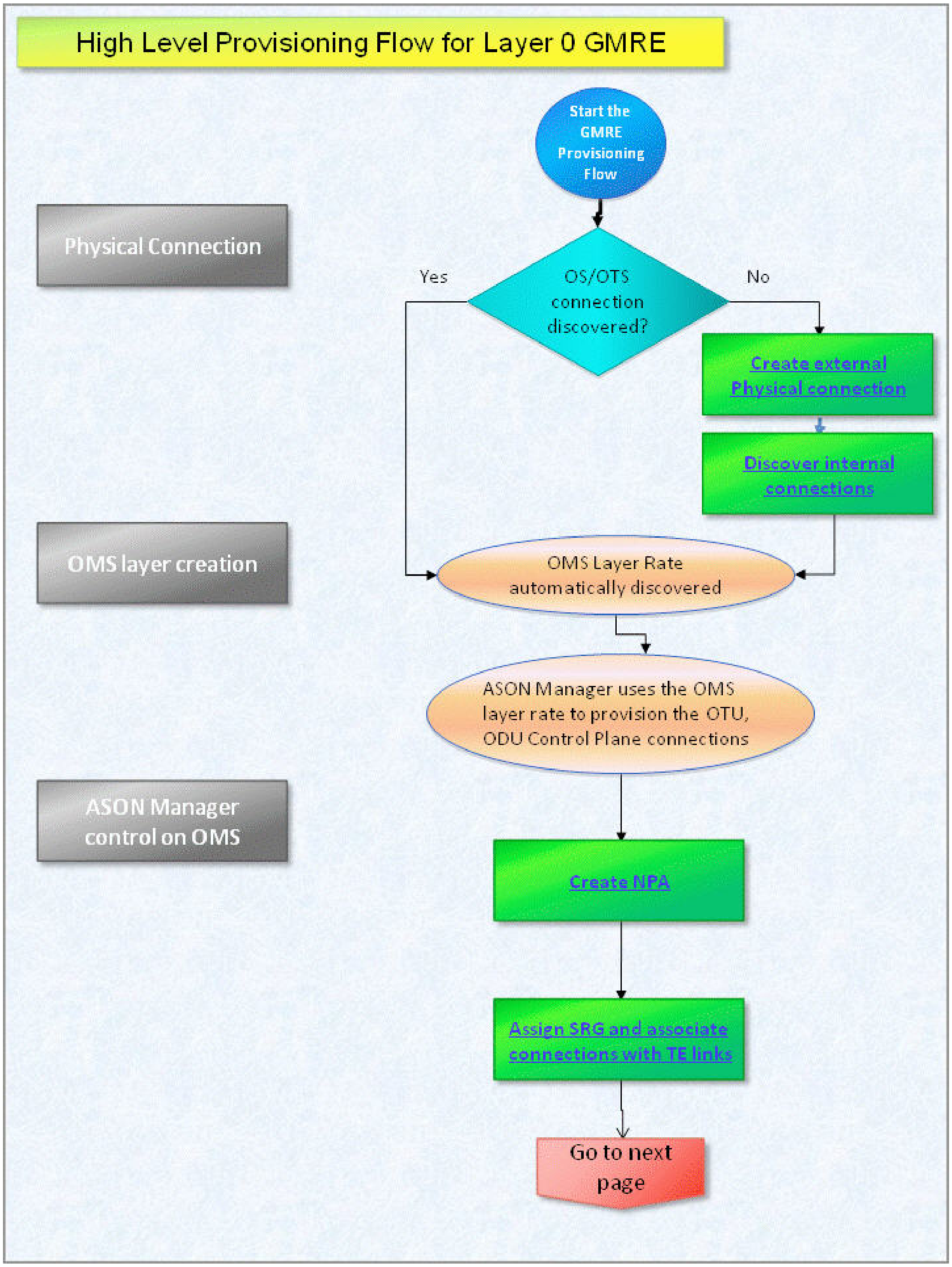
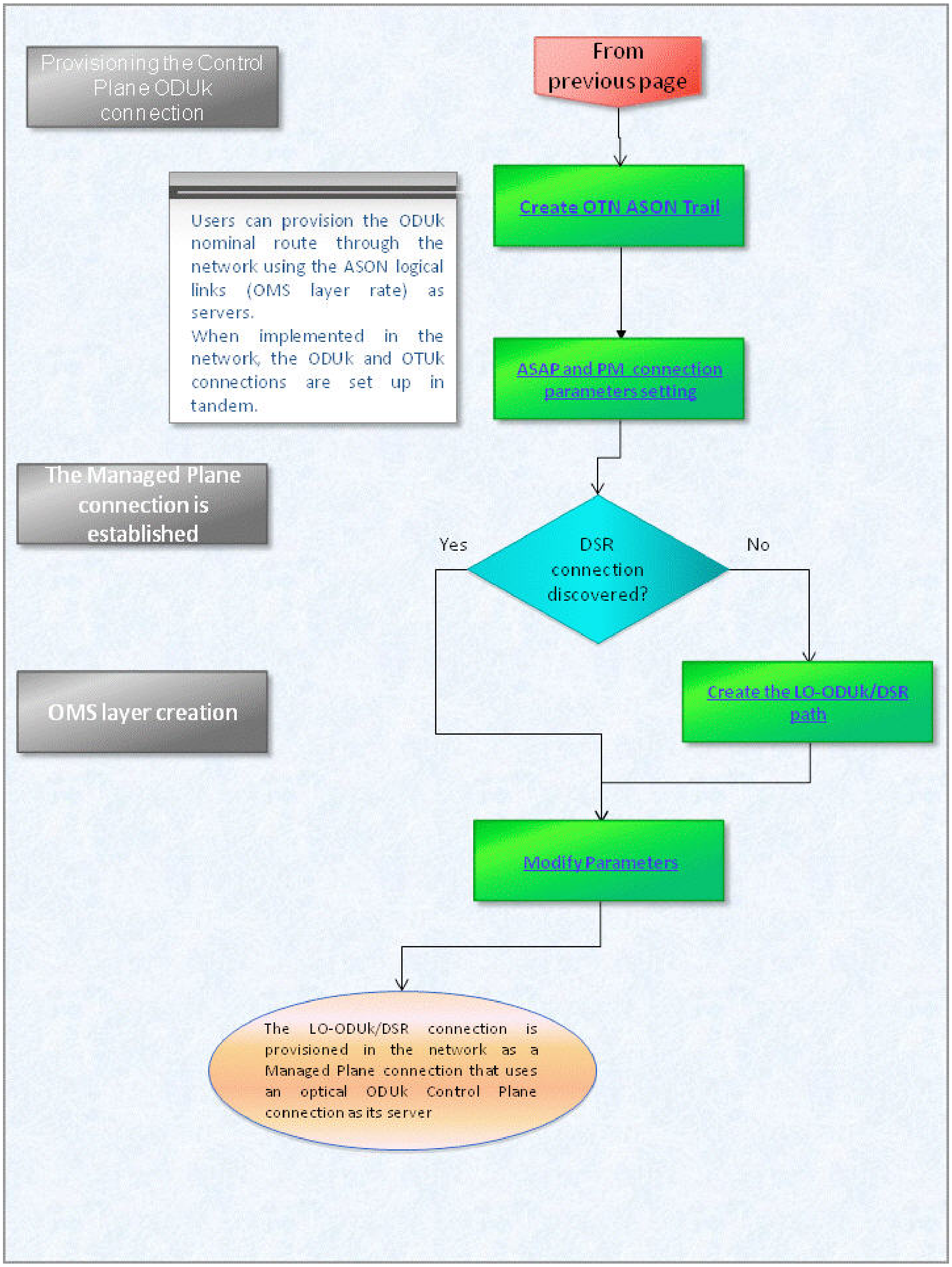


Figure 3-36 Provisioning the Control Plane ODUK connection



3.16 High-level provisioning flow for Layer 1 GMRE

Layer 1 GMRE provisioning flow

The Layer 1 GMRE is a Control Plane network at the ODUk layer rate that is supported by the 1830 PSS OCS NEs. The overall process of establishing connections follows the G.709 standard. Each layer rate is established in the network starting with the physical connectivity. The base network is build up until the connectivity between the 1830 PSS OCS network is established at a rate that supports the ODUk Control Plane layer rate. The optical network connectivity, if it is present in the network via 1830 PSS WDM/photonic NEs, is also established first to provide connectivity between the 1830 PSS OCS NEs.

The high-level provisioning flow for Level 1 GMRE is as follows:

1. Physical connection creation occurs within the optical network

   All required OTS or OS physical connections are typically discovered by the NFM-T. If they are not discovered, they can be created by the user. The physical connections are both external (between NEs) and internal (within an NE). Typically, both are automatically discovered through notifications from the NE or when a synchronization is initiated with the NE.

   All internal and external physical connections are established in the system

2. The OMS layer is created

   The OMS layer rate is automatically discovered by the system.

   Once the physical connections are created, the OTN Manager automatically discovers the OMS layer rate and makes this connection layer available to the ASON Manager.

3. ODU L-OPC is provisioned in case of server photonic network between OCS.

4. L-OPC assignments are made to the NPA and SRG.

   User provisioning includes the following steps:

   - The L-OPC connection is assigned to the ASON Manager for use in ASON connections, which is done by assigning the connection to an NPA within the ASON Manager. The ASON Manager creates a separate connection, called an ASON link after the NPA assignment is made. The ASON link carries the ASON connections.

     When a connection is assigned to an NPA, the ASON Manager notifies the OTN Manager that the connection supports Control Plane traffic and is no longer used to support Managed Plane connections. The OTN Manager tracks and lists the connections that are being used by the ASON Manager by labeling them as ASON logical links.

     Users can view these ASON logical links in the Connection list within the OTN Manager by filtering the Category Column for ASON Logical Links

   - Users must make SRG assignments and associate connections with TE links within the ASON Manager.

5. The ODUk Control Plane connection is established.

   Users can now use the ASON navigation path on the GUI to create an ODUk connection through the network.

   Notes:

   \- For ASAP settings, all ASON connection parameters are set through the ASON Manager.

- For a Mixed Plane, the ASON connection parameters are set through the ASON Manager and the Managed Plane connections are set through the OTN Manager.

- For ASON routed NNI service, ENE is mandatory. For ASON routed UNI service, ENE is not required .

3.17 Layer 1 GMRE provisioning flow for Mixed Plane services

For detailed information to create connections and logical links see "Deploy a new service or infrastructure connection with template" (p. 1216).

1

Create L1 Control Plane Network mix of 1830 PSS12x/ 1830 PSS8x/ 1830 PSS24x and provision OPS/Logical Links between L1 nodes.

2

Add all the OPS/Logical Links to the NPA as NNI, then unlock all the links. See 10.27 "Set the ASON administrative state of links" (p. 1504) and 10.15 "Add links and remove links from ASON" (p. 1462).

3

Create the OPS links between port on the Managed Plane node/External Network and port on Control Plane node.

Note:

- Managed Plane Node can be 1830 PSD, 1830 ONE or any other non GMRE configured node.

4

Add the above created OPS links to NPA as dropped link.

Note: For L1 Control Plane unterminated services with 1830 PSS 24x,1830 PSS 12x, 1830 PSS 8x, the creation of OPS link to external network is necessary. This link must be inserted in ASON NPA as drop link before service creation.

5

Create the Mixed plane service from end to end.

6

Mixed Plane Service is created.

END OF STEPS

4 Protections

4.1 Overview

Purpose

This chapter provides users with the conceptual information that is needed to understand the equipment and network protections managed in NFM-T.

Contents

Protection types

4.2 Equipment protection

Y-Cable protection

Y-Cable protection is a client side protection mechanism which protects the line card, client-side laser, network-side laser, and network-side fibers (assuming diverse fiber routes). Y-Cable protection is based on permanent head end bridging and tail-end selection, with a pair of OT cards at each end. The head-end bridge is done by employing a splitter on the received signal for the client-side ports. The incoming signal from the customer equipment is split and received by both the working and protection OT cards. The tail-end selection is accomplished by one of the working/ protection OT cards by turning on the TX client-side laser, while the other turns off the laser. The TX signal is channeled through a reverse splitter and sent to the customer equipment. Either the working or protection card can drive the signal through the reverse splitter. See 4.4 “Y-Cable protection” (p. 430).

OPSB and OPSB5 protection

Optical Protection Switch Board (OPSB) is a type of protection that is provided by an OPSB, which is an 1830 PSS NE card that supports client-side OPS protection. The OPSB card uses a non-latching switch, which means that upon power failure, the OPSB automatically switches back to the default path of the connection. It provides 1+1 protection with shelf diversity.

The OPSB5 is a multi-ports OPSB client protection that provides five sets of OPSB client protection. OPSB5 supports all the functionality that are supported by OPSB. See 4.5 “OPSB and OPSB5 protection” (p. 447).

OMSP – OMS SNCP

Optical Multiplex Section Protection (OMSP) is the protection that protects both optical amplifiers and transmission fibers. See 4.6 “OMSP – OMS SNCP” (p. 481).

OLP (OTS) protection

Optical Line Protection (OLP) system increases the stability and reliability of the optical network avoiding the problems related to optical fiber faults and line interruption. OLP is based on the principle of the optical switch to build a backup path on free optical fiber. Simple optic protection includes a primary path and a secondary path. The commonly used fiber protection is based on the 1+1 scheme. See 4.7 “Optical Line Protection” (p. 487).

4.3 Network protection

SNC protection

SNC protected connection has managed plane SNC network protection, control plane SNC protection, managed plane client SNC protection or a combination of these types.

Subnetwork Connection Protection (SNCP) can be specified for infrastructure connections (trails) or services to create protected cross connections. MP SNCP is Managed Plane SNCP where the protection group is in the managed plane domain. CP SNCP is the Control Plane SNCP where the protection group is in the control plane domain. A mixed plane connection has MP SNCP, CP SNCP or both. See 4.8 "SNC protection" (p. 495).

Electrical Sub-Network Connection Protection

Electrical Sub-Network Connection Protection (E-SNCP) is a line side (network-side) protection mechanism that protects against the loss of line signal due to an OTM failure, fiber interruption, or a malfunction of an intermediate node or NE. See 4.9 "Electrical Subnetwork Connection Protection (E-SNCP)" (p. 505).

OPS protection

The OPS supports two types of protected line configurations *Internal OT, no SVACs* and *Alien/ External OT, redundant SVACs*. In both cases, there is a single unprotected OT at each end. In both cases, the working and protection lines must be diversely routed across the network (no shared risk groups in common). See 4.10 "OPS protection" (p. 507).

OPSA and OPSFlex protection

Optical Protection Switch Advanced (OPSA) is a type of enhanced network protection using the OPSA board that supports server-side OPS protection. OPSA provides 1+1 OCH, OMSP, or OLP protection over DWDM lines. See "OPSA protection definition" (p. 509).

The OPSFlex card acts as an OPSA, is an OCH optical channel protection card. OPSFlex supports protection of OCH channel with flexgrid. See "OPSFlex protection definition" (p. 511).

See "Protected Connections " (p. 1088) for more details on Protected Connections.

Equipment protection

4.4 Y-Cable protection

Y-Cable definition

A Y-Cable, also called a splitter or signal splitter, is a type of cable that contains three ends. One end of the cable is common; the other end splits into two leads.

Best practice templates for Y-Cable protection

The Y-Cable protection feature is available for SONET, SDH, and Ethernet service connections.

From the NFM-T GUI, navigate to **DEPLOY > New Service/Infrastructure Connection** and select one of the following templates from the **Service/Infrastructure Templates** deploy window to provision Y-Cable service connection:

- **OC-N**, known as the *SONET Y-Cable Protected* template
- **STM-N**, known as the *SDH Y-Cable Protected* template

Y-Cable general provisioning guidelines

The following general provisioning guidelines apply to the SONET Y-Cable Protected and SDH Y-Cable Protected Best Practice templates:

- If connection shape is bidirectional, users can specify the **Switch Mode** to be **Unidirectional** (the default) or **Bidirectional**. For switch modes that are **Bidirectional**, users can optionally enable or disable **Revertive Mode**. If the **Revertive Mode** is enabled, users can then specify the **Wait to Restore Time (min)**.
- If the values of **Switch Mode**, **Revertive Mode**, or **Wait to Restore Time (min)** are different for the A End and Z End of a **2 Ended Bi (I)** connection, the values from the A End connection are set for the connection. A discrepancy is not reported for the connection. The Network Elements Cross Connection list displays the values of all three fields for each protection group.
- All Y-Cable ports must be on the same type of card.

  The **From OT Working Port**, **From OT Protection Port**, **To OT Working Port**, and **To OT Protection Port** must all be on the same type of card. Note that the 11STAR1 and 11STAR1A are considered the same type of card.
- All Y-Cable ports must use the same port number.

  When selecting ports for **To OT Working Port**, **From OT Protection Port**, and **To OT Protection Port**, the port must be the same port number on the same type of card as that of the **From OT Working Port**.
- All Y-Cable ports must have a signal type that matches the service rate of the connection.

  If the **From OT Working Port**, **From OT Protection Port**, **To OT Working Port**, or **To OT Protection Port** is already assigned, it must be assigned with the user selected Service Rate.

  Example: If the Service Rate is 10GbE, an assigned port must have a signal type of 10GbE.
- Working/protection port role designations must be specified consistently for a card.

If the card containing the **From OT Working Port** or **To OT Working Port** has any other protection groups, all ports in the protection group on the card must be the working port of the protection group. Similarly, if the card containing the **From OT Protection Port** or **To OT Protection Port** has any other protection groups, all ports in the protection group on the card must be the protection port of the protection group.

Example: All working ports must be on one OT, and all protection ports must be on the other OT.

In addition:

Each OT can only have Y-Cable connections to one other OT.

The card containing protection port for the existing protection group must be the same as the card containing the **From OT Protection Port** or **To OT Protection Port**. Similarly, the card containing working port for the existing protection group must be the same as the card containing the **From OT Working Port** or the **To OT Working Port**.

Example: If slot 3 has one Y-Cable connection to slot 4, then additional Y-Cable connections from slot 3 can only be made to slot 4.

Note: Provisioning guidelines applies to the 11DPE12/11DPE12E, 11DPM12, 12P120, 1830 PSS-24x with 30AN300 and 4AN400, 1830 PSS-OCS NE with 10AN10GC and 1AN100G, and 1830 PSS PHN with 260SCX2 cards. See the following topics for more details:

- “Y-Cable protection for 11DPE12 and 11DPE12E cards” (p. 431)
- “Y-Cable provisioning guidelines for the 11DPM12 card” (p. 432)
- “Y-Cable protection on 12P120 for additional client types” (p. 435)
- “Y-Cable protection for 1830 PSS-24x with 30AN300 and 4AN400 cards ” (p. 437)
- “Y-Cable protection for 1830 PSS-OCS NE with 10AN10GC and 1AN100G cards” (p. 440)
- “Y-Cable protection for 1830 PSS PHN with 260SCX2 card ” (p. 441)

Y-Cable protection for 11DPE12 and 11DPE12E cards

The following Y-Cable protection guidelines apply to 11DPE12 and 11DPE12E cards:

- Only the 1830 PSS-4 supports Y-Cable protection for 11DPE12 and 11DPE12E cards.
- The cards containing the **From OT Working Port**, **From OT Protection Port**, **To OT Working Port**, and **To OT Protection Port** must all have the same Ethernet Operational mode (Full Rate, Sub Rate, or QinQ mode).
- The same **From OT Working Port**, **From OT Protection Port**, **To OT Working Port**, and **To OT Protection Port** must be selected as the current connections if the connection shape is 2 Ended Bi (I) and the OT Working and Protection Ports are in Sub Rate or QinQ mode and if the **From port ID1** of the format OPS-{shelf}-{slot}-SIG{1...12}-{1-10} is not the first CTP of the OPS-{shelf}-{slot}-SIG{1... 12}OS PTP that is to be used in a connection.

  The same **From OT Working Port** and **From OT Protection Port** must be selected as the current connections if the connection shape is 3 Ended Z Bi (I) and the OT Working and Protection Ports are in Sub Rate or QinQ mode and if the **From port ID1** of the format OPS-{shelf}-{slot}-SIG{1... 12}-{1-10} is not the first CTP of the OPS-{shelf}-{slot}-SIG{1...12}OS PTP to be used in a connection,

  The same **To OT Working Port** and **To OT Protection Port** must be selected as the current connections, if the connection shape is 3 Ended A Bi (I) and the OT Working and Protection

Ports are in Sub Rate or QinQ mode and if the **To port ID1** of the format OPS-{shelf}-{slot}-SIG{1... 12}-{1-10} is not the first CTP of the OPS-{shelf}-{slot}-SIG{1...12}OS PTP to be used in a connection.

If not, the system outputs the following message:

`Y-Cable Ports not the same as existing connections.`

- For Sub Rate or QinQ mode, the Client VTS on the **From OT Working Port**, **From OT Protection Port**, **To OT Working Port**, and **To OT Protection Port** must use the same port number. For example, it must be port **`C1-1`** or all must be **`C1-2`**. If not, the system outputs the following message:

  `All Client VTS on Y-Cable Ports must use the same port number.`

Y-Cable provisioning guidelines for the 11DPM12 card

The following Y-Cable provisioning guidelines apply to the 11DPM12 card:

- The CTP on the **From OT Working Port**, **From OT Protection Port**, **To OT Working Port**, and **To OT Protection Port** must be cross connected to a CTP on the Line Port 1 of the OT; it cannot be cross connected to a CTP on the Line Port 2 of the OT. If not, the system outputs the following message:

  `Y-Cable protection only allowed with Line Port 1 of OT.`

  Example: The 11DPM12-[shelf]- [slot]-L1-1-8 can be cross connected to the **From OT Working Port**, but the 11DPM12-[shelf]-[slot]-L2-1-8 cannot.
- The CTP on the Line Port that is cross connected to the **From OT Working Port** must be the same CTP on the Line Port that is cross connected to the **From OT Protection Port**; and the CTP on the Line Port that is cross connected to the **To OT Working Port** must be the same CTP on the Line Port that is cross connected to the **To OT Protection Port**. If not, the system outputs the following message:

  `The same LO ODUk CTP on the Line Ports must be used for the Working and Protection Paths for Y-Cable protection.`

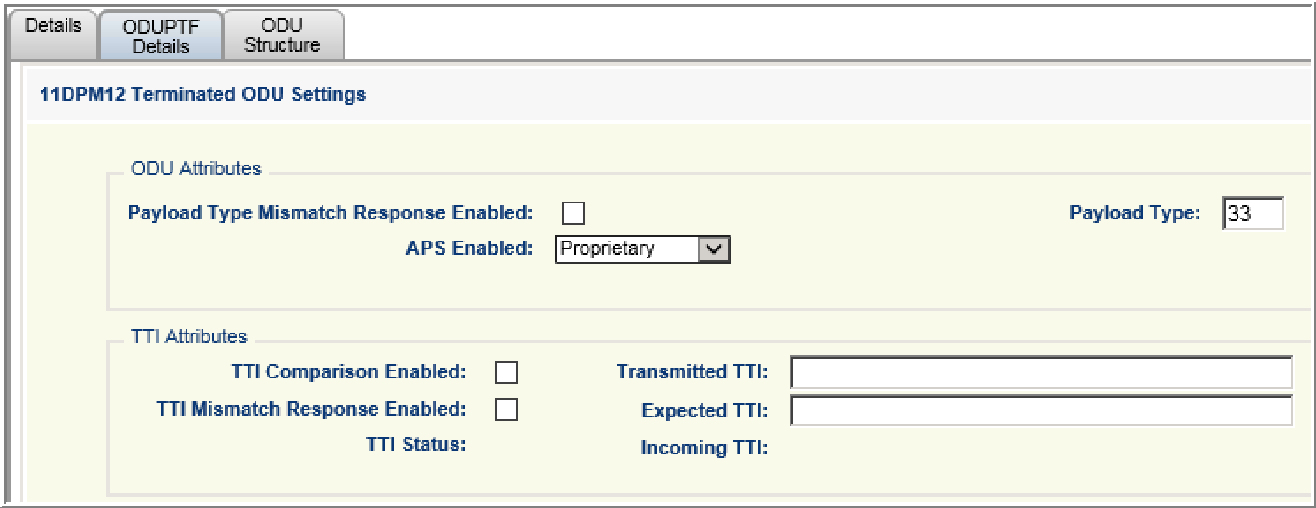
  Example: If the CTP that is cross connected to the **From OT Working Port** is 11DPM12-[shelf]-[slot]-L1-1-8, then 11DPM12-[shelf]-[slot]-L1-1-8 must be the CTP that is cross connected to the **From OT Protection Port**.

Note: For interworking between 11DPM12 and 1830 PSS-OCS services:

If the Y-Cable service involves interworking of 11DPM12 and 1830 PSS-OCS, then during the Infrastructure connection creation, the user has to select the field **APS Enabled** on the **Modify Transmission Parameter** window, the value **`Use NE Value`**, not the default value **`Standard`**.

By default, APS enabled value is set as Proprietary when 11DPM12 card is provisioned, so it is necessary to modify the value during the infrastructure connection creation.

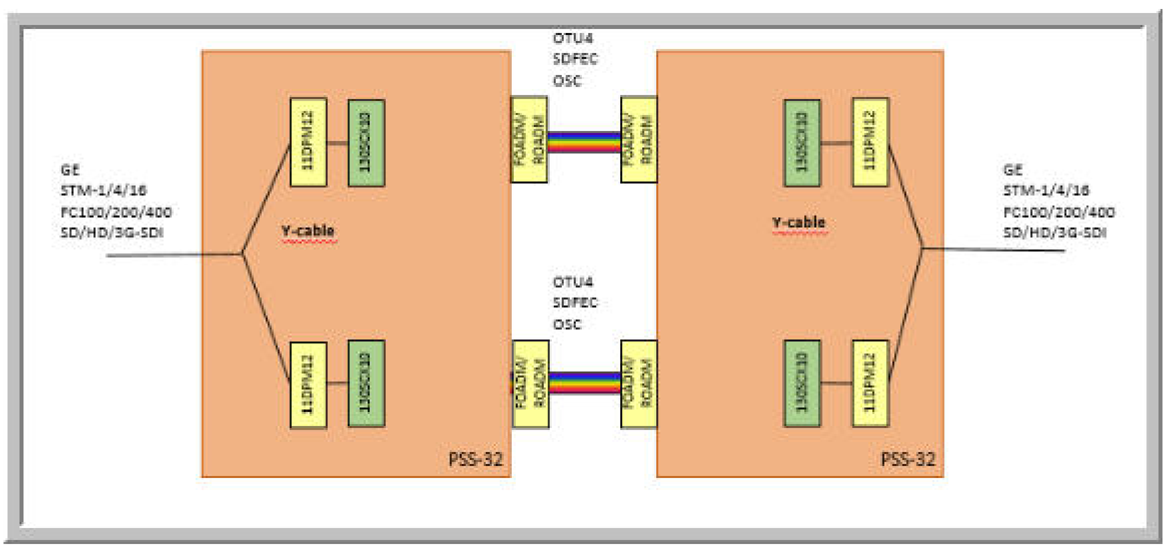
Figure 4-1 Default APS Enabled on NE



The NFM-T supports the enhancement of Y- Cable on 11DPM12 with bidirectional flow and Revertive Switching according to the Wait Time to Restore (WTR) time value.

The following figure displays the applicable scenario:

Figure 4-2 Bidirectional and Revertive Switching on 11DPM12 applicable scenario



The WTR time is set using NFM-T GUI template during the service creation or, alternatively in Modify template.

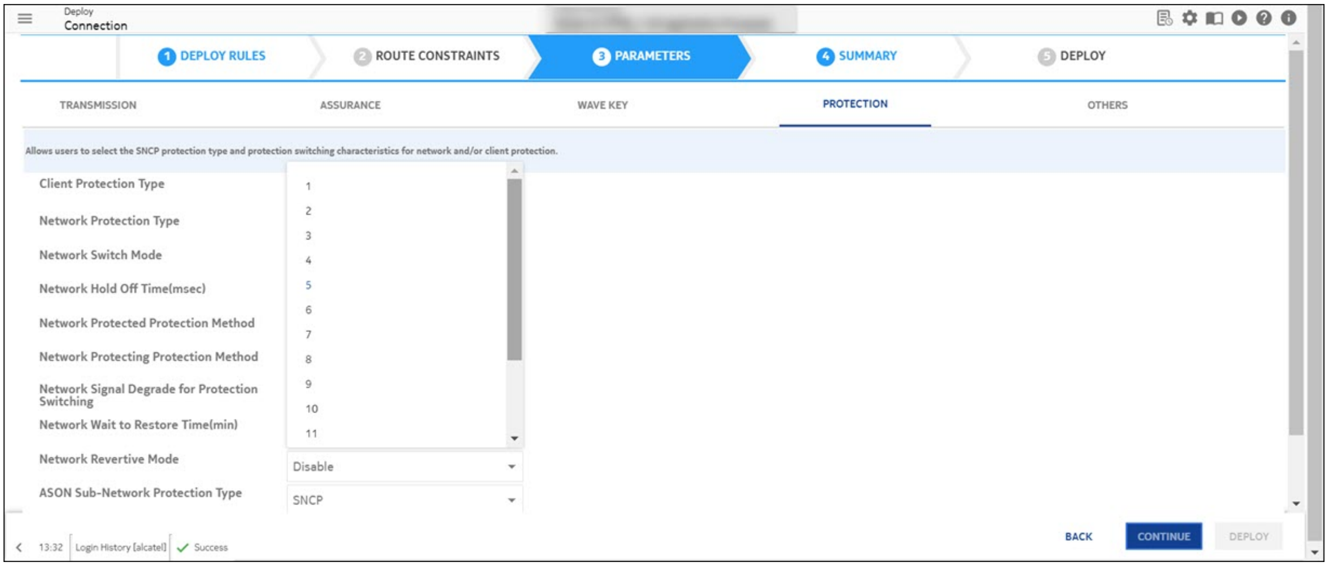
Once the fault condition has cleared, the network enters into the WTR state previously set.

