

Figure 4-70 SNC/Nc protection on 1830 PSS-24x to interwork with SDH NEs

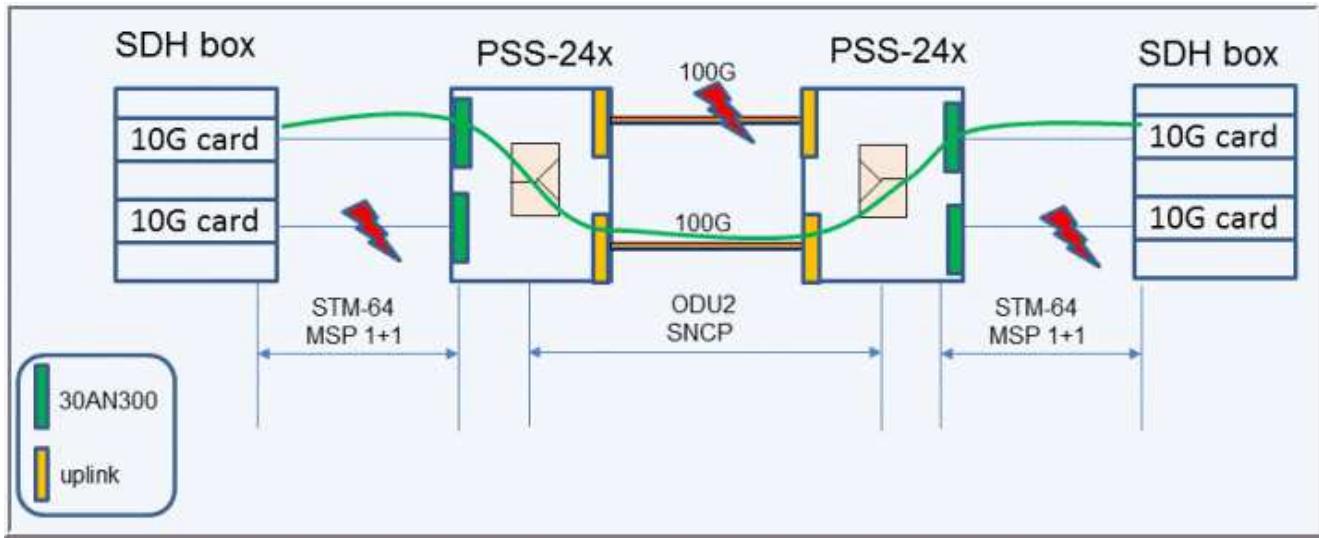
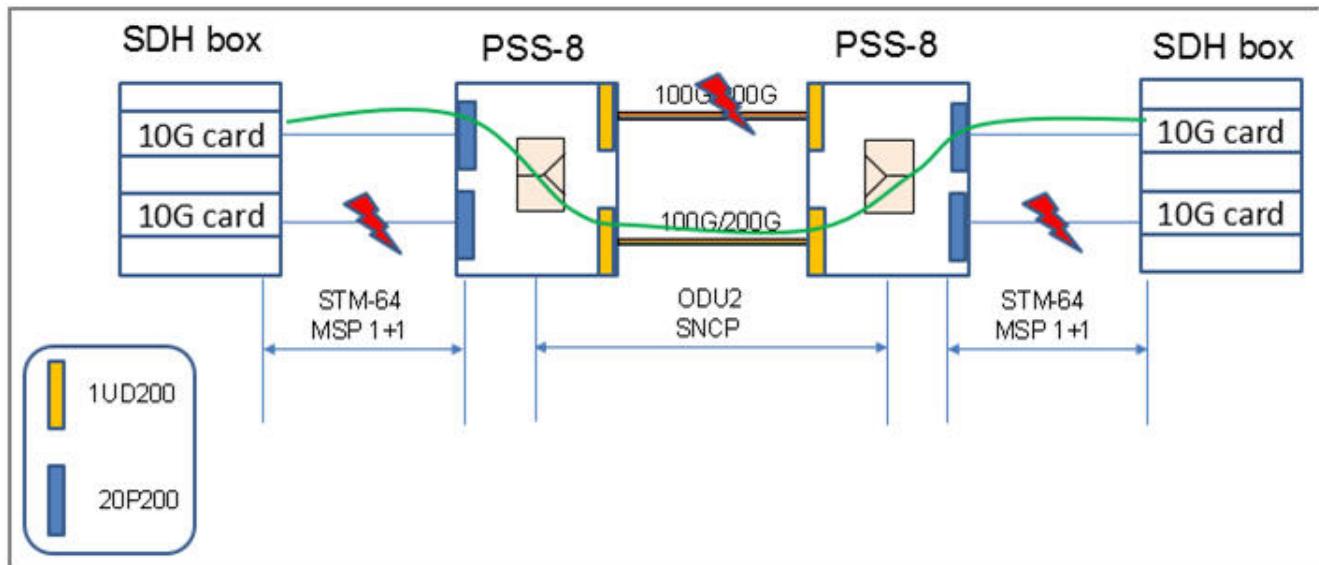


Figure 4-71 SNC/Nc protection on 1830 PSS-8 to interwork with SDH NEs



If the SDH NE is not managed by NFM-T, the service is terminating on the two SDH client ports on 1830 PSS-24x, 1830 PSS-8, and 1830 PSS-16II shelves.

SNC/Nc protection is supported only for Managed Plane.

1+1 ODUj SNC/Nc Protection provisioning guidelines to create a service

Select a template from the **Service/Infrastructure Templates** deploy window to create a Service. From the NFM-T GUI, navigate to **DEPLOY > New Service/Infrastructure Connection** to display the list of templates.

For STM-N, select the **STM-N with external 1+1 MSP Protection** template and click **Deploy**  to create a service.

For OC-N, select the **OC-N with external 1+1 APS Protection** template and click **Deploy**  to create a service.

Select the following to create the service:

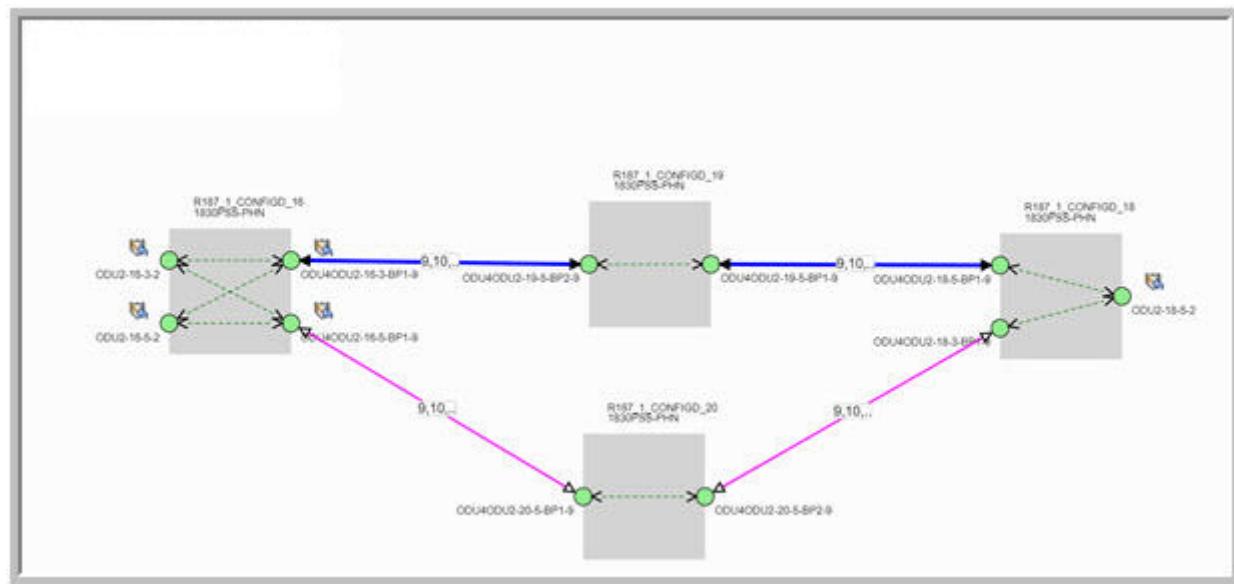
- **Service Rate:** STM-64 (STM-N), or OC-192 (for OC-N)
- Select **Protection** check box.
- **Connection Type:** 3 Ended A Bi (Y), 3 Ended Z Bi (Y), 4 Ended Bi (X), 2 Ended Bi (I), 2 Ended Split Bi (I), or 1-N Broadcast Uni

Set **Client Protection Type** as **SNC-Nc** in the **PARAMETERS > PROTECTION** tab.

Set **Network Protection Type** as **SNC-N**.

The details of the new created service, can be viewed in the *Service* list or through the *Routing Display*. [Figure 4-72, “SNC/Nc 3 Ended protection - Routing Display” \(p. 501\)](#) illustrates an example of 3 Ended SNC/Nc protection.

Figure 4-72 SNC/Nc 3 Ended protection - Routing Display



Configuration rule for 1830 PSS-8 and 1830 PSS-16II

Slot rule need to be followed while creating a SNC-Nc 3 Ended and 4 Ended STM64/OC-192 service connection.

The following is an example of slot configuration supported:

- 3-20P200
- 4-1UD200
- 5-20P2004
- 6-1UD200

The following configuration is *not* supported:

- 3-1UD200
- 4-20P2004
- 5-20P2004
- 6-1UD200

ILKN mode must be set from the EQM in BP2 port of both 20P200 card.

SNCP protection types for Connections

An ODU2e/ODUk/ODUj connection with SNCP Protection can have Control Plane SNCP protection, Managed Plane SNCP network protection, managed plane client SNCP protection or a combination of these types.

When a connection has more than one type of SNCP protection the value displayed in the Protection Type field shall use following precedence:

- Control Plane SNCP Type
- Managed Plane Network SNCP Type
- Managed Plane Client SNCP Type

Guidelines for network protection type value

For Control Plane SNCP protection the value of Protection Type is **SNCP-N**. For Managed Plane network SNCP Protection the value of Protection Type is the Network Protection Type, for example SNC-N, SNC-I, and so on. When a card does not support setting the Network Protection Type the value **SNCP** is equal to the protection type.

For Client SNCP Protection the value of Protection Type is the value of Client Protection Type, for example SNC-N, SNC-Nc, and so on.

There are some cards that let the user choose the type of SNCP protection, for example SNC-N, SNC-I, while for other cards this value cannot be selected by the user. If both the A End and Z End protection groups are on cards where the value cannot be selected by the user, the system does not have a value for Network Protection Type and for these cases the system shows **SNCP** as the protection type.

This occurs only for certain cards on the 1830 PSS-PHN NEs. For 1830 PSS-OCS NEs the Network Protection Type is always set. The user can check the Protection tab and see if there is a value for Network Protection Type. If there is a value for this field it must be the same as the value on the Connection List.

The table below displays the protection values displayed for connections and services.

Table 4-8 Protection Expected Values

Protection Expected Values				
	Full BW (eg 100GB)	Lower BW (eg 10GB/1GB)		
	Managed Plane	L0 Control Plane	Managed Plane	L0 Control Plane
OTUK	OCHP	OCHP	OCHP	OCHP
ODUk LL	OCHP Server Protected	OCHP Server Protected	OCHP Server Protected	OCHP Server Protected
ODU4 Infra (# Term)	(NA)	(NA)	OCHP Server Protected	OCHP Server Protected
ODUj	Unprotected	Unprotected	Unprotected	Unprotected
DSR	Unprotected	Unprotected	Unprotected	Unprotected

4.9 Electrical Subnetwork Connection Protection (E-SNCP)

Electrical Subnetwork Connection Protection definition

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.

The 11DPE12/11DPE12E/11DPE12A can have up to 100 Virtual Time Slots (VTS) for each line port. Ethernet Virtual Private Line (EVPL) services are transported over the 10G line structure with 100 designated VTS.

For 11DPE12, only VTS 1-32 can be used for E-SNCP and the 32 E-SNCP groups meet the sub-50 ms protection switching time. For 11DPE12E/11DPE12A, VTS 1-100 can be used for E-SNCP but only 32 E-SNCP groups meet the sub-50 ms protection switching time, when the E-SNCP groups are larger than 32, the protection switching time may be larger than 50 ms.

It also provides 1+1 dedicated, sub-50 ms, E-SNCP protection for EVPL services by using out-of-band channel for status and protection signaling. Automatic Protection Switching (APS) channel communication is established by using APS/PCC channel in ODU2 overhead of 10G line port, thus not reducing client signal bandwidth.

Each 4DPA4 OTU1 is divided into 16 proprietary Virtual Time Slots (VTS). Services are transported over the 2.7 Gb line structure with the designated VTS depending on the bandwidth requirement of the service.

It also provides 1+1 dedicated, sub-50 ms, E-SNCP protection for services by using out-of-band channel for status and protection signaling. An APS channel communication is established by using APS/PCC channel in ODU1 overhead of line port, thus not reducing client signal bandwidth.

11DPE12 supports two types of E-SNCP through backplane connection:

- A client service protection with one-client port bridged to and selected from the other two-line ports, which locate at a same OT or two adjacent OTs.
- A line service protection with one-line port bridged to and selected from the other two-line ports, which locate at two adjacent OTs or a same OT.

1830 PSS-4 also supports provisioning of GbE protection switching modes: for example, unidirectional switching, revertive/non-revertive switching.

Unidirectional switching

A switching mode in which the selection decision for the service path is made independent of the far-end node switch state. The APS channel is not used to coordinate switching activity between the nodes.

Bidirectional switching

A switching mode in which a channel is switched to the protection path in both directions. Switching of only one direction is not allowed. Head-end to tail-end signaling is accomplished using the APS channel.

Non-revertive switching

A switching mode in which a switch of service to the protection entity is maintained even after the working entity has recovered from the failure or the manual command to protection that caused the switch is cleared.

Revertive switching

In revertive switching mode, the traffic is automatically switched back to the working line when the working line has recovered from the failure or the user command is cleared. In the failure-recovery case, the switch back to working is delayed until working has been continuously good for the number of minutes specified by the wait-to-restore (WTR) parameter. In case of clearing a user switch command, there is no delay.

Both revertive and non-revertive switching can be used in unidirectional protection groups. Both revertive and non-revertive switching can be used in bidirectional protection groups.

i **Note:** 11DPE12 E-SNCP supports unidirectional switching in both revertive/non-revertive modes. Y-cable protection supports both bidirectional and unidirectional switching, in revertive/non-revertive modes. 4DPA4 E-SNCP supports unidirectional switching in non-revertive mode.

4.10 OPS protection

OPS protection definition

For OPS protection of optical channels, the OPS is placed at the Optical Channel (OC) layer, between the Optical Multiplexing layer and the Optical Channel to Optical Signal (OC/OS) adaptation, (that is, the OT function).

The OPS supports two types of protected line configurations. 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).

- Internal OT, no SVACs - The OT line port is connected to the OPS SIG port. The OPS A port and B port are connected to two different lines, either using SFD filter ports, or using CWR8 colorless ports.
- Alien/External OT, redundant SVACs - The alien OT is connected to the OPS SIG port. The OPS A port and B port are connected to two different SVACs. The two SVACs are connected to two different lines, either via SFD filter ports, or via CWR8 colorless ports.

i **Note:** OPS protection can be used with two MVACs. For this type of protection an OPS card is placed on the client-side optical path of the MVACs. Protection is provided against both fiber cuts and MVAC failure.

OPS protection can be used with any supported type of OT (130SCX10, 130SNX10, 112SCA1, 112SNA1, 112SCX10, 112SNX10, 11QPA4, 11QPEN4, 11STAR1, 11STAR1A, 11STGE12, 11STMM10, 12P120, 260SCX2, MVAC, MVACF, MVAC8B, SVAC). There is no restriction on physical location within the NE of the associated OT, OPSA, SFD, CWR, or SVAC cards. The cards can all be in different shelves if desired. For cards in the same shelf, there is no requirement for physical adjacency. In the receive direction (selector function), the two SFD/CWR ports connected to the OPS A and B ports can have different frequencies. In the transmit direction (splitter function), the two SFD/CWR ports must have the same frequency.

Protection groups

The NE supports the definition of an OPS protection group. This logical object is the basis for automatic and manual protection switching operations and notifications. An OPS protection group represents the protection association between the two line-side ports (A and B) of a single OPSA card. Protection switching is performed only within an established protection group. When there is no protection group, no protection switching occurs, either manual or automatic. The user is free to specify either of the line-side ports (A or B) as the working port, and the other port as the protection port.

i **Note:** For OPS protection group creation, ports A and B cannot be in-service. They must be down or in maintenance state (mt). The default OPS port state is down.

In a Managed Plane setup with OCHP, it is not possible to use the protection groups that are created from NE. If protection group already exists from NE, remove the protection group before creating a connection. The protection group is created by the system on connection creation and is removed after the connection is deleted.

Unidirectional switching

OPS protection groups support only unidirectional protection switching. In unidirectional protection switching, each end of an optical channel operates independently of the other. A failure affecting only one direction of transmission will cause a protection switch of only that direction. The unaffected direction of transmission is not switched. OPS protection groups do not use any end-to-end APS protocol. All switch requests are local. The two ends have no knowledge of each other.

Non-revertive switching

OPS protection groups support only non-revertive protection switching. There is no automatic switch from protection back to working because of a recovery of working, or because a user switch to protection is cleared.

Client Side OPS protection

In the Client Side OPS protection configuration, two OTs are used. Protection is provided against a line failure (such as fiber cut or LD failure), OT failure and shelf power failure. The OPSB board with non-latching switch is used for Client Side OPS protection. The following applies:

- The OPSB board is only used in Client Side OPS Protection (OTUP: Optical Translator Unit Protection). The user cannot provision the protection mode type.
- Only the OPSB board can be used as OPS type board in the Client Side OPS Protection configuration.
- The Client Side OPS Protection is supported on TOADM, ROADM, and FOADM nodes. The OPS type board is positioned between unprotected client equipment and OT client side port.

The OT's supported in the Client Side OPS Protection include:

- 11DPM8
- 11QPA4
- 11STAR1
- 1STMM10
- MVAC

i **Note:** OPSB protection is supported on 11DPM8 client ports with below configurations:

- HOLDOFFTIMER: disabled
- LOSPROP: Laser-off

The working and protection OT combinations supported in the Client Side OPS Protection include:

- 11QPA4 with 11QPA4
- 11QPA4 with 11STAR1
- 11QPA4 with 11STAR1A
- 11STAR1 with 11STAR1
- 11STAR1A with 11STAR1
- 11STAR1A with 11STAR1A

-
- 11STMM10 with 11STMM10
 - 112SCA1 with 112SCA1
 - 112SNA1 with 112SNA1
 - 260SCX2 with 260SCX2

OPSA protection definition

Optical Protection Switch Advanced (OPSA) is a type of enhanced network protection provided by the OPSA board that supports server-side OPS protection. OPSA provides 1+1 OCH, OMSP, or OLP protection over DWDM lines.

OPSA protection provisioning guidelines

When you are using OPSA you need an explicit configuration on the first amplifiers internally connected to OPSA/A and OPSA/B ports.

Enabling **Planned for Add/Drop OPS protection** on the LD is a prerequisite for L0 OPSA provisioning.

This parameter can be enabled from:

- EPT, see [11.3 “Network planning using EPT” \(p. 1599\)](#).
- Equipment Manager application, select the LD link in the list on EQM and click the **Details** tab, see Configure Links and Ports. See the chapter Equipment Manager (EQM) in *NE Management Guide*.
- CLI for the NE/Node, use the command : `config ason amplifier adopsplanned 16/14 yes`.

After this operation proceed with the provisioning of the connection.

OPSA protection with Multiple Variable Attenuator Card 8 (MVAC8)

NFM-T can manage the provisioning, with manual routing only, of an end-to-end service with alien channel implemented in a network scenario, described in the [Figure 4-73, “OPSA with MVAC8 scenario” \(p. 510\)](#), which refers to 1830 PSS-36, 1830 PSS-64 uplinks, MVAC8B and OPSA protection.

It is Managed Plane only.

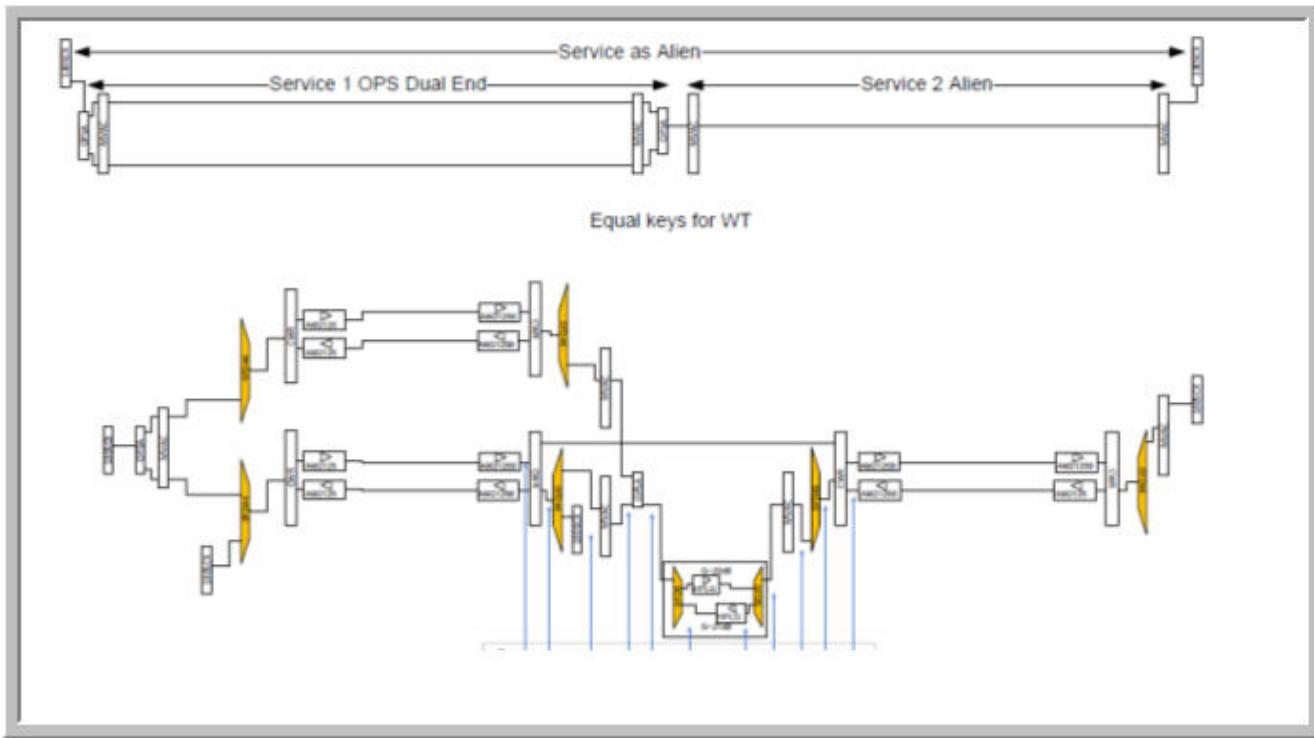
MVAC card is for wave key support of an alien wavelength.

An *Alien Channel*, or *Alien Wavelength*, represents an optical signal originated from equipment not under the direct control of the 1830 PSS network being external to this network.

This means that MVAC inserts wave keys when an Alien Channel comes into the 1830 PSS network, and strip off wave key when it leaves the 1830 PSS network.

The OPSA with MVAC8 scenario is represented in the [Figure 4-73, “OPSA with MVAC8 scenario” \(p. 510\)](#).

Figure 4-73 OPSA with MVAC8 scenario



The service/L0 ODU-k between two OCS nodes is transported over a HO ODU terminated on OCS uplinks that is passing through OPSA and MVAC8B on OPSA line side.

OPSA protection is closed on a SFD/MUX, due to the constraint of a single fiber available in the last part of the channel route.

The service connection provisioning is carried out at nodal level, then discovered by NFM-T.

This scenario, is validated with the following parameters:

- **NE Types/Releases:**
NFM-T 22.6_FP1
NFM-T 22.6_FP1
- **Shelf Types:**
1830 PSS-PHN: 1830 PSS-32, 1830 PSS-16, 1830 PSS-8, 1830 PSS-16II shelves
1830 PSS-OCS: 1830 PSS-36, 1830 PSS-64 shelves (transparent)
- **Card Types:**
OPSA (for OCH protection)
MVAC8B
130SCX10 (as alien wavelength)
- **Configurations:**

Managed Plane: required
L0 and L1 Control Plane: not required

OPSA protection with OTS Connections

When creating or deleting OTS connections for OPS cards, ensure that OPSA ports are in **Out of Service** state before the internal TL creation between OPSA and LD is completed. Otherwise an error occurs for the operation.

If the ports are not in **Out of Service** state, modify the state. See *Equipment Management* section of the NFM-T NE Management Guide for details on the operation on the cards.

After the creation of OTS connections, put the ports back to **InService** state.

OPSFlex protection definition

The OPSFlex card acts as the OPSA, is an OCH optical channel protection card. OPSFlex is capable of supporting the protection of OCH channel with Flex grid. It supports colored and colorless Add/Drop channel protection, for C-band only channels. OPSFlex needs to work with wavekey enabled OT line signals only.

OPSFlex is supported for CDC-F photonic, C-F, IROADM, Any Direction (D' and D") architectures.



Note: For 1830 PSS NE R12.0, topology creation between OPSFlex A/B port to IROADM9R ADT port is not supported.

Cluster and non-cluster configurations are supported in OPSFlex. For example 1830 PSS-32 and 1830 PSS-24x cluster configuration (OPSFlex on one NE and OT card on the other NE) with OPSFlex is supported.

PSI-8L is supported in cluster configuration (cluster tributary nodes and OPS) with OPSFlex for 1830 PSS R13.0.4 onwards for L0 Control Plane.

For connection creation, from the NFM-T GUI, navigate to **DEPLOY > New Service/Infrastructure Connection** and select the dedicated **OCH** template from the **Service/Infrastructure Templates** window. See “[Deploy a new service or infrastructure connection with template](#)” (p. 1216).

Cards interworking with OPSFlex card on Managed Plane:

- 2UC400
- S13X100E
- S13X100R
- D5X500
- D5X500Q
- 4UC400
- MCS ports
- PSC1-6 ports
- S2AD200R
- S2AD200H
- 2UX200

-
- 1UX100
 - 130SCUPH

Cards interworking with OPSFlex card on L0 GMPLS Control Plane:

- D5X500
- D5X500Q
- S13X100R
- S13X100E
- MCS ports
- PSC1-6 ports
- S2AD200H

i **Note:** For Control Plane connections, ensure that the user does not provision OPSFlex in colored configurations, as NFM-T does not support OPSFlex for colored configurations in control plane connections.

The OPSFlex protection supports the Signal Degrade (SD) as switching parameter for the following cards:

- D5X500
- D5X500Q
- S13X100E
- S13X100R
- S2AD200R
- S2AD2100H

The SD parameter is not supported by D5X500Q Half/HalfX5 card.

The OPSFlex with SD is supported in Managed Plane and L0 GMPLS network. The SD parameter is not applicable for CP connections.

The SD value is set during the connection creation in the *Transmission Parameter* panel. Additional details on Transmission Parameter panel are given on “[Transmission Parameters](#)” (p. 711).

Select the **More Parameters** button to access the **Modify Transmission Parameters** window.

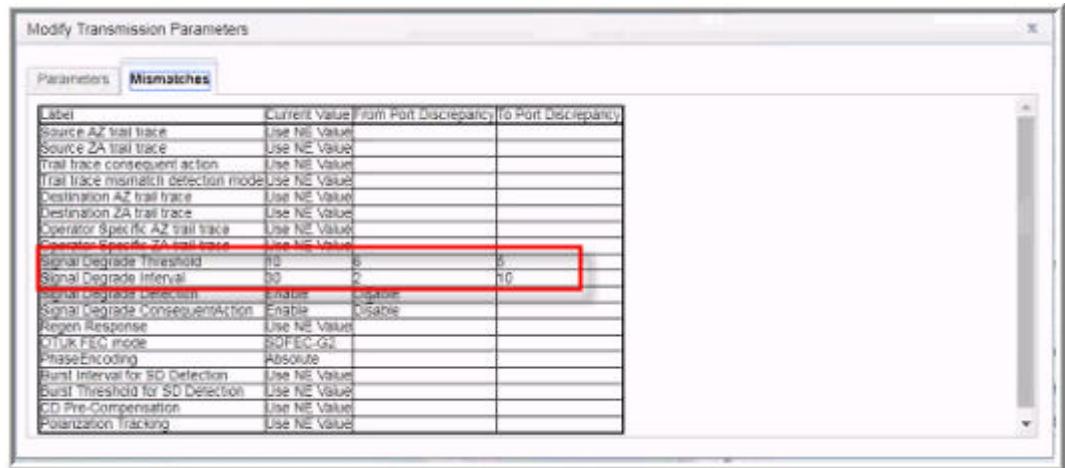
The following fields must be completed:

- **Signal Degrade Threshold.** The range changes according to the card and rate:
 - from 1 to 20000 for S13X100E and S13X100R cards.
 - from 1 to 20000 for D5X500 and D5X500Q cards, with OTU4 rate.
 - from 1 to 10000 for D5X500 and D5X500Q cards, with OTU4x2 rate.
- **Signal Degrade Interval:** enter the appropriate value, possible values are in the range from 1 to 20.
- **Signal Degrade Detection:** from the drop-down list, select **Enable**
- **Signal Degrade Consequent Action:** from the drop-down list, select **Enable**.

Note: When the SD parameters of an end point (A-Z) of the connection are modified via EQM with values different from those set in the *Modify Transmission Parameters* window, a misalignment is highlighted.

The misalignment is displayed in the **Mismatch** tab in the **Modify Transmission Parameters** window that shows the values entered or in the *Network Inconsistencies* window by selecting the **Parameter Mismatches** tab.

Figure 4-74 More Parameters - Modify Transmission Parameters - Mismatches Tab



i Note: OPSA/OPSFlex protection for L0 connections are not supported by NFM-T and NE for configuration involving OPS between OT and OPSA/OPSFlex that are in dangling configuration (external).

NFM-T extends OPSA protection on S13X100R, S13X100E, and S2AD200H for L0 GMPLS configuration in 1830 PSS D/D" configurations.

OPSFlex protection for coherent optimized ROADM with S4X400H

NFM-T extends OPSFlex (line side for OTSi) protection support to OTSig tunnel with S4X400H for Managed Plane and L0 Control Plane configurations. This configuration is supported for 1830 PSS NE (1830 PSS-8, 1830 PSS-16II, and 1830 PSS-32 shelves).

S4X400H supports OPSFlex protected tunnels with 3R in L0 GMPLS and Managed Plane.

As a part of the OPSFlex tunnel creation, two OTSig trails are created automatically and are listed under the **360 ° View > Server** tab of the connection. Protection switch is applicable at OTSig tunnel and not at the OTSig trail. For L0 GMPLS OPSFlex Protected OTSig Tunnel, protection switch is supported from **SNCP** page from **ASON > SNCs**.

OTSig tunnel creation is not supported on fixed grid networks.

i Note:

- The OPSFlex protection is supported with **Provisionable Wave Key** as Keyed only.

- Polarization Tracking is a read-only parameter for modify operation. Polarization tracking value cannot be modified from the connection modification window.
- Link Span is a modifiable parameter at the OTSig trail level.
- Cluster configurations are not supported for OCH Protected OTSig tunnel over L0 CP network.

For more details, see *OPSFlex Protection with S4X400H* and *OPSFlex + 3R Protection with S4X400H* in the *S4X400H* section of the *NE Management Guide*.

OPSFlex protection with 3R Connections

In this scenario, OPSFlex with 3R, ODUk [Non-ADD4] / OTSig Tunnel [ADD4] have multiple OTUk [Non-ADD4] / OTSig Trail [ADD4] servers. The transmission parameters modification must be done on all OTUk/OTSig Trails to have consistent behavior across the OTUk/OTSig Trail.

For 3R connections, ensure to modify transmission parameters for all OTUk/OTSig Trail connections belonging to 3R, to avoid parameter mismatch at **Network Inconsistencies**.

Example: Suppose the user has created a Logical Link with S13X100 card with 3R. At **Servers** tab, this connection has three OTU4 connections, for example, OTU4#1, OTU4#2, OTU4#10. When the user modifies SD parameters for OTU4#1, then the other connections OTU4#10 and OTU4#2 are listed in the **Parameter Mismatch** tab. To avoid this behavior the user must update SD parameters for the three OTU4 connections belonging to 3R.

OPSFlex supports symmetric and asymmetric configurations between two cards of the same type with or without 3R in the middle. For the middle NE with 3R Regen, Regen Response parameter must be enabled.

OPSUM (Optical Protection Switch Universal Multi Carrier)

OPSUM is a single-slot card deployed on 1830 PSS-8, 1830 PSS-16II, 1830 PSS-32, 1830 PSI-M and 1830 PSI-8L shelves. It provides OCH and Line Side Protection for coherent OT's, when operating in Colorless ROADM using broadband drop ports (Excluding FOADM/TOADM configurations). Overall protection switch time less than 50 ms.

OPSUM eliminates the requirement of Protection Switching Tone (PST) and Wavelength Tracker (WT) by utilizing the tunable filter taps to switch based on LOS. It supports both keyed and unkeyed services (NE R14.0 onwards).

The following cards are supported:

- 2UX500 (Managed Plane only)
- 4UC1T (Managed Plane only)
- S5AD400H (Managed Plane and Control Plane)
- S6AD600H (Managed Plane and Control Plane)
- SFM6 (Managed Plane only)

Defined supported Optical Transponders require no support for cluster connectivity, GMRE currently does not support FA-TERM OPS Protected services which terminate on a Cluster NE. When additional OT support is added for older OTU based OT's, cluster support may be required.

OPSUM supports Optical switching protection for up to four Optical Transponders.

4X Port groups (each group has Signal (Sig), Port A, and Port B inputs)

- A1, B1, and Sig1
- A2, B2, and Sig2
- A3, B3, and Sig3
- A4, B4, and Sig4

OPSUM has a tunable optical channel monitor for a configured service. OCM monitors the incoming optical signal on both legs for LOS and uses the LOS detection as a trigger for optical switching.

Following are OCH protections using the OPSUM card (at same level of OPSA/OPSflex):

- OCH and Line Side Optical Protection Switching for coherent OT's
- Supports the C-Band optical frequency band
- Tunable Filter Optical Channel Monitor (OCM) for LOS detection
- OCHP on the OPSUM pack depends on the detection of channel LOS below -25.0 dBm
- Traffic impact on the protection switch is below 50 ms
- Uni-directional switching

OPSUM Configuration	Protection Attributes
1+1 OCHP Group Single Carrier	<ul style="list-style-type: none">• 1+1 OCHP for a single optical carrier• Supports up to four individual OCHP protection groups<ul style="list-style-type: none">- non-revertive switch operation- revertive switch operation• Provisionable <i>Wait to Restore</i> timer in the range between 1 to 20 minutes (default value is 5 minutes)• Automatic switching in response to signal failure• Supports Standard User switching commands

OPSUM card supported Nodal configurations:

CDC-F 2.0 configurations

- CDC-F 2.0 with IRDM20/20-LP/32/32LP + MSH4-FSB + AAR + MCS8-16
- CDC-F 2.0 with IRDM20/20-LP/32/32LP + MSH4-FSB + AAR + MCS1615
- CDC-F 2.0 with IRDM20/20-LP/32/32LP + MSH4-FSB + MXN824 + ASC4

C-F configurations

- C-F IRDM32 C band, C-L with OMDCL
- C-F IRDM20
 - C-F with IRDM20/20-LP/32/32LP MLFSB + PSC1-6
 - C-F with IRDM20/20-LP/32/32LP MLFSB

C-F with IRDM20/20-LP/32/32LP MSH4-FSB + MLFSB

- C-F IR9
 - IRDM20/32 based configuration
- PSC1-6
MLFSB

Mixed grid or fixed grid Add/Drop

- IR9
 - IR9/IR9LP with SFD44/B (ITL optional)
 - IR9/IR9LP with PSC1-6
 - IR9/IR9LP ADT port (direct OT to ADT Port connectivity not currently supported by GMRE)
- IROADM9R
 - IROADM9R/IROADM9R-LP/IR9/IR9LP with SFD44/B (ITL optional)
 - IROADM9R/IROADM9R-LP/IR9/IR9LP with PSC1-6
 - IROADM9R ADT port (direct OT to ADT Port connectivity not currently supported by GMRE)



Note: For ADD4 cards, nodal configuration restrictions are applicable. See the respective NE documentation, for further Information.

5 Features

5.1 Overview

Purpose

This chapter provides the steps required to manage system features. The basic provisioning of the system is explained in the dedicated parts of this manual.

Contents

5.1 Overview	517
NFM-T Frequency bands management	518
5.2 Frequency bands overview	518
5.3 C+L band	519
5.4 Frequency bands visualization	527
5.5 L-band management in ASON	531
5.6 End to End Service C-band and L-band Interworking in L0 Control Plane	535
5.7 33.75 GHz and 70 GHz central frequency granularity for subsea application	537
5.8 Flex Grid technology	545
5.9 37.5 GHz Frequency Band Management	551
Optical Fiber	560
5.10 Transmission over fiber	560
5.11 Optical Line Protection (OLP)	563
5.12 OTS fiber characteristics limitations	564
5.13 Single fiber scenario with single OPS	573
5.14 Single Fiber on S4X400	574
5.15 bi-directional 3R Support for Control Plane Without Re-fibering	578
Additional features	582
5.16 Additional features	582

NFM-T Frequency bands management

5.2 Frequency bands overview

Introduction

In case of optical data communication, there are different frequency bands which are suitable for transmission of signals, providing a large number of different channels in the wavelength range from 1260 nm to 1675 nm.

The different channels are:

- **Original (O-band):** 1260-1360 nm
- **Extended (E-band):** 1360-1460 nm
- **Short Wavelength (S-band):** 1460-1530 nm
- **Conventional (C-band):** 1530-1565 nm
- **Long Wavelength (L-band):** 1565-1625 nm
- **Ultralong Wavelength (U-band):** 1625-1675 nm

Traditional DWDM systems used 44 channels with a channel spacing of 100 GHz from channel to channel or 88 channels with a channel spacing of 50 GHz from channel to channel. The latter is used in DWDM applications, since dual number of channels is available. In both ways, primarily C-band or L-band are used.

ITU-T has established a set of standards for telecommunications that drives all WDM optical systems. In particular, ITU-T G.694.1 recommendation specifies a frequency grid for DWDM applications. The frequency grid, anchored to 193.1 THz, supports a variety of channel spacing of 12.5 GHz, 25 GHz, 50 GHz and 100 GHz. Explanations on the *Flex grid* technology are found in section [5.8 “Flex Grid technology” \(p. 545\)](#).

This chapter provides information on **C-band**, **L-band**, and **C+L band** which are the bands employed in the OTN networks managed by NFM-T.

5.3 C+L band

Introduction

The 1830 PSS C+L optical architecture is for a DWDM NE with a very high channel count to allow extremely high capacity on a single DWDM fiber pair. This is achieved by permitting optical channels occupying both C-band and L-band frequencies. The total number of optical channels are doubled, when compared with C-band only. The following figure shows a high-level functional drawing of C+L band.

Figure 5-1 C+L Band optical architecture support



The following pairs of frequency bands are supported in the C+L band optical channel configuration:

- **C-band:** frequency range [191.275 THz - 196.075 THz], with a center frequency on grid of 6.26 GHz
- **L-band:** frequency range [186.075 THz - 190.875 THz], with a center frequency on grid of 6.26 GHz

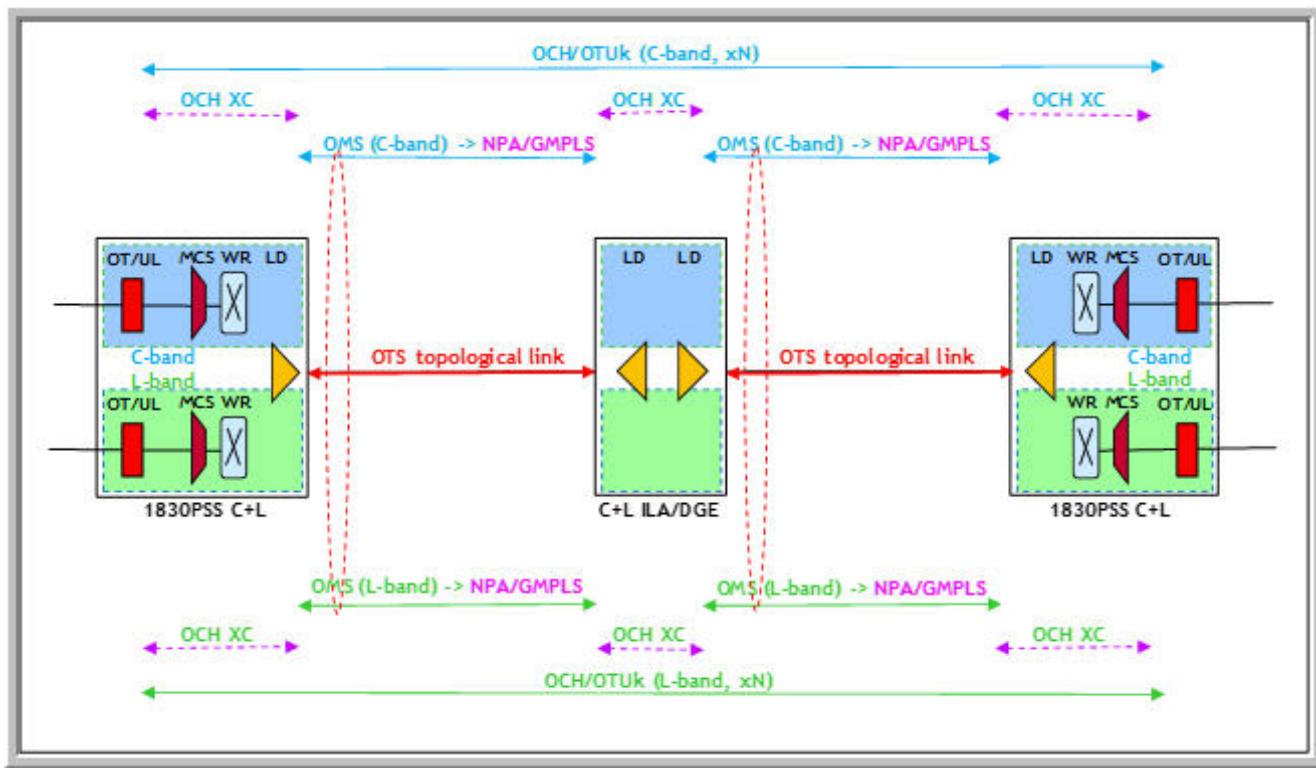
C+L band supports the following node configurations:

- CDC-F ROADM
- CDC-F ILA
- CDC-F DGE
- C-F ROADM Optical Model

Only the C+L band or L-band is a greenfield application, or a C-band network expanding to L-band to extend link capacity. In the latter case, the 1830 PSS C+L is largely a re-use of the existing CDC-F system, with necessary changes (including new LD packs and so on). The L-band hardware is of the same kind as CDC-F design, and with the L-band support.

NFM-T supports the same optical model used for CDC-F also in C+L configuration. In the C-band configuration, a single OMS trail is used for routing purpose. In the C+L configuration, a single OTS TE / topological link contains two OMS trails for routing, one for the C-band and the other for the L-band. The NFM-T optical model for C+L shows one OTS topological link with two OMS trails.

Figure 5-2 C+L band optical model



As for C-band and L-band configurations, C+L band supports both fixed grid and flexgrid channels as well.

1830 PSS C+L support

The following table shows the configuration supported by 1830 PSS, according to the type of bands and NFM-T release.

Table 5-1 Configurations supported by 1830 PSS C+L band

NE Type	Shelf Type	NE Release	C+L	NFM-T Release
1830 PSS-32	1830 PSS-32 1830 PSS-16II PSI-8L MLFSB	R 13.0	C-band (C+L) only support with Managed Plane and Control Plane	R 20.7

Table 5-1 Configurations supported by 1830 PSS C+L band (continued)

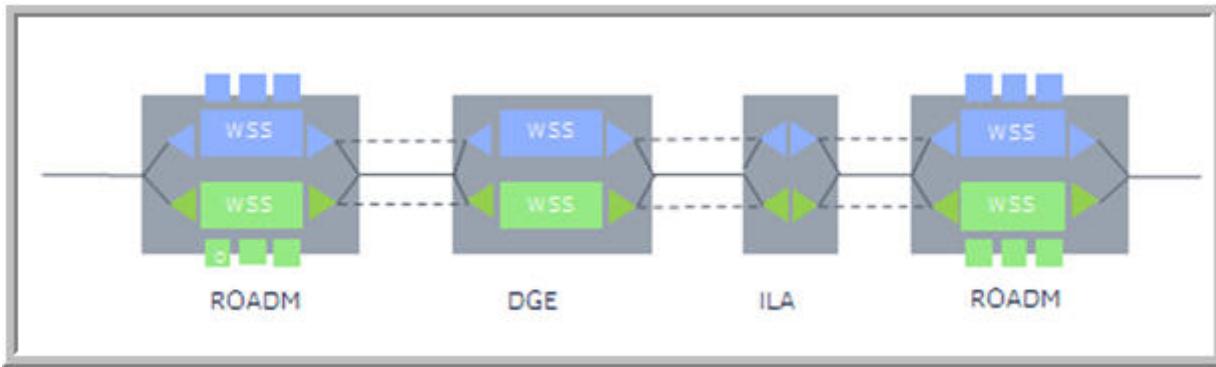
NE Type	Shelf Type	NE Release	C+L	NFM-T Release
1830 PSS-32	1830 PSS-32 1830 PSS-16II	R 11.1	C+L band support with Control Plane	R 19.2
1830 PSS-32	1830 PSS-32 1830 PSS-16II	R 10.0	C+L band managed plane Fixed grid and flex grid support Keyed and unkeyed services Layer 0 control plane support services L-band only	R 18.3
1830 PSS-32	1830 PSS-32 1830 PSS-16II	R 10.0.5	C-band only ("C-L") Flex grid support Keyed services No Layer 0 control plane support services (without MVAC8B)	R 17.12
1830 PSS-32	1830 PSS-32 1830 PSS-16II	R 10.0	L-band only 96 fixed channel support, and flex grid support Keyed and unkeyed services (without MVAC8B) Layer 0 control plane support	R 17.9

Control plane management

In C+L band, GMRE operates like an IP router using nodes and links. Constraints are added to connectivity or lines. The C+L concept is logically associated with two independent nodes running across the same fiber. Therefore, both bands are handled separately apart from shared risk of the amplifier and fiber.

The following figure shows the GMRE concept. The solid lines represent the fibers, the dashed lines represent the logical interfaces between the nodes. The WSS represents the CDC mesh and small boxes on top are Add/Drop with OTs, separated per band.

Figure 5-3 C+L band - GMRE diagram



Managed plane management

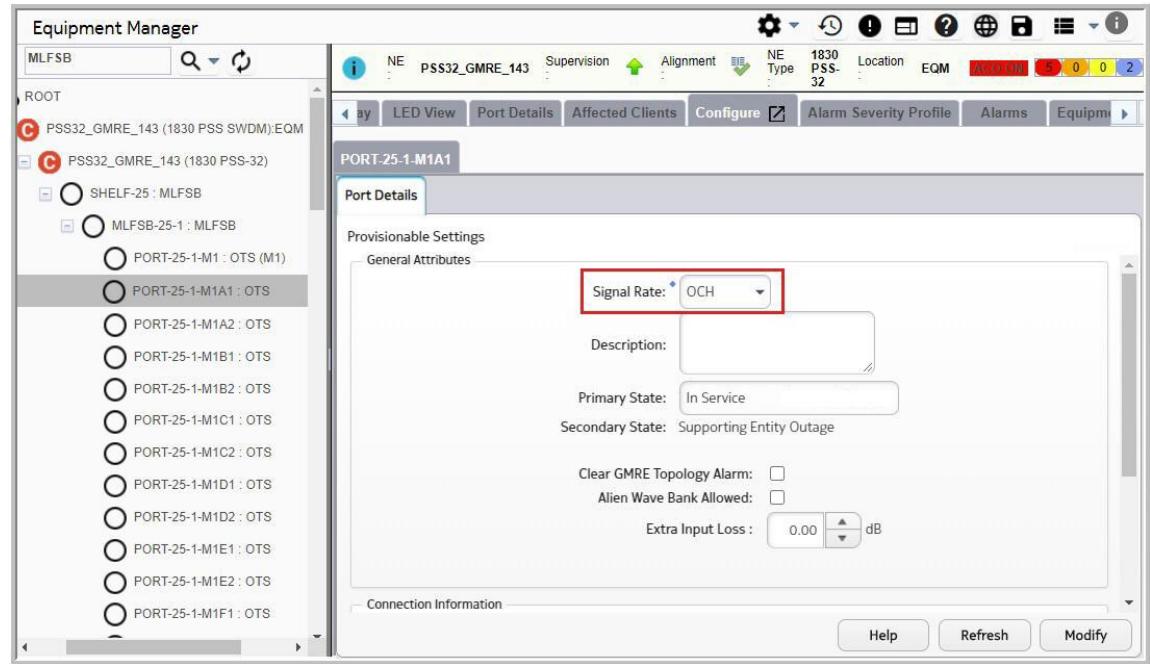
C+L band optical model supports ROADM (IRDM20, IRDM32, and IRDM32L) cards. MLFSB is a passive shelf designed to breakout Multi-fiber Push On (MPO) connectors into Lucent Connector (LC). MLFSB is used in the C-F optical architecture with IRDM20, IRDM32, and IRDM32L cards.

For more information, refer the MLFSB shelf section in the *NE Management Guide*.

MLFSB OCH XC

- Set the direction of the M [1..6][A..F][1,2] of MLFSB using the **Port Role** parameter to *In* or *Out*.
- Set MLFSB client side ports: M [1..6][A..F][1,2] as required; **Signal Rate**: *OTS* (default), *OCH* (provisionable).

Note: Ensure to change the **Signal Rate** to *OCH* before provisioning an OPS connection.



- For NFM-T, when provisioning the Direct OT Add/Drop (Internal, Cluster, External) and wavelength direct Add/Drop with or without MVAC, OCH value on **Signal Rate** of MLFSB on its client port must be provisioned to *OCH* (OTS is the default).
- When NFM-T deletes the topological link, the **Signal Rate** value remains at the set value (that is, default rate OTS or the provisioned rate OCH).
- If OT line port internal topology is connected to MLFSB, OCH XC ends on the OT line port.
- If MVACF G [1..8] ports internal topology is connected to MLFSB, OCH XC ends on the MVAC G [1..8] ports or the opposite direction of MLFSB port.
- If OT line port cluster topology is connected to MLFSB, OCH XC ends on the MLFSB port.
- Dangling external port of MLFSB, OCH XC ends on the MLFSB port.
- For an OCH connection between two Edge NEs (ENEs), ensure to set:
 - Provisionable Wave Key** as *Keyed*.
 - Wave Key type** as *Manual*.

Software Requirements

- Software upgrade from C-F to CDC-F architecture is supported at equipment level (allows hardware addition) and in routing because NFM-T must allow contentionless and directionless once NE is upgraded to CDC-F architecture.
- For a firmware upgrade, Database (DB) backup and restore support is required (not required for **In Service** upgrade)

-
- EPT/CPB (1830 PSS R13 onwards): Upload file is required for transmission parameter setting through the commissioning process.

Supported configurations with no mesh connectivity

- IRDM20, IRDM32, or IRDM32L + MLFSB + OT
- IRDM20, IRDM32, or IRDM32L + MLFSB + PSC1-6 + OT
- IRDM20, IRDM32, or IRDM32L + MLFSB

Supported configurations with Add/Drop block for mesh connectivity

- IRDM + MSH4FSB + AAR/AAR2x8A+MCS (CDC-F)
- IRDM + MLFSB
- IRDM + MLFSB + PSC1-6

C+L provisioning – OTS topological link

When the OTS topological link is created (see [7.19.5 “Task: Create an Bidirectional physical OTS or OPS connection” \(p. 793\)](#)), its OMS trail is auto generated by the NFM-T. Within the C+L optical model, two OMS trails - one in C-band and one in L-band are generated for one OTS span.

The band information reported by the NE is HW driven, when the HW degree changes, the NE generates a notification, and NFM-T automatically updates the OMS trail. The following combinations of configuration changes, for an OTS range are supported by the system:

1. Current configuration **C-band** only, change to:
 - **L-band**: one OMS trail for C-band is deleted impacting on the service, and a new L-band OMS trail is added.
 - **C-band and L-band**: one OMS trail is added for L-band. No impact on the existing C-band OMS trail.
2. Current configuration **L-band** only, change to:
 - **C-band**: one OMS trail for L-band is deleted impacting on the service, and a new C-band OMS trail is added.
 - **C-band and L-band**: one OMS trail is added for C-band. No impact on the existing L-band OMS trail.
3. Current configuration **C-band and L-band** only, change to:
 - **C-band**: one OMS trail for L-band is deleted impacting on the service. No impact on the existing C-band OMS trail.
 - **L-band**: one OMS trail for C-band is deleted impacting on the service. No impact on the existing L-band OMS trail.

C+L 2.0

NFM-T supports OMDCL (Optical Mux/Demux C+L band) uni-directional two-degree LD transmission circuit card, with two C+L band combiners and splitters for supporting two degrees OTS lines (four physical PTP Line ports of layer rate OTS). That is, deployment of C+L band for 1830 PSS NE release 14.0, with IRDM32L card to the same OMDCL configuration.

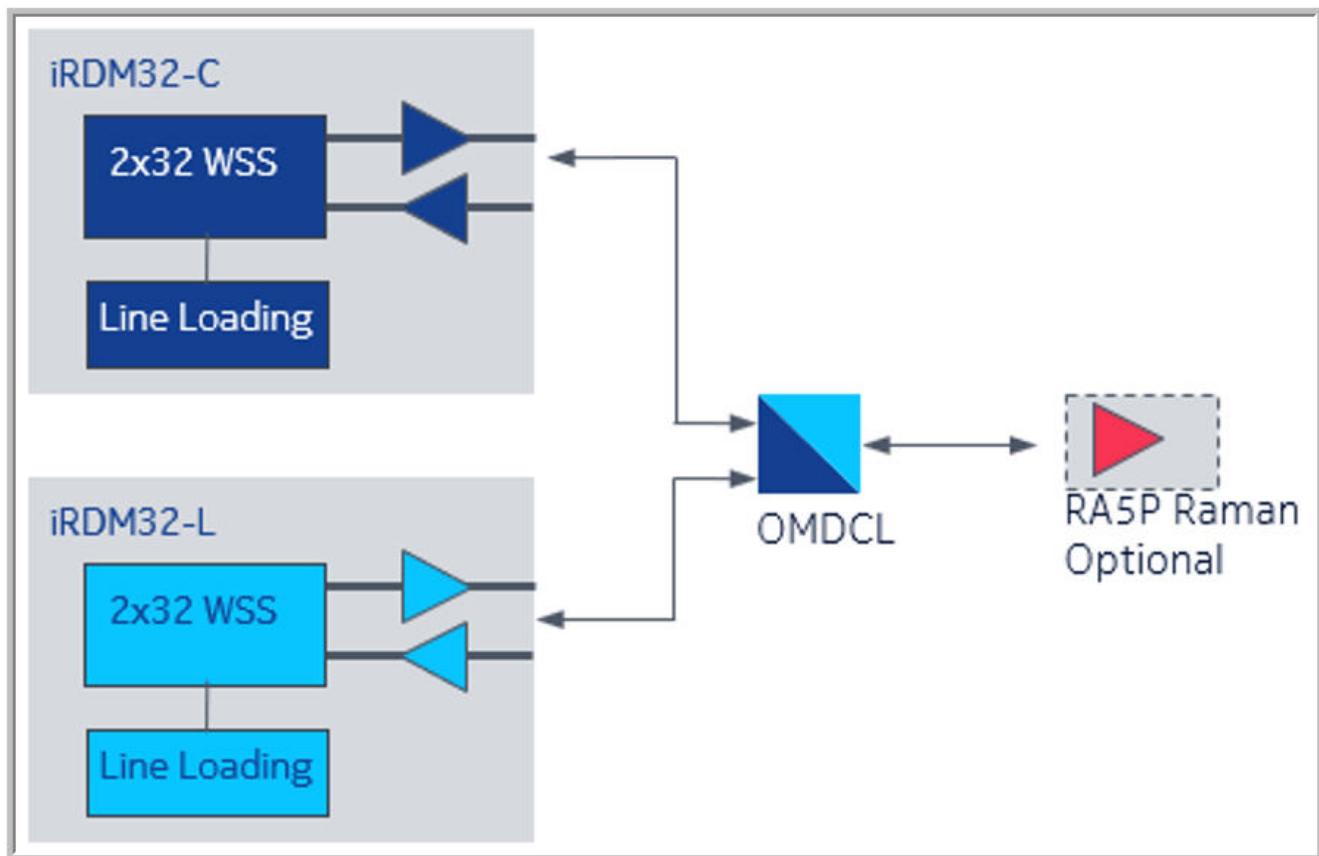
Each PTP has OMS CTP port and OCH CTP port. With OTS topological link layer on Line PTPs. On top of the OTS layer, there is an OMS trail layer on OMS CTPs. OCH Link connections are created from an OMS trail. OCH XC exists on OCH CTPs.

OMDCL supported C+L configurations:

- CDC-F R2.0 (IRDM32, IRDM32L, and MCS)
- C-F R2.0 (IRDM32, IRDM32L, and PSC1-6)

C+L band support on the same OMDCL configuration.

Figure 5-4 C+L band support on the same OMDCL



C+L band 2.0 supports:

- In service upgrade from IRDM32 + OMDCL to IRDM32 + IRDM32L + OMDCL
- Note:** C-band configured with OMDCL is a mandatory prerequisite for this upgrade.
- (Optional) Raman Line amplification
 - RA5P/RA5PB
 - Mixed degree configuration:

-
- IRDM32
 - IRDM32L
 - IRDM32 + OMDCL
 - C-L with IRDM32 + IRDM32L + OMDCL
 - C+L
 - OTS interworking with CDC-F 2.0 or DGE/ILA
 - No support for OLP protection
 - DGE/ILA
AWBILA

Add/Drop block configurations in C+L 2.0

- MCS816L
- PSC1-6 C-F Add/Drop

IRDM32/32L in C+L 2.0

- Seamless upgrade from IRDM32 + OMDCL to IRDM32 + IRDM32L + OMDCL configuration.
- All C-band Add/Drop support (MCS1615/MCS816 based, C-F)
- AllL-band Add/Drop block support (C-F)
- Line amplification: RA5PB or RA5P
- Mixed degree of IRDM32, IRDM32L, IRDM32 + OMDCL C-L, IRDM32 + IRDM32L + OMDCL C+L
- OTS interworking with CDC-F 2.0 or DGE/ILA
- ILA/DGE (single blade DGE) with AWBILA, or with conventional WR20TFM/WR20TFML

Note: OLP/OMSP protection is not required.

RA5PB in C+L 2.0

RA5PB is equipped in 1830 PSS R14.0 with a back-reflection monitor capability to detect LOS. This is assumed to be transparent to NFM-T.

C+L 2.0 and RA5PB configurations:

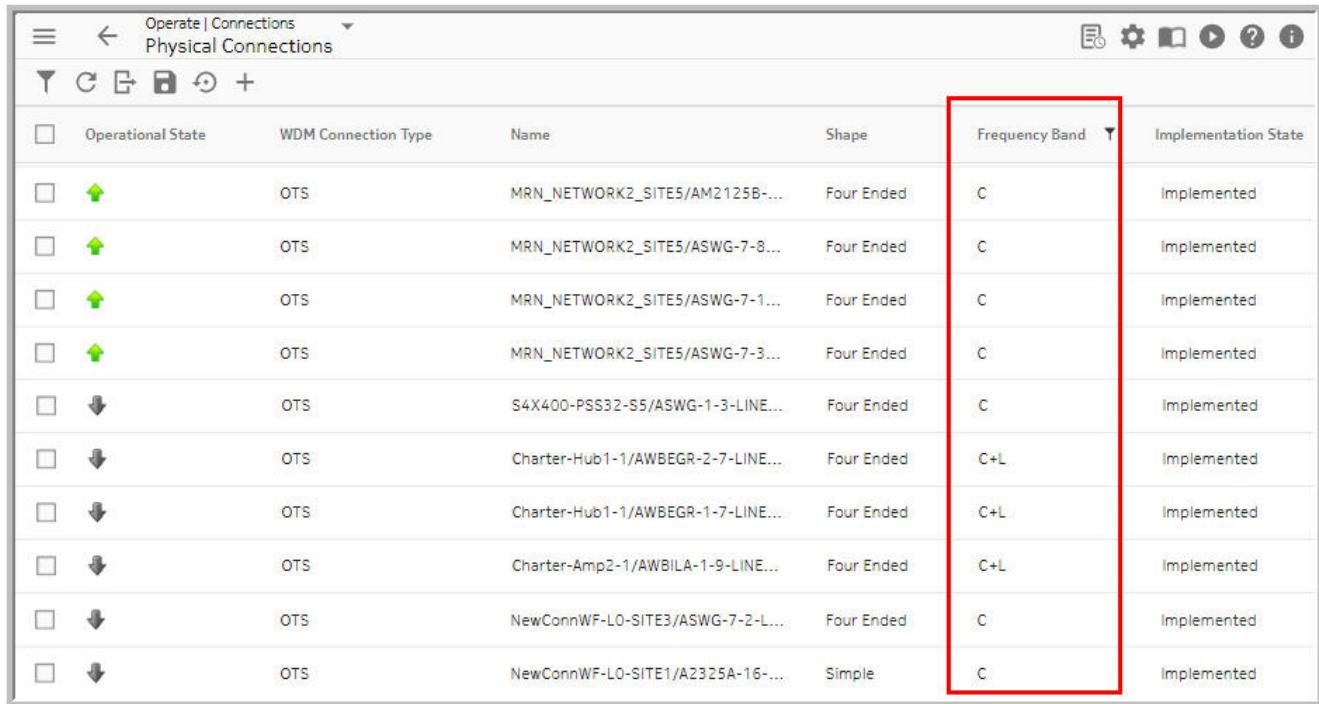
- CDC-F 2.0 C+L: IRDM32L + OMDCL + RA5PB with CDC-F Add/Drop
- C-F C+L: IRDM32L + OMDCL + RA5PB with C-F Add/Drop
- AWBILA + RA5PB
- WR20-TFM/TFML AWB + RA5PB for DGE application

5.4 Frequency bands visualization

Physical connection list

On the **Physical Connection** list, a column named **Frequency Band** is displayed, where the band type is displayed. The value is *L* for *L-band*, *C* for *C-Band* or *C+L* for *C+L band*. If the connection is of type OS/OPS, the value displayed is *N/A*.

Figure 5-5 Physical Connection List



Operational State	WDM Connection Type	Name	Shape	Frequency Band	Implementation State
	OTS	MRN_NETWORK2_SITE5/AM2125B...	Four Ended	C	Implemented
	OTS	MRN_NETWORK2_SITE5/ASWG-7-8...	Four Ended	C	Implemented
	OTS	MRN_NETWORK2_SITE5/ASWG-7-1...	Four Ended	C	Implemented
	OTS	MRN_NETWORK2_SITE5/ASWG-7-3...	Four Ended	C	Implemented
	OTS	S4X400-PSS32-S5/ASWG-1-3-LINE...	Four Ended	C	Implemented
	OTS	Charter-Hub1-1/AWBEGR-2-7-LINE...	Four Ended	C+L	Implemented
	OTS	Charter-Hub1-1/AWBEGR-1-7-LINE...	Four Ended	C+L	Implemented
	OTS	Charter-Amp2-1/AWBILA-1-9-LINE...	Four Ended	C+L	Implemented
	OTS	NewConnWF-LO-SITE3/ASWG-7-2-L...	Four Ended	C	Implemented
	OTS	NewConnWF-LO-SITE1/A2325A-16-...	Simple	C	Implemented

The **OMS trail** and **Infrastructure Connection** list also has a column **Frequency Band**, with C-band or L-band as possible values. This column allows filtering on C-band or L-band OTUk channels.

Frequency bands range

The C, L, and C+L bands frequency range used in NFM-T can be seen in the **Structure** tab of the Physical Connection data table.

Follow the path **Operate > Physical Connections** from the WebUI menu, to display the physical connection list. The physical connections using L-band frequency can be identified from the value *L* in the field **Frequency Band**. Click the Structure tab of the physical connection to see the band frequency range, as shown in following figure.

Figure 5-6 Frequency band

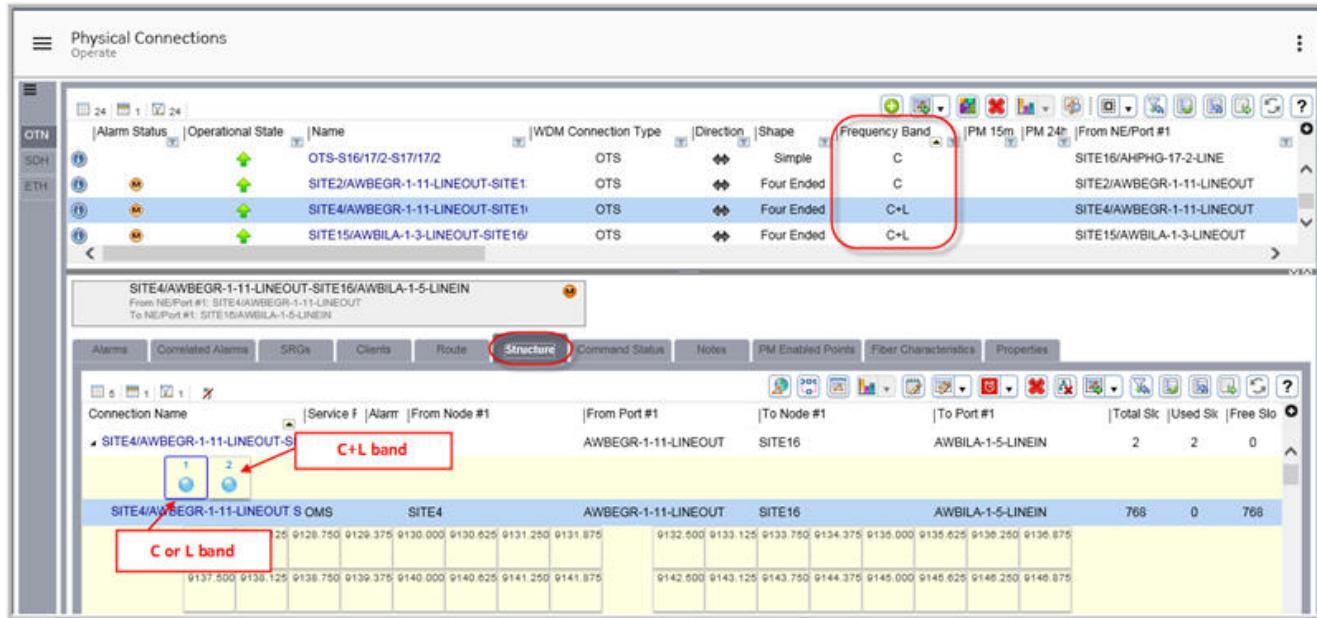
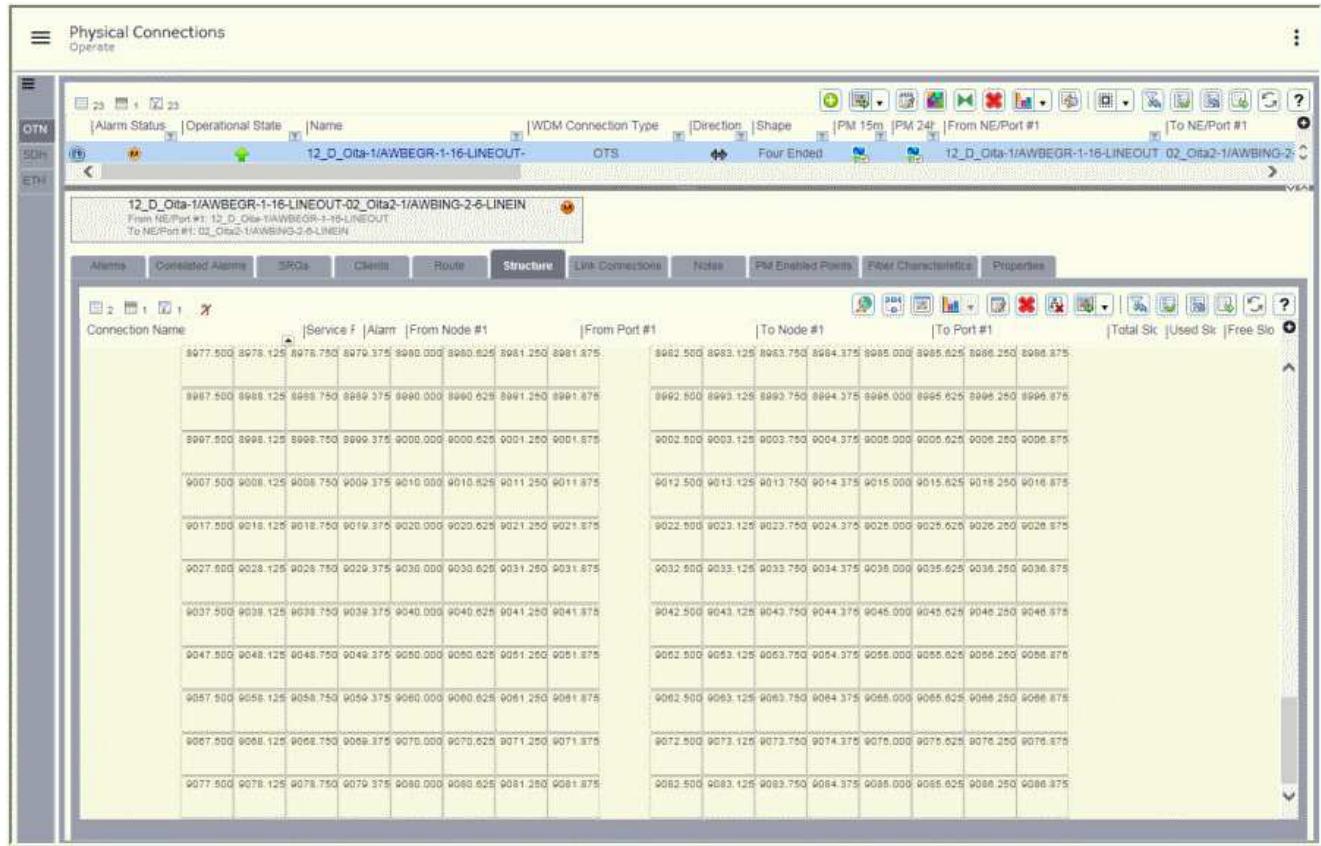


Figure 5-7 Example with L-band frequency range



ODUk Template for L-band

To support the connection creation for an L-band management, a new ODUk Template for ODUK Infrastructure provisioning is supported.

To list and deploy the L-band template, follow the path **DEPLOY > New Service/Infrastructure Connection** from the WebUI. Select the template **/Best Practices/Infrastructure Trail/ Unprotected with ODUk for L Band**. Click **Deploy** () to create a connection.

The specific items for L-band are:

- **Service Rate**: can be one of the following: ODU4, line signal rate on NE: OTU4 (Default), OTU4x2
- **L-band Frequency** checkbox: selected by default, you are creating an L-band connection.
- **Logical Link** checkbox: selected by default.
- **ASON** checkbox: selected by default, for using Layer 0 control plane.
- **Performance management**: under **Parameters > ASSURANCE** tab. 15 minutes and 24 hour are enabled by default for L-band connection, select the preferred one.

Figure 5-8 L-band Template

END POINT SELECTION

Service Rate Type	Rate	Connection type
Trail	ODU4	2-Ended Bi (I)
From Node #1	From Port Type #1	From Port #1
From Node #1	Terminated	From Port #1
To Node #1	To Port Type #1	To Port #1
To Node #1	Terminated	To Port #1

CONNECTION CONTROL

Define the route details related to new service/infrastructure/physical connection to be deployed.

Protection

Logical Link

L Band Frequency

Routing mode Automatic

Allow Ason Resources

ASON

Auto Server Creation

Wave Key Keyed

Customer Name

Connection Alias

Connection Name

Target State Commissioned

Compute Latency

BACK CONTINUE DEPLOY

5.5 L-band management in ASON

Description

A new frequency range is managed in ASON environment for L-band and two OMS Infrastructure are on the same OTS link. ASON manages new links related to L-Band/C-band logical links. This configuration is for using Layer 0 Control Plane. ASWG-L supports configuration of C+L and CDC-F in L-band.

Provisioning Steps

The aim of this description is to give an example of the provisioning of L-band in ASON environment. See also “[D5X500 circuit pack provisioning procedures](#)” (p. 1669) for details on the D5X500 circuit pack and its provisioning, and D5X500 - WDM lines supporting different modulation.

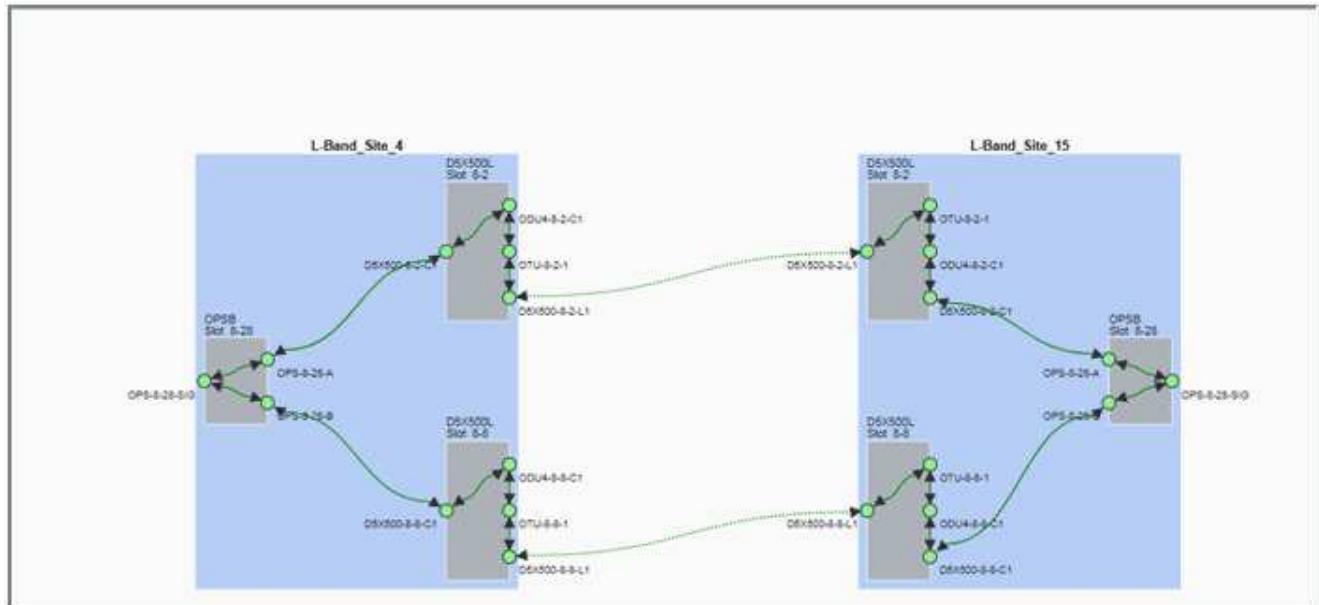
1

Create an OTS connection between ROADM and ROADM network elements using the dedicated template, as described in “[ODUk Template for L-band](#)” (p. 529). The connection can be seen in the list, and it will have the value L in **Frequency Band** field, as explained in “[Physical connection list](#)” (p. 527).

2

The OTS connection can be displayed in the Routing Display window and it is indicated explicitly in the page, as shown in the figure.

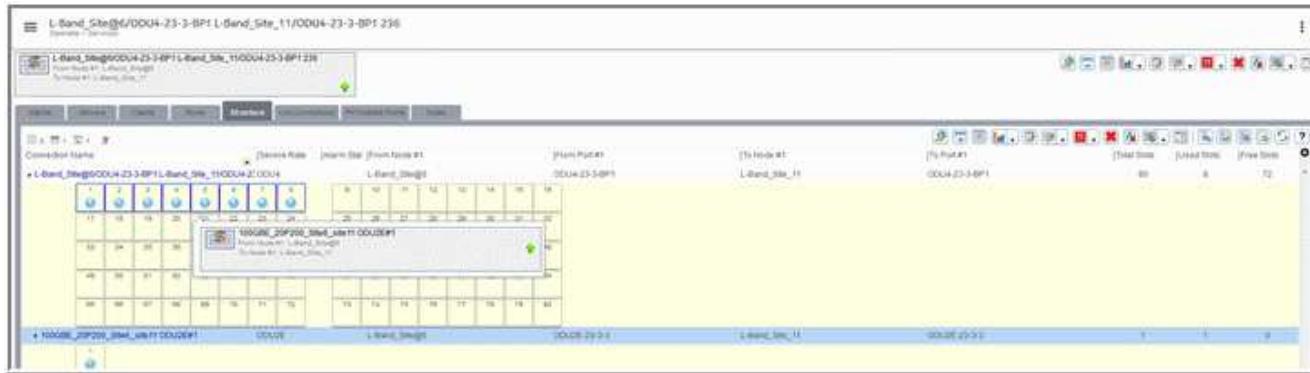
Figure 5-9 L-band in Routing Display



3

The structure of the connection shows the structure of the two ODUk for the connection.

Figure 5-10 Connection - Structure View



4

Assign the L-band OMS created to the NPA. The ASON link has the attribute about the **Frequency Band** that has value L.

5

The following figure shows a protected service on the bi-directional optical power.

Figure 5-11 Service - bi-directional Optical Power



Figure 5-12 Protection - bi-directional optical power

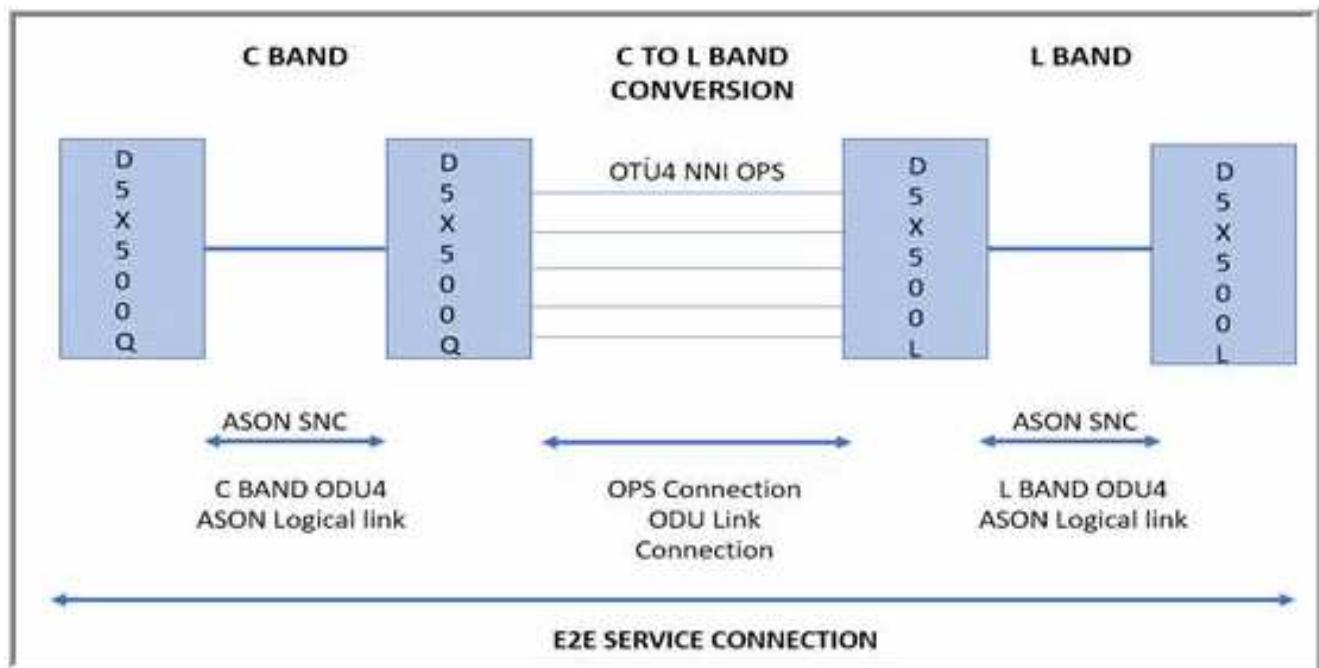


5.6 End to End Service C-band and L-band Interworking in L0 Control Plane

Description

NFM-T supports ODUk across OTUk link in back to back OTs with C-band to L-band conversion. This configuration is in particular B/W on DX500Q/L cards.