Revertive switching means that traffic is switched back to service path once the WTR time previously set is terminated.

This characteristic is useful to reduce latency when the backup path is longer than service path.

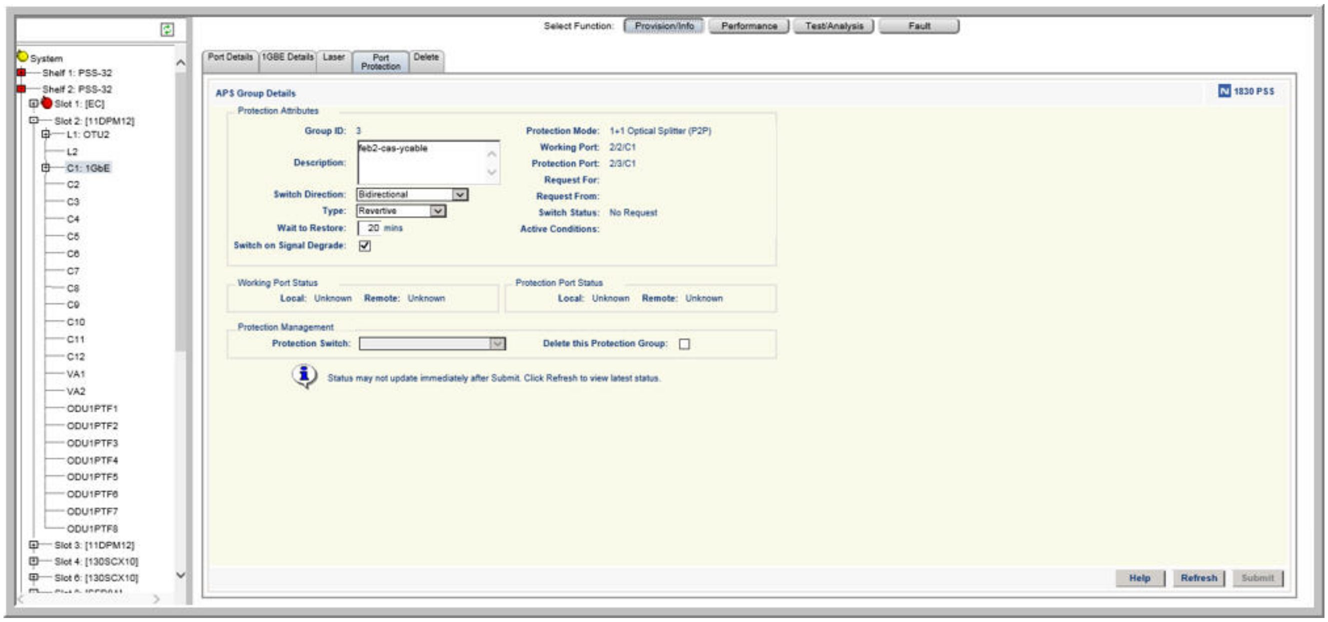
The WTR time can be selected in a time span from 1 to 20 minutes with intervals of 1 minute as shown in Figure 4-3, “Wait Time to Restore Set Up” (p. 433).

Figure 4-3 Wait Time to Restore Set Up



The Y-Cable Revertive Switch feature is displayed once the parameters is set as displayed in Figure 4-4, “Y- Cable Revertive Switching set table” (p. 435) .

Figure 4-4 Y- Cable Revertive Switching set table



Y-Cable protection on 12P120 for additional client types

The NFM-T supports additional client signals for the 12P120 card with Y-Cable protection, Managed Plane.

The Y-Cable protection feature is available for SONET, SDH, and Ethernet service connections.

The possible configurations are:

- Y-Cable for 12P120, up to six pairs of standalone 12P120 cards, with unidirectional, both revertive and non-revertive protection switch.
- CDC-F ROADM, DGE single bladed for CDC-F, ILAs for CDC-F.
- Both Managed Plane and Layer 0 Control Plane are required.

Note: There is no Layer 0 Control Plane for 12P120 Y-Cable. The Managed Plane, Layer 0 Control Plane, and Mixed Plane support is required.

In addition to the above guidelines, the general provisioning guidelines applies to the 12P120 for additional client types. See “Y-Cable general provisioning guidelines” (p. 430).

The following figures outline how the Y-Cable protection is configured in order to implement this feature with 12P120 card in 1830 PSS R9.1:

- Figure 4-5, “Y-Cable client protection scenario with CDC-F at both end” (p. 436)
- Figure 4-6, “Y-Cable client protection scenario with CDC-F at one end” (p. 436)
- Figure 4-7, “Y-Cable client protection scenario without CDC-F” (p. 437)

- Figure 4-8, “Y-Cable client protection scenario with CDC-F at both end, L0 GMPLS” (p. 437)

The managed signal clients are:

- OC-192
- STM-64
- OTU2
- OTU2e
- FC1200

The possible scenarios are shown in the following figures.

Figure 4-5 Y-Cable client protection scenario with CDC-F at both end

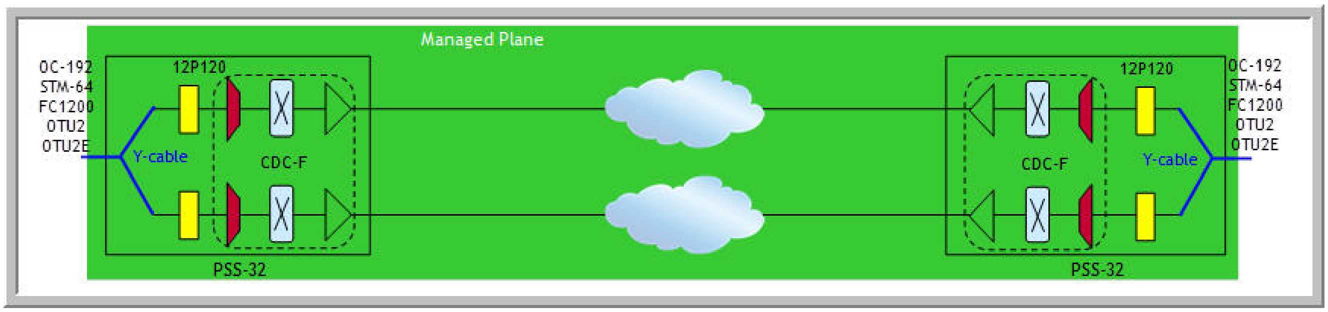


Figure 4-6 Y-Cable client protection scenario with CDC-F at one end

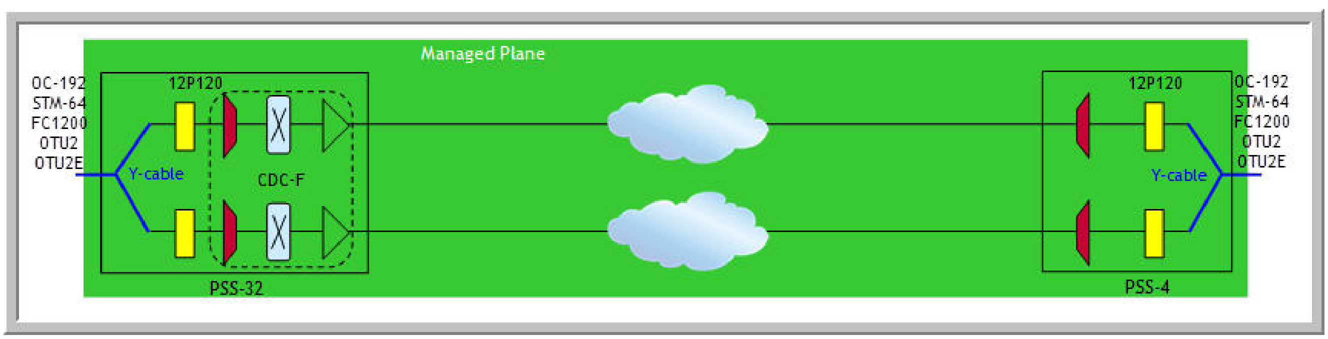


Figure 4-7 Y-Cable client protection scenario without CDC-F

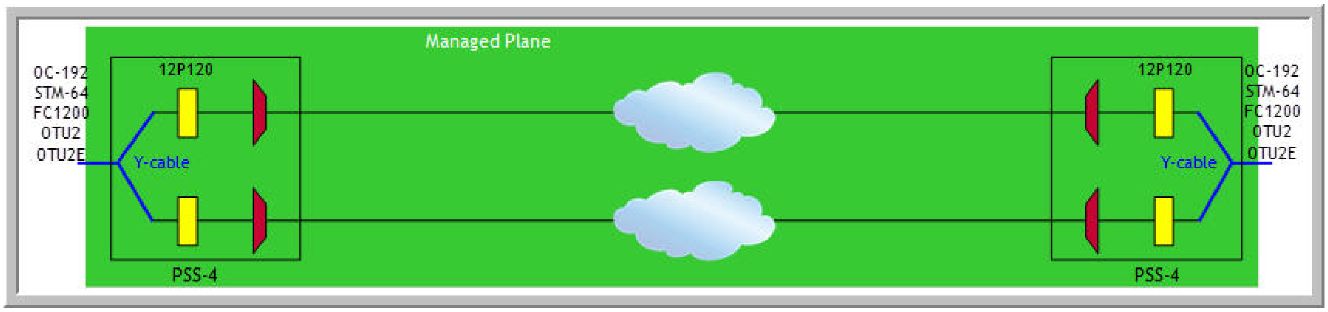
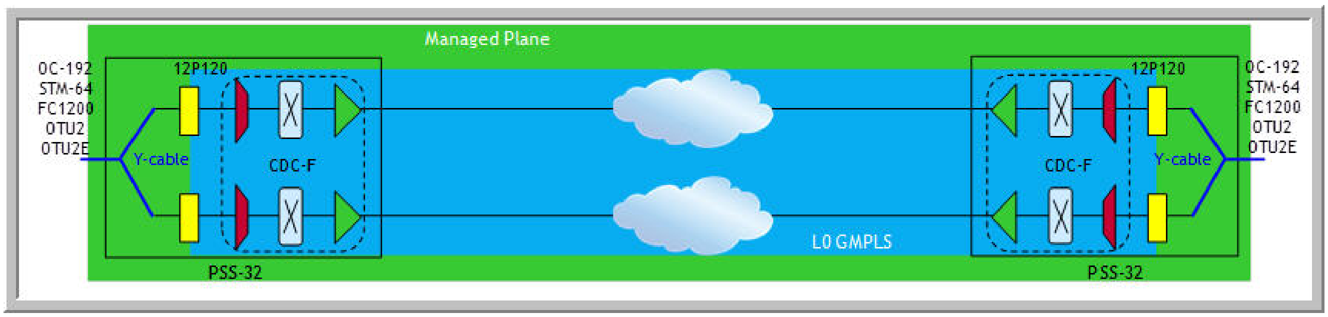


Figure 4-8 Y-Cable client protection scenario with CDC-F at both end, L0 GMPLS



Y-Cable protection for 1830 PSS-24x with 30AN300 and 4AN400 cards

The 1830 PSS-24x supports the Y-Cable protection in one shelf only, supplied with 30AN300 and 4AN400 cards from NFM-T Release 18.3 onwards.

The Y-Cable client protection, is in compliance with ITU-G.873.1 standard.

For the provisioning of the Y-Cable, the following rules apply:

- The cards must be housed in the same shelf (1830 PSS-24x) without any slot restrictions.
- The working and protection ports cannot belong to the same card.
- Only *non OTN* client signal rates are supported like 10GbE, OC-192, STM-64 with 30AN300 card and 100GbE with 4AN400 card. The involved ports must be in **Assigned** state. Working and protection ports must have the same type of client signal, with the same ODU container type.
- The working and protection ports can belong to different types of card, as long as the client signal rate is the same.
- For A-end and Z-end, the four cards involved can be of different card types, as long as the client signal rate must be the same.
- Y-Cable protection group of "G.873.1 Subtype" on the following cards/ports, <protection-port-aid> and/or <working-port-aid>:

- <shelf>-<slot> [1..30] - for client ports of 30AN300 on the NE, OPS- <shelf>-<slot>-C[1..30] is used for the NFM-T.
- <shelf>-<slot> [1..4] - for client ports of 4AN400 on the NE, OPS- <shelf>-<slot>-C[1..4] is used for the NFM-T.

Note: Y-Cable ports cannot be used by any other protection groups or protection group types (for example, SNC/NC).

Y-Cable protection support bidirectional, unidirectional without APS and revertive switching mode.

The following general considerations should be taken into account, to provision an NFM-T connection with Y-Cable protection:

- The provision of the Y-Cable is made by the Service Connection template and supported by OTN.
- The NFM-T/OTN connection supports the auto discovery, including topological link provisioning and protection group provisioning.
- Concerning the connection management:
  - HO-ODUk Infrastructure provisioning is achieved either by **Managed Plane** or **Layer 0 Control Plane** and **Managed Plane**.
  - Client Service provisioning is achieved either by **Managed Plane** or **Layer 1 Control Plane** and **Managed Plane**.
  - End-to-end management is achieved either by **Managed Plane** or **Mixed Plane**.

The Figure 4-9, "Y-Cable protection with 1830 PSS-24x for GbE and STM-16 clients signal" (p. 438) and Figure 4-10, "Y-Cable protection with 1830 PSS-24x and 11DPM12 – L1 mixed plane" (p. 439) depict the example of the interworking scenario between the 30AN300 and 11DPM12 cards:

The protection switching is triggered by the Signal Degrade.

Figure 4-9 Y-Cable protection with 1830 PSS-24x for GbE and STM-16 clients signal

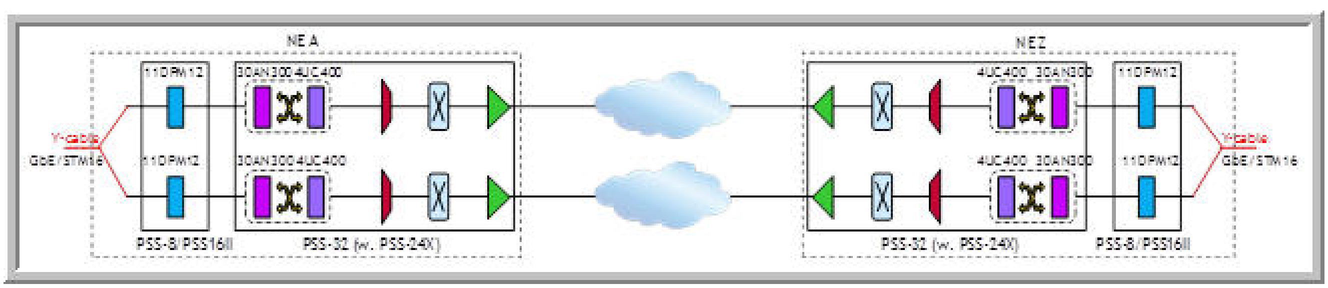
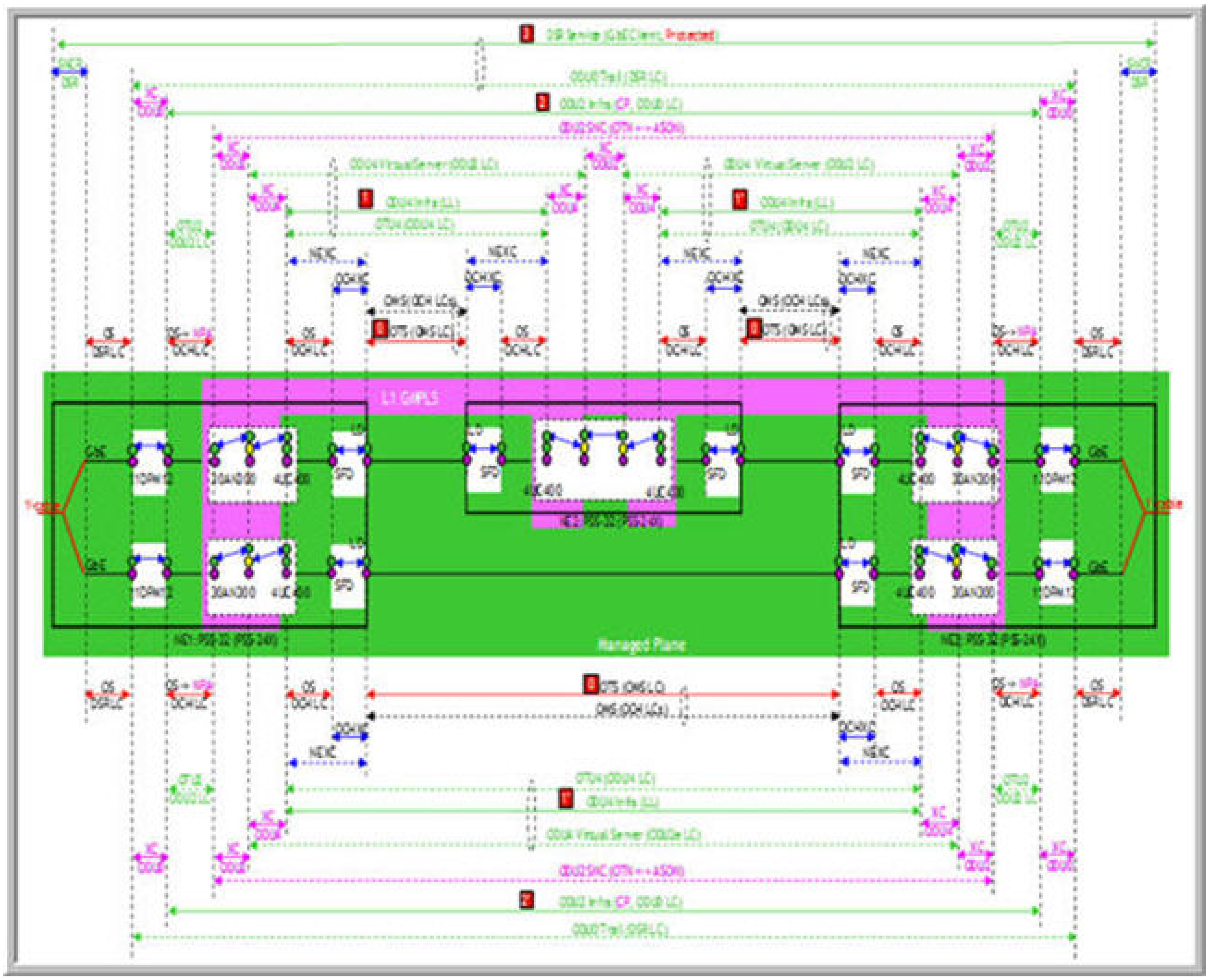


Figure 4-10 Y-Cable protection with 1830 PSS-24x and 11DPM12 – L1 mixed plane



Y-Cable protection for 1830 PSS-nx with Input/Output Cards

NFM-T supports Y-Cable client protection for 1830 PSS-nX (1830 PSS-8x, 1830 PSS-12x, and 1830 PSS-24x) NEs with additional I/O cards.

The following table provides shelves, cards, NE releases, NFM-T release, and the corresponding client signal types (non OTN client signal type only) mapping.

Table 4-1 Shelves, Card, Release, and Client Signal Mapping

Shelves	Card	NE Release onwards	NFM-T Release onwards	Supported Client Signal Types
1830 PSS-24x	10AN400	11.1	20.7	100GbE (ODU4)
1830 PSS-24x	20AN80	11.1	20.7	10GbE (ODU2, ODU2E, ODUflex)
		13.0.4	20.11	sub-10Gbe
1830 PSS-8x 1830 PSS-12x	4MX200	11.1	20.7	100GbE
1830 PSS-8x 1830 PSS-12x	20AX200	10.1 on 1830 PSS-8x 11.1 on 1830 PSS-12x	20.7	10GbE (OTU2, OTU2E, ODU2, ODU2E, ODUflex)
		13.0.4 on 1830 PSS-8x and 1830 PSS-12x	20.11	
1830 PSS-8x 1830 PSS-12x	20MX80	11.1, 13.0.4	20.7, 20.11	10GbE (ODU2, ODU2E, ODUflex)
		13.0.4	20.11	sub-10Gbe

The provisioning guidelines and management for Y-Cable client protection for the 1830 PSS-nX with additional I/O cards is in parity with the existing guidelines for 1830 PSS-24x with 30AN300 and 4AN400 cards. See “Y-Cable protection for 1830 PSS-24x with 30AN300 and 4AN400 cards ” (p. 437) for details.

Y-Cable protection for 1830 PSS-OCS NE with 10AN10GC and 1AN100G cards

NFM-T supports the Y-Cable protection on **1830 PSS-OCS NE**, with **Ethernet** and **SDH** client signals.

The protection applies to 1830 PSS-OCS with R10.0, equipped with 1830 PSS-36 and 1830 PSS-64 shelves and feasible with 10AN10GC and 1AN100G cards.

The managed client signals are:

- Ethernet clients: 10GbE (10AN10GC), 100GbE (1AN100G)
- SDH and SONET clients: STM-64/OC-192 (10AN10GC).

Y-Cable protection support on 1830 PSS-OCS NE:

- Unidirectional and bidirectional switching within 50 ms
- Revertive and non-revertive switching

- Support for hold-off timer

The Y-Cable protection resides in a single OCS shelf, there is no specific port pairing restrictions within the 1830 PSS-36 and 1830 PSS-64 shelf. The client signal type must be the same on the two I/O cards for Y-Cable.

Alarm protection is triggered by one of the following conditions: SF (Signal Fail, CI_SSF, dAID, dOCI, dLCK, dTIM), SD (Signal Degrade, dDEG). Client signal Fail (OPU-CSF) is used for non-OTN clients (from ODUkP) to trigger Y-Cable protection switching at the far-end.

Y-Cable protection for 1830 PSS PHN with 260SCX2 card

The 1830 PSS PHN supports the Y-cable client protection supplied with 260SCX2 card.

The Y-Cable provisioning must be performed using the following rules:

- The NE type is 1830 PSS PHN with 1830 PSS-32, 1830 PSS-16II, 1830 PSS-8 shelves.
- The Y-Cable supported client signal type is 100GbE.
- Protection switch operations supports forced switch, manual switch, and loop back.

Details about Y-Cable protection with Signal Degraded conditions can be found at: “Y-Cable protection triggered by Signal Degrade (SD)” (p. 445)

All the existing configurations that are supported for 260SCX2 are supported with Y-Cable protection.

This applies to Managed Plane and Layer 0 Control Plane.

Note: The Y-Cable provisioning rules should be followed, including both working and protection with the same OT type that means the two OTs should both be 260SCX2.

The following figures, show examples of Y-Cable support protection scenario interworking with 260SCX2 card.

Figure 4-11 General schema

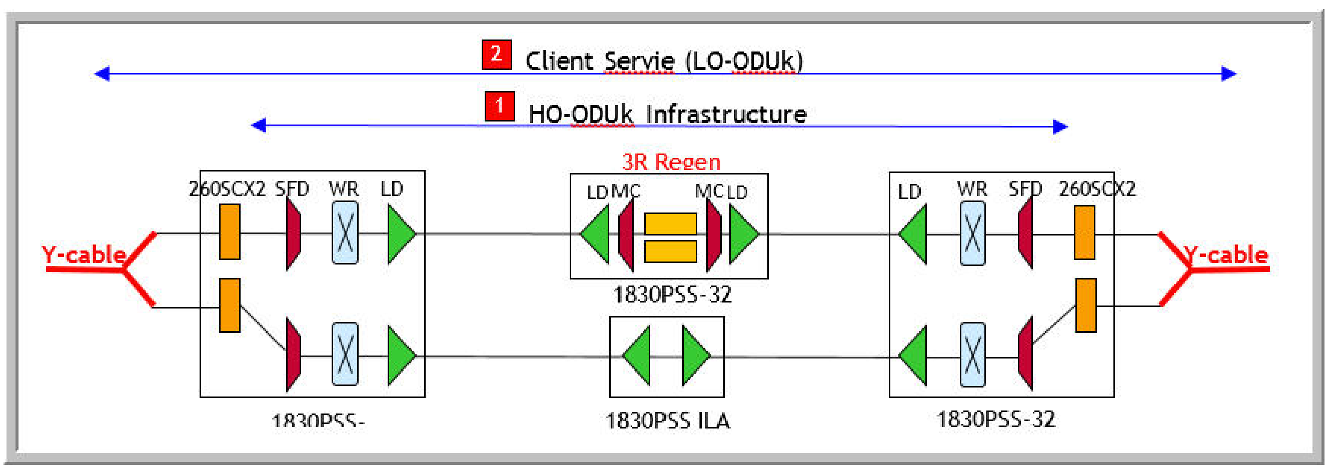


Figure 4-12 260SCX2 with Y-Cable protection – 100GbE Client, MP

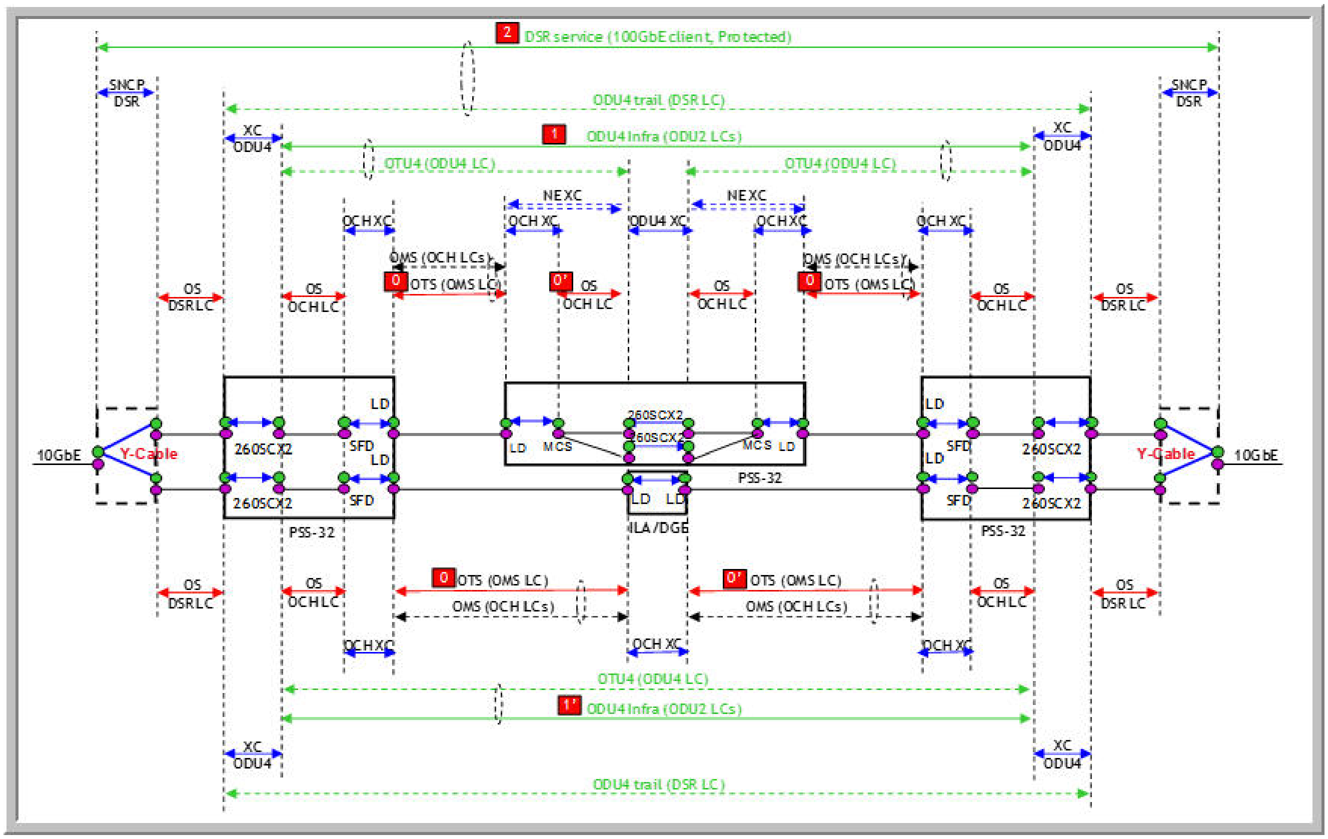
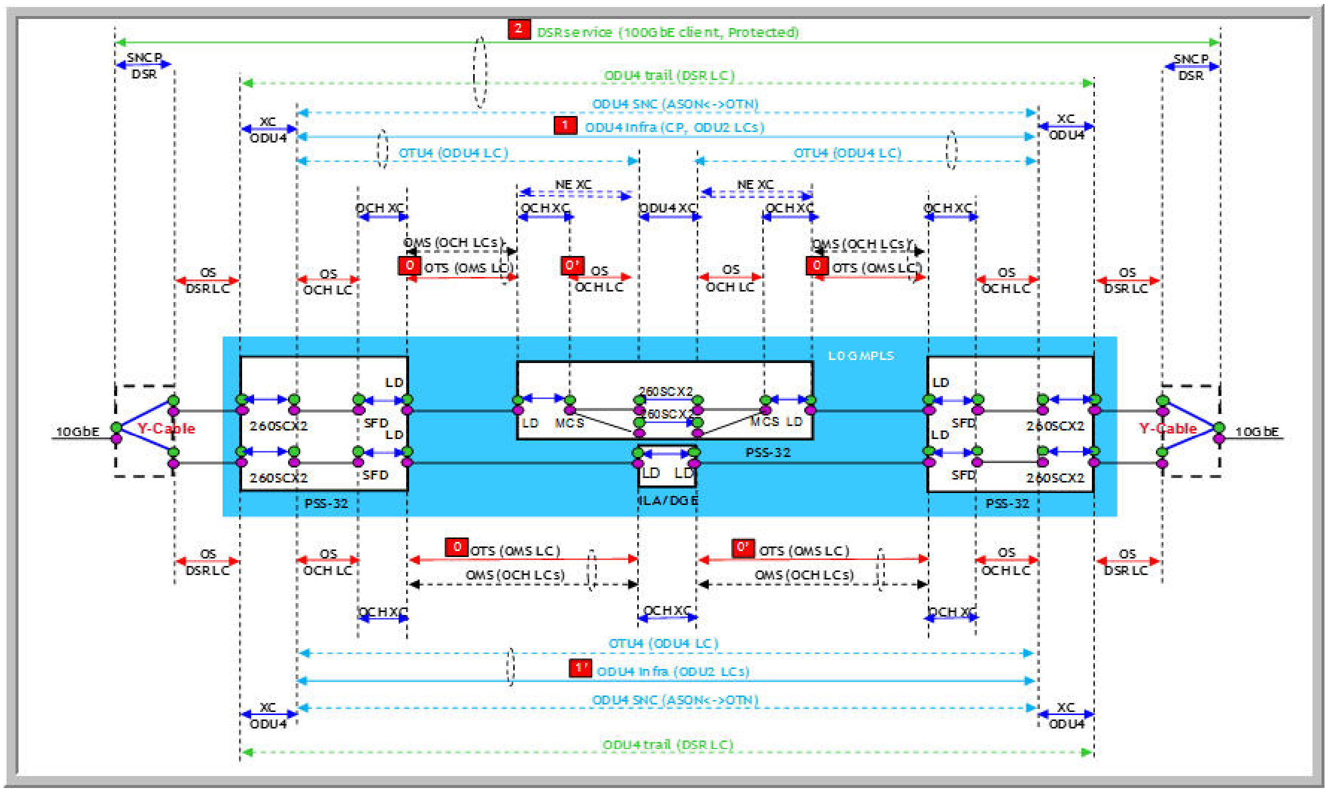


Figure 4-13 260SCX2 with Y-Cable protection – 100GbE Client, L0 CP



Managing Y-Cable protection

Following are some of the methods that are used to manage the Y-Cable protection:

- OS connections automatically created
- Protection group, OS links, and trails automatically deleted
- Y-Cable modifications
- Y-Cable protection triggered by Signal Degrade (SD)

OS connections automatically created

When creating a DSR or ODUk service with Y-Cable protection, the system automatically creates the OS connections between the following:

- The working ports on the Y-Cable cards and the client ports.
- The protected ports on the Y-Cable cards and the client ports.

Table 4-2 Connection Shape – OS Creation

If	Then
The Connection Shape is **2 Ended Bi (I)**	The following OS connections are automatically created: • An OS connection is created between the Working Port on the A End Y-Cable card and the client port that the user selects as the A End Working Port. • An OS connection is created between the Protection Port on the A End Y-Cable card and the client port that the user selects as the A End Protection Port. • An OS connection is created between the Working Port on the Z End Y-Cable card and the client port that the user selects as the Z End Working Port. • An OS connection is created between the Protection Port on the Z End Y-Cable card and the client port that the user selects as the Z End Protection Port.
The Connection Shape is **3 Ended A Bi (Y)**	The following OS connections are automatically created: • An OS connection is created between the Working Port on the Z End Y-Cable card and the client port that the user selects as the Z End Working Port. • An OS connection is created between the Protection Port on the Z End Y-Cable card and the client port that the user selects as the Z End Protection Port.
The Connection Shape is **3 Ended Z Bi (Y)**	The following OS connections are automatically created: • An OS connection is created between the Working Port on the A End Y-Cable card and the client port that the user selects as the A End Working Port. • An OS connection is created between the Protection Port on the A End Y-Cable card and the client port that the user selects as the A End Protection Port.

Note: If the From OT Working Port, From OT Protection Port, To OT Working Port, and To OT Protection Port are on 11DPE12 or 11DPE12E cards with the mode of SubRate or QinQ, all of these automatically created OS connections are created except that OS connections are only created for the first DSR connection that uses a client port.

Protection group, OS links, and trails automatically deleted

To delete a Y-Cable protected service, the user need not delete the protection group, OS links, and any LO-ODUk trails (which are applicable on 11DPM12 cards) to delete the Y-Cable protected service. When users delete a Y-Cable protected service, the system automatically deletes the associated Y-Cable protection group, the OS links that are on the Y-Cable, and its associated LO-ODUk infrastructure connections (trails).

Y-Cable modifications

For modifications of Y-Cable parameters, the following apply:

- If the connection shape is bidirectional, the **Switch Mode** displays the values of **Unidirectional** and **Bidirectional**.
- If the **Switch Mode** is **Bidirectional**, the **Revertive Mode** is displayed and its default value is the current value of the connection. If the connection does not have a current value, the default is **Disabled**.
- If the **Revertive Mode** is **Enabled**, the **Wait to Restore Time (min)** is displayed and its default value is the current value of the connection. If the connection does not have a current value, the default is **5**.

Y-Cable protection triggered by Signal Degrade (SD)

The NFM-T supports **Signal Fail (SF)** and **Signal Degrade (SD)** as Y-Cable switching conditions.

The NFM-T supports the SD protection mechanism for the following OTs:

- 130SCX10 supported by 1830 PSS-32, 1830 PSS-16, 1830 PSS-16II, 1830 PSS-8 shelves (up to 10 protection groups can be supported per card)
- 130SNX10 supported by 1830 PSS-32, 1830 PSS-16II, 1830 PSS-8 shelves (up to 10 protection groups can be supported per card)
- 260SCX2 supported by 1830 PSS-32, 1830 PSS-16II, 1830 PSS-8 (for 100GbE client only, that is, no support for OTU4 client)
- 11DPM12 supported by 1830 PSS-32, 1830 PSS-16, 1830 PSS-16II, 1830 PSS-8, 1830 PSS-4 (up to six separate protection groups are supported on one pair of 11DPM12 cards)
- 43SCX4E

With SD protection, the system detects a signal degrade on the **Rx line side** or the **Rx client side**, and performs a Y-Cable switch upon detection according to the following priority:

- *Rx line side*: **HO-ODU4**: high priority; **LO-ODU2**: low priority
- *Rx client side*: **10GbE client**: high priority; *Other clients*: low priority.

SD switching works with both *revertive* and *non-revertive* Y-Cable switching, assuming both options are supported by the card.

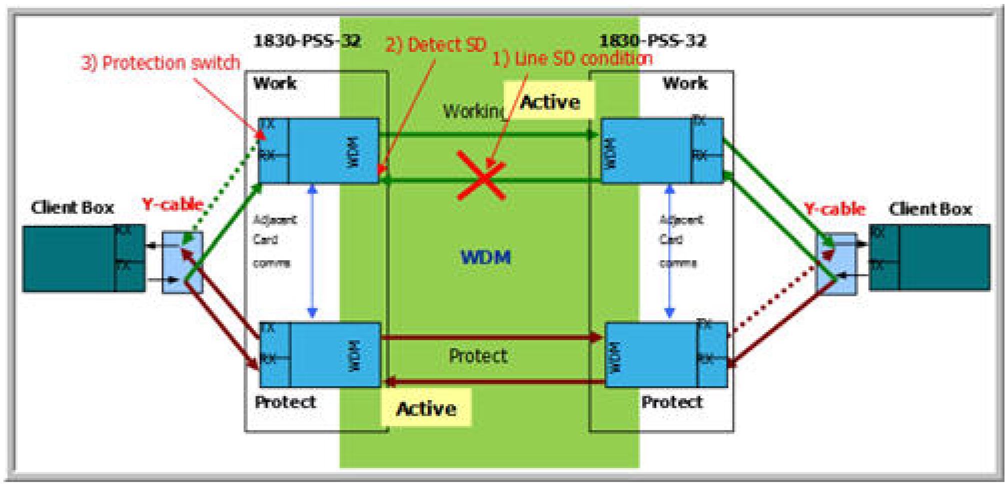
By default, Signal Degrade (SD) Y-Cable protection switching is *disabled*. The user can *enable* the protection switching function, at the DSR client service provisioning stage.

Signal Degrade (SD) feature is supported for both *Managed Plane* and *Layer 0 Control Plane*.

The following examples show the operation of the Y-Cable protection in case the fault is detected on line or client side.

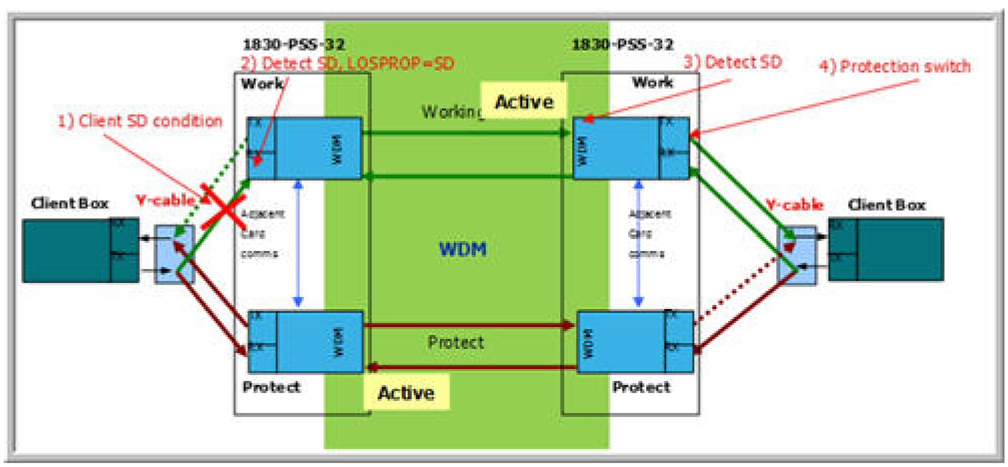
In the first case, the Y-Cable switching is triggered when a Signal Degrade (SD) is detected on the Rx line side (HO-ODU4 dDEG)

Figure 4-14 Signal Degrade (SD) scenario for Y-Cable protection : Line side



In the latter case, the Y-Cable switching is triggered when a signal degrade (SD) is detected on the Rx client side (10GbE).

Figure 4-15 Signal Degrade (SD) scenario for Y-Cable protection : Client side



4.5 OPSB and OPSB5 protection

OPSB protection definition

Optical Protection Switch Board (OPSB) is a type of protection that is provided by an OPSB, which is an 1830 PSS NE card that supports client-side OPS protection. The OPSB card uses a non-latching switch, which means that upon power failure, the OPSB automatically switches back to the default path of the connection. It provides 1+1 protection with shelf diversity.

Best Practice templates for OPSB protection

From the NFM-T GUI, navigate to **DEPLOY > New Service/Infrastructure Connection** and select one of the following template from the **Service/Infrastructure Templates** deploy window to provision an OPSB Protected service connection:

- **OPSB Protected OC-N**
- **OPSB Protected STM-N**
- **OPSB Ethernet**

Supported cards for OPSB protection and restrictions

Users can specify the from/to working and protection ports. The OTU cards that support OPSB protection are the following:

- 11QPA4
- 11STAR1
- 11STAR1A
- 11STMM10

The from/to working and protection ports must all be on compatible cards. The following cards are compatible and are supported:

- 11QPA4 with 11QPA4, or with 11STAR1, or with 11STAR1A
- 11STAR1 with 11STAR1, or with 11STAR1A
- 11STAR1A with 11STAR1A
- 11STMM10 with 11STMM10

In general, the NE allows OPSB protection if the OPSB card, the OT working port, and OT protection port are all on different shelves, or if all are on the same shelf. NE also allows OPSB protection if two of the three cards are on the same shelf, but the third card is on a different shelf. However, since the OPSB is a non-latching switch, when power is removed, the default switch position is the B port regardless if the B port is designated as the working or protection port. To prevent a single shelf failure, the OT port connected to the B port must be a card that is in a different shelf from the OPSB card.

Therefore, when one OT is in the same shelf as the OPSB card and one OT is in a different shelf from the OPSB card, users should adhere to the following supported configurations:

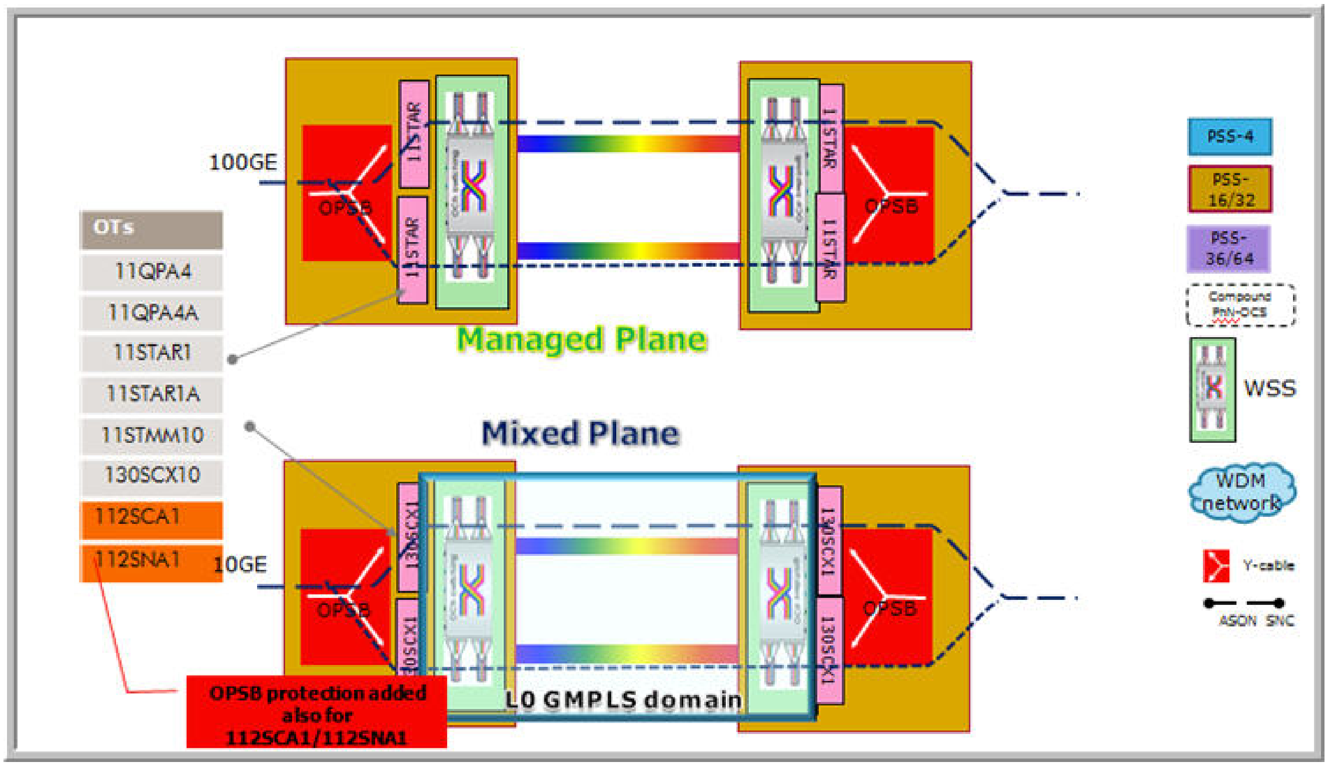
- The OPSB card and the OT working port on the same shelf and the OT protection port on a different shelf configuration is supported if the user specifies the OPSB A port as the working port.
- The OPSB card and the OT protection port on the same shelf and the OT working port on a different shelf configuration is supported if the user specifies the OPSB B port as the working port.

The following configurations are not supported:

- The OPSB card and OT protection port on same shelf and OT working port on different shelf configuration is not supported if the user specifies the OPSB A port as the working port.
- The OPSB card and OT working port on same shelf and OT protection port on different shelf configuration is not supported if the user specifies the OPSB B port as the working port.

The Figure 4-16, “ NFM-T OTN Provisioning – OPSB Client protection for a client signal” (p. 447) illustrates OPSB client protection for a client signal in the Managed Plane and Mixed Plane and the supported cards. Note that OPSB protection can be established between two different Nokia NEs; however, OPSB protection cannot be established between an OT on an 1830 PSS NE and an NE of another vendor. Also note that OPSB protection on a client NNI in a L0 Control Plane is supported on 260SCX2, D5X500, 130SCA1, 130SCX10, 130SNX10, 11QPA4, 112SCA1, and 112SNA1 cards.

Figure 4-16 NFM-T OTN Provisioning – OPSB Client protection for a client signal



OPSB protection provisioning guidelines for OT client ports

Users must consider the following regarding OT client ports and OPSB protection:

- The OT client ports that are connected to the OPSB A and B ports must have the same frequency.
- The frequency for the OT client ports that are connected to the OPSB A and B ports must be 1310 nm or 1500 nm.
- The OT client ports that are connected to the OPSB A and B ports must have the same pluggable module type.

OPSB protection provisioning guidelines for connection shapes

When users specify OPSB protection, the following **Connection Shape** guidelines apply to services:

- For **2 Ended Bi (I)** connections, both endpoints must be provisioned with OPSB protection.
- For **3 Ended A Bi (Y)** connections, OPSB protection cannot be provisioned on the **From Ports**.
- For **Add/Drop Z (bi)** connections, OPSB protection cannot be provisioned on the **To Ports**.

OPSB protection provisioning guidelines for transmission parameters

For OPSB protection, Transmission parameters are displayed based on the **From OT Working Port** and **From OT Protection Port**:

- For OPSB protected services with the **Connection Shape** of **2 Ended Bi (I)**, the Transmission parameters are set for the OT ports that are designated as the **From OT Working Port**, **From OT Protection Port**, **To OT Working Port** and **To OT Protection Port** of the connection.
- For OPSB protected services with **Connection Shape** of **3 Ended A Bi (Y)**, the Transmission Parameters are set for the OT ports that are designated as the **To OT Working Port** and **To OT Protection Port** of the connection.
- For OPSB protected services with **Connection Shape** of **3 Ended Z Bi (Y)**, the Transmission Parameters are set for the OT ports that are designated as the **From OT Working Port** and **From OT Protection Port** of the connection.

OPSB Protection for S13X100 card

The OPSB client protection is supported in conjunction with the S13X100 card.

The switching time is less than 50 ms. Layer 0 Control Plane is required.

This is applicable for 1830 PSS-32 NE with shelf types: 1830 PSS-32, 1830 PSS-8 and 1830 PSS-16**II**, and S13X100 card with variants S13X100R and S13X100E.

The following client signal types are supported:

- 100GbE
- 40GbE
- 10GbE
- OTU4
- OTU2
- OTU2E
- OC192
- STM64
- ODU2e
- ODU4
- ODUFlex

The possible configurations are:

- FOADM
- Legacy ROADMs, CWR ROADMs, Config. D, D’, D”
- CDC-F (MCS)
- CF (PCS1-6)
- iROADM

OPSB support for S13X100 can be performed with different scenarios depending on the referenced S13X100 cards hardware setup.

These cards can be arranged as:

- Two S13X100 cards in two separate shelves.
- Two S13X100 cards in two separate NEs.
- One S13X100 card on 1830 PSS and the other OT on a third-party NE.

Figure 4-17, “S13X100 Add/Drop with OPSB Client Protection” (p. 450), Figure 4-18, “S13X100 with OPSB Client Protection – 10GbE Client, MP” (p. 452), Figure 4-19, “S13X100 with OPSB Client Protection – 10GbE Client, L0 CP” (p. 452), Figure 4-20, “S13X100 Standalone Add/Drop HO-ODUk with OPSB Client Protection – 3R Regen” (p. 453), Figure 4-21, “S13X100 with OPSB Client Protection + 3R Regen – 10GbE Client, MP” (p. 453), and Figure 4-22, “S13X100 with OPSB Client Protection + 3R Regen – 10GbE Client, L0 CP” (p. 454) aims to illustrate these scenarios completed with notes on behaviors when applicable.

Two S13X100 cards in two separate shelves

Figure 4-17 S13X100 Add/Drop with OPSB Client Protection

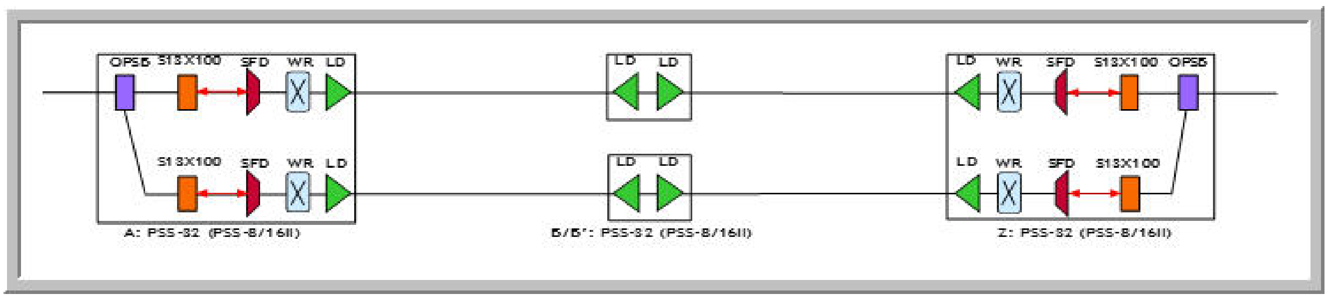


Figure 4-18 S13X100 with OPSB Client Protection – 10GbE Client, MP

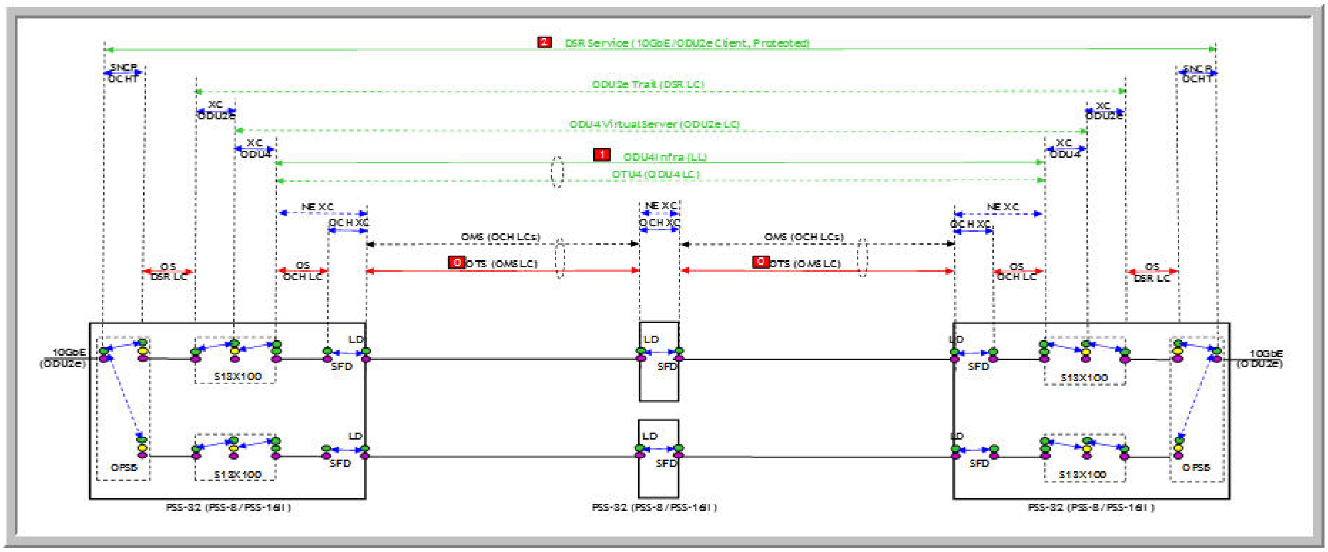


Figure 4-19 S13X100 with OPSB Client Protection – 10GbE Client, L0 CP

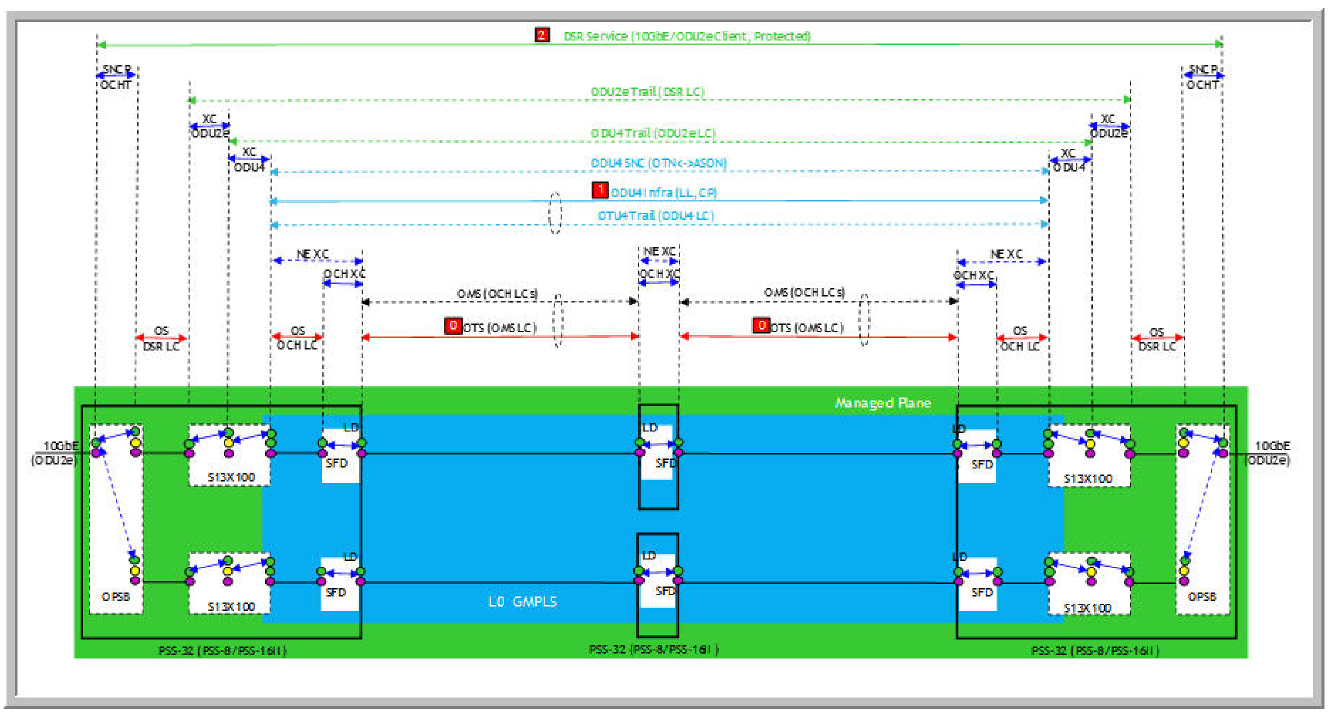


Figure 4-20 S13X100 Standalone Add/Drop HO-ODUk with OPSB Client Protection – 3R Regen