Figure 5-13 E2E Service C-band and L-band Interworking in L0 Control Plane Example



Service provisioning example

The example, depicted in the figure, manages an end-to-end split service between the C-band and L-band with a OTU4 between D5X500L and D5X500Q in L0 Control Plane domain. The D5X500 cards must be set in Interworking mode. The steps to set up the interworking service are:

1

If the card variant is **D5X500Q**, set the DX500Q cards Interworking Mode to Legacy. This operation is not required for other variants.

Follow the path **Operate > Equipment Manager**, navigate to the card to set the parameter. Select **Configuration** tab and then **Card Config** tab. Select **Legacy** in the **Interworking Mode** field.

2

If ...	Then
The OTU4 connection is created between two nodes	Create a physical connection of type OPS to connect the C-band node and the L Band node. Follow the path Deploy > New OTN Physical Connection , in the field WDM Connection Type select OPS. Insert the corresponding A end Point and Z end point.
The C-band to L-band conversion is in the same node	Create an internal OS between the client ports of D5X500/Q and D5X500L cards. See Configure Links and Ports in the <i>NFM-T NE Management Guide</i> .

3

Create a logical link and flag the **ASON Routed** parameter in the ODU4 connection you are creating. The link is between the two C-band nodes.

4

Create a logical link and flag the **ASON Routed** parameter in the ODU4 connection you are creating. The link is between the two L-band nodes.

5

Finally create the service between the C-band node and the L-band node.

Follow the path **DEPLOY > New Service/Infrastructure Connection** and deploy the service using ODUk/Unprotected template, in the field **Service Rate** in the **DEPLOY RULES** tab select the value 100 GbE for the service. Insert the corresponding From Node and To Node.

6

Deploy the service.

5.7 33.75 GHz and 70 GHz central frequency granularity for subsea application

Overview

The 33.75 GHz frequency management is introduced for supporting capacity driven subsea application. Currently flexgrid optical channel supports a channel width of 6.25 GHz grid for the following frequencies: 50 GHz, 62.5 GHz, 75 GHz, and 37.5 GHz. For more information on Flexgrid technology, bandwidth exploiting and provisioning, see [5.8 "Flex Grid technology" \(p. 545\)](#).

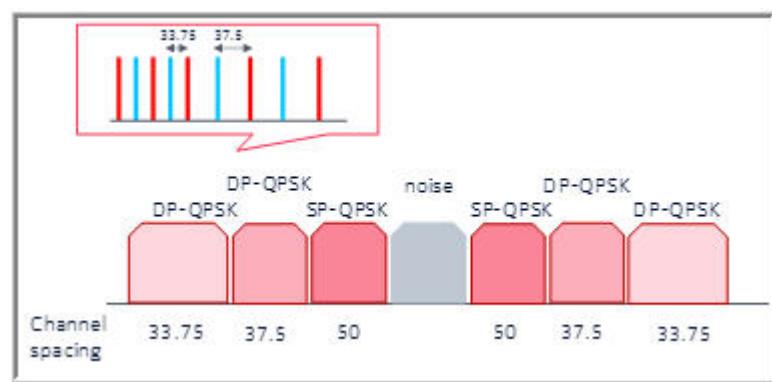
To maximize the channel capacity and to help the arbitrary arrangement of the optical channel, the central frequency of the 33.75 GHz and 70 GHz optical channel is changed from current flexgrid of 6.25 GHz grid to 1.25 GHz.

Optical channel grid, width and spacing

The optical channels are divided into "Even" (in red) and "Odd" (in blue) channels, by the user. The submarine optical channels use a grid equal to 1.25 GHz. For this, the user must set an optical channel on the 6.25 GHz grid, with offset values of: **0, +/- 1, +/- 2**.

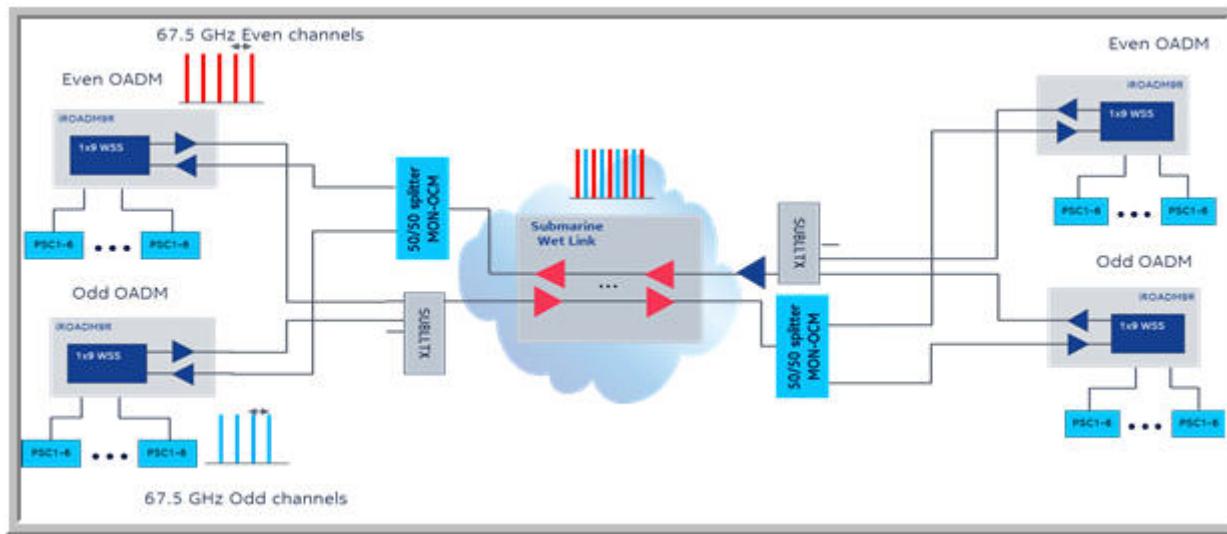
The following figure displays the maximization of the bandwidth.

Figure 5-14 Interleaved Optical channel



The following figure shows an example with a subsea optical system architecture.

Figure 5-15 Subsea Optical architecture



Even channels are marked in red, and odd channels marked in blue, which are transmitted by two ROADM degrees. They are then combined by a SUB TX direction and sent to the subsea link. On the receiving side, the combined signals are split to two ROADM degrees at the RX direction. Each channel is partially filtered by WSS and further filtered in OT packs.

The 33.75 GHz frequency band is managed by 1830 PSS NE Release 11.1 onwards for D5X500 and D5X500Q cards, with the following type of node configuration:

- C-F ROADMs: WR20-TF, with AHPHG, AHPLG, IROADM9R, and .
- CDC-F: WR20-TFM, with ASWG, IROADM20
- *Dangling OT, Cluster configurations*

The 70 GHz frequency band is managed by 1830 PSS NE Release 13.1 onwards for S4X400 card.

This feature is supported on the following 1830 PSS PHN NE shelves:

- 1830 PSS-32
- 1830 PSS-8
- 1830 PSS-16II
- 1830 PSI-M

This feature is supported on the following cards:

- D5X500Q
- D5X500
- S4X400H
- S6AD600H
- SFM6

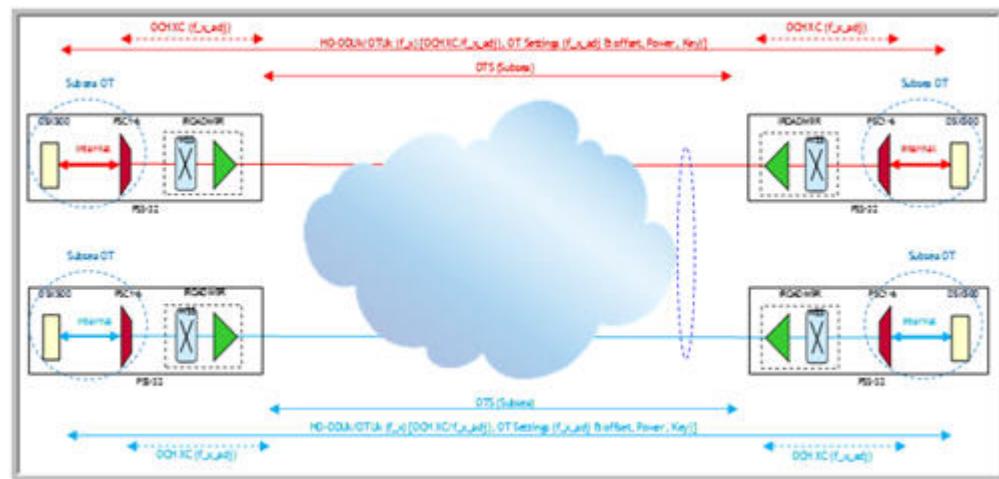
Provisioning description

The following figure provides an example of the provisioning of a subsea connection of 33.75 GHz frequency for D5X500 and D5X500Q with 1.25 GHz grid. Two connections are manually provisioned one for each channel type, **Even (red)** and **Odd (blue)**.

i Note: S4X400H supports 70 GHz frequency.

The following figure displays a scenario based on 1830 PSS Line System and Add/Drop OTs in which the A-end and Z-end NEs are 1830 PSS-32, with the Line system and Add/Drop OTs.

Figure 5-16 Subsea Connection Schema



The following scenarios are also supported:

3rd Party Line System and 1830 PSS OTs in which the A-end and Z-end NEs are 1830 PSS Add/Drop OTs as Dangling OTs, with 3rd party line systems.

1830 PSS Line System and 1830 PSS Dangling OTs in which the A and Z-end NEs are all 1830 PSS-32 (the line system plus the OTs), but the OTs are used as dangling OTs.

3R Regen between Subsea and Terrestrial DWDM Networks. in which 3R Regen OTs can be used between Subsea links and the Terrestrial DWDM networks.

Provisioning Steps

Physical connection creation

1

Create a physical connection between the far ends of the subsea connection. To do this, follow the path **OPERATE > Physical Connections** and click the **Create** icon.

2

In the *Connection Type* field, select **2 Ended split Bi**

3

In the *WDM Connection Type*, select **OTS** or **OPS**. For OPS, the *Interface Type* is selected as **NNI** by default.

4

Populate the **End Points** panel with the required information. See “[Physical Connections](#)” (p. 784)

Note: This step must be performed for both **Even** and **Odd** connections.

Figure 5-17 Example of physical connection creation

The screenshot shows the 'Deploy New OTN Physical Connection' interface. The process is divided into four steps: 1. DEPLOY RULES (active), 2. PARAMETERS, 3. SUMMARY, and 4. DEPLOY. The 'END POINTS' section contains fields for 'Physical Link Type' (set to 'OTS'), 'Connection Type' (set to 'Bidirectional'), and two sets of 'A Node' and 'Z Port' inputs. The 'Grid Type' field in the 'CONNECTION CHARACTERISTICS' section is highlighted with a red box. At the bottom, there are 'BACK', 'CONTINUE', and 'DEPLOY' buttons.

Result: The physical connection is created. The corresponding OMS connection is automatically created.

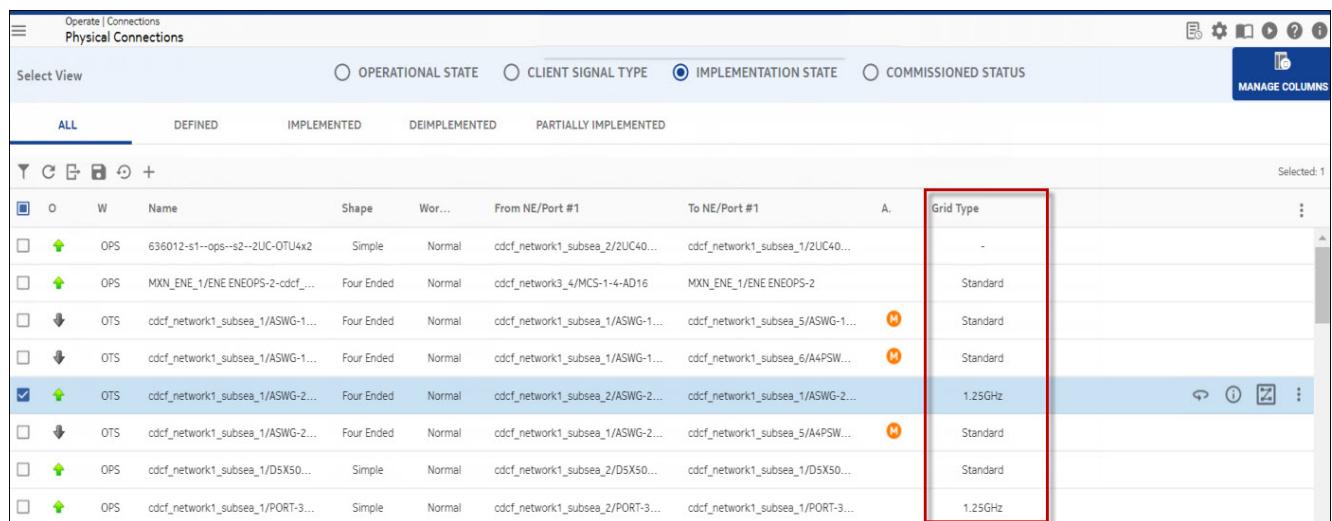
Provisioning Note:

- When creating an OTS physical connection with 1.25 GHz **Grid Type**, *Flexgrid* and *Grid Type* must be enabled on the line ports of the following cards: ASWG, AHPHG, IRDM20 and IRDM9R.
- When creating an OPS physical connection, select Standard **Grid Type** for SFM6 card.

5

Optional : To view the optical channel centre frequency in **OPERATE > Physical Connections**, click the **More**  icon at the top right corner, click **MANAGE COLUMNS** button , and select **GRID TYPE** from the list of options. The **Grid Type** column is displayed with the selected value.

Figure 5-18 Grid Type field



	O	W	Name	Shape	Wor...	From NE/Port #1	To NE/Port #1	A.	Grid Type	⋮
<input type="checkbox"/>			OPS 636012-s1--ops--s2--2UC-OTU4x2	Simple	Normal	cdcf_network1_subsea_2/2UC40...	cdcf_network1_subsea_1/2UC40...		-	
<input type="checkbox"/>			MXN_ENE_1/ENE ENEOPS-2-cdcf_...	Four Ended	Normal	cdcf_network3_4/MCS-1-4-AD16	MXN_ENE_1/ENE ENEOPS-2		Standard	
<input type="checkbox"/>			OTS cdcf_network1_subsea_1/ASWG-1...	Four Ended	Normal	cdcf_network1_subsea_1/ASWG-1...	cdcf_network1_subsea_5/ASWG-1...		Standard	
<input type="checkbox"/>			OTS cdcf_network1_subsea_1/ASWG-1...	Four Ended	Normal	cdcf_network1_subsea_1/ASWG-1...	cdcf_network1_subsea_6/A4PSW...		Standard	
<input checked="" type="checkbox"/>			OTS cdcf_network1_subsea_1/ASWG-2...	Four Ended	Normal	cdcf_network1_subsea_2/ASWG-2...	cdcf_network1_subsea_1/ASWG-2...		1.25GHz	
<input type="checkbox"/>			OTS cdcf_network1_subsea_1/ASWG-2...	Four Ended	Normal	cdcf_network1_subsea_1/ASWG-2...	cdcf_network1_subsea_5/A4PSW...		Standard	
<input type="checkbox"/>			OPS cdcf_network1_subsea_1/D5X50...	Simple	Normal	cdcf_network1_subsea_2/D5X50...	cdcf_network1_subsea_1/D5X50...		Standard	
<input type="checkbox"/>			OPS cdcf_network1_subsea_1/PORT-3...	Simple	Normal	cdcf_network1_subsea_2/PORT-3...	cdcf_network1_subsea_1/PORT-3...		1.25GHz	

Infrastructure connection creation

6

Navigate to the following path: **DEPLOY > New Service/Infrastructure Connection**. Select the **/Best Practices/Infrastructure Trail/Unprotected with ODUk or OTSiG Tunnel** template and click **Deploy** ().

For D5X500 AND D5X500Q, create a logical link infrastructure connection with **ODU4** as the **Rate**.

For S4X400H, S6AD600H and SFM6, create an OTSig Tunnel with **OTSig Tunnel** as the **Rate**.

7

Under **DEPLOY RULES** tab, select **ROUTING MODE** as *Manual*.

For S6AD600H and SFM6, in the **OPTICAL LINE CHARACTERISTICS** pane, the supported profiles are 27 and 29.

In NFM-T R22.6, 1.25GHz central frequency granularity for S6AD600H and SFM6 is supported for Managed Plane connections only.

8

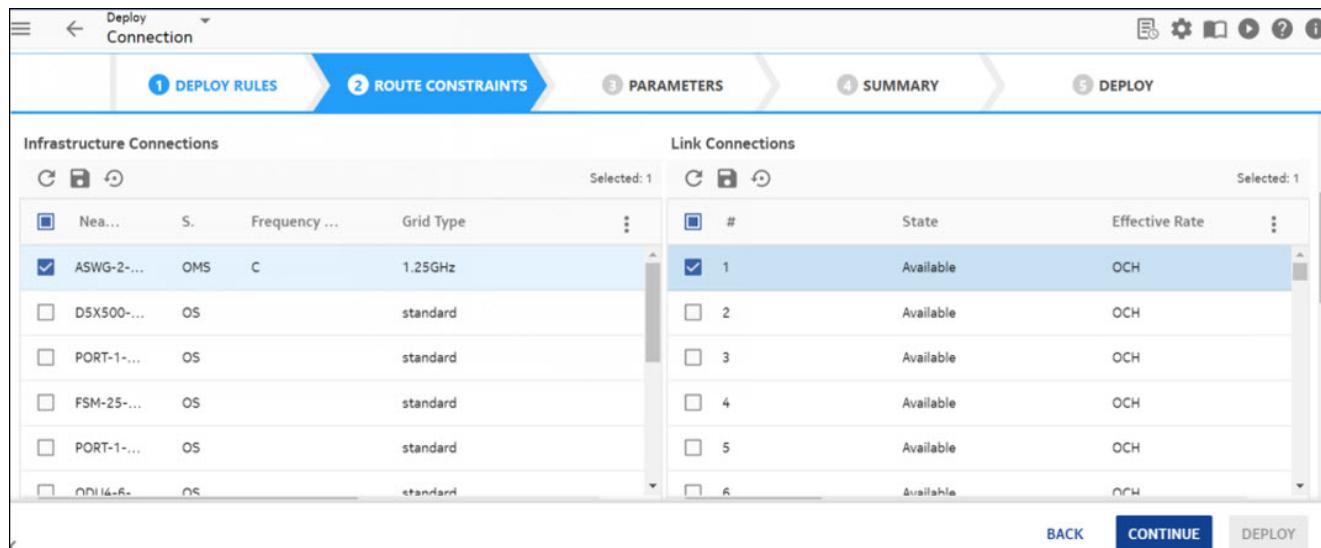
Under **ROUTING CONSTRAINTS > Frequency** tab, uncheck the **System Assigned Frequency** and select the **Subsea (1.25 GHz)** checkbox.

Note: For S6AD600H and SFM6, continue with the **System Assigned Frequency** default selection, and select **SubSea (1.25GHz)** checkbox.

9

To provision the OCH channel, from the **ROUTE CONSTRAINTS** tab select a connection that supports 1.25 GHz **Grid Type**. The corresponding Link Connections are displayed with **Effective Rate** as OCH, on the right side of the window. Select a frequency and click **INCLUDE**.

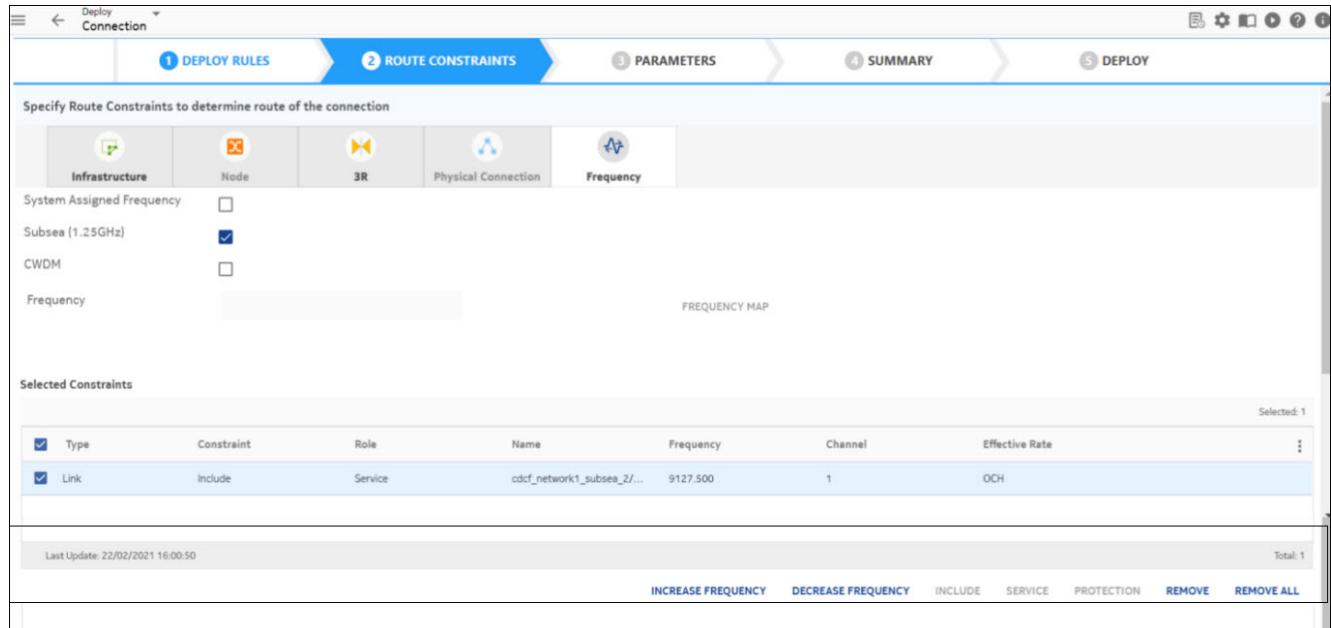
Figure 5-19 Routing Constraints



Result: The selected link connections get populated in the **Selected Constraints** panel. Select the Link from the **Selected Constraints** panel and click **CONTINUE**.

10

To change the frequency off set, click the **INCREASE FREQUENCY** or **DECREASE FREQUENCY** buttons. The allowed increase and decrease values are +2, +1, 0, -1, -2. With every increase or decrease in frequency, the values will change by 1.25 GHz.



Result: To view the assigned frequency, navigate to **OPERATE > Infrastructure Connections** page after deployment or the NE WebUI.

11

Verify the parameters in the **PARAMETERS** tab and click **CONTINUE** and **DEPLOY**.

Result: In the **OPERATE > Infrastructure Connections** page, the corresponding OTSig tunnel or logical link connection is displayed.

Service connection creation

12

Navigate to the following path: **DEPLOY > New Service/Infrastructure Connection**. Select the **/Best Practices/Service/Ethernet/Unprotected/Full Rate with 100G Ethernet** template and click **Deploy** ().

13

Create an 100G service on top of the OTSig tunnel or infrastructure connection.

Result: In the **OPERATE > Services** page, the corresponding service is displayed.

Note: S6AD600H and SFM6 supports 400G service rate.

Features

NFM-T Frequency bands management

33.75 GHz and 70 GHz central frequency granularity for subsea application

Nokia NFM-T

For more information on provisioning a service, see [8.8 “Deploy a Service” \(p. 1294\)](#)

5.8 Flex Grid technology

Introduction

Flex Grid, represents the possibility to define channels with different modulations and width (50 GHz, 62.5 GHz, 75 GHz and 37.5 GHz) so to allocate them on without being constrained on ITU-T 50 GHz grid to achieve better DWDM optical channel spectral efficiency and enabling the possibility to define super channels. The user can implement this feature modifying the width of channel in multiples of 6.25 GHz slices.

Flex Grid management, is a feature of 1830 PSS in Release 9.1 In order Flex Grid is enabled on a link, both nodes at the endpoints, must be Release 9.1 with HW ready to support this feature. It is mandatory to have WTOCM-F in addition to Flex Grid WSS.

Flex Grid Features

When operating with Flex Grid, both center frequency and width of a channel can be provisioned by the user.

Their items, are therefore flexible and their values can be set up following these rules:

- Once the center frequency (CF) is fixed, the other center frequencies or edges of channel slots are calculated as multiple of 6.25 GHz either above or below from the fixed CF value.
- Flexible channel width or spacing is set up as multiple, m times, of 12.5 GHz.

Hence, for the flexible DWDM grid, the allowed frequency slots have a nominal central frequency (in THz) defined by:

- $193.1 + (n \times 0.00625)$: where n is a positive or negative integer including 0 and 0.00625 is the nominal central frequency granularity in THz.

and a slot width defined by:

- $(m \times 12.5)$: where m is a positive integer and 12.5 is the slot width granularity in GHz.

Any combination of frequency slots is allowed pay attention to not overlap frequencies.

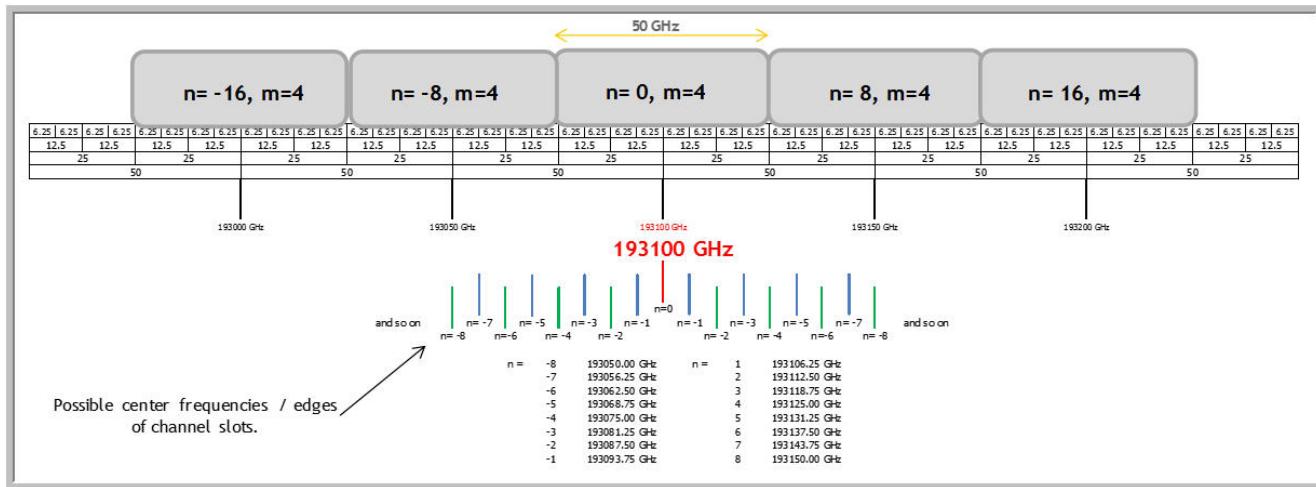
According to **ITU-T G.694.1**, the flexible grid reference frequency is 193100 GHz with $n=0$.

All other frequencies on the grid, are found from the formula:

- $(193100 \text{ GHz} + n \times 6.25 \text{ GHz})$: where n can be positive or negative.

Channels are constructed from a center frequency (CF) and $m \times 12.5$ GHz frequency slices or width. The Optical Channel Frequency Plan is shown in the next picture.

Figure 5-20 Optical Channel Frequency Plan



The Flex Grid frequency support covers the following conditions:

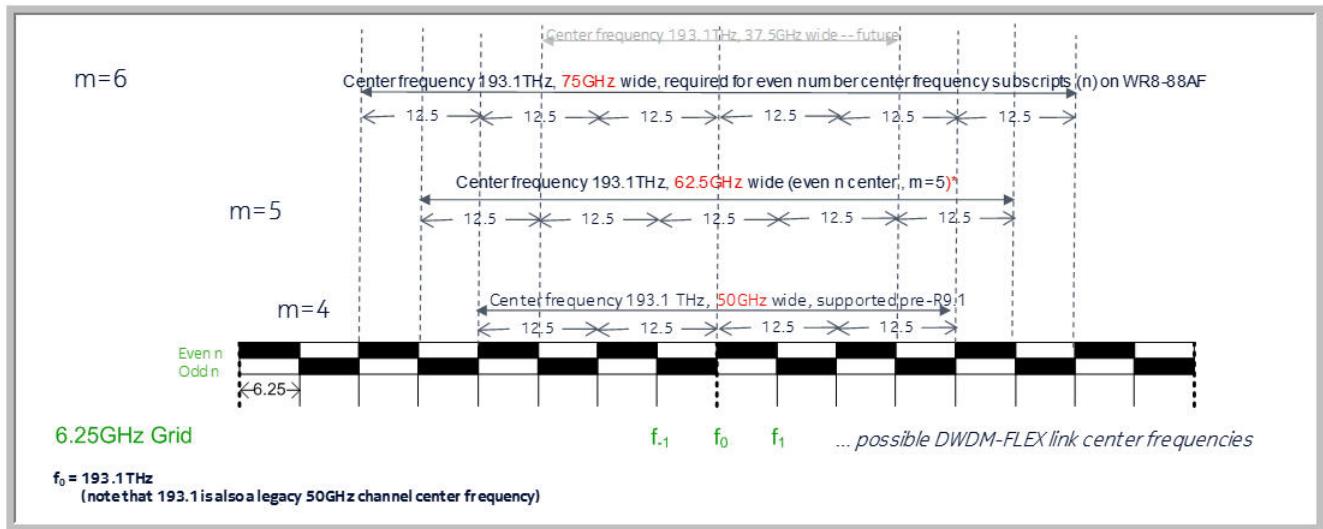
- Flexible Grid Channel Plan supports channels with center frequency on a grid of 6.25 GHz.
- The Grid Channels can have widths of 50 GHz (fixed), 62.5 GHz (flexible) or 75 GHz (flexible).

The Flexible Grid plan supports the C-Band channels in the range 191.275 and 196.075 THz.

The number of channels supported by NFM-T can be structured according to the following arrangements:

- Basic arrangement with 88 C-band DWDM channels on 50 GHz grid.
- Adding 8 channels on 50 GHz grid to get 96 channels.
- Multiplying by 8 to move to a 6.25 GHz grid of center frequencies to get 761 slices.

Figure 5-21 Optical channel bandwidths



The Flex Grid feature is referred to the management of spectrum in C-band and central frequency according to the following paradigms:

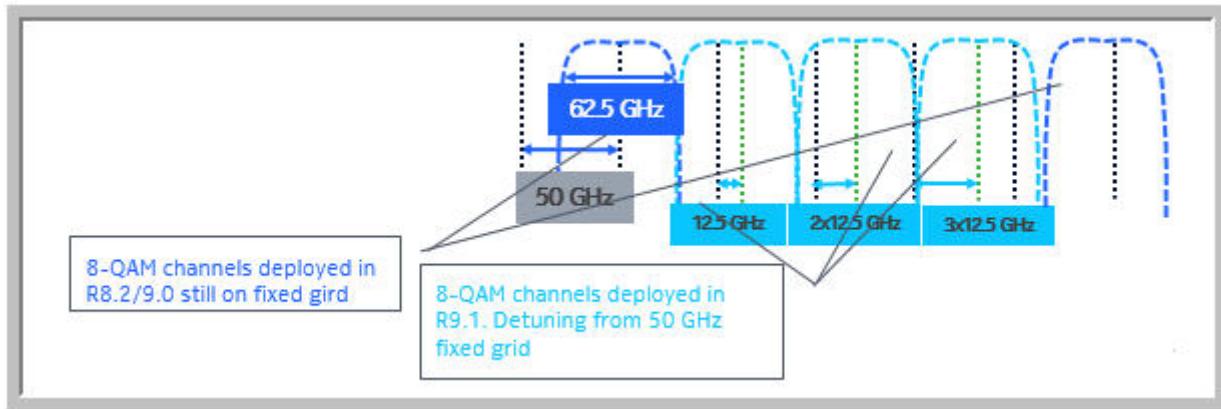
- Grid de-tuning management from fixed 50 GHz to 6.25 GHz slices.
- Mixed grid for interworking between fixed and flex grid nodes links.
- The NFM-T supports the Flex Grid for CDC-F node (50 GHz), ROADM node based on WR8-88AF (75 GHz) and C-F node (62.5 GHz) as well as the interworking between Flex Grid and Fixed Grid nodes/links defining the best path taking into account all the hardware constraints associated to the grid.

Figure 5-22 Channel Frequency Format and Channel Width

Total Number of Channels	Frequency Range	Delta/Grid	Channel Width	PSS-32 Release	PSS-4 Release	OCS Release (Uplink Card)	OMS Release
88	[9170-9605]	5 (50GHz)	5 (50GHz)	<= R9.0, or 9.0.1	<= R9.0, or 9.0.1	<= R9.0, or 9.0.1	<= R14.0 or 14.1
96	[9130.000-9605.000]	5.000 (50GHz)	5.000 (50GHz)	R9.1-	N/A	N/A	R14.2-
761, Flexgrid	[9130.000-9605.000]	.625 (6.25GHz)	5.000 (50GHz), 6.25 (62.5GHz), 7.5 (75GHz)	R9.1-	N/A	R9.1-	R14.2-

The capability of exploiting a better spectrum usage, allows to put, close each other, channels with different width since it is no more necessary to keep channels aligned to IUT-T 50 GHz fixed grid as next figure outlines.

Figure 5-23 Spectrum usage



Frequency Format

In order to support Flex Grid feature, the optical frequency with 6.25 GHz granularity requires the 4.3 digit format. An example of frequencies values expressed in 4.3 digit is shown in the table:

Min Frequency value	Max Frequency value	Frequency step
9130.000	9605.000	0.625

Provisioning

The existing provisioning template, supporting selection of different modulations to create 50 GHz and 62.5 GHz channels width, is now enhanced with a specific frequency map to allow operator to specify the central frequency of each channel in term of 6.25 GHz slice instead of a frequency on 50 GHz fixed grid.

Using the new template, operator can select a specific 6.25 GHz slice as central frequency.

The NFM-T automatic routing, takes into account constraint on central frequency and channel width in route calculation to avoid overlap with existing channels.

The user can still specify the frequency, indicating the number of the central channel slice, if already planned or decided as per R 14.0 behavior.

Frequency map is available in *Routing Constraints* section of the new template as represented in the next figures.

Figure 5-24 Routing Constraints - Frequency map button

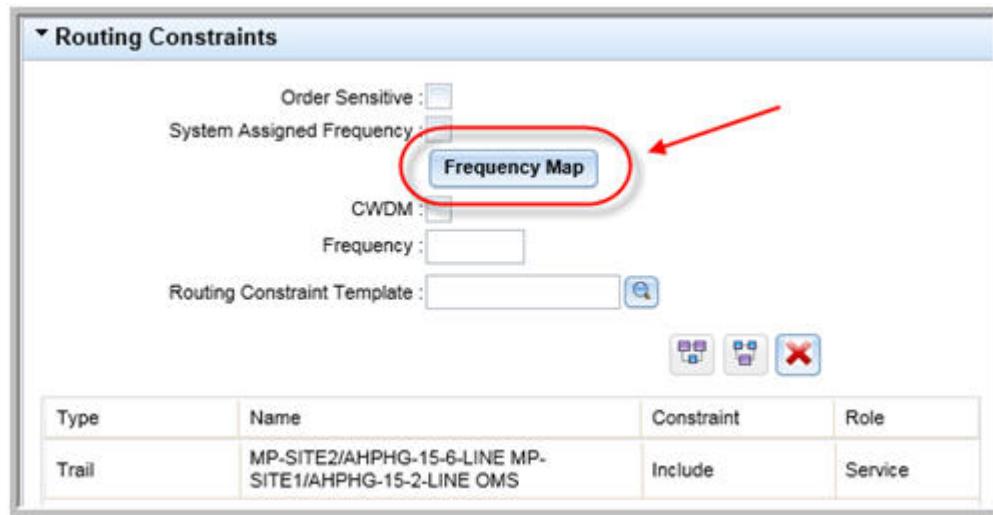
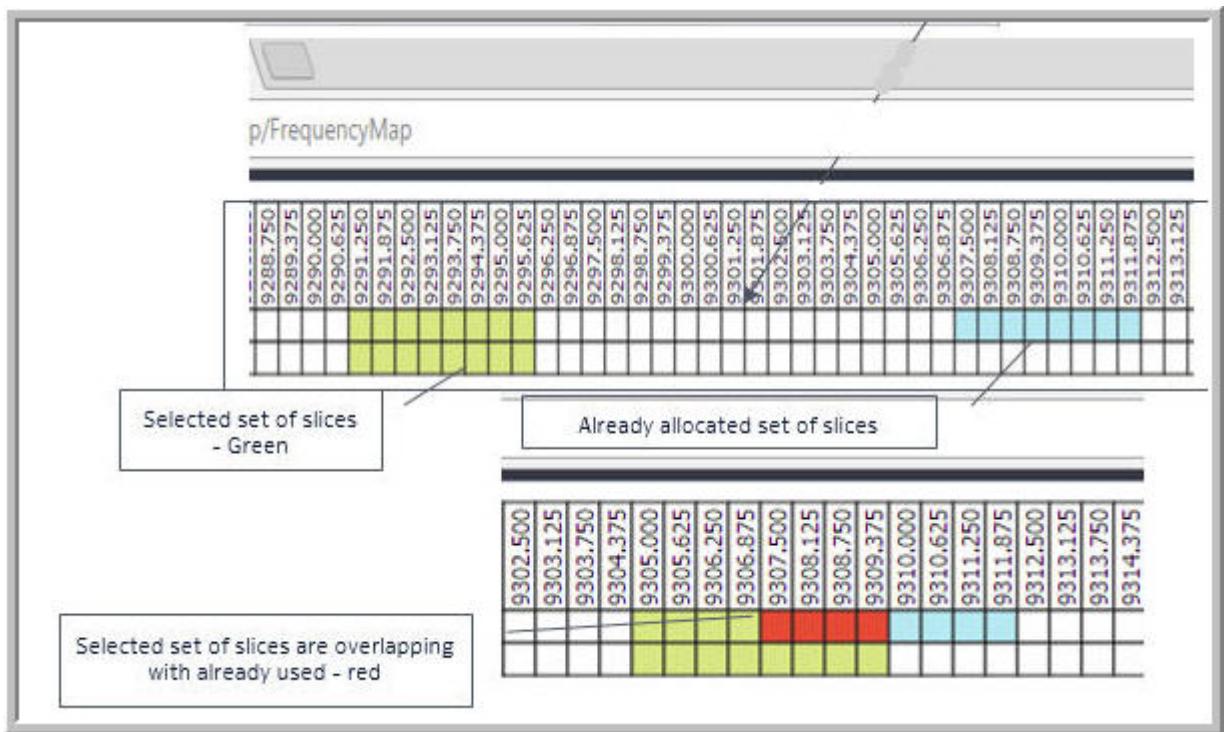


Figure 5-25 Routing Constraints - Frequency map display



The user has to select different links, NFM-T connections, crossed by the channels.

The frequency map shows, in a single window, all the selected links and related available 6.25 GHz slices to allow operator to understand where the channel can be defined according to the number of slices necessary to accommodate the channel modulation selected.

The number of slices are dynamically selected moving the mouse pointer on the frequency map according to channel modulation width.

The map of the frequencies uses different colors to indicate:

- Selected slices are highlighted in green.
- Slices already used by channels in light blue.
- Overlap slices between already used and selected slices are highlighted in red.

Physical connection view

Physical connection structure view has also been enhanced to show also how channels are allocated when operating with Flex Grid.

When operating with fixed OTS links, these are shown as a *block* for each ITU-T 50 GHz grid channel. If operating with Flex grid OTS links, the view shows a *block* per each 6.25 GHz slice.

All slices belonging to the same provisioned channel are grouped together. If the operator clicks on a slice, all the ones belonging to the same channel are highlighted. In addition, the block with central 6.25 GHz slice is marked with **C**.

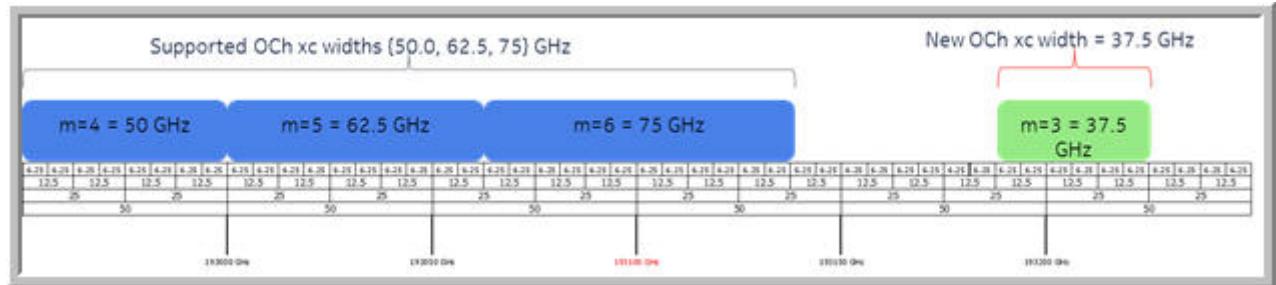
5.9 37.5 GHz Frequency Band Management

Overview

37.5 GHz complete frequency grid management is introduced with 50 GHz, 62.5 GHz, and 75 GHz in Flex grid technology. For additional information see [5.8 “Flex Grid technology” \(p. 545\)](#).

The following figure shows where the 37.5 GHz band is allocated in the optical channel frequency plan.

Figure 5-26 Optical channel frequency plan



37.5 GHz management with NFM-T

NFM-T supports the management of the 37.5 GHz from release 19.2 onwards. The 37.5 GHz requires less spectrum width compared to 50 GHz and 62.5 GHz. This frequency band only supports 16QAM and QPSK encoding mode.

The 37.5 GHz band supports CDC-F and C-F based architectures nodes, including ILAs and DGE for C-band, L-band, and C+L-band with point-to-point connections, that is, no ROADM card is used in between the nodes.

OCH XC with 37.5 GHz width is supported with point-to-point and/or Filterless DGE networks only. OT line with 33 Gbaud rate (for example, 100 G, 33 Gbaud, QPSK) is supported. OTUk routing with LC generation of an OMS trail with 37.5 GHz channel width is supported. Dangling OT and cluster support is based on OTUk connection with existing support of OTs/ULs configuration.

Whenever 37.5 GHz is used as a XC width, NFM-T will start filling the bandwidth of the underlying OMS LCs from the left of the spectrum to the right of the spectrum. When any other XC width is used, NFM-T will fill from the center of the spectrum to the right of the spectrum. If there is a mix of 37.5 GHz with other XC width, there will be a loss of bandwidth when the OMS LCs reach the center of the spectrum.

The following table provides information on the bandwidth usage for the different XC width and also for the combination/consecutive bandwidth usage:

Table 5-2 XC Width and bandwidth usage

XC Width	Bandwidth usage
37.5 GHz only	Loss of bandwidth exists
50 GHz only	No loss of bandwidth
62.5 GHz only	No loss of bandwidth
75 GHz only	No loss of bandwidth
50 GHz and 62.5 GHz	Loss of bandwidth exists Note: If a 50 GHz only XC width is created and then consecutively 62.5 GHz XC width is created, then there is no loss of bandwidth)
62.5 GHz and 75 GHz	No loss of bandwidth
37.5 GHz and 62.5 GHz	Loss of bandwidth exists

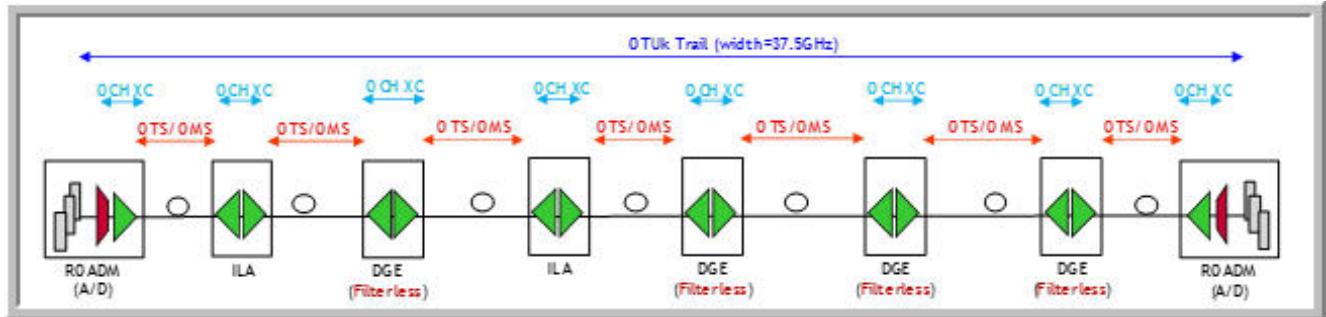
Hardware requirements

- IROADM9R and ROADM
- CDC-F (WR20-TFM): R 2.0 with iRDM20, iRDM32, iRDM32L
- C-F (WR20-TF): R 2.0 with iRDM20, iRDM32, iRDM32L
- Single blade DGE (WR* based, Filterless)
- Dual blade DGE (WR* based, Filterless)
- ILA
- CDC C+L (WR20-TFM and WR20TFML): R 2.0 with iRDM20, iRDM32, iRDM32L

For more information on ROADM cards, see *1830 PSS Card Management* section of *NE Management Guide*.

The following figure shows an example of a typical network in which 37.5 GHz can be applied. Note that the optical Add/Drop multiplexer (ROADM) is employed in far end nodes, while in the middle are employed with DGE and ILA. DGEs must be configured as *Filterless*. For the DGEs setting refer to *Equipment Management* section of the NFM-T NE Management Guide.

Figure 5-27 37.5 Ghz Frequency Band - Example of Network



Provisioning note

The 1830 PSS involved in the 37.5 GHz provisioning must be in Release 11.1 or higher and all cards must support the Flex Grid technology.

This feature applies to the following shelves 1830 PSS-32, 1830 PSS-8, 1830 PSS-16II and packs:

- IRDM packs: IROADM9R and IRDM20
- WR packs: WR20-TF, WR20-TFM, WR20TFML
- LDs: ASWG, AWBILA, AWBING, AWBEGR, ASWG-L, IPREAMP, RA2P, RA2P-96, RA5P
- OCM packs: WTOCMs (WTOCM-F and WTOCM-FL)
- OT/Uplink packs: D5X500, D5X500Q, D5X500L, 2UC400, 4UC400 (with 2AC200H), 1UX100 (with 2AC200H), 2UX200, LCI2000, DA2C4, S2AD200H with OTU4 rate, and ADD4 OTs and Uplink (for B100G OTs/ULs).

Provisioning steps

Perform the following steps to provision the OTU layer with 37.5 GHz frequency band cross-connect between two ROADM cards.

1

Create an *ODUk/OTUk* connection between ROADM and ROADM (for example, IROADM9R and IRDM20 cards) network elements using the dedicated template for the integrated provisioning, which allows to create an *ODUk* with *OTU* on Managed Plane network.

1. Navigate to **DEPLOY > New Service/Infrastructure Connection**
2. Select the template **/Best Practices/Infrastructure Trail/Unprotected with ODUk or OTSiG Tunnel**
3. Click **Deploy** ()

2

Ensure to set the parameters: **Encoding**, **Wave Shape**, and **Channel Width** under **Paramters > TRANSMISSION** tab according to the type of cards selected in the *Deploy Rules* tab.

For example, for 37.5 GHz connection between IROADM9R and IRDM20 cards:

- Set **Encoding** to **QPSK**
- Set **Wave Shape** to **Single Channel** (for **QPSK** encoding)
- Set **Channel Width** to **37.5**

Result: The ODU4, OTU connections, and the connected OMS server connections are created.

Use the *OCH XC Width for Non-ADD4 OTs* table for setting the parameters **Encoding**, **Transmit Shape**, and **Channel Width** for different cards.

Table 5-3 OCH XC Width for Non-ADD4 OTs

Rate	Baud Rate (Gbaud)	Encod-ing	FEC Mode	Wave shape	Channel width	OTs
100G (OTU4)	32.5	QPSK	[SDFEC-G2] [SDFEC-ACC] [AFEC] [SCFEC]	Single Channel	37.5, 50.0 (default), 62.5, 75.0, 87.5	D5X500, D5X500Q, D5X500L *1,*2,*3
					37.5, 50.0 (default), 62.5, 75.0, 87.5	S2AD200H/R *1,*3
				Alien	50.0 (default), 62.5, 75.0, 87.5	DA2C4/E *1,*3
						S13X100R/E/L *1,*3
						2UC400/E (*1,*2,*3)
						4UC400/2AC100 (50.0 only)
						4UC400/2AC100 *3 (50.0 only)
						4UC400/2AC100H *1,*2,*3
						1UX100/2AC100 *3 (50.0 only)
						1UX100/2AC100H *1,*2,*3
						2UX200/C4ACO *1,*2,*3
						6PX800/C4ACO *1,*2,*3

Table 5-3 OCH XC Width for Non-ADD4 OTs (continued)

Rate	Baud Rate (Gbaud)	Encoding	FEC Mode	Wave shape	Channel width	OTs
100G (OTU4)	44.5	SP-QPSK	SDFEC-G2	Single Channel	62.5, 75.0	D5X500, D5X500Q, D5X500L *1,*2,*3
				Super Channel	N/A	2UC400, 2UC400E *1,*2,*3
				Alien	62.5, 75.0	
200G (OTU4x2)	44.5	8QAM	SDFEC-G2	Single Channel	62.5, 75.0	D5X500, D5X500Q, D5X500L *1,*2,*3
				Super Channel	N/A	2UC400, 2UC400E *1,*2,*3
				Alien	62.5, 75.0	
200G (OTU4x2)	32.5	16QAM	SDFEC-G2	Single Channel	50.0 (default), 62.5, 75.0	D5X500, D5X500Q, D5X500L *1,*2,*3
						S2AD200H/R *1,*3
						DA2C4/E *1,*3
				Super Channel	37.5, 50.0 (default), 62.5, 75.0	2UC400, 2UC400E *1,*2,*3
						2UX200/C4ACO *1,*2,*3
				Alien	50.0 (default), 62.5, 75.0	6PX800/C4ACO *1,*2,*3

Table 5-3 OCH XC Width for Non-ADD4 OTs (continued)

Rate	Baud Rate (Gbaud)	Encod-ing	FEC Mode	Wave shape	Channel width	OTs
50G (OTU4 Halfline)	32.5	BPSK	SDFEC-G2	Single Channel	50.0 (default), 62.5, 75.0	D5X500, D5X500Q, D5X500L *1,*2,*3
				Super Channel	50.0 (default), 62.5, 75.0	
				Alien	50.0 (default), 62.5, 75.0	
500G (250G/ OTU4Halfx5)	41.7	16QAM —250G	SDFEC-G2	Single Channel	62.5, 75.0	D5X500, D5X500Q, D5X500L *1,*2,*3
						LCI2000

- *¹: Single Channel
- *²: Super Channel
- *³: Alien

3

If the traffic is routed through ILAs and DGEs objects as in the example [Figure 5-27, “37.5 Ghz Frequency Band - Example of Network” \(p. 553\)](#), set ILAs and DGEs in the **PARAMETERS > OTHERS** tab. See [7.6 “Routing Constraints” \(p. 731\)](#).

Note that automatic routing is also supported without passing any constraints.

Click **DEPLOY** to create the connections.



Note: OCH XC width selection is not supported, that is, to reroute a connection with a different channel width (for example from 37.5 GHz to 50 GHz), delete the existing OTUk trail (of 37.5 GHz) and recreate an OTUk trail with the new channel width (of 50 GHz).

4

View the created connections in the **Infrastructure Connection** list.

1. Navigate to **OPERATE > Infrastructure Connections**
2. Select the **OTUk** connection
3. Click on the **360° view** icon

4. From the new window select the **Servers** tab

The **OMS** connections automatically created by the system, are displayed.

Note: The **Channel Width** parameter is displayed on the **Infrastructure Connections** page.

Figure 5-28 37.5 GHz - Occupied Frequency Channels

	Alarm ...	Operational State	Implementation Status	Service Rate	Connection Name	Protection	Frequency	From Node #1	From Port #1	To #1	⋮
<input type="checkbox"/>	M ↓	Commissioned	Completed	OTSig	narInfraOTSig_1_2 IR20-Si...	Unprotected	9365.000	IR20-Site1-1	OTSIG-1-13-1	IR2	
<input type="checkbox"/>	↑	Commissioned	Completed	OS	IR20-Site2-1/MCS-1-4-AD...	Unprotected	N/A	IR20-Site2-1	MCS-1-4-AD3	IR2	
<input type="checkbox"/>	↑	Commissioned	Completed	OS	IR20-Site1-1/MCS-1-4-AD...	Unprotected	N/A	IR20-Site1-1	MCS-1-4-AD3	IR2	
<input type="checkbox"/>	↑	Commissioned	Completed	OMS	IR20-Site1-1/IROADM-1-3...	Unprotected	N/A	IR20-Site1-1	IROADM-1-3-LI...	IR2	
<input type="checkbox"/>	M ↓	Commissioned	Completed	OT5	IR20-Site1-1/IROADM-1-3...	Unprotected	N/A	IR20-Site1-1	IROADM-1-3-LI...	IR2	

5

View the occupied slots for the 37.5 GHz crossconnect.

1. Navigate to **OPERATE > Infrastructure Connections**
2. Select the **OTUk** connection
3. Click the **three dots More... (⋮)** icon
4. Select **Structure**.

The **Structure** window is displayed with the occupied slots. For the 37.5 GHz frequency band the occupied slots are six, for 50 GHz it's eight slots and for 62.5 GHz it's ten slots. Each slot is 6.25 GHz.

Figure 5-29 37.5 GHz - Occupied Slots

Structure narInfraOTSig_1_2										
Connection Name	Service Rate	Alarm St	From Node #1	From Port #1	To Node #1	To Port #1	Total Slots	Used Slots	Free Slots	⋮
narInfraOTSig_1_2	OTSig Tunnel	IR20-Site1-1	OTSIG-1-13-1	IR20-Site2-1	OTSIG-1-13-1		6	0	6	
		1	2							



Note: When the system automatically allocates the centre frequency, it is based on the distance of 50 GHz from its neighbor. It is also possible to use frequency constraints to overwrite the centre frequency selection by system.

Optical Fiber

5.10 Transmission over fiber

Bi-directional transmission management on a single fiber

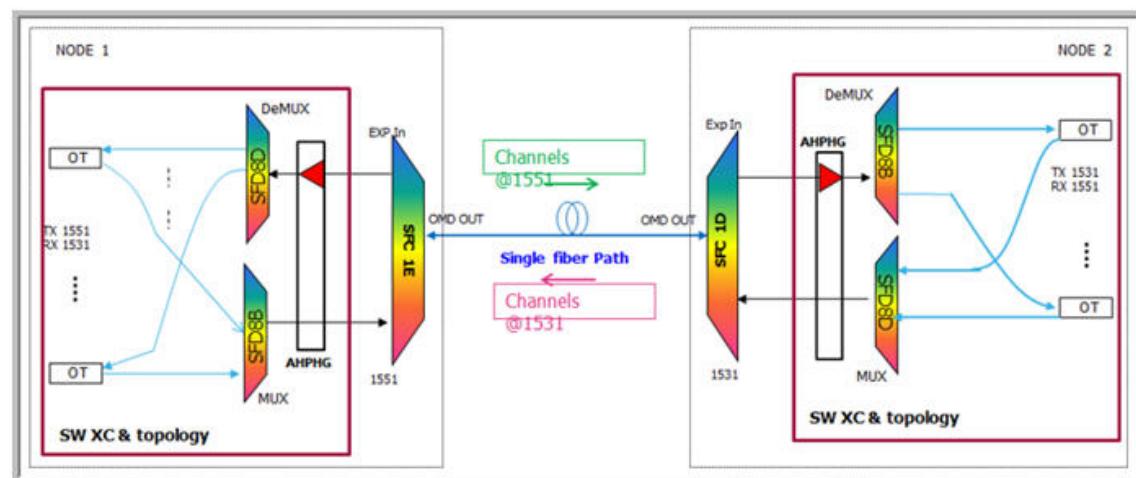
Bi-directional transmission is usually performed employing two optical fiber one for each direction. NFM-T platform, can manage *bi-directional transmission on a single fiber* for both **DWDM** and **CWDM**, to reduce the number of the fibers and the cards employed, additionally the OTS capacity is reduced by half. CWDM was already supported by NFM-T, while DWDM solution has been introduced with 14.2 release.

In a single fiber solution there is a single fiber for TX and RX channels, two different frequencies are used. Therefore, TX and RX ports on OT are set to two different frequencies. Bi directional transmission applies to **FOADM** application.

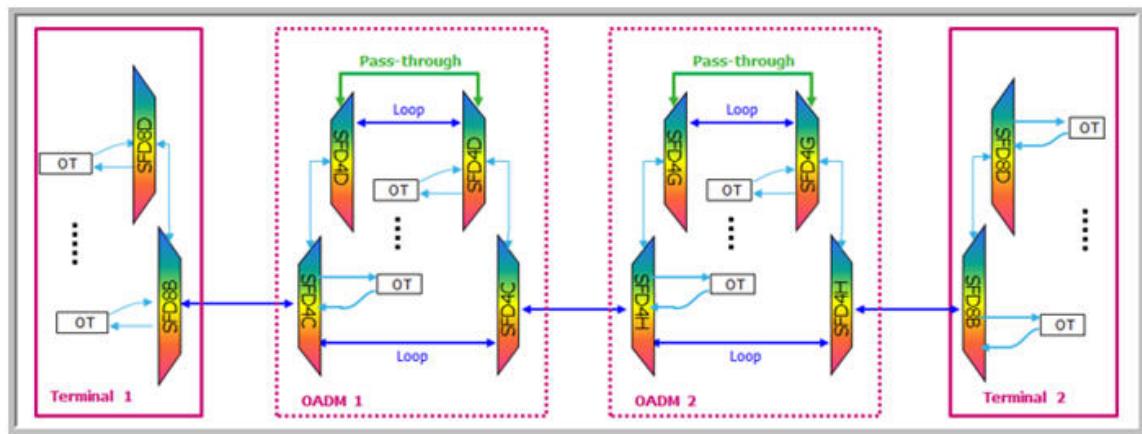
According on the type of multiplexing, NFM-T manages different types of configurations:

- support the **CWDM** single fiber for bi-directional transmission feature for 2-Degree FOADM, where the two SFCs on both ends are identical
- support the **DWDM** single fiber for bi-directional transmission feature for FOADM application with and without **optical amplifiers**, the latter configuration is used for short link.

The following figure shows an *amplified* configuration where the transmission is point-to-point over a single span.



A typical *unamplified* configuration is composed of two end terminals and two OADM sites, as showed in the following figure:



Additionally, bi-directional transmission feature is supported for CWDM-DWDM regeneration.

The above configurations are managed by the following type of shelves: **1830 PSS-4**, **1830 PSS-8**, **1830 PSS-16**, **1830 PSS-16II** and **1830 PSS-32**.

For long distance application, *Single fiber* configuration support the *multi span* transmission. This feature is supported by the following type of shelves: **1830 PSS-8**, **1830 PSS16II**, **1830 PSS-32** in **FOADM** configuration with the following OTs: 130SCX10, 130SNX10, 260SCX2, D5X500, 2UC400 and 1UD200.

Bi-directional transmission on a single fiber supports a multi spans scenario with **iROADM9R**, in which iROADM9R is used supporting both channel termination and optical pass-through.

The external Red/Blue filter is also supported. This component can be used instead of passive with defined band , blue band is defined as 1527nm-1546nm, Red band is defined as 1546nm-1564nm.

How to set and display the fiber mode

The selection between *Single fiber* and *Dual fiber* configuration is made during the creation of the physical connection. See [7.19.5 “Task: Create an Bidirectional physical OTS or OPS connection” \(p. 793\)](#)

The fiber configuration can be displayed in a dedicated column labeled **Span Type** in the physical connection data table, following the path **Operate > Physical Connections**.

Display a passive HW

Some network configurations require the employment of some passive HW components.

For some single fiber configurations, you can view these components as Y cable combining Red/ Blue channels, SFC passive filters or 3rd party passive filters like an icon, by using the **Routing display**. These objects, not being a real equipment objects, do not contain physical ports and do not support real topological connections. These objects are automatically discovered by the NFM-T but are not managed.

NE provides the NFM-T information if on an *OTS single fiber* link a passive HW is present. This information is elaborated at OTS creation.

5.11 Optical Line Protection (OLP)

OLP definition and working operation

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. Optical line protection 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 that based on the 1 + 1 scheme. See [4.7 “Optical Line Protection” \(p. 487\)](#) for more details.

5.12 OTS fiber characteristics limitations

Description

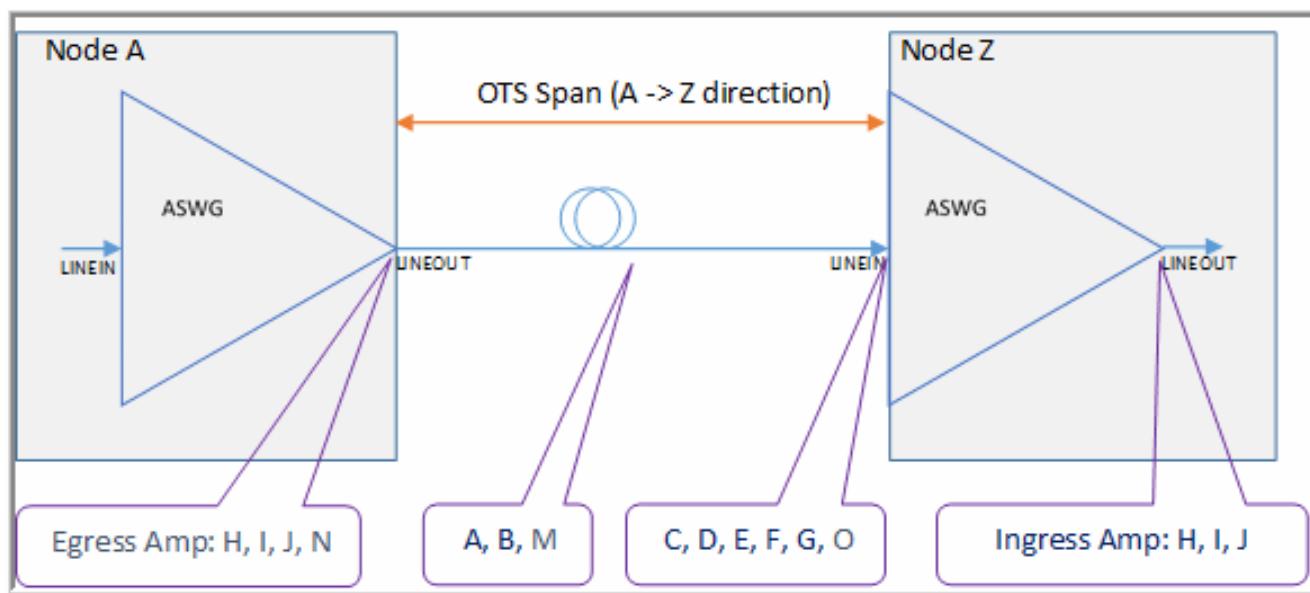
Refer to the set of configurations in this section which cover uni-directional, bi-directional, iROADM amplifiers.

Refer [Table 5-4, "Legend for the diagrams" \(p. 570\)](#) for mapping between OTS fiber characteristics items and parameters.

i **Note:** Performing a calculated span loss request through NFM-T while an APR-LINE condition exists on that specific span is an invalid action and will not provide actual information. The user must verify the available alarms on Port/Link before proceeding to check the calculated span loss.

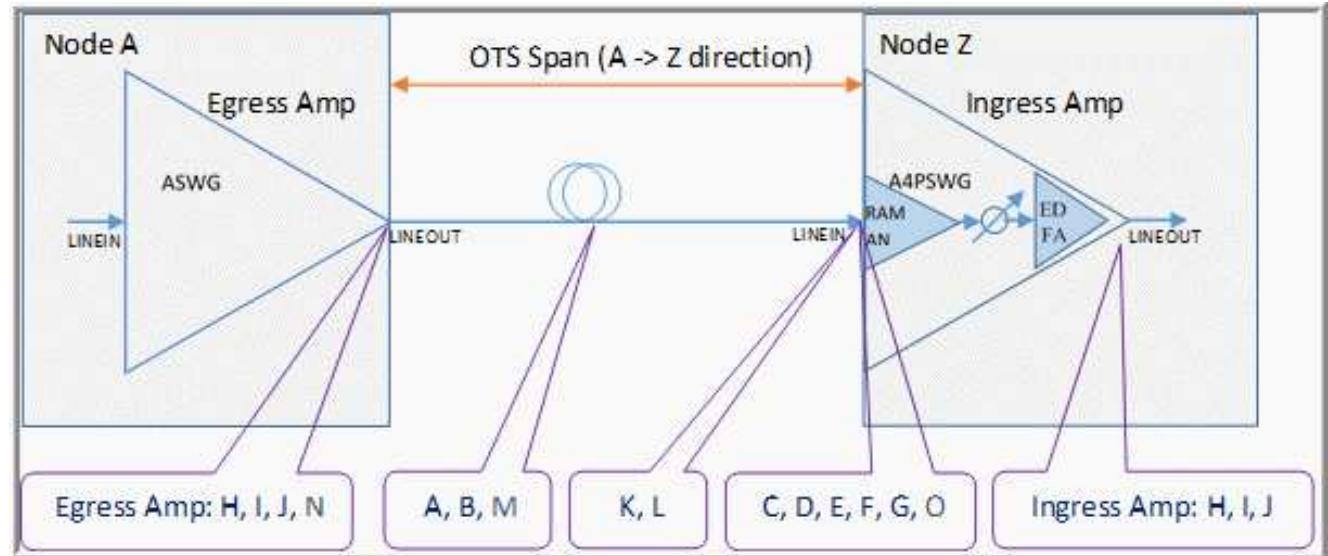
OTS span with uni-directional CDC-F Amps

Figure 5-30 OTS Span with two uni-directional EDFA amps (CDC-F Node Configuration)



OTS span with uni-directional CDC-F Amps: Egress ASWG and Ingress A4PSWG hybrid amps

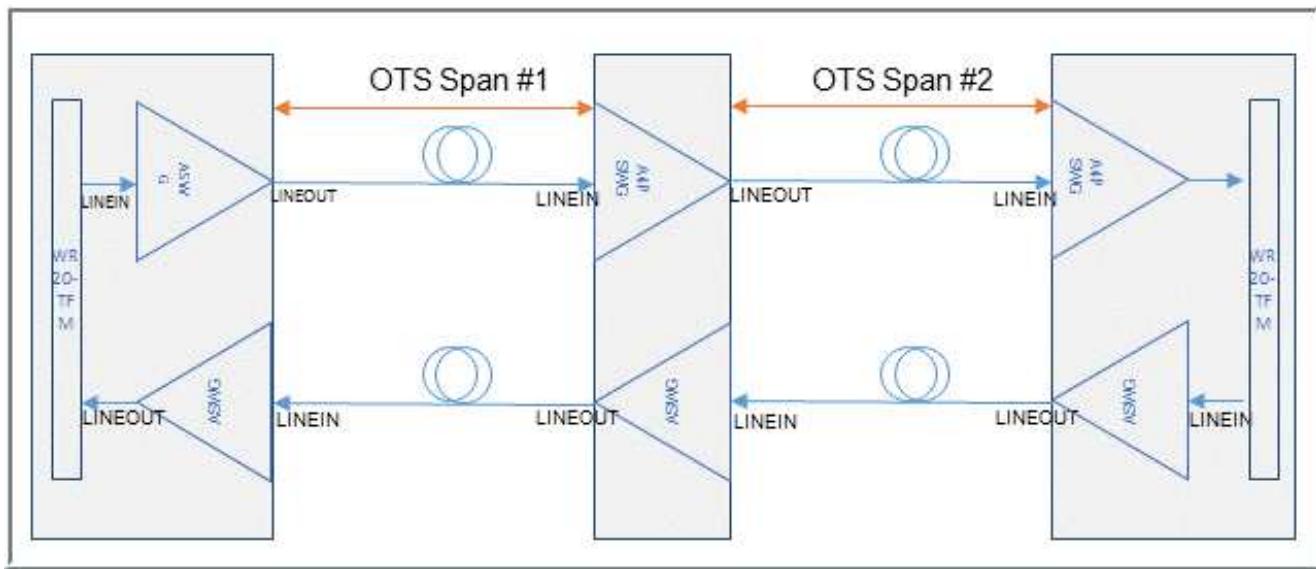
Figure 5-31 OTS span with EDFA and A4PSWG Hybrid Amp (CDC-F Node Configuration)



Typical CDC-F ROADM to ROADM route with one ILA in the middle

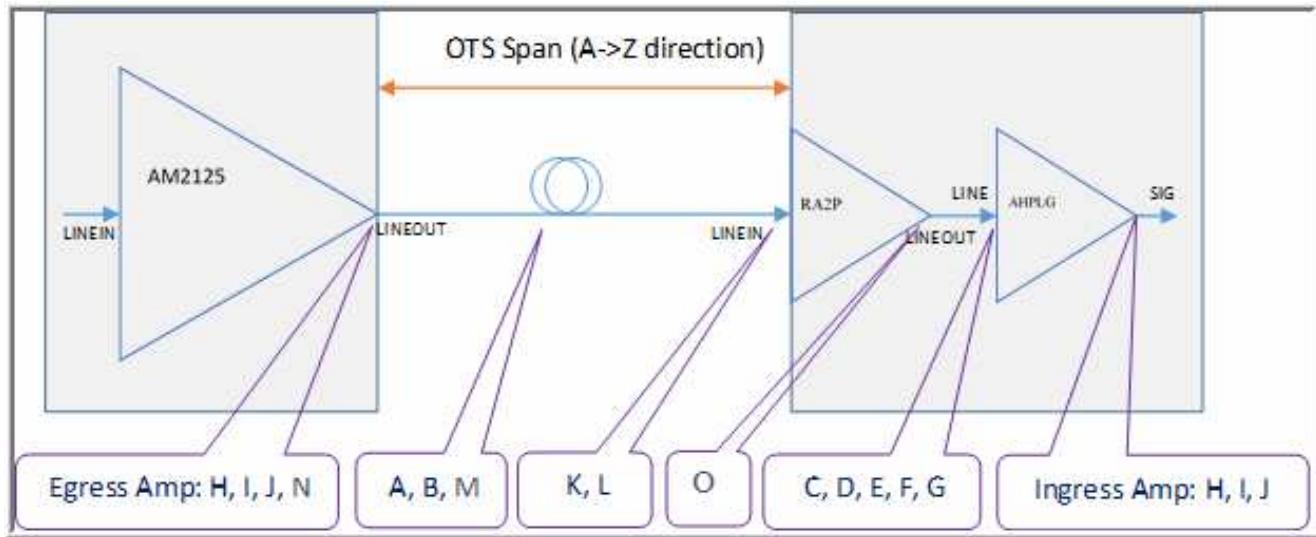
The methodology described above for a single direction of one span to longer optical systems consisting of multiple spans is illustrated in following picture. The OTS Fiber characteristics tab shows Ingress and Egress Amplifier (+ Raman, if equipped) gain properties, planned and measured loss values and fiber properties per each direction for each individual span.

Figure 5-32 Typical DWDM OMS section with ILA in the middle (CDC-F)



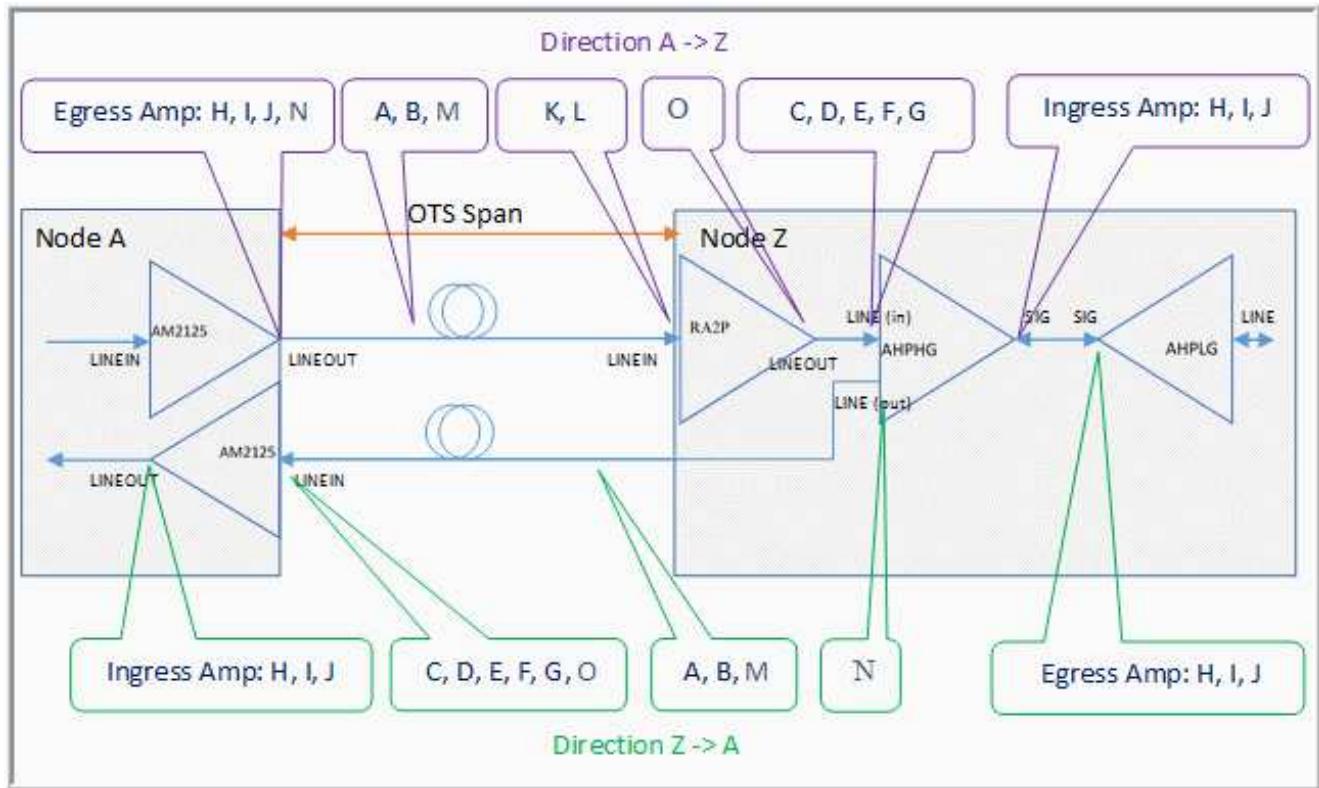
OTS span with uni-directional Egress and bi-directional Ingress with Raman

Figure 5-33 OTS Span with standalone Raman Amp and uni-directional EDFA amps



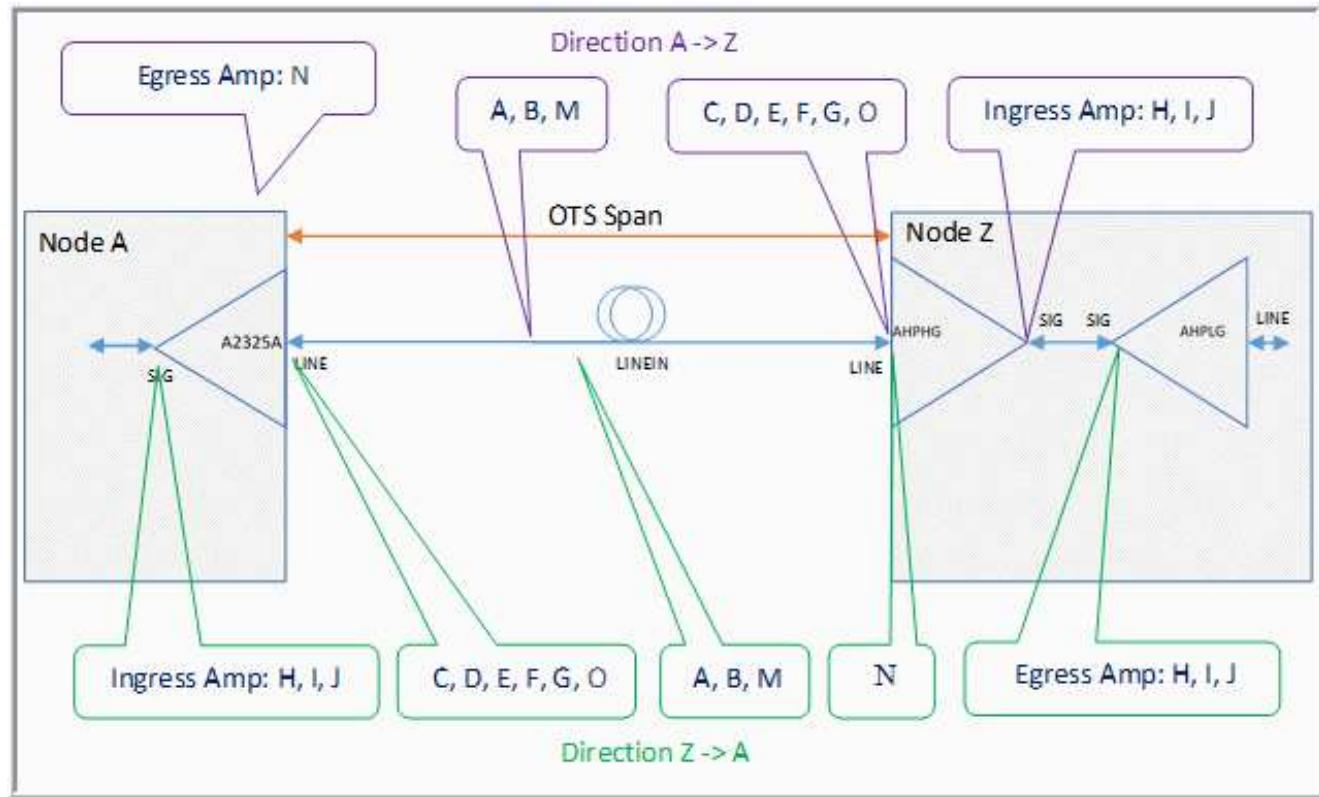
Interworking of uni-directional and bi-directional w/ Raman amps

Figure 5-34 OTS Span, interworking of uni-directional amps with Ingress/Egress bi-directional amps



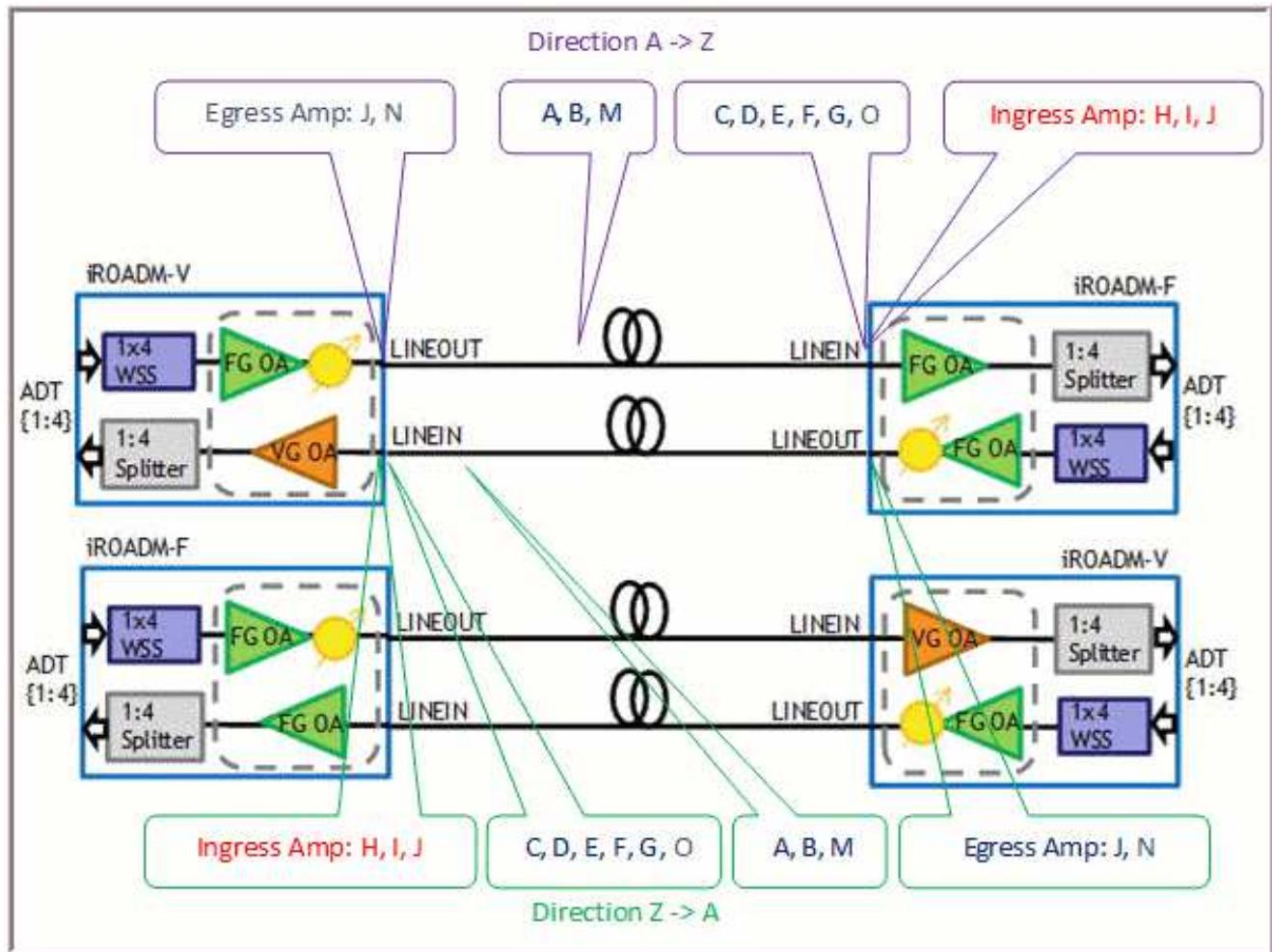
OTS span with bi-directional amps: one end with Ingress amp only (Egress not equipped) and other end Ingress & Egress amps

Figure 5-35 OTS Span, interworking of single Egress with Ingress/Egress bi-directional amps



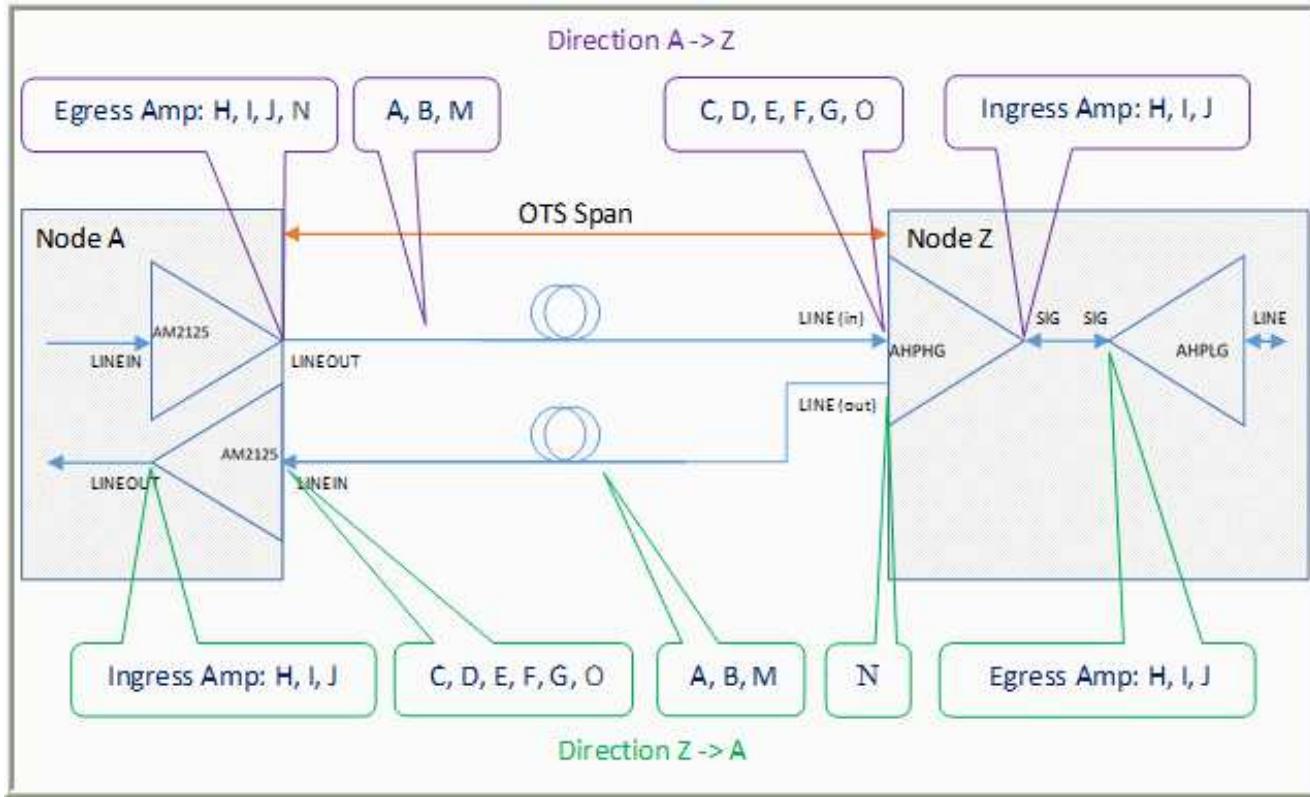
OTS span with iROADM cards

Figure 5-36 OTS Span, iROADMs



Interworking of uni-directional and bi-directional amps

Figure 5-37 OTS Span, interworking of uni-directional amps with Ingress/Egress bi-directional amps



Mapping between Fiber Characteristics parameters and MIB attributes

Table 5-4 Legend for the diagrams

Diagram reference	OMS displayed value	Amplifier Type	Port
A	Fiber Length	IROADM	LINEOUT
		Other than IROADM	None
B	Fiber Type	IROADM	LINEOUT
		RAMAN (RAXP) and Hybrid (A2P2125 and A4PSWG)	LINEIN
		Other	None

Table 5-4 Legend for the diagrams (continued)

Diagram reference	OMS displayed value	Amplifier Type	Port
C	Design Span Loss	All except standalone RAMAN amps (RAxP)	LINE, LINEIN
		Raman amps	None
D	Max Planned Span Loss	All except standalone RAMAN amps (RAxP)	LINE, LINEIN
		Raman amps	None
E	Min Planned Span Loss	All except standalone RAMAN amps (RAxP)	LINE, LINEIN
		Raman amps	None
F	Commissioned Span Loss	All except standalone RAMAN amps (RAxP)	LINE, LINEIN
		Raman amps	None
G	Measured Span Loss	All except standalone RAMAN amps (RAxP)	LINE, LINEIN
		Raman amps	None
H	Max Planned Gain	bi-directional amps	SIG
		Unidirectional amps	LINEOUT
		IROADM	LINEIN
		Hybrid Amps (A2P2125 and A4PSWG)	LINEOUT
		RAMAN	None*
I	Min Planned Gain	bi-directional amps	SIG
		Unidirectional amps	LINEOUT
		IROADM	LINEIN
		Hybrid Amps (A2P2125 and A4PSWG)	LINEOUT
		RAMAN	None*
J	Current Gain	bi-directional amps	SIG
		Unidirectional amps	LINEOUT
		IROADM	LINEIN
		Hybrid Amps (A2P2125 and A4PSWG)	LINEIN* (Raman Gain)
		Hybrid Amps (A2P2125 and A4PSWG)	LINEOUT (EDFA Gain)
		Standalone RAMAN (RAxP)	LINEIN*

Table 5-4 Legend for the diagrams (continued)

Diagram reference	OMS displayed value	Amplifier Type	Port
		IROADM	LINEOUT
K	Target Gain	Standalone Raman (RAxP) and Hybrid Amps (A2P2125, A4PSWG)	LINEIN
L	Achieved Gain	Standalone Raman (RAxP) and Hybrid Amps (A2P2125, A4PSWG)	LINEIN
M	Fiber Loss (exclude RAMAN Gain)	IROADM – IROADM	
		IROADM – non-IROADM	
		non-IROADM – IROADM	
		non-IROADM, without RAMAN	
		non-IROADM, with RAMAN	
N	Egress Power Out	IROADM	
		Non-IROADM	
O	Ingress Power In	IROADM	
		Non-IROADM without RAMAN	
		Non-IROADM with RAMAN	

5.13 Single fiber scenario with single OPS

Description

This function considers a specific network scenario based on a CWDM single fiber link with transponder to muxponder client channel. Since the muxponder client doesn't support cross -connections for CWDM, this scenario is managed creating two OPS links between client muxponder and transponder lie port over single fiber link. NFM-T creates uni-directional OPS/OS connections between LINE to CLIENT ports of the OT packs.



Note: Once the OPS is deleted from database, on discovering the OPS through the function **External discovery of physical link**, it is necessary to do a port synchronization to discover all the connections riding on it.

Scenario setup

To setup a single fiber connection with single OPS follow the steps:

1

Create a physical connection. Select following parameters:

- **Connection Type**=2 Ended Split bi
- **WDM Connection Type**=OTS
- **Span Type**=Dual Fiber
- Assign the four ports to be used.

2

Modify the Signal Rate using the EQM application.

Follow the path **Operate > Equipment Manager**, modify the link to Signal Rate=OPS.

We have now two uni-directional OPS links created.

3

The OTUk channel/ODUk connections are automatically discovered once the two uni-directional OPS links created.

4

Selecting the infrastructure connection in the list displayed following the path **Operate > Infrastructure Connections**, in the client tab, the two OTUk channel has two separated frequencies.

5

Create the ODUk connection manually.

5.14 Single Fiber on S4X400

Description

The single fiber configuration is supported on S4X400H packages. The service/infrastructure creation provisioning work flow uses the template and structure OTSiG Tunnel and Service. The network discovery is also available for this configuration. The support is for DWDM frequencies (CDWM is not supported).

Profiles supported are: 1, 2, 3, 4, 5, 8 and 15.

Items supported for single fiber configurations are UnKeyed wavekey type.

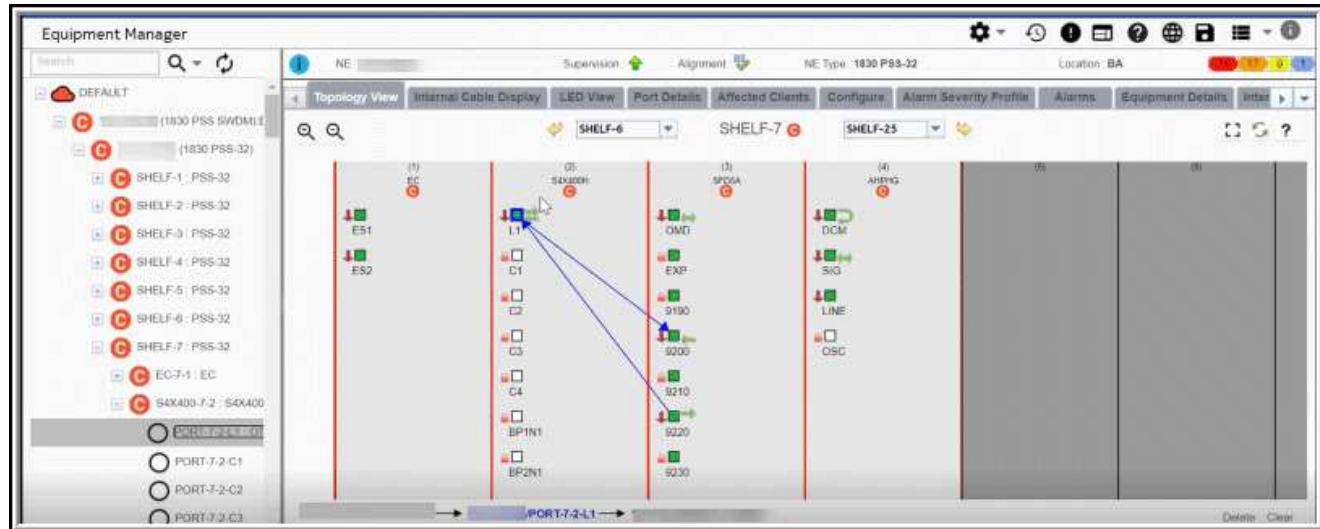
Example flow and configuration

On the NE, OT and Filter packs are configured. To cover single fiber connectivity, use two frequencies and setup two connections from the S4X400 to cover the transmission and receive frequencies.

1

From the Equipment Manager application on the **From NE** create a uni-directional OS connection between the line port and one of the frequencies (transmission), then another OS connection between the other frequency and the line port (receive).

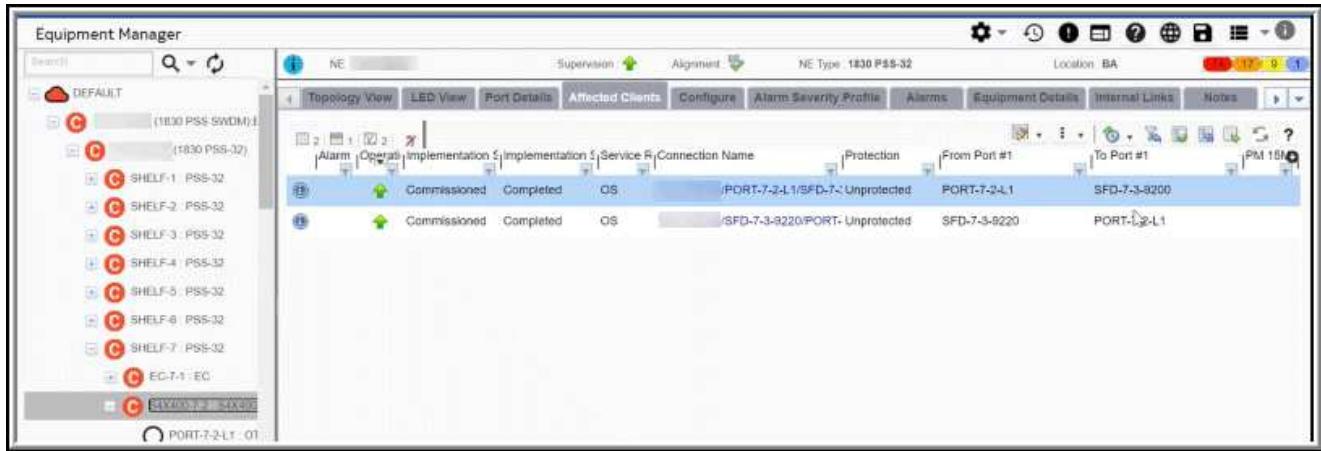
Figure 5-38 Single Fiber on S4X400 - OS Connections - Topology View



2

The two uni-directional OS links are displayed.

Figure 5-39 Single Fiber on S4X400 - OS Links



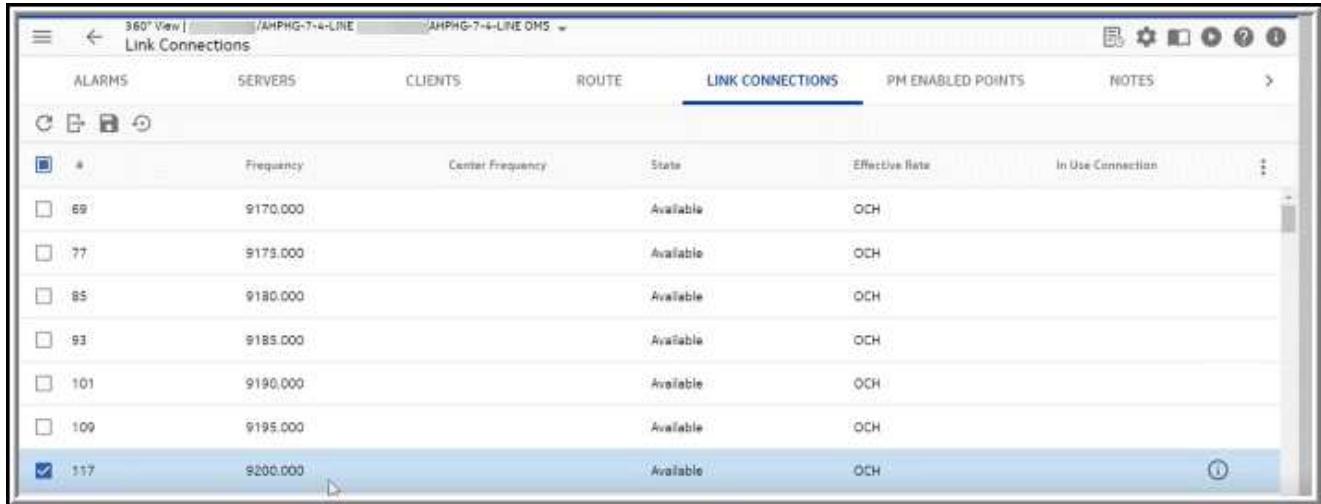
3

Then on the **To NE** we create the uni-directional OS connections, the opposite as on the From NE, the transmit is the receive and the receive is the transmit.

4

Create a Physical connection with **WDM Connection Type = OTS** and **Span Type= Single Fiber**

Figure 5-40 Single Fiber on S4X400 - Physical Connection - Link Connections



5

Create a connection.

From the WebUI follow the path **DEPLOY > New Service/Infrastructure Connection**.

- Select the template **/Best Practices/Infrastructure Trail/Unprotected with ODUk or OTSiG Tunnel**
- Click **Deploy** ()

6

For the connection, insert the following parameters

As general parameters:

- Service Rate Type: Trail
- Rate: OTSig Tunnel
- From and To Nodes: the two nodes we are using for the single fiber connection.

In the Connection Characteristics panel select:

- Provisionable Wave Key: Unkeyed
- Insert the name for the connection.

In the Optical Line Characteristics panel select:

- Choose a Profile Number from the list.
- Depending on the chosen profile, the Channel Width selection is different. You can choose the desired width for the connection.

Click **DEPLOY** to create the connection.

The created connection has picked as servers all the OS, OMS and OTSig links.

Figure 5-41 Single Fiber on S4X400 - Created Connection - OCH Links



#	Frequency	Center Frequency	State	Effective Rate	In Use Connection	⋮
101	9190.000		Available	OCH		
109	9195.000		Alternate Used by In Effect	OCH		
117	9200.000	Center	Used in InEffect/Impleme...	OCH	SF-DEMO	
125	9205.000		Alternate Used by In Effect	OCH		

For each frequency three LCs are reserved in the connection creation.

Figure 5-42 Single Fiber on S4X400 - Created Connection - LCs Reserved

<input type="checkbox"/> 141	9215.000	Alternate Used by In Effect	OCH
<input type="checkbox"/> 149	9220.000	Used in InEffect/Impleme...	OCH SF-DEMO
<input type="checkbox"/> 157	9225.000	Alternate Used by In Effect	OCH

Assigning frequency on the NE - important considerations

Assigning frequency on the NE after the OTSIG tunnel creation in the Single Fiber scope, is not reflecting at Tunnel level for point to point scenario.



Note: bi-directional optical Power, Power monitoring, is not applicable for OTSIG trail in the point to point configurations for the single fiber, as there isn't any OCH cross-connection on the NEs. Therefore the navigation from the OTSIG tunnel to OTSIG trail for Point to point scenario is blocked

When direct SingleFiber OPS is created between S4X400—S4X400

- Two UNI OPS Links are shown from **Nodes > Impacted Connections Tab** and one four ended OPS in **Physical Connections** window
- Frequency at OTSIG Trail/OTSIG Tunnel level is displayed as **N/A**
- The **TX Frequency** and **RX Frequency** columns in Physical Connections data table show the TX and RX frequencies assigned to both End Ports and **Only** these columns should be used to refer the frequencies in Direct OPS scenario.
- For checking the frequency on the E2E routing display of the Direct OPS/OTSIG connections on top of it, user has to navigate from **Impacted Connections tab** by clicking on individual UNI OPS Links only. No other Link's E2E Routing Display show the Frequency.

5.15 bi-directional 3R Support for Control Plane Without Re-fibering

Overview

Prior to NFM-T Release 19.9, uni-directional cabling was supported, where uni-directional 3Rs are cross-cabled to maintain symmetric connection in the mesh. This required the users to re-cable the fibers when using an OT in Add/Drop Mode to Regen Mode and vice-versa.

Currently, this feature supports the usage of bi-directional fibers (symmetrical fibers) between OT packs (D5X500 variants) and filter (MCS) packs, with the OT pack having a minimum of two line ports. These two line ports implicitly create port pair for 3R when it is set to Regen Mode from Add/Drop Mode and vice versa. In case of bi-directional configuration the ports have to be selected on the same card. The cross-connects are automatically created.

Note:

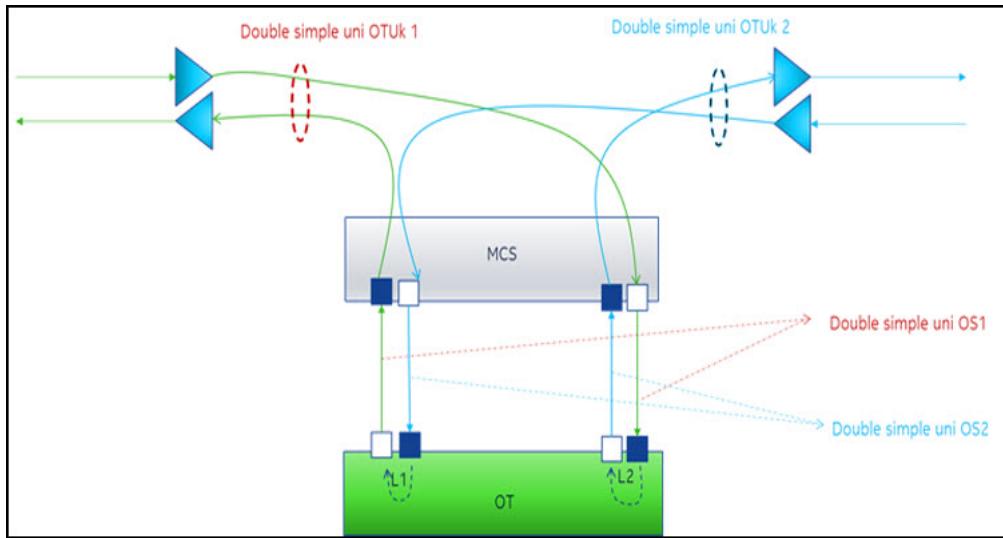
- For Managed Plane and Control Plane connections, ensure to set the **Operational Mode** to **Regen** (before creating any internal links), to make the Line port (L1 or L2) as signal regenerating port.
- If you set the **Operational Mode to Regen** from **Add/Drop** or **Add/Drop to Regen**, delete the internal OS connected to the Regen ports from the Equipment Manager page or the NE WebUI page and recreate it. However, you do not have to re-fiber physical cable for bi-directional 3R.

This feature is applicable for D5X500, D5X500Q, and D5X500L cards with CDC any-directional configurations for Control Plane connections. With bi-directional fiberizing, the users need not re-cable the fibers when using an OT in Add/Drop Mode to Regen Mode and vice-versa.

If D5X500 is 3R and bi-directional cabled, implicitly the partner port is the other line port of the D5X500 card.

i **Note:** Bi-directional cable is supported from R19.9. So if the user has already created OS or have services on this OS in cross-cable way, the user must delete all the old connections including OS and then change the cable between OT packs and the filter packs. That is, the user must re-fiber physical cable from cross-cable to bi-directional cable.

Figure 5-43 bi-directional 3R support for control plane without re-fibering



Before you begin

Ensure that the D5X500 card is assigned as 3R by EPT/NFM-T.

Task: to manage 3R support for control plane without re-fibering

The steps to manage 3R support for Control Plane without re-fibering are:

1

In the **OPERATE > Equipment Manager** window, perform the following operations:

1. In the **Configure** tab, provision the cards and ports.
2. Select the Line port (L1 or L2). In the **Line Details** tab, set the **Operational Mode** to **Regen** or **Add/Drop**. Click **Modify**.

Note:

- Ensure to set the **Operational Mode** to **Regen** (before creating internal links), to make the Line port (L1 or L2) as signal regenerating port.
 - If the in L1 port, the L2 port is also automatically set to **Regen** mode. Similarly, if the **Operational Mode** is set to **Regen** in L2 port, the L1 port is also automatically set to **Regen** mode.
3. In the **Topology View** tab, create four uni-directional links or two bi-directional internal link between D5X500 L1 and L2 port with the MCS port.

Result: The OTN discovers two double uni-directional OS connections based on either four uni-directional TL links from the NE or two bi-directional topological links on the NE.

The bi-directional cable is displayed in the **Used Ports** tab of **OPERATE > Nodes** page.

2

In the **OPERATE > NPAs** page, perform the following operations:

1. Create an NPA and assign TL links to NPA.
2. In the **Links** tab, unlock the TL links.
3. In the **3R** tab, click the plus icon to create 3R.
4. In the **3R Creation** window, select the applicable Node and the L1 and L2 line ports.
At 3R creation, the user must assign the two ports of the same card as 3R ports.
5. Click **Deploy**.

Result: The selected node and the line ports to create a 3R are added, which can be used as a constraint during infrastructure creation.

3

Navigate to **DEPLOY > New Service/Infrastructure Connection**. Deploy an ASON Routed ODU4 connection with 3R as the constraint.

Note: Both bi-directional and uni-directional (which is already supported) can be used as a Routing Constraint in the same Infrastructure connection.

Result: The connections are displayed in the **OPERATE > Infrastructure Connections** page or **OPERATE > SNCs** page.

4

Select **Operate > ASON SNCs > Routes** tab, to view the start and the end points of the route.

Result: The **Routes** tab displays the **Nominal Route** and the **Current Route** details.

Figure 5-44 Nominal Route and Current Route with 3R Support for Control Plane

Nominal Route		Current Route	
Resource	Type	Restored Time	Type
Main		13/06/2019 20:46:56	4
SVT-L0-SITE3/D5X500-1-2-L2	9300.000	SVT-L0-SITE3/D5X500-1-2-L2	9250.0
AutoDisc-SVT-L0-SITE3/MCS8-16-MCS-9-5-	9300.000	AutoDisc-SVT-L0-SITE3/MCS8-16-MCS-9-5-	9250.0
SVT-L0-SITE3/MCS-9-5-AD14	9300.000	SVT-L0-SITE3/MCS-9-5-AD14	9250.0
SVT-L0-SITE3/ASWG-7-2-LINEIN	9300.000	SVT-L0-SITE3/ASWG-7-2-LINEIN	9250.0
SVT-L0-SITE3/ASWG-7-3-LINEOUT-SVT-L0-	9300.000	SVT-L0-SITE3/ASWG-7-3-LINEOUT-SVT-L0-	9250.0
SVT-L0-SITE4/ASWG-7-2-LINEIN	9300.000	SVT-L0-SITE4/ASWG-7-2-LINEIN	9250.0
SVT-L0-SITE4/MCS-9-5-AD3	9300.000	SVT-L0-SITE4/A4PSWG-7-6-LINEIN	9250.0



Note: 3R cross-cable port pair and bi-directional 3R ports on the same NE in the same connection is not currently supported.

END OF STEPS

Additional features

5.16 Additional features

Introduction

This part of the chapter includes a list of additional features supported by the NFM-T Platform.

OTM-0.1 (OTU1) Interface support for 24ANMB

The existing 24ANMB pack of the 1830 PSS-OCS has an OTU1 client support, where a set of new SFPs are provided.

The feature of this pack, is applicable with 1830 PSS-36 and 1830 PSS-64 shelves.

The support of OTM-0.1 client signal on 24ANMB pack, represents a new client type with respect to previous releases.

This pack supports OTM-0.1 with the following feature set:

- Support of pluggable SFPs and DWDM SFP for FOADM applications.
- Interoperability with 4DPA4 and 4QPA8.
- Support of ODU1 inside OTU1/OTM-0.1 line signal (un channelized) or 2x ODU0 inside OTU1/OTM-0.1 (channelized).
- Support of GCC0 and GCC1 to manage a remote 1830 PSS NE hosting 4QPA4 and 4QPA8.
- 1+1 ODUk protection for FOADM applications as protection client side.
- Support of STM16/OTU-1 BIDISFP.

The cross-connect rate, XC and SNCP, are ODU1 and ODU0.

This client signal only interwork with itself, and all of the GbE client applicable configurations are supported for Managed Plane, also protected and unprotected.

Facility and Terminal loopbacks are also supported.

Next figures aim to show the possible network scenarios applicable with the acceptable client signals.

Figure 5-45 24ANMB – OTU1 Client, Managed Plane

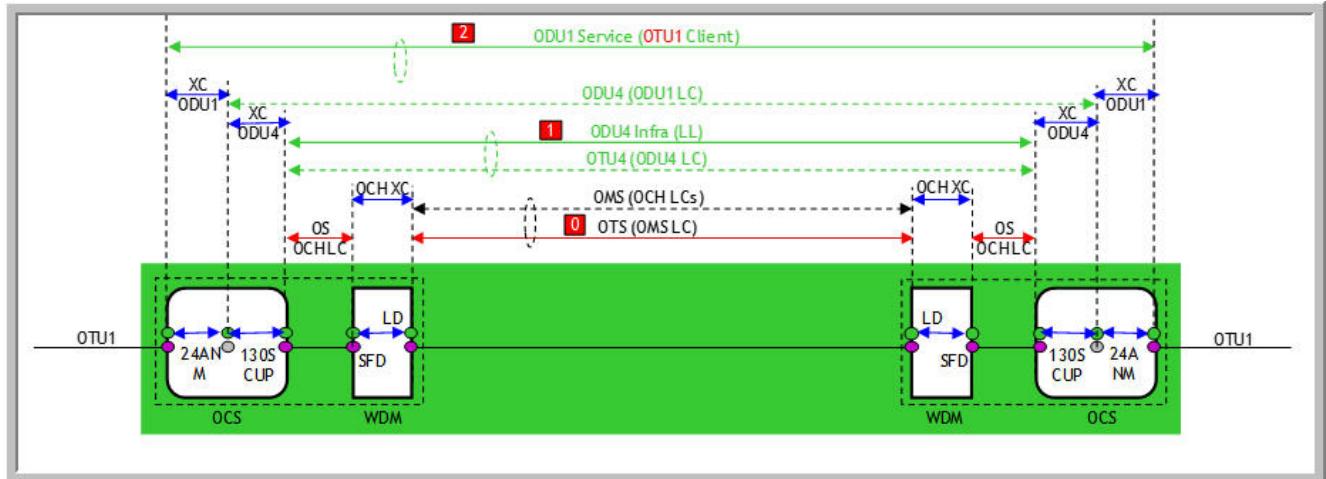


Figure 5-46 24ANMB Protected – OTU1 Client, Managed Plane

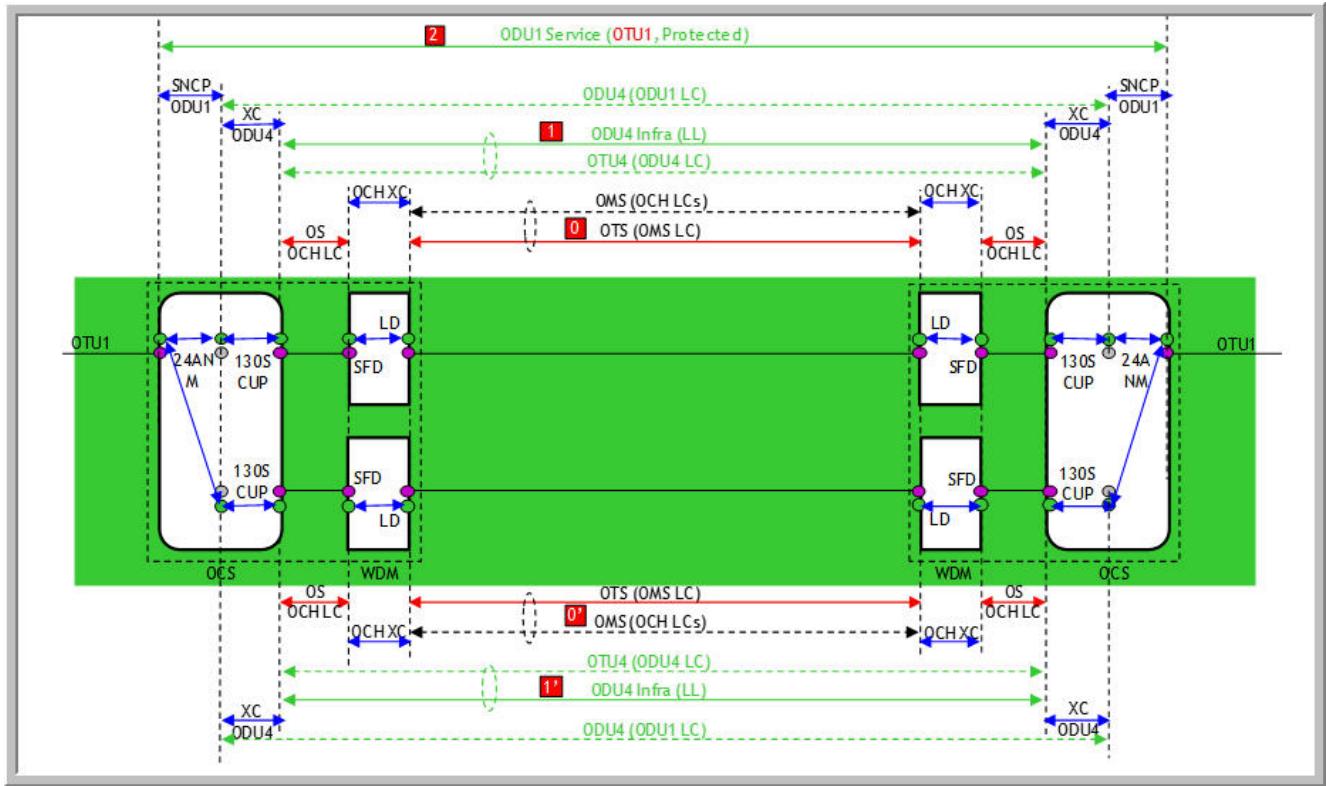
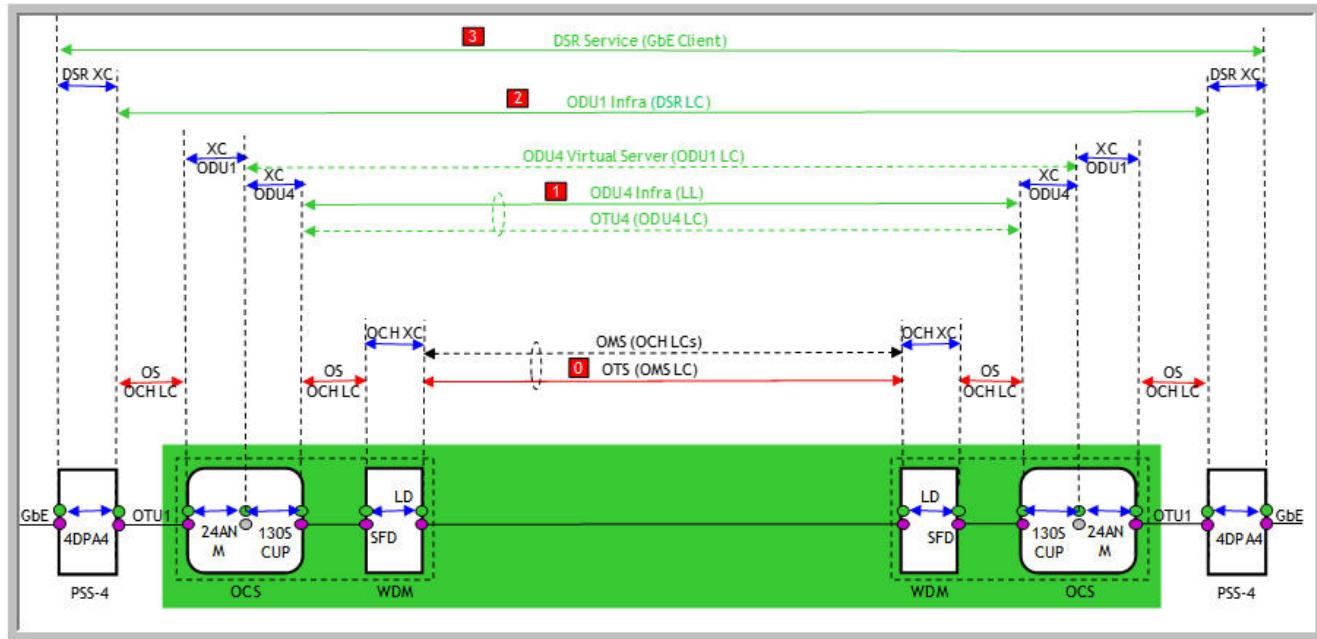


Figure 5-47 24ANMB Interworking 4DPA4 via OTU1 – GbE Client, Managed Plane



The 4DPA4, refers to the following client signals.

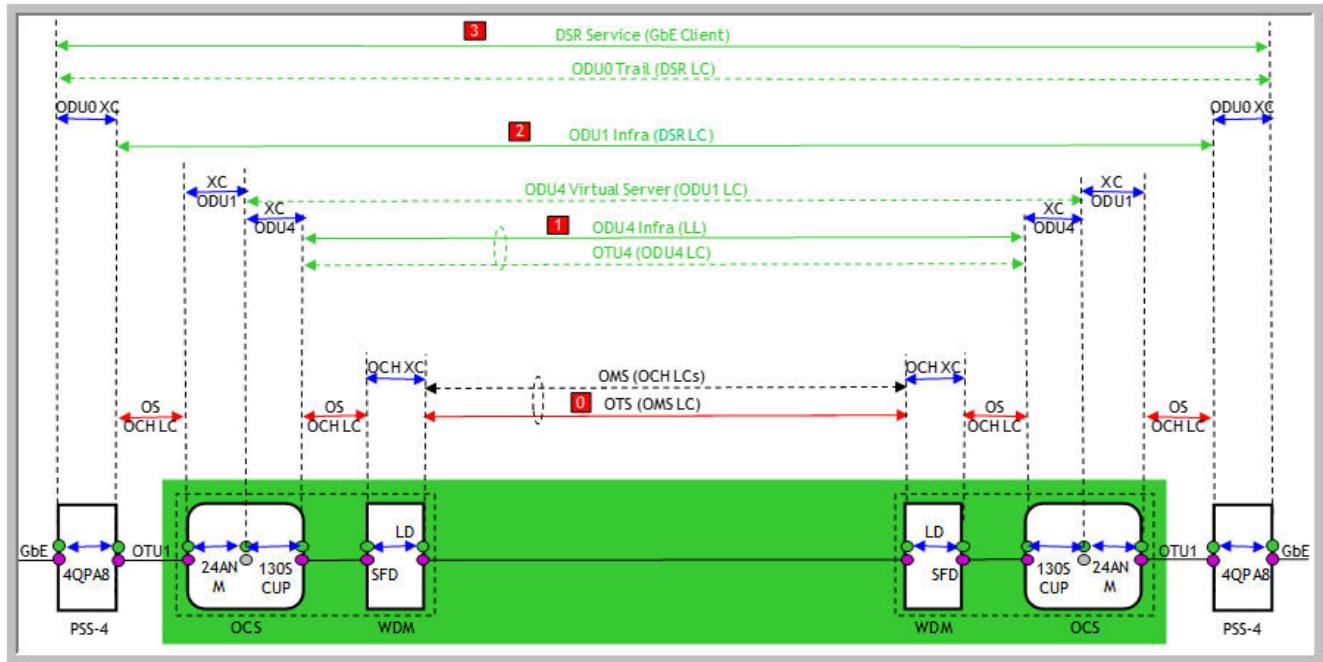
As FlexMUX:

- 1 GbE
- DVBAISI
- FC100
- FC200
- FE
- HDSDI
- OC3/STM1
- OC12/STM4
- OC48/STM16
- SDSDI

As Dual Trans:

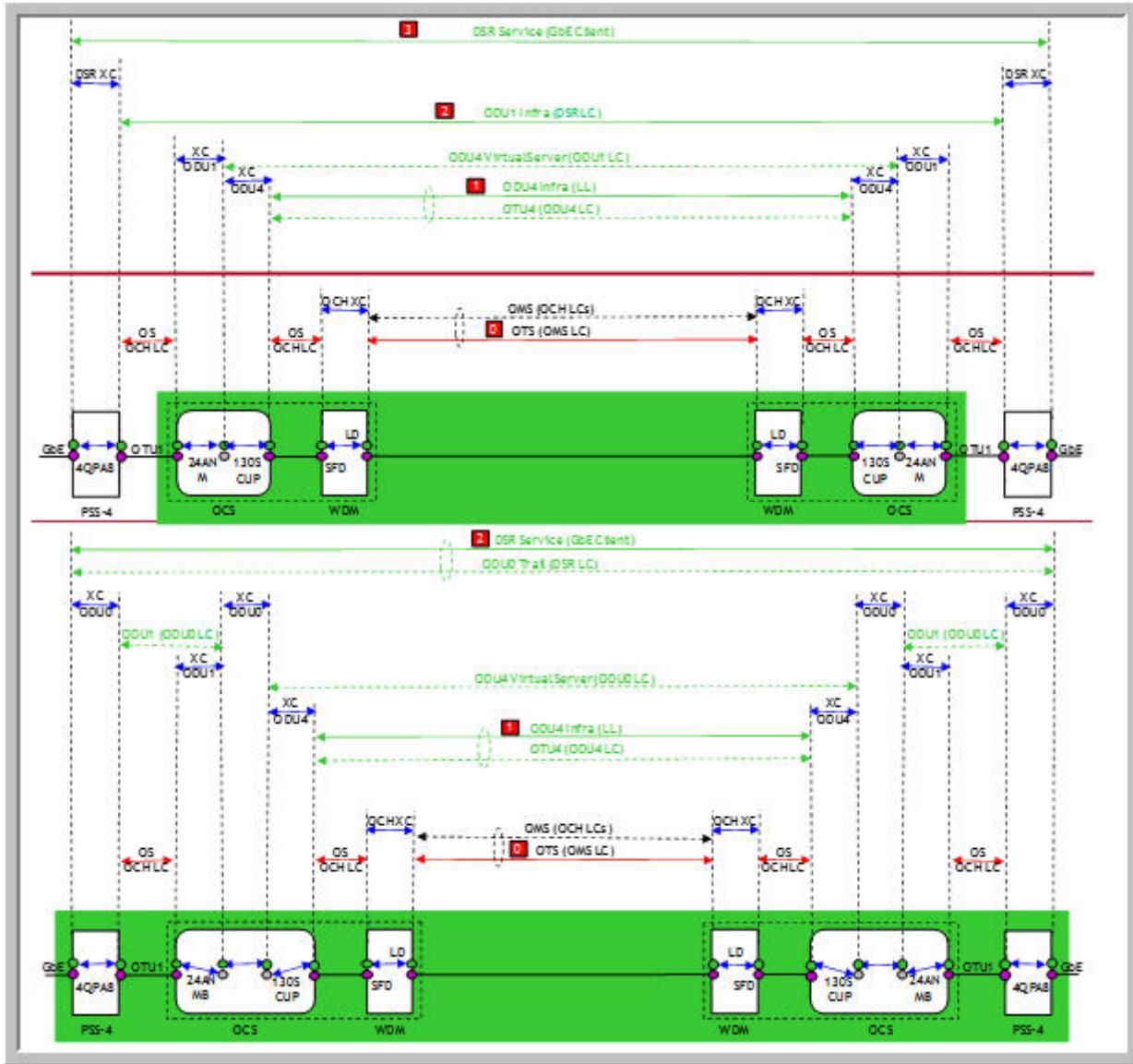
- FC400

Figure 5-48 24ANMB Interworking 4QPA8 via OTU1 – GbE Client, Managed Plane



The 4QPA8 client signal rate is 1 GbE (ODU0).

Figure 5-49 24ANMB Interworking 4QPA8 via OTU1 – GbE/FE/OC-3/12/18 Client, Managed Plane



The 4QPA8 client signal rates are:

- 1 GbE (OPTSG)
- FE (OPTSG)
- OC3/STM1 (OPTSG)
- OC12/STM4 (OPTSG)
- OC48/STM16 (OPTSG)

100 G Coherent CFP for 112SDX11

The NFM-T, is able to manage the 100G Coherent pluggable CFP for 112SDX11 line port in order to support the 88 x 100 G channel in FOADM and ROADM.

This represents a new CFP pluggable module 100GBASE-LR4 with the OTU4 colored DWDM 88 channel interface.

This interface is supported by the following configurations:

- FOADM: CFP with colored OTU4 to SFD44/ITL or SFD5/8.
- ROADM: CFP with colored OTU4 to SFD/ITL/WR8-88A or WR8-88AF packs.
- TOADM: CFP with colored OTU4 to CWR8 or CWR8-88 packs.
- IROADM: CFP with colored OTU4 to iROADMF or iROADMV or iROADM9M packs.

When considering this pluggable CFP, the supported shelves (112SDX11) are: 1830 PSS-32, 1830 PSS-16, 1830 PSS-8, 1830 PSS-4.

The following rules should be followed when the 100 G coherent CFP is used on the 112SDX11 line side:

- Only L1 port can be used while ports from L2 to L4 are not available for use.
- Optical channels: 88 DWDM channels, [9170.000-9605.000], delta=5.000.
- TX and RX share the same laser, and their frequency should be the same. L1 FEC mode: HPFEC, RSFEC.
- OCH XC: from 112SDX11 L1 to LD port for both bi-directional LDs and uni-directional LDs, or SFD/OMD for an NE without LDs, or ITLB for an NE without LDs.
- Port ID on L1 of OTU4 as contained CTPs.
- No line side protection is supported while OMSP is supported.
- FM: same as other DWDM OTU4/ODU4
- PM: same as other DWDM OTU4/ODU4
- Loopback on L1: facility and terminal loopback are supported

Managed plane configurations is supported.

The 112SDX11 pack supports different client signals according to different criteria.

These values refer to main client signals:

- FC1600.
- 40GbE.
- 10GbE.

The following instead refer to 112SDX11 pack client signals with low priority:

- FC1200
- FC800
- FC400
- OTU2

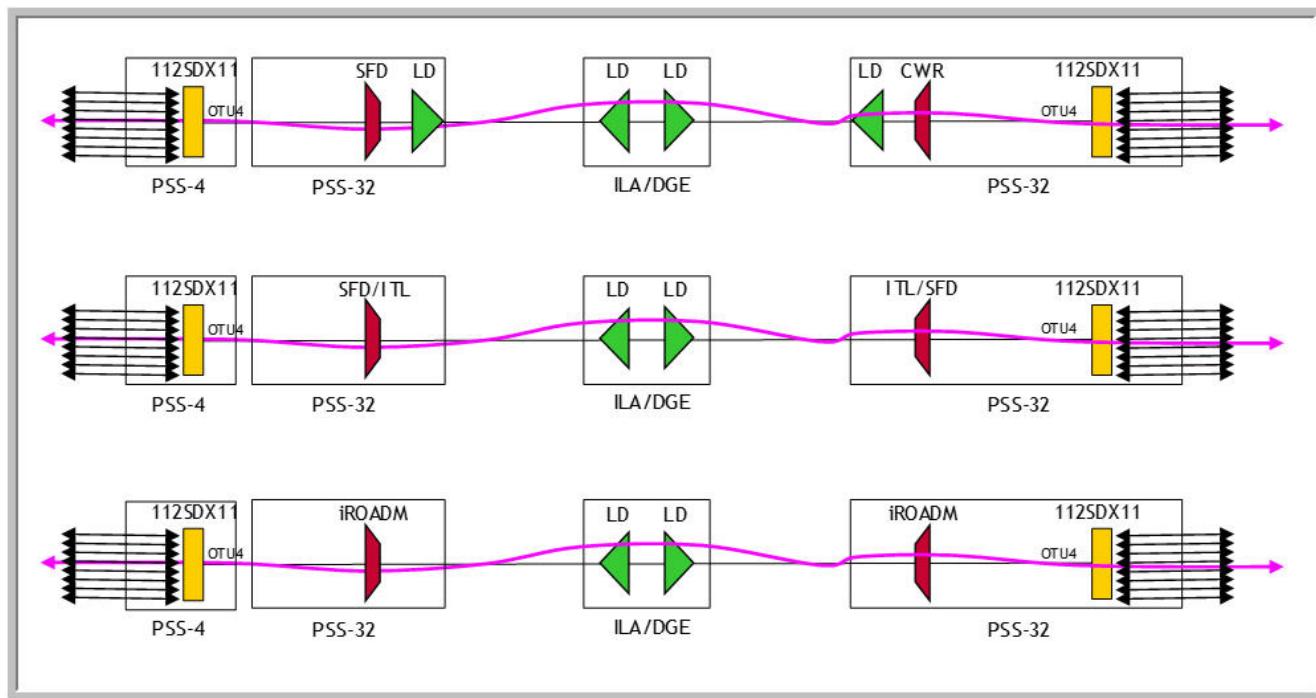
- OTU2e
- OTU1f
- 100 GbE via fan-out cable, CBR10G3
- DDR

The coherent CFP itself does not support wave key service.

If keyed services are envisaged, MVAC must be used.

Basically, the configuration refers to unkeyed services as shown by next figure.

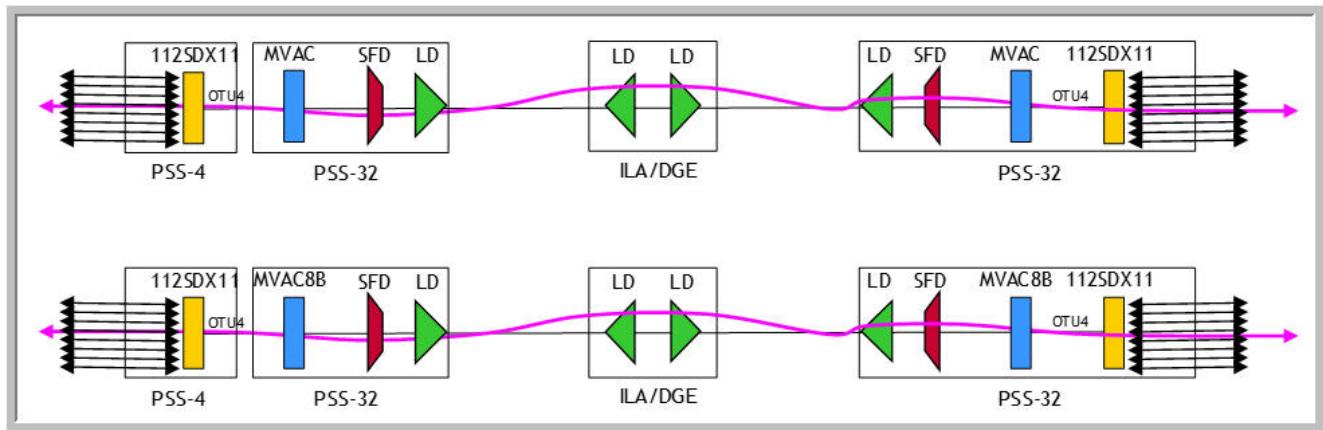
Figure 5-50 112SDX11/OTU4 coherent colored CFP to SFD/CWR/WR/iROADM



For keyed services, MVAC or MVAC8B packs need to be used, since the 112SDX11 pack itself does not support this type of services.

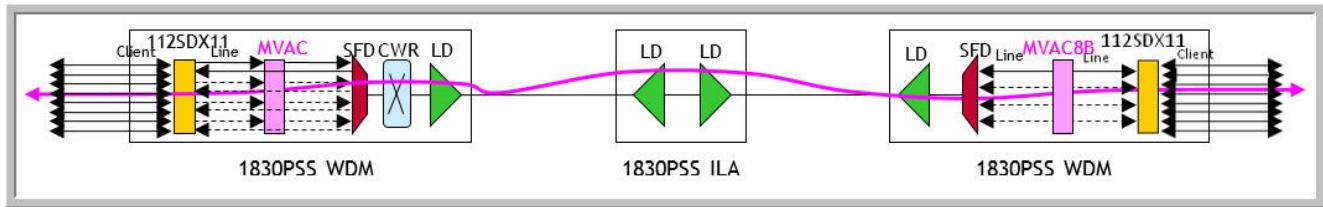
Refer to the following figure for details.

Figure 5-51 112SDX11/OTU4 coherent colored CFP to MVAC or MVAC8B keyed services



It is possible to support also scenario with MVAC and MVAC8B used at the A node and Z node separately as shown in the following figure.

Figure 5-52 112SDX11/OTU4 coherent colored CFP to MVAC and MVAC8B keyed services



100GBASE-ER4 40km on 1AN100 and 260SCX2

The NFM-T supports Dual Rate CFP2, Rate 100 GBASE-ER4 and 4L1-9C1F, client pluggable modules for 260SCX2 and 1AN100G packs.

The extension ER4, defines four optical lanes with capability to reach up to 40km using single mode fiber.

This is a new 4 x 25 G Dual Rate CFP2 pluggable module, for 100 GbE and OTU4 client signal rates.

Each lane of these four, provides 25.78125 Gb/s data rate equivalent to 100Gb client signal.

In case of OTU4 client, data rate becomes 27.9525 Gb/s equivalent to 28Gx4.

This pluggable unit can be used on different shelf types depending on packs as indicated:

- 1830 PSS PHN: 1830 PSS-32, 1830 PSS-16, 1830 PSS-8, 1830 PSS-16II shelves (260SCX2)
- 1830 PSS OCS: 1830 PSS-36, 1830 PSS-64 shelves (1AN100G)

Next figures aim to show the possible configurations applicable to 260SCX2 and 1AN100G packs with 100 GbE and OTU4 clients.

Figure 5-53 260SCX2 with CFP2 (C2CER4DC) – 100 GbE Client, MP

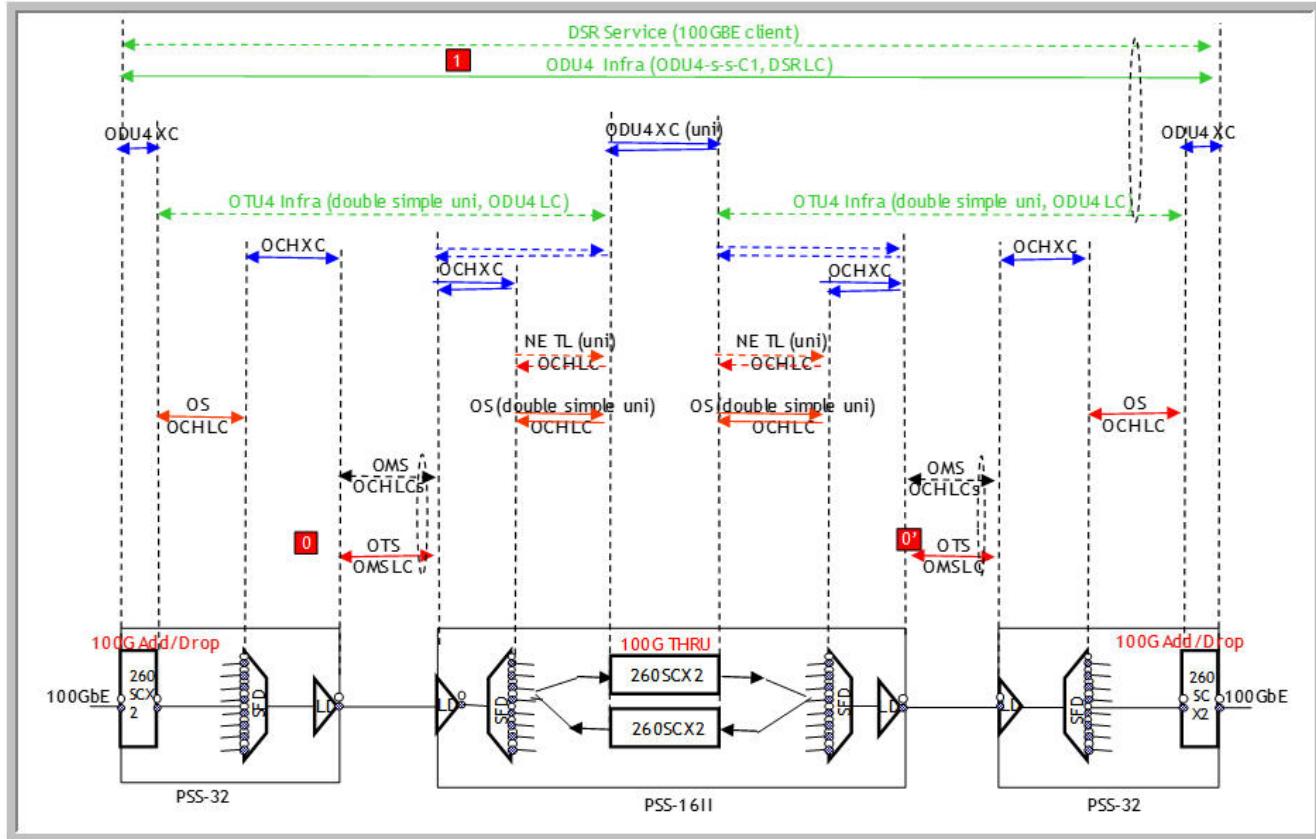


Figure 5-54 260SCX2 with CFP2 (C2CER4DC) – OTU4 Client, MP

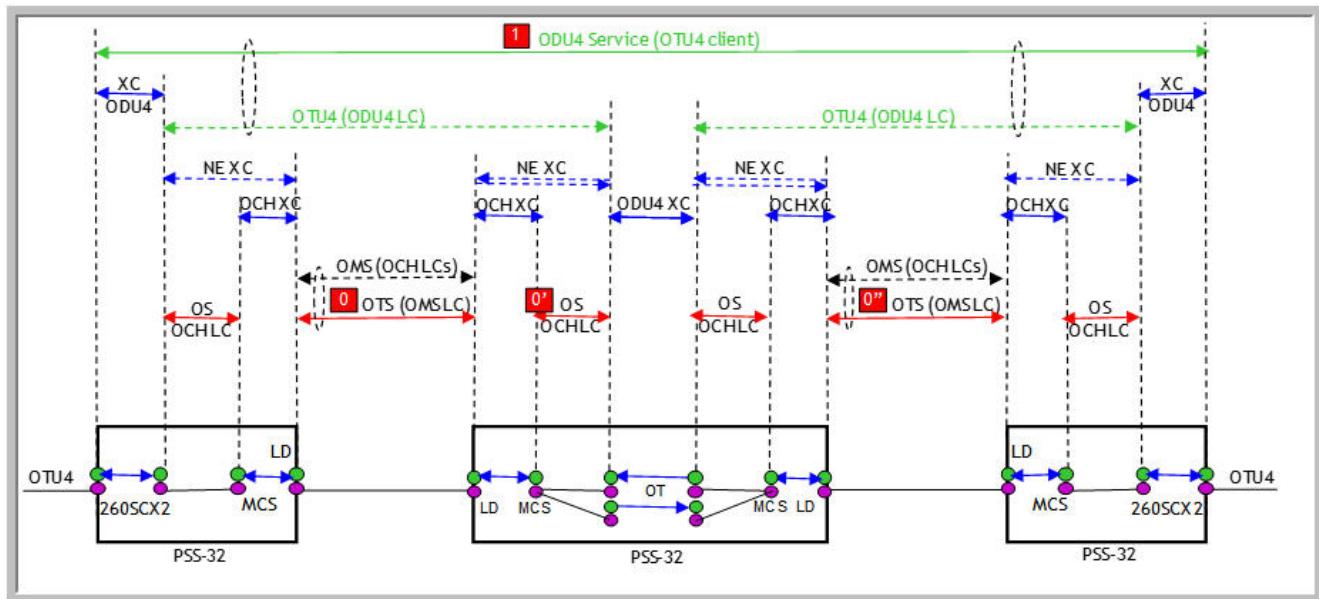


Figure 5-55 260SCX2 with CFP2 (C2CER4DC) Y-cable Protected – 100 GbE Client, MP

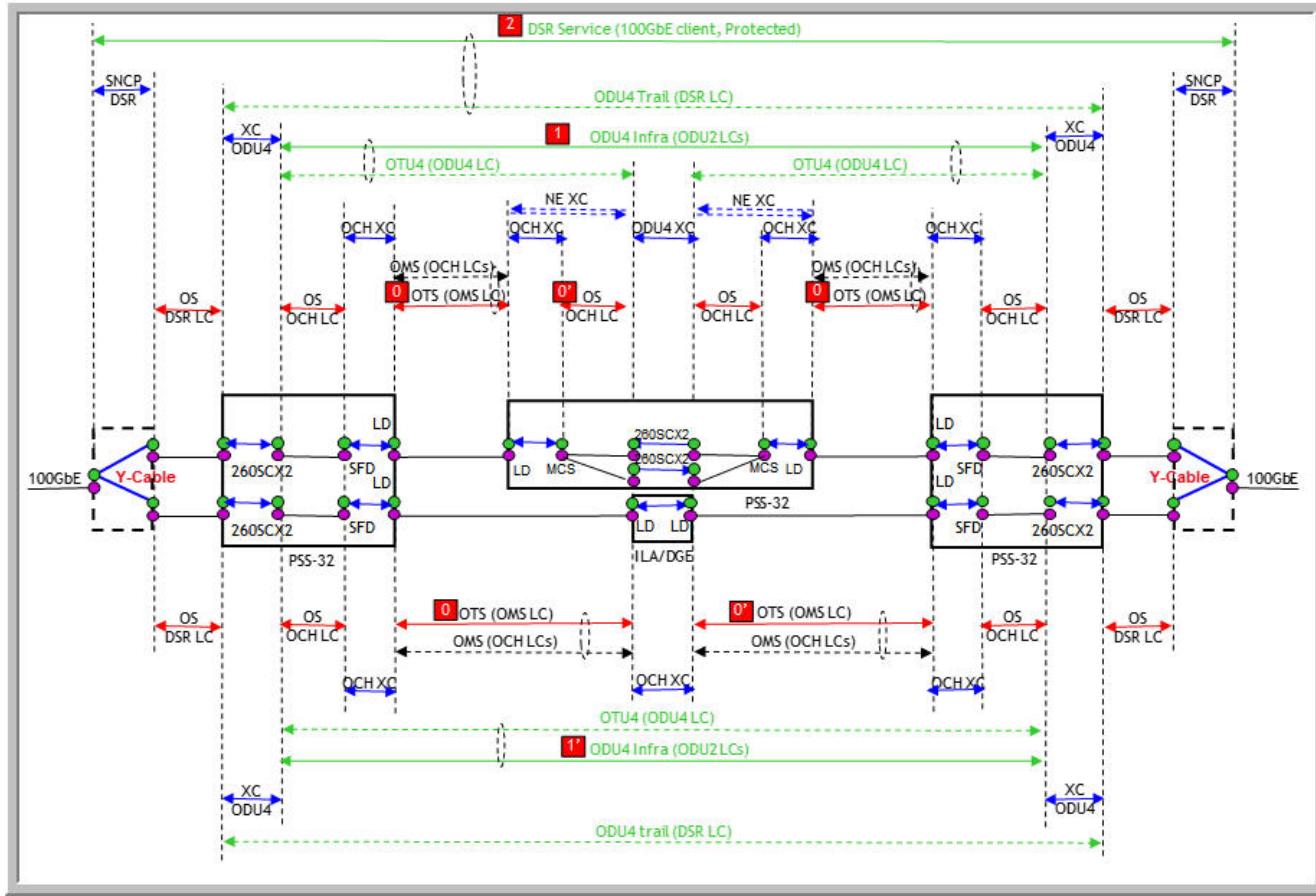


Figure 5-56 260SCX2 with CFP2 (C2CER4DC) OPSB Protected – OTU4 Client, MP

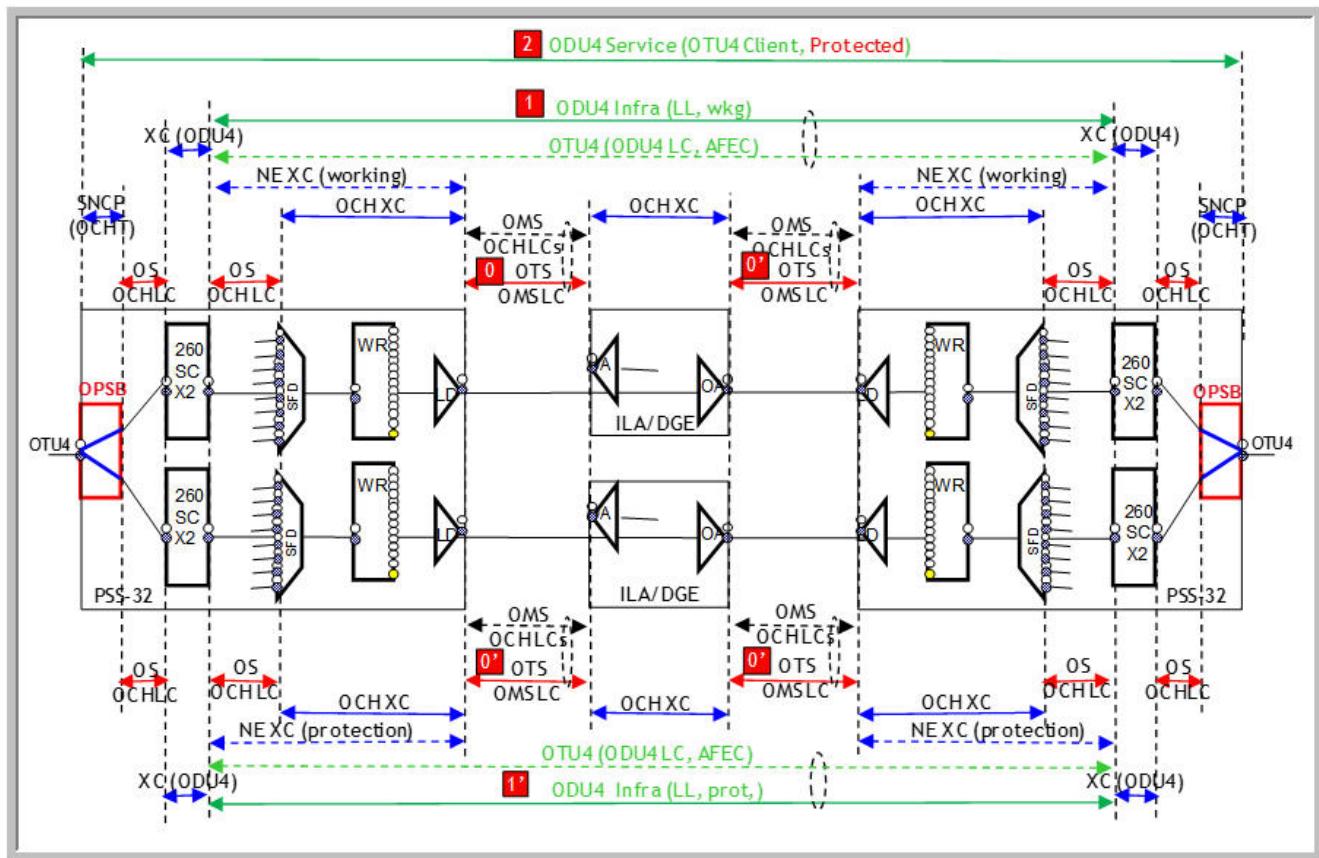


Figure 5-57 1AN100G with CFP2 (ER42W112GAUC) SNCP – 100 GbE Client, MP

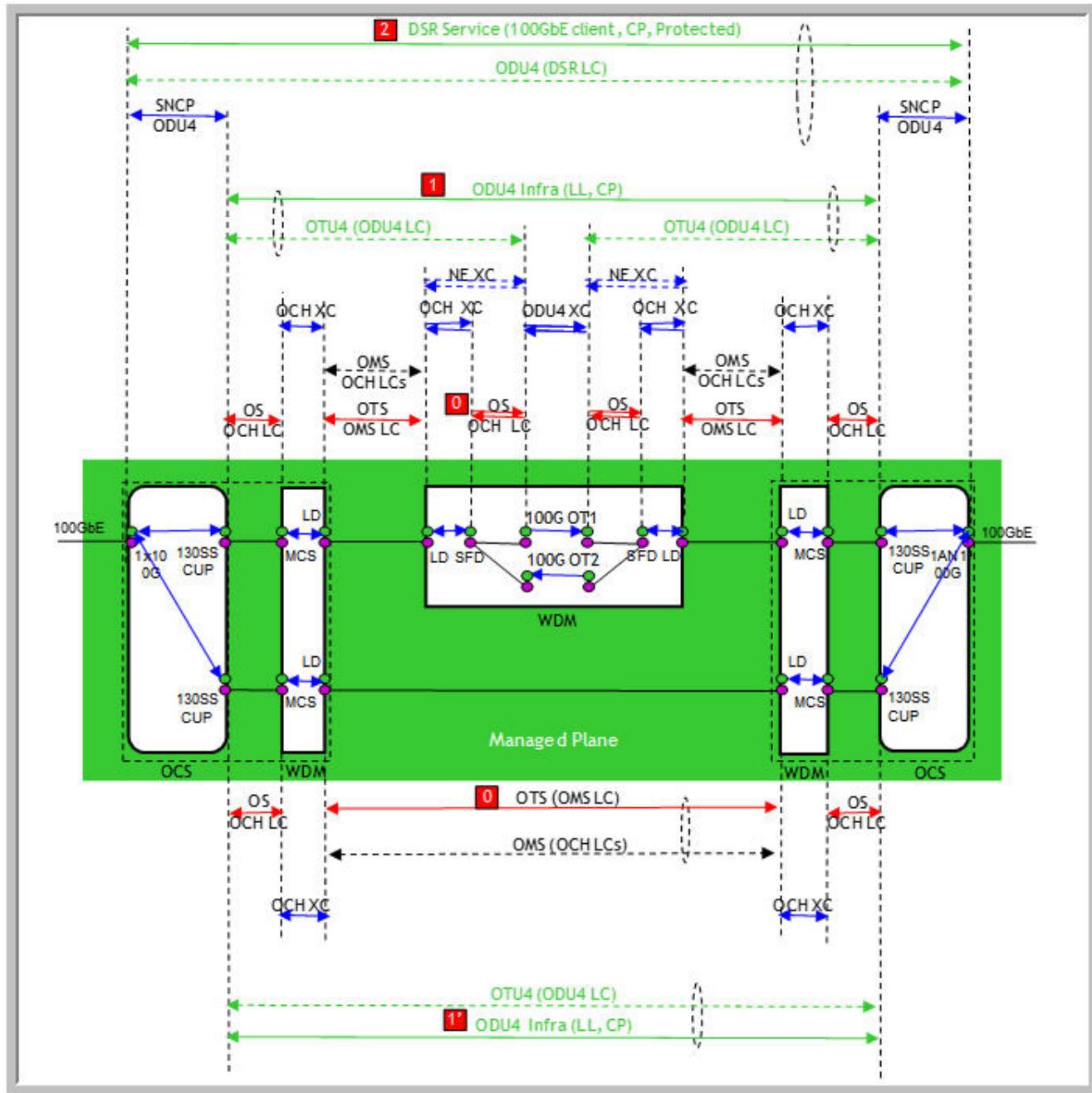


Figure 5-58 1AN100G with CFP2 (ER42W112GAUC) SNCP – 100 GbE Client, L0 CP

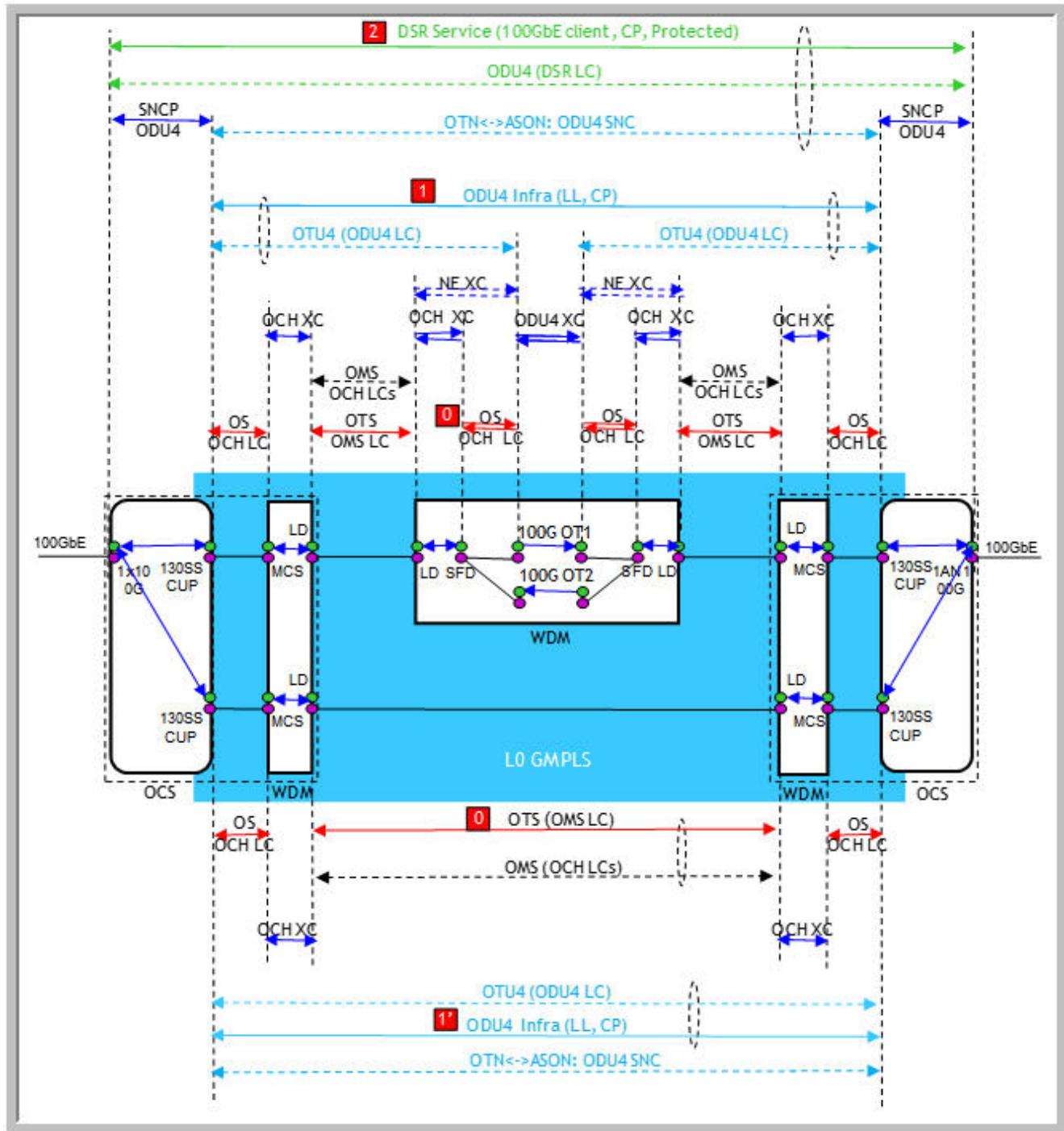
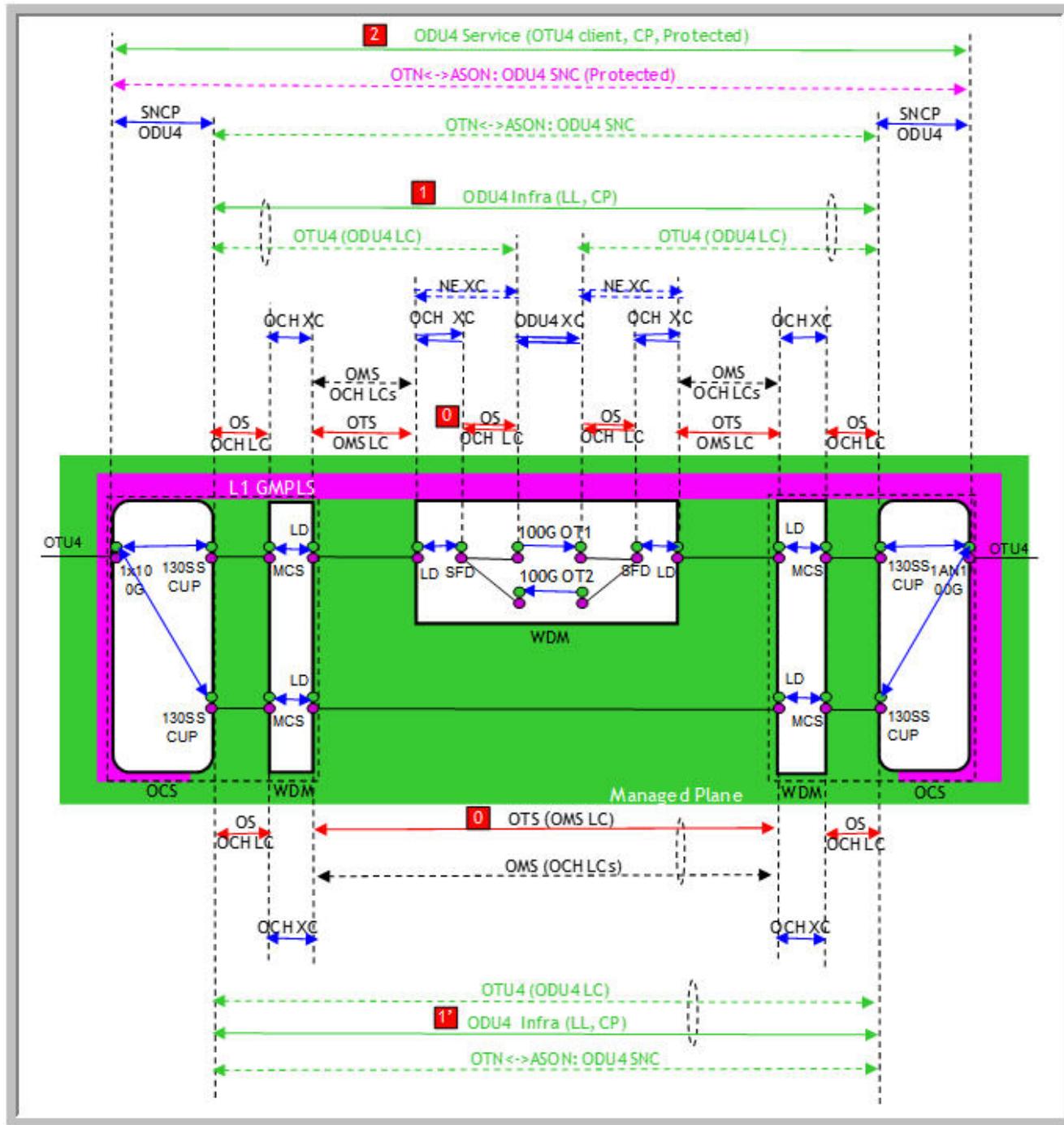


Figure 5-59 1AN100G with CFP2 (ER42W112GAUC) SNCP – OTU4 Client, L0 CP



Channel Width for 100 GHz, 112.5 GHz, and 125 GHz on Nokia OT

The NFM-T supports three Network types:

- Fix Grid Network
- Flex Grid Network
- Flex Grid capable Fix Grid Network

From NFM-T Release 21.12 cross connection management supports 100 GHz, 112.5 GHz, and 125 GHz.