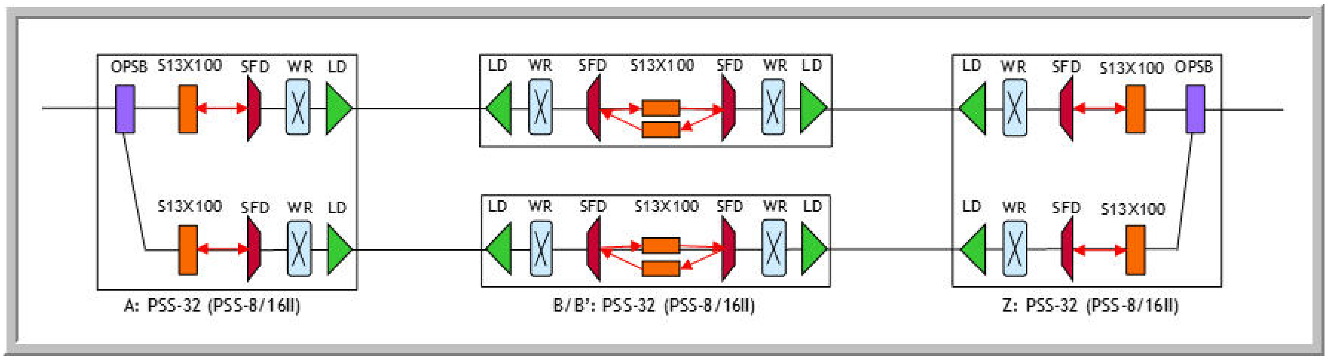


Figure 4-21 S13X100 with OPSB Client Protection + 3R Regen – 10GbE Client, MP

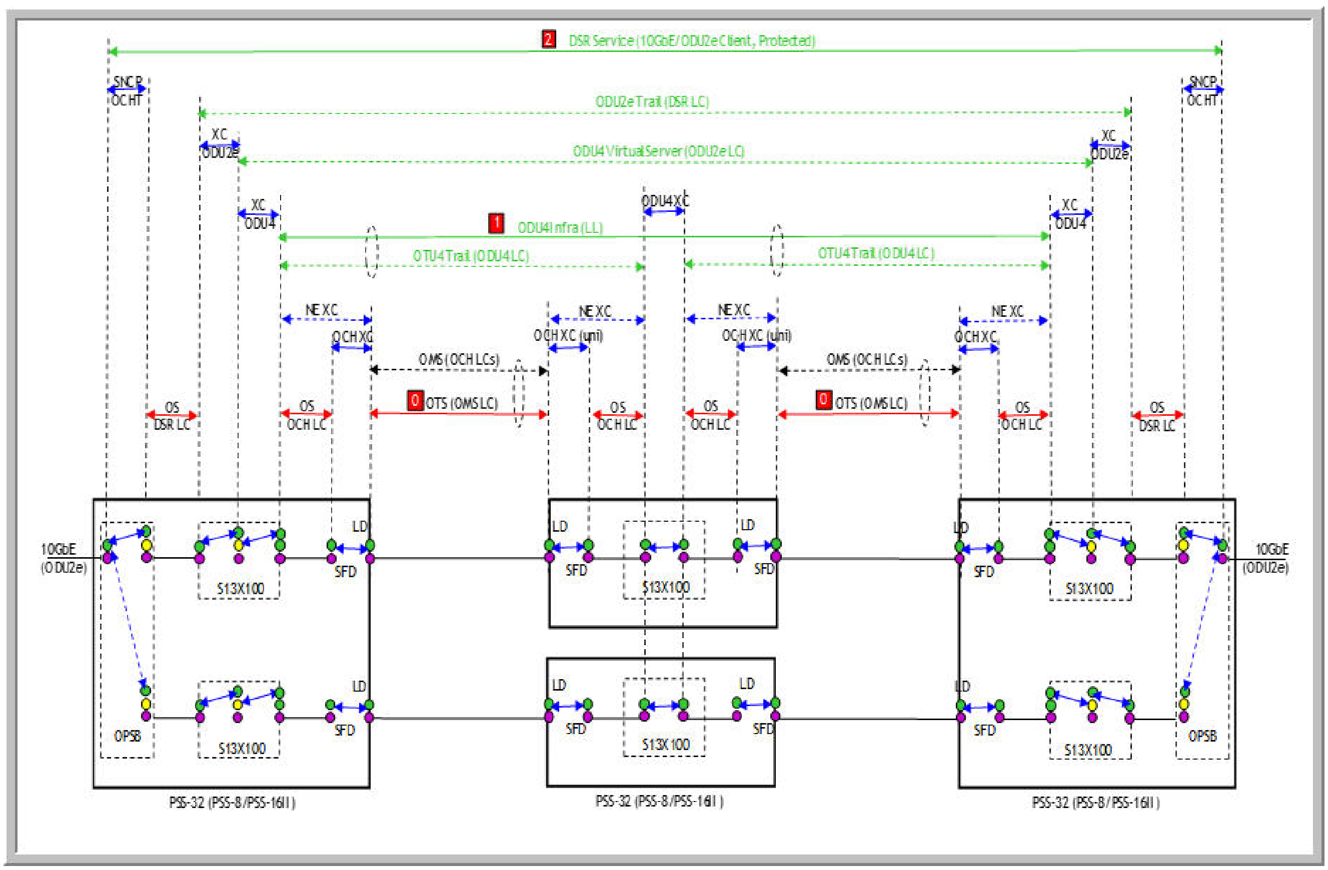


Figure 4-22 S13X100 with OPSB Client Protection + 3R Regen – 10GbE Client, L0 CP

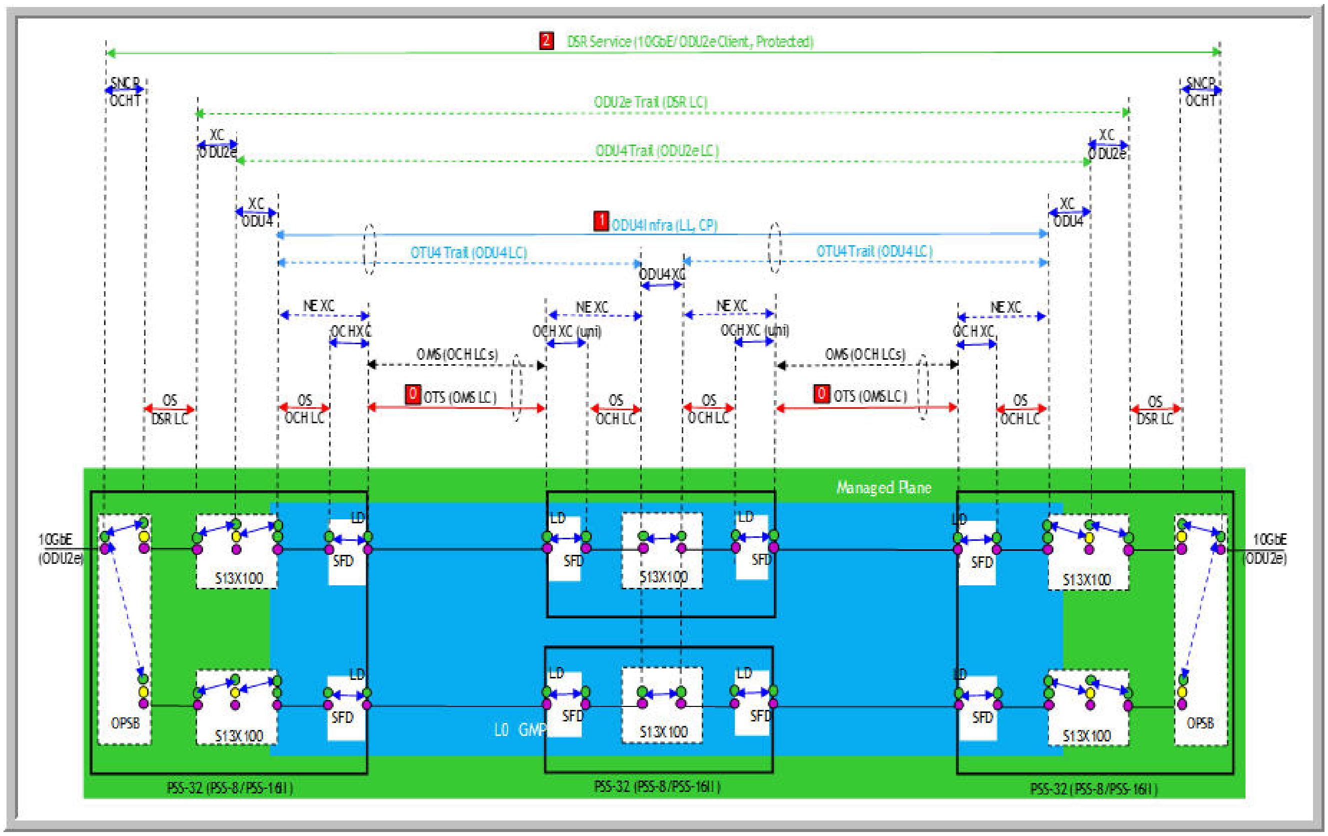


Figure 4-23 S13X100 Standalone Add/Drop HO-ODUk with OPSB Client Protection – 100GbE Client

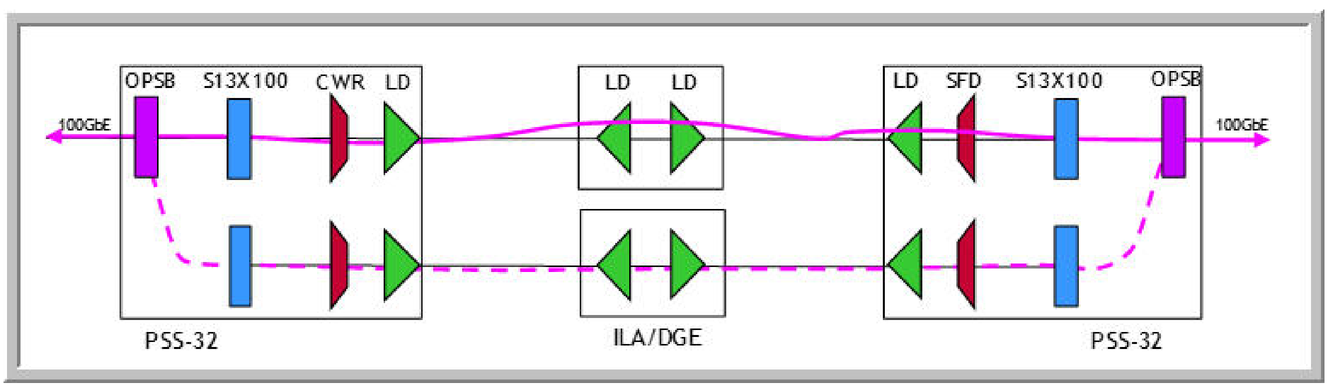
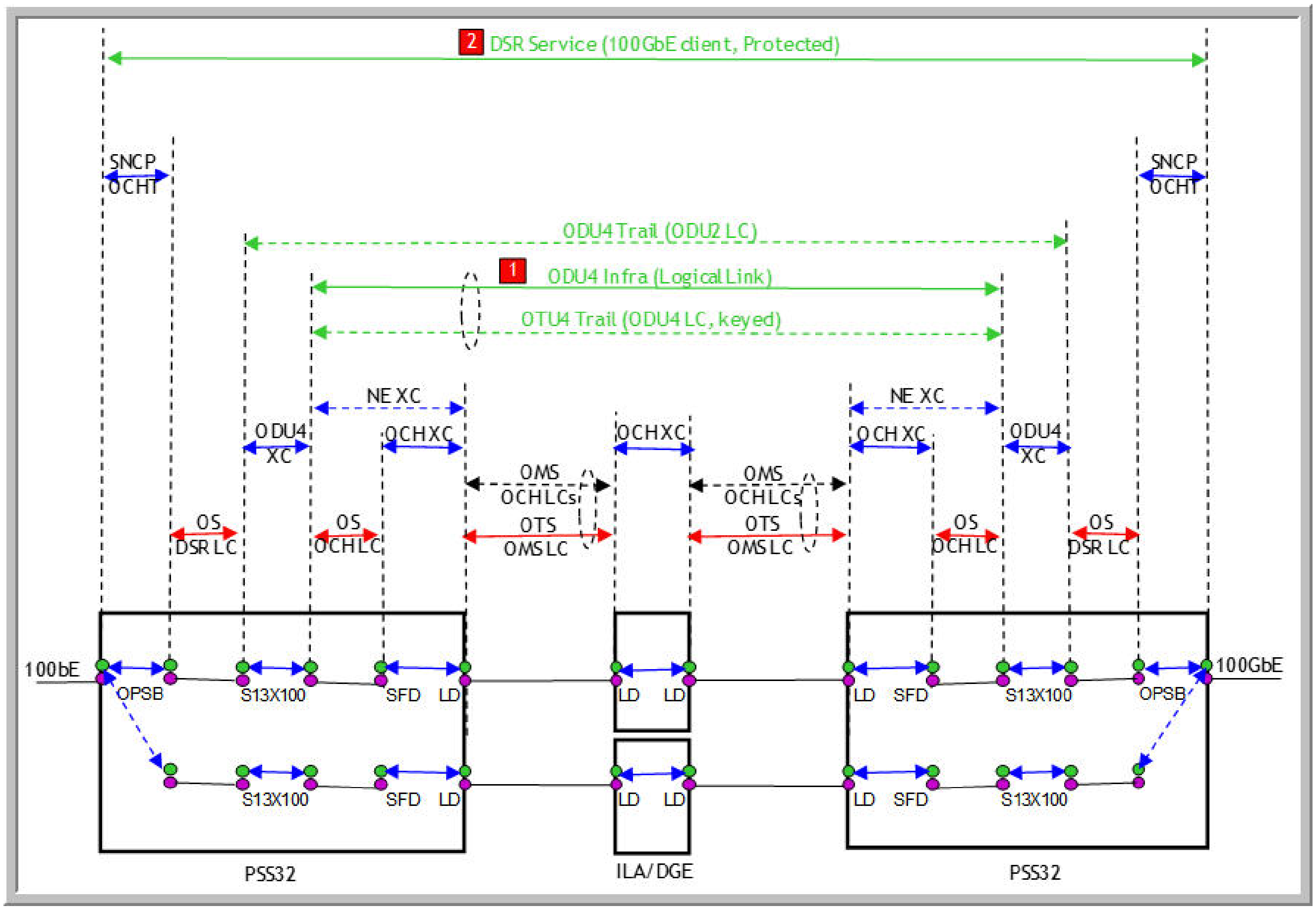


Figure 4-24 S13X100 with OPSB Client Protection – 100GbE Client, MP



Behavior:

- S13X100 is Standalone with BP ports unassigned on 1830 PSS-32, 1830 PSS-16II, and 1830 PSS-8 shelves.
- Operational Mode must be set to Add/Drop on both A and Z NE, and Regen on the middle two S13X100 cards.
- The OTU4 trail supports both fixed and flex grid.
- The OTU4 trail supports both encryption enabled and disabled for S13X100E.
- The OTU4 trail supports both Keyed and Unkeyed services.
- Client signal types with OPSB client protection:10GbE, OC192, OTU2, OTU2e, STM64; C21: 100GbE, OTU4; C31: 40GbE; C32: 40GbE, 100GbE, OTU4; Line: OTU4 (SDFEC-G2, AFEC; QPSK).

Two S13X100 cards located on two different 1830 PSS NEs

In this configurations, the two OTs are on different 1830 PSS PHN NEs and one of them is required to use External topological link.

This configuration can be implemented with and without ENE/VNE.

When OPSB is extended to ENE, the ports on ENE should also have the keyword "OPS" and "SIG" so that it will ensure that the OPSB panel /required CTPs will be generated.

Figure 4-25 Two S13X100 cards Located on two different 1830 PSS NEs

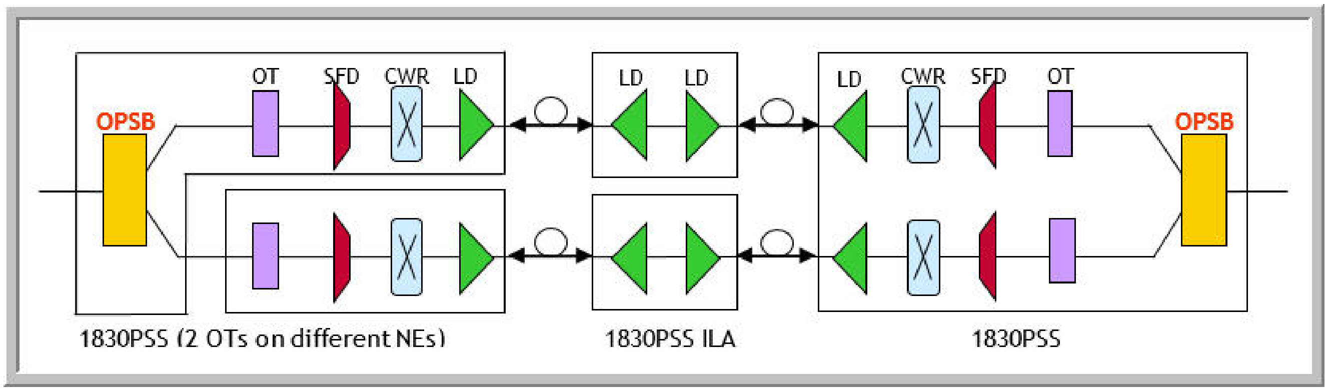


Figure 4-26 Optical Model for OPSB Client Protection – S13X100 cards on two 1830 PSS NEs

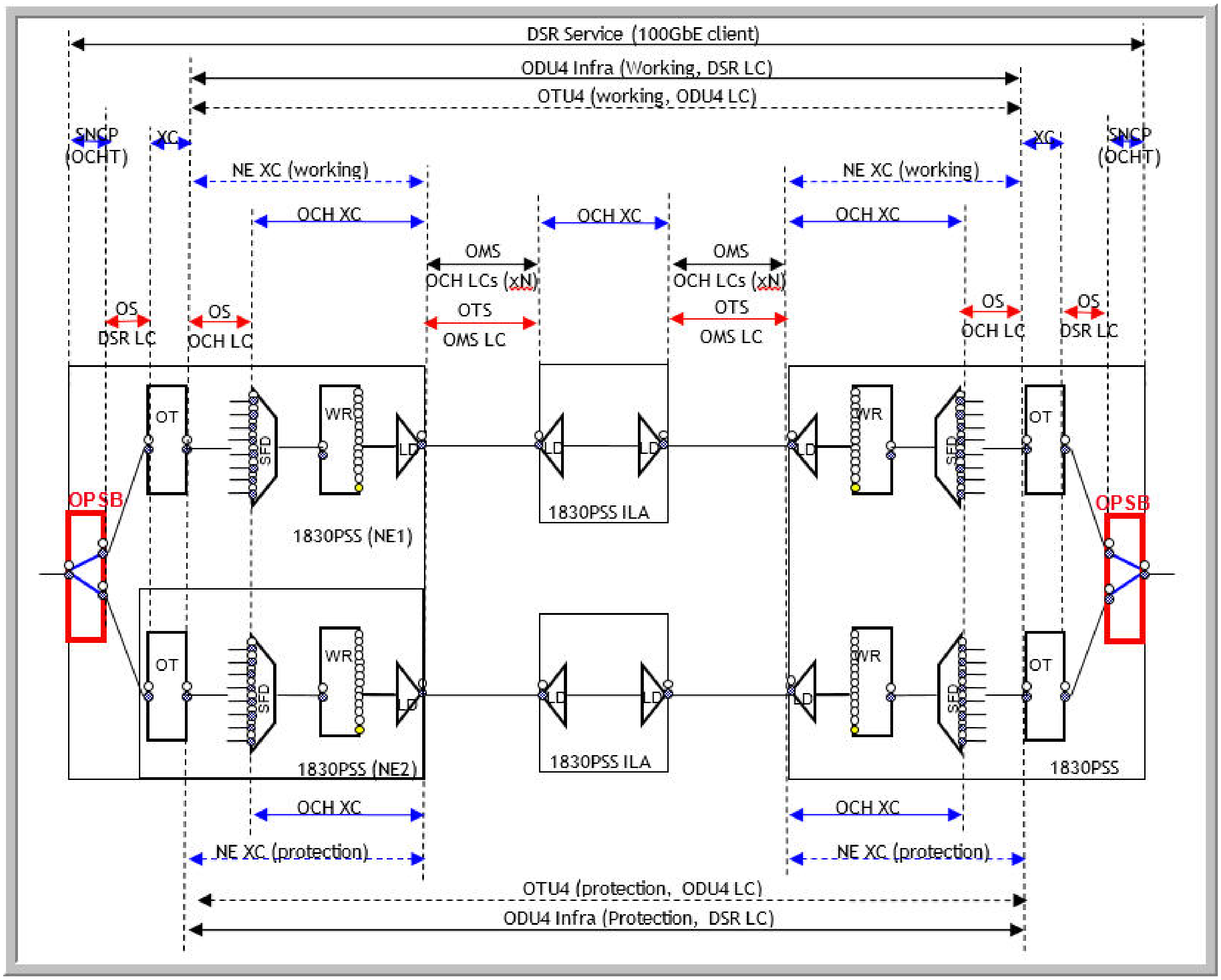
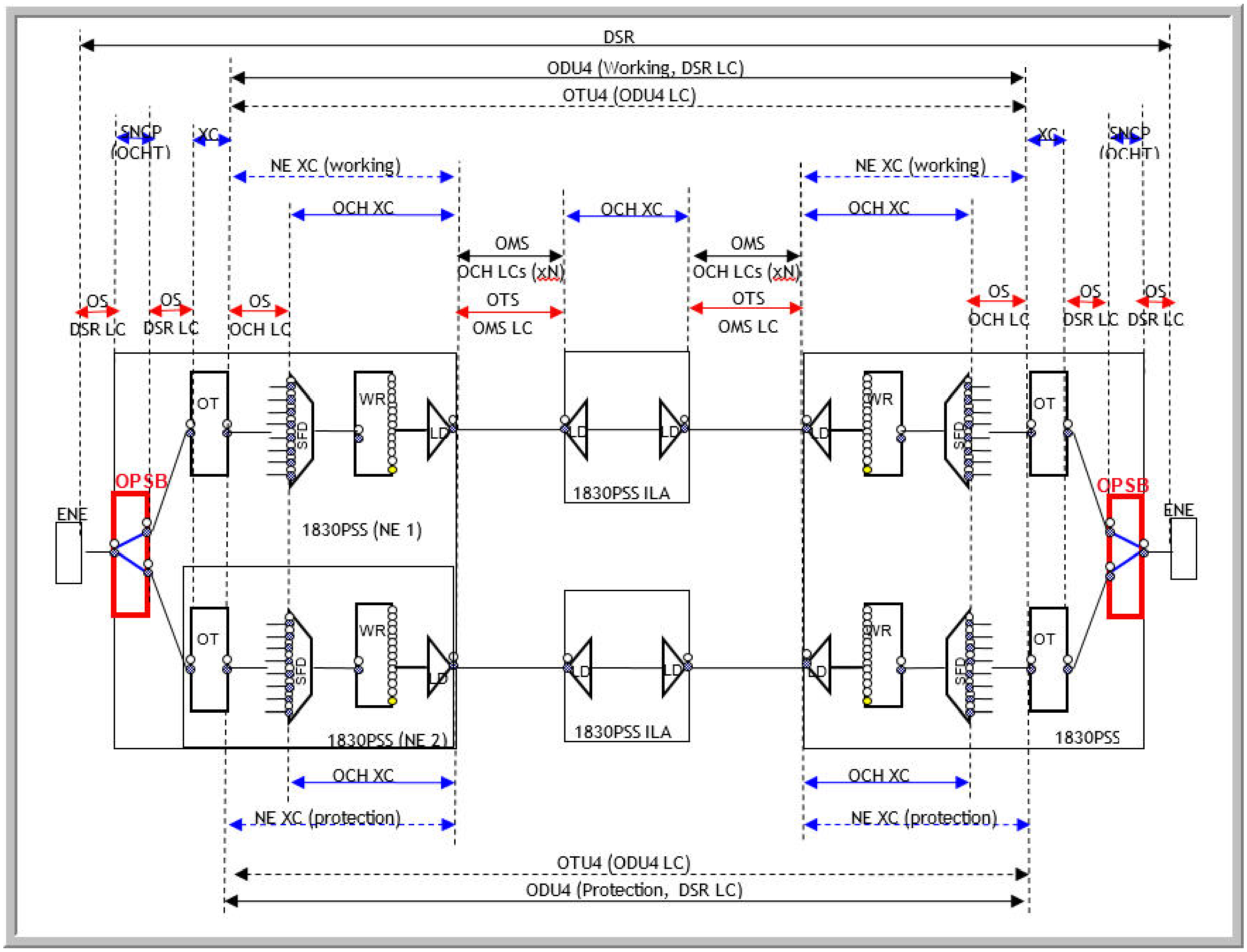


Figure 4-27 Optical Model for OPSB Client Protection – S13X100 cards on two 1830 PSS NEs



One S13X100 card on 1830 PSS and the other OT on third-party NE

This configuration provides one OT on 1830 PSS NE and the other on a third-party NE.

An ENE should be used, and an External topological link is used to connect to it.

The reliable port side should support both with and without ENE/VNE.

When OPSB is extended to ENE, the ports on ENE should also have the keyword "OPS" and "SIG" so that it will ensure that the OPSB panel /required CTPs will be generated.

Figure 4-28 One S13X100 card in 1830 PSS NE and the other card in a third-party NE

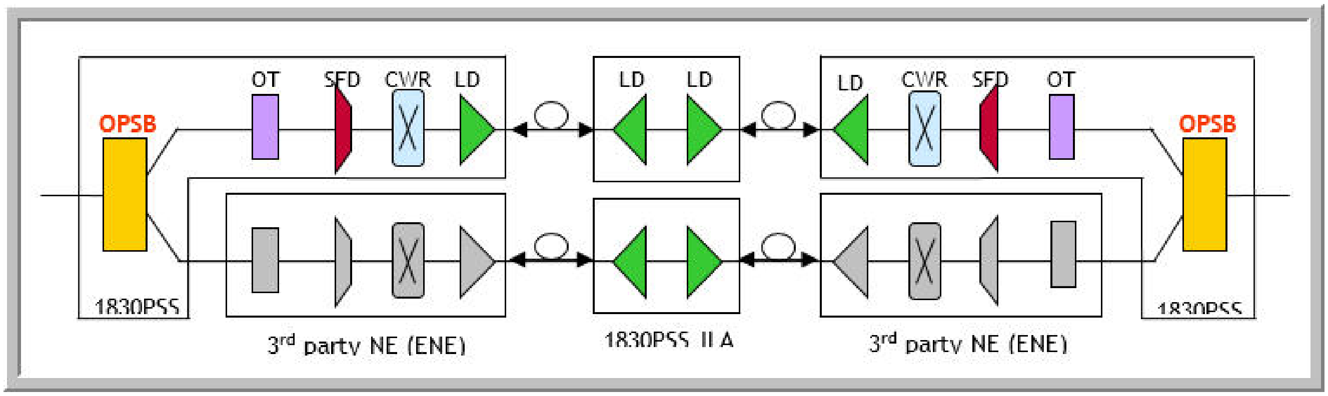
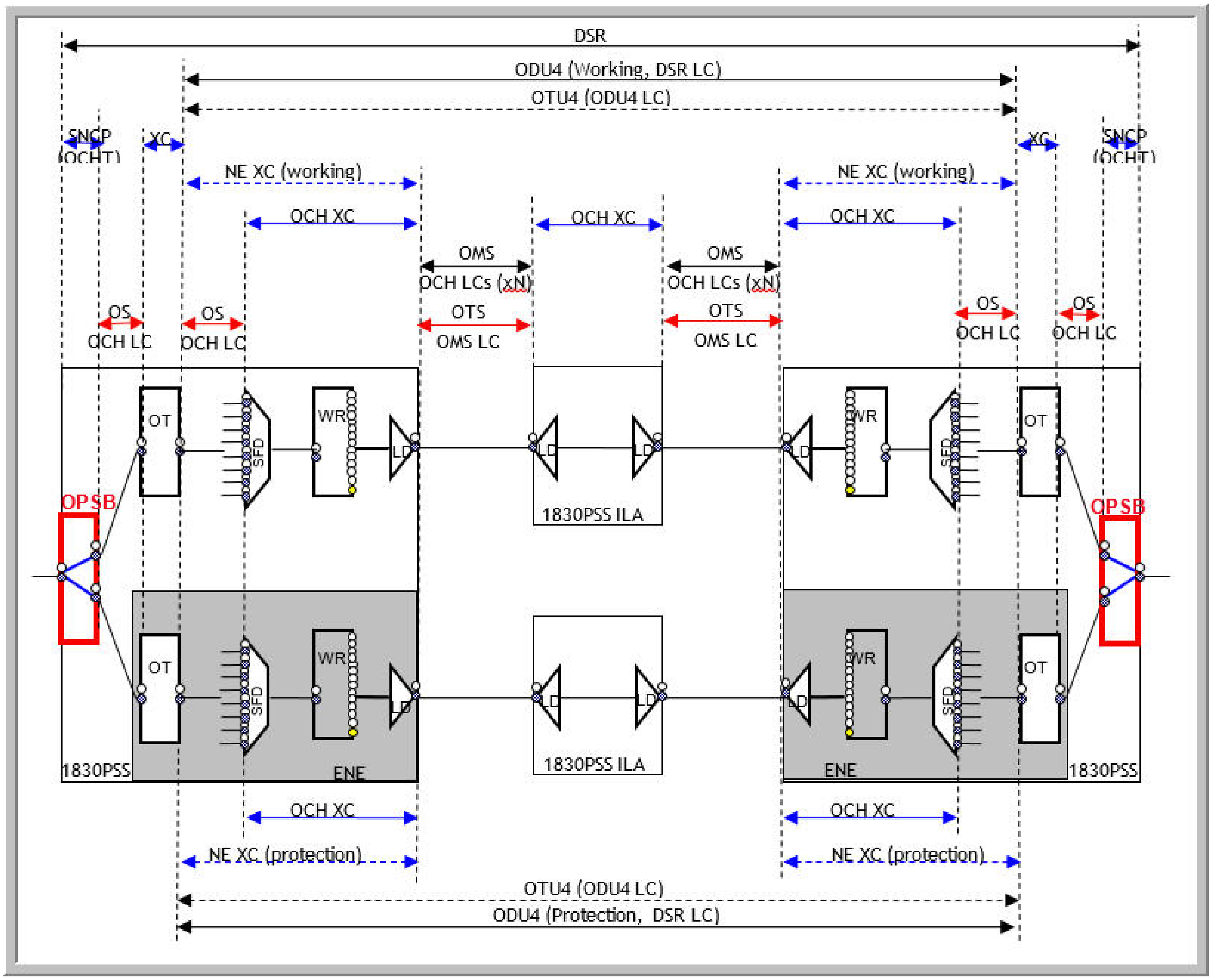


Figure 4-29 Optical Model for OPSB Client Protection – S13X100 cards on two 1830 PSS NEs



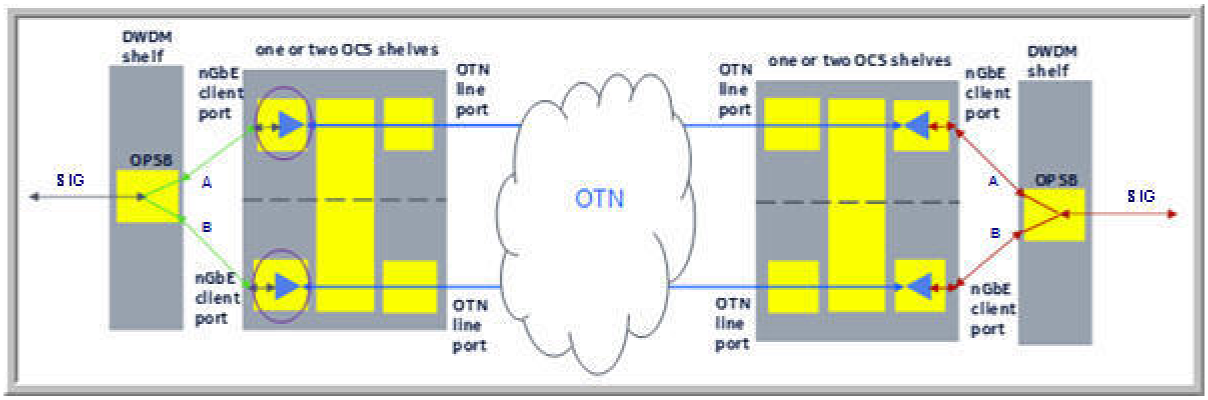
OPSB protection on 1830 PSS-OCS switching shelf

OPSB protection is supported on 1830 PSS-OCS for SONET, SDH, and Ethernet client ports.

OPSB protection on Ethernet client ports

1830 PSS WDM shelves support optical protection switch (OPS), refer to 4.5 "OPSB and OPSB5 protection" (p. 447). In an 1830 PSS cluster consisting of WDM shelves and OCS shelves, OPSB protection on OCS ETH client ports is supported. In this protection scheme, the OPSB card is located in a WDM shelf. For example, in a 1830 PSS-32 shelf; that is co-located with the OCS shelf or shelves, as showed in the Figure 4-30, "OPSB configuration" (p. 461).

Figure 4-30 OPSB configuration



Bridge and selector of the OPSB protection scheme are implemented by an OPSB card at both ends of the protected domain. In one direction, the OPSB card includes an optical switch to select the output signal of the SIG port between the two input signals of ports A and B. For the other direction an optical splitter bridges the input signal of the SIG port to the two output signals of ports A and B.