Connection Type	Maximum Channel Width	Notes
Fix Grid Network	Upto 87.5 GHz	NE only supports upto 87.5 GHz channel width in Fix Grid Network.
Flex Grid Network and Flex Grid capable Fix Grid Network	<ul style="list-style-type: none">• SFM6 on 1830 PSI-M R6.0 supports channel width beyond 87.5 GHz, such as, 100 GHz and 112.5 GHz channel width assigned to 400G and 600G carrier profiles.• S6AD600H on 1830 PSS R14.0 supports channel width beyond 87.5 GHz, such as, 100 GHz and 112.5 GHz channel width assigned to 400G and 600G carrier profiles.	Link Connections in network is updated according to the network type.

The routing algorithm accommodates the new channels in the spectrum as per optimal allocation rules.

As part of alien wavelength service 125 GHz channel width is supported.



Note:

- From NFM-T Release 21.12, cross connection management for 100Ghz, 112.5Ghz and 125Ghz channel width for OCH alien wavelength service is supported for Managed Plane. This is applicable for flex-grid photonic architectures based on IRDM20/32/32L.
 - 1830 PSI-8
 - 1830 PSI-8L
 - 1830 PSS-16 II
 - 1830 PSS-32
- For foreign connections, changes to any **SNC** parameters through the WebUI requires a cross connection sync to be performed in NFM-T.
- When a user creates an alien service, depending on the **Channel Width** selected, the **Technology Type** parameter is set on the NE. This parameter can be edited from the NE WEBUI only.
- The **Technology Type** parameter modified only at the Source Node/Head Node is updated at the Connection level in NFM-T through Notification flow and Cross Connect

Synchronization flow. The **Technology Type** parameter modified at any other node, that is, pass through /Destination Node is not updated at the Connection level in NFM-T.

The **Technology Type** parameter is non editable from NFM-T . From NFM-T, this parameter can be viewed in:

1. Cross Connect tab of Nodes page
2. Modify Parameter Screen for the Alien Service
3. Modify Route Screen for Alien Service

Part II: Connections and services

Overview

Purpose

This chapter contains the conceptual content that users need to understand how to setup connection and services on the NFM-T. Beside users can enhance their understanding of the network profiles, Shared Risk Groups, Color Profiles and Alarm Profiles.

Contents

Chapter 6, Network Profiles	601
Chapter 7, Design, deploy and operate connections	663
Chapter 8, Deploy Connections	1215

6 Network Profiles

6.1 Overview

Purpose

The Network Profiles includes Shared Risk Groups (SRG), Color Profiles and Alarm Profiles. This chapter explains how to use these profiles to manage the network failures in the most efficient way.

Contents

6.1 Overview	601
Shared Risk Group (SRG)	
6.2 Shared Risk Group (SRG) Overview	603
6.3 SRGs table columns	604
6.4 Create a SRG	605
6.5 Change or assign the TE link to a SRG	608
6.6 Correlate a SRG with a Physical Connection	610
6.7 Correlate a SRG with an infrastructure connection	614
6.8 Control the deployment of the Physical Connections associated with a Shared Risk Group	617
6.9 Delete a Shared Risk Group	619
6.10 Manage the ASON Links Assigned to a Shared Risk Group	620
6.11 Manage the TE links assigned to a Shared Risk Group	621
6.12 View the Shared Risk Groups	622
6.13 View tabbed topics for a Shared Risk Group	624
Color Profiles	627
6.14 Resource Coloring	627
6.15 Resource Coloring strategies and allocation example	629
6.16 Associate a colored link Over an existing ASON domain	632
6.17 Create a Color Profile	637
6.18 Manage ASON Links assigned to a Color Profile	639
6.19 Manage ASON SNCs assigned to a Color Profile	640
6.20 Manage TE Links assigned to a Color Profile	641

6.21 View a list of Color Profiles	642
6.22 View tabbed topics for a Color Profile	646
Alarm Profiles	649
6.23 Alarm Profiles	649
6.24 Create an Alarm Profile	651
6.25 Determine the Network Alarm Profile Assigned to a Connection	653
6.26 Modify an Alarm Profile	656
6.27 View Alarm Profiles	658
6.28 View Tabbed Topics for an Alarm Profile	660

Shared Risk Group (SRG)

6.2 Shared Risk Group (SRG) Overview

Definition of a Shared Risk Group

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 SRGs is to provide a redundant route through the network of an existing route to avoid problems that disturb both routes, for example a link failure.

SRGs are identified by means of SRG values which need to be unique within a GMRE domain. One or more SRG identifiers then must be assigned to the TE links in the GMRE domain network that share at least one risk. A SRG attribute can be empty, may comprise a single SRG identifier, or may comprise a list of multiple SRG identifiers in case the entity is vulnerable to a number of different failures. Two or more Service/Connections are fully SRG diverse, if the intersection of their SRG attributes is empty, that is, if the respective Service/Connections do not have any SRG values in common.

Managing SRGs

To manage SRGs perform the following actions:

- [6.4 “Create a SRG” \(p. 605\)](#)
- [6.6 “Correlate a SRG with a Physical Connection” \(p. 610\)](#)
- [6.6.5 “Remove the Correlation \(Uncorrelate\) of a Physical Connection to a Shared Risk Group” \(p. 613\)](#)
- [6.7 “Correlate a SRG with an infrastructure connection” \(p. 614\)](#)
- [“Remove the Correlation \(Uncorrelate\) of an Infrastructure Connection to a Shared Risk Group” \(p. 616\)](#)
- [6.9 “Delete a Shared Risk Group” \(p. 619\)](#)
- [6.5 “Change or assign the TE link to a SRG” \(p. 608\)](#)

ASON Environment

Manage SRGs in an ASON environment

- [6.10 “Manage the ASON Links Assigned to a Shared Risk Group” \(p. 620\)](#)
- [6.11 “Manage the TE links assigned to a Shared Risk Group” \(p. 621\)](#)
- [6.8 “Control the deployment of the Physical Connections associated with a Shared Risk Group” \(p. 617\)](#)

6.3 SRGs table columns

SRGs table

To display the SRGs table use the procedure [6.12 “View the Shared Risk Groups” \(p. 622\)](#)

Column	Description
ASite, ZSite	The ASite and the ZSite columns display the names of the originating (ASite) and terminating (ZSite) locations for the Shared Risk Group (SRG).
Comment	The Comment column displays user comments about the object that is listed.
ID	The ID column displays the identification number of the SRG in the database.
Name	Shared Risk Group name assigned during creation.
SRG Probability	The SRG Probability column displays the probability that is assigned to the Shared Risk Group to be undefined [0], very low [10], low [100], medium [1000], high [10000] (the default), or very high [100000]. Origin: Users supply the SRG Probability during SRG provisioning.
SRG Type	The SRG Type column displays the Shared Risk Group type to be Other , Node , Cable (the default), Right-of-Way , Physical Connection , or Conduit . Origin: Users supply the SRG Probability during Shared Risk Group provisioning.

6.4 Create a SRG

When to use

Use this task to create a Shared Risk Group (SRG).

Related information

See the following topics in this document:

- [6.6 “Correlate a SRG with a Physical Connection” \(p. 610\)](#)
- [6.6.5 “Remove the Correlation \(Uncorrelate\) of a Physical Connection to a Shared Risk Group” \(p. 613\)](#)
- [6.7 “Correlate a SRG with an infrastructure connection” \(p. 614\)](#)
- [“Remove the Correlation \(Uncorrelate\) of an Infrastructure Connection to a Shared Risk Group” \(p. 616\)](#)

Before you begin

You can also create SRGs from the **Link Maintenance** window.

Task

Complete the following steps to create a SRG.

1

From the WebUI, follow this navigation path:

OPERATE > Network Profiles > Shared Risk Groups.

OPERATE > Physical Connections > 360° View > SRG

Result: The system displays the list of **Shared Risk Groups** in a data table.

2

Click **Create Shared Risk Group** () icon.

Result: The system displays the **SRG Creation** window.

Figure 6-1 SRG Creation window

The screenshot shows the 'SRG Creation' window. At the top left is the title 'SRG Creation' under 'Shared Risk Groups'. The window contains three main sections: 'SRG Identification' (User Label: 'test'), 'Risk Level' (Risk Type: 'Cable', Probability: 'high'), and 'Additional Info' (Comment, A-Site, Z-Site). At the bottom right are 'RESET' and 'OK' buttons.

3

In the **Label** field, enter a name to identify the SRG that you are creating.

4

In the **Risk Type** field, select one of the following from the drop-down list:

- **Other**
- **Node**
- **Right of Way**
- **Physical Connection**
- **Conduit (the default)**
- **Cable**

5

In the **Probability** field, select undefined [0], very low [10], low [100], medium [1000], high [10000] (the default), or very high [100000] from the drop-down list.

6

Optional: Click **Additional Information** panel. In the **Comment** field, enter any notes to further identify or clarify the SRG that you are creating.

7

Optional: Click **Additional Information** panel. In the **A-Site** and **Z-Site** fields, enter the appropriate user labels for both sites.

8

Click **OK**.

Result: A **Success** message is displayed at the bottom left of the page.

The SRG is created and added to the **Shared Risk Groups** data table.

END OF STEPS

6.5 Change or assign the TE link to a SRG

When to use

Use this task to assign or change the assignment of a Shared Risk Group to a traffic engineering (TE) link.

Before you begin

Ensure that the equipment in the network has been properly set, according to the deployed network.

Ensure that the NPAs are created and implemented.

The SRG must be created and the physical connection must be created. The SRG and the physical connection must be correlated. The SRG then propagates to all of the physical connections that are bundles in TE link.

For GMRE L0, one TE link has been automatically created for each OMS trail. In turn, each OMS trail has been automatically created for each OTS physical connection.

For GMRE L1, the relationship of the TE link - OTU trail is 1:n based on the bundling rules.

Task

Complete the following steps to assign or change the assignment of a Shared Risk Group to a TE link.

1

For a selected SRG, follow this navigation path from the WebUI

OPERATE > Network Profiles > Shared Risk Groups > 360° View > TE IINKS

Result: The system displays the list of TE links.

2

On the selected link, click **More**  icon and select **Modify TE link**.

Result: The system displays the **Modify TE link** window.

3

In the **TE link** panel, configure the following parameters:

- The **Name** field is auto populated.
- In the **Cost/Metric** field, select a value. For I-NNI links, the **Cost/Metric** values for GMRE releases earlier than R14.0.8 range from 0 to 100 and for GMRE release later than or equal to R14.0.8, the range is from 0 to 100,000. Both the NEs should be GMRE release later than or equal to R14.0.8, only then the value till 100,000 is allowed. The default is **20**.
- In the **Latency (microsec)**, select a value from the scroll buttons
- Select the color profile from the **Color Profile** window.

4

In the **SRGs** panel, select SRG from the **SRGs** window.

5

Click **OK**.

Result: The TE link is updated based on the selections and applied to all the links (physical connections) that belongs to TE link.

END OF STEPS

6.6 Correlate a SRG with a Physical Connection

When to use

Use this task to correlate a Shared Risk Group (SRG) with a physical connection.

When you correlate a SRG with a particular physical connection, assign that physical connection to the SRG.

Related information

See [7.19 “Create an OTN physical connection” \(p. 784\)](#).

Before you begin

The SRG must already be created.

The physical connection must belong to a Defined NPA. If the NPA is in the **Implemented** state, the operation is available on a TE link and is applied to all the physical connections inside the TE link.

The physical connection or TE link that you correlate to one SRG can be correlated to another SRG; meaning, one physical link or one TE link can be correlated to multiple SRGs.

You can also correlate a SRG with a physical connection from the Physical Connections data table.

Task

Complete the following steps to correlate a SRG.

1

From the WebUI, follow this navigation path:

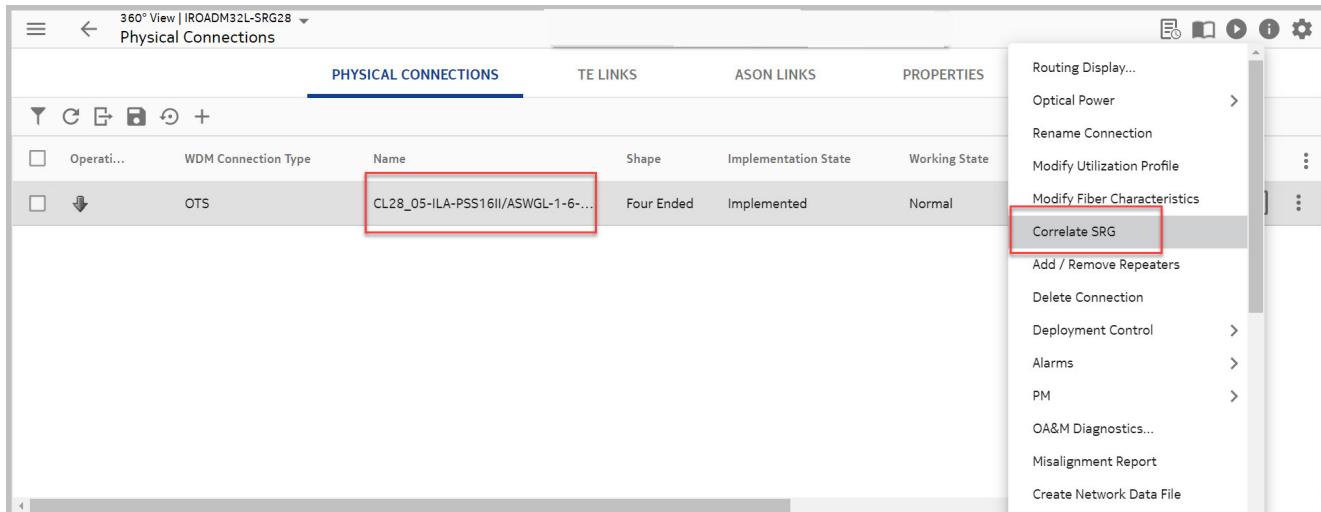
OPERATE > Network Profiles > SHARED RISK GROUPS > 360° View > PHYSICAL CONNECTIONS.

Result: The system displays a list of physical connections in the data table.

2

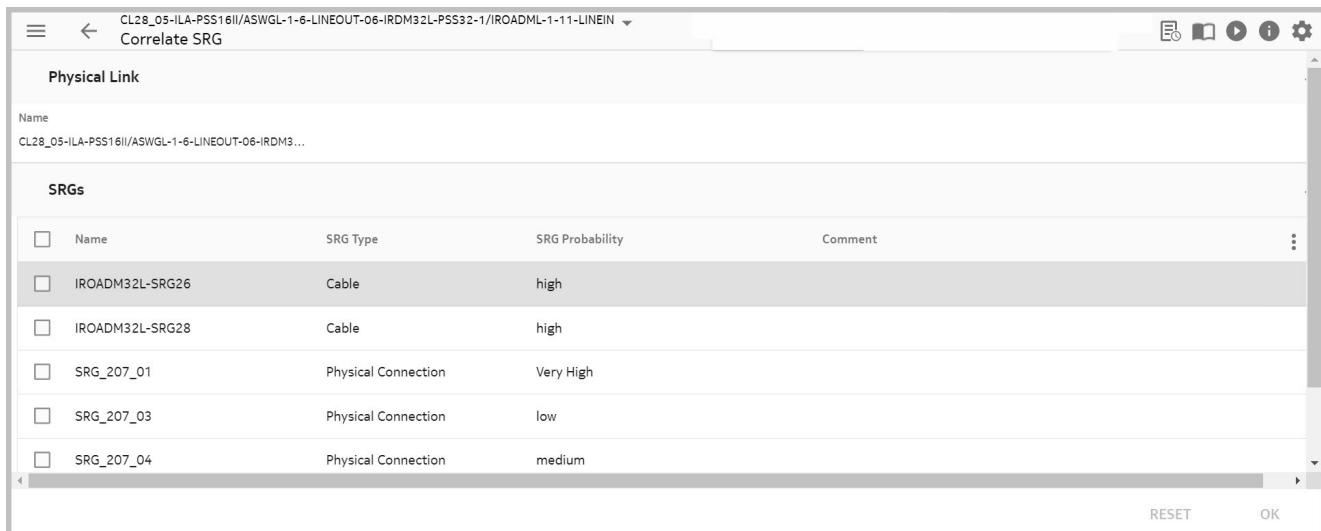
On the selected physical connection click **More**  icon and select **Correlate SRG**.

Figure 6-2 Correlate SRG for a Physical Link



Result: The system displays the **Correlate SRG** window.

Figure 6-3 Correlate SRG window



3

In the **SRGs** window, select the SRG.

4

Click **OK** to apply the changes. Select **RESET** to reset the selection.

Result: The system displays a success message.

END OF STEPS

Direct SRG Association from Physical Connections - SRG Tab

The SRG is also correlated when creating new SRG on the selected physical connection.

SRG correlation steps:

1

On the WebUI, navigate as:

OPERATE > Physical Connections > 360° View > SRGS tab

Result: SRGS data table is displayed.

2

Click **Create Shared Risk Group** () icon.

Result: SRG Creation page is displayed.

3

Click **Correlate with selected Physical Connection** check box to correlate the SRG with the Physical connection.

4

In the **Label** field, enter a name to identify the SRG that you are creating.

5

In the **Risk Type** field, select one of the following from the drop-down list:

- Other
- Node
- Right of Way
- Physical Connection
- Conduit (the default)
- Cable

6

In the **Probability** field, select undefined (0), very low (10), low (100), medium (1000), high (10000) (the default), or very high (100000) from the drop down list.

7

Optional: Click **Additional Information** panel. In the **Comment** field, enter any notes to further identify or clarify the SRG that you are creating.

8

Optional: Click **Additional Information** panel. In the **A-Site** and **Z-Site** fields, enter the appropriate user labels for both sites.

9

Click **OK**.

Result: A **Success** message is displayed at the bottom left of the page.

The system creates, correlates, and adds the SRG to the **SHARED RISK GROUPS** data table.

END OF STEPS

Remove the Correlation (Uncorrelate) of a Physical Connection to a Shared Risk Group

The physical connection must belong to a **Defined** NPA. If the NPA is in the **Implemented** state, the operation is available on TE link and it will be applied to all physical connections inside the TE Link.

From the Shared Risk Groups list that is displayed, select the SRG to remove the physical connection correlation, navigate as **360° View > More**  icon. In the **PHYSICAL CONNECTIONS** tab of the window, do one of the following:

- Click **Remove** icon.
- Mouse over the icons, click on the **SRG Correlate** icon. In the **SRG Correlation window**, click **Delete** icon and click **Deploy**.

The physical connection and the SRG that you selected are now uncorrelated and the system outputs a  **Success** message at the bottom left of the window.

Mouse over the icons and click on the **Refresh** icon, the physical connection is removed from the data table in the **Physical Connections** tab.

6.7 Correlate a SRG with an infrastructure connection

When to use

Use this task to correlate a Shared Risk Group (SRG) with an infrastructure connection.

When you correlate a SRG with a particular infrastructure connection, assign that infrastructure connection to the SRG.

Before you begin

The SRG must already be created.

The infrastructure connection must belong to a DEFINED NPA. If the NPA is in the **Implemented** state, the operation is available on a TE link and is applied to all the infrastructure connections inside the TE link.

The infrastructure connection or TE link that you correlate to one SRG can be correlated to another SRG; meaning, one logical link or one TE link can be correlated to multiple SRGs.

Task

i Note: Follow one of the following steps to correlate a SRG:

- **OPERATE > ASON > NPAs > 360° View > LINKS tab > More  icon > TE link assignment.** See [10.17 “Assign an ASON I-NNI link to a TE Link and SRG” \(p. 1473\)](#) for more details.
- **OPERATE > ASON > NPAs > 360° View > TE LINKS tab > More  icon > Modify TE link.** See [10.24 “Modify TE Links” \(p. 1495\)](#) for more details.
- **OPERATE > ASON > NPAs > 360° View > LINKS tab > Add Links to NPA > LINK PARAMETERS tab.** See the following steps for more details.

Complete the following steps to correlate a SRG.

1

From the WebUI, follow this navigation path:

OPERATE > ASON > NPAs > 360° View > LINKS tab.

Result: The system displays the associated links.

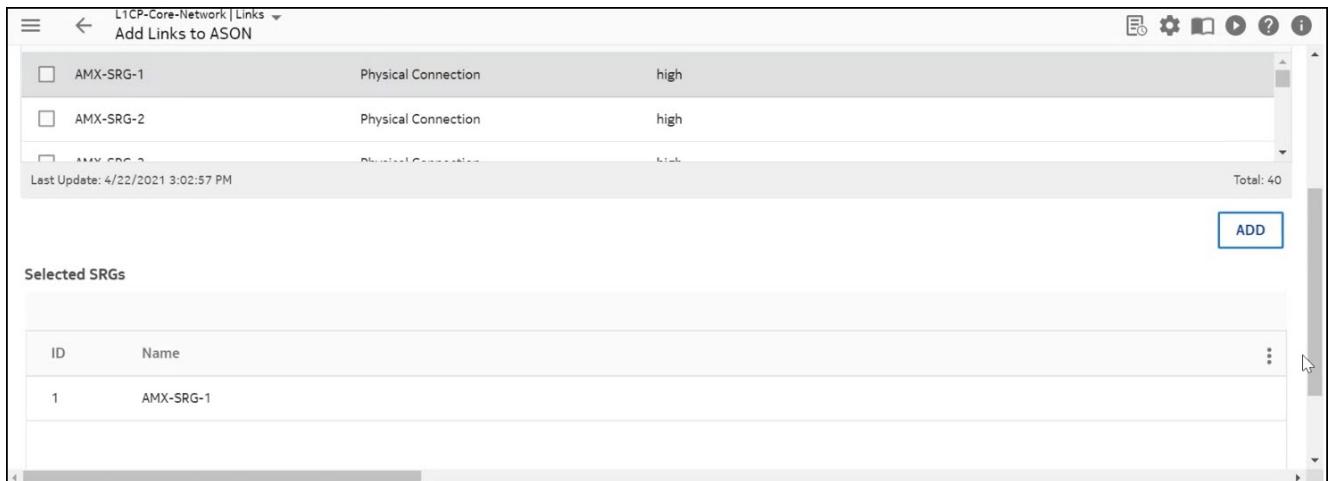
2

Click **Add Links to NPA**.

3

In the **LINK PARAMETERS** tab, **SRGs** sub-tab, select the SRG to correlate and click **ADD**.

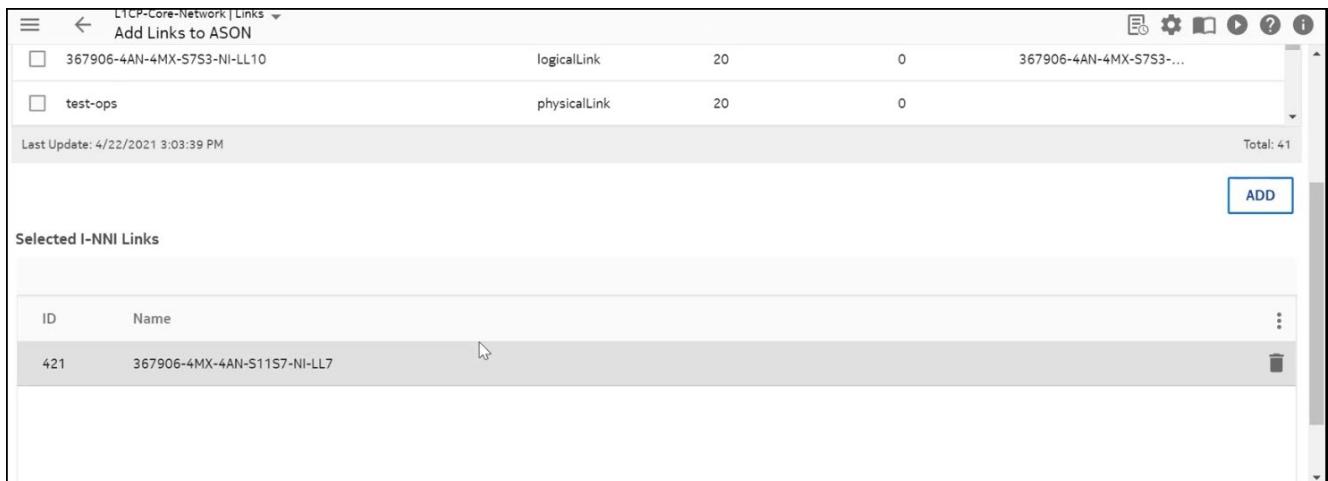
Figure 6-4 Add SRG



4

From **I-NNI LINKS** tab, select the logical link and click **ADD**.

Figure 6-5 Add I-NNI



5

Click **OK**.

Result: The selected SRG is correlated with the selected infrastructure connection.

END OF STEPS

Remove the Correlation (Uncorrelate) of an Infrastructure Connection to a Shared Risk Group

The infrastructure connection must belong to a **Defined** NPA. If the NPA is in the **Implemented** state, the operation is available on TE link and it will be applied to all infrastructure connections inside the TE Link.

Complete the following steps to remove the infrastructure correlation:

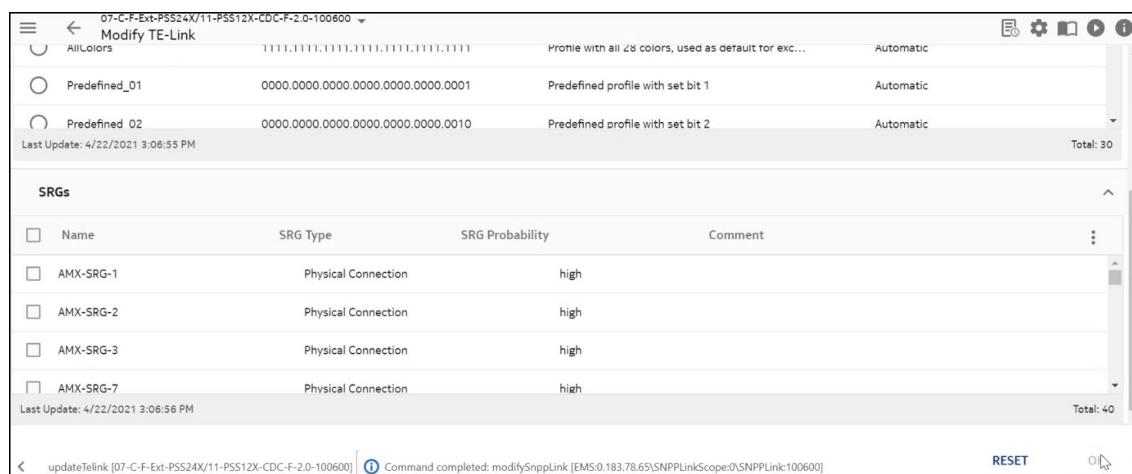
1. From the WebUI, follow this navigation path:

OPERATE > ASON > NPAs > 360° View > TE LINKS tab.

Result: The system displays the list of TE Links in the data table.

2. Select a logical link to remove the correlation, click **More**  icon, and click **Modify TE link**.
3. In the **SRGs** field, clear the check box of the SRG to remove correlation.
4. Click **OK**.

Result: The infrastructure connection and the SRG that you selected are now uncorrelated and the system displays a ✓ **Success** message at the bottom of the window.



Name	Profile	State
Predefined_01	Profile with all 28 colors, used as default for ex...	Automatic
Predefined_02	Profile with set bit 1	Automatic

Name	Type	Probability	Comment
AMX-SRG-1	Physical Connection	high	
AMX-SRG-2	Physical Connection	high	
AMX-SRG-3	Physical Connection	high	
AMX-SRG-7	Physical Connection	high	

6.8 Control the deployment of the Physical Connections associated with a Shared Risk Group

When to use

Use this task to control the deployment of the physical connections that are associated with a SRG.

Related information

See the following topics in this document:

- [6.4 “Create a SRG” \(p. 605\)](#)
- [6.6 “Correlate a SRG with a Physical Connection” \(p. 610\)](#)
- [6.9 “Delete a Shared Risk Group” \(p. 619\)](#)

Before you begin

This task enables you to change the service state and the implementation state of the physical connection that is associated with a SRG.

The SRG must already be created and the physical connections must be correlated with (assigned to) the SRG.

Task

Complete the following steps to control the deployment of the physical connections that are associated with a SRG.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Network Profiles > SHARED RISK GROUPS > 360° View > PHYSICAL CONNECTIONS

Result: The PHYSICAL CONNECTIONS data table is displayed.

2

From the Shared Risk Groups list that is displayed, select the SRG where you want to control the deployment of its associated physical connection and perform one of the following operations as required :

- If you want to implement a physical connection that is Defined (not yet implemented), go to [Step 3](#).
- If you want to deimplement a physical connection that is already implemented, go to [Step 4](#).
- If you want to set the service state of an not-in-service physical connection to in service, go to [Step 6](#).
- If you want to set the service state of an in-service physical connection to not-in-service, go to [Step 7](#).

Control the deployment of the Physical Connections associated with a Shared Risk Group

3

In the **PHYSICAL CONNECTIONS** tab of the window, select the connection to be implemented, and do the following:

- On the selected physical connection, click **More :** icon, navigate as : **Deployment Control > Implement** and click **Implement** .

Result: The implementation state of the physical connection is first changed to **Partially Implemented** and then to **Implemented**.

4

In the **PHYSICAL CONNECTIONS** tab of the window, select the connection, and do the following:

- On the selected physical connection click **More :** icon, navigate as : **Deployment Control > Deimplement** and click **Deimplement** .

Result: The system outputs the following message:

Are you sure that you want to perform <deimplement>>

5

To deimplement the deployment, click **OK**.

Result: The implementation state of the physical connection is first changed to **Partially Implemented** and then to **Defined**.

6

In the **PHYSICAL CONNECTIONS** tab of the window, select the connection to be put into service, and do the following:

- Click **More :** icon on the physical connection, navigate as : **Deployment Control > Set Service State (in service)** and click **Set Service State (in service)** .

Result: The service state of the physical connection is changed to **In Service** and the system outputs a ✓ **Success** message at the bottom left of the window.

7

In the **PHYSICAL CONNECTIONS** tab of the window, select the connection to be put out-of-service, and do the following:

- Click **More :** icon on the physical connection, navigate as : **Deployment Control > Set Service State (not in service)** and click **Set Service State (not in service)** .

Result: The service state of the physical connection is changed to **Not in service** and the system outputs a ✓ **Success** message at the bottom left of the window.

END OF STEPS

6.9 Delete a Shared Risk Group

When to use

Use this task to delete a Shared Risk Group (SRG).

Related information

See the following topics in this document:

- [6.4 “Create a SRG” \(p. 605\)](#)
- [6.6 “Correlate a SRG with a Physical Connection” \(p. 610\)](#)
- [6.6.5 “Remove the Correlation \(Uncorrelate\) of a Physical Connection to a Shared Risk Group” \(p. 613\)](#)

Before you begin

The SRG must already be created and it cannot be correlated to any physical connection.

You can also delete SRGs from the **Link Maintenance Window**; refer to the [10.25 “Perform link maintenance” \(p. 1497\)](#) task for detailed steps.

Task

Complete the following steps to delete a Shared Risk Group (SRG).

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Network Profiles > SHARED RISK GROUPS

Result: The **SHARED RISK GROUPS** data table is displayed.

2

Select the SRG that you want to remove and do the following:

- On the selected SRG, Click **More**  icon and click **Remove** from the pop up menu.

Result: The system displays a confirmation window that asks:

Are you sure you want to remove the selected object(s)

3

Click **OK**.

Result: The SRG is removed from the **SHARED RISK GROUPS** data table and the system outputs a ✓ **Success** message at the bottom left of the window.

END OF STEPS

6.10 Manage the ASON Links Assigned to a Shared Risk Group

Purpose

Use this task to manage the ASON links (Links) that are assigned to a SRG.

The **ASON LINKS** tab provides the same actions and functions as the **LINKS** tab that is displayed for ASON NPAs. On the WebUI, follow the path for a selected ASON LINK : **OPERATE > Network Profiles > SHARED RISK GROUPS > 360° View > ASON LINKS > More**  icon.

Task

Complete the following steps to manage the ASON links (Links) that are assigned to a SRG.

1 _____
To set the **Administrative State**, see [10.27 “Set the ASON administrative state of links” \(p. 1504\)](#)

2 _____
To change the add or remove links, see [10.15 “Add links and remove links from ASON” \(p. 1462\)](#).

3 _____
For **Link Maintenance Window**, see [10.25 “Perform link maintenance” \(p. 1497\)](#).

4 _____
For **Change ASON WTR** (wait time to restore), see [10.18 “Change ASON WTR” \(p. 1475\)](#).

5 _____
For **Add Links to ASON**, go to the “[Task: Add links to ASON](#)” (p. 1463) task.
For **Remove Links from ASON**, go to the “[Task: Remove links from ASON](#)” (p. 1466) task.

6 _____
For **Auto Restoration**, see [10.20 “Enable or disable auto restoration of links” \(p. 1480\)](#).

7 _____
For **Misalignment Report**, see [10.14 “Access and view the misalignment report for a link” \(p. 1461\)](#).

8 _____
For **Jobs**, select the link and either right click and select **Jobs** or click on the **Jobs** icon to display the current Jobs for link.

END OF STEPS _____

6.11 Manage the TE links assigned to a Shared Risk Group

Purpose

Use this task to manage the TE links that are assigned to a SRG.

The **TE LINKS** tab provides the same actions and functions as the **TE LINKS** tab that is displayed for ASON NPAs. On the WebUI, follow the path for a selected TE LINK : **OPERATE > Network Profiles > SHARED RISK GROUPS > 360° View > TE LINKS > More**  . icon.

Task

Complete the following steps to manage the TE links that are assigned to a SRG.

1

To Modify TE links, see [10.24 “Modify TE Links” \(p. 1495\)](#).

2

For Misalignment Report, see [10.14 “Access and view the misalignment report for a link” \(p. 1461\)](#).

3

For Jobs, see [“Jobs” \(p. 1194\)](#).

END OF STEPS

6.12 View the Shared Risk Groups

Purpose

Use this task to view a list of Shared Risk Groups (SRGs).

Ensure that the SRGs are created.

Task

Complete the following step to view a list of SRGs.

1

From the WebUI, follow this navigation path:

OPERATE > Network Profiles > SHARED RISK GROUPS.

Result: The system displays a list of SRGs.

Figure 6-6 SRG - Shared Risk Group List

Name	SRG Type	SRG Probability	Comment
SRG-01	Cable	high	
SRG_01_07	Cable	high	
SRG_01_05	Cable	high	
SRG_04_07	Cable	high	
SRG_05_06	Cable	high	
SRG_06_07	Cable	high	

2

To view the additional attributes, click the **Properties** icon.

3

To create a SRG, click **Create** icon. See [6.4 "Create a SRG" \(p. 605\)](#).

4

To delete a SRG, on the selected SRG, click **More**  icon and click **Remove** option from the pop up menu.

END OF STEPS

6.13 View tabbed topics for a Shared Risk Group

When to use

Use this task to view tabbed topics for a Shared Risk Group (SRG), which includes SRG related information on **PHYSICAL CONNECTIONS**, **TE LINKS**, **ASON LINKS** and **PROPERTIES**.

Related information

See the following topics in this document:

- [6.4 “Create a SRG” \(p. 605\)](#)
- [6.6 “Correlate a SRG with a Physical Connection” \(p. 610\)](#)
- [6.6.5 “Remove the Correlation \(Uncorrelate\) of a Physical Connection to a Shared Risk Group” \(p. 613\)](#)
- [6.9 “Delete a Shared Risk Group” \(p. 619\)](#)

Before you begin

You can view tabbed topics for a SRG in following way:

- You can view tabbed topics for a SRG using the following path on WebUI.
OPERATE > Network Profiles > SHARED RISK GROUPS

Task

Complete the following steps to view tabbed topics for a SRG.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Network Profiles > SHARED RISK GROUPS

Result: The **SHARED RISK GROUPS** list is displayed.

Figure 6-7 SHARED RISK GROUPS – Data Table

The screenshot shows a web-based application interface for managing network profiles. At the top, there's a header bar with the title 'Network Equipment | Network Profiles' and 'Shared Risk Groups'. Below the header is a toolbar with various icons for navigation and operations. The main area is a data table titled 'SHARED RISK GROUPS'. The table has columns for 'Name', 'SRG Type', 'SRG Probability', and 'Comment'. There are seven rows in the table, each representing a different SRG entry. The first row ('SRG-01') is selected, indicated by a grey background. The last row ('SRG_06_07') has a tooltip icon over it. The bottom of the table has a 'More' icon (three dots) and a 'Delete' icon.

Name	SRG Type	SRG Probability	Comment
SRG-01	Cable	high	
SRG_01_07	Cable	high	
SRG_01_05	Cable	high	
SRG_04_07	Cable	high	
SRG_05_06	Cable	high	
SRG_06_07	Cable	high	

2

Do one of the following:

- To view the tabbed topics for a SRG, follow this navigation path from the WebUI : **OPERATE > Network Profiles > SHARED RISK GROUPS > 360° View** and click on one of the available tabs.

The available tabs are the following:

- [25.33 “OTN Physical Connections Tab” \(p. 2126\)](#)
- [25.55 “TE Links Tab” \(p. 2172\)](#)
- [25.7 “ASON Links Tab” \(p. 2069\)](#)
- [25.39 “Properties Tab” \(p. 2141\)](#)

Important Usability Notes:

- The More icon that are provided with the **PHYSICAL CONNECTIONS** tabbed topic are the same functions that are provided when you access this object directly from the **OPERATE > PHYSICAL CONNECTIONS** navigation path. icon. The detailed tasks for physical connections are found in the [“Physical Connections” \(p. 784\)](#) section and in this section of the document.

Result: The system activates the tabs and the SRG related information is displayed directly below the data table for the SRG.

Note: To return to the original data table, click the browser back arrow.

3

Optional: To view the details of a selected item in either the top or bottom data table, click on the icon. Refer to [“View additional attributes for a selected item in a data table” \(p. 2194\)](#) for details.

Result: The system displays detailed information for the selected item.

END OF STEPS —

Color Profiles

6.14 Resource Coloring

Resource Coloring definition

Resource Coloring is a NFM-T feature that enables users to create and assign a color profile to specific management system links in the NFM-T OTN, NFM-T SDH, and NFM-T 16x6 Photonic applications in the ASON environment. All SDH, photonic, and WDM electrical networks are supported.

Resource Coloring functional description

Resource Coloring helps users to assign colors to links (such as TE links), in order to separate traffic and to identify unique routes that are used to upload and carry traffic. Users can choose different strategies to color-code their networks for ease of visibility. Refer to “[Resource Coloring strategy 1](#)” (p. 629), “[Resource Coloring strategy 2](#)” (p. 629), and “[Resource Coloring strategy 3](#)” (p. 630) for examples.

Color Profiles

Resource Coloring is made available to users through the use of color profiles that are accessed from this navigation path of the NFM-T GUI:

OPERATE > COLOR PROFILES

Within color profiles, users can select the following profiles:

- **NoColor** is a neutral profile that does not contain any colors. **NoColor** is characterized by a binary bit set of **0000.0000.0000.0000.0000.0000**.
- **AllColors** is a profile that includes all 28 colors. **AllColors** is characterized by a binary bit set of **1111.1111.1111.1111.1111.1111..** It is a default profile that is used for exclusions.
- **Predefined_01....Predefined_28** is a profile that is a specific color.

Note: The 28 predefined colors are a GMRE limitation. Each predefined color has a specific binary bit set that includes certain colors.

When users create a connection, the color profile is, by default, automatically defined as *includeAnyColor*, which is **NoColor**, and *excludeAnyColor*, which is **AllColors**. For TE links and physical connections, the default profile is **NoColor**.

User Interaction with Color Profiles

From the Color Profile level, the management system enables users to create a new color profile, delete a user created color profile, and view all color profiles.

- [6.17 “Create a Color Profile” \(p. 637\)](#)
- [6.16 “Associate a colored link Over an existing ASON domain” \(p. 632\)](#)
- [6.18 “Manage ASON Links assigned to a Color Profile” \(p. 639\)](#)
- [6.20 “Manage TE Links assigned to a Color Profile” \(p. 641\)](#)

-
- [6.22 “View tabbed topics for a Color Profile” \(p. 646\)](#)

6.15 Resource Coloring strategies and allocation example

Resource Coloring strategy 1

Resource Coloring using strategy 1 provides a simple view of the network. Each link has a specific predefined color and the connections (infrastructure and services) allocation rules are simple.

For instance it is possible to divide the links of the network into three parts and assign a color to each of these parts (red, green, blue), and the red connections can cross only red links, green connections only green links and blue connections only blue links.

A disadvantage of this strategy is that users must set the colors for the attributes of all the links and of all considered connections; otherwise, the connections will not be allocated over colored links.

To set up a colored network using strategy 1, do the following:

- All links must be colored with predefined color profiles only (such as blue, red, green).
- All connections must be routed over links with the same color.

To route a connection on a colored link, for example a red link, the following two options are possible:

1. includeAnyColor = **red** and excludeAnycolor = **No color (or blue & green)**
2. includeAnyColor = **NoColor** and excludeAnycolor = **blue & green**

Resource Coloring strategy 2

Resource Coloring using strategy 2 includes links that can be uncolored or colored with a predefined color profile only. For example some links are colored in red, others in blue or green. Connections are routed over uncolored links or links with the same color. The advantage of this strategy is that users can leave the default values for uncolored links and connections.

This strategy implements the same partition as above adding a shared pool of resources at the **Not Colored** links.

To route a connection on uncolored links, leave the default values:

- includeAnyColor = **NoColor**
- excludeAnyColor = **AllColors**

To route a connection only on links with a specific color, such as red, do the following:

1. includeAnyColor = **red**
2. excludeAnyColor = **NoColors (or blue & green)**

To route a connection both on uncolored links and links with a specific color, such as red, do the following:

1. includeAnyColor = **NoColor**
2. excludeAnyColor = **blue & green**

Extension of strategy 2

In this extension of strategy 2, links can be uncolored or they can be colored using the predefined color profiles, such as blue, red, or green. Connections are routed over uncolored links, or links with a single color, or even links with two or more different colors.

The three types of connections that are set up in strategy 2 are still in effect. In addition, to route a trail to links of two specific colors, such as red and blue, make the following two settings:

- `includeAnyColor = red & blue`
- `excludeAnyColor = NoColor (or green)`

To route a connection on uncolored links of two specific colors, such as red and blue, make the following two settings:

- `includeAnyColor = NoColor`
- `excludeAnyColor = green`

Resource Coloring strategy 3

Resource Coloring using strategy 3 includes links that can be uncolored or colored with a predefined color profile, such as blue, red, green, or even a user-defined profile that includes blue and red. only. Connections are routed over uncolored links or links with the same color.

To route a connection on links with a specific color, such as red, including links red and blue, do the following:

- `includeAnyColor = red`
- `excludeAnyColor = NoColor (or green)`

To route a connection on links with a specific color, such as red, but not including links red and blue, do the following:

- `includeAnyColor = red`
- `excludeAnyColor = blue & green`

To route a connection on both uncolored links and links with a specific color, such as red but not links red and blue, do the following:

- `includeAnyColor = NoColor`
- `excludeAnyColor = blue & green`

To route a connection on both uncolored links and links with a specific color, such as red, including links red and blue, do the following:

- `includeAnyColor = NoColor & blue`
- `excludeAnyColor = blue & green`

Resource Coloring in ASON

From the Color Profile level, the system enables users to manage the coloring in ASON environment.

- [6.16 “Associate a colored link Over an existing ASON domain” \(p. 632\)](#)

-
- 6.18 “Manage ASON Links assigned to a Color Profile” (p. 639)
 - 6.19 “Manage ASON SNCs assigned to a Color Profile” (p. 640)
 - 6.20 “Manage TE Links assigned to a Color Profile” (p. 641)

6.16 Associate a colored link Over an existing ASON domain

When to use

Use this task to associate a colored link over an existing ASON domain.

When associating a color link over an ASON domain, associate the color link with an NPA, its physical link (connection); and optionally, associate it with a SRG.

Related information

See the following topics in this document:

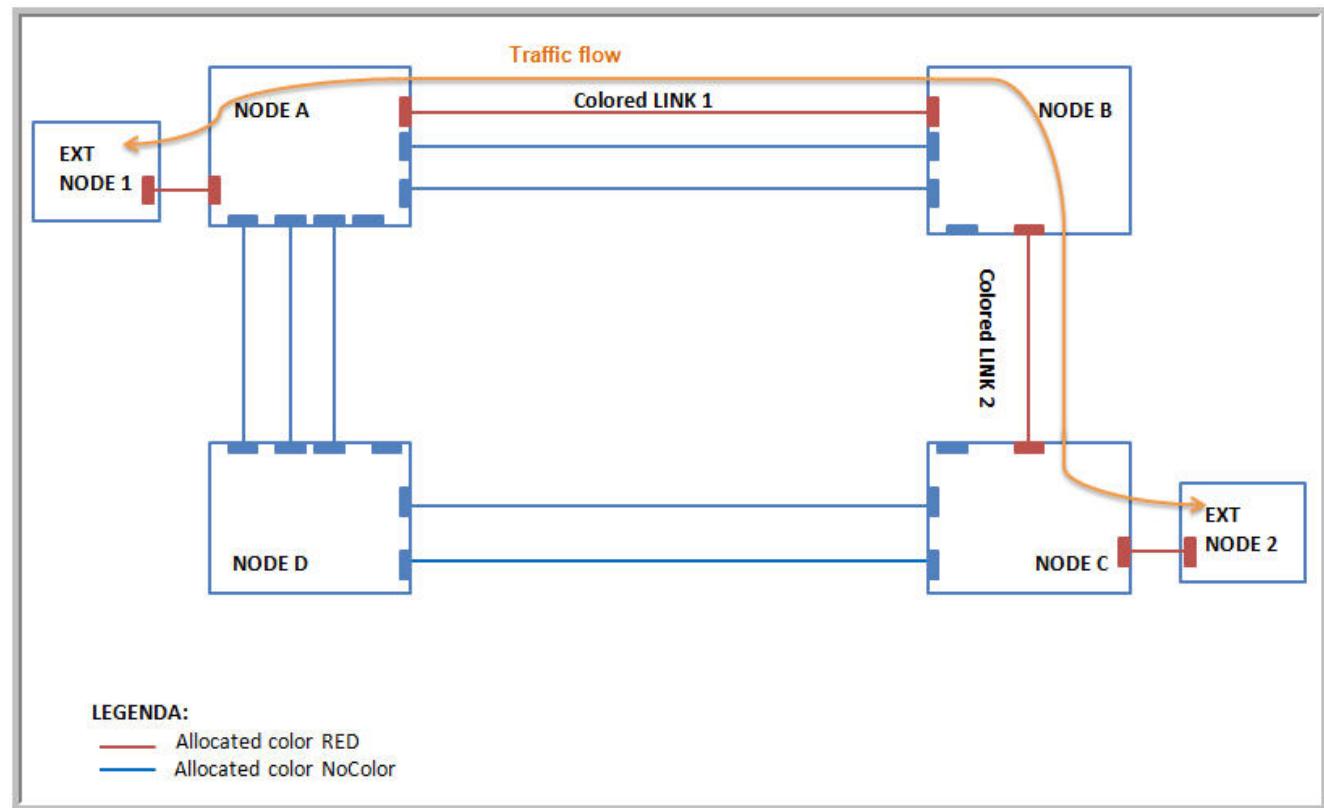
- [10.8 “Create and remove an NPA” \(p. 1443\)](#)
- [7.19 “Create an OTN physical connection” \(p. 784\)](#)
- [6.17 “Create a Color Profile” \(p. 637\)](#)
- [7.8 “Design and publish a template for a connection” \(p. 741\)](#)
- [7.12 “Deploy a template to make a connection” \(p. 754\)](#)
- [“Include Any Color Name” \(p. 717\)](#)
- [“Exclude Any Color Name” \(p. 717\)](#)

Before you begin

You can color links and traffic to set up a well identified, valid path for the traffic type where the selected color refers.

Example: The following figure illustrates two colored links in an ASON domain that includes two external nodes and four networked nodes. One color link connects **Node A** and **Node B**. The second color link connects **Node B** and **Node C**. The color that is assigned to both colored links is **red**.

Figure 6-8 COLOR PROFILES – Colored Link Example



To associate a color link with an NPA, its physical link (connection), and optionally, a SRG, this task provides you examples that relate to [Figure 6-8, “COLOR PROFILES – Colored Link Example” \(p. 633\)](#) and instructs you to go to the “Task: Add links to ASON” (p. 1463) task and complete the steps in the task.

Task

Complete the following steps to associate a colored link with a physical connection and NPA over an existing ASON domain.

- 1 If a physical connection has not already been created, create the physical connection. Refer to the [7.19 “Create an OTN physical connection” \(p. 784\)](#) task for detailed steps.
- 2 If an NPA has not already been created, create an NPA. Refer to the [10.8 “Create and remove an NPA” \(p. 1443\)](#) task for detailed steps.

Associate a colored link Over an existing ASON domain

3

From the WebUI, follow this path:

OPERATE > Network Profiles > COLOR PROFILES > More [More] > Used In

Result: The system displays the Color Profiles data table.

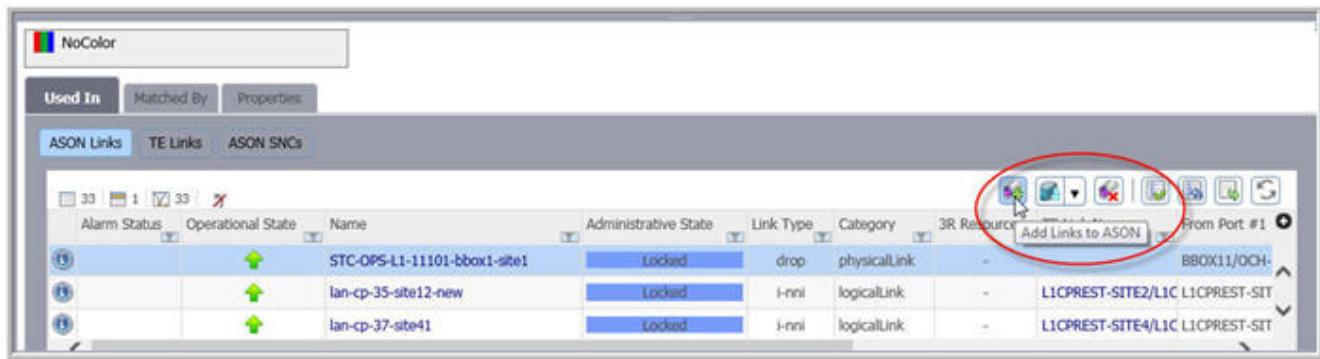
4

From the bottom data table, click on the icon **Add links to ASON**.

Result: The **Add links to ASON** panel is displayed. Through this window begin to associate a link to an NPA ASON.

Example: Looking at [Figure 6-8, "COLOR PROFILES – Colored Link Example" \(p. 633\)](#), begin to configure the resources in this step from **Node A** to **Node B**. Repeat this step, and the following steps, for **Node B** to **Node C**.

Figure 6-9 Color Profile – Add links to ASON Window



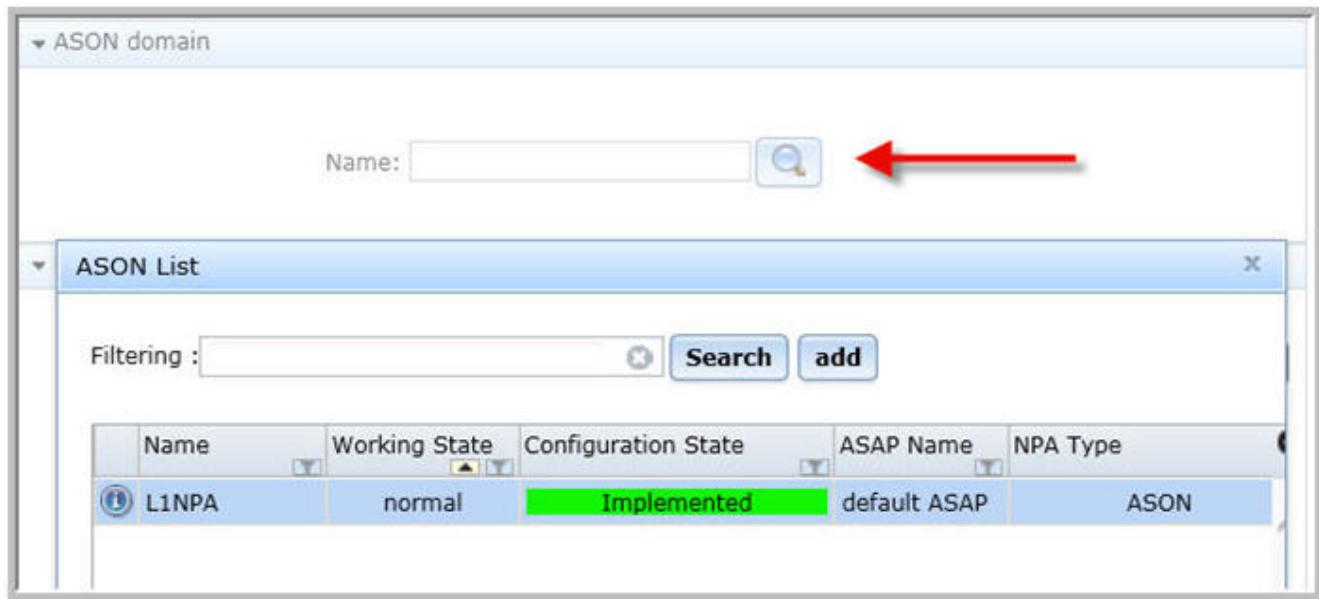
5

In the **ASON Domain** panel, click on the **Add** button to select the ASON domain to which the colored link must be included.

Result: The ASON List Window is displayed.

Associate a colored link Over an existing ASON domain

Figure 6-10 Color Profile – ASON Domain – ASON List Window



6

Perform the [10.15 “Add links and remove links from ASON” \(p. 1462\)](#) task.

Example: Looking at [Figure 6-8, “COLOR PROFILES – Colored Link Example” \(p. 633\)](#), in the **Color Profile** field in the **Link Parameters** panel, if you were to assign a color profile for **Node A** to **Node B** you would select **Red (Predefined_01)**. In addition, you would then have to select **Red (Predefined_01)** for **Node B** to **Node C**.

7

Click **Deploy**.

Result: The system adds your parameter specifications to the NPA and outputs a ✓ Success message at the bottom of the window.

8

Optional: To further associate resources, for example those in [Figure 6-8, “COLOR PROFILES – Colored Link Example” \(p. 633\)](#) from **Node B** to **Node C**, repeat [Step 4](#) to [Step 7](#).

9

Create a service or infrastructure connection. Refer to [7.8 “Design and publish a template for a connection” \(p. 741\)](#) and [7.12 “Deploy a template to make a connection” \(p. 754\)](#).

In **ASON** panel of the **Advanced Settings** for the deployed service or infrastructure, specify the color policy (the color template) of the connection to be **Include Any Color Name** or **Exclude Any Color Name**. Refer to “[Include Any Color Name](#)” (p. 717) and “[Exclude Any Color Name](#)” (p. 717).

END OF STEPS

6.17 Create a Color Profile

Purpose

Use this task to create a new color profile.

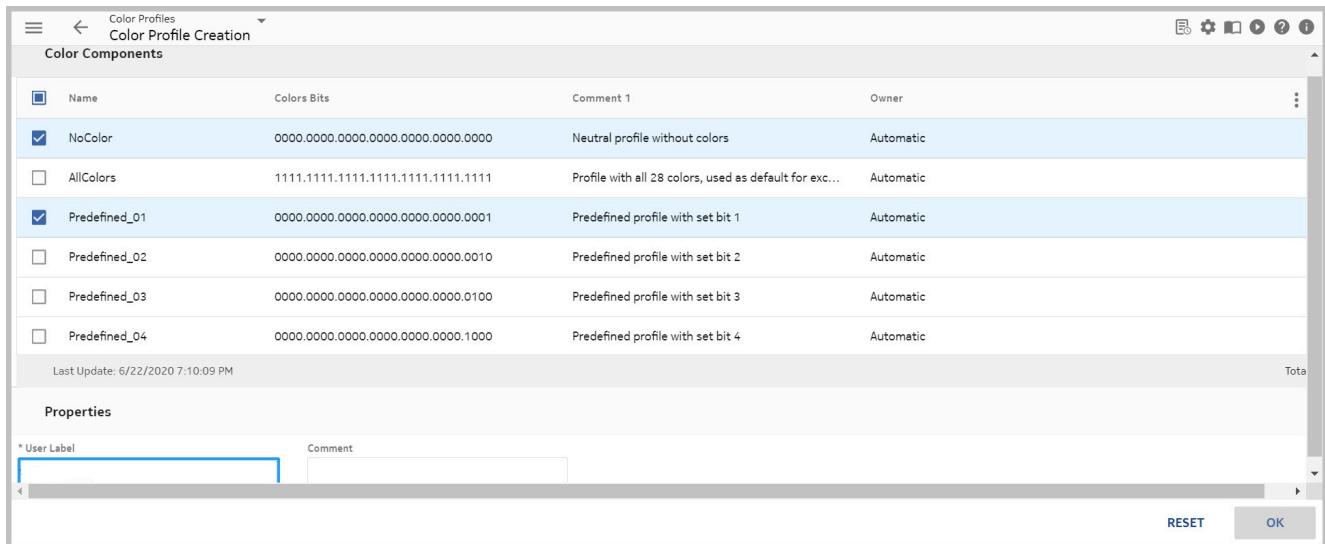
This task enables the users to add the color components that are needed to create a New Color Profile. To create a New Color Profile, users must select more than one existing color profile.

Task

Complete the following steps to create a new color profile.

- 1 _____
From the WebUI, follow one of these navigation paths:
OPERATE > Network Profiles.
- 2 _____
Click **COLOR PROFILES** tab.
Result: The system displays the list of color profiles in the data table.
- 3 _____
Click **Create Color Profile**() icon.
Result: The system displays the **Color Profile Creation** window.

Figure 6-11 Color Profile Creation window



4

In the **Color Components** panel, select the color profiles.

 **Note:** Ensure that at least two color profiles are added.

5

In the **Properties** panel, enter the name and comment in the **User Label** and **Comment** fields respectively.

6

Click **OK**.

Result: The New **Color Profile** is created and added to the **Color Profile** list.

END OF STEPS

6.18 Manage ASON Links assigned to a Color Profile

Purpose

The Color Profile data table has tabs for **Used In** and **Matched By**. These tabs have a sub-tab for ASON Links. The **ASON Links** sub-tab and **LINKS** tab, which is displayed for **ASON NPAs**, provide the same actions and functions for links. On the WebUI, follow the path : **OPERATE > Network Profiles > COLOR PROFILES > More :** > **Used In > ASON Links tab**

Task

Complete following steps to manage ASON Links assigned to a Color Profile.

- 1 _____
To set the administrative state, see [10.27 “Set the ASON administrative state of links” \(p. 1504\)](#).
- 2 _____
To change the add or remove links, see [10.15 “Add links and remove links from ASON” \(p. 1462\)](#).
- 3 _____
For Link Maintenance Window, see [10.25 “Perform link maintenance” \(p. 1497\)](#).
- 4 _____
For Change ASON WTR (wait time to restore), see [10.18 “Change ASON WTR” \(p. 1475\)](#).
- 5 _____
For automatic restoration, see [10.20 “Enable or disable auto restoration of links” \(p. 1480\)](#).
- 6 _____
For Misalignment Report, see [10.14 “Access and view the misalignment report for a link” \(p. 1461\)](#).

END OF STEPS _____

6.19 Manage ASON SNCs assigned to a Color Profile

Purpose

Use this task to manage the ASON SNCs that are assigned to a color profile.

The Color Profile data table has tabs for **Used In** and **Matched By**. These tabs have a subtab for ASON SNCs. The **ASON SNCs** sub-tab and **ASON SNCs** tab, which is displayed for **ASON NPAs**, provide the same actions and functions for SNCs. On the WebUI, follow the path : **OPERATE > Network Profiles > COLOR PROFILES > More  icon > Used In > ASON SNCs (tab)**.

Task

Complete the following steps to manage the ASON links that are assigned to a color profile.

- 1 _____
For Display Route on Map, see [10.41 “Manage SNCP in ASON SNC” \(p. 1553\)](#)
- 2 _____
To enable and disable test mode, see [10.40 “Enable/Disable the test mode for an SNC \(p. 1550\)](#).
- 3 _____
For Convert current to nominal, Switch to Nominal, and Switch to Backup, see [10.44 “Switch SNC routes” \(p. 1560\)](#).
- 4 _____
For Modify Attributes, see [10.43 “Modify the attributes of an SNC” \(p. 1557\)](#).
- 5 _____
For SNC Constraints Management, see [10.42 “Manage SNC constraints” \(p. 1554\)](#).
- 6 _____
For Inherited Priorities, see [10.37 “View the inherited priorities of an SNC” \(p. 1542\)](#).
- 7 _____
For Correlate ASAP see [10.39 “Correlate an ASAP with SNC” \(p. 1546\)](#).
- 8 _____
For Misalignment report, see [10.38 “View a misalignment report for an SNC” \(p. 1544\)](#).
- 9 _____
For Jobs, see [“Jobs” \(p. 1194\)](#)

END OF STEPS _____

6.20 Manage TE Links assigned to a Color Profile

Purpose

Use this task to manage the TE links that are assigned to a color profile.

The Color Profile data table has tabs for **Used In** and **Matched By**. These tabs have a sub-tab for TE Links. The **TE Links** sub-tab and **TE LINKS** tab, which is displayed for ASON NPAs, provide the same actions and functions for links. On the WebUI, follow the path : **OPERATE > Network Profiles > COLOR PROFILES > More  icon > Used In > TE LINKS (tab)**.

Task

Complete the following steps to manage the TE links that are assigned to a color profile.

- 1 _____
To Modify TE links, see [10.24 “Modify TE Links” \(p. 1495\)](#).
 - 2 _____
For Misalignment Report, see [10.14 “Access and view the misalignment report for a link” \(p. 1461\)](#).
 - 3 _____
For Jobs, see [“Jobs” \(p. 1194\)](#)
- END OF STEPS** _____

6.21 View a list of Color Profiles

Purpose

Use this task to view the list of color profiles in the data table.

Task

Complete the following steps to view the list of color profiles in the data table.

1

From the WebUI, follow the path:

OPERATE > Network Profiles

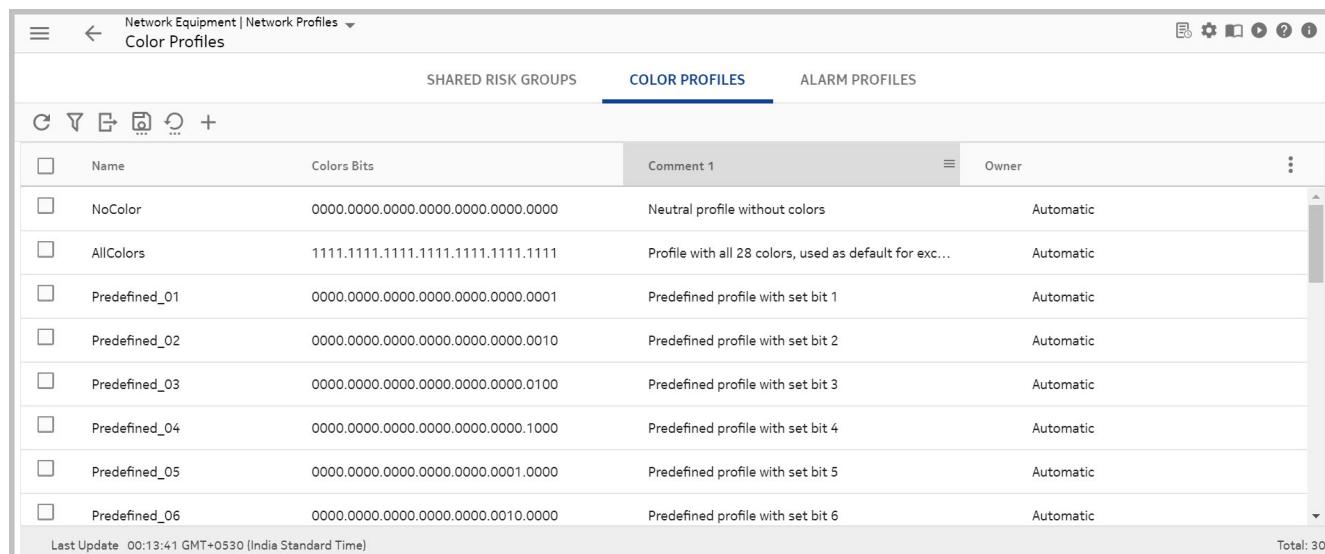
Result: The system displays the list of network profiles in the data table.

2

Click **COLOR PROFILES** tab.

Result: The system displays the Color Profiles in the data table

Figure 6-12 List of Color Profiles



The screenshot shows a web-based interface for managing network profiles. At the top, there's a navigation bar with icons for back, forward, search, and other system functions. Below the bar, the title 'Network Equipment | Network Profiles' is followed by a dropdown menu and the specific section 'Color Profiles'. The main area is a data table with three tabs at the top: 'SHARED RISK GROUPS', 'COLOR PROFILES' (which is currently selected and highlighted in blue), and 'ALARM PROFILES'. The table has columns for 'Name', 'Colors Bits', 'Comment', and 'Owner'. There are 30 entries listed, each with a checkbox next to the name. The first few entries are: 'NoColor' (Colors Bits: 0000.0000.0000.0000.0000.0000), 'AllColors' (Colors Bits: 1111.1111.1111.1111.1111.1111), 'Predefined_01' (Colors Bits: 0000.0000.0000.0000.0000.0001), 'Predefined_02' (Colors Bits: 0000.0000.0000.0000.0000.0010), 'Predefined_03' (Colors Bits: 0000.0000.0000.0000.0000.0100), 'Predefined_04' (Colors Bits: 0000.0000.0000.0000.0000.1000), 'Predefined_05' (Colors Bits: 0000.0000.0000.0000.0000.0001), and 'Predefined_06' (Colors Bits: 0000.0000.0000.0000.0000.0010). The 'Comment' column provides a brief description of each profile, and the 'Owner' column shows 'Automatic' for all. At the bottom of the table, it says 'Last Update 00:13:41 GMT+0530 (India Standard Time)' and 'Total: 30'.

3

To view the additional attributes, click **Properties**  icon.

Figure 6-13 COLOR PROFILES Properties

COLOR PROFILES				
	Name	Colors Bits	Comment	Owner
<input type="checkbox"/>	NoColor	0000.0000.0000.0000.0000.0000.0000	Neutral profile without colors	Automatic
<input type="checkbox"/>	AllColors	1111.1111.1111.1111.1111.1111.1111	Profile with all 28 colors, used as default for exc...	Automatic
<input type="checkbox"/>	Predefined_01	0000.0000.0000.0000.0000.0000.0001	Predefined profile with set bit 1	Automatic
<input type="checkbox"/>	Predefined_02	0000.0000.0000.0000.0000.0000.0010	Predefined profile with set bit 2	Automatic
<input type="checkbox"/>	Predefined_03	0000.0000.0000.0000.0000.0000.0100	Predefined profile with set bit 3	Automatic
<input type="checkbox"/>	Predefined_04	0000.0000.0000.0000.0000.0000.1000	Predefined profile with set bit 4	Automatic
<input type="checkbox"/>	Predefined_05	0000.0000.0000.0000.0000.0001.0000	Predefined profile with set bit 5	Automatic
<input type="checkbox"/>	Predefined_06	0000.0000.0000.0000.0000.0010.0000	Predefined profile with set bit 6	Automatic

4

Click the **More** icon and follow the popup menu item **Remove** or **Used In** or **Matched By**.

If you select the item **Used In**, a new window is displayed that has ASON Links, TE Links and ASON SNC tabs.

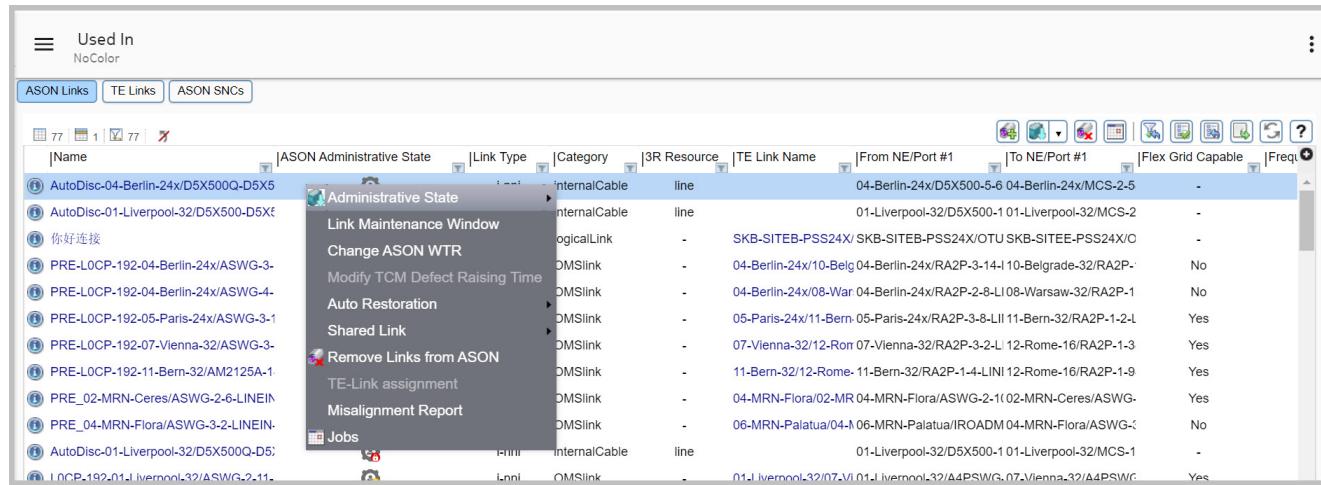


Note: The **Remove** item is enabled only for customized color profiles.

Click **ASON Links** (tab)

Result: The system displays the ASON links. Right click an object and for more information on the right click navigations, see the following:

Figure 6-14 Actions on ASON links tab of Color Profiles



To set the administrative state, see [10.27 “Set the ASON administrative state of links” \(p. 1504\)](#).

To view the Link Maintenance window, see [10.25 “Perform link maintenance” \(p. 1497\)](#).

To change ASON WTR, see [10.18 “Change ASON WTR” \(p. 1475\)](#).

To enable or disable auto restoration of ASON links, see [10.20 “Enable or disable auto restoration of links” \(p. 1480\)](#).

To add or remove links from ASON, see [10.15 “Add links and remove links from ASON” \(p. 1462\)](#).

To assign TE links, see [10.17 “Assign an ASON I-NNI link to a TE Link and SRG” \(p. 1473\)](#).

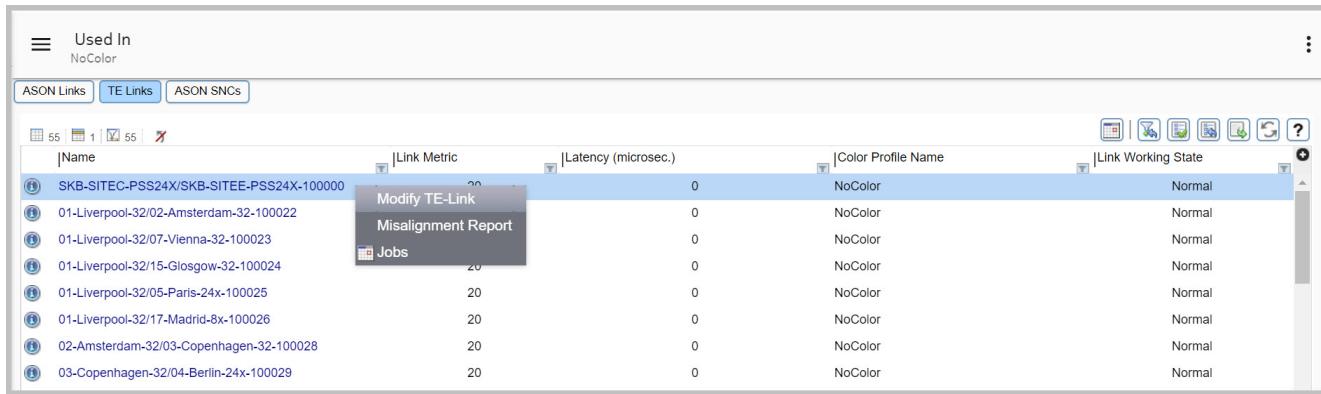
To view the misalignment report, see [10.14 “Access and view the misalignment report for a link” \(p. 1461\)](#)

5

Click on the **TE links** tab.

Result: The system displays the TE links. Right click an object and for more information on the right click navigations, see the following:

Figure 6-15 Right click actions on TE links tab of Color Profiles



END OF STEPS

6.22 View tabbed topics for a Color Profile

When to use

Use this task to view the tabbed topics for a color profile.

Related information

See the following topics in this document:

- [6.14 “Resource Coloring” \(p. 627\)](#)

Before you begin

The data table for color profiles includes automatic color profiles, which are system-supplied, and user-created color profiles.

- The automatic color profiles are named **NoColor**, **AllColors**, and **Predefined_01....Predefined_28**.
- The user-created color profiles are named any name except **NoColor**, **AllColors**, and **Predefined_01....Predefined_28**.

The automatic color profiles include **NoColor**, **AllColors**, and **Predefined_01....Predefined_28**.
The user-created color profiles have any other name except **NoColor**, **AllColors**, and **Predefined_01....Predefined_28**.

Task

Complete the following steps to view the tabbed topics for an infrastructure connection or service.

1

From the WebUI, follow the navigation path :

OPERATE > Network Profiles > COLOR PROFILES

Result: The system displays the Color Profiles data table.

2

Click on the **COLOR PROFILES** tab.

Result: The data table for COLOR PROFILES is displayed.

Figure 6-16 COLOR PROFILES – Data Table

The screenshot shows a software interface titled "Network Equipment | Network Profiles" with a sub-section "Color Profiles". At the top, there are tabs for "SHARED RISK GROUPS", "COLOR PROFILES" (which is currently selected), and "ALARM PROFILES". Below the tabs is a toolbar with icons for search, refresh, and other operations. The main area is a table with columns: "Name", "Colors Bits", "Comment 1", "Owner", and a vertical ellipsis. The table contains eight rows, each representing a color profile. The profiles are: "NoColor" (bitmask 0000.0000.0000.0000.0000.0000), "AllColors" (bitmask 1111.1111.1111.1111.1111.1111), "Predefined_01" (bitmask 0000.0000.0000.0000.0000.0001), "Predefined_02" (bitmask 0000.0000.0000.0000.0000.0010), "Predefined_03" (bitmask 0000.0000.0000.0000.0000.0100), "Predefined_04" (bitmask 0000.0000.0000.0000.0000.1000), "Predefined_05" (bitmask 0000.0000.0000.0000.0001.0000), and "Predefined_06" (bitmask 0000.0000.0000.0000.0010.0000). The "Comment 1" column provides a brief description of each profile. The "Owner" column shows "Automatic" for all profiles. The bottom of the table displays "Last Update 00:13:41 GMT+0530 (India Standard Time)" and "Total: 30".

Name	Colors Bits	Comment 1	Owner
NoColor	0000.0000.0000.0000.0000.0000	Neutral profile without colors	Automatic
AllColors	1111.1111.1111.1111.1111.1111	Profile with all 28 colors, used as default for exc...	Automatic
Predefined_01	0000.0000.0000.0000.0000.0001	Predefined profile with set bit 1	Automatic
Predefined_02	0000.0000.0000.0000.0000.0010	Predefined profile with set bit 2	Automatic
Predefined_03	0000.0000.0000.0000.0000.0100	Predefined profile with set bit 3	Automatic
Predefined_04	0000.0000.0000.0000.0000.1000	Predefined profile with set bit 4	Automatic
Predefined_05	0000.0000.0000.0000.0001.0000	Predefined profile with set bit 5	Automatic
Predefined_06	0000.0000.0000.0000.0010.0000	Predefined profile with set bit 6	Automatic

3

Do one of the following:

- The available options for an automatic color profile are **Used In**, **Matched by**, and **Remove**.

The available tabs for a user-created color profile are **Elementary Colors**, **Matched by**, and **Properties**.

Important Usability Notes:

- For automatic profiles, the **Used In** and **Matched by** topics have a secondary set of tabs, which are the following:

[25.7 “ASON Links Tab” \(p. 2069\)](#)

[25.55 “TE Links Tab” \(p. 2172\)](#)

[25.9 “ASON SNC Tab” \(p. 2073\)](#)

- For user-created profiles, the **Matched by** tabbed topics has a secondary set of tabs, which are the following:

[25.7 “ASON Links Tab” \(p. 2069\)](#)

[25.55 “TE Links Tab” \(p. 2172\)](#)

[25.9 “ASON SNC Tab” \(p. 2073\)](#)

- The functions that are provided with the **ASON Links**, **TE Links**, and **ASON SNCs** tabbed topics are the same functions that are provided when you access NPAs and SNCs directly from the **OPERATE > ASON** navigation path. Refer to [6.18 “Manage ASON Links assigned to a Color Profile” \(p. 639\)](#), [6.20 “Manage TE Links assigned to a Color Profile” \(p. 641\)](#), and [6.19 “Manage ASON SNCs assigned to a Color Profile” \(p. 640\)](#) to be redirected to the appropriate task under the **OPERATE > ASON** navigation path.

Result: The system activates the tabs and the color profile-related information is displayed directly below the data table for the color profile.

Note: To return to the original data table, click the browser back arrow.

4

Optional: To view the details of a selected item in either the top or bottom data table, click on the  icon. Refer to "["View additional attributes for a selected item in a data table" \(p. 2194\)](#)" for details.

Result: The system displays detailed information for the selected item.

END OF STEPS

Alarm Profiles

6.23 Alarm Profiles

Alarm Profile definition

An *alarm profile* is a user-created description of the type and severity of the correlated alarms that are to be monitored for the 1830 PSS photonic (PHN) and 1830 PSS OCS network elements (NEs).

Alarm profile functional description

The NFM-T supplies users with a default system connection profile, which is called the *default ASAP*. The *default ASAP* consists of default values for the user label, severities, and correlated alarm probable causes (CA PC) names. The *default ASAP* is applicable to all OTN connections.

By using a clone of the system-supplied *default ASAP*, users can change the settings of the *default ASAP* and create their own user-defined correlated Alarm Severity Assignment Profiles (ASAPs) to suit their installation.

Users can correlate their ASAP settings to the following:

- To individual or multiple (all) connections whose correlation is managed by OTN (logical and physical) in the **Implemented** state, regardless of whether an **Add**, or **Discover**, or **Re-arrange** order exists for the connection.
- To individual or multiple (all) mixed plane, end-to-end connections in which ASON probable cause (PC) severities are set from OTN and implemented by ASON.
- To a particular connection layer rate in the system if users filter the connection list that is displayed on the data table via **Service Rate**.

Can assign network ASAP to connections of a particular layer rate if you filter the connection list via layer rate. Otherwise, there is no specific workflow to assign ASAP to a particular layer rate

Example:

- A user can create an alarm profile and change the default severity of a **Transport Failure** from **Major** to **Critical** and the default severity of a **Client Failure** from **Minor** to a **Warning**.

Once users create their alarm profiles and apply them to existing connections or layer rates, the correlated alarm probable cause severities that are associated with these connections change and are displayed accordingly in the affected NFM-T GUI screens, which include the Alarms tab, the Dashboard, the Routing Display, the data tables that are associated with the connection.

Alarm profiles and Auto Discovery

When a connection is initially discovered in the network, the **default ASAP** is correlated to the discovered connections.

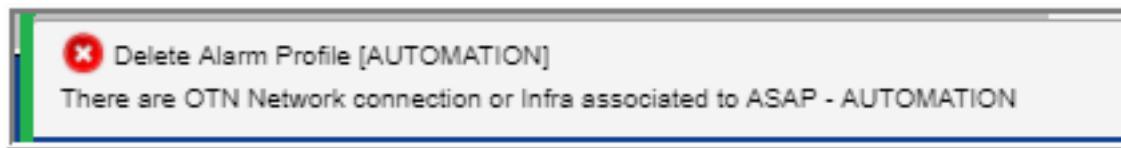
When an existing connection and its clients are deleted (*DBdeleted*) and then rediscovered, any existing correlations to alarm profiles are lost and the **default ASAP** is correlated to the connection during discovery.

Delete an Alarm Profile

To delete an alarm profile follow the path **OPERATE > Network Profiles > ALARM PROFILES**. Select the Alarm Profile to delete, click **More**  icon and select the option **Remove** on the popup menu. A confirmation box is displayed to confirm the operation.

When an alarm profile is deleted, there is a check to prevent the ASAP Profile deletion if the profile is associated to any OTN Infrastructure Connection, Physical Connection, ASON SNC or ASON NPA. An error message is displayed in the log panel.

Figure 6-17 Alarm Profile deletion - Error Message Example



User interaction with Alarm Profiles

Users can view, create, modify, and remove Alarm Profiles. In addition, users can view the alarm profiles that are associated with particular connections and users can correlate an alarm profile to a physical or logical connection. Refer to the following tasks for detailed steps:

- [6.27 “View Alarm Profiles” \(p. 658\)](#)
- [6.28 “View Tabbed Topics for an Alarm Profile” \(p. 660\)](#)
- [6.24 “Create an Alarm Profile” \(p. 651\)](#)
- [6.26 “Modify an Alarm Profile” \(p. 656\)](#)
- [6.25 “Determine the Network Alarm Profile Assigned to a Connection” \(p. 653\)](#)
- [7.29 “Correlate an OTN physical connection with an ASAP” \(p. 830\)](#)
- [“Task: Correlate a commissioned connection to an ASAP” \(p. 925\)](#)

6.24 Create an Alarm Profile

Purpose

Use this task to create an alarm profile.

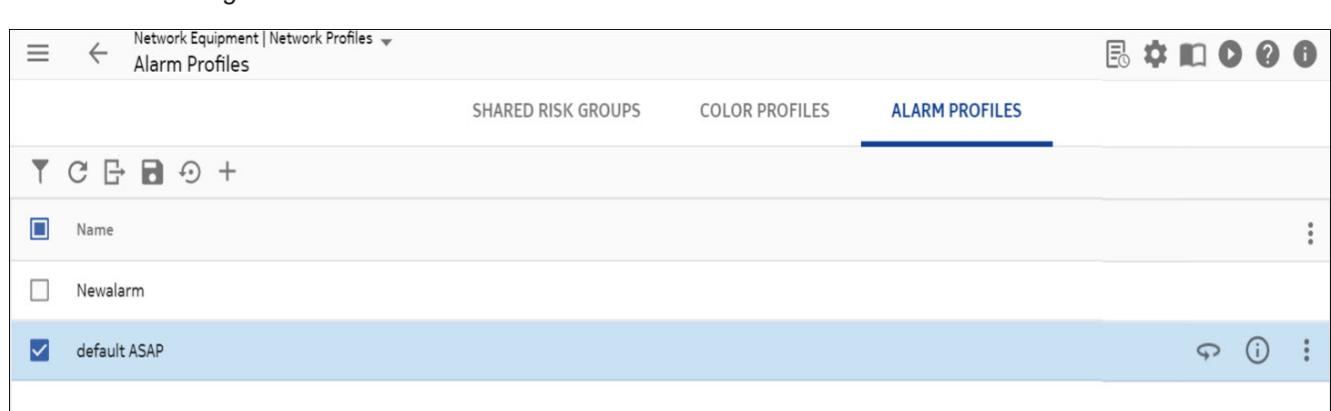
If the alarm profiles have not been created, the only alarm profile that is displayed on the data table list is that of the default ASAP.

Task

Complete the following steps to create an alarm profile:

- 1 _____
From the WebUI, follow this navigation path:
OPERATE > Network Profiles.
- 2 _____
Click on the **ALARM PROFILES** tab.
Result: The system displays the Alarm Profiles data table.
- 3 _____
On the top left, **Create Alarm Profile** () icon.
Result: The Alarm Profile Identification window is displayed.

Figure 6-18 ALARM PROFILES – Alarm Profile Identification window



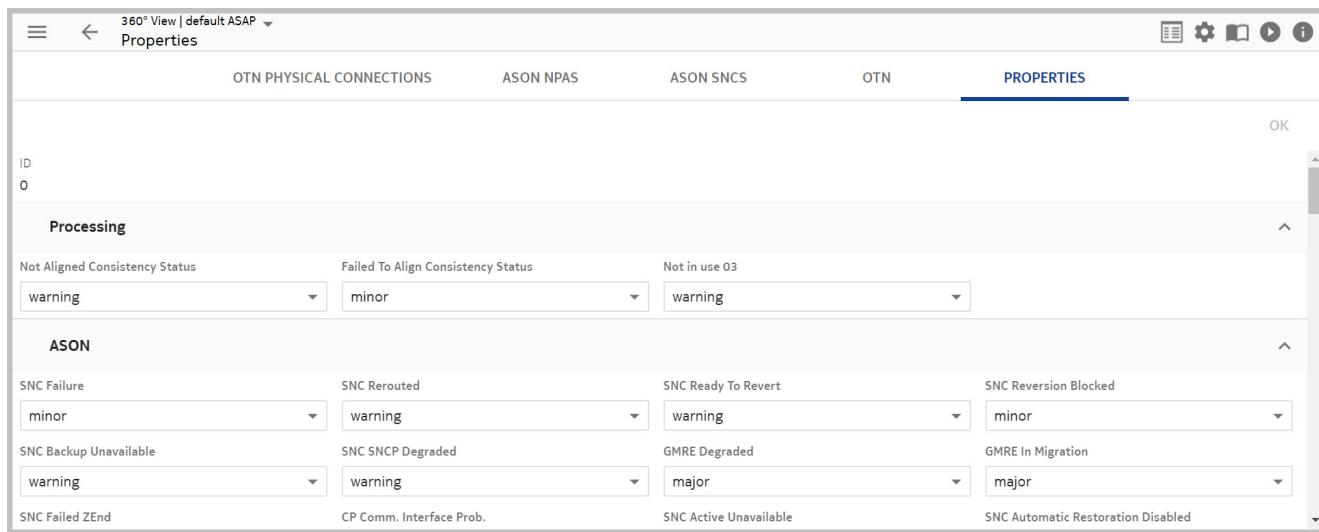
- 4 _____
In the **Name** field, enter a name to identify the alarm profile that you are creating.
Result: The system displays a ✓ Success message at the bottom of the Alarm Profile Identification window and enters the profile that you created in the Alarms Profile data table.

5

To change the default settings in the profile that you just created, from the WebUI, follow the navigation path : **OPERATE > Network Profiles > ALARM PROFILES > 360° View** and click **PROPERTIES** tab .

Result: The system displays the panels of the **PROPERTIES** tab.

Figure 6-19 ALARM PROFILES – Panels in the PROPERTIES TAB



6

To change the required parameter settings, click the down arrow next to the field name and select a new option.

7

To save your changes, click on the **OK** option, which is located in the upper right corner of the window.

Result: The correlated alarm profile is created and modified according to your change requests. The affected OTN WebUI screens, which include the Alarms tab, the Dashboard, the Routing Display, the data tables that are associated with the connection are updated accordingly.

END OF STEPS

6.25 Determine the Network Alarm Profile Assigned to a Connection

Purpose

Use this task to determine the network alarm profile that is assigned to a connection.

By default, the default ASAP is assigned to all the OTN connections. By accessing the data table for a Physical Connection, an Infrastructure Connection, or a Service; this task enables you to determine if an ASAP, other than the default ASAP, is assigned to a selected connection.

Task

Complete the following step of this task to determine the network alarm profile that is assigned to a connection.

1

Do one of the following

- **OPERATE > Physical Connections**
- **OPERATE > Infrastructure Connections**
- **OPERATE > Services**

Result: The system displays the data table for the selected object.

2

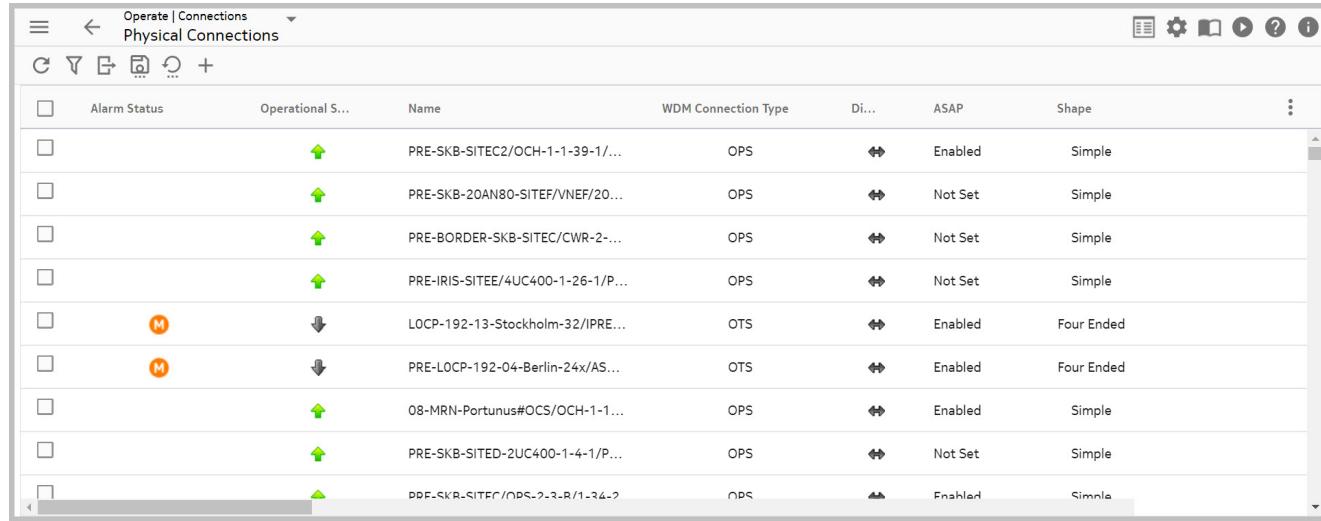
Locate the connection or connections, and do one or both of the following:

For Physical Connections and Infrastructure Connections:

1. Click **More**  icon on the top right hand corner.
2. Click on **Manage Columns...**, Manage Columns window pops up.
3. Scroll through the list and select **ASAP**.

Determine the Network Alarm Profile Assigned to a Connection

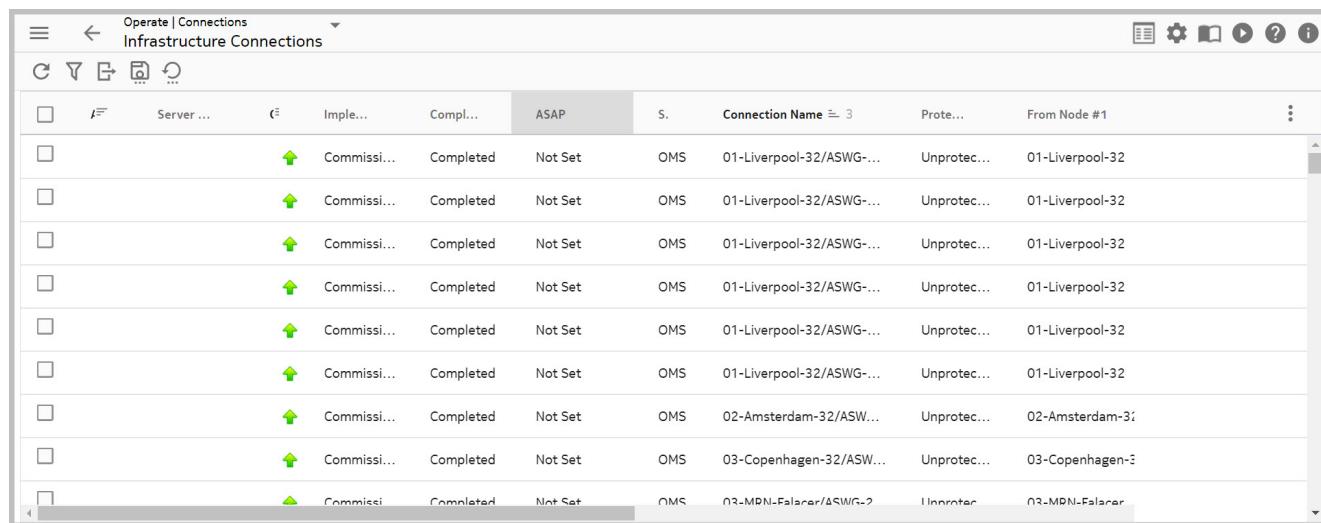
Figure 6-20 ASAP column for Physical Connections



The screenshot shows a table titled "Physical Connections". The columns are: Alarm Status, Operational S..., Name, WDM Connection Type, Di..., ASAP, Shape, and a More icon. The "ASAP" column is highlighted in grey. The data rows include:

Alarm Status	Operational S...	Name	WDM Connection Type	Di...	ASAP	Shape	More
		PRE-SKB-SITEC2/OCH-1-1-39-1/...	OPS	↔	Enabled	Simple	⋮
		PRE-SKB-20AN80-SITEF/VNEF/20...	OPS	↔	Not Set	Simple	⋮
		PRE-BORDER-SKB-SITEC/CWR-2...	OPS	↔	Not Set	Simple	⋮
		PRE-IRIS-SITEE/4UC400-1-26-1/P...	OPS	↔	Not Set	Simple	⋮
	M	LOCP-192-13-Stockholm-32/IPRE...	OTS	↔	Enabled	Four Ended	⋮
	M	PRE-LOCP-192-04-Berlin-24x/AS...	OTS	↔	Enabled	Four Ended	⋮
		08-MRN-Portunus#OCS/OCH-1-1...	OPS	↔	Enabled	Simple	⋮
		PRE-SKB-SITED-2UC400-1-4-1/P...	OPS	↔	Not Set	Simple	⋮
		PDF-SKR-SITEF/OPSL-2-2-R/1-24-2	OPS	▲	Enabled	Simple	⋮

Figure 6-21 ASAP column for Infrastructure Connections



The screenshot shows a table titled "Infrastructure Connections". The columns are: Server ..., Imple..., Compl..., ASAP, S., Connection Name, Prote..., From Node #1, and a More icon. The "ASAP" column is highlighted in grey. The data rows include:

Server ...	Imple...	Compl...	ASAP	S.	Connection Name	Prote...	From Node #1	More
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	01-Liverpool-32/ASWG-...	Unprotect...	01-Liverpool-32	⋮
		Completed	Not Set	OMS	02-Amsterdam-32/ASW...	Unprotect...	02-Amsterdam-32	⋮
		Completed	Not Set	OMS	03-Copenhagen-32/ASW...	Unprotect...	03-Copenhagen-32	⋮
		Completed	Not Set	OMS	03-MRN-Falster/ASW/G-2	Unprotect...	03-MRN-Falster	⋮

For Services:

1. Click **More**  icon on the top right hand corner.
2. Click on **Manage Columns...**, Manage Columns window pops up.
3. Scroll through the list and select **NML ASAP**.

Determine the Network Alarm Profile Assigned to a Connection

Figure 6-22 NML ASAP column for Services

	Server ...	Im... ▾	Compl...	S.	Connection Name	▀ 3	NML ASAP	Prote...	From Node #1	⋮
□	■ M	▼	Commissioned	Completed	10...	RENAME-DSR-L1CP-10GbE	default ASAP	Unprotect...	SKB-SITEC-PSS24	

Result: The system displays the **ASAP/NML ASAP** column in the visible portion of the data table.

END OF STEPS

6.26 Modify an Alarm Profile

Purpose

Use this task to modify an existing alarm profile.

If alarm profiles have not been created, the only alarm profile that is displayed on the data table list is that of the **default ASAP**.

Task

Complete the following step this task to modify an existing alarm profile

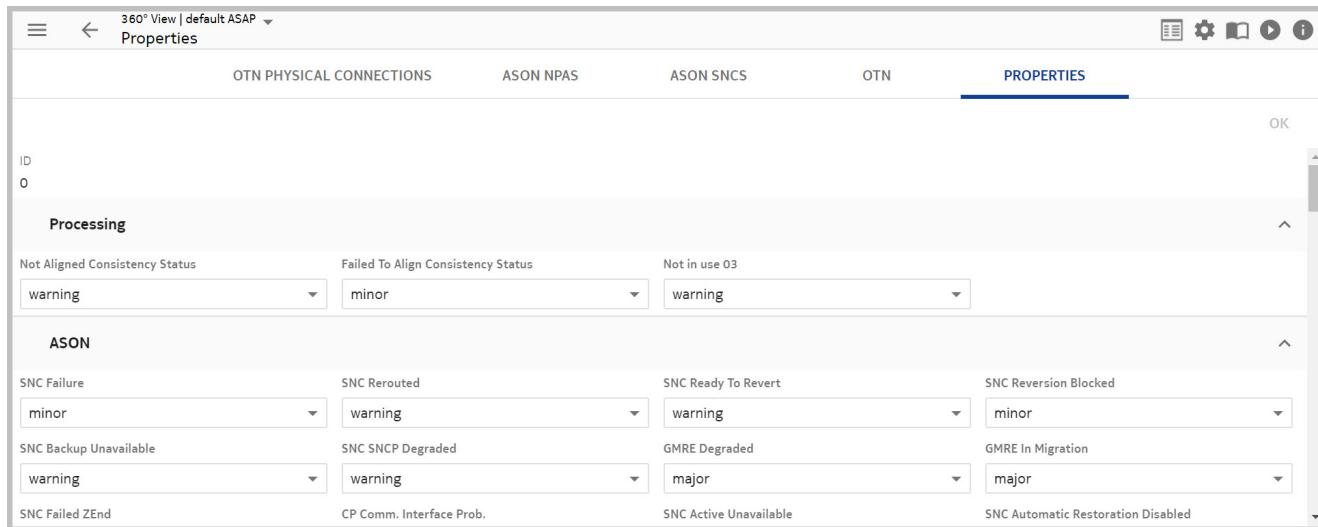
1

From the WebUI, follow this navigation path for the selected alarm profile:

OPERATE > Network Profiles > ALARM PROFILES > 360° View > PROPERTIES (tab)

Result: The system displays the panels of the **PROPERTIES** tab

Figure 6-23 ALARM PROFILES – Panels in the PROPERTIES Tab



2

Depending on the needs of your installation, open any of the panels of the **PROPERTIES** tab and change the required parameter settings by clicking on the down arrow next to the field name and selecting a new option.

3

To save your modifications, click **OK**.

Result: The system displays a message similar to the following at the bottom of the window:

Modify <alarm profile name>: ✓ Success

The correlated alarm profile is modified. The affected NFM-T GUI screens, which include the Alarms tab, the Dashboard, the Routing Display, the data tables that are associated with the connection, are updated accordingly.

END OF STEPS

6.27 View Alarm Profiles

Purpose

Use this task to view a list of alarm profiles.

If alarm profiles have not been created, the only alarm profile that is displayed on the data table list is that of the **default ASAP**.

Task

Complete the following steps to view a list of alarm profiles

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Network Profiles

Result: The system displays the **Network Profiles** data table.

2

Click on the **ALARM PROFILES** tab.

Result: The system displays the Alarm Profiles data table.

Figure 6-24 Alarm Profiles – Data Table

Figure 6-25 ALARM PROFILES – Data Table with Additional Columns Checked

The screenshot shows a data table titled "ALARM PROFILES". The table has columns: Name, CEP Fail..., Degraded Transmiss..., Encrypted Key I..., Failure On Repeater NSA, Failure On Repeater ... (partially visible), and Fast Photonic Re... (partially visible). A row is selected with the name "default ASAP" and the status "major" under the first two columns. The table includes standard UI elements like a header bar with back, forward, and search icons, and a toolbar with icons for create, edit, delete, and more.

Name	CEP Fail...	Degraded Transmiss...	Encrypted Key I...	Failure On Repeater NSA	Failure On Repeater ...	Fast Photonic Re...
default ASAP	major		major	minor	major	

3

Click **Properties** icon to view the additional attributes.

4

On the selected alarm profile, click **More** icon

Result: The system displays the following options:

Remove: to remove the selected alarm profile.

This screenshot shows the same "ALARM PROFILES" table as above, but with a different selection. The rows for "default ASAP", "test", and "AUTOMATION" are now selected. A blue rectangular box highlights the "Remove" button in the bottom right corner of the table area. The footer of the screen shows "Last Update: 3/12/2020 4:21:51 PM" and "Total: 3".

Name
default ASAP
test
AUTOMATION

END OF STEPS

6.28 View Tabbed Topics for an Alarm Profile

Purpose

Use this task to view tabbed topics for an alarm profile.

Task

Complete the following steps to view tabbed topics for an alarm profile.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Network Profiles

Result: The system displays the **Network Profiles** data table.

2

Click on the **ALARM PROFILES** tab:

Result: The system displays the Alarm Profiles data table.

Figure 6-26 ALARM PROFILES – Data Table

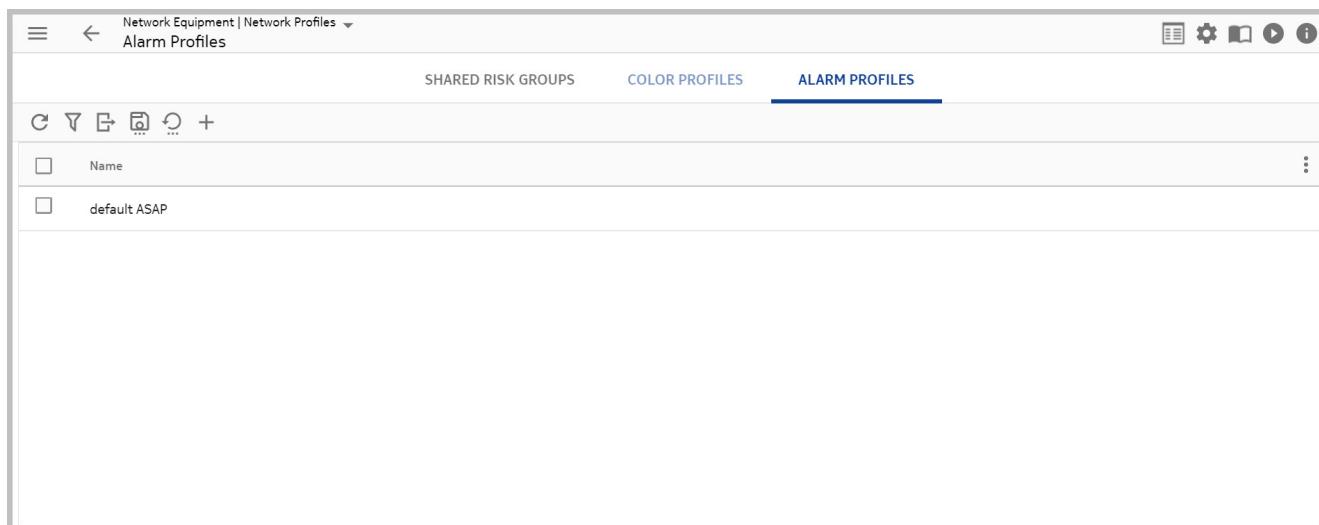


Figure 6-27 ALARM PROFILES – Data Table with Additional Columns Checked

Name	CEP Fail...	Degraded Transmiss...	Encrypted Key I...	Failure On Repeater NSA	Failure On Repeater ...	Fast Photonic Re...
default ASAP	major		major	minor	major	

3

To view the tabbed topics for an alarm profile, follow the navigation path :

OPERATE > Network Profiles > ALARM PROFILES > 360° View

The available tabs are the following:

[25.33 “OTN Physical Connections Tab” \(p. 2126\)](#)

[25.8 “ASON Network Protection Architecture \(NPA\) Tab” \(p. 2071\)](#)

[25.9 “ASON SNC Tab” \(p. 2073\)](#)

OTN Tab

[25.39 “Properties Tab” \(p. 2141\)](#)

Important Usability Notes:

- The functions that are provided with the **OTN Physical Connections** tabbed topic are the same functions that are provided when you access this object directly from the **OPERATE > Physical Connections** navigation path. Detailed tasks for physical connections can be found in the “Physical Connections” (p. 784) section.
- The functions that are provided with the **ASON NPAs** and **ASON SNCs** tabbed topics are the same functions that are provided when you access these objects directly from the **OPERATE > ASON > NPAs** and **OPERATE > ASON > SNCs** navigation paths. Detailed tasks for NPAs and SNCs can be found in the “Operate ASON NPAs” (p. 1438) and “Operate ASON SNC” (p. 1521) section.
- The functions that are provided with the **OTN** tabbed topic are the same functions that are provided when you access infrastructure connections and services directly from the **OPERATE > Infrastructure Connections** and **OPERATE > Services** navigation paths. Detailed tasks for these logical connections can be found in the “Infrastructure Connections and Services” (p. 913) section.

Result: The system activates the tabs and the connection-related information is displayed directly below the data table for the alarm profile.

Note: To return to the original data table, click the browser back arrow.

4

Optional: To view the details of a selected item in either the top or bottom data table, click on the  icon. Refer to “[View additional attributes for a selected item in a data table](#)” (p. 2194) for details.

Result: The system displays detailed information for the selected item.

END OF STEPS

7 Design, deploy and operate connections

7.1 Overview

Purpose

This chapter supplies user with the step required to Design, Deploy and make operative a connection.

Contents

7.1 Overview	663
Design and deploy a new service/infrastructure connection with templates	669
7.2 Connection template location and types	669
7.3 Field descriptions for Best Practices templates	675
7.4 Service definition field descriptions for deploy Best Practices templates	688
7.5 Advanced Settings field descriptions for deploy Best Practices templates	708
7.6 Routing Constraints	731
7.7 Access and view a connection template	738
7.8 Design and publish a template for a connection	741
7.9 Modify a template for a connection	745
7.10 Publish/Unpublish a connection template	748
7.11 Copy an existing template or delete a template	750
7.12 Deploy a template to make a connection	754
7.13 Unterminated service or ODU unterminated with NNI client	765
7.14 Different modes of creating a connection	766
7.15 Node or physical link as constraint	770
Component Templates	771
7.16 Overview	771
7.17 Manage Routing Constraints	772
7.18 Manage Transmission Parameters	777
Physical Connections	784
7.19 Create an OTN physical connection	784

7.20 Manage the inventory view of Physical Connections	806
7.21 Manage data columns on Physical Connections page	811
7.22 Delete an OTN physical connection	813
7.23 Delete OTS and OPS connections from NFM-T	815
7.24 Associate/Disassociate dark fiber to physical connection	817
7.25 Configure alarms of an OTN physical connection	820
7.26 Configure the service state of an OTN physical connection	822
7.27 Configure OLC State for connections and services	823
7.28 Correlate an OTN physical connection with an SRG	827
7.29 Correlate an OTN physical connection with an ASAP	830
7.30 Delete the clients of OTN physical connection	833
7.31 Implement/Deimplement an OTN physical connection	835
7.32 Manage GMRE enabled ASON Link from OTN physical connections	837
7.33 Move Traffic from a link for L0 Control Plane and MRN	840
7.34 Move Traffic from a link for Managed Plane	845
7.35 Manage repeaters for an OTN OTS physical connection	850
7.36 Manage third party vendor networks for a physical connection	868
7.37 Modify the fiber characteristics of an OTN physical connection	877
7.38 Modify Utilization Profile for a physical/infrastructure connection	881
7.39 Rename an OTN physical connection or/and of its port on an ENE	884
7.40 View a misalignment report for an OTN physical connection	886
7.41 View Physical Connections	888
7.42 View the 360° tabs for a physical connection	890
7.43 Physical Connections list further actions	893
7.44 Physical Connections table columns	896
Import Physical Connections and Nodes from CSV file	900
7.45 Import from CSV function	900
7.46 Import Physical Connections from CSV file	901
7.47 Import CSV Template file to Create a Node(s)	907
Infrastructure Connections and Services	913
7.48 Overview	913

7.49 Control the deployment of a connection	915
7.50 Clone a connection	918
7.51 Delete a commissioned connection	919
7.52 Delete a commissioned infrastructure and clients	922
7.53 Manage alarms for a connection	924
7.54 Clear ASAP inconsistencies on a connection	936
7.55 Manage additional text attribute (Alias) - Infrastructure Connections and Services	947
7.56 Manage protection groups (MSP/SNCP) for a protected connection	952
7.57 Manage NIM for a connection	954
7.58 Manage protection for a connection in Managed Plane and Control Plane	960
7.59 Manage protection for a Mixed Plane service	968
7.60 Manage the service state of connection	975
7.61 Manage 3R for Managed Plane connections	978
7.62 Modify the parameters of a connection	981
7.63 Modify Route (Reroute) of a connection	987
7.64 Rename Connection and Customer Name	997
7.65 Manage the inventory view of Infrastructure Connections	1000
7.66 Manage Columns on Infrastructure Connections page	1004
7.67 Manage the inventory view of Services	1006
7.68 Manage data columns on Services page	1010
7.69 Set transmission parameters	1012
7.70 View Failure Analysis for an infrastructure connection or service	1013
7.71 View Jobs for an infrastructure connection or service	1016
7.72 View Infrastructure Connections or Services	1019
7.73 View Eline connection on Carrier Ethernet Links and Carrier Ethernet OAM pages in ESM	1022
7.74 View slots for an infrastructure connection	1024
7.75 1830 PSD Service Testing and BER Monitor	1025
7.76 View tabbed topics for an infrastructure connection or service	1032
7.77 View various route displays for an infrastructure connection or service	1036

7.78 View the Routing Display of a selected connection	1042
7.79 Infrastructure Connections columns	1054
7.80 Services columns	1059
7.81 Infrastructure Connections list further actions	1063
7.82 Services list further actions	1067
7.83 Resize ODUFlex Bandwidth	1071
7.84 Service Analytics Dashboard	1080
Protected Connections	1088
7.85 Manage Protected Connections	1088
7.86 View Protected Connections	1091
7.87 View tabbed topics for a protected connection	1095
7.88 OTN Protected Connections data columns	1098
7.89 Perform Synchronize Switch Position	1103
7.90 Perform protection switching	1106
7.91 Perform Force Switch Operation	1112
7.92 Manage OPSA protection with revertive mode	1114
TCM on Infrastructure Connections and Services	1117
7.93 Create TCM in Control Plane and Managed Plane connections	1117
7.94 Create TCM in Mixed Plane connection	1120
7.95 Create TCM from end or intermediate ports from Routing Display	1125
7.96 Navigating to TCM 360° View	1128
7.97 TCM TPs from the NE	1130
7.98 View TCM and TCM ASAP Enabled connections	1132
7.99 Show TCM TPs	1134
7.100 Delete TCM trail	1136
7.101 TCM on-demand latency measurement	1138
Ethernet Service Manager	1142
7.102 Access the Ethernet Service Manager	1142
Looped back connections	1143
7.103 Initiate Facility Loopback Testing on an NE	1143
7.104 Initiate Terminal Loopback testing on an NE	1146

7.105 Release the loopback on a connection	1149
7.106 Synchronize loopback status on an NE	1152
7.107 View Looped Back Connections	1153
7.108 View tabbed topics for a Looped Back Connection	1155
Network Inconsistencies	1157
7.109 Inconsistent connections description	1157
7.110 ASAP Mismatches	1159
7.111 Download Disable Mismatches	1160
7.112 Parameter Mismatches	1161
7.113 Show Parameter Mismatches	1162
7.114 SNC Mismatches	1164
7.115 Uncorrelated Cross Connections	1166
7.116 Manage ASAP Mismatches	1167
7.117 Manage Download Disabled Mismatches	1171
7.118 Manage Parameter Mismatches	1173
7.119 Parameter Mismatches list further actions	1178
7.120 Manage SNC Mismatches	1179
7.121 SNC Mismatches list further actions	1185
7.122 Manage Uncorrelated Cross Connections	1186
7.123 Uncorrelated Cross Connections list further actions	1189
Wavelength Usage Report	1190
7.124 Wavelength Usage Report description	1190
7.125 Manage Wavelength Usage Report	1193
Jobs	1194
7.126 Jobs description	1194
7.127 Jobs table columns	1197
Schedule Path Synchronization	1198
7.128 Schedule Path Synchronization description	1198
7.129 Delete the last Scheduled Path Synchronization request	1199
7.130 Schedule or Reschedule Path Synchronization	1201
7.131 View the Path Synchronization job	1205

7.132 Abort Path Synchronization	1207
Flex Framer 3 (FF3) pool handling	1208
7.133 Overview	1208
7.134 Flex Framer 3 (FF3) pool handling	1209

Design and deploy a new service/infrastructure connection with templates

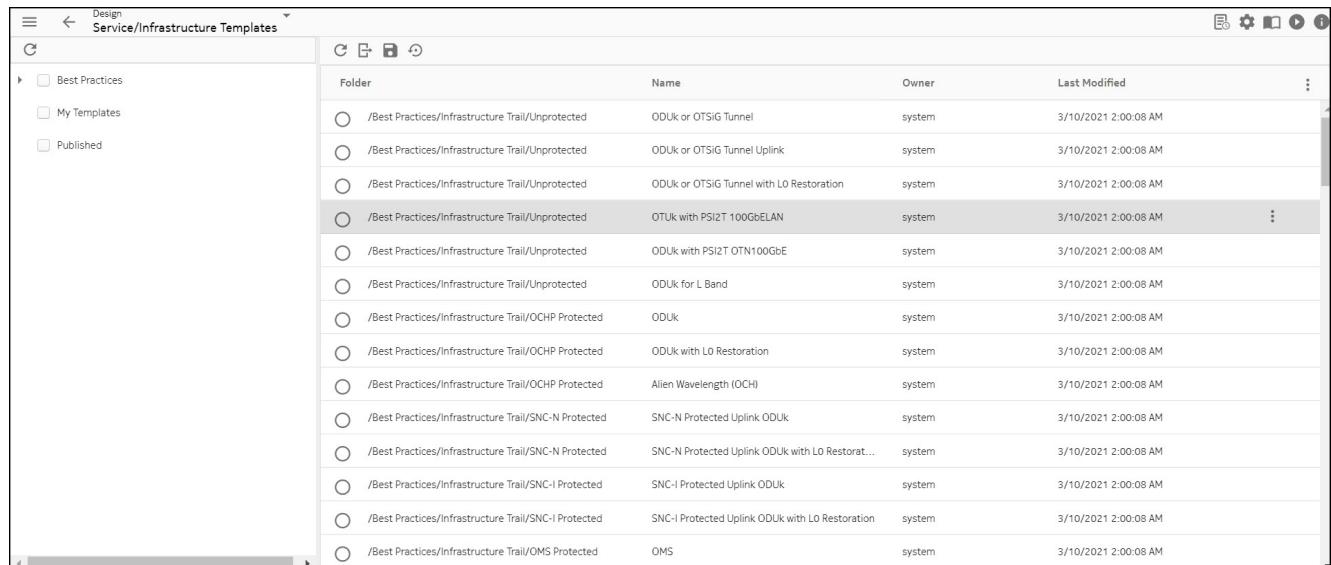
7.2 Connection template location and types

The template tree and the default configuration window

All connection templates reside in a Tree, which is in the left portion of the Design or Deploy window.

The following figure illustrates the default view for infrastructure connection and service templates when they are accessed from the **DESIGN >** navigation path.

Figure 7-1 Connection templates – configuration window – initial default view



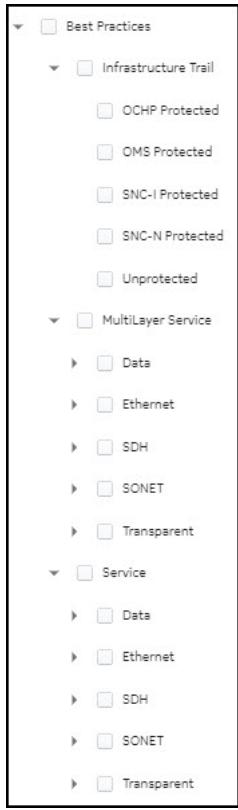
The Tree contains folders that can house three types of templates: “[Best Practices templates](#)” (p. 669), “[My templates](#)” (p. 671), and “[Published templates](#)” (p. 671).

Best Practices templates

In the NFM-T OTN application, a predefined, factory supplied set of **Best Practices** templates is provided to users for the provisioning of the logical connections that a given NFM-T OTN release supports. These logical connections include infrastructure connection templates for trails and logical links and service templates. Each Best Practices template is technology and connection type specific, and each template provides a proven combination of the parameters that are needed to create a working service.

Best Practices templates are **system** owned templates; therefore, they cannot be unpublished or modified; but, they can be saved to another name.

Figure 7-2 Connection templates – NFM-T OTN Best Practices template types



i Note: The unprotected Infrastructure trail ODUk template is extended to include OTSig tunnel. This Signal Rate is applicable for S4X400H (1830 PSS card) and DFC12/DFC12E (1830 PSI-M).

Figure 7-3 Best Practices templates with OTSigTunnel

Design Service/Infrastructure Templates				
	Folder	Name	Owner	Last Modified
Best Practices	/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel	system	3/10/2021 2:00:08 AM
Infrastructure Trail	/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel Uplink	system	3/10/2021 2:00:08 AM
	/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel with LO Restoration	system	3/10/2021 2:00:08 AM
	/Best Practices/Infrastructure Trail/Unprotected	OTUk with PSI2T 100GbELAN	system	3/10/2021 2:00:08 AM
	/Best Practices/Infrastructure Trail/Unprotected	ODUk with PSI2T OTN100GbE	system	3/10/2021 2:00:08 AM
Unprotected	/Best Practices/Infrastructure Trail/Unprotected	ODUk for L Band	system	3/10/2021 2:00:08 AM

To enable the OPSB/OPSB5 protection for UNI rates, use the predefined **OPSB Ethernet** template. The **OPSB Ethernet** template is available in the path: **Best Practices > Service > Ethernet > Protected > Full Rate > OPSB Ethernet**.

To extend the OPSB/OPSB5 protection for NNI rates, a predefined **OPSB ODUk** template is available in the path: **Best Practices > Service > Transparent > Protected > OPSB ODUk** in which the **Auto Server Creation** functionality must be unchecked.

Figure 7-4 Best Practices templates for NNI rates

Service/Infrastructure Templates			
C	Folder	Name	Owner
<input checked="" type="checkbox"/> Best Practices	/Best Practices/Service/Transparent/Unprotected	Alien Wavelength (unkeyed OCH)	system
<input type="checkbox"/> My Templates	/Best Practices/Service/Transparent/Protected	CBR 2.5G	system
<input type="checkbox"/> Published	/Best Practices/Service/Transparent/Protected	ODUK	system
	/Best Practices/Service/Transparent/Protected	OPSB ODUk	system
	/Best Practices/Service/Transparent/Protected	ODUK with OTN Restoration	system
	/Best Practices/Service/Transparent/Protected	OCHP Protected Alien Wavelength (OCH)	system
	/Best Practices/Service/Ethernet/Unprotected/Full Rate	Fast Ethernet	system
	/Best Practices/Service/Ethernet/Unprotected/Full Rate	Gigabit Ethernet	system

My templates

Considering many sites require special configurations, the NFM-T OTN application also provides users with the ability to create, save, and share their own templates in the **My Templates** folder from the **DESIGN >** navigation path. With this customization ability, users do not have to sacrifice the ease-of-use and speed that templates offer.

The templates that reside in the **My Templates** folder are **user** owned templates; therefore, if they are not published, they can be modified.

Published templates

If users modify and save a Best Practices template to create their own template in the **My Templates** folder, users can then publish their template so it is free for others to use. These templates reside in the **Published** folder.

The templates that reside in the **Published** folder are **user** owned templates and subsequently, users cannot modify or delete them unless they first unpublish them.

Design and deploy templates allowed user actions

The following tables summaries the user actions that the system allows in the **DESIGN** and **DEPLOY** phases for templates that reside in the **Best Practices**, **My Templates**, and **Published** folders.

DESIGN > and DEPLOY > Template Actions						
Phase > Folder	Allowed User Actions					
	Delete*	Deploy	Modify*	Publish* Unpublish*	Refresh	Save As
DESIGN > Best Practices					✓	✓
DESIGN > My Templates	✓	✓	✓	✓	✓	✓
DESIGN > Published	✓	✓	✓	✓	✓	✓

*Users cannot delete or modify a published template unless they first unpublish the template.

To view more details about the connection template

Follow the below steps to view more details about the connection template:

1

Click the **More**  icon at the right end of corresponding template, and then click **Details**.

Result: The following parameters corresponding to the template appears:

Figure 7-5 Connection template - details

	GENERAL	PROTECTION	CONNECTION	TRANSMISSION PARAMETERS	ASSURANCE	ASON
Folder	/Best Practices/Infrastructure Trail/Unpro...					
Template Name	ODUk or OTSIG Tunnel					
Owner	system					
Template Type	Connection					
Published	<input checked="" type="checkbox"/>					
Description						



Note: In this mode, you cannot edit the fields in the parameters.

END OF STEPS

To edit parameters in the connection template

1

Click the **More** icon at the right end of corresponding template, and then click **Save As**.

Result: The parameters corresponding to the template appears in tabs on top of the screen.

Figure 7-6 Connection template - Save As

	GENERAL	PROTECTION	CONNECTION	TRANSMISSION PARAMETERS	ASSURANCE	ASON
Folder	/My Templates					
Template Name	ODUk or OTSiG					
Owner	user					
Template Type	Connection					
Description						

2

Select the parameter to make changes.

Result: The fields corresponding to the selected parameter appears.

3

Click **OK** to confirm the changes.

Result: The changes appear in the parameters.

4

Click **RESET** to cancel the changes.

Result: The fields in the parameters are reset with the previous values.

END OF STEPS

7.3 Field descriptions for Best Practices templates

General

The **GENERAL** panel appears in each infrastructure connection and service template. It contains basic information for the particular infrastructure connection and service.

The following figure illustrates an example of the **GENERAL** panel.

Figure 7-7 Connection templates – general panel example – infrastructure connection

	GENERAL	PROTECTION	CONNECTION	TRANSMISSION PARAMETERS	ASSURANCE	ASON
Folder	/Best Practices/Infrastructure Trail/Unpro...					
Template Name	ODUk or OTSIG Tunnel					
Owner	system					
Template Type	Connection					
Published	<input checked="" type="checkbox"/>					
Description						

The fields, options, and values for the **GENERAL** panel are in alphabetical order as follows:

Folder

The **Folder** field displays the full path of the selected template.

Template Name

The **Template Name** field displays the name of the template. For Best Practices templates, the **Template Name** is the same name that is displayed on the Tree. For My Templates, the **Template Name** is a user supplied name for the customized template.

Owner

The **Owner** field displays who owns the selected template. For Best Practices templates, the **Owner** is **system**. For My Templates, the **Owner** is **user**.

Template Type

The **Template Type** field displays the word **Connection** as a default for Best Practices templates and My Templates.

Published

The **Published** field is a check box. If checked, which is the default, the template will be published. If not checked, the template will not be published. Published templates are those Best Practices templates and those My Template that are free for any users to use and that reside in the **Published** folder in the Tree. Published templates in the My Templates folder cannot be modified or deleted unless they are first unpublished.

Description

The **Description** field is an optional field that is provided for any wording that can further identify or clarify the particular connection. For Best Practices templates, the **Description** field is empty. For My Templates, the **Description** can be completed by the user.

Protection

The **PROTECTION** panel appears in each infrastructure connection and service template.

Figure 7-8 Connection templates – protection panel example – unprotected infrastructure connection

	GENERAL	PROTECTION
Protection Type	Unprotected	
Network Protection Mode	None	
Client Protection Mode	None	
Switch Type	NA	
Reversion Timer	N/A	
OCHP Revertive Mode	Disable	
Wait To Restore Time (min)	5	

The fields, options, and values for the **PROTECTION** panel are in alphabetical order:

Protection Type

The **Protection Type** field values varies depending on the type of protected connection being provisioned. For protected infrastructure connections and services, the **Protection Type** values are **Unidirectional** with these two exceptions: For bidirectional Ethernet full rate (Gigabit, 100G, 10G, 10G with LO-OTN restoration, Fast Ethernet, 40G) services, the **Protection Type** value is **Bidirectional**; and, for SDH SNC-NC protected STM-N with external 1+1 MSP protection, the **Protection Type** value is **NA**, which is *not available*. For unprotected infrastructure connections and services, the **Protection Type** is **N/A**, which is *not available* with this exception: For data unprotected HD-SDI data link services and data service services, the **Protection Type** is **Unidirectional**.

Network Protection Mode

The **Network Protection Mode** field value is **None** for unprotected infrastructures and services, and the following services: Service Ethernet protected Full rate, SDH Unprotected and the following Transparent protected services ODUk, PSA and ODUk with OTN restoration. The **Network Protection Mode** field value is the named type of protection for infrastructures and services.

Client Protection Mode

The **Client Protection Mode** field is **None** for all protected and unprotected infrastructure connections and services, with the following exceptions: the **Client Protection Mode** field is **SNC-NC** for SONET SNC-NC Protected OC-N with external 1+1 APS Protection and for SDH SNC-NC Protected STM-N with external 1+1 MSP Protection connections.

Switch Type

The **Switch Type** is a drop-down list. The available values are: **NA** which is default, **Unidirectional**, and **Bidirectional**.

Reversion Timer

The **Reversion Timer** field varies depending on the type of protected connection being provisioned. For all protected infrastructure connections and services, the **Reversion Timer** field value is **Default**. For unprotected infrastructure connections and services, the **Reversion Timer** is **N/A**, which is *not applicable* with these two exceptions: The **Reversion Timer** field values for unprotected data HD-SDI data link services and unprotected data services is **Default**.

OCHP Revertive Mode

The OCHP Revertive Mode fields allows to enable the OCHP revertive mode, that is the traffic is automatically switched back to the working circuit. Possible values are: enabled, disabled. The default value of OCHP Revertive Mode is **Disabled**.

Wait to Restore Time (min)

The Wait to Restore Time (min) is displayed if the value of OCHP Revertive Mode is **Enabled**. The default value of Wait to Restore Time is 5 minutes.

Soft Revertive SNCP Mode

The parameter supported values:

- *NoReversion*
- *NodeDefault*, this value is managed by GMRE at node level, the node values are propagated by GMRE at installation time. This is the default value at Connection creation.
- *MainNominal*, as soon as Main Nominal is available, traffic is switched to Main Nominal.
- *AnyNominal*, as soon as Main Nominal or Spare is available, traffic is switched to Main Nominal or Spare.

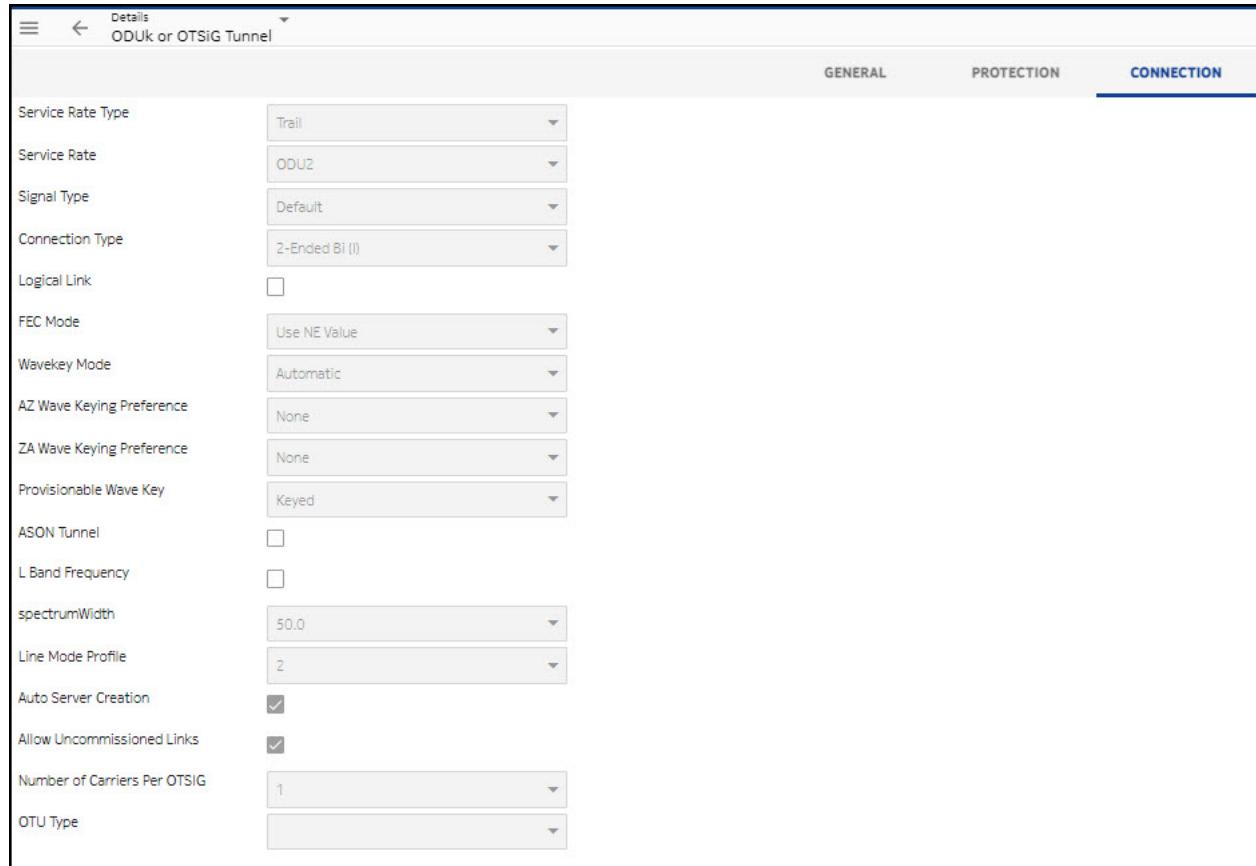
Soft Revertive SNCP Timeout

The parameter to insert the timer value, time in seconds (range 60-600), less than 60 seconds is not allowed.

Connection

The **CONNECTION** panel appears in each infrastructure connection and service template.

Figure 7-9 Connection templates – connection panel example



The fields, options, and values for the **CONNECTION** panel are in alphabetical order as follows:

Service Rate Type

The **Service Rate Type** field is **Trails** for infrastructure connections. The **Service Rate Type** field is **SONET** for SONET service templates, **Optical** or **CBR** for Transparent service templates, **Data** for Data service templates, **Ethernet** or **Subrate Ethernet** for Ethernet service templates, or **SDH** for services.

Service Rate

The **Service Rate** field is **ODU0** for Optical infrastructure connections. The **Service Rate** field depends on the Service Rate Type of the selected template, **SONET**, **Optical** or **CBR**, **Data**, **Ethernet** or **Subrate Ethernet** for Ethernet service templates, or **SDH**.

Signal Type

The **Signal Type** field is **Default** for an infrastructure connection, except OMS-P Protected is **OMS** and OPSA-Protected is **OCH**. The **Signal Type** field varies for **SONET**, **Transparent**, **Data**, **Ethernet**, or **SDH** services.

Connection Type

The **Connection Type** field is **2-Ended Bi (I)** for all infrastructure connections. The **Connection Type** field is **2-Ended Bi (I)** for all services with this exception: The **Connection Type** field is **4 Ended Bi (X)** for the SONET SNC-NC Protected OC-N with external 1+1 APS Protection and SDH SNC-NC Protected STM-N with external 1+1 MSP Protection services.

The connection shapes for NFM-T OTN infrastructure connections and services also include bidirectional (bi) shapes of **3 Ended A/Z Bi (I)**, **4 Ended Bi (X)**, and **2 Ended Bi (I)**, along with the unidirectional (uni) shape of **2 Ended Split Bi (I)**.

Note: The letters in parenthesis represent the shape of the connection.

The following figures illustrate the valid connection shapes for NFM-T OTN infrastructure connections and services:

Figure 7-10 Connection Templates – 2 Ended Bi (I) Connection Shape



Figure 7-11 Connection Templates – 3 Ended A Bi (Y) Connection Shape



Figure 7-12 Connection Templates – 3 Ended Z Bi (Y) Connection Shape



Figure 7-13 Connection Templates – 4 Ended Bi (X) Connection Shape

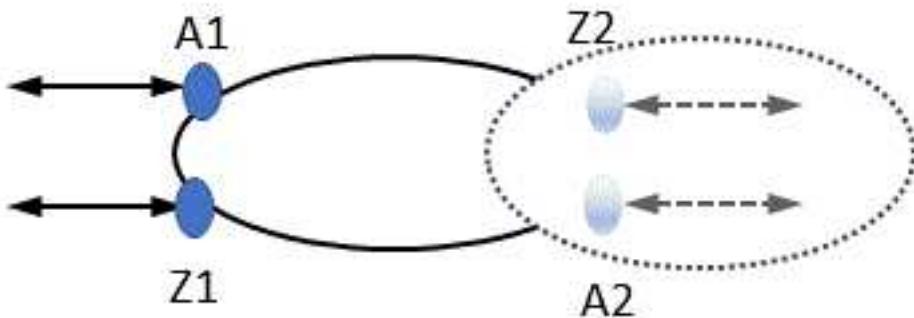


Figure 7-14 Connection Templates – 2 Ended Split (Bi) Connection Shape



The 4 Ended Open Add/Drop Connection is a configuration that occurs when there is a ring and only part of the ring is in the managed domain. At the A1 and Z1 points the traffic is Add/Drop. At the A2 and Z2 points the traffic leaves the managed network.

Figure 7-15 Connection Templates – 4 Ended Open Add/Drop Connection Shape



Logical Link

The **Logical Link** field is displayed for all infrastructure connections. If the infrastructure connection is a logical link, the check box must be checked. Refer to the [2.8 “Determine the Infrastructure to be created” \(p. 168\)](#) task for a detailed explanation and steps.

FEC Mode

The **FEC Mode** field is Forward Error Correction. The **FEC Mode** field is **Use NE Value** as default for infrastructure connections. The **FEC Mode** field can be selected from a list of possible values.

Wavekey Mode

The **Wavekey Mode** field is **Auto** for all infrastructure connections.

The **Wave Key Config** field is **N/A** for all services with the following exception:

- For Transparent services, the **Wavekey Config** field is **Automatic** for all services except for the Transparent Unprotected and the Transparent Protected Services, which are **N/A**.
- For Transparent Unprotected, Alien Wavelength (unkeyed OCH) services, the **Wavekey Mode** field is **Manual**.

AZ Wave Keying Preference and ZA Wave Keying Preference

The **AZ Wave Keying Preference** (From/To preference) and the **ZA Wave Keying Preference** (To/From preference) fields are drop-down lists. Values are **None** (the default), **Duplicates Allowed**, or **No Duplicates Allowed**.

Provisionable Wave Key

The **Provisionable Wave Key** field is displayed for all infrastructure connections as **Keyed**.

For Transparent Unprotected Alien Wavelength (OCH) services, the **Provisionable Wave Key** field is displayed as **Keyed**. For Transparent Unprotected Alien Wavelength (unkeyed OCH) services, the **Provisionable Wave Key** field is displayed as **UnKeyed**.

Alien Wavelength Bank connection is always unkeyed as there is no MVAC support.

For Transparent OCHP Protected Alien Wavelength (OCH) services, the **Provisionable Wave Key** field is displayed as **Keyed**.

The 1830 PSS supports both keyed and unkeyed optical channels. For services or connections with keyed optical channels, Wavelength Tracker functionality is enabled.

A lightpath service is a new alien wavelength service that does not require an MVAC pack. A NE can be used for lightpath service configuration, if the NE is licensed with the feature. Contact the Nokia support team for more information.

ASON Tunnel

The **ASON Tunnel** field is a check box. It must display a check mark if the connection is to be an ASON tunnel. If the box is unchecked, the connection becomes a Control/Mixed Plane.

L Band Frequency

This parameter check box when enabled, is used for creating a connection with L band frequency range.

Spectrum Width

This is defined as the range of wavelengths that the source emits around the main central wavelength for which it was designed.

Line Mode Profile

It indicates the profile number applicable for the OTSig tunnel.

Auto Server Creation

The **Auto Server Creation** field determines if the user or the NFM-T system creates the server layer for the infrastructure connection or service.

Allow Uncommissioned Links

The **Allow Uncommissioned Links** field is a checkbox. Users should check this box if they want the system to create the connection regardless of the commission status of the optical amplifiers. If users check this box, they must make any manual power adjustments from Wavelength Tracker for both egress and ingress ports on the uncommissioned link. If users do not check this box, the connection fails if any optical amplifier in the connection is not commissioned.

Number of Carriers per OTSIG

This parameter is available only for DFM6/DFM6E cards to select single or dual carrier. Select 1 for single carrier or 2 for dual carrier from the drop-down as required.

OTU Type

Specifies the rate supported for the selected profile number. For example,

Select OTU4 for 100 GbE connections.

Select OTUC4 for 400 GbE connections.

Transmission parameters

The **TRANSMISSION PARAMETERS** panel appears in each infrastructure connection and service template.

Note: If you are provisioning a *control plane connection*, Transmission parameters cannot be set.

Figure 7-16 Connection templates – transmission panel example – infrastructure connection/services defaults

	GENERAL	PROTECTION	CONNECTION	TRANSMISSION PARAMETERS
Container Rate				
LOS Propagation	Use NE Value			
Transmission Actual Bit Rate	Default			
Polarization Tracking	Use NE Value			
Link Span	Amplified			

The fields, options, and values for the **TRANSMISSION PARAMETERS** panel are in alphabetical order:

Container Rate

The **Container Rate** field values vary depending on the type of connection being provisioned. For all infrastructure connections and services, the **Container Rate** field value is **Default** with the exceptions listed in the following table:

Table 7-1 Transmission Parameters - Container Value Exceptions

Container Value other than Default	Template/Connection
ODU0	All Protected and Unprotected, Full Rate, Fast Ethernet and Gigabit Ethernet, Service Paths
ODU1	Transparent, Protected and Unprotected, CBR 2.5G Service Paths Data, Protected and Unprotected, HD-SDI Data Link Service Paths
ODU2	All Ethernet, Protected and Unprotected, Not Full Rate, Service Paths
ODU2e	Ethernet, Protected and Unprotected, 10G and 10G w/LO-OTN, Full Rate Service Paths
ODU3e2	Ethernet, Protected and Unprotected, 40G, Full Rate Service Paths
ODU4	Ethernet, Protected and Unprotected, 100G, Full Rate Service Paths
OMS	Unprotected ODUk for TDM Infrastructure Connection OPSA Protected Alien Wavelength, OCH, infrastructure connection Transparent, Unprotected, Alien Wavelength, OCH, Service Path Transparent, Protected OPSA Alien Wavelength, OCH, Service Path
OTS	OMS-P Protected OMS infrastructure connection

LOS Propagation

The **LOS Propagation** field value is **Use Node Value** for all infrastructures. The **LOS Propagation** field value is **Both A and Z End** for all services.

Transmission Actual Bit Rate

The **Transmission Actual Bit Rate** field value is **Default** for all infrastructure connections and services.

Polarization Tracking

Polarization tracking allows the user to provision the speed at which the coherent line receiver tracks state of polarization changes. The field values are: **Use NE value**, **Normal**, and **Fast**.

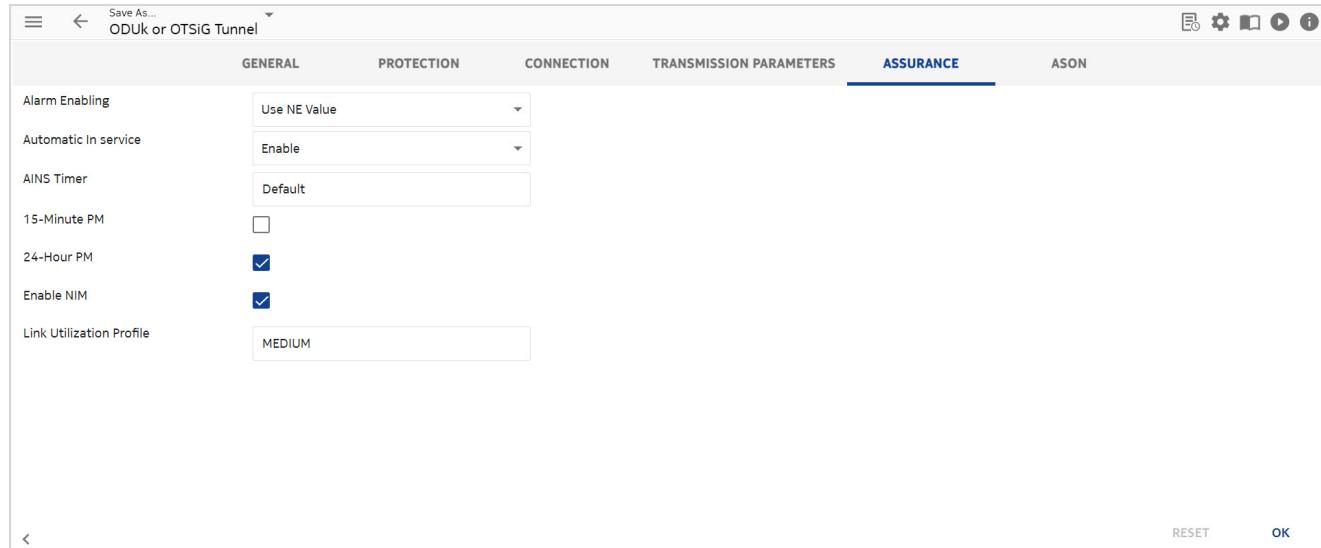
Link Span

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. The field values are: **Use NE value**, **Amplified**, and **Unamplified**.

Assurance

The **ASSURANCE** panel appears in each infrastructure connection and service template.

Figure 7-17 Connection Templates – Assurance Panel Example – Services



The fields, options, and values for the **Assurance** panel are in alphabetical order:

Alarm Enabling

The **Alarm Enabling** field is a drop-down list. It defaults to **Use_NE_Values**.

Automatic in Service

The **Automatic in Service** field is a drop-down list. It defaults to **Enable**, which is Automatically In Service. This field is applicable for Infrastructure Connection only. For Services, this parameter is available in Transmission Parameters.

AINS Timer

The **AINS Timer** field is set to **Default**.

15-Minute PM

The **15-Minute PM** field is a check box. If checked **15-Minute PM** is enabled. If unchecked, which is the default, **15-Minute PM** is disabled.

24-Hour PM

The **24-Hour PM** field is a check box. If checked, which is the default, **24-Hour PM** is enabled. If unchecked, **24-Hour PM** is disabled.

Enable NIM

The **Enable NIM** field is a check box. The **Enable NIM** field allows the operator to enable NIM when setting up a connection. The check box is made available and selected if either or both the 15-Minute and 24-Hour PM is enabled. The Enable NIM check box can be unselected if NIM should not be enabled for the connection. By default, it is checked.

The **Enable NIM** check box is also available in the Templates.

i **Note:** There are certain protection schemes that require NIM to be enabled for proper switching.

When creating a connection, NIM is enabled on all ports.

- If any one of the port involved in a connection has NIM = Disabled, the Connection will have the NIM status as Disabled.
- Only if all the ports involved in the connection has NIM = Enabled, the Connection will have the NIM status as Enabled.
- If none of the ports support NIM (irrespective of NIM being enabled or disabled), then after connection creation is successful, the Connection will have the NIM status as N/A .

NIM is applicable for OCS modeled cards. NIM is applicable for ODUK Infra/Services and not for OTUk Infra/Services. **Enable NIM** is applicable for CTPs and not FTPs.

During ODUk, 10GBE infrastructure/service connection provisioning, if the **Auto Server Creation** check box is not checked in the template, then the **Enable NIM** check box is not visible to the user. For NNI Services, checking the **Auto Server Creation** check box is not applicable. Even if the **Auto Server Creation** check box is unchecked, **Enable NIM** is enabled by default.

On the NE, both POM and EGPOM are enabled if the ports are endpoints. POM is enabled only for NNI. During a logical link creation, **Enable NIM** is not applicable. However, after the logical link is created, you can enable or disable the NIM. For a detailed information on NIM, refer [7.57 “Manage NIM for a connection” \(p. 954\)](#).

Link Utilization Profile

The **Link Utilization Profile** field sets the threshold profile for the link or infrastructure connection. This field defaults to **Medium** and is not applicable for services.

See [22.1 “Link Utilization Profile” \(p. 1959\)](#), to know in detail of all the applicable profiles.

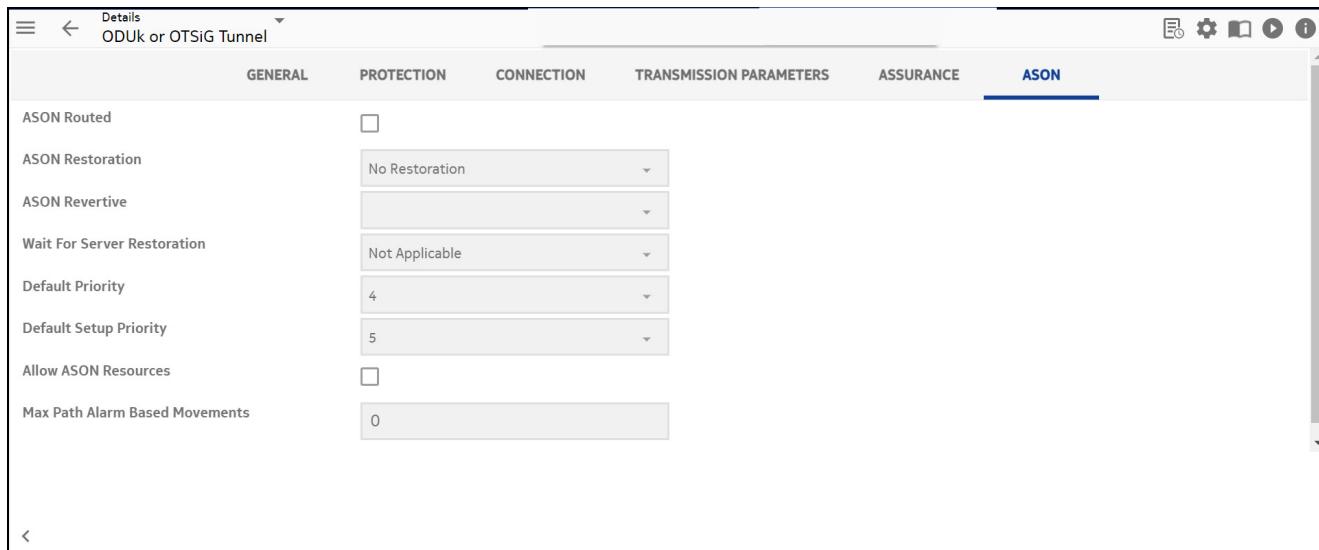
See [7.38 “Modify Utilization Profile for a physical/infrastructure connection” \(p. 881\)](#), to modify the threshold profile after creating the link or connection.

ASON

The **ASON** panel appears in each infrastructure connection and service template. It contains the ASON fields for each template.

Important! All ASON fields for the Best Practices infrastructure connections and services templates are turned off by default.

Figure 7-18 Connection templates – ASON panel example – infrastructure connection



The fields, options, and values for the **ASON** panel are in alphabetical order:

ASON Routed

The **ASON Routed** field is a check box. It must display a check mark if the connection is to be a Control/Mixed plane connection or an ASON tunnel. If the box is unchecked, the connection becomes a Managed Plane or Logical Drop Link. This field is not applicable for OTUk connection rates. For ASON routing constraints, refer to “[Nodes as a constraint for routing traffic](#)” (p. 732) and “[Physical connections as a constraint for routing](#)” (p. 733).

ASON Restoration

The **ASON Restoration** field defaults to **No Restoration** for all non-restoration named templates. The **ASON Restoration** field defaults to **Source-based Restoration** for all restoration-named templates.

ASON Revertive

The **ASON Revertive** field defaults to **N/A**, which is not applicable, for all non-restoration named templates. The **ASON Revertive** field defaults to **Non-revertive** for all restoration-named templates.

Wait for Server Restoration

The **Wait for Server Restoration** field defaults to **N/A**, which is not applicable, for all non-restoration named templates. The **Wait for Server Restoration** field defaults to **No** for all restoration-named templates.

Default Priority

The **Default Priority** field is a text field that has default value 4. Users can specify another value when creating the connection.

Default Setup Priority

The **Default Setup Priority** field is a text field that has default value 5. Users can specify another value when creating the connection.

Allow ASON Resources

The **Allow ASON Resources** field defaults to not checked. The **Allow ASON Resources** parameter is used for the connection creation of HO ODUK trail and ODUk service integrated provisioning of Managed Plane connections. The user must check this check box to create managed plane using ASON resources.

Max Path Alarm Based Movements

The **Max Path Alarm Based Movements** field is a text field that has default value 0. Path Alarm attributes are enabled only when head node version >= 14.0.8 and the user must check the ASON check box with valid configurations for L0 and MRN only.

7.4 Service definition field descriptions for deploy Best Practices templates

Overview

Once a Best Practices Template is deployed, users must specify the From/To NEs and ports along with other parameters that are optional and that depend on the selected template.

Service definition

The following fields are displayed in the Service Definition panel for deployed infrastructure connection and service templates.

Template

The **Template** field value displays the full path of the deployed template. Compare the **Template** field to the **Folder** field.

Rate

Optional: For an infrastructure connection, the **Rate** field is a drop-down list that displays all available rates for the particular deployed template. Users can select a **Rate**.

Service Rate

Optional: For a service, the **Service Rate** field is a drop-down list that displays all available service rates for the particular deployed template. Users can select a **Service Rate**.

Container

The **Container** field is a drop-down list that is displayed for certain service templates that have a connection rate of DSR. Refer to [Table 7-2, “Service definition – containers – service rates and container options” \(p. 688\)](#) for details. Depending on the template selected and the service being created, users must select the appropriate container for the connection being created.

When DSR connections are automatically discovered (either through application notification, Auto Discovery, or database synchronization), the system automatically sets the **Container** parameter when only a single container value is possible or only multiple container values are possible. In addition, when DSR connections are automatically discovered, the system sets the **Container** parameter based on the value of container.

Table 7-2 Service definition – containers – service rates and container options

Service template	Service Rate	Container options
All SONET Templates	OC-768	ODU3
	OC-192	ODU2
	OC-48	ODU1 OPTSG ¹
	OC-12	ODU0, OPTSG ¹
	OC-3	ODU0, OPTSG ¹

Table 7-2 Service definition – containers – service rates and container options (continued)

Service template	Service Rate	Container options
Transparent Protected CBR 2.5G Template Transparent Unprotected CBR 2.5G Templates	CBR2G5	N/A, ODU0, ODU1, ODU2, ODU3, ODU4, ODU2E, ODU3E2, OPTSG ¹ , ODUflex, Use Node Value
	CBR10G3²	ODU2E
Ethernet Unprotected Full Rate Templates Ethernet Protected Full Rate Templates	Fast Ethernet	ODU0, OPTSG ¹
	1GbE Gigabit Ethernet	ODU0, OPTSG ¹
	1GbEConv	ODU0, OPTSG ¹
	10GbE⁴ (10G Ethernet)	ODU2E ⁵ , ODU2 ⁵
	10GbE⁴ (10G Ethernet with LO OTN Restoration)	ODU2E ⁵ , ODU2 ⁵
	40GbE	ODU3
	40GbE MLD	ODUflex
	100GbE	ODU4
	400GbE	ODUflex
	Flexible Rate Client	ODUflex
Data Templates	FC100 (Default for Data Service Templates)	ODU0
	FC200	ODU1
	FC400	ODUflex, ODU1
	FC800³	ODU2, ODUflex
	FC1200³	ODUflex, ODU2, ODU3, ODU4, ODU2E
	FC1600³	ODUflex, ODU2, ODU3, ODU4
	HDSDI (Default for HD-SDI Data Link Templates)	ODU1
	SDSDI	ODU0
	DVBASI	N/A, ODU0, ODU1, ODU2, ODU3, ODU4, ODU2E, ODU3E2, OPTSG ¹ , ODUflex, Use Node Value
	DDR³	ODUflex
	3GSDI	ODUflex

Table 7-2 Service definition – containers – service rates and container options (continued)

Service template	Service Rate	Container options
All SDH Templates	STM-256	ODU3
	STM-64	ODU2
	STM-64MS	ODU2
	STM-16	ODU1, OPTSG¹
	STM-16M	ODU1
	STM-4	ODU0, OPTSG¹
	STM-1	ODU0, OPTSG¹

Notes:

¹For OPTSG, only 1830 PSS and 1830 PSS-4 NEs are displayed for NE selection and only ports on the 11DPM12 and 4QPA8 circuit packs are displayed for selection.

²For CBR10G3 with ODU2E, one or more connection endpoints are ports on an 112SDX11 circuit pack.

³For FC800, FC1200, FC1600, DDR or 40GbE MLD with ODUflex, one or more connection endpoints are ports on an 112SDX11 circuit pack.

⁴For 10GbE with an ODU2E container, the Encapsulation Mode parameter is set to CBRLAN11.096 on the Transmission Parameters panel, regardless of if the user opens the Transmission Parameters panel.

⁵For 10GbE with an ODU2 container, the Encapsulation Mode parameter is based on the end point of the connection. In this case the Encapsulation Mode parameter are circuit pack dependent. The possible values are as follow:

Circuit pack	Encapsulation Mode value
S13X100E,S13X100R	GFP-F
20P200	GFP-F
12P120	CBRFC1200, GFP-F and Use NE Values
11QPA4,11QPEN4	CBRLAN11.049, GFP-F and Use NE Values
30AN300, 20MX80, 20AX200 and 20UC200	GFP-F, GFP-PPOS, GPF-PPOS-OLD and Use NE Values
43STX4, 43STX4P	GFP-F, GFP-P and Use NE Values
All other packs	CBRLAN11.049, GFP-F, GFP-P and Use NE Values

i Note:

- If you have a 10GbE connection, you can choose as a container either **ODU2** or **ODU2e**. This determines the encapsulation mode. Even though you choose an **ODU2e** as a

container, in the **Servers Tab** list, the server connection visualized for the 10GbE service connection, is an **ODU2** even if have effective rate of **ODU2e**.

- As there are scenarios where endpoints need to support different types of encapsulation modes, by default the option **Use NE Value** is pre-populated. User needs to change the value of the encapsulation mode based on the supported configuration.

In the *Data Service* template for some **Service Rate**, the **Container** type is dependent on the type of circuit pack at the end points. Refer to the table [Table 7-3, “Service definition – containers – circuit pack options” \(p. 690\)](#) for details.

This applies to circuit packs hosted in the 1830 PSS NE with release 12.0 onwards.

Table 7-3 Service definition – containers – circuit pack options

Service Rate	Container	Circuit pack
FC100	ODU0	11DPM8
FC200	ODU1	11DPM8
FC400	ODUflex	11DPM8
FC800	ODUflex	12P120
FC1200	ODU2e	S13X100R, S13X100E
FC1600	ODUflex	S13X100R, S13X100E

Note: If the selected container is not allowed for the considered circuit pack, the connection commissioning will not be implemented.

Protection Type

Optional: The **Protection Type** field is a drop-down list that displays **Unprotected** or **Protected**. Users can select a **Protection Type**.

OMS Protection

Optional: For OMS-P protected OMS infrastructure connections (trails) only, choose **Protected** for the protection type field. The **OMS Protection** field is displayed. From the drop-down list that displays **OPSPortA** (the default) or **OPSPortB**, select which port should be the working port of the OMS-protection group.

Connection Type

Optional: The **Connection Type** field is a drop-down list that displays all available connection type/shape for the deployed template. Users can select a **Connection Type**.

Logical Link

The **Logical Link** field is a check box that is displayed for all infrastructure connections. A logical link is an unterminated entity that provides contiguous, fixed connectivity to the far end, which can be terminated or unterminated. If the infrastructure connection is a logical link, the check box must be checked. The **Logical Link** field defaults to unchecked, with these exceptions: The **Logical Link** box is checked by default for all SNC-I, SNC-N Protected infrastructure connections and for

Unprotected OCS Uplink ODUk infrastructure connections; and, the OPSA Alien Wavelength and the OMS-P Protected OMS templates do not have a **Logical Link** field.

The **Enable NIM** is not applicable for a logical link during creation. You can enable or disable the NIM after logical link is created.

Refer to the [2.8 “Determine the Infrastructure to be created” \(p. 168\)](#) task for a detailed explanation and steps.

Show All Ports

Optional: For infrastructure connections and services, the **Show All Ports** field is a check box. Users can check this field if they want all available ports and ports that are already in use to be displayed in the ports list when they select the **From Port** and **To Port**. Users can uncheck this field if they want to view only all available ports in the ports list when they select the **From Port** and **To Port**.

There are certain tandem ports that are reserved while creating the connection with any container types. To list the tandem port, select the **Show All Ports** option.

Regarding the selection of unterminated ports for DSR connections, when users select an HO ODU CTP, the LO ODU CTPs of the HO ODU CTP that have the same rate as the container rate of the connection are displayed. If **Show All Ports** is checked, all LO ODU CTPs for the HO ODU are displayed. If **Show All Ports** is not checked, only the available LO ODU CTPs for the HO ODU are displayed.

Example: For a DSR connection with an ODU3 container, if **Show All Ports** is checked, 80 ODU3 LO CTPs are displayed for an HO ODU4. If **Show All Ports** is not checked, and 10 ODU3 CTPs are used by other connections, the 70 available ODU3 LO CTPs are displayed.

If **Show All Ports** is not checked, when an HO ODU port is already channelized and if enough available timeslots do not remain on the port, the port does not appear on the From/To Port selection list.

Example:

The connection endpoint is an ODU4 port that has 80 timeslots. Of the 80 timeslots, 73 timeslot are already used by other connections; therefore, only 7 timeslots are currently available. If the user wants to create an ODU2 connection, the ODU4 port is not displayed on the From/To Port selection list. If the user wants to create an ODU1 or ODU0 connection, the ODU4 port is displayed on the From/To Port selection list.

From Node

The **From Node** is an icon-activated field; or, if you start to type in the node name, the system displays a drop-down list from which you can select the node. The **From Node** is the node in which the connection is to originate. For 2-ended connections, users must click the icon adjacent to the **From Node** field to display the node selection window and they must select the first and only **From Node**. For 3-ended Y connections and for 4-ended X connections, users must click the icon adjacent to the **From Node** field to display the node selection window and they must select the second **From Node**. The node name that the user selects in this field is the same node name that appears in the data table for the particular connection.

From Port Type

For DSR service connections only, the **From Port Type** field is used to determine if a UNI or NNI port is created when an MDL port is selected as the connection endpoint in regards to the **From Node**. In addition, the selection of a **From Port Type** is used to filter the ports that appear for Port Selection. The **From Port Type** field is a drop-down list. For all container values except **ODUflex** and **OPTSG**, users can select **Terminated** (the default) or **Unterminated**. If the container is **ODUflex** or **OPTSG**, the value is **Terminated**.

Important Provisioning Considerations:

- For 3-ended Y connections and for 4-ended X connections, multiple **From Port Type** fields are displayed, depending on the display of the **From Port** field.
- When DSR connections are automatically discovered (either through application notification or Auto Discovery), the **From/To Port Type** parameter is set for all connection endpoints.
- If the **From Port Type** is **Terminated** in the Port Selection list, the rate for unassigned ports is equal to the **Service Rate** of the connection except for ports on 103SCEC packs.
- Ports on 103SCEC packs are displayed for connections with service rate of 100GbE, 40GbE, and 10GbE.
- For DSR service connections with an **Unterminated** port type and for ODUk/LO-ODUj service connections, the rate for unassigned ports in the Port Selection list is equal to the rate of the NNI port that is supported for the card. With the exception of cards that support both ODU2 and ODU2e, no cards support more than one NNI rate.

Example:

For MDL ports on 1XANY100G cards, the rate is ODU4; and for MDL ports on 2XANY40G cards, the rate is ODU3. For cards that support both ODU2 and ODU2e (such as the 10XANY10G), if the container of the connection is ODU2e, the rate will be ODU2e; otherwise, the rate will be ODU2.