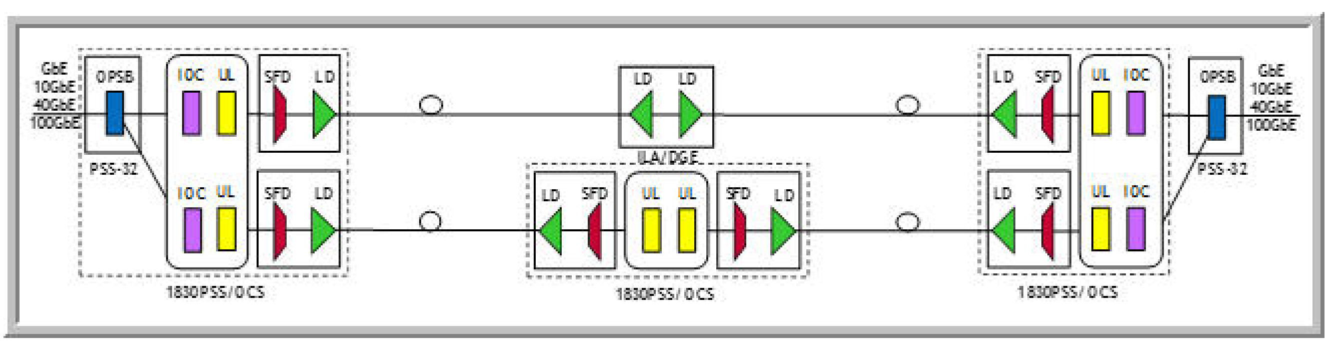
The OPSB card of 1830 PSS-32 NE provides protection for nGbE (1GbE, 10GbE, 40GbE and 100GbE) ports of the OCS shelves (1830 PSS-36/1830 PSS-64).

Protection is supplied for the following client signal type and cards:

- 1GbE of 24ANMB
- 10GbE of 10AN10G/10AN10GC/10ET10GC (ODU2/ODU2e containers)
- 40GbE of 2AN40G
- 100GbE of 1AN100G

Note that the OPSB can be on either a cluster with the 1830 PSS-OCS and 1830 PSS-32, as showed in the left side of the picture below or a separate 1830 PSS-32 NE, as showed in the right side of the picture.

Figure 4-31 Example of OPSB Client Protection with OCS I/O cards – 10GbE/40GbE/100GbE Client



OPSB protection switch behavior

Autonomous protection switching of the OPSB card is based on the detection of an optical signal at its two input ports A and B. If not blocked by an external switch command of higher priority, the optical switch of the OPSB card will switch away from an input port for which a LOS is detected.

The OPSB protection switching is triggered by the following factors, highlighted in the Figure 4-30, “OPSB configuration” (p. 461):

1. ODUk trail, due to an SSF contribution, marked with a blue line in the Figure 4-30, “OPSB configuration” (p. 461).
2. Head end fibers and upstream LAN due to CSF, marked with a red line in the Figure 4-30, “OPSB configuration” (p. 461). Fiber failures are included between far end OPSB card and OCS I/O client port.
3. Back end fibers. These are implicitly protected, since LOS is detected by the OPSB card, marked with the green line in the Figure 4-30, “OPSB configuration” (p. 461).
4. Equipment failures due to a local client card or port, marked with a purple circle in the Figure 4-30, “OPSB configuration” (p. 461).

OPSB protection provisioning

User must provision external topological links between the A and B ports of the OPSB on 1830 PSS-32 NE and the I/O cards on the 1830 PSS-OCS NE. The nGbE ports must be configured on the 1830 PSS-OCS NE before the external links are provisioned. For an OPSB protected end-to-end client service connection, four external topological links between OPSB and WDM/Mux_DeMUX, must be provisioned. The provisioning of the external topological links between OPSB and OCS I/Os is made through the NPR/EQPT.

The following rules apply when provisioning the external topological links:

1. On either A-end or Z-end, select the two I/O cards of the 1830 PSS-OCS NE from two different shelves.
2. When point 1 is not applicable, on either A-end or Z-end, select the two I/O cards of the 1830 PSS-OCS NE from the same shelf.
3. When point 2 is not applicable, on either A-end or Z-end, select two ports of the same rate from the same I/O card of the 1830 PSS-OCS NE.

Basically, the maximum hardware redundancy must be considered by the user.

OPSB protection on SDH and SONET client ports

OPSB protection also applies to SDH and SONET client ports, with the same behavior as the Ethernet ports described in “OPSB protection on 1830 PSS-OCS switching shelf” (p. 460)

The following client signals and cards are supported:

- STM-64/OC-192 on 10AN10GC
- STM-1/OC-3, STM-4/OC-12 and STM-16/OC-48 on 24ANMB

The OPSB protection group resides in one 1830 PSS-OCS shelf, but there are no specific port pairing restrictions within the 1830 PSS-36 and the 1830 PSS-64 shelf; the client signal type must be the same on the two I/O cards.

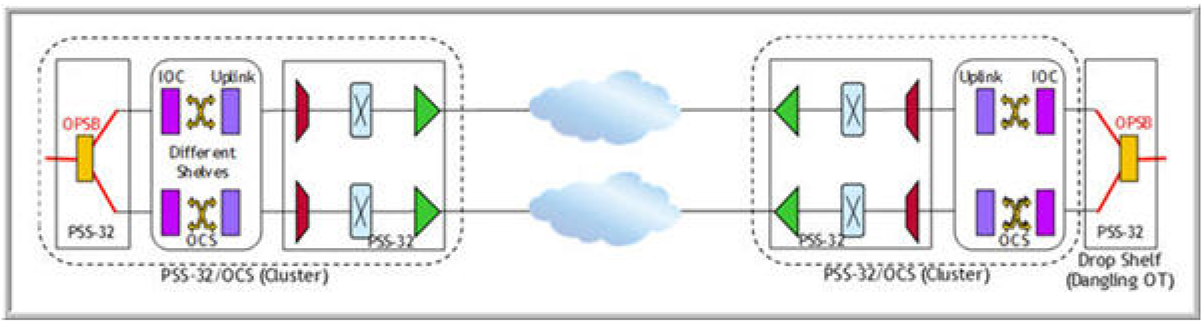
The protection switching for SDH and SONET client ports is triggered by CSF, such as the equipment failures on the local client side.

OPSB supported network scenarios with 1830 PSS-OCS

The following scenarios show the possible OPSB protection configurations with 1830 PSS-OCS/ 1830 PSS-32 NE, depending on where the I/O cards are located.

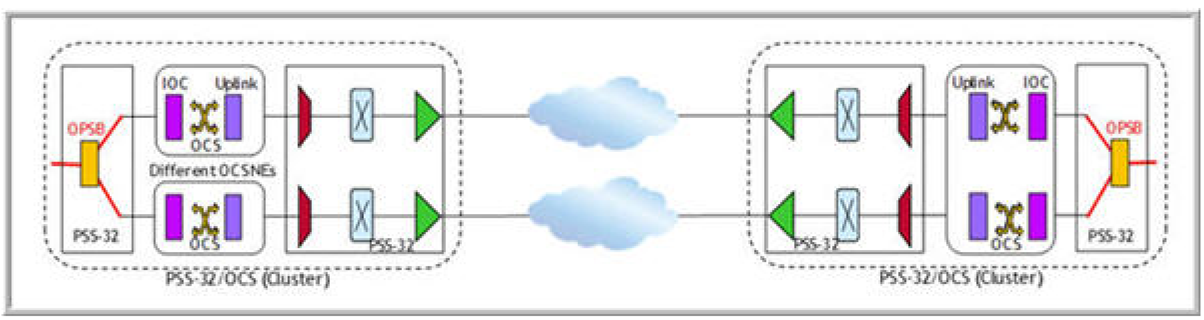
In this scenario, both I/O cards are in the same 1830 PSS-OCS NE. Note if possible, I/O cards must be on different shelves.

Figure 4-32 I/O cards in the same 1830 PSS-OCS NEs



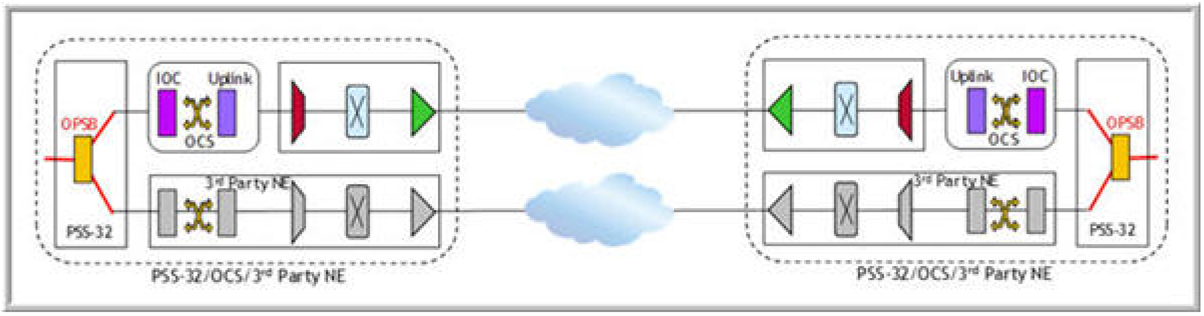
In this second scenario both I/O cards are in two different 1830 PSS-OCS NEs.

Figure 4-33 I/O cards in two different 1830 PSS-OCS NEs



In the last scenario one I/O card is located in a 1830 PSS-OCS NE and the other I/O or OT card in a third-party NE.

Figure 4-34 I/O card in a 1830 PSS-OCS NE and I/O or OT card in a 3rd party NE

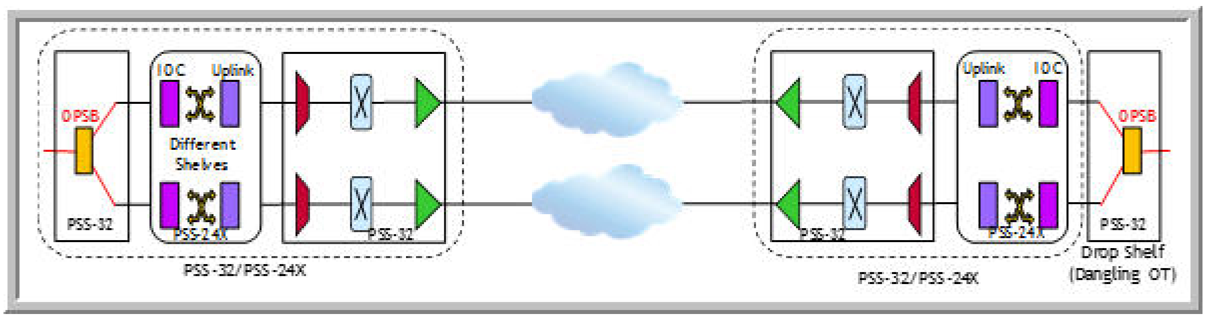


OPSB protection supported network scenarios with 1830 PSS-24x

The scenarios shown in the previous section are feasible by installing the I/O card on the 1830 PSS-24x shelf. The following diagrams show the same configuration with 1830 PSS-OCS shelves, using the 1830 PSS-24x shelf.

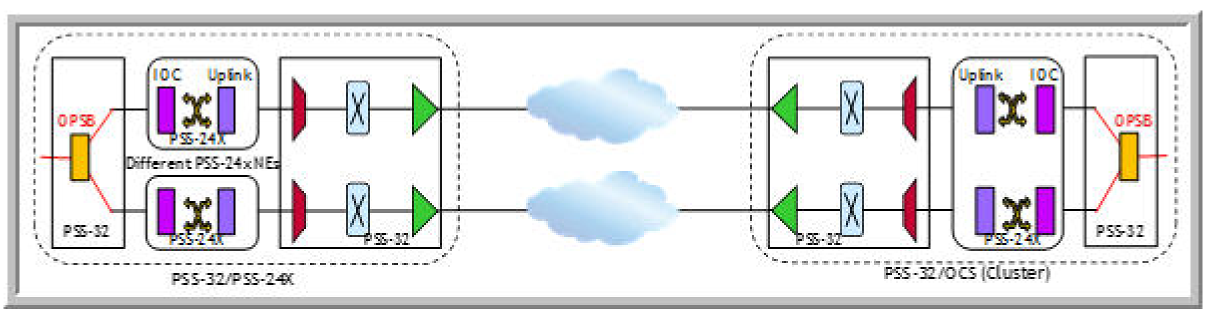
In this scenario, both I/O cards are in the same 1830 PSS-OCS NE.

Figure 4-35 Network scenarios with 1830 PSS-24x - Example 1



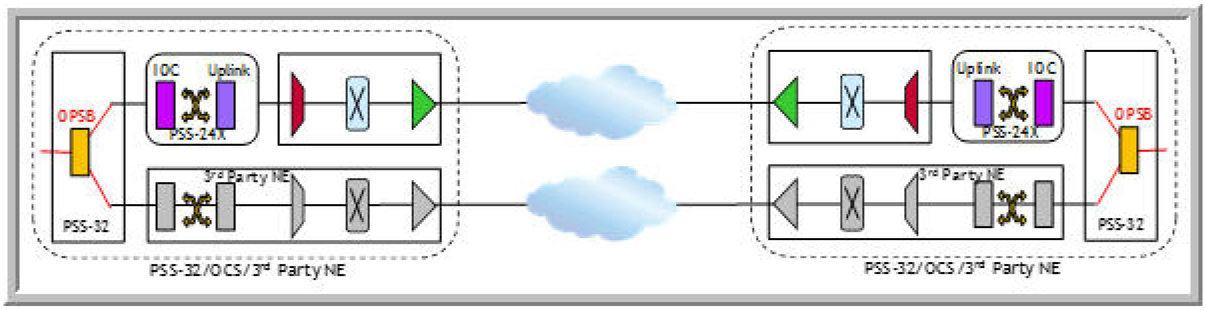
In this second scenario both I/O cards are in two different 1830 PSS-24x NEs.

Figure 4-36 Network scenarios with 1830 PSS-24x - Example 2



In the last scenario one I/O card is located in a 1830 PSS-24x NE and the other I/O or OT card in a third-party NE.

Figure 4-37 Network scenarios with 1830 PSS-24x - Example 3



Multi-port OPSB card (OPSB5) definition

The OPSB5 card is a multi-ports OPSB client protection card. The OPSB5 card supplies five sets of OPSB client protection. The OPSB5 is a full height and one-slot wide card with five pair of client ports or 10 client ports (it is 20 client fiber LC connectors, because each client port has two RX and TX LC connectors). Each pair has two client ports - one for working and the other for protection.

Switching a particular service has no impact on other services defined on the same card. All functions available on OPSB card are available on multi-port OPSB (OPSB5) card as well.

OPSB5 card supports the OTs interworking with the following cards with 1830 PSS-8, 1830 PSS-16II, 1830 PSS-32 shelves, and 1830 PSS-32 R11.0 NE:

- D5X500, D5X500L, D5X500Q
- S13X100E, S13X100R
- 20P200 in mate configuration with D5X500/D5X500Q.

Only a client signal with 10G and 100G rate is supported.

The following features are supported:

- Protected DSR creations on both A-end and Z-end
- Protected DSR creation on OPSB5 A-end and OPSB on Z-end.

Switching Block

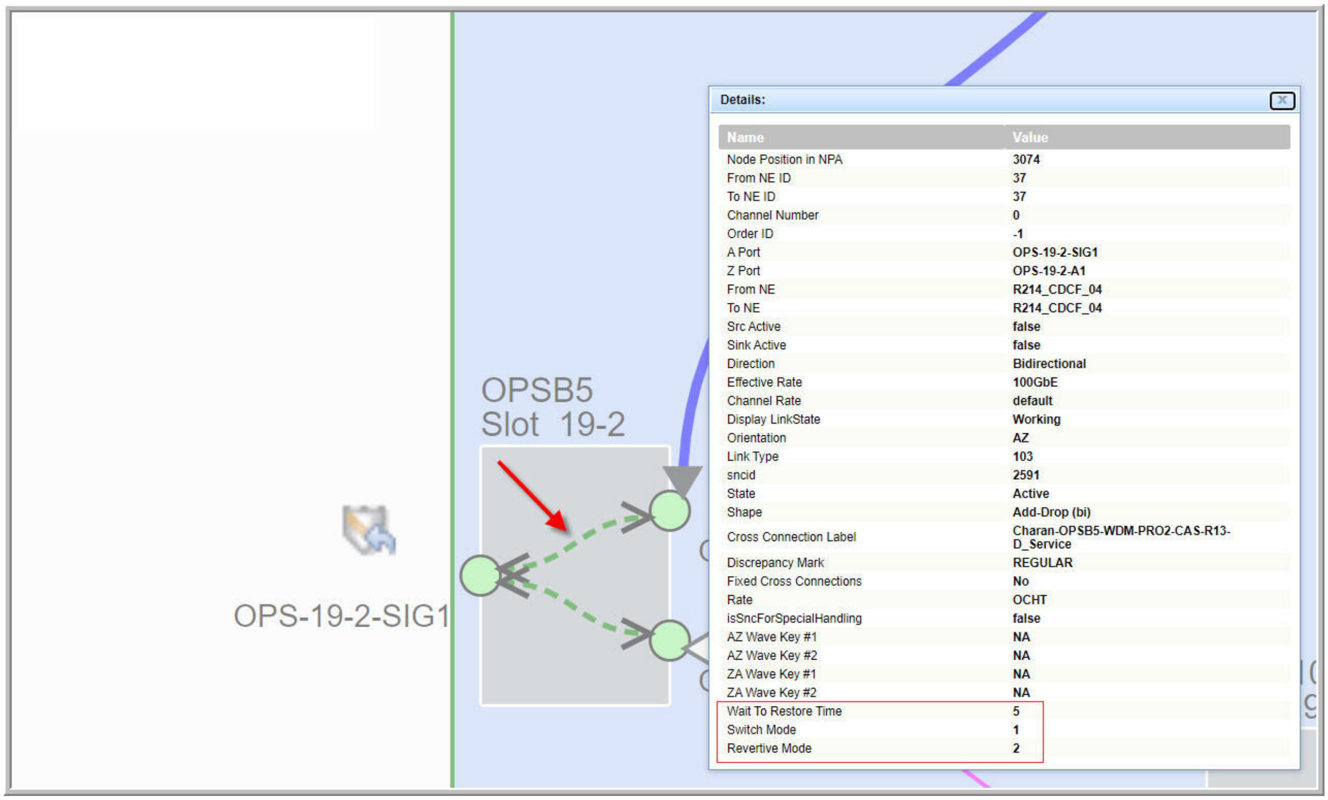
OPSB and OPSB5 protection supports revertive switching mode. This behavior applies to the shelves: 1830 PSS-8, 1830 PSS-16II, 1830 PSS- 32, and 1830 PSS-24x starting from 1830 PSS NE release 11.1 onwards.

The **Revertive Mode** and the **Wait To Restore Time** value, are set using NFM-T GUI template during a service creation, see “OPSB Port” (p. 705) in the **Modify Connection**.

Both the values are displayed by selecting the **Properties** in the **Routing Display** window or by selecting the **360 ⁰ View > PROTECTION** tab of a connection.

The following figure is an example of the details supplied with the Routing Display Properties. To view the OPSB details click the dotted line or on the Protection Group icon.

Figure 4-38 Routing Display - Properties - OPSB Switching mode details



OPSB protection provisioning guidelines for client ports involving PHN OT card

The signal rate must be assigned before to create a connection, if the OPS creation involves client ports of any PHN OT card that support *containerType*.

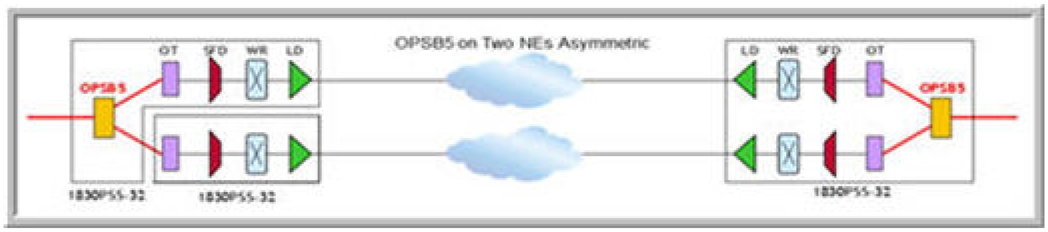
OPSB/OPSB5 protection applies to all the UNI and NNI rates.

Note: OPSB for NNI rates in managed plane and L1 control plane are not supported for OCS and 1830 PSS-8x, 1830 PSS-12x, and 1830 PSS-24x cards due to NE limitations. OPSB/OPSB5 is not applicable for L0 Control Plane.

Note: For OPSB NNI service to be successful with OT cards involving fixed cross connections (for example, 130SCX10, 130SNX10), the user must DB delete the auto-generated ODUk or ODUj that is generated due to fixed cross connections ending at the client port.

This allows a proper creation of the FTP ports during the OPS connection creation. This case is mainly for configuration shown in the Figure 4-39, “OPSB OPS connection creation” (p. 466).

Figure 4-39 OPSB OPS connection creation



NFM-T supports line side signal degrade (SD) and signal failure (SF) triggered OPSB or OPSB5 on S13X100E, S13X100R and D5X500Q cards with different client rates.

NFM-T supports the following type of protection on the D5X500Q card on the following client signal types:

- 100GBE

The following client signal types are supported on S13X100E and S13X100R for use with client side OPS protection and for contribution of Signal Degrade as a switching criteria:

- 10GBE
- 100GBE
- STM64/OC192

For more information, see “OPSB or OPSB5 Protection Triggered by Signal Degrade” (p. 714).

OPSB or OPSB5 protection for 1830 PSS-8x and 1830 PSS-12x shelves

NFM-T supports OPSB or OPSB5 client protection for the 1830 PSS-8 and 1830 PSS-12 Input/ Output (I/O) cards, that is, 4MX200, 20AX200, and 20MX80 with sub-10G, 10G, and 100G rates.

OTN clients are supported from 1830 PSS NE release 13.1 onwards.

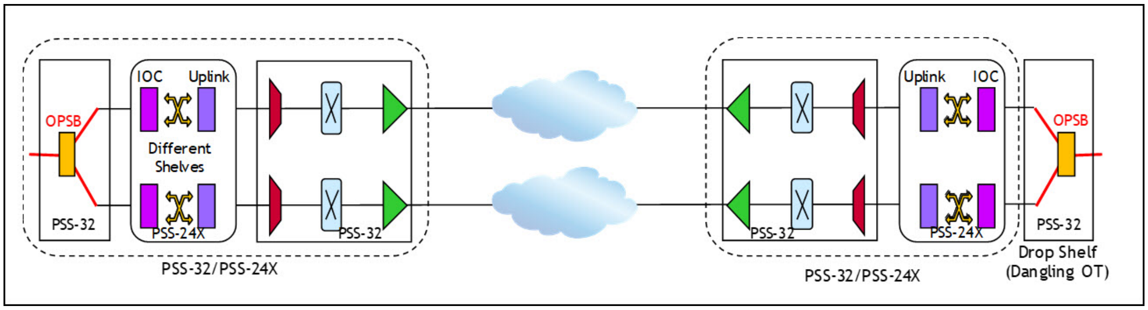
OPSB and OPSB5 support the following Input/Output cards with associated client rates:

Table 4-3 Supported Client Signal Rates for 1830 PSS-8X and 1830 PSS-12X

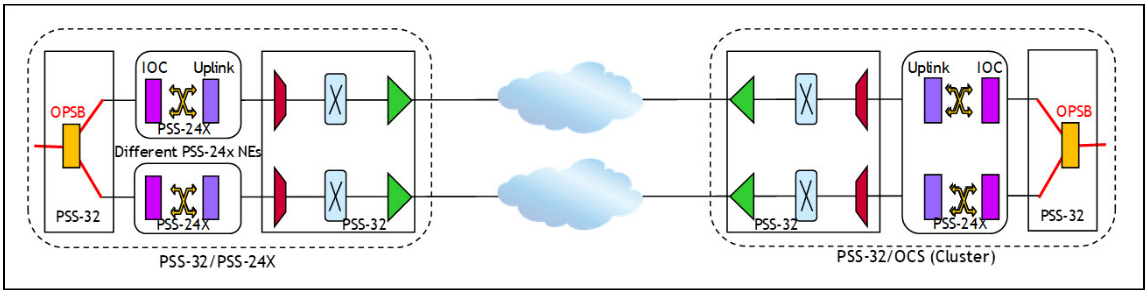
Card name	Client signal rate
4MX200	100GbE, OTU4
20AX200	10GbE, STM64, OC192, OTU2, OTU2e
20MX80	OC3, OC12, OC48, OC192, STM1, STM4, STM16, STM64, GbE, 1GbEconv, 10GbE (ODU2, ODU2e), OTU2, OTU2e

NFM-T supports OPSB and OPSB5 protections with two 1830 PSS-nX/PSS-32 for the following configurations:

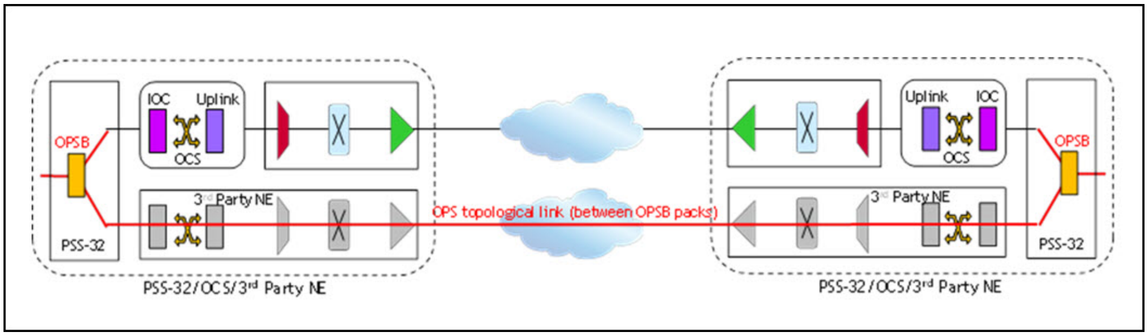
- The Input/Output Circuit (IOC) cards are on the same 1830 PSS-nX shelves. The positioning of the IOC cards can be on different shelves.



- The IOC cards are on two 1830 PSS-nX NEs (1830 PSS-32 NEs)



- One IOC card on the 1830 PSS-nX shelf/NE and the other IOC card on a symmetric 3rd party NE



OPSB or OPSB5 protection cards support the following:

- Protection parameters for a protected client service connection using OPSB5
- L1 Control Plane connections

- Non-OTN clients (for example, Ethernet clients, SDH clients) and OTN clients (for example, OTU4, OTU2/e)
- Unidirectional switching within 50 ms

Note:
- All NEs should be of the same release. From the NFM-T release 21.8 onwards, OPSB or OPSB5 is not supported for mixed release.
- To discover the service for OPSB NNI ENE scenario, perform DB delete and recreate the OPS from OPSB A/B port to OPSB B/B port.

OPSB or OPSB5 protection for 1830 PSS-24x shelves

NFM-T supports OPSB or OPSB5 client protection for the 1830 PSS-24x I/O cards, that is, 10AN400, 20AN80, 30AN300, 20UC200, 10AN1T, and 4AN400. NFM-T supports sub-10G rates (for example, 1 GbE) for OPSB5 card in connections that are created with 20AN80 cards on both the A-End and Z-End.

OPSB and OPSB5 support the following Input/Output cards with associated client rates:

Table 4-4 Supported Client Signal Rate for 1830 PSS-24X

Card name	Client signal rate
20UC200	10GbE, STM64/OC192, OTU2, OTU2e
4AN400	100GbE, OTU4
10AN400	100GbE, OTU4
30AN300	10GbE, STM64/OC192, OTU2, OTU2e
20AN80	OC3, OC12, OC48, OC192, STM1, STM4, STM16, STM64, GbE, 1GbEconv, 10GbE (ODU2, ODU2e), OTU2, OTU2e
10AN1T	100GbE, 400GbE, OTU4

OPSB or OPSB5 protection cards support the following:

- Protection parameters for a protected client service connection using OPSB5
- L1 Control plane connections
- Non-OTN clients (for example, Ethernet clients, SDH and SONET clients)
- Unidirectional switching within 50 ms

Note: All NEs should be of the same release. From the NFM-T release 21.8 onwards, OPSB or OPSB5 is not supported for mixed release.

NFM-T supports OPSB and OPSB5 protections triggered by **Signal Degrade** on 1830 PSS-24x for the following cards : 20AN80, 30AN300, 10AN400, 4AN400, 20UC200, 10AN1T and signal rate: 1GbE, 10GbE, 100GbE. For more information, see "OPSB or OPSB5 Protection Triggered by Signal Degrade" (p. 714).

Selection of OPSB protected service connections for protection switching

Perform the following steps to select OPSB protected service connections and perform the protection switching operation.