- If the port type is **Unterminated** and the user changes to the container to **ODUflex** or **OPTSG**, and the system changes the **From Port Type** to **Terminated**.
- If the user has selected a port and changes the port type, the system deselects the port; meaning, the port value is changed to blank.

Examples:

If the service rate is 10GbE, the container is ODU2, the MDL port is on a 10XANY10G card, and the port type is **Terminated**, a 10GbE port is created; and, if the port type is **Unterminated** an OTU2 port is created.

If the service rate is 10GbE, the container is ODU2, the MDL port is on a 1XANY100G card, and the port type is **Unterminated**, a 10GbE port is created; and, if the port type is **Unterminated**, an OTU4 port is created.

From Port

The **From Port** field is an icon-activated field; or, if you start to type in the port name, the system displays a drop-down list from which you can select the port. The **From Port** is the port in which the connection is to originate on the **From Node**. For 2-ended connections, users must click the icon adjacent to the **From Port** field to display the From Port selection window and they must select the

appropriate **From Port** for the first and only **From Node**. For 3-ended Y connections and for 4-ended X connections, users must click the icon adjacent to the **From Port** field to display the From Port selection window and they must select the appropriate **From Port** for the second **From Node**. The port name that the user selects in this field is the same port name that appears in the data table for the particular connection.

For Y-Cable protection, users are to select a known Y-cable port. By selecting a known Y-cable port, the **Y-Cable Port** panel is activated. Refer to “[Y-Cable Port](#)” (p. 721) for details.

For service connections with the connection rate of ODU0, ODU1, ODU2, ODU2e, and ODU3, users can check the **Show Channelized Ports** check box on the From/To Port selection list.

If **Show Channelized Ports** is checked, the following apply:

- Users can select channelized ports in addition to the unterminated, unchannelized ports.
- The From/To Port selection list includes HO ODU CTPs that are a higher rate than the connection rate and that can be channelized. However, the HO ODU CTPs cannot be selected as connection endpoints.

Examples:

- For an ODU2 connection, HO ODU CTPs with the rate of ODU4, ODU3e2 and ODU3, which can be channelized, are displayed.
- For an ODU3 connection, HO ODU CTPs with the rate of ODU4 and ODU3e2, which can be channelized, are displayed.
- When the user selects an HO ODU CTP, the system displays the LO ODU CTPs of the HO ODU CTP, which have the same rate as the connection rate.

If the **Show Channelized Ports** is unchecked or if the **Show Channelized Ports** field does not appear on the From/To Port selection list, the list includes only unterminated, unchannelized ports. For ODUk/LO-ODUj service connections, the unterminated, unchannelized ports that are displayed in the From/To Port selection list are ports that have the same rate as the service rate of the connection.

From Port Timeslot

When a channelized port is selected in the **From Port** field, users must select an available **From Port Timeslot** from the multi-selection list or enter the port ID.

When creating a DSR connection, a port that is selected on the Port Selection list is a *channelized* when the port rate is ODUn and the port rate is greater than the container rate of the connection. When creating an LO-ODUj service connection, a port that is selected on the Port Selection list is a *channelized* when the port rate is greater than the connection rate.

Example: For a 10GbE connection with an ODU2 container, if the port selected is an ODU3 or ODU4 port, the port is *channelized*; but, if the port selected is an ODU2 port, the port is *not channelized*.

Important Provisioning Considerations:

- For 3-ended Y connections and for 4-ended X connections, multiple **From Port Timeslot** fields are displayed, depending on the display of the **From Port** field.
- Users can select any set of available timeslots. Timeslots do not have to be selected consecutively. The default value for all timeslot fields is blank, except when timeslots are selected

for the **From Port Timeslots** field, the following applies: If the **From Port <x>** or the **To Port <x>** uses the same channel number as the **From Port** and the same timeslots are available for the **To Port Timeslots**, the system automatically selects the timeslots. Users can change the automatically selected **To/From Port <x> Timeslots**.

- When DSR and ODUk service connections are automatically discovered (either through application notification or Auto Discovery) the **From/To Port Timeslot** parameter is automatically set for channelized connection endpoints.
- When you select Link Connection based routing, if a connection endpoint is a channelized port on a black box, and the link connection of the OS connection between the black box and the managed NE that is selected as a routing constraint do not correspond to the timeslots selected for the connection endpoint, the link connection selection overrides the timeslot selection. The system automatically updates the timeslot field for the connection endpoint to reflect the link connection selection.
- Depending on the rate of the DSR and LO-ODUj service connections, a prescribed number of timeslots are required. Refer to [Table 7-4, “Service Definition – DSR and LO-ODUj Rates and the Required Number of Timeslots” \(p. 695\)](#) for details. If the user enters too few or too many timeslots, the system outputs a message similar to the following:

[Container rate] requires [number of timeslot required] and [number of timeslots selected by user] are selected.

In addition, the system validates if the timeslot is equal to the channel number of the selected port. If the validation fails, the system outputs a message similar to the following:

Timeslot [number] must be selected.

Table 7-4 Service Definition – DSR and LO-ODUj Rates and the Required Number of Timeslots

DSR Rate	LO-ODUj Rate	Required Timeslots
ODU0	Not Applicable	1
ODU1	ODU1	2
ODU2	ODU2	8
ODU2E and the port is an ODU3ODU2E	ODU2E and the port is an ODU3ODU2E	9
ODU2E and the port is an ODU3E2ODU2E	ODU2E and the port is an ODU3E2ODU2E	8
ODU2E and the port is an ODU4ODU2E	ODU2E and the port is an ODU4ODU2E	8
ODU3 and the port is an ODU3E2ODU3	ODU3 and the port is an ODU3E2ODU3	32
ODU3 and the port is an ODU4ODU3	ODU3 and the port is an ODU4ODU3	31

Table 7-4 Service Definition – DSR and LO-ODUj Rates and the Required Number of Timeslots (continued)

DSR Rate	LO-ODUj Rate	Required Timeslots
ODUC4 and the port is an OTUODU4	ODUC4 and the port is an OTUODU4	80

From Port Pluggable Module

If the user selects an unassigned port on a 1830 PSS OCS NE that is not a fixed port as the **From Port** and the pluggable module is not equipped and not known at the time of port creation, the **From Port Pluggable Module** field is displayed as a drop-down list; all possible pluggable modules are displayed. If the user selects an unassigned port on a 1830 PSS OCS NE that is not a fixed port as the **From Port** and the pluggable module is equipped and known at the time of port creation, the **From Port Pluggable Module** field is automatically populated with the pluggable module type.

The valid pluggable modules for the port are based on the card type of the port and the service rate of the port. For 2-ended connections, users must select one **From Port Pluggable Module**. For 3-ended Y connections and for 4-ended X connections, users must select a pluggable module for each unassigned port.

Important provisioning considerations!

- For easy recognition, unassigned ports have the format: *MDL-bay-shelf-slot-port*.
- Third party pluggable modules are supported and are identified on the drop-down list as **USER**.
- For DSR connections, if the **Port Type** is **Terminated**, the **From/To Pluggable Module** drop-down list for a port contains the valid pluggable modules for the port that are based on the card type of the port and the service rate of the connection. For DSR connections, if the **Port Type** is **Unterminated**, the **From/To Pluggable Module** drop-down list for a port contains the valid pluggable modules for the NNI ports of the card.
- For ODUK infrastructure connections, users must select a valid **Signal Type** in the **Transmisison Parameters** panel when they use unassigned ports as connection endpoints. Users must select a pluggable module for every port for which the **From Port Pluggable Module** is displayed. If a pluggable module is not selected for a port, the system outputs a message that is similar to the following:

Pluggable Module is mandatory for <PortName>.

If user selects **Other** in the**From Port Pluggable Modules Type** drop-down list, a new text field appears.

Enter the value of the pluggable module for provisioning. For example, User.

For valid **User Pluggable** values, see *Equipment Management* section of the NFM-T NE Management Guide.

For example, the following figure illustrates that users can select **LR42W103GEUC**, **LR42W112GAUC**, **SR101W103GEUC**, **C24L2W28G40C**, **ER42W112GAUC**, **USER**, or **Other**.

To Node

The **To Node** is an icon-activated field; or, if you start to type in the node name, the system displays a drop-down list from which you can select the node. The **To Node** is the node in which the connection is to terminate. For 2-ended connections, users must click the icon adjacent to the **To Node** field to display the node selection window and they must select the first and only **To Node**. For 4-ended X connections, users must click the icon adjacent to the **To Node** field to display the node selection window and they must select the second **From Node**. The node name that the user selects in this field is the same node name that appears in the data table for the particular connection.

To Port Type

For DSR service connections only, the **To Port Type** field is used to determine if a UNI or NNI port is created when an MDL port is selected as the connection endpoint in regards to the **To Node**. In addition, the selection of a **To Port Type** is used to filter the ports that appear for Port Selection. The **To Port Type** field is a drop-down list. For all container values except **ODUflex** and **OPTSG**, users can select **Terminated** (the default) or **Unterminated**. If the container is **ODUflex** or **OPTSG**, the value is **Terminated**.

Important Provisioning Considerations:

- For 3-ended Y connections and for 4-ended X connections, multiple **To Port Type** fields are displayed, depending on the display of the **To Port** field.
- When DSR connections are automatically discovered (either through application notification or Auto Discovery), the **From/To Port Type** parameter is set for all connection endpoints.
- If the port type is **Unterminated** and the user changes to the container to **ODUflex** or **OPTSG**, and the system changes the **To Port Type** to **Terminated**.
- For DSR service connections with an **Unterminated** port type and for ODUk/LO-ODUj service connections, the rate for unassigned ports in the Port Selection list is equal to the rate of the NNI port that is supported for the card. With the exception of cards that support both ODU2 and ODU2e, no cards support more than one NNI rate.

Example:

For MDL ports on 1XANY100G cards, the rate is ODU4; and for MDL ports on 2XANY40G cards, the rate is ODU3. For cards that support both ODU2 and ODU2e (such as the 10XANY10G), if the container of the connection is ODU2e, the rate will be ODU2e; otherwise, the rate will be ODU2.

- If the user has selected a port and changes the port type, the system deselects the port; meaning, the port value is changed to blank.

Examples:

If the service rate is 10GbE, the container is ODU2, the MDL port is on a 10XANY10G card, and the port type is **Terminated**, a 10GbE port is created; and, if the port type is **Unterminated** an OTU2 port is created.

If the service rate is 10GbE, the container is ODU2, the MDL port is on a 1XANY100G card, and the port type is **Unterminated**, a 10GbE port is created; and, if the port type is **Unterminated**, an OTU4 port is created.

To Port

The **To Port** field is an icon-activated field; or, if you start to type in the port name, the system displays a drop-down list from which you can select the port. The **To Port** is the port in which the connection is to terminate on the **To Node**. For 2-ended connections, users must click the icon adjacent to the **To Port** field to display the Port selection window and they must select the appropriate **To Port** for the first and only **To Node**. For 4-ended connections, users must click the icon adjacent to the **To Port** field to display the Port selection window and they must select the appropriate **To Port** for the second **To Node**. The port name that the user selects in this field is the same port name that appears in the data table for the particular connection.

For Y-Cable protection, users select a known Y-cable port. The successful selection of a known Y-cable port, activates the **Y-Cable Port** panel.

For service connections with the connection rate of ODU0, ODU1, ODU2, ODU2e, and ODU3, users can check the **Show Channelized Ports** check box on the From/To Port selection list.

If **Show Channelized Ports** is checked, the following apply:

- Users can select channelized ports in addition to the unterminated, unchannelized ports.
- The From/To Port selection list includes HO ODU CTPs that are a higher rate than the connection rate and that can be channelized. However, the HO ODU CTPs cannot be selected as connection endpoints.

Examples:

- For an ODU2 connection, HO ODU CTPs with the rate of ODU4, ODU3e2 and ODU3, which can be channelized, are displayed.
- For an ODU3 connection, HO ODU CTPs with the rate of ODU4 and ODU3e2, which can be channelized, are displayed.
- When the user selects an HO ODU CTP, the system displays the LO ODU CTPs of the HO ODU CTP, which have the same rate as the connection rate.

If the **Show Channelized Ports** is unchecked or if the **Show Channelized Ports** field does not appear on the From/To Port selection list, the list includes only unterminated, unchannelized ports. For ODUk/LO-ODUj service connections, the unterminated, unchannelized ports that are displayed in the From/To Port selection list are ports that have the same rate as the service rate of the connection.

To Port Timeslot

When a channelized port is selected in the **To Port** field, users must select an available **To Port Timeslot** from the multi-selection list or enter the port ID.

When creating a DSR connection, a port that is selected on the Port Selection list is a *channelized* when the port rate is ODU n and the port rate is greater than the container rate of the connection. When creating an LO-ODU j service connection, a port that is selected on the Port Selection list is a *channelized* when the port rate is greater than the connection rate.

Example: For a 10GbE connection with an ODU2 container, if the port selected is an ODU3 or ODU4 port, the port is *channelized*; but, if the port selected is an ODU2 port, the port is *not channelized*.

Important provisioning considerations:

- For 3-ended Y connections and for 4-ended X connections, multiple **To Port Timeslot** fields are displayed, depending on the display of the **To Port** field.
- Users can select any set of available timeslots. Timeslots do not have to be selected consecutively. The default value for all timeslot fields is blank, except when timeslots are selected for the **From Port Timeslots** field, the following applies: If the **From Port <x>** or the **To Port <x>** uses the same channel number as the **From Port** and the same timeslots are available for the **To Port Timeslots**, the system automatically selects the timeslots. Users can change the automatically selected **To/From Port <x> Timeslots**.
- When DSR and ODUk service connections are automatically discovered (either through application notification or Auto Discovery) the **From/To Port Timeslot** parameter is automatically set for channelized connection endpoints.
- Depending on the rate of the DSR and LO-ODUj service connections, a prescribed number of timeslots are required. Refer to [Table 7-4, “Service Definition – DSR and LO-ODUj Rates and the Required Number of Timeslots” \(p. 695\)](#) for details. If the user enters too few or too many timeslots, the system outputs a message similar to the following:

[Container rate] requires [number of timeslot required] and [number of timeslots selected by user] are selected.

In addition, the system validates if the timeslot is equal to the channel number of the selected port. If the validation fails, the system outputs a message similar to the following:

Timeslot [number] must be selected.

To Port Pluggable Module

If the user selects an unassigned port on a 1830 PSS OCS NE that is not a fixed port as the **To Port** and the pluggable module is not equipped and not known at the time of port creation, the **To Port Pluggable Module** field is displayed as a drop-down list; all possible pluggable modules are displayed. If the user selects an unassigned port on a 1830 PSS OCS NE that is not a fixed port as the **To Port** and the pluggable module is equipped and known at the time of port creation, the **To Port Pluggable Module** field is automatically populated with the pluggable module type.

For 2-ended connections, users must select one **To Port Pluggable Module**. For 3-ended Y connections and for 4-ended X connections, users must select a pluggable module for each unassigned port.

Important provisioning considerations!

- For easy recognition, unassigned ports have the format: *MDL-bay-shelf-slot-port*.
- Third party pluggable modules are supported and are identified on the drop-down list as **USER**.
- For DSR connections, if the **Port Type** is **Terminated**, the **From/To Pluggable Module** drop down list for a port contains the valid pluggable modules for the port that are based on the card type of the port and the service rate of the connection. For DSR connections, if the **Port Type** is **Unterminated**, the **From/To Pluggable Module** drop down list for a port contains the valid pluggable modules for the NNI ports of the card.
- For ODUk infrastructure connections, users must select a valid **Signal Type** in the **Transmisison Parameters** panel when they use unassigned ports as connection endpoints. Users must select a

pluggable module for every port for which the **To Port Pluggable Module** is displayed. If a pluggable module is not selected for a port, the system outputs a message that is similar to the following:

Pluggable Module is mandatory for <PortName>.

ODUflex Bandwidth (Gps)

The **ODUflex Bandwidth (Gps)**, is a field that is enabled when user select the **Flexible Rate Client as Service rate**. The ODUflex (GFP) rate is a multiple of approximately 1.25 Gbit/s, to correspond to the capacity of an integer number of higher order ODU time slots, and the packet flow is adapted to that rate using GFP.

The number of ODU0 time slots used is fixed, depending on bandwidth selected. The number of the time slots is visible from the Infrastructure connection list.

The number of time slots is obtained dividing the ODUflex Bandwidth (Gps) by 1.25 Gbit/s. Refer to "[ODUflex](#)" (p. 256) for details on ODUflex connection.

Channel Width

The **Channel Width**, is a field that is displayed if the selected template is an **Alien Wavelength** template and the selected from and to Nodes are ENEs or PHN Nodes. The values are 50Ghz, 62.5Ghz, 75Ghz, displayed in a drop-down list, from where the desired value can be selected.

FEC

Optional: The **FEC** field is a drop-down list for infrastructure connections. When creating an OTUk connection or when creating an ODUk integrated provisioning order that auto creates the OTUk, users can select the type of Forward Error Correction for the particular connection. Options include **RSFEC** (Reed-Solomon FEC, the default), **EFEC** (Enhanced FEC), **EFEC2** (Enhanced FEC2), **AFEC** (Adaptive FEC), **SDFEC** (Soft Decision FEC), **SDFEC-G2**, **SDFEC-ACC**, **SDFEC-V NOFEC** (no Forward Error Correction) or **Use NE Values** (the default). The **FEC** parameter is not displayed when **ASON Routed** connections are created. Moreover, the user need not select FEC for ASON routed connection as the GMRE software on the NE determines the best FEC type that is compatible for add/drop and regen in ASON connections.

The following guidelines apply for certain circuit packs:

- If any endpoint is a line port on a 112SDX11 or a port on a 4AN400 display, the option is RSFEC.
- If any endpoint is a client port on D5X500 display the options are RSFEC, NOFEC, Use NE Values (default).
- If any endpoint is a client port on a 112SCA1, 112SNA1 or 130SCA1, the options are RSFEC, NOFEC, Use NE Values (default).
- If any endpoint is a Line Port on a 112SCA1 or 112SNA1, the option is AFEC.
- If any endpoint is a Client Port on a 260SCX2, the options are AFEC, SDFEC, RSFEC, NOFEC, and Use NE Values (default).
- If any endpoint is on a 4UC400, the options are SDFEC-G2, FEC, and Use NE Values (default).
- If any endpoint is on a 2UC400, the option is SDFEC-G2.
- If any endpoint is a line port on D5X500, the option is SDFEC-G2.

- If any end point is on a S2AD200H, the options are SDFEC-G2 or SDFEC-ACC. The connection rate is set to ODU4 for both supported line rates OTU4 and OTU4x2. Mainly, SDFEC-ACC is for long haul applications. This applies to Add/Drop and point to point configurations where both ends are S2AD200H.
- For all other cases the options are AFEC, SDFEC, and Use NE Values (the default).

Transmission Mode

Conditional: The **Transmission Mode** field is a drop-down list that enables users to select the Modulation Format and Wave Shape if the following connection rates and types are being provisioned:

- The **Rate** is OTU4x2 and at least one endpoint is on a D5X500 or 2UC400 circuit pack.
- The **Rate** is OTU4 and at least one endpoint is on a D5X500, 4UC400, or 2UC400 circuit pack.
- The **Rate** is ODU4, **Auto Server Creation** is selected, and at least one endpoint is on a D5X500, 4UC400, or 2UC400 circuit pack.
- The **Rate** is ODU4, the server is OTU4, and **ASON Routed** is selected.

The **Transmission Mode** values that can be selected differ for each pack, for each connection **Rate**, and some are dependent on the **ASON Routed** selection:

- For the 4UC400 pack and for all connection rates, the **Transmission Mode** value is **QPSK Single Channel**.
- For the 2UC400 pack, if the rate is OTU4 or if the rate is ODU4 and the server is OTU4, the **Transmission Mode** values are **QPSK Single Channel** and **SP-QPSK Single Channel**. If the connection rate is OTU4x2 or if the rate is ODU4 and the server is OTU4x2, the **Transmission Mode** values are **8QAM Single Channel** and **16QAM Single Channel**.
- For the D5X500 pack, if the rate is OTU4 or if the rate is ODU4 and the server is OTU4 and the **ASON Routed** field is *not selected* the **Transmission Mode** values are **QPSK Single Channel**, **QPSK Super Channel**, **QPSK Alien**, **SP-QPSK Single Channel**, **SP-QPSK Super Channel**, and **SP-QPSK Alien**; conversely, if **ASON Routed** is *selected* the **Transmission Mode** values are **QPSK Single Channel**, **SP-QPSK Single Channel**, and **Use NE Values**. If the rate is OTU4x2 or if the rate is ODU4 and the server is OTU4x2 and if the **ASON Routed** field is *not selected*, the **Transmission Mode** values are **8QAM Single Channel**, **8QAM Super Channel**, **8QAM Alien**, **16QAM Single Channel**, **16QAM Super Channel**, and **16QAM Alien**. If the rate is OTU4x2 or if the rate is ODU4 and the server is OTU4x2 and the **ASON Routed** field is *selected*, the **Transmission Mode** values are **8QAM Single Channel** and **16QAM Single Channel**.
- If none of the endpoints are on D5X500, 2UC400 or 4UC400 packs, the rate is ODU4 and the server is OTU4 and **ASON Routed** is *selected*, the **Transmission Mode** values are **QPSK Single Channel**, **SP-QPSK Single Channel**, and **Use NE Values**.

Provisioning Considerations:

- When you create an OTU4x2 or OTU4 connection with one or more endpoints on a D5X500 pack, all OCH cross connections in the route must have a bandwidth that is compatible with the selected **Transmission Mode** (Encoding and Wave Shape).
- When more than one **Transmission Mode** value exists, if the **ASON Routed** field is *not selected*, the initial value of the **Transmission Mode** field is the currently provisioned value of **Transmission**

Mode for the From Port. If the **From Port** is not specified or if the **From Port** is not on a D5X500, 4UC400 or 2UC400 pack, the initial value of the **Transmission Mode** is the currently provisioned value of **Transmission Mode** for the **To Port**.

- For ASON routed connections only, if neither the **From Port** or the **To Port** are a D5X500, 4UC400 or 2UC400 pack, the initial value of the **Transmission Mode** is **QPSK Single Channel** for all ODU4 connections.
- If a port does not support the Wave Shape parameter, **Single Channel** is displayed. For example: the 2UC400 pack does not support the Wave Shape parameter; therefore, only the Encoding parameter is applicable.
- The Encoding and Wave Shape values must be the same on both line ports on the D5X500 card. In addition, the Encoding and Wave Shape values must be the same on both line ports on the 2UC400 card. In both cases, since the NE only allows line port L1 to be modified, the L1 port identifier is used when the connection end point is either the L1 or L2 line port.
- When the Encoding value is changed on the NE, the **Phase Encoding** parameter is reset to its default value. In addition, when the Encoding value is changed on the NE, the CD Pre-Compensation value is reset to its default value regardless of the current value of the CD Pre-Compensation for the port.

Auto Discovery and DSR Synchronization Considerations:

When OTU4x2 connections that have one or more endpoints on D5X500, 2UC400, or 4UC400 packs are automatically discovered or when DSR connections are updated during the synchronization process, if the first **From Port** is a port on a D5X500, 2UC400, or 4UC400 pack, the Encoding and Wave Shape values are those received for the first **From Port**; otherwise, the Encoding and Wave Shape values are those received for the first **To Port**.

When OTU4 and OTU4x2 connections that have one or more endpoints on D5X500 packs are automatically discovered or when DSR connections are updated during the synchronization process, if the first **From Port** is a port on a pack, the Encoding and CD Pre-Compensation values are those received for the first **From Port**; otherwise, the Encoding and CD Pre-Compensation values are those received for the first **To Port**. (Note: **CD Pre-Compensation** is a parameter in the **More Parameters** section of the **Transmission Parameters** panel. **CD Pre-Compensation** values can range from 0 to 4300 in increments of 100 or can be **Use NE Values**, the default.)

Phase Encoding

Conditional, for D5X500 circuit packs only: The **Phase Encoding** field is displayed if at least one connection end point is on a D5X500 pack and if the connection rate is OTU4 or OTU4x2 or if the connection rate is ODU4, **Auto Server Creation** is selected, **ASON Routed** is not selected.

The **Phase Encoding** field is a drop down list. Users can select **Phase Encoding** to be **Absolute**, which is a compatibility mode with pilot, or **Differential**, which is the high performance mode without pilot.

Provisioning Considerations:

- The initial value of the **Phase Encoding** field is the currently provisioned phase encoding value of the **From Port**. If users do not select a **From Port** or if the **From Port** is not on a D5X500 pack, the initial value of the **Phase Encoding** field is the currently provisioned phase encoding value of the **To Port**.

-
- The **Phase Encoding** field must have the same value on both line ports (L1 and L2) on the D5X500 pack. Since the NE only allows modification of line port L1, when the connection endpoint is either the L1 or L2 line port, L1 is used as the port identifier.

Customer Name

Optional: The **Customer Name** field is a drop down list. Users can select the **Customer Name** that is to be associated with the connection being created.

The customer names that are displayed on the drop-down list are names that users enter from the **Administer > Customers** navigation path on the NFM-T GUI. Refer to the **Administer - Customers** section in the *Administration Guide* for details.

For auto-discovered connections and system auto-generated connections, the customer name is **None**.

Connection Name

Optional: The **Connection Name** field is a text field. Users can enter the **Connection Name** that is to be associated with the connection being created. The name that the user inputs in this field is the same name that appears in the data table for the particular connection. In addition, the **Connection Name** field is controlled by installation parameters. Refer to [2.26 “Connection names and aliases” \(p. 260\)](#) for details.

Connection Alias

Optional: The **Connection Alias** field is a text field. Users can enter the **Connection Alias** that is to be associated with the connection being created. The alias that the user inputs in this field is associated with the name that is supplied in the **Connection Name** field. In addition, the **Connection Alias** field is controlled by installation parameters. Refer to [2.26 “Connection names and aliases” \(p. 260\)](#) for details.

Roll Back On Failure

The **Roll Back On Failure** field is a check box. It must display a check mark for all types of Service and Infrastructure creation templates. When the user checks this option during the connection creation, on failure of connection, the creation is cancelled.

Compute Latency

The **Compute Latency** field is a checkbox. By default, **Compute Latency** is checked.



Note: The **Compute Latency** function is only available for NE R11.1 or greater.

Latency measurement is used to compute the amount of time taken by a signal in traveling from the AEnd to the ZEnd for a service. This measurement is only available for created services with UNI rates (that is, 10GbE, 100GbE, STM, and SONET rates). It is not available for created services with NNI rates (ODU2, ODU3 rates).

After **Compute Latency** is executed, four new values are displayed in the **Services** page:

- **Actual Latency-WORK (microsec)**, the computed working latency
- **Actual Latency-PROTECT (microsec)**, the computed protected latency

- **Latency Status**, an indication of the status of the **Compute Latency** operation. Possible values are:
 - SUCCESS indicates that latency computation was successful
 - NOT COMPUTED indicates that latency computation was not performed
 - “DMF” indicates that the DM test failed (for example, when there is a failure in one of the paths of a protected scenario, such as OPSB/YCABLE/ESNCP)
 - NOT SUPPORTED indicates that the selected card does not support latency computation
- **Latency Timestamp**, the time of execution for the **Compute Latency** operation.



Note:

- For ODU protected connections (Low Order ODU or High Order ODU), NFM-T is not tracking the latencies on working and protection path. It is ONLY going to report latency on ACTIVE path. The separate columns, **Actual Latency-WORK (microsec)** and **Actual Latency-PROTECT (microsec)** are significant only for client, DSR protected services (ycable or OPSB), where two values for each underlying ODU are available. Clearly the values are filled for a WORKING and PROTECTION ODU that can be measured individually in the network at the same time.
- For a client-protected service with working and protection legs, the **Latency Timestamp** is the timestamp from the last measurement operation.
- When there is no latency, the actual latency for working and protection services are not applicable. So **Actual Latency-WORK (microsec)** and **Actual Latency-PROTECT (microsec)** displays 0 on the GUI.

The success/failure of the **Compute Latency** operation is logged in the **Jobs** page and User Activity Log.

While **Compute Latency** can be enabled at service creation time, for an already created service **Compute Latency** can be enabled from the:

- **Service** page
- **Modify Connection** dialog
- **Routing Display**
- **REST API**



Note: Latency can be computed for no more than ten services at a time. Attempting to compute latency for more than ten services at a time results in an error message.

ASON Routed

The **ASON Routed** field is a check box. It must display a check mark if the connection is to be a Control/Mixed plane connection or an ASON MRN terminated or unterminated tunnel. If the box is unchecked, the connection becomes a Managed Plane or Logical Drop Link. This field is not applicable for OTUk connection rates.

Considerations:

When the **ASON Routed** field is checked in the **Service Definition** panel, the system activates field option for **ASON Restoration**.

If **ASON Routed** is checked in the **Service Definition** panel, when creating a connection or when modifying the route of a connection, drop link connections or link connections that belong to connections with drop link connections cannot be selected from the Routing Constraints table when **Manual** routing is selected.

For ASON routing constraints, refer to “[Physical connections as a constraint for routing](#)” (p. 733).

ASON Restoration

Optional: If the **ASON Routed** field is checked for infrastructure connections and services, the **ASON Restoration** field is displayed as a drop-down list. Users can select the restoration method that is appropriate for the connection to be **No Restoration**, **Sourced-based Restoration** (the default), or **Guaranteed Restoration**.

CIR Rate

Optional: For substrate Ethernet services only, the **CIR Rate** field is a drop-down list that displays the Committed Information Rate. Users can select a value.

CBS

Optional: For substrate Ethernet services only, the **CBS** field is a drop-down that displays the Committed Burst Size. Users can select a value.

EIR Rate

Optional: For substrate Ethernet services only, the **EIR Rate** field is a drop-down list that displays the Error Information Rate. Users can select a value.

EBS

Optional: For substrate Ethernet services only, the **EBS** field is a drop-down list that displays the Error Burst Size. Users can select a value.

CE VLAN

Optional: For substrate Ethernet services only, the **CE VLAN**, or Carrier Ethernet VLAN, field is a text field. Users can enter a value.

S VLAN

Optional: For substrate Ethernet services only, the **S VLAN**, or Service VLAN, field is a text field. The default is **Default**. Users can enter a value.

OPSB Port

For the deployed templates that support the OPSB protection, the OPSB port panel is visualized above the Advance Settings after users select the From/To Node ports in the Service Definition panel. For OPSB protection only SIG ports must be selected.

In the **From A Side/To A side** fields define the type of the path. From the drop down menu users can select between **Working** or **protection**. The **From B Side/To B Side** are populated accordingly.

The **From Node/To Node** fields are populated according to choices made in the *Service Definition* panel. Complete the **From Port/To Port** field from the drop-down menu. For details of the supported packs refer to [4.5 “OPSB and OPSB5 protection” \(p. 447\)](#)

The **Revertive Mode** default value is **Disable**, to enable the revertive mode from the drop-down menu select **Enable**.

When the revertive mode is enabled, the **Wait to Restore Time** field is visualized and its default value is 5 m. The value is expressed in minutes, the user can select it in a range from 0 to 360.

Optical line characteristics

This panel is enabled when the user selects **OTSig Tunnel** as the **Rate**. The OTSig Tunnel is enabled for cards that are equipped with ADD3 and ADD4 ASIC. The line port rate is OTSi regardless of the line capacity. The client ports signal rates is 100GBE with ODU4 container and OTU4.

Currently, ADD4 ASIC is supported for S4X400H, DFC12, DFC12E, DFM6, SFM6, , 2UX500 and DFM6E, and ADD3 is supported for 8UC1T card.

Figure 7-19 Optical line characteristics panel

The screenshot shows the 'Deploy Connection' wizard at step 3, 'PARAMETERS'. The 'Rate' dropdown is set to 'OTSig Tunnel', which has highlighted the 'OPTICAL LINE CHARACTERISTICS' section. The 'Profile Number*' dropdown is set to '2'. Other parameters like 'Channel Width*' are also visible.

Click the **Search** icon in the **Profile Number** field to select the **Line Mode Profiles**. Depending on the **Profile Number** selection, the values of the rest of the parameters change. The options available in the **Channel Width** field depends on the option selected in the Profile Number.

Currently, NE supports profiles 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 15, 2126, 27, 29.

See [Table 8-15, “Profile and Card Mapping” \(p. 1267\)](#) for more information on the mapping between the profile and supported cards.

See [Table 8-4, “Profile Number and supported Parameter values ” \(p. 1236\)](#) for more information on the profiles and the supported parameter details.

Buttons

The following buttons are displayed in the Service Definition panel for deployed infrastructure connection and service templates.

Deploy

The **Deploy** button is used to deploy the template. Users must click on this button so the connection can be made in the system.

Save as Template

The **Save as Template** button is used to save the deployed template as a My Templates template. Users must click on this button to save the template as a My Templates.

Cancel

The **Cancel** button is used to cancel the request to deploy the template. Users must click on this button to cancel the request to deploy the template.

7.5 Advanced Settings field descriptions for deploy Best Practices templates

Overview

There are two main panels available in **Advanced Settings**. The example on the left illustrates the **Advanced Settings** panels that are displayed for all templates/connections, whereas right illustrates the additional **Advanced Settings** panels that are displayed for ASON and SNC protection.

Connection Controls

The **Connection Controls** panel is used to specify the parameters that control the connection as it is being deployed.

Routing

The **Routing** field is a drop-down list. Values are **Automatic** (the default) or **Manual**.

Automatic routing supports unprotected and protected routes. With unprotected routes, traffic is not protected at any layer (its own layer or at the server layers) and does not contain any pre-emptible segment. The server layers can be the immediate server of the provisioned connection or its indirect server layer. With protected routes, traffic is protected from end-to-end (either at the physical level or at the logical level).

If Routing mode is Automatic, the user can specify partial constraints, that is, end-to-end connectivity is not needed. It is sufficient to include or exclude the preferences. The constraints supported are as detailed already. For Managed Plane, the user can include/exclude server trails and 3R constraint.

Automatic routing is only supported for the deployment of new connections (**Add** orders). Automatic routing does not support the modification (the **Rearrange**) of optical layer connections.

i Note: If routing mode is **Automatic**, the user can just specify the frequency constraint for Managed Plane without selecting any trails. The user must specify atleast one trail and frequency constraint for ASON routed connections.

If routing mode is **Manual**, the user needs to specify all the trails for the end-to-end connectivity or all the link connections for the end-to-end connectivity in addition to 3R constraint as needed. It can be in any order but end-to-end connectivity must be specified. The internal links, within the same node, are determined by the system and there is no need for the user to specify them.

Target State

The **Target State** field is a drop-down list. Values are **Commissioned** (the default), **Defined**, **Allocated**, or **Implemented**.

Auto Server Creation

The **Auto Server Creation** field is a check box. The **Auto Server Creation** field determines if the user or the NFM-T system creates the server layer for the infrastructure connection or service.

When the **Auto Server Creation** box is checked, the NFM-T automatically creates the server layer for the infrastructure connection or for the service that the user is currently creating, if the server layer is needed.

Subsequently, these connections, meaning the infrastructure connection and the service that are being created, along with the server layer connection, will become part of a group and will be managed as a group. For example: if the infrastructure connection or service connection is removed, the servers that were originally created for the particular connection are also removed. When the box is unchecked, users must create each connection layer separately.

Provisioning notes:

- If the **Auto Server Creation** field is checked and the server of the connection that is being created already exists in the Allocated, Implemented, or Commissioned step, the system rejects the provisioning request and outputs an error message. Users must cancel the server connection from the connection data table and re-submit the provisioning request.
- When users create HO-ODUk infrastructure trail connections using pool ports for compound node uplink configurations that include multiple hops or protected ODUk infrastructure trails, the **Auto Server Creation** box must not be checked during connection provisioning.

For example, for an ODU4 infrastructure connection between an 130SCX10 line and an ODU pool that rides on an ODU4 between the 130SCX10 and an 130SCUP, users must not check the **Auto Server Creation** box. Users must create the OTU4 infrastructure trail, then the ODU4 infrastructure that terminates on the pool port, then the ODU2 protected connection, and lastly the DSR service connection.

- When users create HO-ODUk infrastructure trails using pool ports for compound node uplink configurations that include single hops and unprotected ODUk infrastructure trails, the **Auto Server Creation** box must be checked during connection provisioning.

For example, for an OTU4 infrastructure connection between an 130SCUP and an SCUPB that has an ODU4 infrastructure connection between an ODU pool, users must check the **Auto Server Creation** box. Users must create an ODU4 logical link that terminates on the OTU/ODU4 ports of the uplink card and then create the DSR service with LO-ODUk servers and also check the **Auto Server Creation** box when creating the DSR. The system automatically creates the ODU4 connection on the pool ports, so the user does not have to create the connection to the pool ports manually. Note, however, that if users create the DSR service (with an ODU4 server layer) on an 1XANY100G circuit pack, the ODU4 that terminates on the pool ports cannot be created because the ODU4 is the server for the DSR service; therefore, the ODU4 is simply terminated on the 1XANY100G pack.

If users choose to use the **Manual** instead of the **Automatic** routing option for creating the DSR service, when creating the first DSR, the link connection(s) from ODU4 logical link that terminate on the OTU/ODU4 ports of the uplink card should be used as the routing constraints. For the second consecutive DSR, the link connection(s) from the system created ODU4 connection that terminate on ODU pool ports should be used as the routing constraints. The **Auto Server Creation** box should be checked for all of this DSR service provisioning.

If the **Auto Server Creation** check-box is not checked during service/connection creation, then NIM is not enabled on that service/connection. For NNI services, the **Auto Server Creation** is not applicable. Even if the **Auto Server Creation** check-box is unchecked, NIM is enabled and the **Enable NIM** is checked.

Allow Uncommissioned Links

The **Allow Uncommissioned Links** field is a check box. Users should check this box if they want the system to create the connection regardless of the commission status of the optical amplifiers. If users check this box, they must make any manual power adjustments from Wavelength Tracker for both egress and ingress ports on the uncommissioned link. If users do not check this box, the connection fails if any optical amplifier in the connection is not commissioned.

Allow Uncommissioned Links Background: The NFM-T OTN allows users to create an OCH or OTUk connection for 1830 PSS, 1830 PSS-4, or 1830 PSS-1 NEs even if the commissioned status of all of the optical amplifiers in the connection are not commissioned. The NFM-T displays the commissioned status of the optical amplifiers on the External OTS connections. An External OTS connection is considered an uncommissioned link if any optical amplifier in the connection is not commissioned. Users can view the commissioning status of the External OTS connections from the Physical Connection list.

Provisionable Wave Key

Depending on the template/connection type, the **Provisionable Wave Key** field is displayed as drop-down list. Values are **Keyed** (the default), **UnKeyed**, or **N/A**. The **Provisionable Wave Key** field is required for NEs that allow users to select if Wavelength Tracker functionality is enabled or disabled for an OCH/OTUk/OTU4x2/OTL4.4 connection. If the connection does not contain any NEs that support provisionable Wavelength Tracker, users must select the value **N/A**. If the connection contains at least one NE that supports provisionable Wavelength Tracker, users must select **Keyed**. If the connection contains at least one NE that supports provisionable Wavelength Tracker, users can select **UnKeyed** to disable Wavelength Tracker.

The system displays the Provisionable Wave Key parameter when users create any one of the following types of logical connections:

- An OTUk or OCH infrastructure connection.
- An OCH service connection.
- An ODUk infrastructure connection if one or more connection endpoints is an HO-ODUk port or an ODUk CTP on a 260SCX2 pack and **Auto Server Creation** is checked.
- An ODUk infrastructure connection if one or more connection endpoints is an ODUk CTP on a 1UD200 pack and the **Auto Server Creation** field is checked.
- An ODUk service connection if one or more connection endpoints is an HO-ODUk port and **Auto Server Creation** is checked.
- An ODUk infrastructure connection or an ODUk service connection if one or more connection endpoints is an ODUk CTP on a pack that supports a NNI client port rate that is equal to the line port rate (11STAR1, 11STAR1A, 43STA1P, 43SCA1, 11QPA4, 11QPEN4, 112SCA1, 112SNA1 and 130SCA1) and **Auto Server Creation** is checked.
- An ODUk infrastructure connection if one or more connection endpoints is an ODUk CTP on a D5X500 pack and the **Logical Link** field is checked and the **Auto Server Creation** field is checked.

The following conventions hold for the services that support Provisionable Wave Key configuration:

- For Transparent Alien Wavelength (OCH) services, the **Provisionable Wave Key** field is set as **Keyed** by default.

- For Transparent Alien Wavelength (unkeyed OCH) services, the **Provisionable Wave Key** field is set as **UnKeyed** by default.
- For Transparent OCHP Protected Alien Wavelength (OCH) services, the **Provisionable Wave Key** field is set as **Keyed** by default.

If users select **Keyed**, the system validates that neither end ports of the connection are on an unsupported NE or circuit pack. If the validation fails, a message similar to the following is displayed:

Keyed operation is not supported for selected route...

Important! During Single Step Provisioning if an OTUk/OTU4x2/OTL4.4 connection already exists and does not need to be created by the system, the host ignores any value that is entered for the OTUk **Provisionable Wave Key** field; meaning, if users select the value **Keyed** and the existing OTUk connection is **Unkeyed**, the system uses the existing OTUk connection as a server and an error is not reported.

OTN Provisionable Wave Key

Depending on the template/connection type, the **OTN Provisionable Wave Key** field is displayed as drop-down list. Values are **Keyed** (the default), **UnKeyed**, or **N/A**. The **OTN Provisionable Wave Key** field is displayed for HO-ODUk connections, for ODUk connections on 260SCX2 packs, for ODUk connections on 1UD200 packs, for ODUk logical links on D5X500 packs, and for ODUk connections on packs with NNI port rate equal to the line port rate (such as the 11QPA4, 112SCA1).

Table 7-5 Provisionable Wave Key for ADD4 cards

ADD4 cards	Managed Plane	Control Plane
S4X400	Provisionable Wavekey: Unkeyed WaveKey Type: Manual with Dangling OT configuration WaveKey Type: Auto with Cluster OT configuration	Provisionable Wavekey: Unkeyed WaveKey Type: Auto with Cluster OT configuration
DFC12 and DFC12E	Provisionable Wavekey: Unkeyed WaveKey Type: Manual with Dangling OT configuration WaveKey Type: Auto with Cluster OT configuration	Provisionable Wavekey: Unkeyed WaveKey Type: Auto with Cluster OT configuration

i Note: NFM-T does not support System Generated Manual Wave Keys for ADD4 cards.

Transmission Parameters

The **Transmission Parameters** panel is used to specify and, in some cases, to modify the parameters that control the transmission of the connection as it is being deployed.

Panel Behavior

All transmission parameters are *optional*. The transmission parameters that are displayed in the panel depend on the connection rate, the service type, and the end NEs that are selected for the

connection. If users type in the NE name instead of selecting it from the system, the **Transmission Parameters** panel is not enabled; the system then sets the transmission parameters for the connection to **Use NE Values**. In addition, refer to “[More Parameters](#)” (p. 714) for other **Transmission Parameters** panel behavior details.

For certain connections, the **Transmission Parameters** panel is also equipped with a **More Parameters** button, which enables users to access the Modify Transmission Parameters window.

Forward Error Correction Type— MoreTransmission Parameters

The **FEC Type** parameters are available in the **Modify Transmission Parameter** window, based on the service and the cards chosen (either S13X100 cards or S2AD200 cards). These parameters are used to set the FEC type, and are applicable during service creation with client ports. Select the **Flexible Rate** as **ODUFlex** to view these parameters.

Select the type of Forward Error Correction from the **A End Client FEC Type** and **Z End Client FEC Type, New** drop-down.

i Note: WaveLite supports BJFEC FEC type for 100GbE client ports, only on WLM200B, WLM200OPB, and WLA200B packs.

LOS Propagation

The **LOS Propagation** fields can be found in the Modify Transmission Parameter window, these parameters determine the action that should be taken when a loss of signal occurs for the connection. Values are **From End LOS Propagation**, **To End LOS Propagation**. The values can be **Laser On** and **Laser Off**.

Signal Type

The **Signal Type** field is a drop-down list that defaults to **Default** or the appropriate signal type for the selected connection. For example: **OMS** is the default for an OMS-P Protected, OMS connection; **OCH** is the default for an OPSA Protected, Alien Wavelength (OCH) connection.

Provisioning Consideration:

When creating an ODU4 connection, all connection endpoints must have the same **Signal Type**. This means that all endpoints must be OTU4 or all endpoints must be OTU4X2.

Line Port Time Slot(s)

The **Line Port Time Slot(s)** field is a text field. Users can type a list of time slots separated by the ampersand symbol (&).

The number of entries that are required in the **Line Port Time Slot(s)** field is based on the **Signal Type** of the client port:

- For a **Signal Type** of OC3, STM1, or FE, users must enter one entry in the **Line Port Time Slot(s)** field.
- For a **Signal Type** of OC12 or STM4, users must enter four entries in the **Line Port Time Slot(s)** field.

The **Line Port Time Slot(s)** field is required in these configurations:

- When the line port for the 4DPA4 and PSS1MD4 circuit packs is in Flex mode.

- When a client port on a 4DPA4 or PSS1MD4 circuit pack is in FlexMux mode and is the endpoint of the connection.

OTUk and OTU4x2 subpanels for D5X500 circuit packs

For the D5X500 circuit pack, there is no OTU4/OTU4x2 server connection; therefore, all transmission parameters for the OTU4/OTU4x2 layer are set with the ODU4 connection when users create or modify a connection. Explanations of each transmission parameter are available when users mouse over the parameters in the data table. In addition, users should refer to the documentation for the particular 1830 PSS NE for circuit pack and transmission parameter details. Also note that for the OTU4x2 connection, two sets of data are collected; one set for each OTU4 port.

Configurable Hold-off Timer

Starting with 1830 PSS Release 10.1, users can configure a hold-off timer to delay consequent action signaling on output ports in case of Server Signal Failure (SSF) by defining the **SSF Delay Timer (ms)** parameter. This option applies to 1830 PSS PHN Network Elements and 1830 PSS OCS Network Elements with client cards and service rates as summarized in the following tables.

Table 7-6 Applicable Cards and Service Rates for 1830 PSS OCS Network Elements

Card Type	Service Rate
10AN10GC	10GbE

Table 7-7 Applicable Cards and Service Rates for 1830 PSS PHN Network Elements

Card Type	Service Rate
20AX200	OC192, STM64, 10GbE
20AN80 20MX80	OC3 OC12 OC48 OC192 STM1 STM4 STM16 STM64 1GbE LAN 1GbE Conv 10GbE
30AN300	OC192, STM64, 10GbE

The **SSF Delay Timer (ms)** works together with the **SSF Delay Consequent Action** and **SSF Consequent Action** transmission parameters, that is configured by clicking the **More Parameters** button. See “[More Parameters](#)” (p. 714) for more information.

The **SSF Delay Timer (ms)** field is a numerical field with values in the range of 0 to 2550 ms in 10 ms steps.

Configuration State of Polarization Tracking Speed on D5X500

Polarization tracking allows the user to provision the speed at which the coherent line receiver tracks state of polarization changes. The State of Polarization (SOP) at the output of an optical fiber link can randomly fluctuate in time due to environmental stresses, for example temperature or mechanical shock. In the presence of polarization-sensitive equipment at the end of the optical link, a coherent receiver, the stabilization of the SOP at the fiber output requires polarization control with relatively high tracking speed. Slower tracking speed typically means less adaptation noise. Faster tracking speed results in a reduced optical reach of the transmitted signal; however, it provides increased tolerance to mechanical fiber stresses seen in certain deployments.

D5X500, D5X500Q and D5X500L circuit packs provides a new configuration parameter, which refers to the line ports. The parameter is **Polarization State Change Tracking**.

This parameter allows to configure the speed at which the coherent receiver tracks polarization state changes. Depending on the value set on the card, the optical reach is reduced, but at the same time the signal gets an increased tolerance against anomalies such as fiber mechanical stress. The unit of measure is *Krad/msec*. The default value is 1 Krad/msec for all modulations.

This field is displayed only if at least one connection endpoint is on a D5X500, D5X500L or D5X500Q circuit packs. The default value is **Use NE Values**. Choose the value from the drop-down list. Modifying this parameter is a service impacting event. Possible values are:

- **Normal**
- **Fast**

This parameter is applied on **1830 PSS** for rate OTU4, OTU4x2, OTU4Half, OTU4Halfx5 and on **PSI-2T** for rate OTU4, OTU4x2, OTU4Halfx5.

More Parameters

For some connection configurations involving certain circuit packs, users can click the **More Parameters** button. The system displays the **Modify Transmission Parameters** window for the selected connection type and service rate along with the NE transmission parameters that can be modified. Descriptions of the transmission parameters are available when users hover over the parameter names in the **Parameters** tab. In addition, users must refer to the documentation for the particular 1830 PSS or PSS OCS NE for circuit pack and transmission parameter details.

OPSB or OPSB5 Protection Triggered by Signal Degrade

NFM-T supports OPSB or OPSB5 client protection with Signal Degrade (SD) or Signal Fail (SF) trigger for S13X100R, S13X100E, and D5X500Q circuit packs supported for NE release R11.0.

Moreover, the system supports OPSB or OPSB5 triggered by Signal Degrade for 1830 PSS24x (rel 11.1) with the following packs 20AN80, 30AN300, 10AN400, 4AN400.

To trigger signal degrade for protected OPSB or OPSB5 protections, complete the following steps:

1. Create an OPSB or OPSB5 protected connection for the considered packs.

2. Select a service from the **Operate > Services** page, right-click and select **Modify > Parameters**.
3. On the **Modify connection** page, expand the **Transmission Parameters** pane and click **More Parameters** button.
4. In the **Modify Transmission Parameters** window, set the value of the following parameters.

Parameter	Description
A End SSD Consequent Action	<ul style="list-style-type: none">• Laser Off• No Action• Use NE Value
Z End SSD Consequent Action	<ul style="list-style-type: none">• Laser Off• No Action• Use NE Value

i **Note:** The user must select an OPSB template for OPSB service creation of different rates, such as Ethernet, SDH, and SONET. If the user is using any other template, the **Transmission Parameters (SSD and LOS Propagation)** needs to be explicitly set as per the requirement mentioned in the table below. Else, an error message is displayed during service creation. **SSD Consequent Action cannot be set to Laser Off when LOS Propagation is Laser On.**

If	Then
the SSD Consequent Action is Laser Off	LOS Propagation cannot be changed to Laser On
the LOS Propagation is Laser On	SSD Consequent Action cannot be changed to Laser Off

If the user does not modify any Transmission parameters and deploy OPSB service connection, the following values are set by default:

1. LOS Propagation is set to Laser Off
2. SSD Consequent Action is set to Laser Off

Transmission Parameters : Port Administrative State

The Transmission Parameters panel in the **DEPLOY > New Service/Infrastructure Connection** template for service creation has additional fields to set the **Port Administrative State** and the **AINS Timer**. This includes NNI services (un-terminated ODUk).

During service provisioning, the client port administration state can be set to **AINS** or **IS**. The default value is **AINS**. The user can set a timer at which the administrative state of the client port can be automatically set to in service using the **AINS Timer** field. If user sets the port administrative state to **IS**, then the **AINS Timer** field is not displayed.

OCHP

If the deployed template is an OCHP, SNC-I or SNC-N protected infrastructure trail template, the **OCHP Protection** panel is displayed in **Advanced Settings**.

OCHP Revertive Mode

Optional: The OCHP Revertive Mode fields allows to enable the OCHP revertive mode, that is the traffic is automatically switched back to the working circuit. Possible values are: enabled, disabled. The default value of OCHP Revertive Mode is **Disabled**.

Wait To Restore Time (min)

The Wait to Restore Time (min) is displayed if the value of OCHP Revertive Mode is **Enabled**. The default value of Wait to Restore Time is 5 minutes.

ASON

If the **ASON Routed** check box is checked in a non-deployed template, the **ASON** panel in **Advanced Setting** is displayed.

The **ASON** panel is used to specify the parameters that control the routing of the connection for the Automatic Switched Optical Network (Control Plane, G.7718). These parameters include Tandem Connection Monitoring, along with timing, priority, and restoration parameters.

TCM Level

The **TCM Level** field is a drop-down list that determines the Tandem Connection Monitoring level. Values are **no TCM** (the default), **Level 1**, **Level 2**, **Level 3**, **Level 4**, **Level 5**, or **Level 6**.

Max Latency

The **Max Latency** field is a text field. Users can enter the value that is needed.

Default Priority

The **Default Priority** field is text field that defaults to **4**. Users can specify another value by clicking on the **X** and typing the preferred value.

Default Setup Priority

The **Default Setup Priority** field is a text field that defaults to **5**. Users can specify another value by clicking on the **X** and typing the preferred value.

Reversion Mode

The **Reversion Mode** field is a drop-down list. Values are **Manual** (the default), **Auto** or **Soft Automatic**.

Wait for Server Restoration

The **Wait for Server Restoration** field is a drop-down list. Values are **Disable** (the default), **Enable**, or **Not Applicable**.

Include Any Color Name

The **Include Any Color Name** field is an icon-activated field. Users must click the icon adjacent to the **Include Any Color Name** field to display the Include Any Color Name selection window and they must select the appropriate color profile from the data table that is displayed. The color specified must be same color that is allocated to the link.

Resource Coloring helps users to assign colors to links (such as TE links, physical/logical connections, trails, paths, or subnetwork connections (SNCs) in order to separate traffic and to identify unique routes that are used to upload and carry traffic. Users can choose different strategies to color-code their networks for ease of visibility.

Exclude Any Color Name

The **Exclude Any Color Name** field is an icon-activated field. Users must click the icon adjacent to the **Exclude Any Color Name** field to display the Exclude Any Color Name selection window and they must select the appropriate color profile from the data table that is displayed. The color must be same color that is allocated to the link.

Resource Coloring helps users to assign colors to links (such as TE links, physical/logical connections, trails, paths, or subnetwork connections (SNCs) in order to separate traffic and to identify unique routes that are used to upload and carry traffic. Users can choose different strategies to color-code their networks for ease of visibility.

SNC Protection

If the deployed template is an SNC-I or SNC-N protected infrastructure trail template or an SNC-NC SONET or SDH protected service template, the **SNC Protection** panel is displayed in **Advanced Settings**.

The **SNC Protection** panel is used to specify the Subnetwork Connection (SNC) protection parameters for the connection. SNC Protection is a level of subnetwork connection protection that can be specified for infrastructure connections (trails) or services in order to create protected cross connections on 1830 PSS OCS NEs or on 30AN400 and 4AN400 circuit packs pack or black boxes or a port on the Virtual Plane (which is a port with slot identifier equal to 71).

Note that when you create a connection that contains any SNC protected cross connections on 20P200, 30AN400, 4AN400 packs or on ports on the Virtual Plane, the **SNC Protection** panel is automatically enabled for any Modify Transmission Parameters requests.

Users can specify SNC parameters for the following types of infrastructure connections (trails) and services if the following apply:

- For connections in which the connection **Rate** is ODUk or the connection **Rate** is DSR and **Auto Server Creation** is selected.
- For infrastructure connections (trails) and services in which the **Connection Shape** is **2 Ended Bi (I)**, **2 Ended Split Bi (I)**, **4 Ended Bi (X)**, **3 Ended A Bi (Y)**, or **3 Ended Z Bi (Y)** (and are collectively referred to as one of the supported **Bi** shapes).
- For infrastructure connections (trails) and services in which 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 in which the **Y-Cable Protection** parameter is disabled (set to **No**).
- For services in which the connection level **OPSB Protection** parameter is disabled (set to **No**).

Important!

For Managed Plane connections, which are those in which the **ASON Routed** check box is not checked, the fields in the **SNC Protection** are not listed under Managed Plane and Control Plane categories. For Mixed Plane/Control Plane connections, which are those in which the **ASON Routed** check box is checked, the fields in the **SNC Protection** are listed under Managed Plane and Control Plane categories. These parameters are marked as: <Managed Plane> Network ...> in this section.

Client Protection Type

If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 30AN300 pack, a 4AN400 pack, a 20P200 pack or a black box and for connections where the **Connection Shape** is one of the **3-Ended** or **4-Ended** shapes, the **Client Protection Type** field is activated and displayed as drop-down list. For SNC protection, the values are **SNC-I** (which is SNC protection with inherent monitoring and is only displayed if all connection end points are on an 1830 PSS OCS NE or a black box), **SNC-N** (which is SNC protection for network ports), **SNC-Nc** (which is SNC Protection for network client ports. See “[1+1 ODUj SNC/Nc protection interworking with SDH NEs](#) (p. 500)”), or **None**. For other protection types, the value is **None**. If the user selects **None**, the remaining **Client Protection Type** parameters are no longer displayed.

Client Hold Off Time (msec)

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, or a black box and the Connection Shape is one of the supported **Bi** shapes, the **Client Hold Off Time (msec)** field is activated and displayed as drop-down list, which ranges from 0 to 10,000 in 20 msec increments up to 100, and 100 msec increments thereafter until 10,000 msec.

Client Protected Protection Method

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, or a black box and the Connection Shape is one of the supported **Bi** shapes, the **Client Protected Protection Method** field is activated and displayed as drop-down list. If **Client Protected Protection Method** is **SNC-I**, the default is **ODUk Path Adaptation**, that is only displayed if all connection end points are on 1830 PSS OCS NEs or black boxes. If the **Client Protected Protection Method** is **SNC-N**, the default is **ODU Path NIM Protection**; other **SNC-N** values include **TCM-1**, **TCM-2**, **TCM-3**, **TCM-4**, **TCM-5**, and **TCM-6**.

Client Protecting Protection Method

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, or a black box and the Connection Shape is one of the supported **Bi** shapes, the **Client Protecting Protection Method** field is activated and displayed as drop-down list. If the **Client Protecting Protection Method** is **SNC-I**, the default is **ODUk Path Adaptation**, that is only displayed if all connection end points are on 1830 PSS OCS NEs or black boxes. If the **Client Protecting Protection Method** is **SNC-N**, the default is **ODU Path NIM Protection**; other **SNC-N** values include **TCM-1**, **TCM-2**, **TCM-3**, **TCM-4**, **TCM-5**, and **TCM-6**.

Client Signal Degrade for Protection Switching

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, or a black box and the Connection Shape is one of the supported **Bi** shapes, the **Client Signal Degrade for Protection Switching** field is activated and displayed as drop-down list, which can be specified as **Enable** or **Disable**.

Client Wait to Restore Time (min)

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, or a black box and if the **Client Protection Type** is **SNC-N** or **SNC-I**, the **Client Wait to Restore Time (min)** field is activated and displayed as drop-down list. The **Client Protection Type** can be specified as 1 to 15 minutes if the value of the **Client Protection Type** is **SNC-N** or **SNC-I**.

Client Revertive Mode

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, or a black box and if the **Client Protection Type** is **SNC-N** or **SNC-I**, the **Client Revertive Mode** field is activated and displayed as drop-down list. The **Client Revertive Mode** field can be specified as **Enable** or **Disable** if the value of the **Client Protection Type** is **SNC-N** or **SNC-I**.

Network Protection Type

Optional: If ASON Routed is not selected, the **Network Protection Type** field is displayed a drop-down list. For SNC protection, the values are **SNC-I** (which is SNC protection with inherent monitoring and is only displayed if all connection endpoints are on an 1830 PSS OCS NE or black box), **SNC-N**, or **None**. If all connection endpoints are on 11DPM8 circuit packs and black boxes, **SNC-Nc** is displayed. For other protection types, the value is **None**. If the user selects **None**, the remaining **SNC Protection** parameters are no longer displayed.

Network Hold Off Time (msec)

Optional: If ASON Routed is not selected and the Network Protection type is not **SNC-Nc**, the **Network Hold Off Time (msec)** field is displayed as a drop-down list. Values are **0** (the default) to **100** in 20 msec increments and **100** to **10000** in 100 msec increments.

Network switch mode

This field define the network switching mode for SNC protection. The values could be **Unidirectional** or **Bidirectional** for **SNC-N** protection, **Unidirectional** for **SNC-I** protection.

Network Protected Protection Method

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, a port on a Virtual Plane (that is a port with a slot identifier that is equal to 71), or a black box, and if ASON Routed is not selected, the **Network Protected Protection Method** field is activated and displayed as drop-down list. If the **Network Protection Type** is **SNC-I**, the default is **ODUk Path Adaptation**, that is only displayed if all connection end points are on 1830 PSS OCS NEs or black boxes. If the **Network Protection Type** is **SNC-N**, the default is **ODU Path NIM Protection**; other **SNC-N** values include **TCM-1**, **TCM-2**, **TCM-3**, **TCM-4**, **TCM-5**, and **TCM-6..** If the **Network Protection Type** is **SNC-Nc**, only **ODU Path NIM Protection** is displayed.

Network Protecting Protection Method

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, a port on a Virtual Plane (which is a port with a slot identifier that is equal to 71), or a black box, and if ASON Routed is not selected, the **Network Protecting Protection Method** field is activated and displayed as drop-down list. If the **Network Protection Type** is **SNC-I**, the default is **ODUk Path Adaptation**, which is only displayed if all connection end points are on 1830 PSS OCS NEs or black boxes. If the **Network Protection Type** is **SNC-N**, the default is **ODU Path NIM Protection**; other **SNC-N** values include **TCM-1**, **TCM-2**, **TCM-3**, **TCM-4**, **TCM-5**, and **TCM-6**. If the **Network Protection Type** is **SNC-Nc**, only **ODU Path NIM Protection** is displayed.

Network Signal Degrade for Protection Switching

Optional: If ASON Routed is not selected and the Network Protection type is not **SNC-Nc**, the **Network Signal Degrade for Protection Switching** field is displayed as a drop-down list. Values are **Enable** (the default) or **Disable**.

Network Wait to Restore Time (min)

Optional: If ASON Routed is not selected and the Network Protection type is not **SNC-Nc**, the **Network Wait to Restore Time (min)** field is displayed as a drop-down list. Values are **1** to **15** minutes. The default is **5** minutes.

Network Revertive Mode

Optional: If ASON Routed is not selected and the Network Protection type is not **SNC-Nc**, the **Network Revertive Mode** field is displayed as a drop-down list. Values are **Enable** or **Disable** (the default).

<Managed Plane> Network Protection Type

Optional: If ASON Routed is selected, the **<Managed Plane> Network Protection Type** field is displayed a drop-down list. For SNC protection, the values are **SNC-I** (which is SNC protection with inherent monitoring and is only displayed if all connection endpoints are on an 1830 PSS OCS NE or black box), **SNC-N** (which is SNC protection for network ports). If all connection endpoints are on 11DPM8 circuit packs and black boxes, **SNC-Nc** is displayed. For other protection types, the value is **None**. If the user selects **None**, the remaining **SNC Protection** parameters are no longer displayed.

<Managed Plane> Network Hold Off Time (msec)

Optional: If ASON Routed is selected and the Network Protection type is not **SNC-Nc**, the **<Managed Plane> Network Hold Off Time (msec)** field is displayed as a drop-down list. Values are **0** (the default) to **100** in 20 msec increments and **100** to **10000** in 100 msec increments.

<Managed Plane> Network Protected Protection Method

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, a port on a Virtual Plane (which is a port with a slot identifier that is equal to 71), or a black box, and if ASON Routed is selected, the **<Managed Plane> Network Protected Protection Method** field is activated and displayed as drop-down list. If the **Network Protection Type** is **SNC-I**, the default is **ODUk Path Adaptation**, which is only displayed if all connection end points are on 1830 PSS OCS NEs or black boxes. If the **Network Protection Type** is **SNC-N**, the default

is **ODU Path NIM Protection**; other **SNC-N** values include **TCM-1, TCM-2, TCM-3, TCM-4, TCM-5, and TCM-6..** If the **<Managed Plane> Network Protection Type** is **SNC-Nc**, only **ODU Path NIM Protection** is displayed.

<Managed Plane> Network Protecting Protection Method

Optional: If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 pack, a 4AN400 pack, a port on a Virtual Plane (which is a port with a slot identifier that is equal to 71), or a black box, and if ASON Routed is selected, the **<Managed Plane> Network Protecting Protection Method** field is activated and displayed as drop-down list. If the **Network Protection Type** is **SNC-I**, the default is **ODUk Path Adaptation**, which is only displayed if all connection end points are on 1830 PSS OCS NEs or black boxes. If the **Network Protection Type** is **SNC-N**, the default is **ODU Path NIM Protection**; other **SNC-N** values include **TCM-1, TCM-2, TCM-3, TCM-4, TCM-5, and TCM-6..** If the **<Managed Plane> Network Protection Type** is **SNC-Nc**, only **ODU Path NIM Protection** is displayed.

<Managed Plane> Network Signal Degrade for Protection Switching

Optional: If ASON Routed is selected and the Network Protection type is not **SNC-Nc**, the **<Managed Plane> Network Signal Degrade for Protection Switching** field is displayed as a drop-down list. Values are **Enable** (the default) or **Disable**.

<Managed Plane> Network Wait to Restore Time (min)

Optional: If ASON Routed is selected and the Network Protection type is not **SNC-Nc**, the **<Managed Plane> Network Wait to Restore Time (min)** field is displayed as a drop-down list. Values are **1** to **15** minutes. The default is **5** minutes.

<Managed Plane> Network Revertive Mode

Optional: If ASON Routed is selected and the Network Protection type is not **SNC-Nc**, the **<Managed Plane> Network Revertive Mode** field is displayed as a drop-down list. Values are **Enable** or **Disable** (the default).

ASON Sub-Network Protection Type

Optional: If the **ASON Routed** field is selected and the **Connection Shape** is one of the supported **Bi** shapes, the **ASON Sub-Network Protection Type** field is activated and displayed as a drop-down list. Values are **None** or **SNCP-N** (the default).

Y-Cable Port

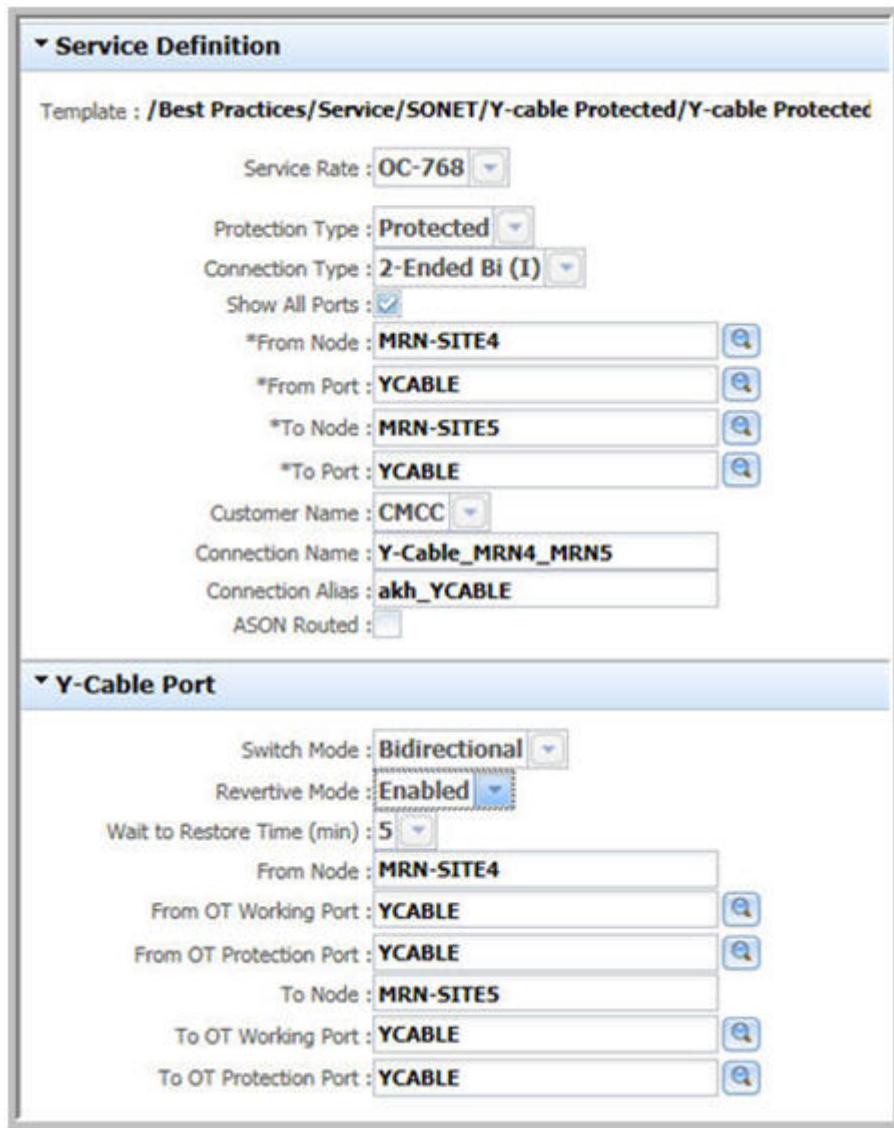
If the deployed template is a SONET or SDH Y-Cable protected template, the **Y-Cable Port** panel is displayed (above the **Advanced Settings** panel) after users select the From/To Node ports in the **Service Definition** panel.

The **Y-Cable Port** panel is used to specify the **Switch Mode** and from/to OT working and protection ports. Refer to the [4.4 “Y-Cable protection” \(p. 430\)](#) section for details regarding the feature, provisioning guidelines, and restrictions.

If Y-cable protection applies to **OCS** NEs, additional fields appears to provision **MDL** ports.

Connection Templates – Y-Cable Port Panel – SONET – WRT

Figure 7-20 Connection Templates – Y-Cable Port Panel – SONET – WRT



Switch Mode

The **Switch Mode** is a drop-down list. The values are **Unidirectional** (the default) or **Bidirectional**.

Revertive Mode

Optional: If the **Switch Mode** is **Bidirectional**, users can specify the **Revertive Mode**.

The **Revertive Mode** is a drop-down list. The values are **Enabled** (the default) or **Disabled**.

Wait to Restore Time (min)

Optional: If the **Revertive Mode** is **Enabled**, users can specify the **Wait to Restore Time (min)**.

The **Wait to Restore Time (min)** is a drop-down list. The numerical values represent the number of minutes, of which **5** minutes is the default.

Signal Degrade for Protection Switching

Optional: For all connection shapes, the **Signal Degrade for Protection Switching** field is displayed as a drop-down list. The values are **Disabled** (the default) or **Enabled**.

From/To Node

The **From Node** or the **To Node** field is an icon-activated field. The **From Node** is the node where the connection originates. The **To Node** is the node where the connection terminates.

For 2-ended connections, users must click the icon adjacent to the **From/To Node** field to display the NE selection window and they must select the first and only **From/To Node**. For 3-ended Y connections and for 4-ended X connections, users must click the icon adjacent to the **From/To Node** field to display the NE selection window and they must select the second **From/To Node**. The node name that the user selects in this field is the same node name that appears in the data table for the particular connection.

From/To OT Working Port

The **From OT Working Port** and/or **To OT Working Port** field is an icon-activated field. The **From OT Working Port** is the OT working port in which the connection is to originate. The **To OT Working Port** is the OT working port in which the connection is to terminate.

For 2-ended connections, users must click the icon adjacent to the **From/To OT Working Port** field to display the port selection window and they must select the first and only **From/To OT Working Port** that is listed and that is a known Y-cable port (**YCABLE**). For 3-ended Y connections and for 4-ended X connections, users must click the icon adjacent to the **From/To OT Working Port** field to display the port selection window and they must select the second **From/To Working Port** that is listed and that is a known Y-cable port.

From/To OT Protection Port

The **From OT Protection Port** and/or **To OT Protection Port** field is an icon-activated field. The **From OT Protection Port** is the OT protection port in which the connection is to originate. The **To OT Protection Port** is the OT protection port in which the connection is to terminate.

For 2-ended connections, users must click the icon adjacent to the **From/To OT Protection Port** field to display the port selection window and they must select the first and only **From/To OT Protection Port** that is listed and that is a known Y-cable port (**YCABLE**). For 3-ended Y connections and for 4-ended X connections, users must click the icon adjacent to the **From/To OT Protection Port** field to display the port selection window and they must select the second **From/To OT Protection Port** that is listed and that is a known Y-cable port.

Routing Constraints

The **Routing Constraints** panel is used to specify the parameters that control the routing of the connection.

Selecting one of the fields, the user leaves the system to assign the frequency to the selected connection or choose himself the frequency.

The following figure illustrates the default fields in the **Routing Constraints** panel.

The **Order Sensitive** field is applicable when the user selects **Manual Routing**. When the Order Sensitive field is checked, the system follows exactly the order of the selected link connections listed in the *Routing Constraint* table. The selection of the path through the network must be done in the transmission sequence. Loops in the route and duplicate link connections are also allowed if *Auto Server Creation* is unchecked and the servers are created separately. If an inter-shelf connectivity is present and Manual Routing is used, the **Order Sensitive** field must be selected.

The **Order Sensitive** must be flagged when the ODU0 link connection is included in the routing constraint panel during service provisioning. Selecting the field, the OS internal connections are included as routing constraint. The order sensitive applies only to L1 MP layer for ODU0 connections.

Selecting the **System Assigned Frequency** field, the frequency is automatically assigned by the system.

Description of the frequency allocation procedure is provided in the following chapter [24.5 “Quick Help – The OA&M Diagnostics Window” \(p. 1990\)](#)

Frequency

Important Considerations for Line Side OTU4x2 Connections on D5X500!

Because the line side of the D5X500 is an OTU4x2 connection, which is made up of two OTU4 connections, each OTU4 connection requires channel spacing of 62.5 GHz, instead of the typical 50 GHz. Consequently, the two channels on either side of the selected channel are unavailable for use. These unavailable channels, which are known as *adjacent channels*, cannot be used to support any other service. When selecting Routing Constraints, the system only displays spare Link Connections that have a spare or an *adjacent channel* on both sides of the displayed **Frequency**.

Important Considerations for HO-ODU4 Connections on 112SDX11Circuit Packs!

When you create an HO ODU4 connection that terminates on an 112SDX11 circuit pack, the system automatically creates the server OTU4 and four server OTU4/OTL4.4 connections. So when you select the route of the HO ODU4 connection, choose link connections or trails to constrain the OTU4/OTL4.4 connections. You will only have to select the route for the first server OTU4/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 OTU4/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 OTU4/OTL4.4, the route of the three remaining OTU4/OTL4.4 connections, which are L2, L3, and L4, is fixed.

In addition, for the 112SDX11 circuit pack, **Rearrange** is supported for the OTL4.4 connections, but not for the OTU4 connection. Endpoint change and frequency change are not supported for **Rearrange** of OTL4.4 connections.

Important Consideration for Physical Link Reuse in a Service Route

NFM-T supports reuse of an OTS link in a service connection having more than two nodes and trails. This can be done by configuring **Enforce Physical Link Diversity** parameter under **Routing Constraints**.

The **Enforce Physical Link Diversity** parameter is available on **Service Definition** provisioning. It includes Ethernet/Sonet/SDH/Data rate templates and transparent services.



Note: In case of Auto Routing, when **EnforcePhysicalLinkDiversity** flag is set to true, routing will always find a route with given user requests or constraints. In case of protection with no constraints, routing will find the service and protection segments that do not share the same physical connectivity. If it is unable to find a protected route, unprotected route would be found.

If the **Enforce Physical Link Diversity** parameter is disabled, the routing engine finds the shortest path to create a connection. If an alternate path is available with OTS reused, provide some constraints.

Table 7-8 Connection Templates – Advanced Settings – Routing Constraints - Actions

Parameter	Description
System Assigned Frequency	Check this box if you want the system to assign the frequency. If this box is not checked, the system prompts the user to choose if the desired frequency is DWDM or CWDM. Based on this selection, the field displays a drop down list of values to choose from
Enforce Physical Link Diversity	Check box for reusing the OTS link. By default, this field is enabled.
	Changes the service role that is assigned to a routing constraint.
	Changes the protection role that is assigned to a routing constraint.
	Removes the constraint.
<i>Column Descriptions</i>	
Type	Specifies the type.
Name	Specifies the name.
Select	Specifies the action, whether the action was Include or Exclude.

Table 7-8 Connection Templates – Advanced Settings – Routing Constraints - Actions
(continued)

Parameter	Description
Role	Specifies the Role, whether Service or Protection.
Frequency	Specifies the frequency.
Channel	Specifies the channel.

Note: The **Routing Constraints** panel can be used in conjunction with the **Planning Tool** tab that is displayed on the left pane of the window. The **Planning Tool** tab is only displayed if the NPT is part of the deployed solution for the user network. In addition, if NPT is part of the solution for the user network, the **Planning Tool** tab is only displayed during the creation of a connection; the **Planning Tool** tab is not displayed when users modify the route or the parameters of a connection.

The **Planning Tool** tab is only displayed if the Create Connection Planning Tool is set in the NFM-T preferences. See the Administer – Preferences section in the *NFM-T Administration Guide*.

Assurance

The **Assurance** panel is used to specify Alarm Management and Performance Monitoring (PM) parameters for the connection being deployed. The **Assurance** panel specifies alarm parameters and Link Utilization Profile parameters for the connection being deployed.

Alarm Profile

The **Alarm Profile** field is a drop-down list in the Alarm Management section of the panel. Values are **Use_NE_Values** (the default), **Enable Alarm Profile**, or **Disable all alarms**. **Use_NE_Values** does not allow the use of the ASAP feature; but, it does enable alarm reporting. The alarm severity values that are set on the NE prevail. **Enable alarm profile** sets the ASAP per port role and per layer rate, and alarm reporting is enabled. **Disable all alarms** sets the alarm severities to NR (Not Reported) on each port that is involved in the connection. To disable alarm reporting on a particular infrastructure connection or service for an 1830 PSS NE, select **Disable all alarms**.

Provisioning Considerations

- When users create an DSR connection and the system, in turn, automatically creates HO-ODUk/ODUk connection, the value that was selected for Alarm Profile applies for the DSR and HO-ODUk/ODUk connections.
- When users create an HO-ODUk service or infrastructure connection and the system, in turn, automatically creates OTUk connection(s), the value that was selected for Alarm Profile applies for the ODUk and OTUk connections.
- When users create an ODUk connection and the system, in turn, automatically creates OTU4x2 connection(s), the value that was selected for Alarm Profile applies for the ODUk and OTU4x2 connections.
- For the D5X500 circuit packs, when users create a DSR connection and the system automatically creates an ODU4 infrastructure connection, the value that was selected for Alarm Profile applies for the DSR and ODU4 connections. The Alarm Profile is set for the OTU4 ports on the D5X500 card as part of the setting Alarm Profile for the ODU4 connection. In addition, when users create an ODU4 connection, the Alarm Profile is set for the OTU4 ports on the D5X500 pack as part of the

setting Alarm Profile for the ODU4 connection.

- For the 2UC400 circuit pack, when users create an ODU4 connection and the system automatically creates an OTU4x2 infrastructure connection, the value that was selected for Alarm Profile applies for the DSR and OTU4x2 connections. The Alarm Profile is set for the OTU4 CTPs on the 2UC400 pack as part of the setting Alarm Profile for the ODU4 connection.
- For the 11SDX11 circuit pack, when the user creates an ODU4 connection and the system, in turn, automatically creates one OTU4 connection and four OTL4.4 connections, the value that was selected for Alarm Profile applies for the ODU4, OTU4 and OTL4.4 connections.

Link Utilization Profile

The **Link Utilization Profile** field sets the threshold profile for the link or infrastructure connection. This field defaults to **MEDIUM** and is not applicable for services.

Wave Key

The **Wave Key** panel is used to specify the Wave Key parameters for the connection.

The **Wave Key** panel is displayed depending on the template and connection type:

For infrastructure connections, if the selected connection is an:

- OTUk rate, the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs.
- OCH rate, the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs, or black boxes.
- ODUk rate, one or more connection endpoints is an HO-ODUk port, the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs.
- ODUk, one or more connection endpoints is a ODUk port on a 260SCX2 card, the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs.
- ODUk, one or more connection endpoints is a ODUk port on a D5X500 card, the **Provisionable Wave Key** field is set to **Keyed** and all connection endpoints are on 1830 PSS OCS, 1830 PSS, 1830 PSS-1, or 1830 PSS-4 NEs.
- ODUk, one or more connection endpoints is a ODUk port on a 1UD200 card, the **Provisionable Wave Key** field is set to **Keyed** and all connection endpoints are on 1830 PSS OCS, 1830 PSS, 1830 PSS-1, or 1830 PSS-4 NEs.
- ODUk rate, one or more connection endpoints is an ODUk port on a circuit packs that support a NNI client port rate that is equal to the line port rate (11STAR1, 11STAR1A, 43STA1P, 43SCA1, 11QPA4, 11QPEN4, 112SCA1, 112SNA1 and 130SCA1), the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs.

For services, if the selected service connection is an:

- OCH rate, the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs, or black boxes.
- ODUk rate, one or more connection endpoints is an HO-ODUk port, the **Provisionable Wave**

Key field is **Keyed**, and all connection end points are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs, or black boxes.

- ODUk rate, one or more connection endpoints is an ODUk port on a circuit packs that support a NNI client port rate that is equal to the line port rate (11STAR1, 11STAR1A, 43STA1P, 43SCA1, 11QPA4, 11QPEN4, 112SCA1, 112SNA1 and 130SCA1), the **Provisionable Wave Key** field is **Keyed**, and all connection endpoints are on 1830 PSS NEs, 1830 PSS OCS NEs, 1830 PSS-1 NEs, 1830 PSS-4 NEs, or black boxes.

Important! Connections with 1830 PSS NEs must use **Automatic** Wave Key Provisioning or **Manual** Wave Key Provisioning.

Wave Key Type

The **Wave Key Type** field is a drop-down list. For connections or services that support a **Provisionable Wave Key** that is **Keyed**, two types of Wave Key assignments are supported, which are **Automatic** (the default) or **Manual**.

When a **Keyed** connection uses **Automatic** Wave Key assignment, users do not have to be aware of current Wave Key usage in the network because the NE automatically assigns the Wave Key pairs. The NFM-T OTN uses **Automatic** Wave Key assignment whenever possible. When a **Keyed** connection uses the **Manual** Wave Key assignment, users must select the Wave Key pairs, which means that users must be aware of the current Wave Key usage in the network to avoid Wave Key collisions. Users must be aware of the Wave Key pairs that are assigned by both **Manual** and **Automatic** Wave Key assignments since a single pool of Wave Key pairs is used by both **Manual** and **Automatic** assignments.

For Transparent Alien Wavelength (unkeyed OCH) services, by default, the **Provisionable Wave Key** is set as **UnKeyed**, and **Wave Key Type** is set as **N/A**.

AZ Wave Keying Preference and ZA Wave Keying Preference

The **AZ Wave Keying Preference** (from/to preference) and the **ZA Wave Keying Preference** (to/from preference) fields are drop-down lists. Values are **None** (the default), **Duplicates Allowed**, or **No Duplicates Allowed**, which is only displayed if the Wave Key Type is **Automatic**.

None means that wave keys are to be assigned for the connection based on the current value of frequency level locking. (A frequency can be locked or unlocked for the reuse of wave keys. Initially, all frequencies are locked. *Locked* means that all wave keys must be unique within the domain. *Unlocked* means that wave keys can be reused within the domain.)

Duplicates Allowed means that the reuse of wave keys is allowed for the connection and the frequency level value is unlocked.

No Duplicates Allowed means that the connection must have unique wave keys regardless of the current state of frequency level locking.

Wave Key Assignment

If the **Wave Key Type** is **Manual**, the **Wave Key Assignment** field is activated. The **Wave Key Assignment** field is a drop-down list. Values are **User Selected** and **System Assigned**, which is not displayed if **AZ Wave Keying Preference** or **ZA Wave Keying Preference** is set to **Duplicates Allowed**. If **User Selected** is selected, users must select the exact Wave Key pairs that are assigned to the connection. For **Automatic** routing, users must choose the Lambda (frequency)

before selecting the Wave Key pairs. For **Manual** routing, users must choose at least one link connection before selecting the Wave Key pairs because valid Wave Key pairs are based on the frequency of the connection. If **System Assigned** is selected, users are allowing the **NFM-T** system to choose the Wave Key pairs that are to be assigned to the connection.

Note:

The NFM-T assigns a Wave Key pair that is unique across the network, regardless of the selection of the AZ/ZA Wave Keying Preference fields.

AZ Wave Key Pair and ZA Wave Key Pair

The **AZ Wave Key Pair** (the from/to pair) and **ZA Wave Key Pair** (the to/from pair) fields are text fields. Enter a numeric value from 9170 to 9605 in increments of 5 (for example: 9170, 9175, 9180, 9185, ...9600, 9605). If users selected the **Wave Key Assignment** to be **User Selected**, the **AZ Wave Key Pair** and **ZA Wave Key Pair** must be entered.

Typically, Wave Key value pairs that have a zero Tone Overlap are the most desirable, followed by pairs that have a one Tone Overlap, and lastly pairs that have two Tone Overlaps; except, pairs that have the values of 181, 795, 706, 1230, 1754 and 3753 should always be used last because these pairs contain a tone that falls near a SONET/SDH frequency harmonic.

Important notes:

The **AZ Wave Key Pair** and **ZA Wave Key Pair** fields are not displayed for OTU4 and OTL4.4 connections on 112SDX11 circuit packs.

For manual wave key provisioning of connections with 112SDX11 endpoints, four pairs of wave keys are required. For the 112SDX11 pack, the OTU4 connection has four server OTL4.4 connections each with a distinct frequency. One wave key pair is required for each frequency. The **Frequency 1/2/3/4 AZ/ZA Wave Key Pair** fields must be used instead of the **AZ Wave Key Pair** and **ZA Wave Key Pair**.

For manual wave key provisioning of connections on 112SDX11 circuit pack, when the signal type of the PTP containing the endpoints is OTL4.4, for each OTL4.4 connection an **AZ Wave Key 1** and **AZ Wave Key 2** wave key pair and a **ZA Wave Key 1** and **ZA Wave Key 2** wave key pair must be generated.

Frequency 1/2/3/4

The Frequency 1, Frequency 2, Frequency 3, and Frequency 4 fields are read-only fields that are displayed when one or more connection endpoints is on a 112SDX11 circuit pack, the connection that is being created is an OTU4, the signal type of the PTP containing the endpoint is OTL4.4, and the **Wave Key Assignment** field is **User Selected**.

The following conditions determine the read-only population of the Frequency 1, Frequency 2, Frequency 3, and Frequency 4 fields:

- If the **Routing** field in the Connection Controls panel is set to **Automatic**, and a value has been selected for the **Constrain to this Lambda** field, the selected value is populated in the **Frequency 1** field.
- If the **Routing** field in the Connection Controls panel is set to **Automatic**, and a value has not been selected for the **Constrain to this Lambda** field, the Frequency 2, Frequency 3, and Frequency 4 fields are blank.

- If the **Routing** field in the Connection Controls panel is set to **Manual**, the frequency of the link connection that is selected in the Routing Constraints panel is populated in the **Frequency 1** field.
- If the **Routing** field in the Connection Controls panel is set to **Manual** and the frequency of the connection cannot be determined (for example, the routing information has not been completed on the Routing Constraints Panel or the link connections that have been selected as Routing Constraints have more than one frequency), the Frequency 2, Frequency 3, and Frequency 4 fields are blank.
- If the frequency of the connection is not in the range of 9170 to 9575 in increments of 5 (for example, 9170, 9175, 9180...9570, 9575), the Frequency 2, Frequency 3, and Frequency 4 fields are blank.

The values for the Frequency 2, Frequency 3, and Frequency 4 fields are derived according to the following:

- Frequency 2 = Frequency 1 +10
- Frequency 3 = Frequency 1 +20
- Frequency 4 = Frequency 1 +30

Frequency 1/2/3/4 AZ/ZA Wave Key Pair

The Frequency 1 AZ/ZA Wave Key Pair, the Frequency 1 AZ/ZA Wave Key Pair, Frequency 1 AZ/ZA Wave Key Pair, and Frequency 1 AZ/ZA Wave Key Pair fields are displayed when one or more connection endpoints is on a 112SDX11 circuit pack, the connection that is being created is an OTU4, the signal type of the PTP containing the endpoint is OTL4.4, and the **Wave Key Type** is **Manual** and the **Wave Key Assignment** is **User Selected**.

Typically, Wave Key value pairs that have a zero Tone Overlap are the most desirable, followed by pairs that have a one Tone Overlap, and lastly pairs that have two Tone Overlaps; except, pairs that have the values of 181, 795, 706, 1230, 1754 and 3753 should always be used last because these pairs contain a tone that falls near a SONET/SDH frequency harmonic.

7.6 Routing Constraints

Introduction

Routing Constraints allow users to specify the route to be taken for the connection that is to be created in the network. The Routing Constraints tab is used in conjunction with the Routing Constraints panel of the Create Connection window.

When users create either an infrastructure or a service connection, they can provide a suggestion to the system on how to route the connection. The system takes into account the user's specific suggestion while it considers the hardware configuration, internal NE topology, and the available capacity to route the connection.

Users can do any of the following to institute routing constraints:

- Users can select **Include Trails/Links**, which refers to infrastructure connections (**Trails**) or logical links (**Links**) for the creation of L1 connections.
Users can specify specific trails for setting up the intermediate cross-connects. The system aids the user by displaying trails that have the ability to carry the connection that is being created.
Users can specify the connectivity to be full end-to-end-connectivity or they can partially specify the connectivity and let the system choose the remaining parts.
When users specify more links than are needed to establish the connectivity, the system discards the additional links. The system picks up any available frequency or time slot on the selected links.
When users specify more trails, the system doesn't discard additional trails, instead it validates them and gives a failure message.
- Users can select **Include Physical Links** or **Exclude Physical Links**. This constraint enables users to suggest which OTS to select for L0 Control Plane connections and logical links/tunnels for L1 Control Plane connections.
Refer to "[Physical connections as a constraint for routing](#)" (p. 733) for details.
- Users can select **Exclude Trails/Links**, which enables them to indicate which trails and links the system should avoid picking as a resource while routing.
- Users can select **Include Node** or **Exclude Node**. When specifying the **Include Node** constraint, the system attempts to route the connection by using any ingress/egress trail/link available that is on the node.
When specifying the **Exclude Node** constraint, the system ensures that no immediate server is available on the excluded node.
Refer to "[Nodes as a constraint for routing traffic](#)" (p. 732) for details.
- Users can select **Include 3R** and specify which 3R ports the system should select to regenerate the signal when they need to create a long span ODUk infrastructure that requires regeneration.

The table below depicts the types of Routing Constraints and the support on Managed Plane, Control Plane, and Mixed Plane connections.

Table 7-9 Connection creation support

Constraint Type	Managed Plane	Control Plane	Mixed Plane
Trail/Link Constraint	√	√	√
3R Constraint	√	√	√
Node Constraint	√***	√	√*
Physical Link Constraint	√***	√	√**

i Note:

- * The scope of node constraints is only within ASON domain. Trail constraints to be added as support for non ASON domain in the connection.
- ** The scope of physical link constraints is only within ASON domain. Trail constraints to be added as support for non ASON domain in the connection.
- *** In case of Auto Routing user can assign Node and Physical Connection constraints in Managed Plane. For Managed plane, node and physical link constraints are supported because, by default in the NFM-T GUI, routing mode is set as *automatic*, so, Node based and Physical link based constraints can be used.
 - The Node Constraint and Physical Link Constraint options are only displayed on the management system when the user selects the ASON Routed check box in the Service Definition panel.
 - Manual routing mode implies that user fully specifies the connectivity, user must specify all the trail or Link connection Connectives. For this reason Node and Physical Link constraint is not supported for ASON connection provision with manual routing mode.

Table 7-10 Connection modification support

Constraint Type	Managed Plane	Control Plane	Mixed Plane
Trail Constraint	x	x	x
Link (LC) Constraint	√	√	√
3R Constraint	√	√	√
Node Constraint	x	x	x
Physical Link Constraint	x	x	x

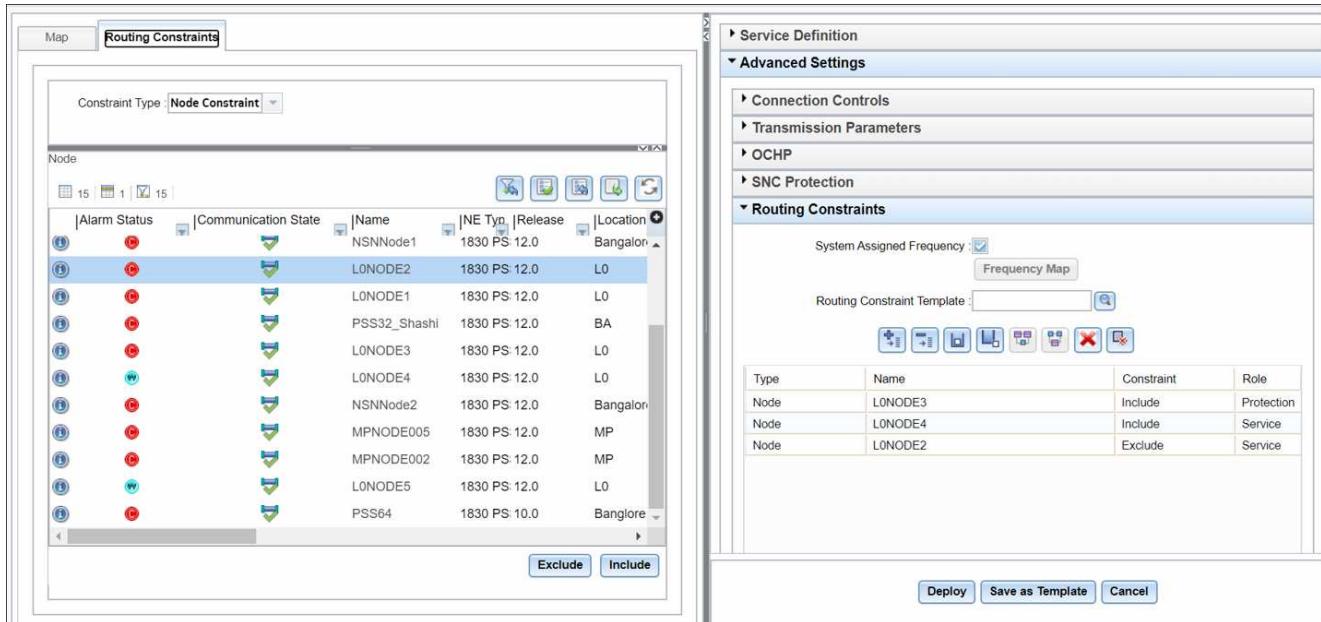
Nodes as a constraint for routing traffic

Users can include or exclude a node as constraint for routing traffic for L1 and L0 Managed, Control or Mixed Plane connections when they are provisioning a new connection from the **Map** part of the Create Connection window or from the **Routing Constraints** tab.

Include > Service or Protection, to add the node as a constraint for the service or protection.

Exclude > Service or Protection, to add the node as a constraint for the service or protection.

Figure 7-21 Connection templates – create connection window - Routing Constraints tab



Include Node Behavior: the routing algorithm attempts to use all included nodes in the user provided list, in the same role (Service or Protection) to find a route from the end points of the user request.

Exclude Node Behavior: the Exclude constraints has the highest priority. The system excludes the selected Node in the specified role (Service or Protection) or in both Service and protection completely. The node is excluded across all layers.

Physical connections as a constraint for routing

The user can specify which links to include or exclude while creating a connection, the goal is to design a route to take even if it is a longer route, the reason is to balance the traffic or to avoid specific risk areas.

Users can include or exclude physical connections as constraint for routing traffic for L1 and L0 Control, managed or mixed Plane connections when they are provisioning a new connection from the **Routing Constraints** tab.

From the map the user can select the physical connection, click on it and a window is displayed with the selected physical connection. Use the **Include** button to add the selected physical connection as included in the constraint table. Use the **Exclude** button to add the selected physical connection as Excluded in the constraint table.

The user selects a Node or type in a node name to filter the list of physical links.

When the user selects the Node from the drop-down list, the table below shows the list of physical connections that can be included or excluded, to include or exclude the selected physical

connection, click on the **Include** or **Exclude** button. The selected physical connections are listed in the Routing Constraints panel on the right of the window.

Include Link behavior: when a user selects a Physical link, the system gets all clients of that link that can serve as a server of the connection being provisioned. These can be loaded into the graph for route computation and these are weighted to be included.

Exclude Link Behavior: the Exclude link has priority over all includes. All trails that could be servers of the requested connections are excluded from the graph and the route computed.

Trail/Link or 3R as constraint

When a Trail is selected as an include constraint then all of the connections that are built using that constraint will ride on channels over that trail (infrastructure connection).

Note: It is not expected that the user uses logical links in a template since this is useful for only one connection. Only one connection can use a logical link at a time. The user can setup this type of template but it is only useful for one connection at a time. Refer also “[Creation of 3R object needs particular sequence to be stored in OTN DB](#)” (p. 2436) for 3R information.

1. To select an Infrastructure Trail, click the plus icon and expand the **Best Practices > Infrastructure Trail** folder or **Published > Infrastructure Trail** folder. Select an infrastructure from any of the sub folders.

-or-

To select a service, click the plus icon and expand the **Best Practices > Service** folder or **Published > Service** folder. Select a service from any of the sub folders.

2. Select an Infrastructure Trail or a service from any one of the available folders.

3. In the right side of the window, right click the selected trail or service and click **Deploy**.

-or-

Select a trail or service and click the **Deploy** icon.

When users select the constraint type to be a **Trail/Link Constraint**, the system then displays the Infrastructure Connections data table.

The system guides the user on the selection of trails from the list.

If the user has provided a **From Node** and a **To Node** in the **Service Definition** panel, then the first node that is populated in the **Current Node** is the **From Node**. The infrastructure trails that are displayed in the list then become the list of eligible trails egressing to support the connection. The first column is the far-end node, which allows the user to make a decision on which egress trail to select. Once that node is selected and included or excluded, the far-end is now the **Current Node**. The infrastructure trails that are then displayed are those egressing that node. In this manner, the user can navigate the network and go from the **From Node** towards the **To Node**.

When users select the constraint type to be a **Trail/Link Constraint**, the system then displays the Infrastructure Connections data table.

From the Infrastructure Connection list data table, users can select a connection or a 3R pair port that is to be used as a routing constraint and click on **Include** or **Exclude**. The system then populates the data table in the **Routing Constraints** panel with the selected connection. Multiple routing constraint entries are allowed.

Users can select a 3R port while they are creating the photonic infrastructure. When selecting the 3R port, users can then indicate whether the port should be in the working or in the protection part of the route by clicking on the **Change Role to Service** or **Change Role to Protection** icon.

To delete a routing constraint from the data table in the **Routing Constraints** panel, users can select the constraint to be deleted and click on the red **X**. The system deletes the routing constraint from the data table.

To deploy a connection, click **Deploy** or **Save as Template**

The system displays the **Provision Task Status** window.

Task	Description
Show Failure Analysis	The system displays the failure analysis with cause of failure and corrective action in a new tab.
More	The button displays the extra information of the window.
Close	Click this tab to close the window
Show Run History	Click this tab to display the Run History Window

i **Note:** *10GbE provisioning with an ODU2E container:* In some cases during the selection of Link Connections from the Routing Constraints window, the Effective Rate for some of the link connections are shown as ODU2 rather than ODU2e. It depends on the selected service pack, some service packs utilize secondary parameters, such as Encapsulation Mode, TP Effective Rate or Provisioned Bit Rate, to adjust the bandwidth that can be carried. 130SCX10 is an example. NFM-T displays the correct link connections that can support the ODU2e rate during provisioning. It should be noted that once the 10GbE service has been set up, then the server is marked with an ODU2E rate in the 360 degree server list panel of the connection.

Routing Constraint Template

The **Routing Constraint Templates** are saved from the deploy window during connection creation.

In the left panel when configuring the Routing Constraint the user can select a Routing Constraint Template. See "[Component Templates](#)" (p. 771)

Click on the Search icon near the Routing Constraint Template field. A list of the templates is displayed and the user can select the desired one, consequently the routing constraints field are filled.

Once the user selects one of the templates, the template name is inserted and the details of the template are displayed in the Routing Constraints panel. The user can change, add or delete, any of the imported routing constraints. The user can also add any additional routing constraints to the list.

The user can also select multiple Routing Constraint Templates for a single connection.

Save Routing Constraint as Template

From the Deploy page on the Routing Constraint panel the user can save the inserted constraint as a template. A button **Save Routing Constraint** is displayed on the panel, click the button to save the template.

The Save as RC Template window is displayed. Insert a **Template Name** for the template and a description. Click **OK** or **Apply** button to save the template.

To modify an existing Routing Constraint Template use the procedure “[Task: Modify Routing Constraints](#)” (p. 774)

ASON routing constraints

This part summarizes some hints for users regarding the ASON routing constraint management.

Control plane allocation is the third phase of provisioning for an ASON routed connection. In this phase the system calculates routing inside ASON network and stores it in the database. In order to force routing algorithm to choose a route that is not the cheapest one according to the network description, the user is allowed to add routing constraints.

There are several types of constraints. In theory all these constraints have the same effect, but practically applied this concept is not true. For example, there are some particular constraints that can lead routing algorithm to be very slow as they increase route search computation complexity.

Some hints are listed to help the user choosing the set of constraints that allows finding the desired routing without affecting routing algorithm performances.

General rules:

- Unconstrained routing finds the cheapest routing according to network description: in general it is fast even in big and complex networks.
- Constraints **don't use** on nodes or physical links are always convenient as they reduce network complexity.
- Constraints on objects that are far from endpoints affects performance. For example, a connection from New York to Boston: if the user wants to use a link between Rio De Janeiro and Buenos Aires as constraint and the network is big, this implies that before satisfying constraint routing must perform many other iterations as there are several other short routes (for example: inside USA, North America, although none of these is satisfying the specified constraint). In case this routing is required, it is better to add other constraint in order to use additional resources or even better add **don't use** constraints so that some routes are blocked in advance.

Performance towards selected constraint object:

- *Trail/link connection/3Rs constraints*: are the most effective constraints, as routing takes advantage using the specified object. Only **use** mode is supported.
- *Physical connection constraints*: a type of constraint that is helping route to be quick. Pay attention that sometimes (L1 networks) ASON is not aware of the relation between logical and physical resource, in this case the constraint cannot be satisfied. **use** and **don't use** mode is supported.
- *Node*: it is easiest constraint object, but when nodes are given as constraint, the routing complexity is increased, unless **don't use** is selected. It is suggested to select node constraints in small networks, or in combination with trail/link connection constraints or when the purpose is to **don't use** it .

Hints to speed up ASON routing performances:

- Prefer trail/link connection constraint

-
- Use nodes in combination with trail/link connections or when **don't use** is required
 - Be careful in object selection to avoid providing constraints that can never be satisfied, in this case they force the creation of unsupported connectivity, forbidden due to hardware restrictions or not supported by GMRE, for example segment protection inside ASON NPA.

7.7 Access and view a connection template

When to use

Use this task to access and view a connection template.

Related information

See the following topics in this document:

- [7.3 “Field descriptions for Best Practices templates” \(p. 675\)](#)
- [7.4 “Service definition field descriptions for deploy Best Practices templates” \(p. 688\)](#)
- [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#)

Before you begin

The connection template is for an infrastructure connection (which is a trail or logical link) or a service (which is a path).

The template to be accessed and viewed can be any template that resides in the **Best Practices**, **My Templates**, or **Published** folders.

Optionally, this task provides you with steps on how to access and view the details of any template that resides in the **Best Practices**, **My Templates**, or **Published** folders.

- You can view connection-related details for templates that you access from the **DESIGN >** and **DEPLOY >** navigation paths, which is explained in [Step 5](#).
- You can access and view template-related details for templates that you access from the **DESIGN >** navigation path, which is explained in [Step 4](#).

Task

Complete the following steps to access and view a connection template.

1

From the NFM-T GUI, follow one of these navigation paths:

DESIGN > Service/Infrastructure Template

Result: In the left portion of the displayed window, the system displays a tree with the **Best Practices**, **My Templates**, and **Published** folders. In the right portion of the displayed window, the system displays a data table that lists the templates belonging to the first folder in the left tree.

Figure 7-22 Connection templates – deployed – initial default view

Folder	Name	Owner	Last Modified
/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel Uplink	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel with LO Restoration	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/Unprotected	OTUk with PSI2T 100GbELAN	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/Unprotected	ODUk with PSI2T OTN100GbE	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/Unprotected	ODUk for L Band	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/OCHP Protected	ODUk	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/OCHP Protected	ODUk with LO Restoration	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/OCHP Protected	Alien Wavelength (OCH)	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/SNC-N Protected	SNC-N Protected Uplink ODUk	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/SNC-N Protected	SNC-N Protected Uplink ODUk with LO Restorat...	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/SNC-I Protected	SNC-I Protected Uplink ODUk	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/SNC-I Protected	SNC-I Protected Uplink ODUk with LO Restoration	system	3/24/2021 7:12:14 PM
/Best Practices/Infrastructure Trail/OMS Protected	OMS	system	3/24/2021 7:12:14 PM

2

In the tree, click the drop-down to expand the tree and drill down to locate the template in the **Best Practices**, **My Templates**, or **Published** folders to access and view.

3

In the tree, select the template to access and view.

Result: Depending on your selection, the system displays the data table for the template. When designing a template (**DESIGN >**), the data table for the connection includes an **i** icon for **Additional Attributes** regarding the template itself and two sets of icons that provide counts of the selected object (on the left) and are used to perform actions on the template (on the right). When deploying a template (**DEPLOY >**), the data table does not include the **i** icon or the set of icons.

Figure 7-23 Connection templates – data table – Best Practices template – DESIGN >

Folder	Name	Owner	Last Modified
/Best Practices/Infrastructure Trail/Unprotected	ODUk or OTSIG Tunnel	system	3/24/2021 7:12:14 PM

4

Optional: When designing a template (**DESIGN >**), click the **i** icon for **Additional Information** regarding the template itself.

Result: The system displays the Additional Attributes window, which provides details regarding the template itself (and not the connection).

5

Optional: Click the **More**  icon at the right end of corresponding template, and then click **Details**.

Result: The following parameters corresponding to the template appears:

The following example illustrates the abbreviated details of a Best Practices template for an unprotected ODUk infrastructure trail.

Figure 7-24 Connection template - details

	GENERAL	PROTECTION	CONNECTION	TRANSMISSION PARAMETERS	ASSURANCE	ASON
Folder	/Best Practices/Infrastructure Trail/Unpro...					
Template Name	ODUk or OTSIG Tunnel					
Owner	system					
Template Type	Connection					
Published	<input checked="" type="checkbox"/>					
Description						

END OF STEPS

7.8 Design and publish a template for a connection

When to use

Use this task to design and publish a template for an infrastructure connection or service.

Related information

See the following topics in this document:

- [7.3 “Field descriptions for Best Practices templates” \(p. 675\)](#)
- [7.4 “Service definition field descriptions for deploy Best Practices templates” \(p. 688\)](#)
- [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#)

Before you begin

The connection template is for an infrastructure connection (which is a trail or logical link) or a service (which is a path).

Task

Complete the following steps to save a connection template.

1

From the NFM-T GUI, follow this navigation path:

DESIGN > Service/Infrastructure Template

Result: In the left portion of the displayed window, the system displays a tree with the **Best Practices**, **My Templates**, and **Published** folders.

2

Click the drop-down menu to expand the tree and drill down to locate the particular template in the **Best Practices**, **My Templates**, or **Published** folders.

3

Click the **More**  icon at the right end of corresponding template, and then click **Save As**.

Result: The parameters corresponding to the template appear in tabs on top of the screen.

Figure 7-25 Connection template - Save As

	GENERAL	PROTECTION	CONNECTION	TRANSMISSION PARAMETERS	ASSURANCE	ASON
Folder	/My Templates					
Template Name	ODUk or OTSiG					
Owner	user					
Template Type	Connection					
Description						

RESET OK

4

Select the parameter where you want to make changes.

Result: The fields associated with the selected parameter appears.

Figure 7-26 Connection templates – Template Name

GENERAL	
Folder	/My Templates
Template Name	ODUk or OTSiG Tunne
Owner	user
Template Type	Connection
Description	

Example: In this example, the fields associated with **GENERAL** parameter is explained.

5

To name or rename the template, in the **Name** field, enter a name for the template.

6

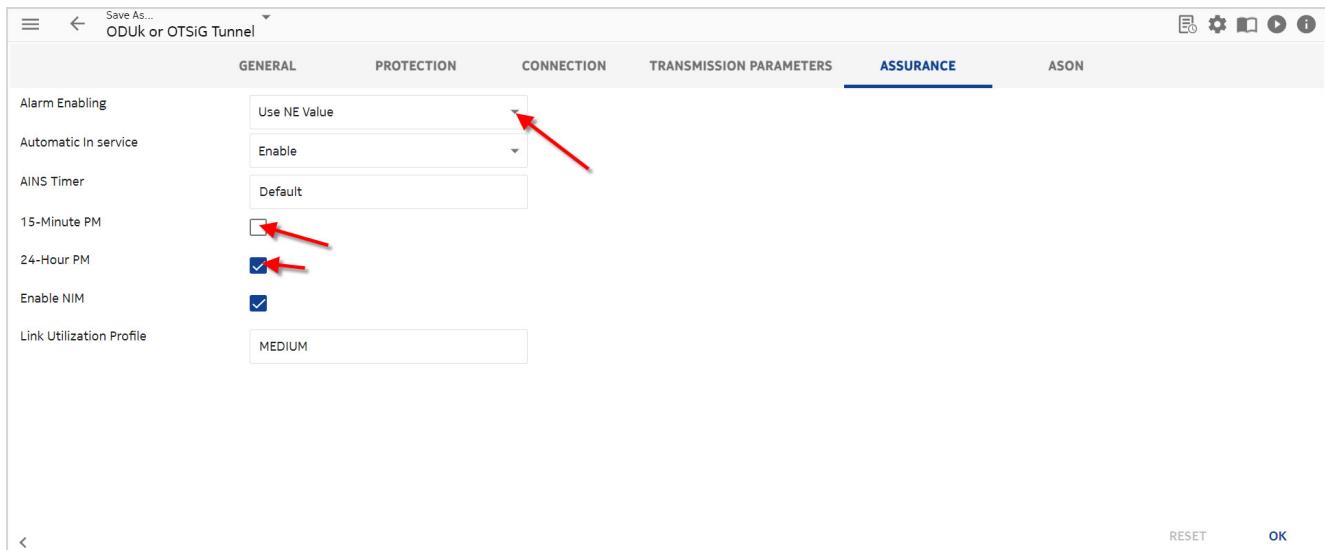
In the **Description** field, enter any information that can further describe the template that you are creating.

7

Select the **ASSURANCE** tab parameter.

Example: The following figure illustrates two changes that have been made in the **Assurance** panel. The Alarm Profile and 24 minute PM data collection have been enabled by default. The 15 minute PM is disabled by default. User can enable it.

Figure 7-27 Connection templates – modify the FM and PM settings in the Assurance panel



Note: PM is not supported on logical link for D5X500.

8

Click **OK** option at the right-bottom of the screen to confirm the changes.

Result: The changes appear in the parameters.

9

Click **RESET** to cancel the changes.

Result: The fields in the parameters are reset with the previous values.

10

Optional/Hint: If the template is not visible in the directory that you selected, refresh the browser page or open a new browser window.

END OF STEPS

7.9 Modify a template for a connection

When to use

Use this task to modify a template for an infrastructure connection or service connection.

Related information

See the following topics in this document:

- [2.6 “Provision a NFM-T OTN network” \(p. 160\)](#)
- [2.8 “Determine the Infrastructure to be created” \(p. 168\)](#)
- [7.3 “Field descriptions for Best Practices templates” \(p. 675\)](#)
- [7.4 “Service definition field descriptions for deploy Best Practices templates” \(p. 688\)](#)
- [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#)

Before you begin

To modify a connection template, the following guidelines apply:

- Published templates in the **DESIGN > Best Practices** folder, where the owner is **system**, cannot be modified.
- Unpublished templates, in **DESIGN >**, where the owner is **user**, can be modified.
Published templates, in **DESIGN >**, where the owner is **user**, can be modified. To modify a published template in **DESIGN >**, where the owner is **user**, the template has to first be unpublished. Refer to the [7.10 “Publish/Unpublish a connection template” \(p. 748\)](#) task for details.
- If NPT is part of the solution for the user network, the **Planning Tool** tab is only displayed during the creation of a connection; the **Planning Tool** tab is not displayed when users modify the route or the parameters of a connection.
The **Planning Tool** tab is only displayed if the Create Connection Planning Tool is set in the NFM-T preferences. See the Administer – Preferences section in the *NFM-T Administration Guide*.

Detailed explanations of the template fields are provided in [7.3 “Field descriptions for Best Practices templates” \(p. 675\)](#), [7.4 “Service definition field descriptions for deploy Best Practices templates” \(p. 688\)](#), and [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#).

Task

Complete the following steps to modify a template for an infrastructure connection or service connection.

1

From the NFM-T GUI, follow one of these navigation paths:

DESIGN > Service/Infrastructure Template

Result: Depending on your selection, the system displays the corresponding window. In the left portion of the window, the system displays a tree that shows the available folders, that includes the **Best Practices**, **My Templates**, and **Published** folders.

2

Click the drop-down menu to expand the tree and drill down to locate the particular template in the folder.

3

Click the **More**  icon at the right end of corresponding template, and then click **Save As**.

Result: The parameters corresponding to the template appear in tabs on top of the screen.

4

Select the parameter in which you want to make changes.

Result: The fields associated with the selected parameter appears.

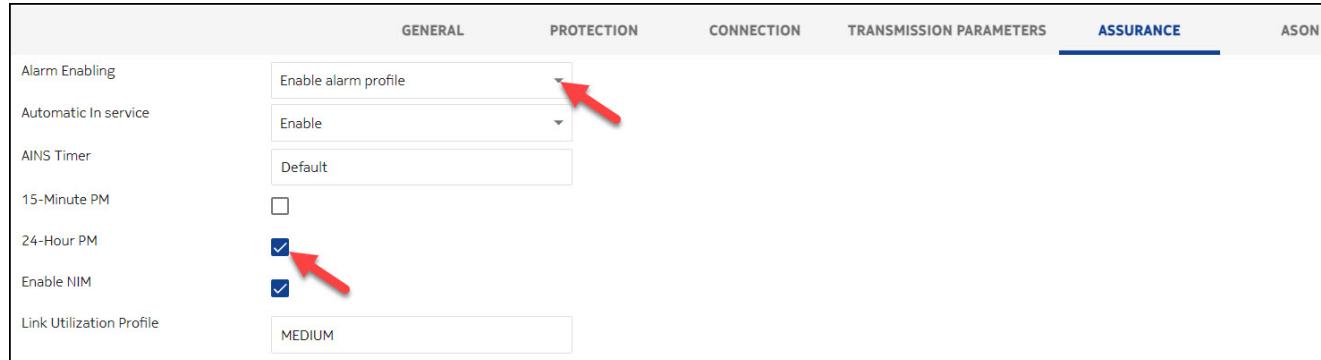
5

Change any of the values in the displayed fields. For an explanation of the fields that are displayed, refer to 7.3 “Field descriptions for Best Practices templates” (p. 675), 7.4 “Service definition field descriptions for deploy Best Practices templates” (p. 688), and 7.5 “Advanced Settings field descriptions for deploy Best Practices templates” (p. 708).

Example: The following figure illustrates the changes that have been made in the **Assurance** panel. The Alarm Enabling, 24-Hour PM data collection, and Enable NIM have been enabled.

 **Note:** The Enable NIM value in the Deploy screen is based on the setting on the template, either 15-Minute PM or 24-Hour PM. Either one of the granularity 15-Minute PM or 24-Hour PM should be checked for the **Enable NIM** field to be enabled/activated. If both 15-Minute PM and 24-Hour PM are unchecked, then **Enable NIM** field is disabled. For a detailed information on NIM, refer 7.57 “Manage NIM for a connection” (p. 954).

Figure 7-28 Connection templates – modify the FM and PM settings in the Assurance panel





Note: PM is not supported on logical link for D5X500.

6

Click **OK** option at the right-bottom of the screen to confirm the changes.

Result: The changes appear in the parameters.

7

Click **RESET** to cancel the changes.

Result: The fields in the parameters are reset with the previous values.

END OF STEPS

7.10 Publish/Unpublish a connection template

Purpose

Use this task to publish or unpublish a template for an infrastructure connection or service connection.

Published **Best Practices** templates that are located in the **DESIGN >** areas, where the owner is **system**, cannot be unpublished.

Task: Publish a Connection Template

Complete the following steps to publish a template for an infrastructure connection or service connection.

1

From the NFM-T GUI, follow one of these navigation paths:

DESIGN > Service/Infrastructure Template

Result: Depending on your selection, the system displays the corresponding window. In the left portion of the window, the system displays a tree that shows the available folders, that includes **Best Practices**, **My Templates**, and **Published** folders.

2

Click the drop-down menu to expand the tree and drill down to locate the particular template in the folder.

3

Click the **More**  icon at the right end of corresponding template, and then click **Publish To**.

Result: The published template appears under published folder.

END OF STEPS

Task: Unpublish a connection template

Complete the following steps to unpublish a template for an infrastructure connection or service connection.

1

From the NFM-T GUI, follow this navigation path:

DESIGN > Service/Infrastructure Template

Result: The system displays the design window. In the left portion of the window, the system displays a tree that shows the available folders, that includes the **Best Practices**, **My Templates**, and **Published** folders.

-
- 2** _____
Click the plus signs to expand the tree and drill down to locate the particular template in the folder.
- 3** _____
In the tree, click on the particular published template that you want unpublish.
- 4** _____
Click the **More**  icon at the right end of corresponding template, and then click **Unpublish**.
- Result:** The unpublished template is removed under published folder.

END OF STEPS _____

7.11 Copy an existing template or delete a template

Purpose

Use this task to copy an existing or to delete a template.

The template to be copied can only reside in the **My Templates** or **Published** folders. Only a template that has been copied to the **My Templates** or **Published** folders are deleted.

A template cannot be added to or deleted from the **Best Practices** folder.

Before a template is deleted, it must be Unpublished. Refer to “[Task: Unpublish a connection template](#)” (p. 748) for detailed steps.

Task: Copy an existing template

Complete the following steps to copy an existing template.

1

From the NFM-T GUI, follow this navigation path:

DESIGN > Service/Infrastructure Template

Result: In the left portion of the design window, the system displays a tree with the **Best Practices**, **My Templates**, and **Published** folders.

2

In the tree, locate and select template to be copied in the **Best Practices**, **My Templates**, or **Published** folder.

Result: The system displays the template in data table format in the right pane of the window.

3

Click the **More**  icon at the right end of corresponding template, and then click **Save As**.

Result: The parameters corresponding to the template appear in tabs on top of the screen.

Figure 7-29 Connection template - Save As

The screenshot shows the 'Connection template - Save As' dialog box. At the top, there are tabs: GENERAL (which is selected), PROTECTION, CONNECTION, TRANSMISSION PARAMETERS, ASSURANCE, and ASON. Below the tabs, there are five input fields:

Folder	/My Templates
Template Name	ODUK or OTSiG
Owner	user
Template Type	Connection
Description	(empty)

At the bottom right of the dialog box are two buttons: 'RESET' and 'OK'.

4

Select the **GENERAL** tab.

Result: The fields associated with the **GENERAL** parameter appears.

Figure 7-30 Connection templates – Template Name

The screenshot shows the 'Connection templates – Template Name' dialog box. At the top, there is a tab labeled 'GENERAL'. Below the tab, there are five input fields:

Folder	/My Templates
Template Name	ODUK or OTSiG Tunnel
Owner	user
Template Type	Connection
Description	(empty)

5

To name or rename the template, in the **Name** field, enter a name for the template.

6

In the **Description** field, enter any information that can further describe the template that you are creating.

7

To rename the template, in the **Name** field, enter a unique name for the template.

8

In the **Description** field, enter any information that can further describe the template that you are creating.

Result: By default, the template is stored under /My Templates Folder.

9

Click **OK** option at the right-bottom of the screen to confirm the changes.

Result: The success message appears at the left-bottom of the screen.

END OF STEPS

Task: Delete a template

Important! Before a template can be deleted, it must be Unpublished. Refer to “[Task: Unpublish a connection template](#)” (p. 748) for detailed steps.

Complete the following steps to delete an unpublished template.

1

From the NFM-T GUI, follow this navigation path:

DESIGN > Service/Infrastructure Template

Result: In the left portion of the design window, the system displays a tree with the **Best Practices**, **My Templates**, and **Published** folders.

2

In the tree, locate and select template to be deleted in the **My Templates**, or **Published** folder.

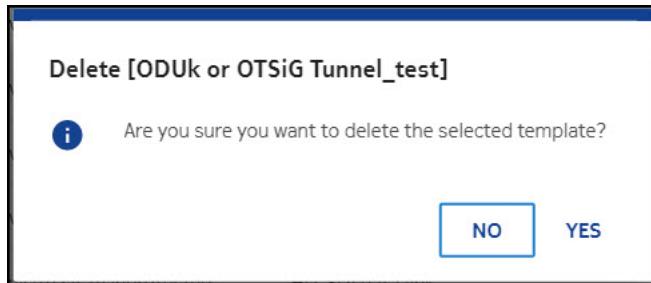
Result: The system displays the template in data table format in the right pane of the window.

3

Click the **More**  icon at the right end of corresponding template, and then click **Delete**.

Result: The deletion confirmation dialog appears.

Figure 7-31 Deletion - confirmation dialog



4

Select YES.

Result: The system deletes the template from the Tree.

END OF STEPS

7.12 Deploy a template to make a connection

When to use

Use this task to deploy a template to make an infrastructure connection or service connection.

Related information

See the following topics in this document:

- [2.6 “Provision a NFM-T OTN network” \(p. 160\)](#)
- [2.8 “Determine the Infrastructure to be created” \(p. 168\)](#)
- [7.3 “Field descriptions for Best Practices templates” \(p. 675\)](#)
- [7.4 “Service definition field descriptions for deploy Best Practices templates” \(p. 688\)](#)
- [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#)
- [“Service connection label” \(p. 763\)](#)
- [“Before creating a connection” \(p. 228\)](#)

Before you begin

Before a template is deployed, it must be published. Refer to [“Task: Publish a Connection Template” \(p. 748\)](#) for detailed steps.

Before you deploy any template to create a connection, refer to the [2.6 “Provision a NFM-T OTN network” \(p. 160\)](#) task to determine if you are ready to deploy a template.

This is a generic task; therefore, the template to be deployed is any template that resides in the available folders, that includes the **Best Practices**, **My Templates**, or **Published** folders.

If you are creating an infrastructure, refer to the [2.8 “Determine the Infrastructure to be created” \(p. 168\)](#) task to determine if you should create a trail or logical link.

Detailed explanations of the template fields are provided in [7.3 “Field descriptions for Best Practices templates” \(p. 675\)](#), [7.4 “Service definition field descriptions for deploy Best Practices templates” \(p. 688\)](#), and [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#).

i **Note:** In case of 10GbE rate, the user is responsible to select ports with appropriate container or unassigned ports, because the port selection window lists all ports irrespective of unassigned ports, 10GbE-ODU2/10GbE-ODU2E assigned port rates.

Task

Complete the following steps to deploy a template to make an infrastructure connection or service connection.

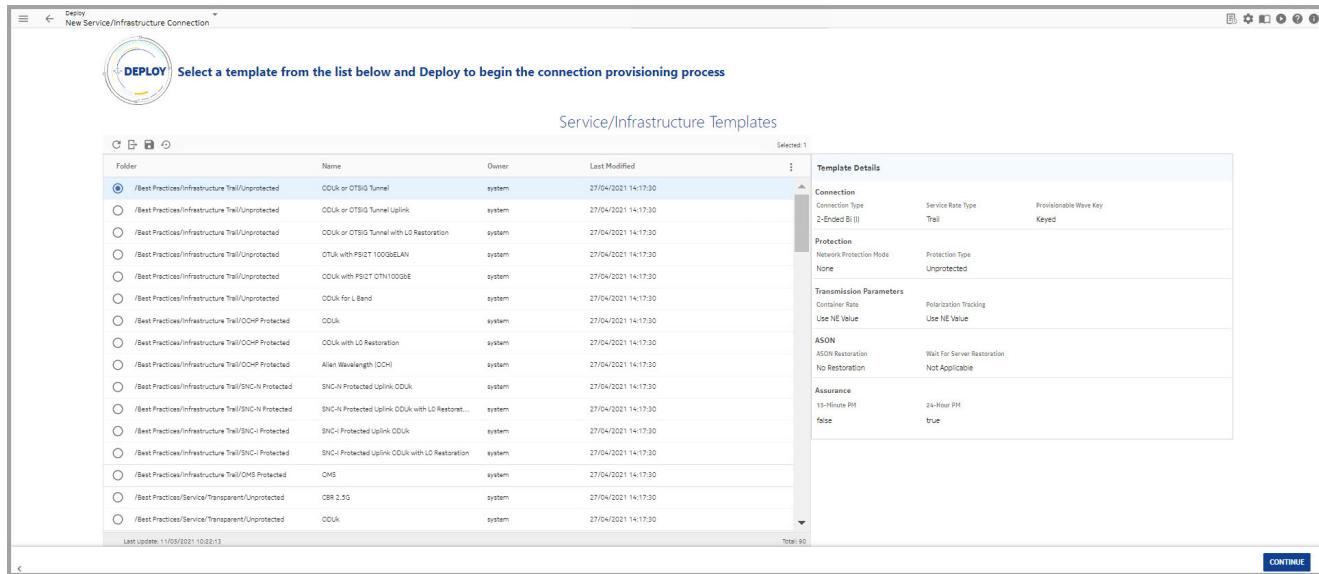
1

If you are deploying a connection for a particular customer and you want to associate the connection with a customer name, enter the customer into the NFM-T. Go to the task [Add a](#)

new Customer in the *Administration Guide* for detailed steps. Refer to the **Administer - Customers** section in the *Administration Guide* for details.

- 2 _____
Before a template can be deployed, it must be published. Complete the steps in the “[Task: Publish a Connection Template](#)” (p. 748) task.
- 3 _____
From the NFM-T GUI, follow this navigation path:
DEPLOY > New Service/Infrastructure Connection
Result: In the left portion of the displayed window, the system displays a tree that shows the available folders, which can include the **Best Practices**, **My Templates**, and **Published** folders.
- 4 _____
Click the plus signs to expand the tree and drill down to locate the particular template in the folder.
- 5 _____
In the tree, click on the particular template that you want modify.
- 6 _____
In the data table, right click on the particular template that you want deploy and select **Deploy**.
Result: The selected template is displayed. The Network Map is displayed in the left portion of the window. The Service Definition panel is displayed in the right portion of the window.

Figure 7-32 Connection templates – deploy – create connection window



7

Complete the following **required From/To NE** and **From/To Port** fields in the **Service Definition** panel of the template. Adjust the Network Map to better view the connection that you are creating.

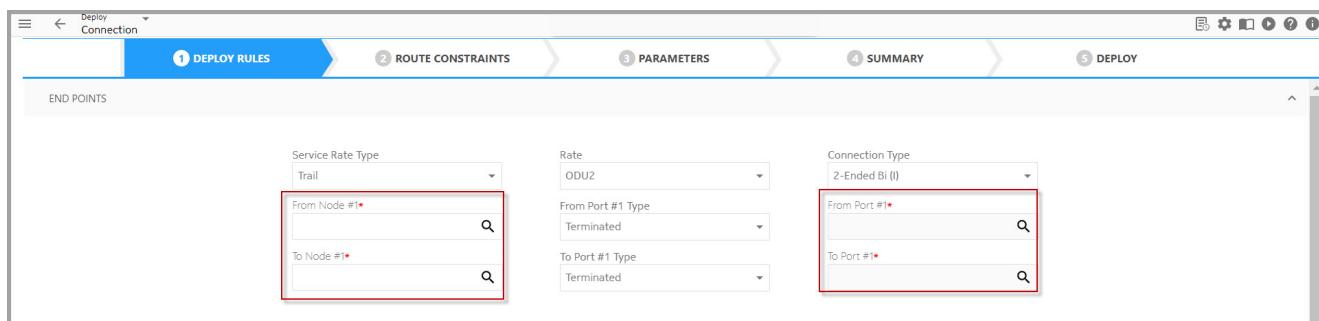
- In the **From NE** and **From Port** fields, click on the icon to the right to display the list of available NEs and Ports. Click on an NE and a port from the displayed lists.

Optional: The NE can be selected double clicking on the NE in the map.

- In the **To NE** and **To Port** fields, click on the icon to the right to display the list of available NEs and Ports. Click on an NE and a port from the displayed lists.

Optional: The NE can be selected double clicking on the NE in the map.

Figure 7-33 Connection templates – complete From/To NE and Port assignments in the Service Definition



8

Optional: Change any of the remaining fields in the any of the template panels to make appropriate choices for your site. For details on any of the fields, refer to 7.3 “Field descriptions for Best Practices templates” (p. 675), 7.4 “Service definition field descriptions for deploy Best Practices templates” (p. 688), and 7.5 “Advanced Settings field descriptions for deploy Best Practices templates” (p. 708).

Important provisioning notes:

- When creating an infrastructure connection, the system defaults to a trail. To create a logical link, check the **Logical Link** box in the **Service Definition**. For details on whether to create an infrastructure trail or logical link, refer to the 2.8 “Determine the Infrastructure to be created” (p. 168) task.
- If the deployed template is a SONET or SDH Y-Cable protected template, the **Y-Cable Port** panel is displayed *after* you select the From/To Node in the **Service Definition** panel.
- If the deployed template is an ALIEN Wavelength (OCH) template you can assign the **Channel Width** after selecting the two NEs and corresponding ports. Possible values are 50, 62.5 and 70 Ghz. This value can be assigned only if the selected NEs are ENEs and PHN nodes.
- The **Auto Server Creation** check box in the **Connection Controls** panel has provisioning considerations that apply to whether the system or the user creates the server layer for the infrastructure connection or service that is being created. Refer to “[Auto Server Creation](#)” (p. 708) for a detailed explanation.
- To specify manual routing, open the **Connection Controls** panel under **Advanced Settings** and change the **Routing** field to **Manual**.
- If **ASON Routed** is checked in the **Service Definition** panel, when creating a connection or when modifying the route of a connection, drop link connections or link connections that belong to connections with drop link connections cannot be selected from the Routing Constraints table when **Manual** routing is selected.
- To change the target state of the connection to a state other than **Commissioned**, open the **Connection Controls** panel and change the **Target State** field to your choice.
- To add routing constraints, open the **Routing Constraints** panel and select the **Routing Constraints** tab. Refer to “[Routing Constraints](#)” (p. 723) and 7.6 “[Routing Constraints](#)” (p. 731) for detailed instructions.
- Regenerator ports are displayed in the **Routing Constraints** panel when you create an infrastructure connection or modify the route of an infrastructure connection if the connection rate is ODUK and **ASON Routed** is selected and if the connection rate is ODUK and the **Auto Server Creation** field is selected. When you modify the route of an infrastructure connection, you can view the regenerator ports in the Routing Constraints table, but you cannot add or remove regenerator ports as routing constraints.
- If you select a regenerator port in the **Routing Constraints** panel and the **Provisionable Wave Key** field is set to **Keyed**, the **Wave Key Type** must be set to **Automatic**.

-
- When you select **Link Connection** based routing, if a connection endpoint is a channelized port on a black box, the link connection of the OS connection between the black box and the managed NE corresponding to the connection endpoint must be selected as a routing constraint.

Example:

If the endpoint is ODU4ODU2-[PTP_ID]-5, link connection #5 in the OS connection between the black box and the managed NE must be selected.

- When you select **Link Connection** based routing, if a connection endpoint is a channelized port on a black box, the link connection of the OS connection between the black box and the managed NE corresponding to the connection endpoint must be the lowest number link connection of the OS connection between the black box and the managed NE that is chosen as a routing constraint.

Example:

If the endpoint is ODU4ODU2-[PTP_ID]-5, you must not select LC#1 through LC #4 in the OS connection between the black box and the managed NE.

- For protected managed plane connections, you must enter the 3R ports in transmission sequence for the working and protection paths.
- If you selected the Route ID of a connection from the **Planning Tool** tab, the system does a scheduled or a manual synchronization between NPT and the NFM-T so the newly deployed connection is sent to the NPT. Using the service rate and connection endpoints, NPT finds the associated route ID in its database and marks the Route ID as implemented.

Note: The **Planning Tool** tab is only displayed if the NPT is part of the deployed solution for the user network. In addition, if NPT is part of the solution for the user network, the **Planning Tool** tab is only displayed during the creation of a connection; the **Planning Tool** tab is not displayed when you modify the route or the parameters of a connection.)

The **Planning Tool** tab is only displayed if the Create Connection Planning Tool is set in the NFM-T preferences. See the Administer – Preferences section in the *NFM-T Administration Guide*.

- To change any FM or PM settings, open the **Assurance** panel.

9

If you want to use this template and not make any changes, go to [Step 19](#).

If you want to reuse and save this template, go to [Step 10](#).

10

To reuse and save this template, click **Save as a Template**.

Result: The OTN Templates Details window for the particular template is displayed.

11

Click on **Select folder**.

Result: The Template Name and Folder Dialog window is displayed.

Figure 7-34 Connection Templates – Deploy – Template Name and Folder Dialog Window



12

To name/rename the template, in the **Name** field, enter a name for the template.

13

In the **Description** field, enter any information that can further describe the template that you are creating.

14

Select a folder from the tree.

Result: The system displays the folder that you selected in the **Folder** field of the Template Name and Folder Dialog window.

15

Click **OK**.

Result: The system puts the same information that you entered in the Name and Description fields in the OTN Templates Details window into the corresponding fields in the template.

16

Click **OK** or **Apply**.

Result: The system displays the name of the template that you have created in the appropriate folder in the Tree.

Figure 7-35 Connection templates – template created stored in the selected directory in DESIGN

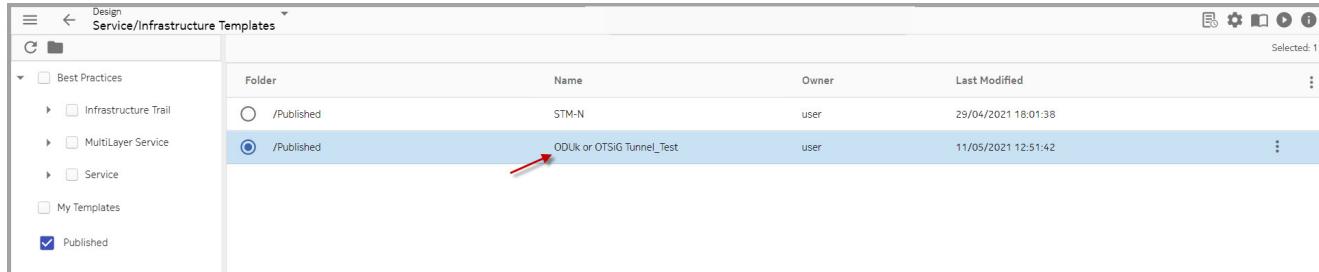
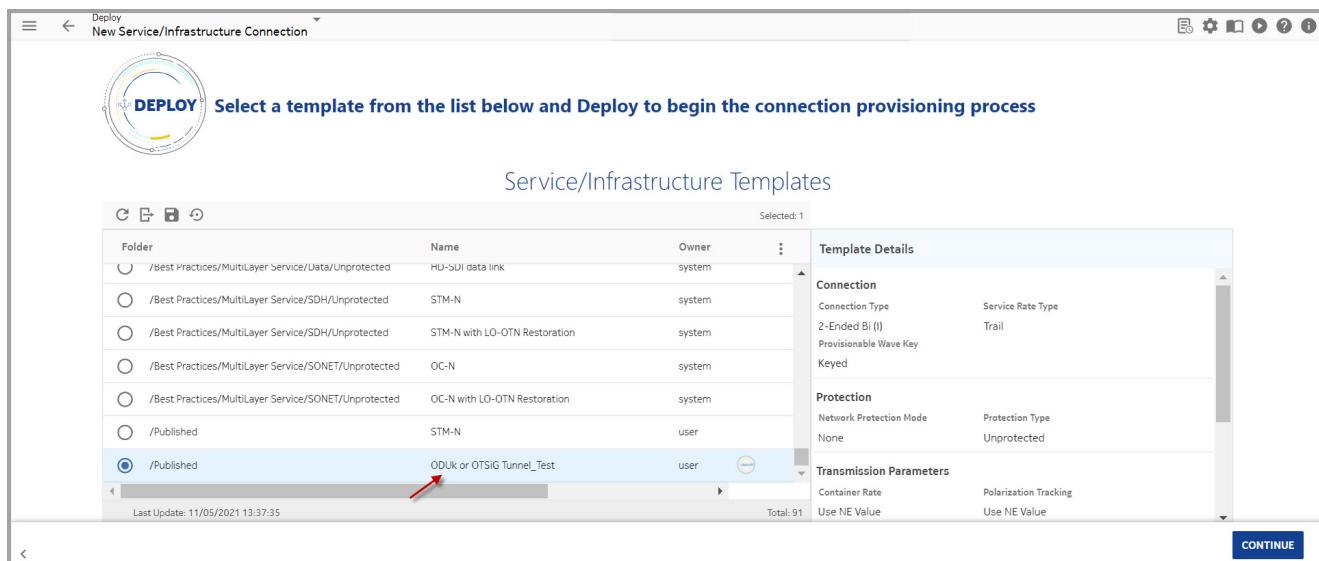


Figure 7-36 Connection templates – template created stored in the selected directory in DEPLOY



17

Click the plus signs to expand the tree, open the appropriate folder, and drill down to locate the template that you just saved.

Hint: If the template is not visible in the directory that you specified and selected, refresh the browser page or open a new browser window.

18

Right click on the newly created template and go to [Step 19](#).

19

Click **Deploy**.

Result: The system outputs a Provision Task Status – <Connection Name> window. Initially, this window displays hollow arrow icons, the number of which is determined by the plane where the connection is created (Managed Plane or Control Plane) and the **Target State** of the connection, which you select from the **Connection Controls** panel. You can press the **More** button for additional information or the **Close** button to exit the window.

When the connection moves to a **Deployed** or **Commissioned** state, the arrows are displayed in green for successful execution. In addition, when the connection moves to a **Deployed** or **Commissioned** state, the **Show New Connection(s)** button is activated. Click **Show New Connection(s)** button to view the connection on the appropriate list. Any failures are displayed in red.

If the connection fails, the **Show New Connection(s)** window is replaced by the **Show Failure Analysis** button. Click this button to access the Failure Analysis window, which is only available for infrastructure connections or services that are in the **Defined** state and that have an Implementation Status of **Failed**. Refer to [7.70 “View Failure Analysis for an infrastructure connection or service” \(p. 1013\)](#) for details.

Additionally, when the connection moves to a **Commissioned** state, the **Optical Power** button is also activated.

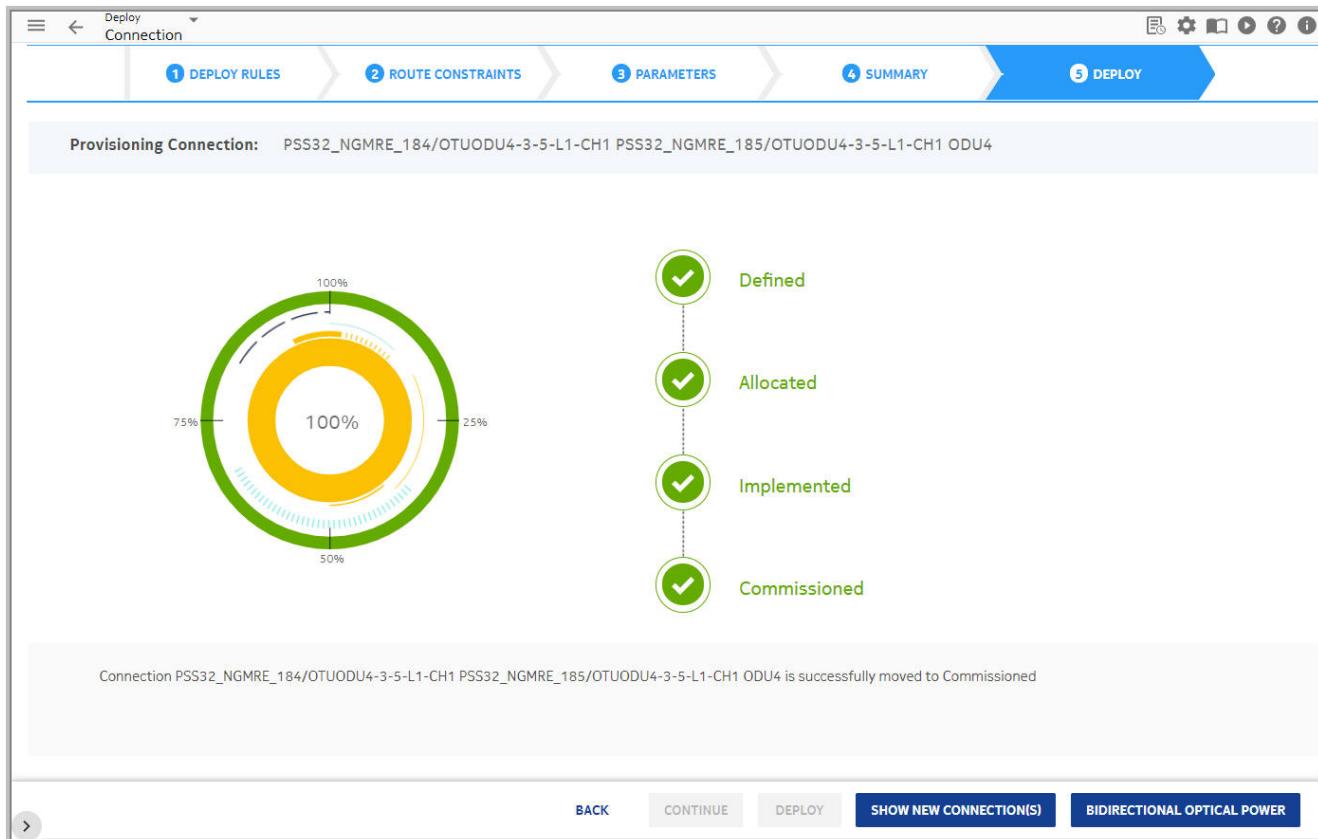
Click the **Optical Power** button to view one of the following:

- For an ODUk infrastructure connection or a service, the **Bidirectional Optical Power** window opens. See [17.15 “View Bidirectional Optical Power display for ODUk infrastructure connections and services” \(p. 1859\)](#) for more information about bidirectional power display.
- For an OTUk infrastructure connection, the **OTUk WLT** window for the A->Z direction opens. See [17.17 “Manage optical power for an OTUk infrastructure connection” \(p. 1868\)](#) for more information about OTUk power display. To view the power in the opposite direction, click **Connection Optical Power Z->A**.

Note: For an OTUk or OTSig ASON Implicit Server connection, the option to navigate to **Optical Power** window is not available. User may need to navigate to the optical power of client ODU/OTSig tunnel infrastructure or DSR service optical power, and click on the appropriate OTUk/OTSig icon to view the optical power of the selected OTUk/OTSig or OCH. You can also access the Failure Analysis window from **Show Failure Analysis** button on the **Progress Bar** when you are creating a connection.

The following figure is added as example showing the Provision Task Status window for a successful Control Plane connection that has a **Target State** of **Commissioned**.

Figure 7-37 Connection templates – provision task status – successful – Control Plane, commissioned



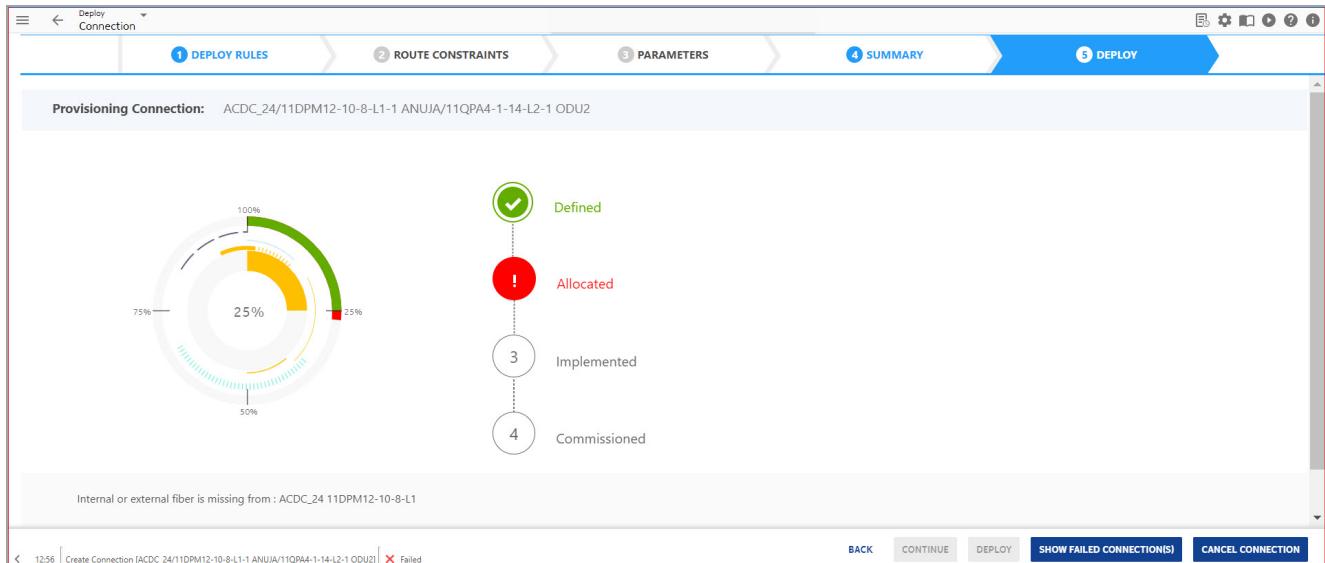
Drop link provisioning notes

In the Drop Link (L0 Drop link on Client port whose Line end on OT), configure the following:

- Create (Defined/Allocated state) a Trail using these Drop Links and OMS Links.
- Identify the end drop ports and check if the data bearer is already created in the GMRE.
- Remove the Drop Link from NPA and re-add.
- If the data bearer is present the system displays an error message. The user must remove the Drop link and re-add the drop link.

Upon successful completion of the connection, the system displays the connection on the Network Map and on the data tables for infrastructure connections or services.

Figure 7-38 Error Message: Network Route Not Found



To implement the trail, create a data bearer on the Drop Port. OPSA in set Command will be sent ONLY in case of OPSA set up. Else, the OPSA attribute is not set in NE.

To deimplement the trail

- Deletes the LSP from GMRE
 - Deletes the Data bearer of the Drop Port
 - Marks the Drop Link in NPA as Locked
- The user can remove the drop link from NPA.

i Note: If the network has a mix of directional Add/Drop and multidirectional Add/Drop and you try to create OPSA L0 CP, it is not always guaranteed to find a route by auto-routing. In case of error you have to provide OTS constraints for working and protection legs or partial constraints either for working or protection.

END OF STEPS

Service connection label

The system parameter SERVICE_LABEL_SUFFIX defines the generated user label suffix. The value can be **DSR** or **RATE**.

If the service user label is automatically generated by the system, it contains **DSR** as suffix regardless if the service is a STM-x, a 1/10/100Gb GBe or any other service type.

- in case of ODU services, the suffix is the *ODU* rate itself. When the system parameter *Service Label Suffix* is set to RATE, the suffix is the OTU rate.

- for discovered and auto created services the suffix rate is set accordingly.

If the service suffix is set to **RATE**, the suffix is one of the following rate, according to the port type:

- ETH: FE, 1 GbE, 10GbE, 100GbE
- SONET: OC3/OC12/OC48/OC192
- SDH: STM1, STM4, STM16, STM64
- FC: FC100, FC200, FC400, FC800, FC1200
- OTN: OTU1, OTU2, OTU2e, OTU3, OTU4
- SD-SDI, HD-SDI, 3G-SDI

The user label with the rate as suffix is not the default. To modify the value of the parameter, see the procedure *Modify an Installation Parameter* in the *Administration Guide: System Maintenance and Troubleshooting*.

In the figure an example of services with rate suffix.

Figure 7-39 Services list with rate suffix

Conn...	NA	UP	DOWN	DEGRADED	Name	Protection	From Node #1	From Port #1	To Node #1	To Port #1	Al...
Conn...	NA	UP	DOWN	DEGRADED	s4x-nni-s1	Unprotected	R214_S5AD400H...	OTUODU4-4-3-C1...	R214_S5AD400H...	OTUODU4-4-3-C1...	■
Commissioned	ODU4				PM-TEST-11DPM12-OC3 ODU#1:3 DSR:1	Unprotected	R214_CONFIGD_11	11DPM12-6-6-C3	R214_CONFIGD_13	11DPM12-6-6-C3	
Commissioned	OC-3				PM-TEST-11DPM12-OC48 ODU#1:4 DSR:1	Unprotected	R214_CONFIGD_13	11DPM12-6-6-C4	R214_CONFIGD_11	11DPM12-6-6-C4	
Commissioned	OC-48				R214_CONFIGD_11/11DPM12-6-6-C1 R214_CO...	Unprotected	R214_CONFIGD_13	11DPM12-6-6-C1	R214_CONFIGD_11	11DPM12-6-6-C1	
Commissioned	1 GbE				R214_CONFIGD_11/11DPM12-6-6-C2 R214_CO...	Unprotected	R214_CONFIGD_11	11DPM12-6-6-C2	R214_CONFIGD_13	11DPM12-6-6-C2	
Commissioned	FE				R214_CONFIGD_11/11DPM12-6-6-C2 R214_CO...	Unprotected	R214_CONFIGD_11	11DPM12-6-6-C2	R214_CONFIGD_13	11DPM12-6-6-C2	
Commissioned	10GbE				TEST-PM-OCS-10G-CONN	Unprotected	R214_OCS_NE1	GBE10-1-1-1-1	R214_OCS_NE2	GBE10-1-1-1-1	
Commissioned	1GbE				TEST-PM-OCS-1G-CONN	Unprotected	R214_OCS_NE1	GBE-1-1-2-1	R214_OCS_NE2	GBE-1-1-2-1	
Commissioned	STM-16				TEST-PM-OCS-STM16-CONN	Unprotected	R214_OCS_NE1	STM16-1-1-2-9	R214_OCS_NE2	STM16-1-1-2-9	
Commissioned	STM-64				TEST-PM-OCS-STM64-CONN	Unprotected	R214_OCS_NE1	STM64-1-1-1-3	R214_OCS_NE2	STM64-1-1-1-3	
Commissioned	100GbE				s5ad-100g-c1 ODU#1 DSR:1	Unprotected	R214_S5AD400H...	PORT-4-2-C1	R214_S5AD400H...	PORT-4-2-C1	

7.13 Unterminated service or ODU unterminated with NNI client

Unterminated Service or ODU Unterminated with NNI Client

Managing unchannelized/channelized services, for example unterminated service or ODU unterminated with NNI client, it is mandatory to have the ENE in case of PSS24X nodes.

An example is described to give the sequence of operation that is necessary to create the transparent service. Refer to 7.12 “Deploy a template to make a connection” (p. 754), “Operate ASON NPAs” (p. 1438) and 10.3 “Connection creation - ASON specific” (p. 1429) for detailed procedures.



Note:

- In the **Service Definition Panel**, if you do not select the **L Band Frequency** option, the routing constraints selection shows the available C and C+L band servers that supports the ODUK NNI service.
- In the **Service Definition Panel**, if you select the **L Band Frequency** option, the routing constraints selection shows the available L and C+L band servers that supports the ODUK NNI service.

Follow these 10 steps to create the transparent service:

1. Supervise the two PSS24x(L1) Nodes.
2. Provision the 4UC400 cards.
3. Create Internal OS, for example between 4UC400 and CWR.
4. Provision the ODU4 Logical Link.
5. Add the Logical Link to NPA and unlock it.
6. Provision 30AN300 pack on both nodes.
7. Create two ENEs.
8. Create the OPS between ENE-1 to PSS24X node1 and OPS between ENE-2 to PSS24X node2
9. Add the OPS (OTU2e rate) as drop link in NPA.
10. Create the end to end transparent service between the ENE-1 to ENE-2

7.14 Different modes of creating a connection

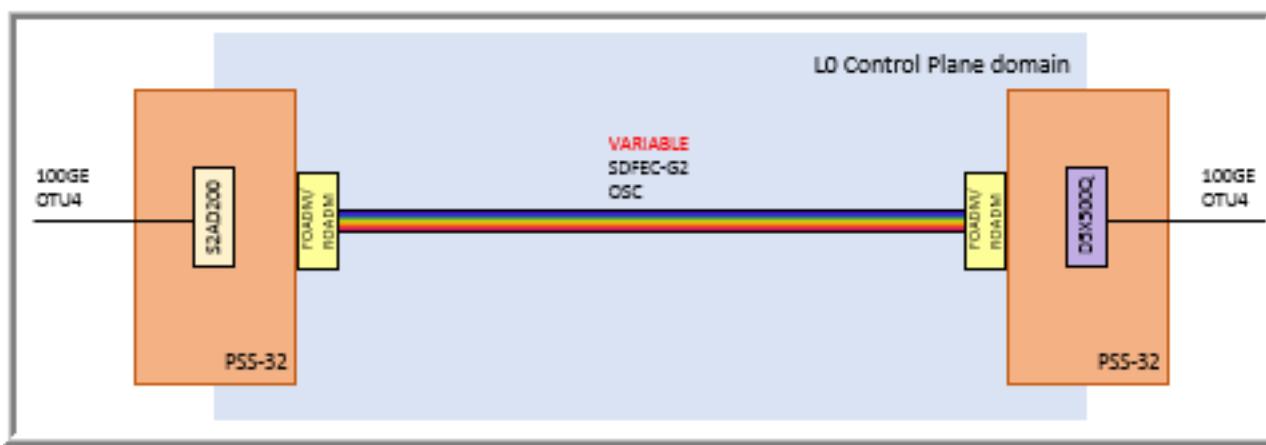
Description

When creating a connection there are several different scenarios to create the connection which is different from the normal provisioning flow.

For example, in case of D5x500Q interworking with other OTs like S13x100R/E, 260SCX2 and S2AD200H/R at NNI rate, the correct workflow is:

- Create an Infrastructure connection with ASON routed Logical Link option selected between the line ports
- If NNI configuration is used, then **do not add** drop links on client ports to NPA
- Create end to end Managed Plane service

Figure 7-40 Example to apply different connection creation mode



See [7.12 “Deploy a template to make a connection” \(p. 754\)](#) for details on the connection creation.

Possible combinations L0 CP for NNI with OTU4 Line signal type

The table summarizes all the possible combinations on L0 Control Plane for NNI with OTU4 line signal type.

i **Note:** The table also applies to the other variants of the cards such as D5x500Q, D5x500L, D5x500, S2AD200H, S2AD200R, S13x100R, S13x100E.

Table 7-11 L0 CP for NNI with OTU4 Line Signal

	D5x500Q (UNI)	S2AD200H (UNI)	S13x100R (UNI)	D5x500Q (NNI)	S2AD200H (NNI)	S13x100R (NNI)	260SCX2 (UNI)	260SCX2 (NNI)
D5x500Q (UNI)	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service over the Logical Link	Create OPS from D5X500Q NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from D5X500Q UNI client port to ENE over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client to ENE.	Create an OPS link from 13X100 NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from D5X500Q UNI client port to ENE over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client port to client port or ENE to ENE.
S2AD200H (UNI)	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create OPS from D5X500 NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from S2AD200 client port to ENE over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client to ENE.	Create OPS link from S13X100 NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from S2AD200 client port to ENE over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client port to client port or ENE to ENE.

Table 7-11 L0 CP for NNI with OTU4 Line Signal (continued)

	D5x500Q (UNI)	S2AD200H (UNI)	S13x100R (UNI)	D5x500Q (NNI)	S2AD200H (NNI)	S13x100R (NNI)	260SCX2 (UNI)	260SCX2 (NNI)
S13x100R (UNI)	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an OPS link from D5X500 NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from S13X100 client port to ENE over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client to ENE.	Create an OPS link from S13X100 NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from S13X100 UNI client port to ENE over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client port to client port or ENE to ENE.
D5x500Q (NNI)	Already covered	Already covered	Already covered	Create an ASON Routed Logical Link between the line ports. DO NOT assign the link to NPA. Create an ODU4 Managed Plane service from client ports over the Logical Link.	Create an OPS link from S2AD200H NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create an ODU4 Managed Plane service from D5X500 client to ENE.	Create an ASON Routed Logical Link between the line ports. Create an ODU4 Managed Plane service from client ports over the Logical Link.	Create an ASON Routed Logical Link between the line ports. Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.	Create an OPS link from NNI client to ENE. DO NOT assign the link to NPA. Create an ASON Routed Logical Link from line port to line port. Create a 100GbE/ODU4 Managed Plane service from client port to client port or ENE to ENE.

Table 7-11 L0 CP for NNI with OTU4 Line Signal (continued)

	D5x500Q (UNI)	S2AD200H (UNI)	S13x100R (UNI)	D5x500Q (NNI)	S2AD200H (NNI)	S13x100R (NNI)	260SCX2 (UNI)	260SCX2 (NNI)
S2AD200H (NNI)	Already covered	Already covered	Already covered	Already covered	<p>Create two OPS links from NNI client to ENE.</p> <p>DO NOT assign the OPSs to NPAs.</p> <p>Create an ASON Routed Logical Link between the line ports.</p> <p>Create an ODU4 Managed Plane service from client ports over the Logical Link.</p>	<p>Create an OPS link from S2AD200H NNI client to ENE</p> <p>DO NOT assign the link to NPA.</p> <p>Create an ASON Routed Logical Link from line port to line port.</p> <p>Create and ODU4 Managed Plane service from S13X100 client to ENE.</p>	<p>Create an ASON Routed Logical Link between the line ports.</p> <p>Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.</p>	<p>Create an OPS link from NNI client to ENE.</p> <p>DO NOT assign the link to NPA.</p> <p>Create an ASON Routed Logical Link from line port to line port.</p> <p>Create a 100GbE/ODU4 Managed Plane service from client port to client port or ENE to ENE.</p>
S13x100R (NNI)	Already covered	Already covered	Already covered	<p>Create an ASON Routed Logical Link between the line ports.</p> <p>DO NOT assign the link to NPA.</p> <p>Create an ODU4 Managed Plane service from client ports over the Logical Link.</p>	<p>Create an OPS link from S2AD200 NNI client to ENE.</p> <p>DO NOT assign the link to NPA.</p> <p>Create an ASON Routed Logical Link between the line port of S13X100 and line port.</p> <p>Create an ODU4 Managed Plane service from S13X100 client port to ENE over the Logical Link.</p>	<p>Create an ASON Routed Logical Link between the line ports.</p> <p>Create an ODU4 Managed Plane service from client ports over the Logical Link.</p>	<p>Create an ASON Routed Logical Link between the line ports.</p> <p>Create a 100GbE/ODU4 Managed Plane service from client ports over the Logical Link.</p>	<p>Create an OPS link from NNI client to ENE.</p> <p>DO NOT assign the link to NPA.</p> <p>Create an ASON Routed Logical Link from line port to line port.</p> <p>Create a 100GbE/ODU4 Managed Plane service from client port to client port or ENE to ENE.</p>

7.15 Node or physical link as constraint

Overview

Use this task to include or exclude node or physical link as constraint for infrastructure connections and services.

For details on **Create Connection** window and deploying an infrastructure connection or service, see [24.2 “Quick Help – The Create Connection Window” \(p. 1970\)](#).

For details on deploying a physical connection with routing constraints, see [8.7 “Deploy a Connection with Routing Constraints” \(p. 1286\)](#)

Component Templates

7.16 Overview

Purpose

The component templates allow saving the routing constraints and transmission parameters separately and applied to the connection. The user is not required to specify the individual routing constraints or transmission parameters during connection provisioning.