1. From the NFM-T GUI, navigate to one of the following paths:

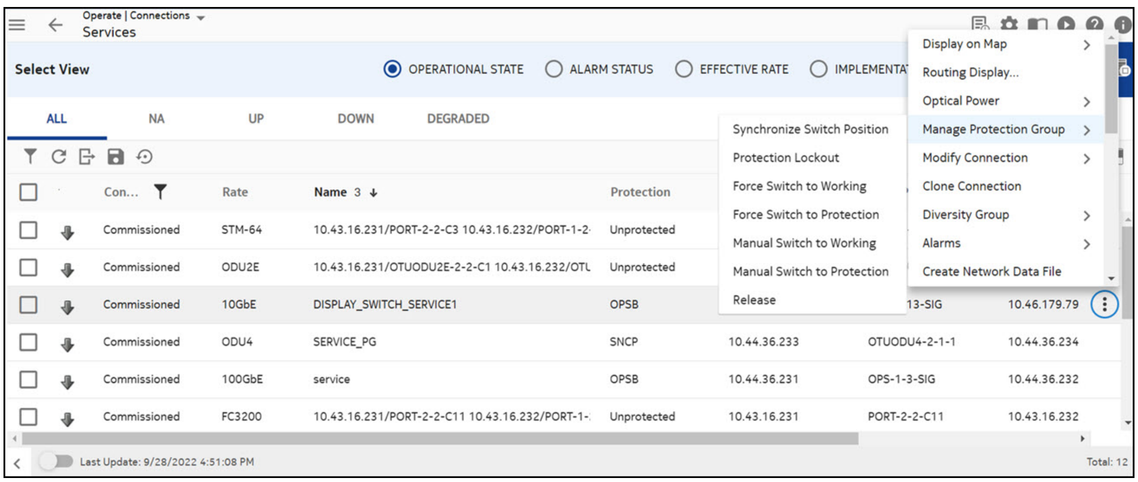
   OPERATE > Services

   OPERATE > Protected Connections

2. Select a service with the **Protection** as **OPSB**.

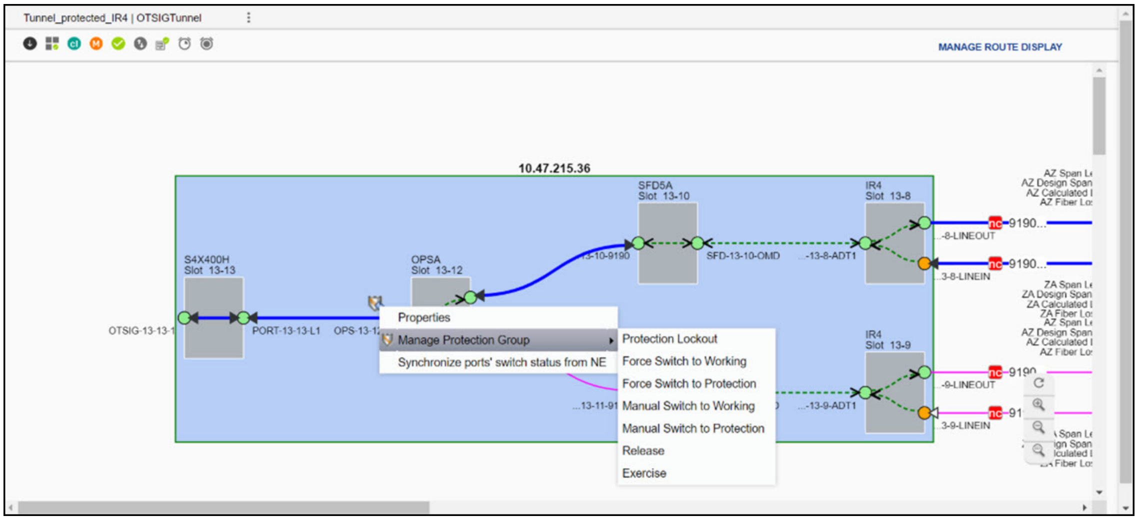
3. Perform one of the following:
   - Click **More** icon **> Manage Protection Group**, refer step 4.
   - Click **Routing Display** icon, on the Routing Display page, right click icon, refer step 5

4. Select the required protection switching operation from the list of protection switching options as shown in the following figure.



5. Select the required protection switching operation from the list of protection switching options as

shown in the following figure.



Result: The system processes your selection and changes the protection switching status to the option that you selected.

OPSB and OPSB5 protection for 20P200

NFM-T supports OPSB and OPSB5 client protection for 20P200 card. The configuration is supported for 1830 PSS-8, 1830 PSS-16II, and 1830 PSS-32 shelves with 1830 PSS NE in release 11.1. The 20P200 supports both protection schemes with 1UD200 and D5X500/D5X500Q/D5X500L cards.

20P200 manages mate configuration with D5X500, D5X500Q cards starting from 1830 PSS NE release 11.0.

The following configurations are supported for OPSB and OPSB5 protections:

1. Two 20P200 cards are installed in one 1830 PSS shelf belonging to one NE.
2. Two 20P200 cards are installed in two different 1830 PSS shelves belonging to one or two NEs.
3. One 20P200 card is installed in one 1830 PSS and the other one in a third-party system.

20P200 supports the following type of Client: 10GbE, STM64/OC192, and OTU2/OTU2e.

The applicable configurations are shown in the following schemes:

Figure 4-40 OPSB and OPSB5 supported configuration with 20P200 - First configuration

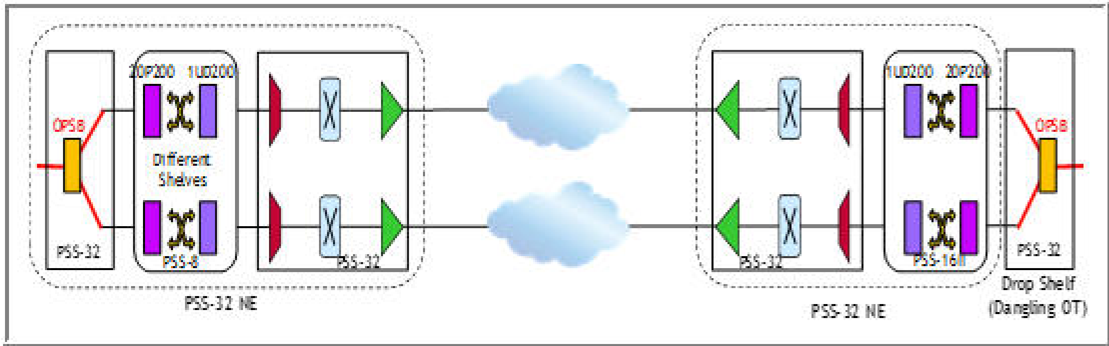


Figure 4-41 OPSB and OPSB5 supported configuration with 20P200 - Second configuration

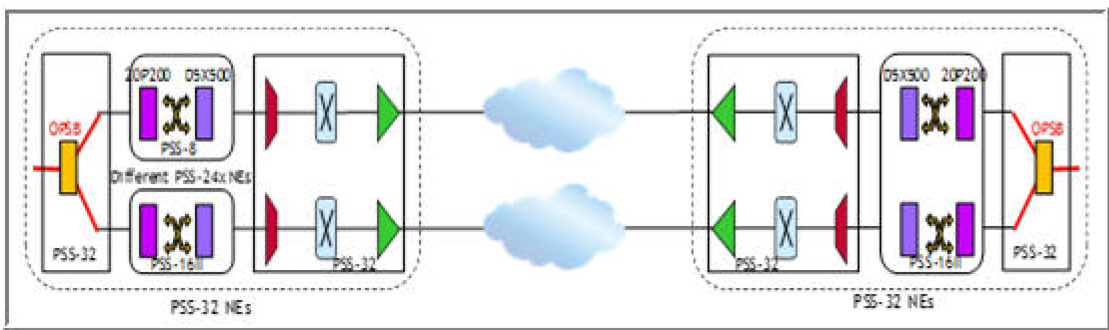
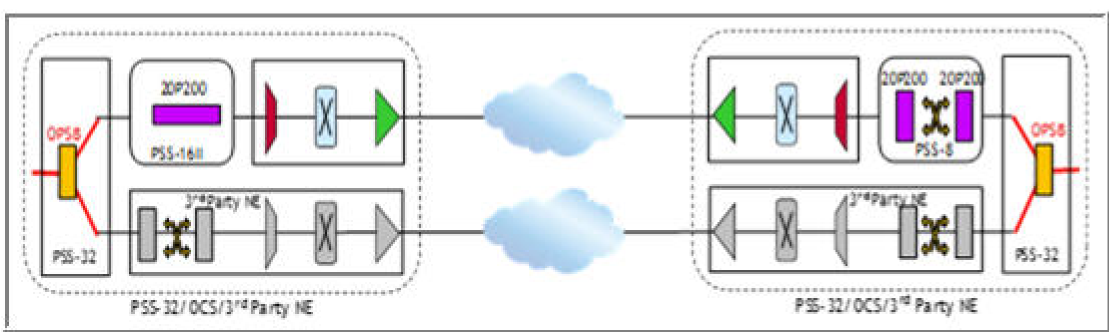


Figure 4-42 OPSB and OPSB5 supported configuration with 20P200 - Third configuration



OPSB can protect either two client ports on the same 20P200 card, or two client ports on two different 20P200 cards, which can be in different shelves or different NEs.

During shelf provisioning the following slot restrictions must be considered:

Table 4-5 Slot restrictions

PSS8 slot group	2	3	4	5
PSS16II slot group	3	4	5	6
	7	8	9	10
Config#1	20P200	D5X500	-	x
Config#2	x	D5X500	-	20P200

When a signal failure is detected on line port, the 20P200 port transmitter is turned off. The port attribute LOSPROP is used to control the status of the client side transmitter during failure on the line port. For additional information see *Troubleshoot OPSB Ports* in the *NFM-T Service Assurance Guide*.

Multi-port OPSB5 or OPSB protection for S4X400H, S5AD400H, and S6AD600H card

NFM-T supports multi-port OPSB5 or OPSB protection for ADD4 cards S4X400H, S5AD400H, and S6AD600H in the following releases:

- S4X400H is supported from NE release 1830 PSS R13.0 and NFM-T R20.7 onwards.
- S5AD400H is supported from NE release 1830 PSS PHN 14.0 and NFM-T R22.6 onwards.
- S6AD600H is supported from NE release 1830 PSS PHN 14.0.8 and NFM-T R22.6 onwards.

OPSB or OPSB5 management on S4X400H, S5AD400H, and S6AD600H card supports the following in Managed Plane and Control Plane configurations:

- 100GbE and OTU4 client signal types
- OTSi line signal
- 400GbE (Only on S6AD600H card)

The client side protection (OPSB or OPSB5) supports automatic internal OS creation. NFM-T automatically creates an internal OS during service creation for Managed Plane.

The internal OS during service creation for Control Plane is based on the following scenarios:

Table 4-6 Client Signal and Internal OS

Client Signal	Internal OS Support
100GbE, 400GbE **Note:** 400 GbE is supported only on S6AD600H card.	Automatic internal OS creation between OPSB or OPSB5 card and ADD4 client.
OTU4	Internal OS between OPSB or OPSB5 card and supported ADD4 cards must be created manually and the links must be assigned in the NPA as drop link.

The OPS module consists of a splitter and a switch. There are no variable optical attenuators (VOAs) at the splitter output (transmit direction). An integrated photodiode (PD) at SIGIN ports detect the client signal. PDs in the receive direction detects LOS that triggers switching. There are no encoders or decoders on the card and switching is based on the LOS detection.

Following are the provisioning guidelines and constraints for OPSB or OPSB5 protection with S4X400H, S5AD400H, and S6AD600H cards:

- The working and protection ports must be from two different cards of the same shelf.
- There are no constraints if the cards are on the same shelf.
- The OPSB or OPSB5 client protection is supported with or without Regen in the middle spans.

The following configurations are supported for OPSB5 protections with S4X400H:

- S4X400H with OPSB5 client protection without Regen (External OPS on both sides with one end as cluster).
- S4X400H on OPSB5 client protection with Regen (Internal OS on both ends).
- S4X400H and 20P200 L0 Mapping with OPSB5 (Managed Plane only).

The applicable configurations are shown in the following figures:

Figure 4-43 S4X400H on OPSB5 client protection without Regen

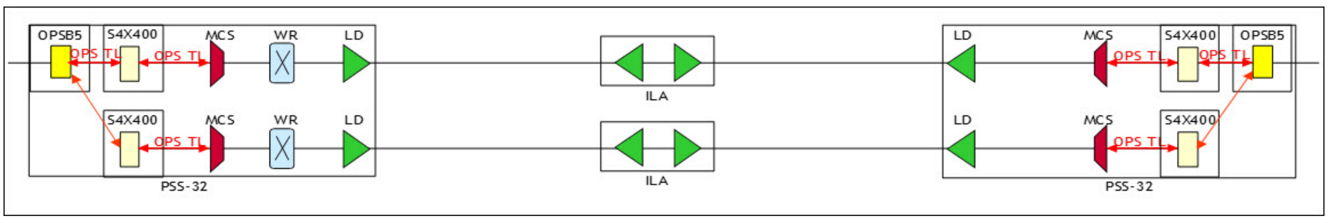


Figure 4-44 S4X400H on OPSB5 client protection with Regen

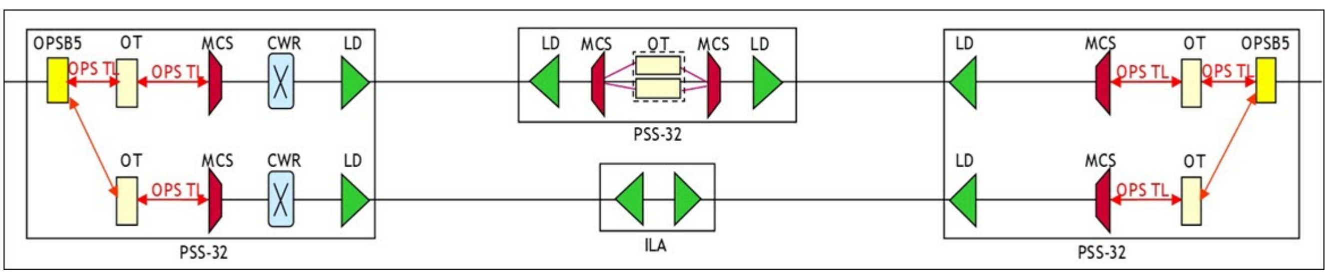
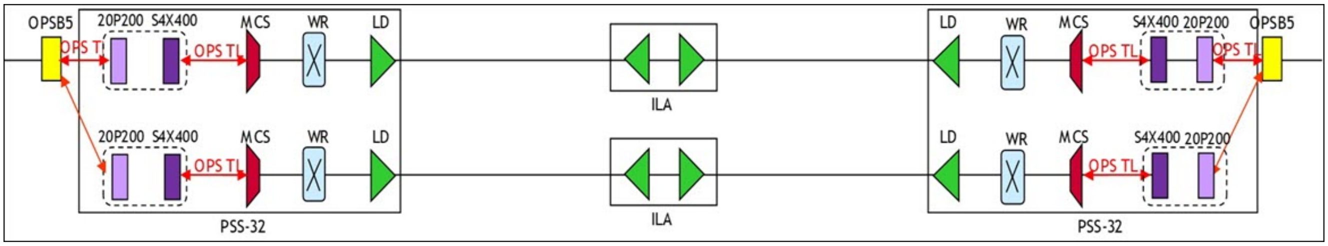


Figure 4-45 S4X400H and 20P200 L0 Mapping with OPSB5 (Managed Plane only)



See “Multi-port OPSB card (OPSB5) definition” (p. 465) for more details.

The following are example configurations supported with OPSB or OPSB5 card:

- ENE connected to an OPSB or OPSB5 card, which in turn is connected to S5AD400H and S6AD400H cards.
- OPSB or OPSB5 card connected to DFC12 card and SFM6 card on one end, S4X400H card and S6AD600H card connected to an OPSB card on the other end.
- OPSB or OPSB5 card connected to two SFM6 cards on one end and two S6AD600H cards on the other end.

OPSB or OPSB5 protection for DFC12 or DFC12E and SFM6 card

NFM-T supports OPSB or multi-port OPSB5 client protection for DFC12 or DFC12E card and SFM6 card in cluster configuration with 1830 PSS or 1830 PSI-8L.

DFC12 or DFC12E card is supported for 1830 PSS-8, 1830 PSS-16II, 1830 PSS-32, and 1830 PSI-8L shelves from 1830 PSS R13.1 and 1830 PSI-M R5.1 onwards.

OPSB or OPSB5 support on SFM6 is from NE version 1830 PSS PHN 14.0.8 and 1830 PSI-M R6.0.8 onwards.

OPSB or OPSB5 management on DFC12 or DFC12E, SFM6 card supports the following in Managed Plane and Control Plane configurations:

- 100GbE and OTU4 client signal types
- OTSi line signal
- 400GbE client signal (Only on SFM6)

External OPS between DFC12 or SFM6 client port to OPSB5 A or OPSB5 B port must be assigned in NPA as a drop link for NNI control plane service creation.

The different configurations supported for OPSB and OPSB5 protections on SFM6 include the following:

- SFM6 with OPSB or OPSB5 client protection with/without Regen (both end as Cluster) (With Regen on S6AD600H):
  - Both the ends of the cards are within the same 1830 PSI-M NE.
  - Both the ends of the cards are between different 1830 PSI-M NE.
- With External NE in the protection leg (Direct OPS between OPSB or OPSB5 cards).

- SFM6 and S6AD600H interworking with/without Regen (With Regen on S6AD600H) (One end with cluster and other end as internal OS).

Following are the provisioning guidelines and constraints for OPSB or OPSB5 protection with SFM6:

- The working and protection ports must be from two different cards of the same shelf.
- There are no constraints if the cards are on the same shelf.
- The OPSB or OPSB5 client protection is supported with or without Regen in the middle spans.

Steps to create the OPSB or OPSB5 connection using SFM6 card:

1. Create a Cluster OPS between the SFM6 line port (L1) and 1830 PHN NE, with interface type as *NNI and Signal Type - OTSi*.
2. Create an external OPS between SFM6 client port and OPSB/OPSB5(A/B) port.
3. Create an OTSiG tunnel with the required profiles.
4. Create an OPSB protected service with supported rates 100GbE, ODU4, or 400GbE.

   Note: In a Control Plane Management setup, for OTU4 rate, the link between OT client port to OPSB A/B ports must be added as drop link in NPA. For configurations with 3R, the internal 3R links must be added as drop link in NPA.

Figure 4-46 Container Type in OPS creation

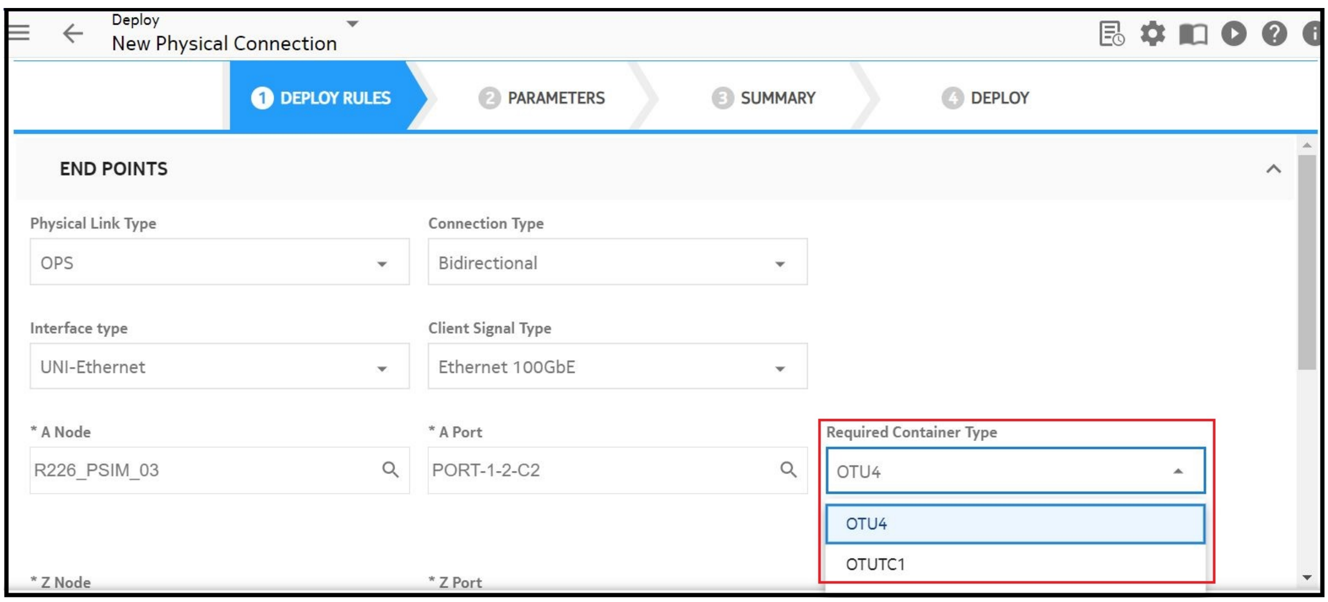


Table 4-7 Container Type and Client Signal Type for OPS

Interface Type	Client Signal Type	Container Type
UNI-Ethernet	100GbE	OTU4 or OTUTC1
	400GbE	OTUTC4 or OTUFlex
NNI	OTU4	-

The following limitations exists with respect to switching and Protection Switch Event (PSE):

- When there is a manual switch to Working or Protection path, PSE are not raised in NFM-T, it is displayed in the events log of WebFM.
- In the following scenarios the synchronize switch position is required to reflect the correct position as per NE:
  - When Wait Time to Restore (WTR) is present, if the alarm on working path is cleared the active route becomes the working path despite the WTR
  - When the WTR time is over and the active route is still on the protection path.

Graphical representation of the applicable configurations are as follows:

Figure 4-47 DFC12 or DFC12E with OPSB or OPSB5 Client Protection

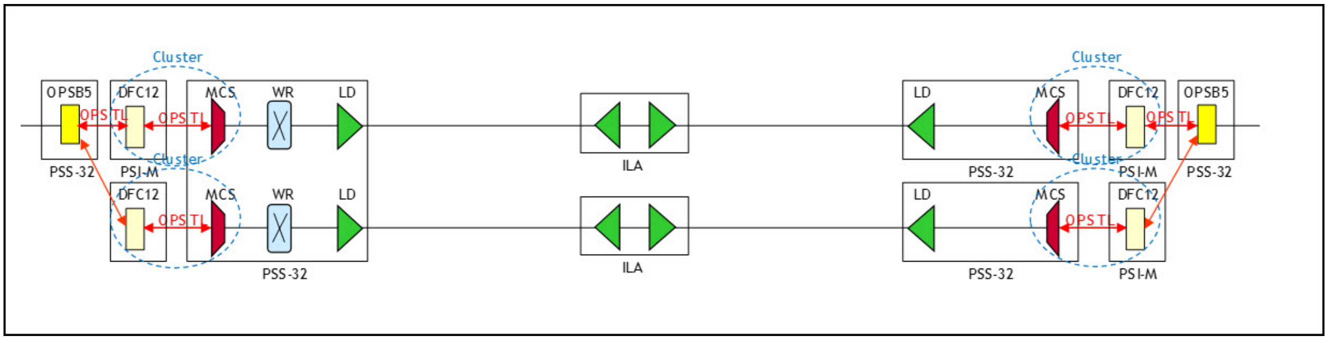


Figure 4-48 SFM6 with OPSB or OPSB5 Client Protection

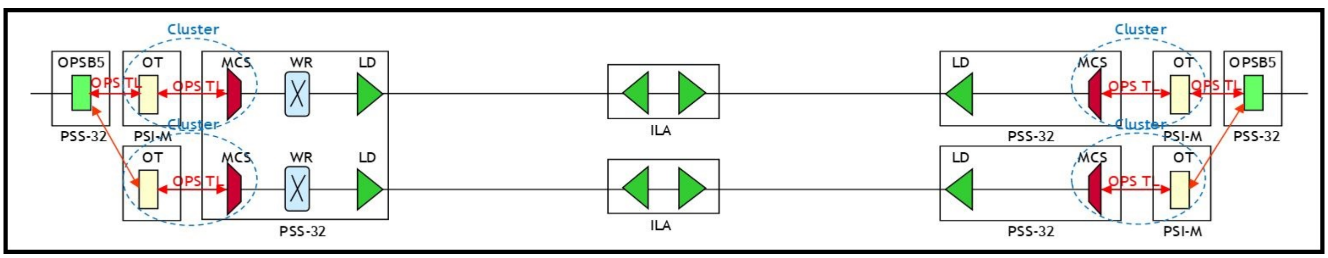
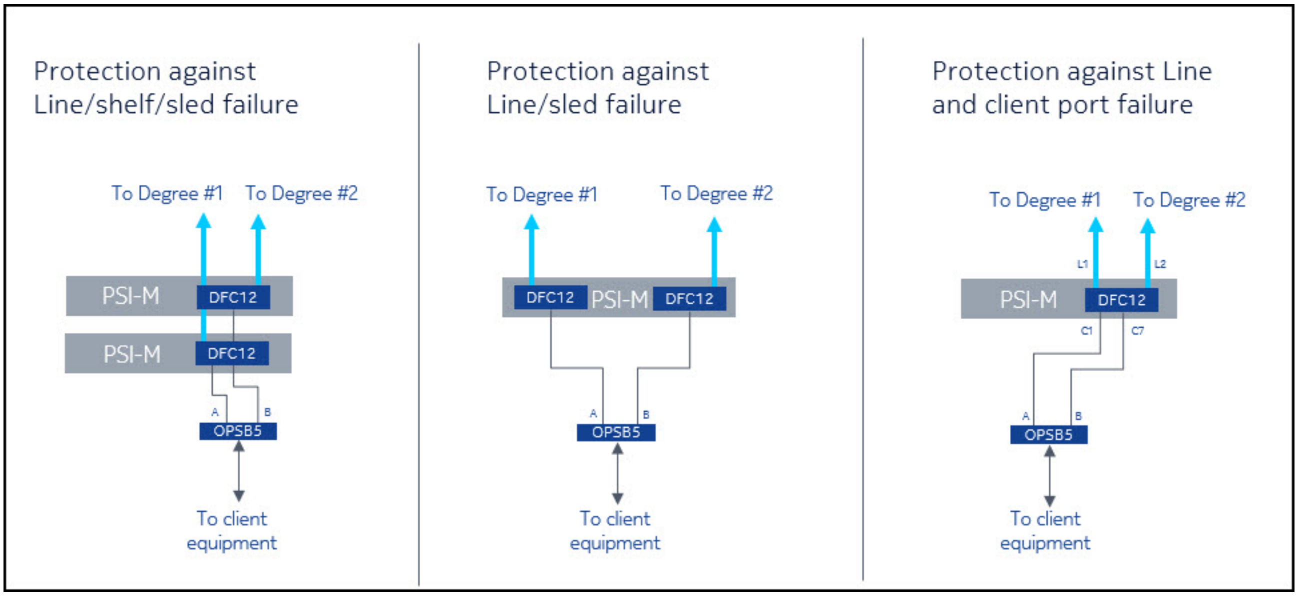


Figure 4-49 PSI-M Client Protection with OPSB or OPSB5 Redundancy Options



Subnetwork Connection (SNC) diversity

For creating OPSB (OPSB5) protected L1 Control Plane connection, Label Switched Path (LSP) is set in diversity mode with two SNCs. In the SNC page, two SNCs get listed as working and protected paths. The working SNC is set to diverse with the protection SNC and vice-versa. For ADD4 cards, to implement the diversity at the tunnel, then manually set it from the NFM-T.

OPSB5 protection in dual NEs configuration

NFM-T supports the OPSB5 protection with dual NEs configuration.

The dual NEs is a configuration where a protection port is connected to an OT plugged on a different 1830 PSS. This configuration is applicable to all OPSB schemas supported by OPSB5.

The OPSB5 with dual NEs configuration can be:

- *Symmetric* where both extremities have the same configuration.
- *Asymmetric* where the dual NE configuration is configured only on an extremity.
- Or, with OPSB in one extremity (single and dual NE configuration).

All the functions supported for OPSB5 with single NE configuration are supported in dual NEs configuration as well.

The configuration is OT and nodal configuration independent. The OPSB5 can be plugged to a Meshed NE or to Add/Drop NE in a Photonic restoration domain (L0-GMPLS).

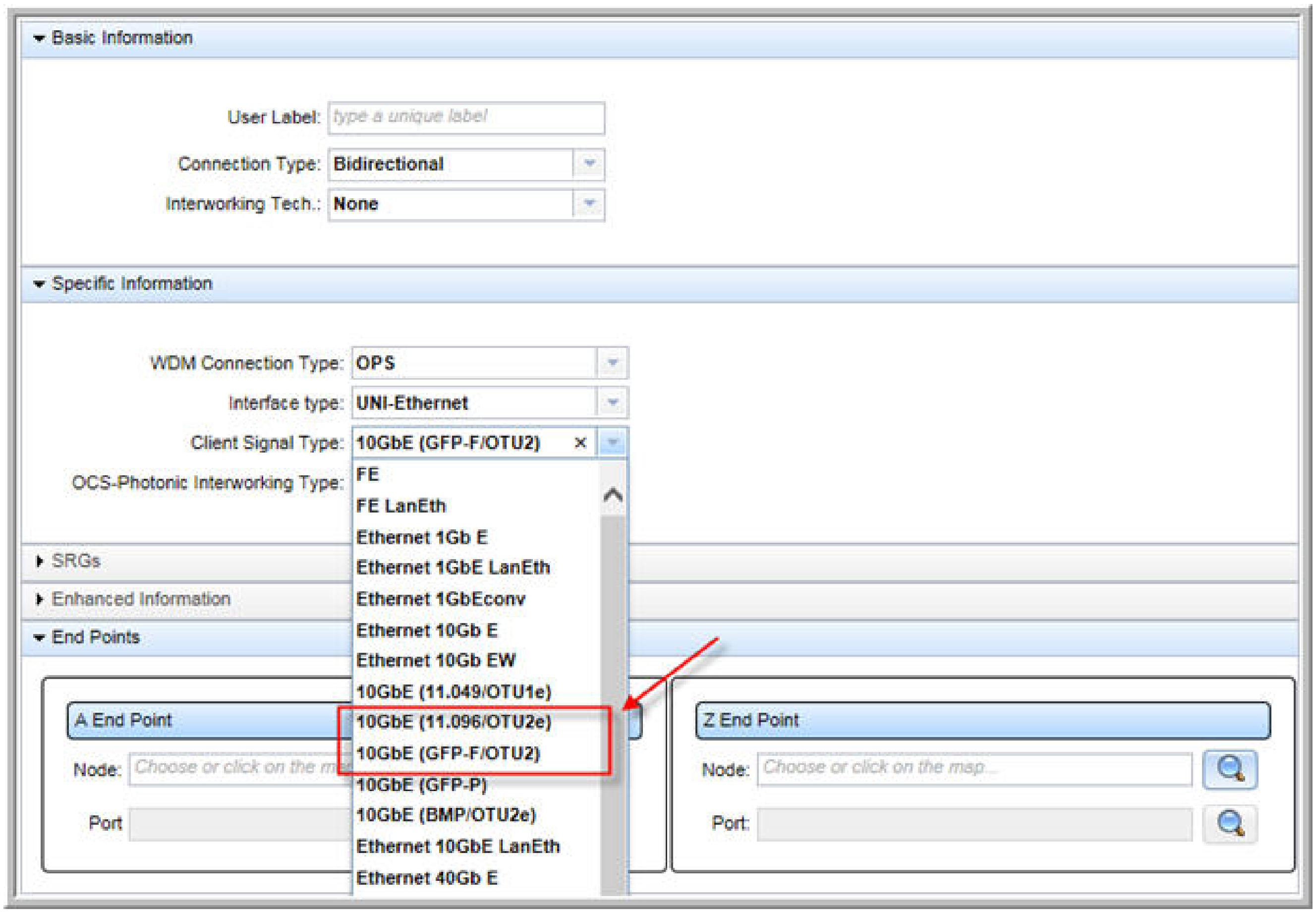
This configuration is supported by 1830 PSS-16II and 1830 PSS-32 shelves, starting from 1830 PSS NE Release 11.0 onwards.

OPSB protection provisioning guidelines for client ports involving PHN OT card

If the OPS creation, with 10GB UNI rate, involves client ports of any PHN OT card that support *containerType*, the following rules apply:

- If the DSR requires an ODU2 container in the physical connection creation window, select **10GbE (GFP-F/OTU2)** as *Client Signal Type*. During OPS creation, the ODU2 container is set in OT card.
- If the DSR requires an ODU2e container in the physical connection creation window, select **10GbE (11.096/OTU2e)** as *Client Signal Type*. During OPS creation, the ODU2e container is set in OT card.

Figure 4-50 OPSB5 - OPS creation window



Managing OPSB protection

Following are some of the methods that are used to manage the OPSB Protection:

- Automatic discovery of OS connections

- Automatic removal of internal links

Automatic discovery of OS connections

When users successfully create a DSR or ODUk service connection with OPSB protection, the management system automatically creates the required OS connections between the following:

- The working ports on the OPSB cards and the OTU client ports.
- The OS connections between the protected ports on the OPSB cards and the OTU client ports.

The DSR or the ODUk connection remains in the **Defined** order step until all OS connections reach the **commissioned** order step.

The number of OS connections that the system automatically creates depends on what **Connection Shape** users specify during service creation.

For a **2 Ended Bi (I)** connection shape, the management system automatically creates these four OS connections:

- One OS connection is created between the working port on the A End OPSB card and the OTU client port that the user selects as the A End working port.
- One OS connection is created between the protection port on the A End OPSB card and the OTU client port that the user selects as the A End protection port.
- One OS connection is created between the working port on the Z End OPSB card and the OTU client port that the users selects as the Z End working port.
- One OS connection is created between the protection port on the Z End OPSB card and the OTU client port that the user selects as the Z End protection port.

For a **3 Ended A Bi (Y)** connection shape, the management system automatically creates these two OS connections:

- One OS connection is created between the working port on the Z End OPSB card and the OTU client port that the users selects as the Z End working port.
- One OS connection is created between the protection port on the Z End OPSB card and the OTU client port that the user selects as the Z End protection port.

For a **3 Ended Z Bi (Y)** connection shape, the management system automatically creates these two OS connections:

- One OS connection is created between the working port on the A End OPSB card and the OTU client port that the user selects as the A End working port.
- One OS connection is created between the protection port on the A End OPSB card and the OTU client port that the user selects as the A End protection port.

Automatic removal of internal links

When users cancel a DSR or ODUk OPSB protected service, the internal links between the working ports on the OPSB cards and the OTU client ports and the OS connections between the protected ports on the OPSB cards and the OTU client ports are automatically removed.

4.6 OMSP – OMS SNCP

Optical Multiplex Section Protection definition

Optical Multiplex Section Protection (OMSP) is the mechanism that protects both optical amplifiers and transmission fibers. OMSP is supported in FOADMs and ROADMs.

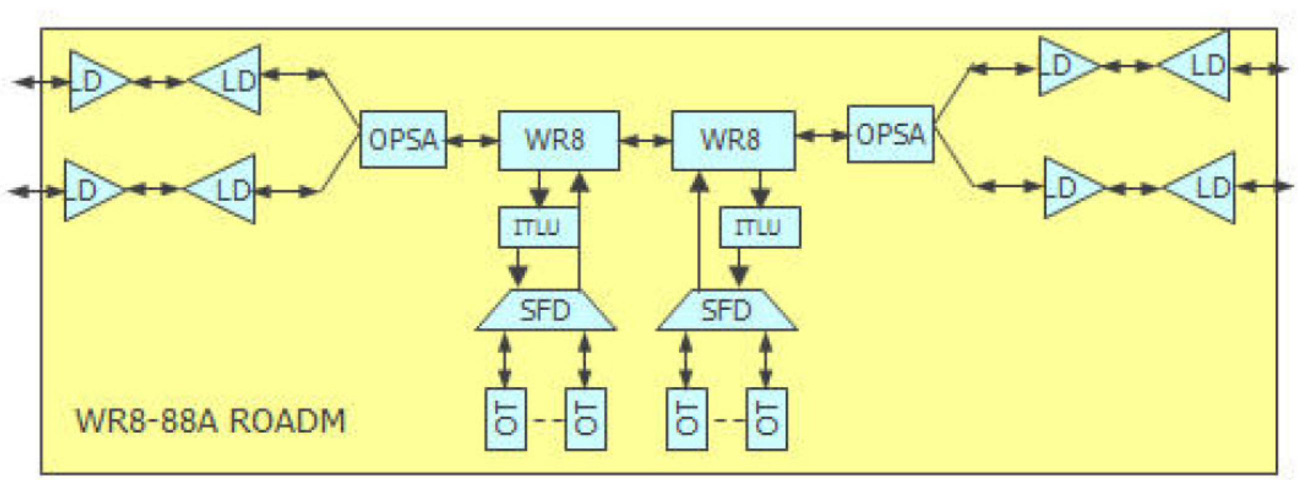
OMSP in ROADM configuration

ROADMs that use OMSP are connected to other ROADMs or FOADMs that use OMSP, with intermediate ILA and DGE sites. DGEs are treated like ILAs for this purpose. Working and protection paths do not terminate at either ILAs or DGEs.

Note: When a fiber break occurs, the service interruption shall not exceed 50 ms.

The following figure illustrates a degree-2 WR8-88A(F) ROADM configured for OMSP. OMSP with WR8-88A(F) ROADMs is supported up to degree 5.

Figure 4-51 Degree-2 WR8-88A(F) ROADM configured for OMSP



Note: OMSP is not supported for unkeyed cross connections.

OMSP links are allowed within linear, mesh and ring network configurations. Only manual power control is supported for these configurations.

Mesh and through connections are supported in OMSP-protected ROADM configurations provided that both optical lines that are involved in the connection are configured for OMSP. Any channel that is routed between an OMSP optical line on a ROADM and a non-OMSP protected optical line on that ROADM shall be regenerated at the ROADM.

OMSP is supported with an intermediate DGE ILA that does not serve as a termination point for the OMSP protection. Regular ILAs and DGE ILAs are supported on the same working or protection leg in an OMS that uses OMSP. The DGE ILA can use WR2-88, WR8-88A or WR8-88A(F) cards.

OMSP ROADM with WR8-88A(F)/WR8-88A is supported on:

- 1830 PSS-32
- 1830 PSS-16
- 1830 PSS-16II

OMSP ROADM with WR2-88 is supported on:

- 1830 PSS-32
- 1830 PSS-16

The following LD cards support OMSP protection on a ROADM:

- Ingress:
  - AHPHG
  - AHPLG
- Egress:
  - None
  - AHPHG
  - AHPLG
  - A2325A

Note: A2325A is not supported as an ingress LD.

For an OMS that is in an OMSP configuration, both unidirectional and bidirectional LDs may be used at ILAs or DGEs.

1830 PSS-32, 1830 PSS-16, and 1830 PSS-16II are the supported shelf types for the core optical equipment used in ROADMs that support OMSP.

OMSP in FOADM configuration

FOADM nodes also support OMSP. In the transmit direction, the SFD/ITLB total output channels are routed to two different DWDM lines by the OPSA card. In the receive direction, the OPSA selector picks one of the two lines as the active path based on power monitoring or user manual selection. 1830 PSS-32 and 1830 PSS-16 shelves support OMSP in FOADMs. Auto power management is not supported for these configurations.

In OMSP protection configuration, the number of consecutive ILAs within a protected link must not exceed five due to possible delay in protection time.

Note: Raman amplification is not allowed on a ROADM line that is configured for OMSP. Raman amplification is not allowed in any ILA or DGE site that is in the working or protection leg of an OMSP-protected optical path.

Figure 4-52 OMSP in SFD end-terminal

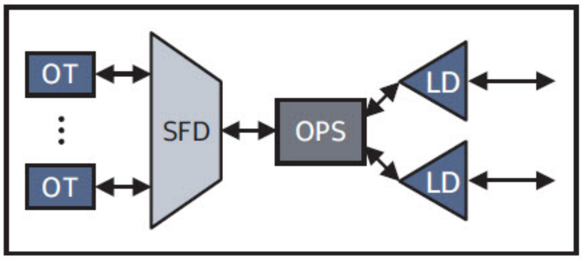


Figure 4-53 Multi-degree FOADM with 2 OMSP protected links

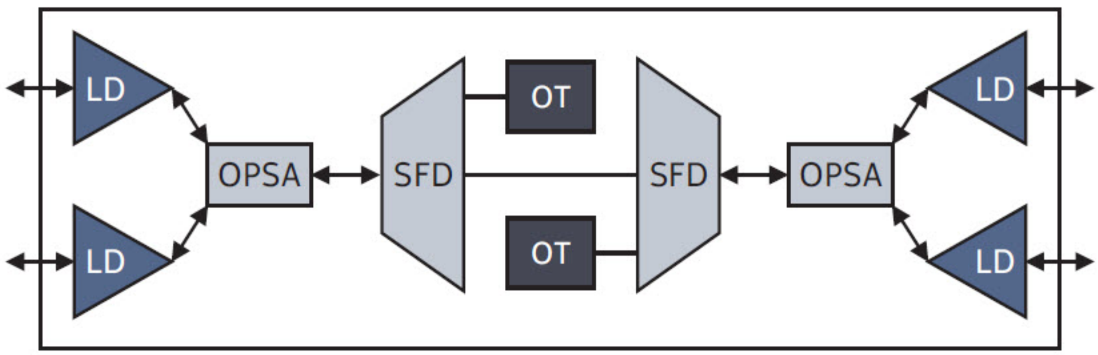
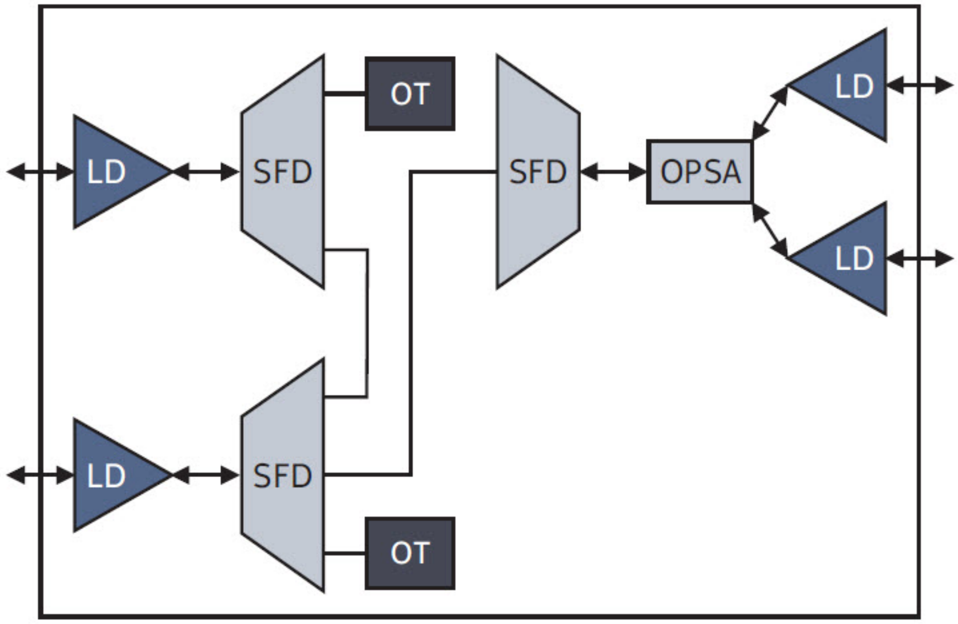


Figure 4-54 Multi-degree FOADM with 1 OMSP protected link and 2 unprotected links



The following cards support OMSP on a FOADM:

- Ingress:
  - ALPHG
  - AHPHG
  - AHPLG
- Egress:
  - None
  - ALPHG
  - AHPHG
  - AHPLG
  - A2325A

The following SFDs and ITLB cards are supported with OMSP on a FOADM:

- SFD5
- SFD8
- SFD40
- SFD40B
- SFD44
- SFD44B

- ITLB

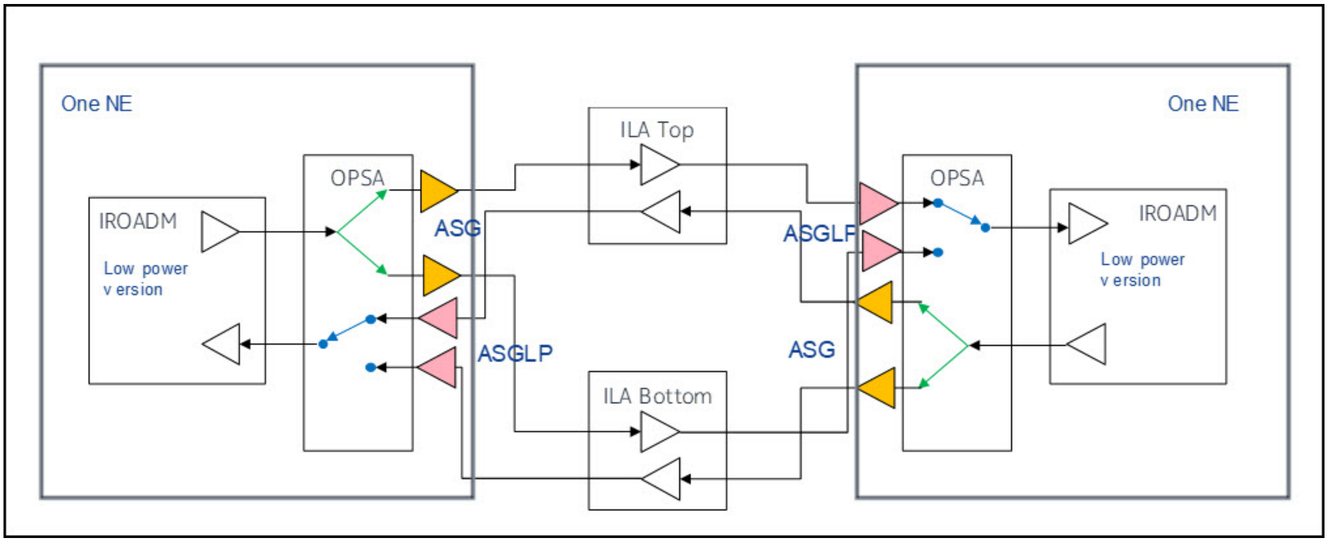
Note: OMSP is not supported on CWDM FOADM nodes.

OMSP Line Side protection for IROADM card

NFM-T extends Line Side protection - OMSP support to IROADM card. Only low power version of the IROADM cards are supported. OPSA card with Protection Mode is set to OMSP mode.

The following figure represents the configuration of IROADM with OMSP protection:

Figure 4-55 IROADM with OMSP Protection



The OMSP Line protection for IROADM card is supported on 1830 PSS NEs from R13.1 onwards on the following shelf types:

- 1830 PSS-32
- 1830 PSS-8
- 1830 PSS-16II
- 1830 PSI-8L

The supported low power variant IROADM cards are as follows:

- IRDM20 (Low Power)
- IRDM32LP
- IR9LP
- OPSA (Protection Mode as OMSP)
- LDs:
  - ASG, ASGLP

- OT/Uplink cards:
  - All supported cards

The route constraints for connection provisioning over OMSP set-up are as follows:

- Automatic Routing with trail route constraint is supported. At least one OMS trail of each OMSP should be added as route constraint.
- Manual routing with Link Connection (LC) as a route constraint
- Manual routing with trail as a route constraint
- Trail provisioning involving Regen in an OMSP set-up is not supported in NFM-T R21.4.
- Infrastructure protected trails over Heterogenous configurations involving mix of OMSP and OMS trails as servers with or without 3R is not supported in NFM-T R21.4.

Note:

- Nested protection is not applicable for OMSP protected trail.
- When creating the Trail Connection over OMSP set up, create the connection as protected connection (**Protection** checkbox as selected), an ODUk/OTSigTunnel unprotected connection will be created with underlying server connection as **OMSP Server Protected**. If not selected as protected, system picks any of the OMS trail that is available and creates an unprotected connection.

  Note: Ensure OMSP trail is created, before creating the ODUk/OTUk on OMSP protected links.

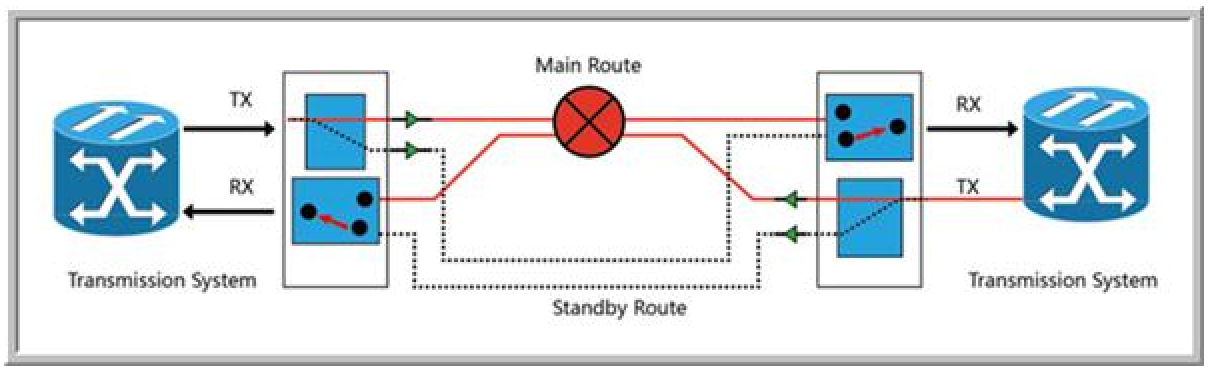
4.7 Optical Line Protection

Optical Line Protection definition

Optical Line Protection (OLP) system increases the stability and reliability of the optical network avoiding the problems related to optical fiber faults and line interruption. OLP is based on the principle of the optical switch to build a backup path on free optical fiber. Simple optic protection includes a primary path and a secondary path. The commonly used fiber protection is based on the 1+1 scheme.

As shown in the Figure 4-56, "1+1 OLP schema" (p. 487), in OLP 1+1, the optical power from Tx are splitted with a split ratio of 50:50 on the main route and the standby route, which means both the main and standby routes are in use no matter whether there is a fault in the main route. While for Rx, the optical signal with better quality will be selected. The advantage of OLP 1+1 system is fast switching and low cost.

Figure 4-56 1+1 OLP schema



Best Practice templates for Optical Line Protection

From the NFM-T GUI, navigate to **DEPLOY > New Service/Infrastructure Connection** and select the **OMS** template from the **Service/Infrastructure Templates** deploy window to provision a connection with OLP.

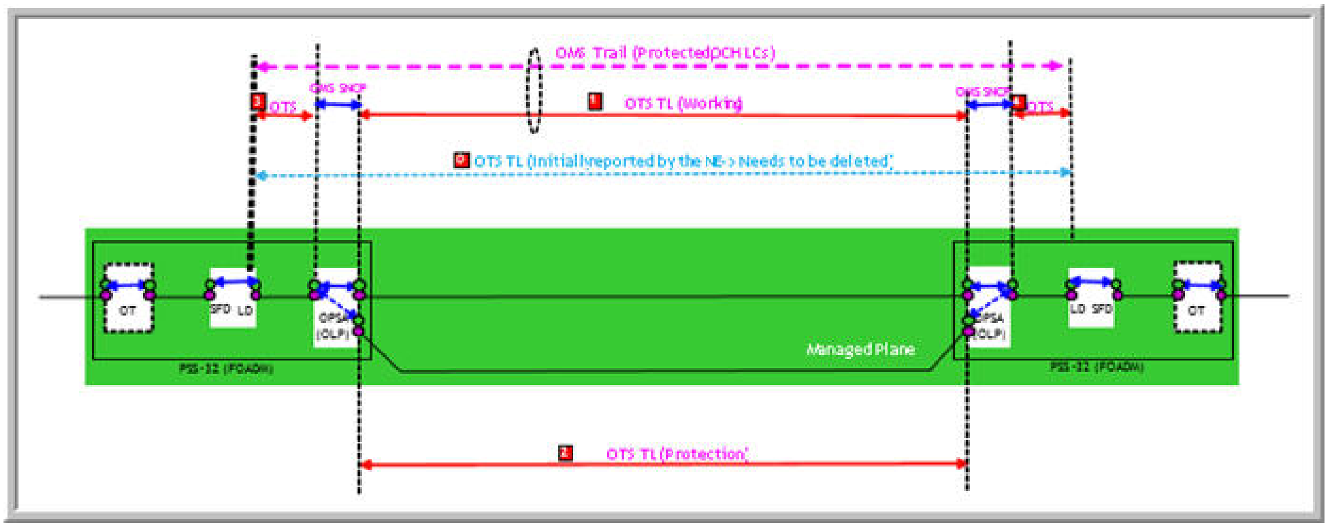
Optical Line Protection provisioning guidelines

Optical Line Protection provisioning guidelines provides information on the OLP protection. There are two scenarios during the provisioning and supported by the system:

- OPSA is in place and fibered but not provisioned
- OPSA is in place, fibered and already provisioned

The scheme reproduces the sequence to be followed for the OLP provisioning.

Figure 4-57 OLP provisioning scheme for bidirectional



Note: For the OLP provisioning scheme for a unidirectional connection, create two unidirectional LDs.

OPSA is in place and fibered but not provisioned

Follow the step to set up the protection configuration with OPSA already installed and not provisioned:

1. The NE indicates a topological OTS connection, # 0 (Dashed Blue), between the LD cards of node A and Z line port, that is discovered by NFM-T. Remove the topological OTS link (# 0).
2. To provision the OPSA card, set the card protection mode to OLP.
3. SIG, A and B ports, must be in admin Down. If any of the three ports is set to admin up, you may run into one of the following cases:
    a. The SIG port must not be already connected to another port before the OPSA card is set to OLP. This means that the OPSA card needs to be provisioned to OLP before the OTS topological link on SIG port to LD’s LINE port for bi-directional and LINEIN/LINEOUT port for unidirectional. This can be provisioned.
    b. A and B ports must not be already connected to an internal port before the OPSA card is set to OLP.
    c. The A and B ports are set to External by the NE.
4. Provision the OTS Working (#1) and Protection (#2) topological links. Provision the internal topological links (#3 and #4). Links are marked with red in the reference scheme.
    a. After the OPSA card is set to OLP mode and the topology link is provisioned between the LD LINE port for bi-directional and LINEIN/LINEOUT port for unidirectional, and OPSA SIG port, the adjacent node IP address and the shelf, slot and port information must be cleared out. After the topology provisioning is done on the adjacent NE, the NPR needs to enter the far

end adjacent node's IP address and the shelf, slot and port information for the OPSA A/B EXTERNAL ports to declare the physical connection to the adjacent network element.

b. A protection group is automatically created by the NE SW after OPSA/SIG port and LD/LINE/LINEIN/LINEOUT port are connected. As default, port A is the Working port, and port B is the Protection port.
c. An OMS SNCP, not existing on the NE, is auto created.
d. The topological link between OPSA/SIG and LD/LINE/LINEIN/LINEOUT is Auto Power managed. This feature is supported for NEs in release 10.1.

5. The topology link between an LD LINE/LINEIN/LINEOUT port is auto discovered as external and the OPSA SIG port of an OLP mode. For bidirectional, the user can provision one internal link between the LD LINE and the OPSA SIG port. For unidirectional, the user can provision two internal topology links between LD LINEIN/LINEOUT and the OPSA SIG port.
6. Once the provisioning is complete, there will be two linked topology EXTERNAL links per OLP degree.
7. The protected OMS trail is auto generated.

OPSA is in place and fibered and already provisioned

The OPSA has been set to OLP, and the OTS topological links are provisioned.

NFM-T auto discovers the OPSA configured with OLP mode and the four OTS topological links, and then generates the protected OMS trail.

OLP on the NFM-T

In the NFM-T system, OLP 1+1 scheme is employed for the protection of the optical line OTS layer. The protection requires two connections: the working (OTS-W) and the protection (OTS-P) connections between the two OPSAs. The two connections could be physically diverse.

Figure 4-58, "Example of OLP protection for Uni-directional with one LD" (p. 489), Figure 4-59, "Example of OLP protection for Uni-directional with two LDs" (p. 490), and Figure 4-60, "Example of OLP protection for Bi-directional" (p. 490) illustrates the examples of OLP protection. Where an OPSA card is used as OLP protection between two ILA NEs. The separate connections, can be differently physically routed.

Figure 4-58 Example of OLP protection for Uni-directional with one LD

Figure 4-59 Example of OLP protection for Uni-directional with two LDs

Figure 4-60 Example of OLP protection for Bi-directional

The OLP protection is supported by the following:

- Cards/NEs: S13X100R, S13X100E, D5X500, D5X500Q,12P120, and 1830 PSI-2T
- Low priority OTs: 112SNA1 and 112SNX10
- CDC-F LDs: Uni-directional, with MCS as Add/Drop block, including iRDM20, ASWG, AM2125A, AM2125B, AM2318A, and AM2032A.
- Nodes: C-F, CDC-F, DWDM, FOADM, ILA
- Low Priority T/ROADM with WR8-88 or CWR-88

LD employed for OLP protection could be bidirectional LDs and unidirectional LDs.

The supported client services rate is 100GbE.

Note:

1. OLP protection cannot be mixed with any other type of protections, for example, OCHP, OMSP, and so on.
2. Deletion of internal TLs is possible only through EQM and when OMS (OLP) does not exist.
3. OMS creation is supported only through manual routing.

To create OMS through manual routing

Ensure the following settings for manual routing of an OMS protected connection:

1

In the NFM-T GUI, navigate to **New Service/Infrastructure Connections**.

Result: In the left portion of the New Service/Infrastructure Connections window, the system displays a tree with the folders **Best Practices** and **Published**.

2

Navigate to select **OMS** template.

Result: The system displays the connections in the data table format in the right pane of the window.

3

Click **Deploy**.

Result: The system displays the **Create Connection** window.

4

In the **Create Connection** window ensure the following settings:

In the **END POINT SELECTION** panel:

- The **Connection Shape** is set to **2-Ended Split Bi (I)**

In the **CONNECTION CHARACTERISTICS** panel:

- The **Protection** is checked.
- The **Protection Mode** is set to **OLP**.
- The **Routing Mode** is set to **Manual**.

5

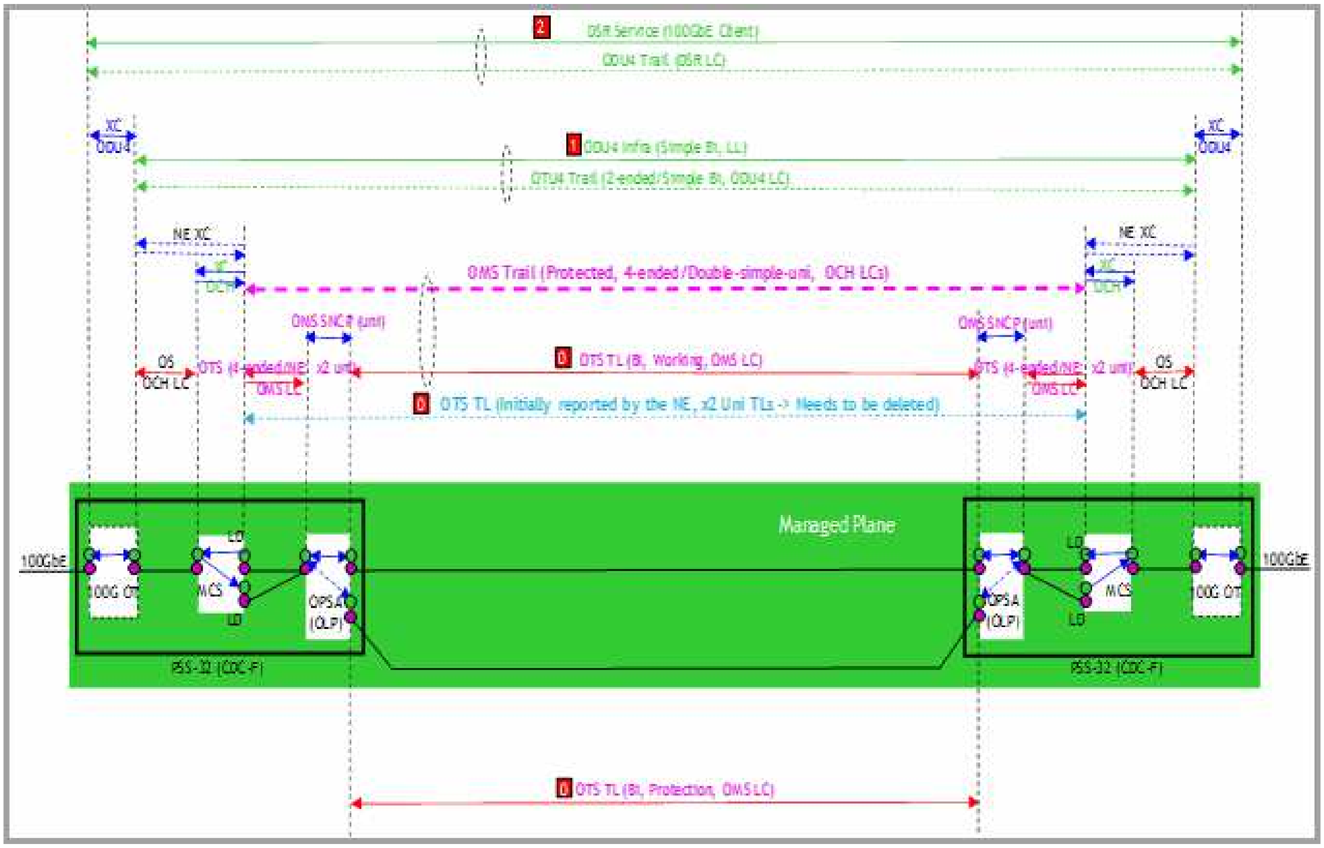
In the left portion of the **Create Connection** window, in the **Routing Constraints** tab, the Constraint Type must be **Trail/Link Constraint**.

END OF STEPS

OLP model

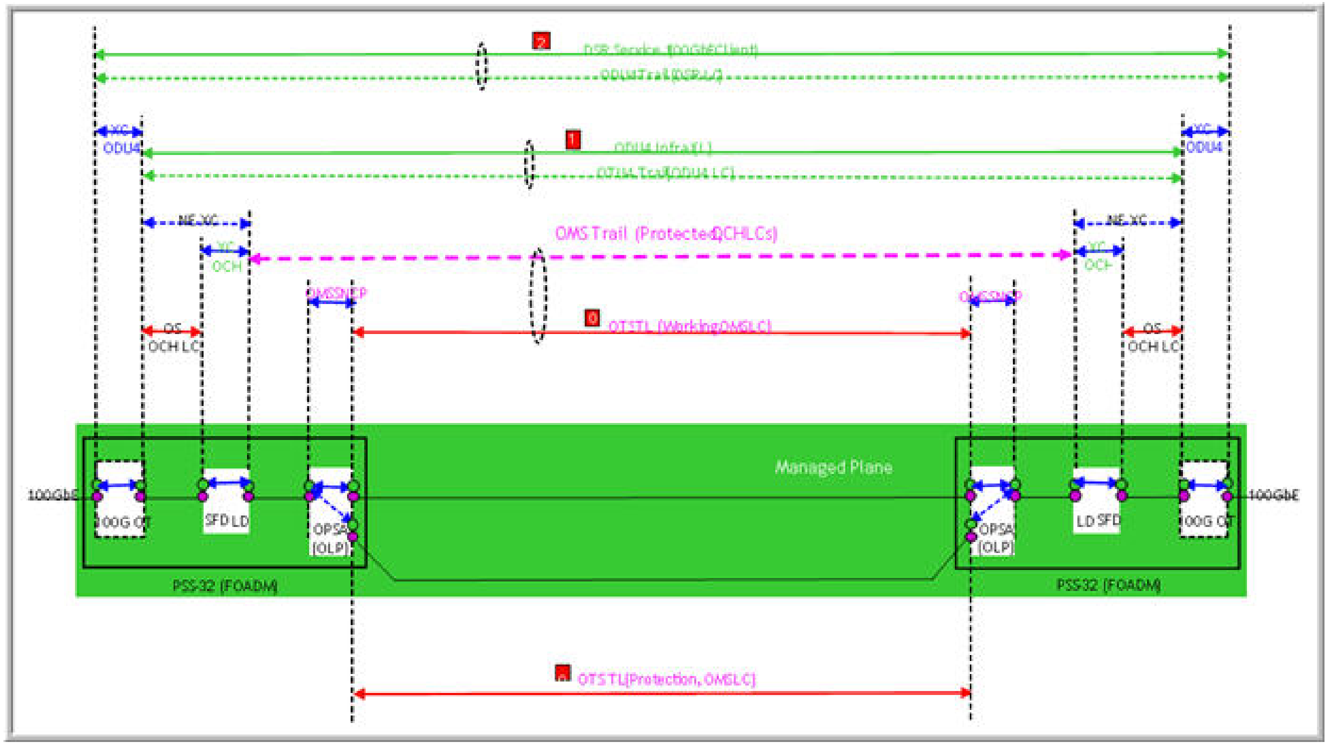
The optical model of the OLP protection for unidirectional LDs is depicted in the Figure 4-61, “OLP protection connection management for uni-directional LDs” (p. 492). As illustrated in the figure, there are two external OTS topological links representing the OLPs working and protection connections. For the OLP protection configuration, two internal OTS topological links are required for the unidirectional LDs. The OPSA card needs to be in the OLP mode and OMS SNCP is automatically created for the OTN. The OMS trail terminates at LD LINE/LINEIN/LINEOUT connecting to SIG port of OPSA.

Figure 4-61 OLP protection connection management for uni-directional LDs



The optical model of the OLP protection for bidirectional LDs is depicted in the Figure 4-62, “OLP protection connection management for bi-directional LDs” (p. 493). For the OLP protection configuration, one internal OTS topological link on each side between the bidirectional LDs and OPSA/SIG port is required.

Figure 4-62 OLP protection connection management for bi-directional LDs



OLP OPSA configuration for fiber characteristics

When OPSA is used in OLP configuration, external OTS links are created between OPS-A ports and OPS-B ports respectively. The OPSA card however, is transparent and not considered for Fiber characteristics data. The fiber characteristics are effectively shown between the LD ports, and not against the OPSA ports that are connected to external OTS link.

OLP and OPSA in ASON networks

NFM-T manages OLP protected links in ASON networks:

- L0 networks: with OTS ASON link supported by OLP. OMS trail protected with OLP are available to be added to ASON NPA as normal ASON Links in L0, no special characterization is needed if they are protected with OLP.
- L1 networks: ASON logical links using OTS with OLP. In this case OLP switching and L1 restoration as GMRE uses fast fault detection and triggers restoration in advance. It waits only 20 ms while OLP switching takes 50 ms. A TCM Defect Raising Time can be configured on L1 link so that restoration is triggered only if OLP switch does not clear the fault.

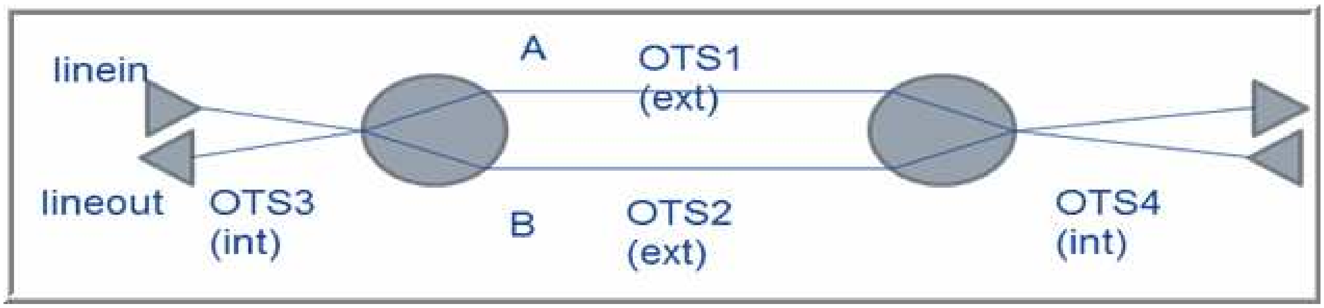
GMRE default value is 20 ms for a TCM monitored link, independently from the server protection (OPSA, OPSFlex, OLP), even unprotected.

OLP - network example

The OLP features applies to OTS protection. Amplifiers are connected to OPSA card and OPSA A/B ports are connected to OPSA A/B ports of remote NE. Amplifiers can be unidirectional or bidirectional C band amplifiers or iROADM cards. Protection in NE is OTS protection but NFM-T models it as OMS protection.

The OPSA card id connected to amplifiers.

Figure 4-63 OLP - Network Example



L0 - If OLP is already configured, an OTS between amplifiers is discovered. Remove the OTS link and then create:

- internal links between amplifiers and OPSA-SIG port using EQM
- external OTS between OPSA A/B ports At this point the ASON logical link should be available to be added to ASON NPA

L1 - Set the TCM Defect Raising Time (TCM delay timer in GMRE) according to the protection schema implemented at server layer.

Network protection

4.8 SNC protection

SNC protection definition

SNC protected connection can have managed plane SNC network protection, control plane SNC protection, managed plane client SNC protection or a combination of these types.

SNCP is specified for infrastructure connections (trails) or services to create protected cross connections on 1830 PSS-OCS NEs or on 2UC400, 4UC400, 30AN400, 4AN400 cards or a port on the Virtual Plane (which is a port with slot identifier equal to 71). MP SNCP is Managed Plane SNCP where the protection group is in the managed plane domain. CP SNCP is the Control Plane SNCP where the protection group is in the control plane domain. A mixed plane connection can have MP SNCP, CP SNCP or both.

NFM-T supports the following SNC protection:

- SNC/I: ODUk subnetwork connection protection with inherent monitoring (1+1, 1:n)
- SNC/N: ODUk subnetwork connection protection with non-intrusive monitoring (1+1)
- SNC/Nc: SNC protection for network client ports
- SNC/S: ODUk subnetwork connection protection with sublayer monitoring (1+1, 1:n)

SNC protection Best Practice templates

From the NFM-T GUI, navigate to **DEPLOY > New Service/Infrastructure Connection** and select one of the following templates from **Service/Infrastructure Templates** deploy window to provision SNC Protected connections for 1830 PSS-OCS NEs:

- **SNC-N Protected Uplink ODUk**
- **SNC-N Protected Uplink ODUk with L0 Restoration**
- **SNC-I Protected Uplink ODUk**
- **SNC-I Protected Uplink ODUk with L0 Restoration**
- **SNCP Protected STM-N**
- **SNCP Protected STM-N with Restoration**
- **STM-N with external 1+1 MSP Protection**
- **SNCP Protected OC-N**
- **SNCP Protected OC-N with Restoration**
- **OC-N with external 1+1 APS Protection**

SNC protection provisioning guidelines for connections and services

Users can specify SNC parameters for the following types of infrastructure connections (trails) and services on the **SNC Protection** panel during connection provisioning:

- The connection **Rate** is ODUk or the connection **Rate** is DSR and **Auto Server Creation** is selected.

- For infrastructure connections (trails) and services where the **Connection Shape** is **2 Ended Bi (I)**, **4 Ended Bi (X)**, **3 Ended A Bi (Y)**, or **3 Ended Z Bi (Y)**.
- For infrastructure connections (trails) and services where the **Routing** field is set to **Automatic** and the **Protection Type** field is set to **Protected**; or the **Routing** field is set to **Manual**.
- For services where the **Y-Cable Protection** parameter is disabled (set to **No**).
- For services where the connection level **OPSB Protection** parameter is disabled (set to **No**).

For details on the SNC Parameters panel, the SNC parameters and their values, refer to "SNC Protection" (p. 717).

SNC protection guidelines for 1830 PSS OCS and 1830 PSS PHN NE

If at least one connection endpoint is on an 1830 PSS OCS NE and at least one connection endpoint is on an 11DPM12 or 11QPA4 card on an 1830 PSS, 1830 PSS-4 NE, users must specify the **Network Protection Type** to be **None** or **SNC-N**.

SNC protection for rerouted connections

The SNC Protection panel is displayed for the reroute of WDM connections if the **Reroute** type is **Add Protection** or **Modify route** and if the connection rate is **ODUk**.

ODUj SNCP protection for 12P120 with FC1200 client

The NFM-T supports the protection ODU2e SNCP for the 12P120 card with FC120 client. This configuration is available for Managed Plane only.

The NE releases supported are the releases starting from 1830 PSS-R10.0 and 1830 PSS-4 R10.0, the supported shelves are: 1830 PSS-32, 1830 PSS-8, 1830 PSS-16II and 1830 PSS-4.

Configurations can be: ODU2e SNCP for 12P120 with FC1200 client and CDC-F ROADM, DGE (Single bladed, for CDC-F), ILAs (for CDC-F). All the configurations are managed plane only.

Network Scenario Example

The example in figure displays a network scenario that is setup for the 12P120 card with FC1200 client and protection SNCP.

Figure 4-64 Network Scenario: 12P120 ODU2e SNCP on FC1200 client – MP only

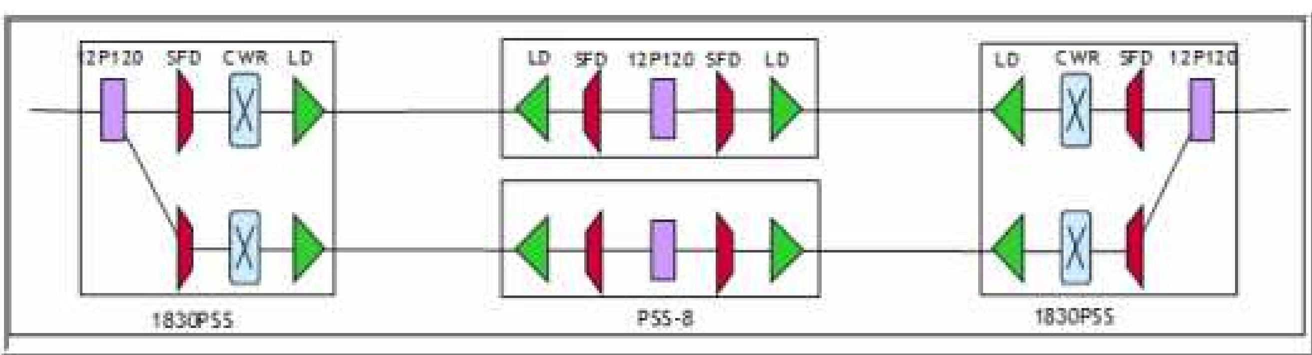
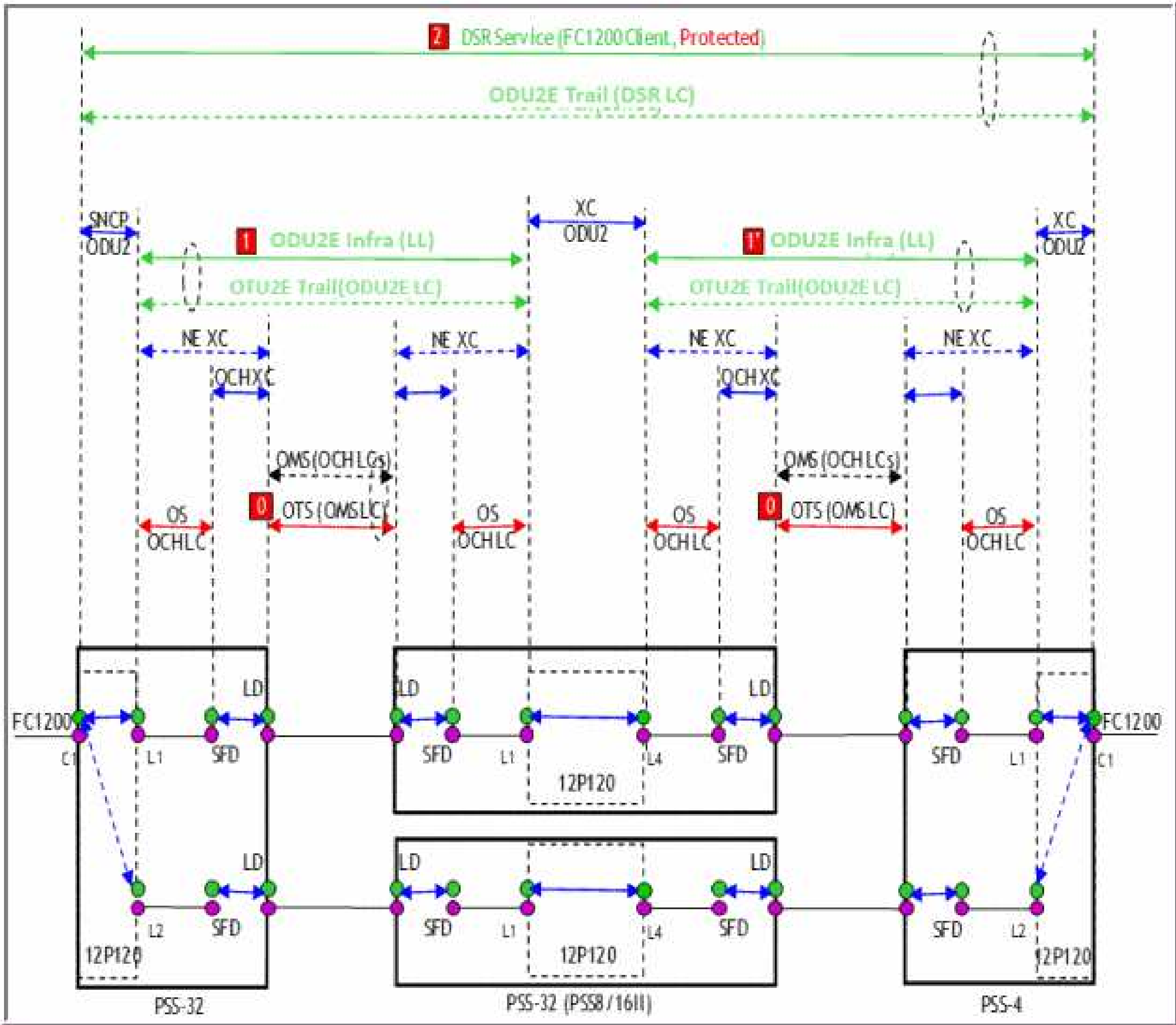


Figure 4-65 12P120 ODU2E SNCP on FC1200 client – MP only



ODUj SNCP protection for 11QPA4B card

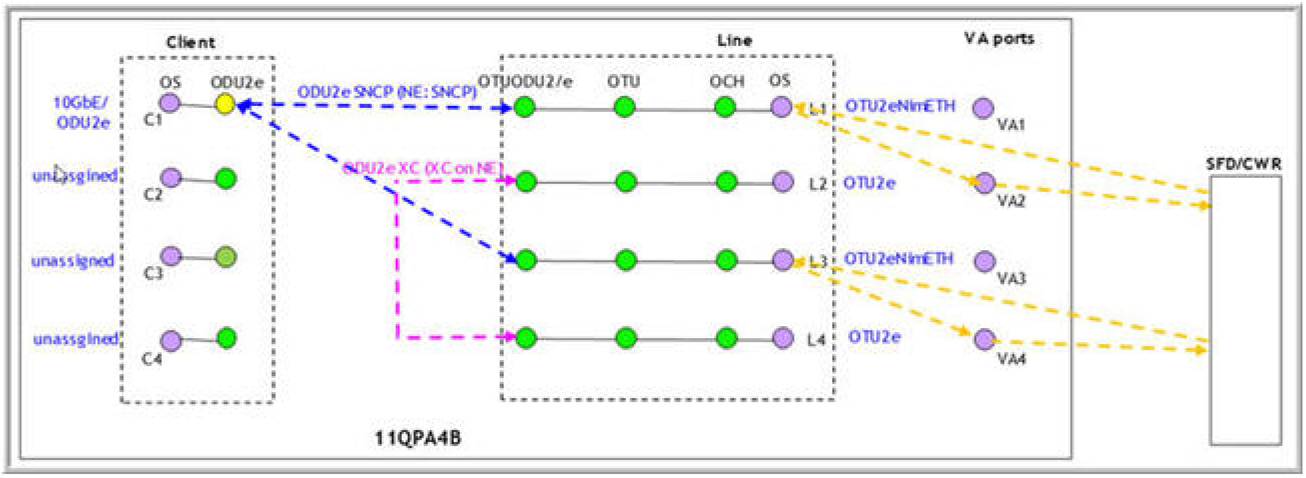
The NFM-T supports the SNCP ODU2/e protection with 11QPA4B card.

The NE releases supported are the releases starting from 1830 PSS-32 R12.0 and 1830 PSS-4 R12.0, the supported shelves are: 1830 PSS-32, 1830 PSS-8, 1830 PSS-16II and 1830 PSS-4.

The 11QPA4B card interworks with 12P120, 20AX200, 30AN300, and 10ANY10 with ODUk protection.

The SNCP with 11QPA4B supports 10GbE LAN client signal protection, with OTU2eNimEth on the line side.

Figure 4-66 11QPA4B - Optical Model with OTU2eNimEth



Important! Creating the OPS Physical connection, the Client Signal type in the Specific Information panel, must be set as **ClientSignalType_otu2eNimEth**.

Network Scenario Example

Figure 4-67, “11QPA4B - Block Diagram” (p. 498) and Figure 4-68, “11QPA4B - Optical Model - SNCP protection on ODU2e” (p. 499) illustrates an example of network scenario with 11QPA4B card. The SNCP protection is performed at ODU2e level.

Figure 4-67 11QPA4B - Block Diagram

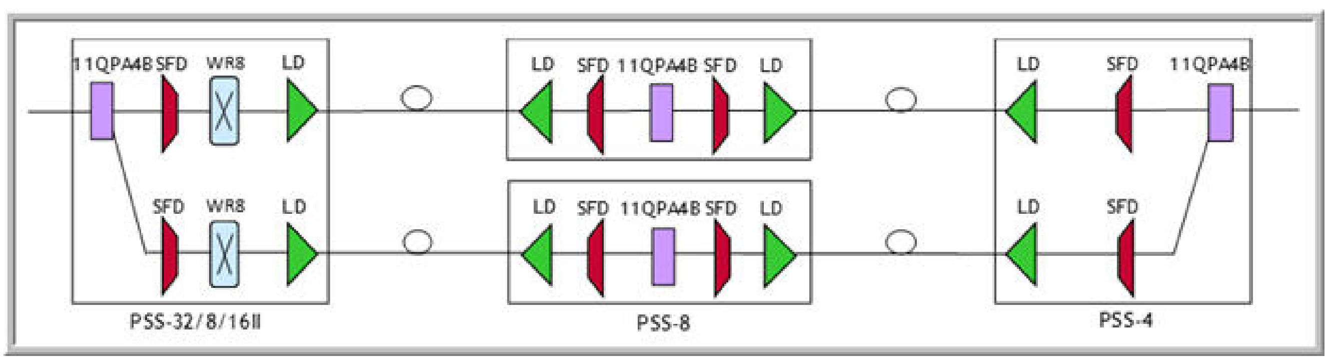
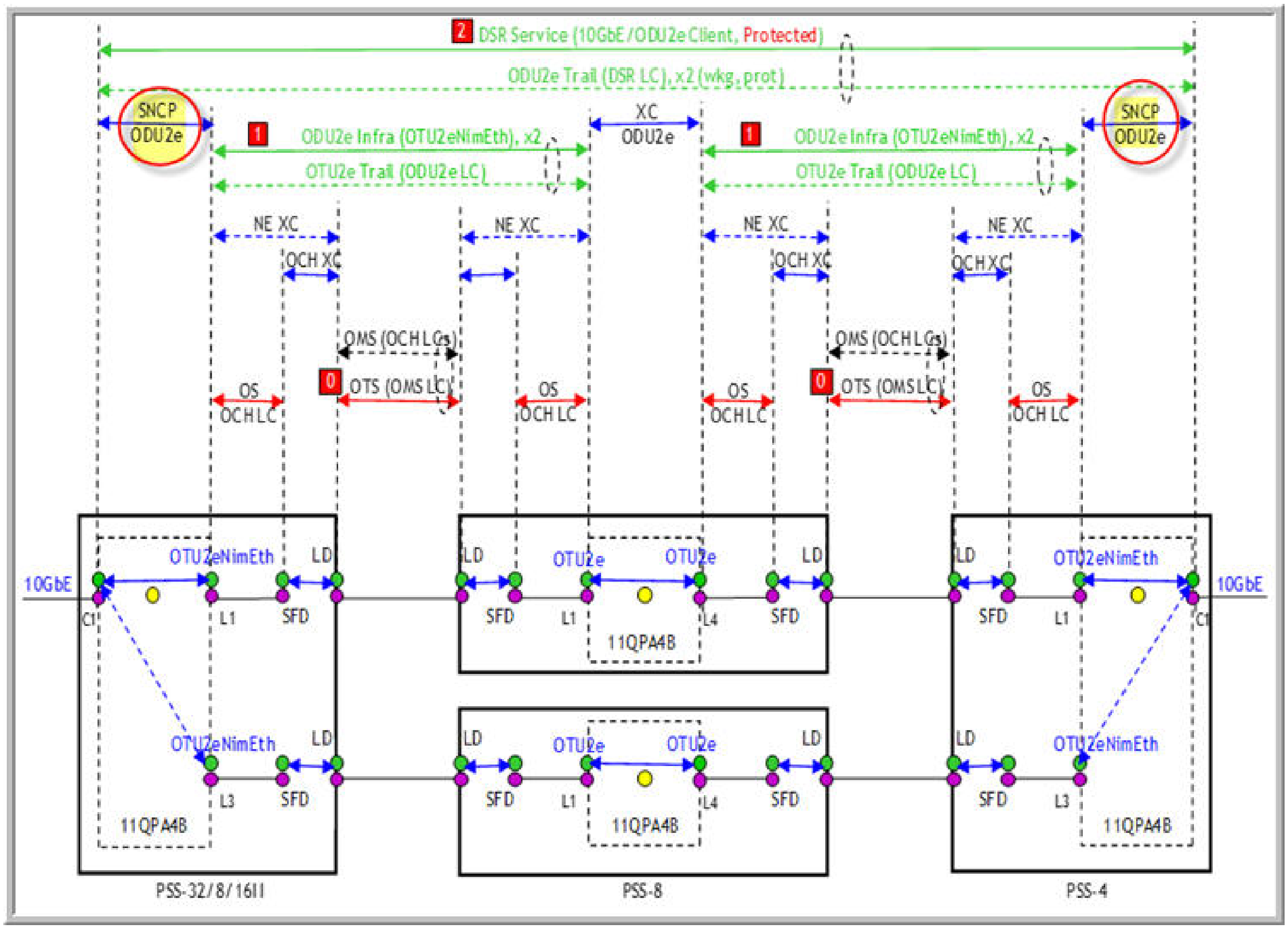


Figure 4-68 11QPA4B - Optical Model - SNCP protection on ODU2e



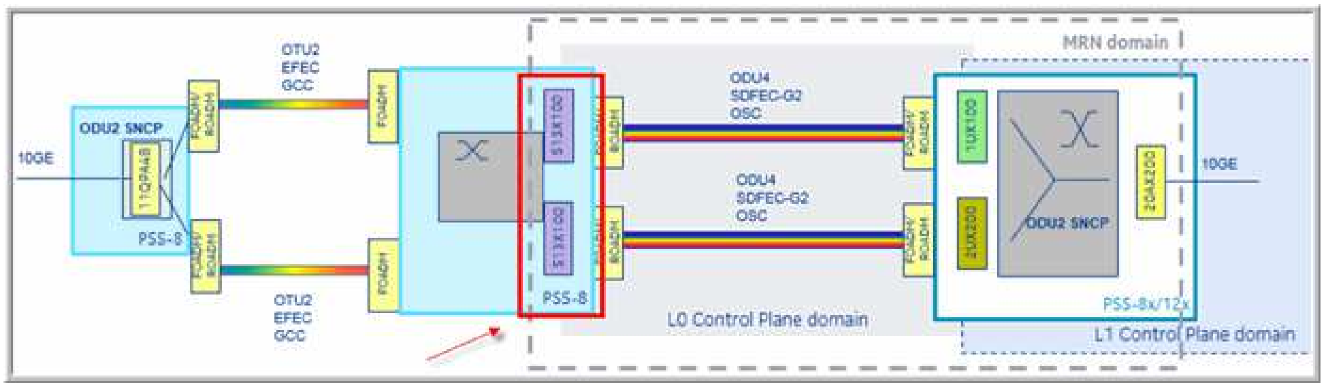
Behavior :

1. ODU2e Infrastructure: **OTU2eNimEth** is set on 11QPA4B line ports on both A and Z nodes, on working and protection line.
2. DSR Service: client rate is 10GbE with ODURate or ODU container of ODU2e, and ODU2e SNCP provisioned on the A and Z nodes.

ODUj SNCP Protection provisioning guidelines for mate configurations

In an SNCP scenario when same card is used for mating on same shelf, for example, four S13X100 cards are used for two different protected services, manual routing must be used for service creation.

Figure 4-69 ODUj SNCP Protection - Example with mate cards



1+1 ODUj SNC/N protection with 1830 PSS-nX

The 1830 PSS-8x, 1830 PSS-12x and 1830 PSS-24x support the bidirectional switching for 1+1 ODUk SNCP (ITU-T G.873.1).

Bidirectional switching means that the selectors at both ends of the protected domain always select the same transport entity. To achieve this target, the coordination between both ends is required is achieved using the priority based APS protocol.

The 1830 PSS-8x, 1830 PSS-12x, and 1830 PSS-24x support the ODUj SNC/N unidirectional and bidirectional protection switch with APS protocol.

The bidirectional switching protection is supported with 1830 PSS-8x from R11.1, 1830 PSS-12x from R11.1 and 1830 PSS- 24x from R10.1.

With 12P120 and FC1200 cards only ODU2e rate must be selected.

1+1 ODUj SNC/N Protection provisioning guidelines with 1830 PSS-nX

The network switching mode must be selected during the Service provisioning from the template, in the SNC protection panel. See “SNC Protection” (p. 717).

The type of protection is showed following the path **OPERATE > Service**, selecting a Service involved in the protection and selecting the **Protection** tab.

1+1 ODUj SNC/Nc protection interworking with SDH NEs

NFM-T supports the 1+1 ODUj SNC/Nc protection to interwork with SDH NEs. SNC/Nc protection is performed with the following shelves: 1830 PSS-24x,1830 PSS-8, and 1830 PSS-16II.

SNC/Nc protection is feasible by configuring the shelves as follows: 1830 PSS-24x supplied with 30AN300 card, 1830 PSS-8 and 1830 PSS-16II with 20P200 and 1UD200 cards.

The same feature is available in NFM-T also with 1830 PSS-36 and 1830 PSS-64 NE configurations.

The following diagrams provide an example of how the shelves are configured and the traffic rerouting in case of failure.