Contents

7.16 Overview	771
7.17 Manage Routing Constraints	772
7.18 Manage Transmission Parameters	777

7.17 Manage Routing Constraints

Purpose

Use this task to manage routing constraints template. The user views the details, modify, and deletes the routing constraint.

Description

Routing constraints are applied to any connection, they are saved as a separate template structure. With the separate structure, the user applies the routing constraint template with any of the other templates.

The **Routing Constraints Templates** are saved from the deploy window during connection creation.

Component Templates window

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

The Components Template window is displayed. The window contains left panel of filters and right panel with a data table of templates. Left panel has two filters: **Routing Constraints** and **Transmission Parameters**. Select either **Routing Constraints** or **Transmission Parameters** check box, the corresponding templates are displayed in the data table.

Figure 7-41 Component Templates window

The screenshot shows the 'Component Templates' window in the 'Design' section of the NFM-T GUI. On the left, there is a filter sidebar with two checkboxes: 'Routing Constraints' (which is checked) and 'Transmission Parameters'. The main area is a data table with columns: 'Folder', 'Name', 'Owner', and 'Last Modified'. There are two entries in the table:

Folder	Name	Owner	Last Modified
/Routing Constraints	SFM6_CF_49_cdcf05_01_conf11_14_cdcf_04	admin	26/08/2021 15:50:14
/Routing Constraints	sfm6_s6ad_new2	admin	26/08/2021 16:13:34

User Actions on Routing Constraints templates

Select a template and click the **More** icon. The system enables user to perform the following actions:

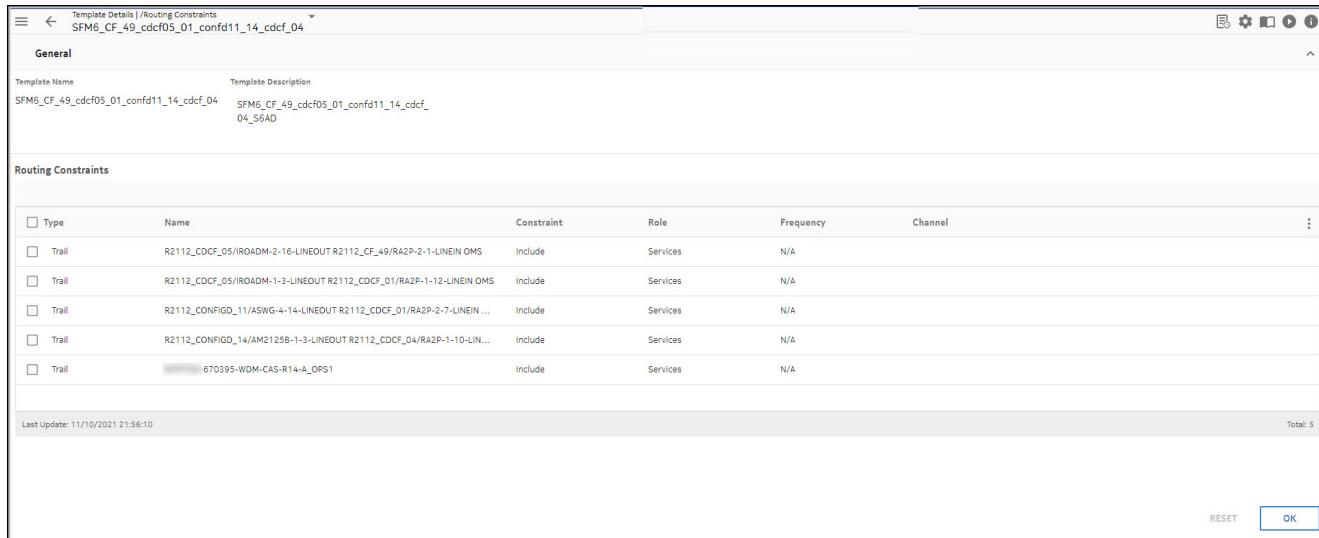
- “Task: View Routing Constraints template ” (p. 773)
- “Task: Modify Routing Constraints” (p. 774)
- “Task: Delete Routing Constraints” (p. 775)

Task: View Routing Constraints template

Complete the following steps to view the routing constraints:

- 1 _____
From the NFM-T GUI, select one of the following navigation paths:
DESIGN > Component Templates
Result: The system displays the **Components Template** window.
- 2 _____
Select the **Routing Constraint** check box.
Result: The templates related to **Routing Constraint** are displayed on the right side data table.
- 3 _____
Click the **More :** icon and select **Details**.
Result: The system displays the **Template Details** window.
- 4 _____
In the **General** panel, following parameters are pre-populated for the selected routing constraint template: **Template Name** and **Template Description**.
- 5 _____
The **Routing Constraints** panel displays the following fields:
 - **Type** - displays the type of constraint.
 - **Name** - displays the name of the constraint.
 - **Constraint** - displays if it is a **Include** or a **Exclude** constraint.
 - **Role** - displays the type of role. Possible values are Services or Protection.
 - **Frequency** - displays the frequency and is applicable for Fiber.
 - **Channel** - displays the channel width.

Figure 7-42 Template Details window



6

Click **OK** or Select **RESET** to reset the template.

END OF STEPS

Task: Modify Routing Constraints

Complete the following steps to modify the routing constraints:

1

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

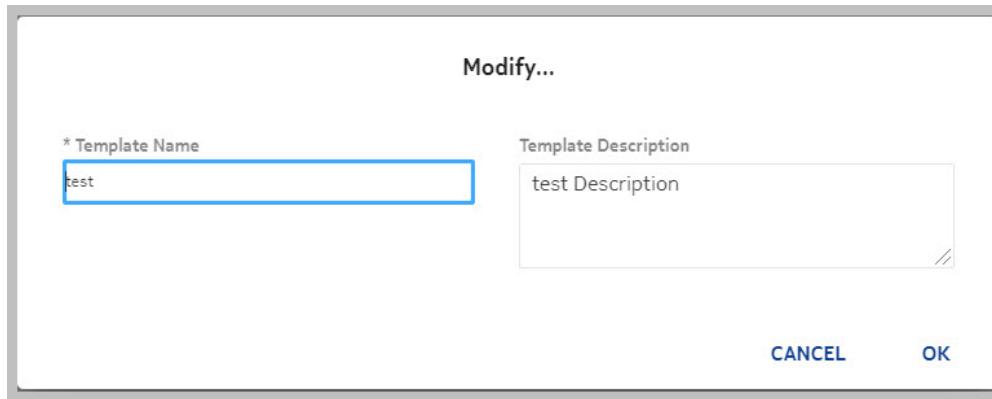
Result: The system displays the **Components Template** window.

2

Select the required routing constraint template. Click the **More** icon and select **Modify**.

Result: The system displays **Modify** window.

Figure 7-43 Modify window



3

Modify the following parameters:

- **Template Name** - Configure the name of the template to be modified.
- **Template Description** - Provide additional information for the template to be modified.



Note: Only these fields can be modified.

Result: The modified fields are displayed.

4

Click **OK** or **CANCEL** to undo the modification.

END OF STEPS

Task: Delete Routing Constraints

Complete the following steps to delete the routing constraints:

1

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

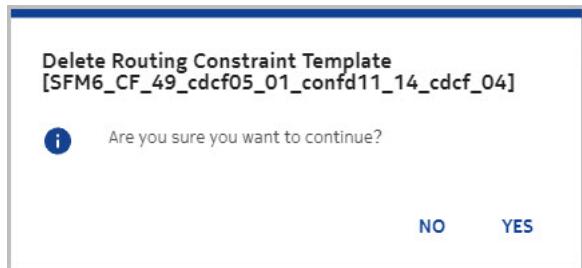
Result: The system displays the **Components Template** window.

2

Select the required routing constraint template. Click the **More** icon and select **Delete**.

Result: A confirmation message *Are you sure you want to continue?* is displayed.

Figure 7-44 Delete window



3

Click **YES** or **NO** to cancel the deletion.

END OF STEPS

7.18 Manage Transmission Parameters

Purpose

Use this task to manage transmission parameter template. The user can view the details, modify, and delete the transmission parameters.

Description

Transmission parameters can be applied to any connection, so they can be saved as separate template structure. With the separate structure, the user can simply apply the Transmission parameters template with any of the other templates.

Component Templates window

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

The Components Template window is displayed. The window contains left panel of filters and right panel with a data table of templates. Left panel has two filters: **Routing Constraints** and **Transmission Parameters**. Select either **Routing Constraints** or **Transmission Parameters** check box, the corresponding templates are displayed in the data table.

Figure 7-45 Component Templates window

The screenshot shows the 'Component Templates' window in the Nokia NFM-T interface. The left sidebar has a filter section with two checkboxes: 'Routing Constraints' (which is checked) and 'Transmission Parameters'. The main area displays a table with the following data:

Folder	Name	Owner	Last Modified
/Routing Constraints	SFM6_CF_49_cdcf05_01_confd11_14_cdcf_04	admin	26/08/2021 15:50:14
/Routing Constraints	sfm6_s6ad_new2	admin	26/08/2021 16:13:34

User Actions on Transmission Parameters templates

Figure 7-46 Transmission Parameters templates window



Select a template and click the **More** icon. System enables user to perform the following actions:

- ["Task: View Transmission Parameters Template" \(p. 777\)](#)
- ["Task: Modify Transmission Parameters" \(p. 780\)](#)
- ["Task: Delete Transmission Parameters" \(p. 782\)](#)

Task: View Transmission Parameters Template

Complete the following steps to view the Transmission Parameters:

1

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

Result: The system displays the **Components Template** window.

Figure 7-47 Component Templates window



2

Select the **Transmission Parameters** check box.

Result: The templates related to **Transmission Parameters** are displayed on the right side data table.

3

Click the **More**  icon and select **Details**.

Result: The system displays the **Template Details** window.

4

In the **General** panel, following parameters are pre-populated for the selected Transmission Parameters template: **Template Name** and **Template Description**.

5

The **Transmission Parameters Template** panel displays the following fields:

- **Parameter** - displays the parameter details.
- **Provisioning Layer** - displays the provisioning layer.
- **Current** - displays the current status and values.

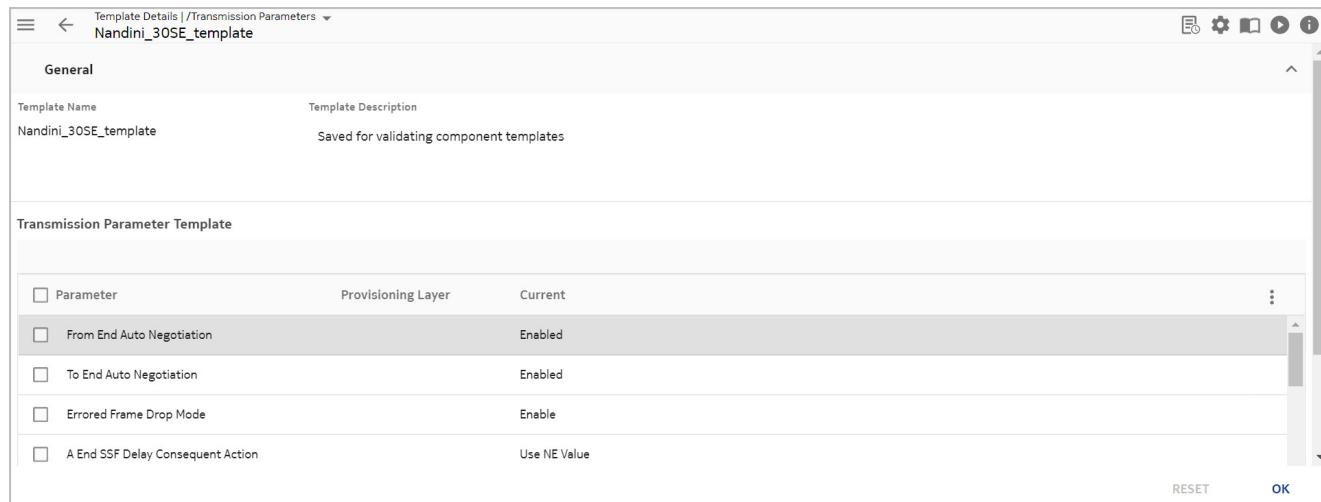
Parameter	Provisioning Layer	Current
From End Auto Negotiation	NA	Enabled
To End Auto Negotiation	NA	Enabled
Errored Frame Drop Mode	NA	Enable
A End SSF Delay Consequent Action	NA	Use NE value
From End Loss Propagation	NA	Laser Off
To End Loss Propagation	NA	Laser Off
A End SSD Consequent Action	NA	Laser Off
ODUk Source AZ trail trace	NA	ODUkSAZ
ODUk Source ZA trail trace	NA	ODUkSZA
ODUk Trail trace mismatch detection mode	NA	Source Enabled
ODUk Trail trace mismatch monitoring	NA	Enable All
ODUk Trail trace mismatch consequent action	NA	Enable
ODUk Payload Type Mismatch Response	NA	Enable
ODUk Payload type	NA	Use NE value
ODUk Burst interval for SD Detection	NA	9

Parameter	Provisioning Layer	Current
ODUk Burst Threshold for SD Detection	NA	900
ODUk From End Loss Propagation	NA	Laser Off
ODUk To End Loss Propagation	NA	Laser Off
From End CSF Type	NA	Use NE value
To End CSF Type	NA	Use NE value
Z End SSF Delay Consequent Action	NA	Use NE value
Z End SSD Consequent Action	NA	Laser Off

Notes:

1. The parameters are dynamic based on the type of connections which is created by the user.

Figure 7-48 Template Details window



6

Click **OK** or Select **RESET** to reset the template.

END OF STEPS

Task: Modify Transmission Parameters

Complete the following steps to modify the Transmission Parameters:

1

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

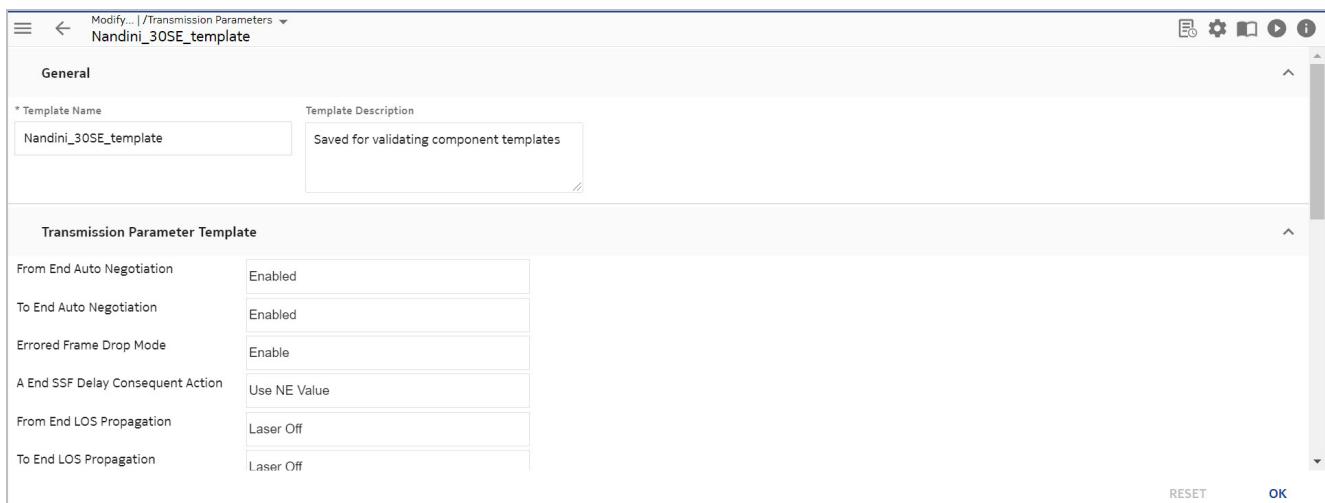
Result: The system displays the **Components Template** window.

2

Select the required Transmission Parameter template. Click the **More**  icon and select **Modify**.

Result: The system displays **Modify** window.

Figure 7-49 Modify window



3

In the **General** panel, modify **Template Name** and/or **Template Description**.

4

In the **Transmission Parameters Template** panel, modify any of the following transmission parameters:

Parameter	Default values
From End Auto Negotiation	Enabled
To End Auto Negotiation	Enabled
Errorred Frame Drop Mode	Enable
A End SSF Delay Consequent Action	Use NE value

Parameter	Default values
From End Loss Propagation	Laser Off
To End Loss Propagation	Laser Off
A End SSD Consequent Action	Laser Off
ODUk Source AZ trail trace	ODUKSAZ
ODUk Source ZA trail trace	ODUKSZA
ODUk Trail trace mismatch detection mode	Source Enabled
ODUk Trail trace mismatch monitoring	Enable All
ODUk Trail trace mismatch consequent action	Enable
ODUk Payload Type Mismatch Response	Enable
ODUk Payload type	Use NE value
ODUk Burst interval for SD Detection	9
ODUk Burst Threshold for SD Detection	900
ODUk From End Loss Propagation	Laser Off
ODUk To End Loss Propagation	Laser Off
From End CSF Type	Use NE value
To End CSF Type	Use NE value
Z End SSF Delay Consequent Action	Use NE value
Z End SSD Consequent Action	Laser Off

5

Click **OK** or **CANCEL** to undo the modification.

END OF STEPS

Task: Delete Transmission Parameters

Complete the following steps to delete the Transmission Parameters:

1

From the NFM-T GUI, select one of the following navigation paths:

DESIGN > Component Templates

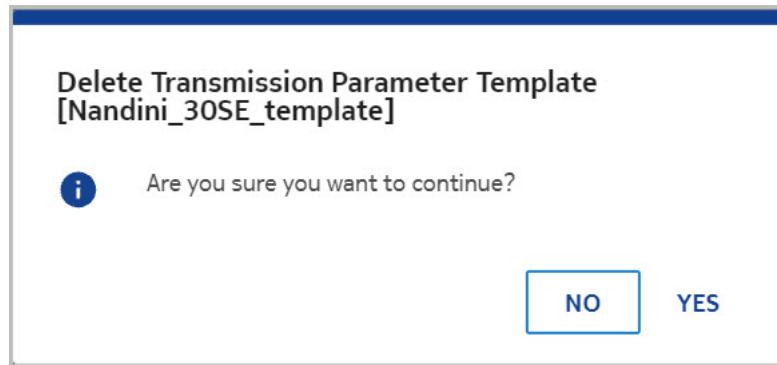
Result: The system displays the **Components Template** window.

2

Select the required Transmission Parameter template. Click the **More**  icon and select **Delete**.

Result: A confirmation message *Are you sure you want to continue?* is displayed.

Figure 7-50 Delete window



3

Click **YES** or **NO** to cancel the deletion.

END OF STEPS

Physical Connections

7.19 Create an OTN physical connection

When to use

Use this task to create an OTN physical connection.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

To create connections for the other NEs managed by NFM-T, refer to the section . Equipment Managed by NFM-T in the *NFM-T NE Management Guide*.

Before you begin

You can also access the Physical Connection Creation window, follow the path: **Deploy > New OTN Physical Connection**.

The OTN physical connection to be created can be one of several types of connections. Refer to the following tasks for detailed steps:

- 7.19.4 “Task: Create a 4-ended OTS or OPS physical connection” (p. 788)
- 7.19.5 “Task: Create an Bidirectional physical OTS or OPS connection” (p. 793)
- 7.19.6 “Task: Create an OTN Y-Cable physical connection” (p. 796)
- 7.19.7 “Task: Create an OTN UNI IETF physical connection” (p. 798)
- 7.19.8 “Task: Create an OTN OPS physical connection for packet switch” (p. 801)

i **Note:** For all UNI rates, if the OPS creation involves Client ports of any PHN OT pack that support **containerType**, the signal rate must be assigned before connection creation. This is a requisite for the correct FTP ports creation during the OPS connection creation.

i **Note:** While creating *OPS Bidirectional* physical connection with **Interface Type UNI-Ethernet** and **Client Signal Type** as *Ethernet 1GbE/10GbE/100GbE*, **New OTN Physical Connection** creation template displays **Required Container Type** field for OTU4 or OTUFlex, if the port is not provisioned.

Container types values depends on selected client signal type:

1. 1GbE: OTU0/ OTUFlex
2. 10GbE: OTU2/ OTU2E/ OTUFlex
3. 100GbE: OTU4/ OTUFlex

This is supported on 1830 PSS NEs from R13.0 onwards on following shelf types: 1830 PSS-24X, 1830 PSS-12X and 1830 PSS-8X. This is supported on the card types 10AN400,

4AN400, 30AN300, 4MX200, 10AN1T, S13X100R, S13X100E, S13X100L, 20UC200, 20AX200, 20MX80, 20AN80, 112SDX11and 8P20.

When creating an OPS connection type with **2 Ended split bi**, the frequency on both ends need to be set manually as indicated for all the NEs:

- A end Tx frequency = Z end Rx frequency
- A end Rx frequency = Z end Tx frequency

Set the signal rate prior to configuring frequency and then create the OPS physical connection.
This condition is applicable for Single Fiber scenario.

Provision DSR between VNEs

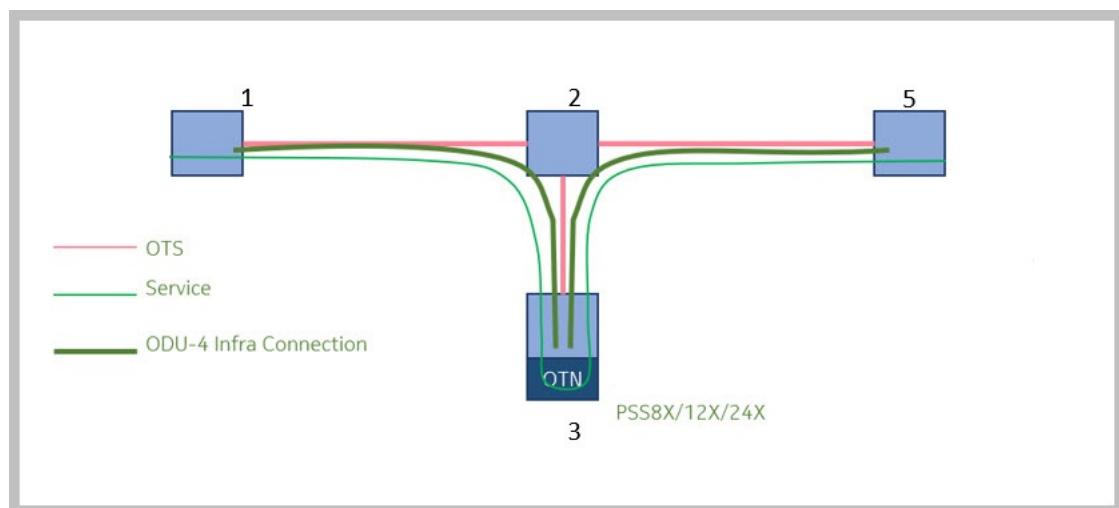
To allow the correct export by OTN application of the SDH DSR path, it is mandatory to create the OPS connection as Bidirectional and set the **Interworking Tech** field to **SDH**. The SDH port, which is the endpoint for the SDH logical link, also needs to be created.

Reuse OTS Link in service route

NFM-T supports reuse of an OTS link in a service connection network having more than two nodes and trails.

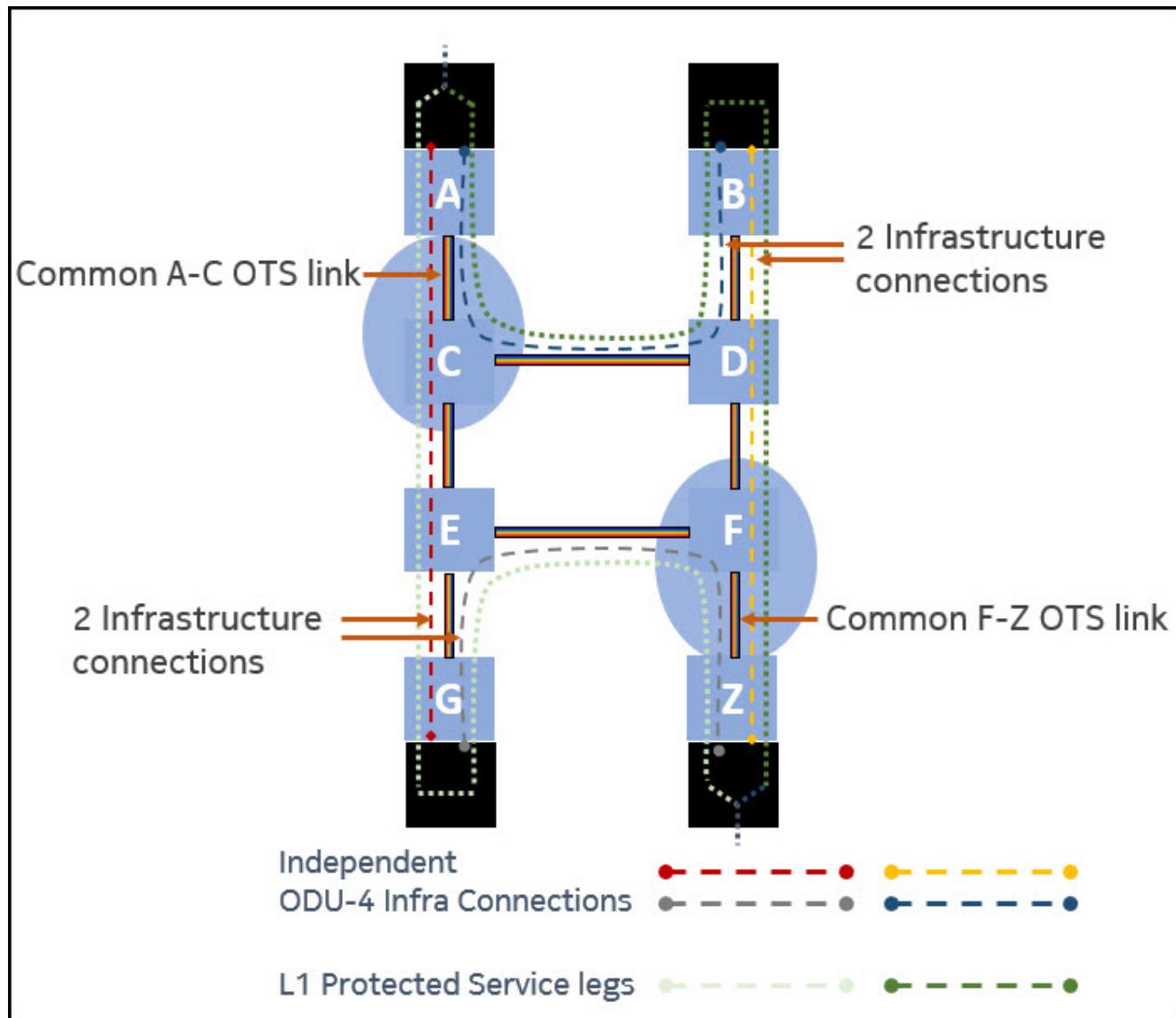
The following [Figure 7-51, “Infrastructure trail links” \(p. 784\)](#) displays the service to reach node 3, the OTS link between node 2 and node 3 can be reused if **Enforce Physical Link Diversity** is disabled for that link.

Figure 7-51 Infrastructure trail links



The following [Figure 7-52, “Reuse of OTS link during automatic routing of a service” \(p. 786\)](#) represents a protected service with different infrastructure connections and reuse of OTS link during automatic routing of a service.

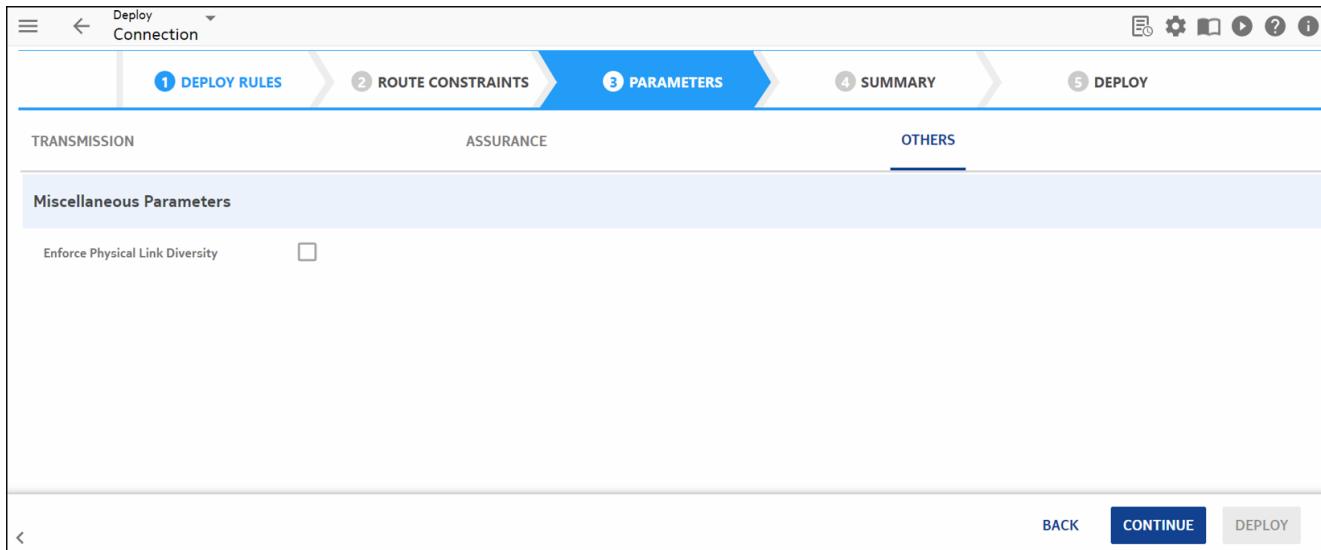
Figure 7-52 Reuse of OTS link during automatic routing of a service



Note: The A-C and F-Z links are reused by both the working and protection legs. In addition, for the working leg, the E-G link is common to both A-C-E-G and G-E-F-Z. For the protection leg, the B-D link is common to both A-C-D-B and B-D-F-Z.

In the **PARAMETERS** tab, disable the **Enforce Physical Link Diversity** field for reusing the OTS link.

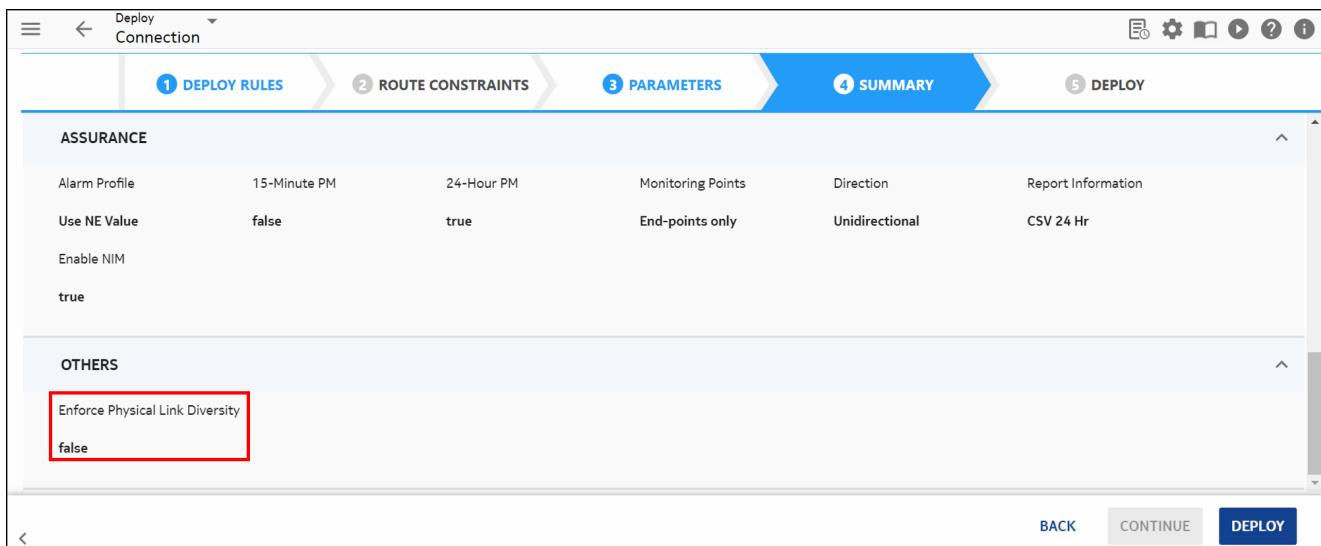
Figure 7-53 Parameters - Enforce Physical Link Diversity



By default, **Enforce Physical Link Diversity** parameter is enabled.

If the **Enforce Physical Link Diversity** is false, then the service and protected paths reuse the OTS link.

Figure 7-54 Enforce Physical Link Diversity - false



Task: Create a 4-ended OTS or OPS physical connection

Complete the following steps to create a 4-ended OTS or OPS connection.

1

From the NFM-T GUI, follow this navigation path:

Use the following navigation paths to open create/deploy physical connections page:

OPERATE > Physical Connections. Click create icon.

DEPLOY > New OTN Physical Connection

Result: The system displays the Physical Connection Creation window, which defaults to an OTS physical connection.

i Note: For the Uni-directional 3R Regen (cluster) and Uni-directional 3R Regen (dangling OT) configurations, port being used should be placed in Regen mode.

Figure 7-55 Physical Connections – physical connection creation window – default

The screenshot shows the 'Deploy PhyConnection' window with the 'DEPLOY RULES' tab selected. The 'END POINTS' section contains fields for 'Physical Link Type' (OTS), 'Connection Type' (Bidirectional), and search boxes for 'A Node', 'A Port', 'Z Node', and 'Z Port'. The 'CONNECTION CHARACTERISTICS' section includes fields for 'User Label', 'Span Type' (Dual Fiber), and 'Grid Type' (Standard). At the bottom right, there are 'BACK', 'CONTINUE', and 'DEPLOY' buttons.

2

Select the OTS and OPS links in **Physical Link Type** field, as following:

- For OTS **Physical Link Type** select **OTS** as **Physical Link Type** and select **2 Ended split bi** from the **Connection Type** drop-down list.
- For OPS **Physical Link Type** select **OPS** as **Physical Link Type** and select **2 Ended split bi** from the **Connection Type** drop-down list.

Result: The system activates additional **2 Ended split bi** specific-panels for OTS or OPS Physical Link Type.

Figure 7-56 Physical Connections – physical connection creation window – 2 Ended split bi OTS

The screenshot shows the 'Deploy New Physical Connection' interface. The top navigation bar includes icons for back, forward, search, and settings. Below the bar, a progress bar indicates four steps: 1. DEPLOY RULES (highlighted in blue), 2. PARAMETERS, 3. SUMMARY, and 4. DEPLOY. The main area is divided into sections: 'END POINTS' and 'CONNECTION CHARACTERISTICS'. In the 'END POINTS' section, 'Physical Link Type' is set to 'OTS' and 'Connection Type' is set to '2 Ended split bi'. Under 'A Node', 'A Sink', and 'A Source', there are search input fields. Similarly, under 'Z Node', 'Z Source', and 'Z Sink', there are search input fields. In the 'CONNECTION CHARACTERISTICS' section, 'User Label' is empty, 'Span Type' is set to 'Dual Fiber', and 'Grid Type' is set to 'Standard'. At the bottom right, there are buttons for 'BACK', 'CONTINUE' (highlighted in blue), and 'DEPLOY'.

Figure 7-57 Physical Connections – physical connection creation window – 2 Ended split bi OPS

The screenshot shows the 'New Physical Connection' creation window. The top navigation bar includes 'Deploy' and 'New Physical Connection'. Below it, a progress bar shows steps 1 through 4: 1 DEPLOY RULES (highlighted in blue), 2 PARAMETERS, 3 SUMMARY, and 4 DEPLOY.

END POINTS

- Physical Link Type: OPS
- Connection Type: 2 Ended split bi
- Interface type: NNI
- Client Signal Type: -
- * A Node: Search field
- * A Sink: Search field
- * A Source: Search field
- * Z Node: Search field
- * Z Source: Search field
- * Z Sink: Search field

CONNECTION CHARACTERISTICS

Define the connection details:

- User Label: Search field
- Grid Type: Standard
- Cluster-Link: Check box

Buttons at the bottom right: BACK, CONTINUE (highlighted in blue), and DEPLOY.

3

For 2 Ended split bi OTS connection:

- In the **END POINTS** panel, select **A Node**, **Z Node**, **Sink** and **Source** ports.
- In the **CONNECTION CHARACTERISTICS** panel, enter **User Label**, select **Span Type** and **Grid Type**.

Optional: For the **User Label** field, see [7.19.9 “Physical connection User Label” \(p. 804\)](#).

Click **CONTINUE**.

Result: The **PARAMETERS** section is displayed.

4

For 2 Ended split bi OPS connection:

- In the **END POINTS** panel, select **A Node**, **Z Node**, **Sink** and **Source** ports.
- In the **CONNECTION CHARACTERISTICS** panel, enter **User Label**, select **Grid Type**. For cluster connections, select the **Cluster-Link** check box.

- For **A Node** and **Z Node** type selected as external nodes, **User Label for New Port** parameter configuration is mandatory.

i Note: For the OPS 2 Ended split bi connection:

- From R21.4 onwards, the option to select Client Signal rate is available in **Client Signal Type** drop-down options under **DEPLOY RULES** section.
- The Interface Type is selected by default as **NNI**, no other interface type is supported.

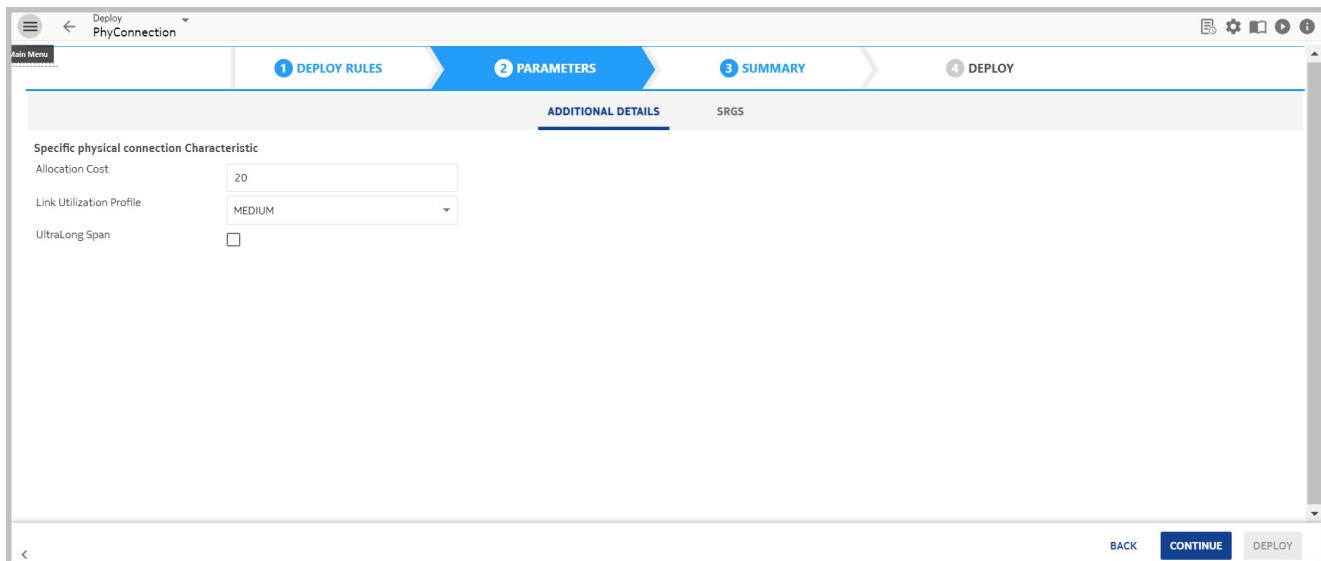
Click **CONTINUE**.

Result: **PARAMETERS** section is displayed.

5

In the **ADDITIONAL DETAILS** panel under **PARAMETERS** section, configure **Allocation Cost**, **Link Utilization Profile**, and **UltraLong Span**.

Figure 7-58 ADDITIONAL DETAILS



For **Allocation Cost**, the values range from **0** to **100,000**. If the link is already added to NPA, then you cannot modify the **Allocation Cost** value in physical connection. There is no NE version check for **Allocation Cost** value during physical link creation. The default is **20**.

Optional, applicable for OTS connections only: In the **ADDITIONAL DETAILS** panel, select the **Link Utilization Profile** from the drop-down. The default value is **MEDIUM**.

To know more about Link Utilization Profiles, see [22.1 “Link Utilization Profile” \(p. 1959\)](#).

Select **UltraLong Span** by selecting the check box.

i Note: For OPS 2 ended split bi connections, only **Allocation Cost** field is available.

6

In the **SRGS** tab, select the SRG(s) to be associated to the physical connection and click **SELECT**.

Figure 7-59 SRGs

The screenshot shows the 'Deploy PhyConnection' wizard. The current step is 'SRGS'. The interface includes tabs for Deploy Rules, Parameters, Summary, and Deploy. Below the tabs is an 'ADDITIONAL DETAILS' section. The main area is titled 'Select the SRG(s) which will be associated to the physical connection under creation'. It contains a table with columns: Name, SRG Type, SRG Probability, and Comment. A checkbox column is present. One row is selected: SRG1 (Cable, high probability, comment 'test'). Other rows include SRG3 (Physical Connection, high probability, comment 'test3'), SRG2 (Cable, low probability, comment 'test1'), and SRG4 (Conduit, high probability, comment 'test4'). At the bottom left is a note: 'Last Update: 3/6/2021 4:33:07 PM' and 'Total: 4'. On the right is a 'SELECT' button. Below this is a 'Selected SRG(s)' section with a table showing the same data as the main table but with a different selection state. At the bottom are buttons for BACK, CONTINUE (highlighted in blue), and DEPLOY.

i Note: Remove the selected SRG(s) by selecting the SRG(s) and clicking **REMOVE** .

Result: The selected SRG(s) are displayed in the **Selected SRG(s)** in the lower panel.

7

Click **CONTINUE**.

Result: The **SUMMARY** section is displayed

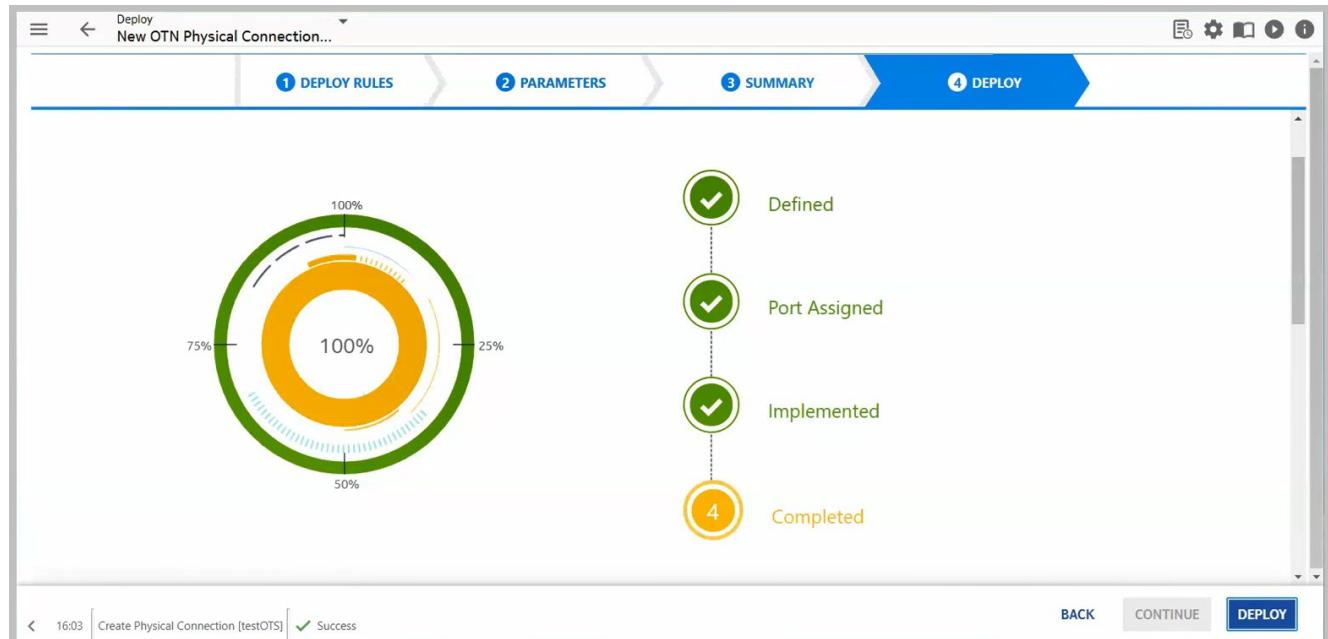
8

Verify the connection parameters in the **SUMMARY** section and click **DEPLOY**.

Result: The **DEPLOY** section is displayed.

As the deployment progresses, the progress bar increases in percentage and the states move from Defined > Port Assigned > Implemented > Completed. Once the deployment is successful a success message is displayed at the bottom of the section.

Figure 7-60 DEPLOY



END OF STEPS

Task: Create an Bidirectional physical OTS or OPS connection

Important! When the network involves 1830 PSS-24X as a cluster NE with an SWDM node, OPS bidirectional physical link between the uplink card and the add-drop block must be created with **Interworking Tech** parameter configured as **None**, **Connection Type** as **Bidirectional**, and **WDM Connection Type** as **OPS**.

Complete the following steps to create an bidirectional physical OTS or OPS connection:

1

From the NFM-T GUI, follow this navigation path:

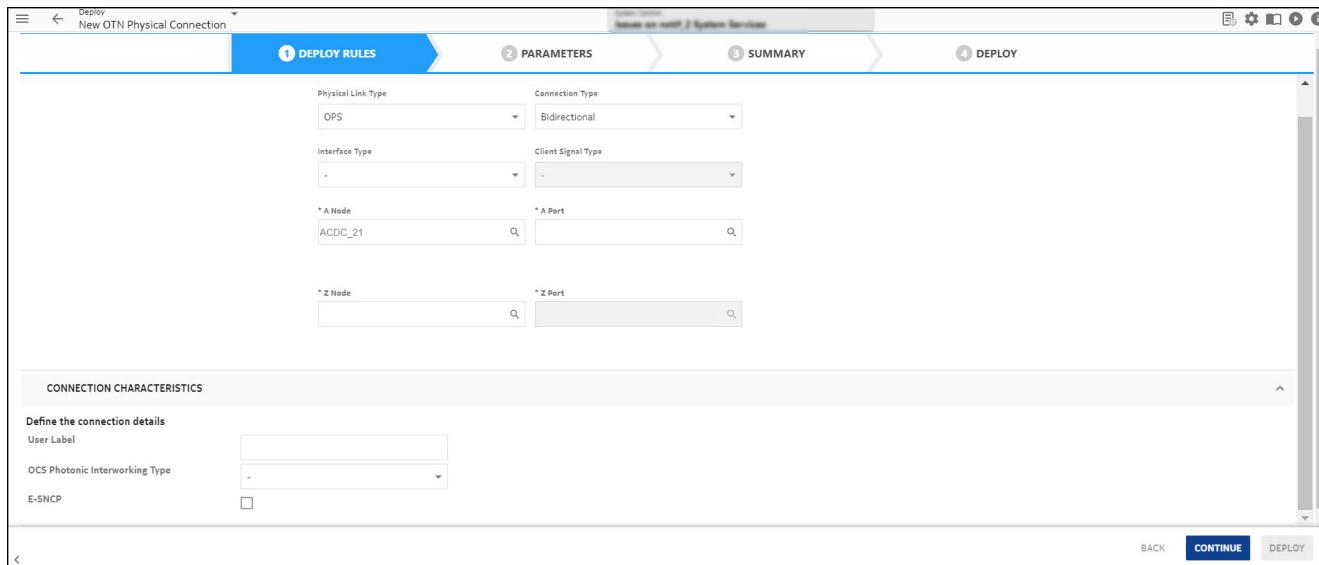
Use the following navigation paths to open create/deploy physical connections page:

OPERATE > Physical Connections. Click create icon.

DEPLOY > New OTN Physical Connection

Result: The system displays the **New OTN Physical Connection** window.

Figure 7-61 New OTN Physical Connection window- Bidirectional physical connection



2

In the **Connection Type** field, select **Bidirectional** from the drop-down list.

Result: The system defaults to an OPS physical connection and activates additional **Unidirectional** specific-panels.

3

If the **Physical Link Type** is **OPS**, go to [Step 4](#).

If the **Physical Link Type** is **OTS**, go to [Step 6](#).

4

In the **Interface Type**, select - (the default, which is not applicable or unknown), **NNI**, **UNI_SDH**, **UNI SONET**, **UNI-Ethernet**, **UNI-miscellanea**, **UNI-CPRI** or **UNI-OBSI**.

Result: The system activates the appropriate **Client Signal Type** depending on your selection.

5

Selecting the type of interface between available choices, the **Client Signal Type** field changes accordingly.

In the **Client Signal Type** field, select - (the default, which is not applicable or unknown) or the specific signal type for your installation:

- **NNI** client interface types include various OTUx client signal types along with **OTSi** for ADD4
- **UNI_SDH** client interface types include various STMx client signal types.

- **UNI SONET** client interface types include various OCx client signal types.
- **UNI-Ethernet** client interface types include various E, FE, GbE, or GB E Ethernet client signal types.
- **UNI-miscellanea** client interface types include various FCx, CBRx, GFCE, DVBASI, SHDSI, HDSI, FICON, DV_SDI, or DV-ASI client signal types.
- **UNI-CPRI** client interface types include various CPRI Rate1 to CPRI Rate 7 client signal types.
- **UNI-OBSAI** client interface types include various OBSAI Rate1, Rate 2, Rate 4 and Rate 8 client signal types.

i **Note:** When the **Interface Type** selected is **NNI**, **OTSi** is populated in the list of options for the **Client Signal Type**.

OTSi is supported for the following scenarios:

- ADD4 line port and filter (both cluster and dangling)
- Two ADD4 line ports
ADD4 client port supports only OTU4 when interworking with ENE.

Provisioning Note: The cards that support OTU2 rate only at Line side (i.e 11QPA4), has at Client side a provisioned bit rate of 10709 by default. The client bit rate can be changed during the OPS creation selecting OUT2 (11.049/OTU1e) or OTU2 (11.096/OTU2e) from the Client Signal Type field.

- 6 _____
Search and select values for **A Node** and **A Port**.
- 7 _____
Search and select values for **Z Node** and **Z Port**.
- 8 _____
Optional: For the **User Label** field, see [7.19.9 “Physical connection User Label” \(p. 804\)](#).
- 9 _____
If the **Physical Link Type** is **OTS**, then in the **Span Type** field select the type of the configuration fiber which can be *Dual Fiber* or *Single Fiber* and in the **Grid Type** field select *Standard* or *1.25GHz*.
- 10 _____
If the **Physical Link Type** is **OPS**, then in the **OCS Photonic Interworking Type** field select *OVERLAY* or *DROP* and select the check box for *E-SNCP* if it is applicable.
- 11 _____
Click **CONTINUE**.
Result: The **PARAMETERS** section is displayed.

12

In the **ADDITIONAL DETAILS** tab under **PARAMETERS** section, enter a value for **Allocation Cost**.

For **Allocation Cost**, the values range from **0** to **100,000**. If the link is already added to NPA, then you cannot modify the **Allocation Cost** value in physical connection. There is no NE version check for **Allocation Cost** value during physical link creation. The default is **20**.

13

In the **SRGS** tab under **PARAMETERS** section, select the SRG(s) to be associated to the physical connection and click **SELECT**.



Note: You can also remove the selected SRG(s) by selecting the SRG(s) and clicking **REMOVE**.

Result: The selected SRG(s) are displayed in the **Selected SRG(s)** in the lower panel.

14

Click **CONTINUE**.

Result: The **SUMMARY** section is displayed.

15

Verify the connection parameters in the **SUMMARY** section and click **DEPLOY**.

Result: The **DEPLOY** section is displayed.

As the deployment progresses, the progress bar increases in percentage and the states move from Defined > Port Assigned > Implemented > Completed. Once the deployment is successful a success message is displayed at the bottom of the section.

END OF STEPS

Task: Create an OTN Y-Cable physical connection

Complete the following steps to create a Y-Cable physical connection.

1

From the NFM-T GUI, follow this navigation path:

Use the following navigation paths to open create/deploy physical connections page:

OPERATE > Physical Connections. Click create icon.

DEPLOY > New OTN Physical Connection

Result: The system displays the **New OTN Physical Connection** window.

2

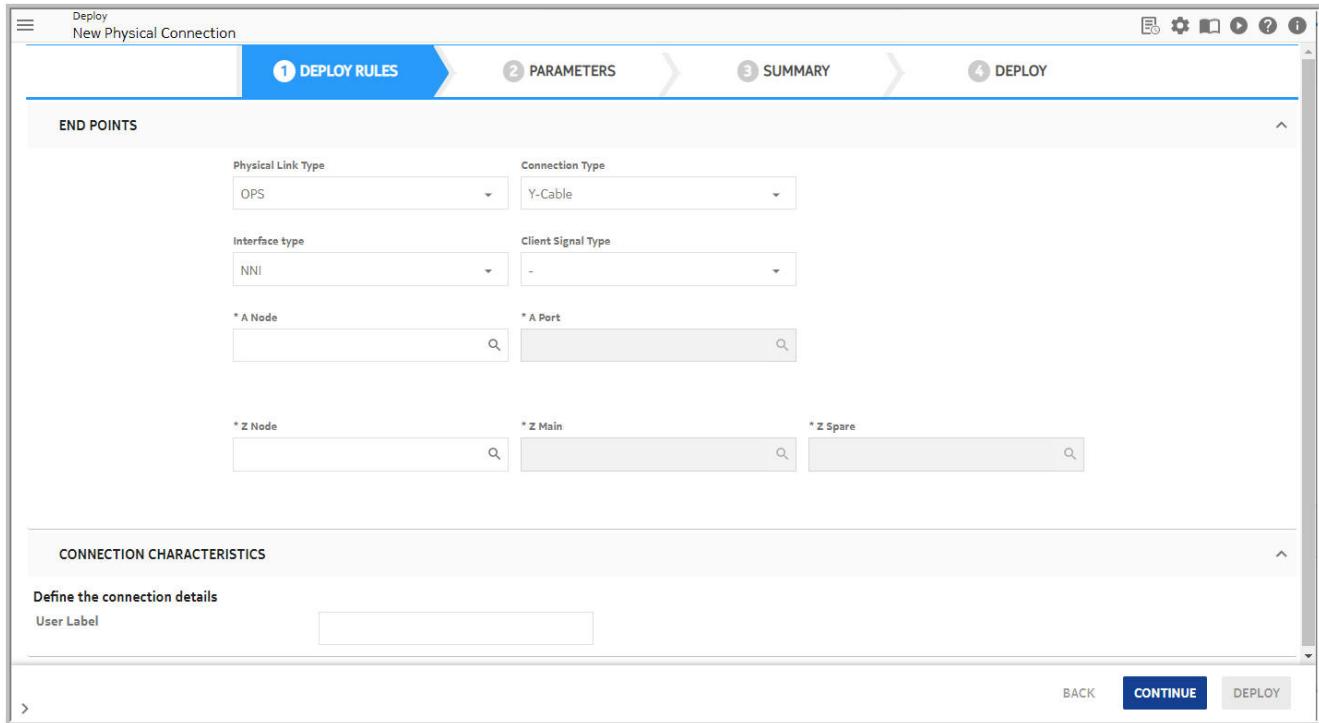
In the **Physical Link Type** field, select **OPS** from the drop-down list.

3

In the **Connection Type** field, select **Y-Cable** from the drop-down list.

Result: The system activates the additional Y-Cable specific-fields.

Figure 7-62 New OTN Physical Connection window Y-Cable



4

In the **Interface Type** field, select **NNI**, **UNI_SDH**, **UNI SONET**, **UNI-Ethernet**, **UNI-miscellanea**, **UNI-CPRI** or **UNI-OBSI**.

5

Depending on the **Interface Type** that you selected, select the appropriate the **Client Signal Type** from the drop-down menu.

Provisioning Note: The cards that support OTU2 rate only at Line side (such as 11QPA4), has at Client side a provisioned bit rate of 10709 by default. The client bit rate can be changed during the OPS creation selecting OUT2 (11.049/OTU1e) or OTU2 (11.096/OTU2e) from the Client Signal Type field.

6

Search and select values for **A Node** and **A Port**.

7 Search and select values for **Z Node** and **main** and **spare** port. The specific cards applicable for Y-Cable connection are displayed.

8 *Optional:* For the **User Label** field, see [7.19.9 “Physical connection User Label” \(p. 804\)](#).

9 Click **CONTINUE**.
Result: System displays **PARAMETERS** section.

10 In the **ADDITIONAL DETAILS** tab under **PARAMETERS** section, configure **Allocation Cost**.
For **Allocation Cost**, the values range from **0** to **100,000**. If the link is already added to NPA, then you cannot modify the **Allocation Cost** value in physical connection. There is no NE version check for **Allocation Cost** value during physical link creation. The default is **20**

11 In the **SRGS** tab under **PARAMETERS** section, select the SRG(s) to be associated to the physical connection and click **SELECT**.
Result: The selected SRG(s) are displayed in the **Selected SRG(s)** in the lower panel. The user also has the option to create an SRG.

12 Click **Continue**.
Result: System displays **SUMMARY** tab.

13 Verify the connection parameters in the **SUMMARY** section and click **DEPLOY**.
Result: The **DEPLOY** section is displayed.
As the deployment progresses, the progress bar increases in percentage and the states move from Defined > Port Assigned > Implemented > Completed. Once the deployment is successful a success message is displayed at the bottom of the section.

END OF STEPS

Task: Create an OTN UNI IETF physical connection

Complete the following steps to create a UNI IETF physical connection between Switch Router ENE and edge nodes of GMRE-managed network. The user can create a link between the router ENE port and the client port of edge node in GMRE-managed network if the user has selected **ASON Client ENE** in the Nodes window.

1

From the NFM-T GUI, follow this navigation path:

Use the following navigation paths to open create/deploy physical connections page:

OPERATE > Physical Connections. Click create icon.

DEPLOY > New OTN Physical Connection

Result: The system displays the **New OTN Physical Connection** window.

2

In the **Physical Link Type** field, select **OPS** from the drop-down list.

3

In the **Connection Type** field, select **Bidirectional** from the drop-down list.

Result: The system enables the following fields: **Interface Type**, **Client Signal Type** and **OCS-Photonic Interworking Type**.

Figure 7-63 New OTN Physical Connection window

The screenshot shows the 'New OTN Physical Connection' window in the Nokia NFM-T GUI. The window has a header with tabs: 1 DEPLOY RULES (selected), 2 PARAMETERS, 3 SUMMARY, and 4 DEPLOY. The main area contains several input fields and dropdown menus. Under 'DEPLOY RULES', there are fields for 'Physical Link Type' (set to 'OPS'), 'Connection Type' (set to 'Bidirectional'), 'Interface Type' (dropdown menu), 'Client Signal Type' (dropdown menu), and search fields for 'A Node' (containing 'ACDC_21') and 'A Port'. Under 'CONNECTION CHARACTERISTICS', there are fields for 'User Label' (dropdown menu), 'OCS Photonic Interworking Type' (dropdown menu), and 'E-SNCP' (checkbox). At the bottom right, there are buttons for 'BACK', 'CONTINUE', and 'DEPLOY'.

4

In the **Interface Type**, select **UNI-Ethernet** from the drop-down list.

5

In the **Client Signal Type**, select, for example, **Ethernet 10 GB E** from the drop-down list.

-
- 6 Search and select values for **A Node** and **A Port**.
- 7 Search and select values for **Z Node** and **Z Port**.
- 8 *Optional:* For the **User Label** field, see [7.19.9 “Physical connection User Label” \(p. 804\)](#).
- 9 Select **OVERLAY** or **DROP** in the **OCS Photonic Interworking Type** field and select the check box for *E-SNCP* if it is applicable.
- 10 Click **CONTINUE**.
Result: The **PARAMETERS** section is displayed.
- 11 In the **ADDITIONAL DETAILS** tab under **PARAMETERS** section, enter a value for **Allocation Cost**.
For **Allocation Cost**, the values range from **0** to **100,000**. If the link is already added to NPA, then you cannot modify the **Allocation Cost** value in physical connection. There is no NE version check for **Allocation Cost** value during physical link creation. The default is **20**
- 12 In the **SRGS** tab under **PARAMETERS** section, select the SRG(s) to be associated to the physical connection and click **SELECT**.
Note: You can also remove the selected SRG(s) by selecting the SRG(s) and clicking **REMOVE**.
Result: The selected SRGs are displayed in the **Selected SRG(s)** in the lower panel.
- 13 Click **CONTINUE**.
Result: The **SUMMARY** section is displayed.
- 14 Verify the connection parameters in the **SUMMARY** section and click **DEPLOY**.
Result: The **DEPLOY** section is displayed.

As the deployment progresses, the progress bar increases in percentage and the states move from Defined > Port Assigned > Implemented > Completed. Once the deployment is successful a success message is displayed at the bottom of the section.

END OF STEPS

Task: Create an OTN OPS physical connection for packet switch

The packet cards (12CE120, 12CE121) interwork with uplink cards (1UD200, 20P200, and S13X100R/S13X100E) in a packet switch configuration. 1CE100 and 1CE100Q interwork with 1UD200, 20P200, and S13X100R uplink cards. Packet switch is a grouping of packet and uplink cards where they together behave as a logical single card. The packet switch is created from ESM, and each packet switch is associated with a packet switch ID.

Complete the following steps to create a OPS Physical Connection for Packet Switch.

1

From the NFM-T GUI, follow this navigation path:

Use the following navigation paths to open create/deploy physical connections page:

OPERATE > Physical Connections. Click create icon.

DEPLOY > New OTN Physical Connection

Result: The **New OTN Physical Connection** window is displayed.

2

In the **Physical Link Type** field, select *OPS* from the drop-down list.

3

In the **Connection Type** field, select *Bidirectional* from the drop-down list.

Result: The system enables the following fields: **Interface Type,, Client Signal Type, OCS-Photonic Interworking Type.**

Figure 7-64

The screenshot shows the 'New OTN Physical Connection' deployment wizard. Step 1: DEPLOY RULES. Physical Link Type: OPS; Connection Type: Bidirectional; Interface Type: dropdown; Client Signal Type: dropdown; * A Node: ACDC_21; * A Port: dropdown; * Z Node: dropdown; * Z Port: dropdown. Step 2: PARAMETERS. CONNECTION CHARACTERISTICS: User Label: dropdown; OCS Photonic Interworking Type: dropdown; E-SNCP: checkbox. Buttons: BACK, CONTINUE (highlighted in blue), DEPLOY.

4

In the **Interface Typefield**, select *NNI* from the drop-down list.

5

In the **Client Signal Type** field, select the respective signal type from the drop-down list:

- **OTU2WANETH**
- **OTU4WANETH**
- **OTU4**
- **OTU2e**

i Note: For S13X100R/E card, the **Client Signal Type** applicable is OTU4 and OTU2e. For a 10GBE and 100GBE service, the signal rate is displayed as DSR.

If the **Interface Type** is UNI-Ethernet, then the **Client Signal Type** applicable are eth10GbE_LanEth, eth1GbE_LanEth, eth100GbE_LanEth.

When S13x100R/E card is used in a packet switch configuration, OTN does not create a DSR connection or link automatically. The user has to create a service on top of the Infrastructure connection for S13X100R/E. When the service is created on top of an infrastructure connection, the **Service Type** should be displayed as **DSR** for both 10GBE and 100GBE service. The same will be exported to **Carrier Ethernet Links** page in ESM. Ethernet Mode should be Access-Uplink for all L2 Packs. The user can modify the port in EQM to set the Ethernet Mode to "Access-Uplink".

-
- 6 Search and select values for **A Node** and **A Port**.
- 7 Search and select values for **Z Node** and **Z Port**.
- 8 *Optional:* For the **User Label** field, see [7.19.9 “Physical connection User Label” \(p. 804\)](#).
- 9 Select **OVERLAY** or **DROP** in the **OCS Photonic Interworking Type** field and select the check box for *E-SNCP* if it is applicable.
- 10 Click **CONTINUE**.
Result: The **PARAMETERS** sections is displayed.
- 11 In the **ADDITIONAL DETAILS** tab under **PARAMETERS** section, enter a value for **Allocation Cost**.
For **Allocation Cost**, the values range from **0** to **100,000**. If the link is already added to NPA, then you cannot modify the **Allocation Cost** value in physical connection. There is no NE version check for **Allocation Cost** value during physical link creation. The default is **20**
- 12 In the **SRGS** tab under **PARAMETERS** section, select the SRG(s) to be associated to the physical connection and click **SELECT**.
Note: You can also remove the selected SRG(s) by selecting the SRG(s) and clicking **REMOVE**.
Result: The selected SRGs are displayed in the **Selected SRG(s)** in the lower panel.
- 13 Click **CONTINUE**.
Result: System displays **SUMMARY** tab.
- 14 Verify the connection parameters in the **SUMMARY** section and click **DEPLOY**.
Result: The **DEPLOY** section is displayed.
As the deployment progresses, the progress bar increases in percentage and the states move from **Defined** > **Port Assigned** > **Implemented** > **Completed**. Once the deployment is successful a success message is displayed at the bottom of the section.



Note: If the **Client Signal Type** is WANETH, the OTN automatically creates a DSR connection and the links are exported to ESM (Operate > Carrier Ethernet Links > OTN) to create Ethernet connections.

If the **Client Signal Type** is LANETH, then the same OPS connections are exported to ESM (Operate > Carrier Ethernet Links > Physical) to create Ethernet Connections.

When a S13X100R/E uplink card is used in a packet switch configuration, OTN does not automatically create a DSR connection or link. The user has to create another service on top of the Infrastructure connection. When the service is created on top of an infrastructure connection, OTN automatically creates a DSR connection that is exported to ESM to further create Ethernet Services. For more information on how to Deploy an infrastructure connection, see [7.12 “Deploy a template to make a connection” \(p. 754\)](#).

For S13X100R/E card, the **Client Signal Type** applicable is OTU4 and OTU2e. For a 10GBE and 100GBE service, the signal rate is displayed as DSR.



Note: OPS connection between L1 CPPSS-16II using the '16DC65T' pack (packs supporting WSTS) and ENE' is not supported in the control panel enabled node.

END OF STEPS

Physical connection User Label

The **User Label** field, contains a name to identify the connection.

In the **User Label** field, the user can enter the desired user label or the field can be left blank, it is not mandatory to fill it. In case it is left blank, the system generates the name automatically when the connection is deployed.

Inserted User Label

In the **User Label** field, enter a name to identify the connection.

Provisioning Note: The valid characters that you can enter for the **User Label** are the following:

Alphanumeric characters **0-9**, **a-z**, and **A-Z** along with these special characters:

space, **!**, **@**, **#**, **\$**, **&**, *****, **(**, **)**, **-**, **_**, **+**, **=**, **{**, **}**, **[**, **]**, **:**, **;**, **<**, **>**, **,**, **,**, **/**, and **?**

The special character **%** is not supported.

NFM-T does not support UTF-8 encoding for the **User Label** field.

System generated User Label

The **User Label** field of the physical connection, that is the Connection Name, can be left blank, it is not mandatory to fill it.

The generated name is composed as follows:

`<NE Name>/<A Port Label>/<Z Port Label> [#<next available number>]`

Rules followed to generate the physical connection User Label:

- The User Label is generated if the field is empty, contains all white spaces, or null.

-
- In case of bidirectional physical connection the user label is generated using the A Port Label – Z Port Label; in case of Four ended Physical connection the generation uses A2 Port Label – Z2 Port Label.

Note: This user label format is the same used during discovery of physical connection.

- User Label size limit is 130 characters.
- If the generated label is not unique, a number is appended at the end of generated label.

7.20 Manage the inventory view of Physical Connections

When to use

Use this task to view the list of OTN physical connections.

Overview

Inventory view on physical connections is enhanced so that users can manage user preference and list of attributes visible on the page. The new inventory view is equipped with multiple tabs. The user can customize filters. The main advantage of the enhanced view is that information is visible to the user and has adequate information required and avoids all unwanted information being displayed.

Task

Complete the following steps to display the list of physical connections:

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists the physical connections.

Figure 7-65 Connections- Physical Connections

Oper...	WDM Connection ...	Name	Shape	Implementation ...	Working State	From NE/Port #1	To NE/Port #1	Alarm Status
<input type="checkbox"/>	WDM Connection ...	OPS	OPS	Simple	Implemented	Normal	PSS32-45.212.242/S13X100-2-...	PSS32-45.212.243/S13X100-2-...
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM3_PSIM4_Direct_1	OPS	Simple	Implemented	Normal	SANITY_PSIM_NODE_3/PORT-1-1-L1	SANITY_PSIM_NODE_4/PORT-1-1-L1
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM3_PSIM4_Direct_2	OPS	Simple	Implemented	Normal	SANITY_PSIM_NODE_3/PORT-1-1-L2	SANITY_PSIM_NODE_4/PORT-1-1-L2
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM3_PSIM4_Direct_3	OPS	Simple	Implemented	Normal	SANITY_PSIM_NODE_3/PORT-1-3-L1	SANITY_PSIM_NODE_4/PORT-1-3-L1
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM3_PSIM4_Direct_4	OPS	Simple	Implemented	Normal	SANITY_PSIM_NODE_3/PORT-1-3-L2	SANITY_PSIM_NODE_4/PORT-1-3-L2
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_1	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_7/PORT-1-1-L1
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_2	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_6/PORT-1-1-L1
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_3	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_7/PORT-1-1-L2
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_4	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_6/PORT-1-1-L2
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_5	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_7/PORT-1-3-L1
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_6	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_6/PORT-1-3-L1
<input type="checkbox"/>	WDM Connection ...	OPS_PSIM_CDCF_Cluster_7	OPS	Simple	Implemented	Normal	SANITY_CDCF_ADD4_PSS_NODE_...	SANITY_PSIM_NODE_7/PORT-1-1-L1

2

From the **Select View** panel, select one of the following options to change the view.

View types	Sub types
OPERATIONAL STATE	<ul style="list-style-type: none">• ALL• DOWN• UP• DEGRADED
ALARM STATUS	<ul style="list-style-type: none">• ALL• PENDING• CRITICAL• MAJOR• MINOR• WARNING• INDETERM• CLEARED

CLIENT SIGNAL TYPE	<ul style="list-style-type: none"> • ALL • NOT PROVISIONED • OC-3 • OC-12 • OC-48 • OC-192 • OC-768 • OTU1 • OTU2 • OTU3 • OTU4 • ODU1 • ODU2 • ODU3 • ODU4 • FE • ETHERNET 1GBE • ETHERNET 10GBE • ETHERNET 10GBEW • ETHERNET 100GBE • ETHERNET E1 • STM-1 • STM-4 • STM-64 • STM-256 • FC 100 • FC 200
IMPLEMENTATION STATE	<ul style="list-style-type: none"> • ALL • DEFINED • IMPLEMENTED • DEIMPLEMENTED • PARTIALLY IMPLEMENTED

COMMISSIONED STATUS	<ul style="list-style-type: none">• ALL• NOT APPLICABLE• NOT COMMISSIONED• COMMISSIONED
WDM CONNECTION TYPE	<ul style="list-style-type: none">• ALL• OPS• OTS• OTSREG
ADMINISTRATIVE STATE	<ul style="list-style-type: none">• ALL• IN SERVICE• NOT IN SERVICE• MAINTENANCE

3

Optional: To view the details of a selected connection in the data table, refer to “[View additional attributes for a selected item in a data table](#)” (p. 2194).

4

Optional: To manipulate the view of the data table, refer to the following:

- “[Sort a single column in a data table](#)” (p. 2187)
- “[Manage the columns displayed in a data table](#)” (p. 2192)

5

Optional: To perform additional actions on a selected connection in the data table, refer to the following: “[Three dots more... icon](#)” (p. 2196).

6

Optional: To export the contents of the data table that is currently displayed to a .CSV file, refer to the [26.6 “Export a Data Table to a .csv File” \(p. 2209\)](#) task for detailed steps.

7

Optional: If you have customized the filters, sorting or column order in data table and you want to save the same and/or if you want to reset a customized view of the data table to its default display, refer to the [26.9 “Save or reset data table preferences on connections \(physical/infrastructure\) and services screen” \(p. 2220\)](#) task for detailed steps.

8

Optional: Click **MANAGE COLUMNS**  icon on top right corner to manage the columns in data table. See [7.21 “Manage data columns on Physical Connections page” \(p. 811\)](#) for more details.

END OF STEPS

7.21 Manage data columns on Physical Connections page

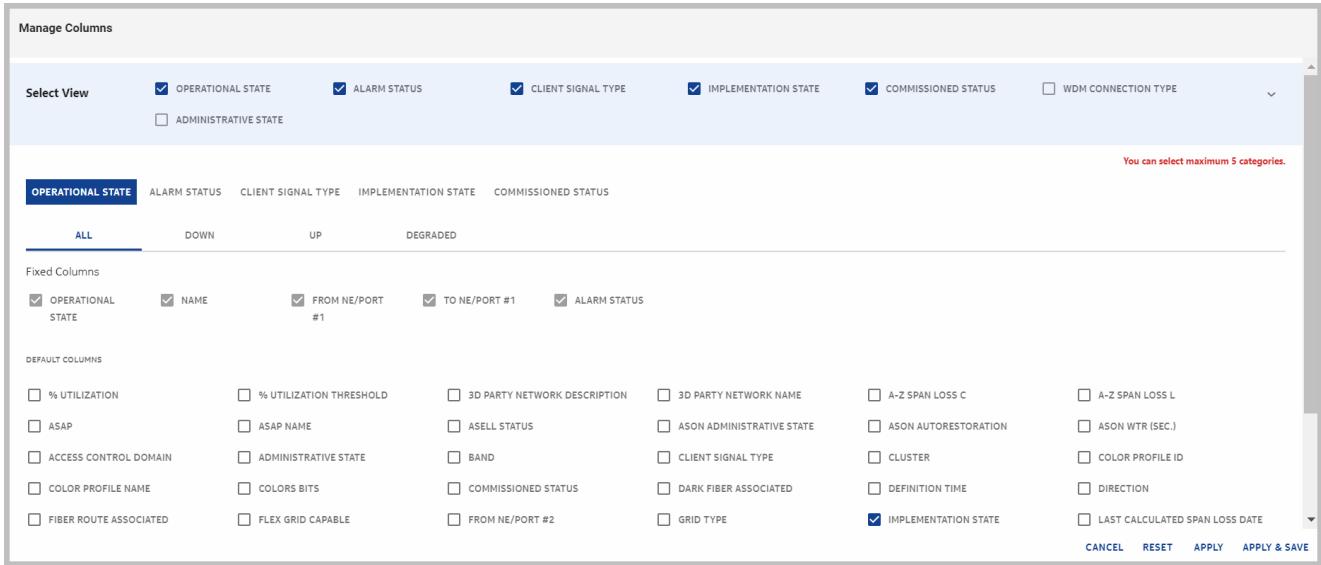
Task

1

Click **MANAGE COLUMNS**  icon on top right corner on **Physical Connections** page.

Result: The system displays **Manage Columns** page.

Figure 7-66 Physical connections- Manage Columns page



2

The user can choose maximum five out of seven view types in **Select View** panel.

Result: The system displays the chosen five view types as tabs under the **Select View** panel.

3

Click one of the view type tab.

Result: The system displays the fixed columns under **fixedColumns**. The system displays optional columns under sub type tab.

4

Click one of view sub type tab. Choose optional columns which shall appear on data table along with the fixed columns. See 7.44 “Physical Connections table columns” (p. 896) for more details on the attributes

5

Click **APPLY & SAVE** to save the changes and apply the modifications on data table in physical connections page. Alternatively, click **RESET** to rest all values to default or click **CANCEL** to return to physical connections page or click **APPLY** to return to physical connections page to view the changes made without saving the changes.

END OF STEPS

7.22 Delete an OTN physical connection

When to use

Use this task to delete (remove) an OTN physical connection.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

You can delete an OTN physical connection for the following types of connections by using the steps that are provided in this task:

- Physical connections
- PM enabled points of a selected physical connection
- Impacted connections for a selected physical connection
 - Impacted connections are those physical connections that are associated with a selected node and its current operational and alarm state
- Used ports for a selected physical connection
 - Used ports are those physical connections that are assigned to a port address on a selected node

You can also delete a physical connection from the following areas of the NFM-T GUI:

- From the **Physical Connections** tab of the Shared Risk Group data table; refer to the 6.13 “View tabbed topics for a Shared Risk Group” (p. 624) task for detailed steps.
- From the **Link Maintenance Window**; refer to the 10.25 “Perform link maintenance” (p. 1497) task for detailed steps.



Note:

For configurations involving PSI-M NEs, the client ports must be unassigned according to the mapping rules:

- C1, C2 → L1
- C3, C4 → L2

before attempting to **Delete an OTN Physical Connection** (OPS connection) between the line side of the DA2C4 and filter pack.

Task

Complete the following steps to delete/remove an OTN physical connection.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

OPERATE > Physical Connections > 360° View > PM Enabled Points (tab)

OPERATE > Physical Connections > 360° View > Structure (tab)

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Highlight and select the connection to remove:

- Click on the **More**  icon and follow this path: **Delete Connection**.

i Note: If the deletion request fails with the error message “One or more client ports are assigned” you will need to unassign the client ports before performing another deletion request.

i Note: For a Packet Switch configuration, the **Client Signal Type** supported are WANETH and LANETH. In case the **Client Signal Type** is WANETH, then the connection clients should be deleted first and then the physical connection.

i Note: When an OPS involving uplink cards is deleted, the signal type is not reset from the NFM-T. If a different signal rate is required (for example, to change the signal type from 100G to 200G) the user must delete and recreate the port.

Result: The system deletes/removes the physical connection from the data table.

END OF STEPS

7.23 Delete OTS and OPS connections from NFM-T

When to use

Use this task to delete the OTS and OPS connections from NFM-T database.

Related information

This function allows to delete from NFM-T database only the OTS or OPS connections made on an NE without de-configuring anything on the node.

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

To successfully remove the connection, no client services can be present.

Ensure the Services are deleted before removing the connection.

The **Delete from NFM-T** operation is supported on the following NE types:

- 1830 PSS PHN/OCS
- 1830 PSI (2T and M)
- 1830 PSD
- 7210 SASK
- WaveLite
- 1830 TPS

Task

Complete the following steps to delete from NFM-T database only the OTS or OPS connections made on NE.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

Result: The system displays the physical connection data table that lists all of the requested connections.

2

Highlight and select the connection that you want to delete the connections from the database and perform the following:

- Click on the **More**  icon and follow this path: **Deployment Control > Delete from NFM-T**.

A confirmation box is displayed, click on **OK** to confirm the deletion.

Result: The system deletes the connection (OTS or OPS) from the database.

This deletes the OPS/OTS physical connection from the NFM-T database and not from the NE. When there is a synchronization operation, the deleted connection is rediscovered from the NE by executing the external link discovery operation.



Important! For 1830 PSD 3-ended Virtual Service connection recreation, you must delete both the Network 1 and Network 2 OPS connections. After the deletion, recreate the OPS connections, and then create the service.

END OF STEPS

7.24 Associate/Disassociate dark fiber to physical connection

When to use

Use this task to associate or disassociate a dark fiber to a physical connection.

Related information

See “[Managing Dark Fibers](#)” (p. 1804).

Task

i **Note:** In NFM-T, a physical connection can be associated to only one dark fiber. The system permits to associate two or more physical links to a single dark fiber. However, when associating an OLP-OTS connection to a dark fiber, ensure not to associate both the working path and protection path to the same dark fiber.

Perform the following steps to associate or disassociate an OTS connection to a dark fiber:

1

From the NFM-T GUI follow the path **OPERATE > Physical Connections**.

Result: The system displays a data table with all the existing physical connections.

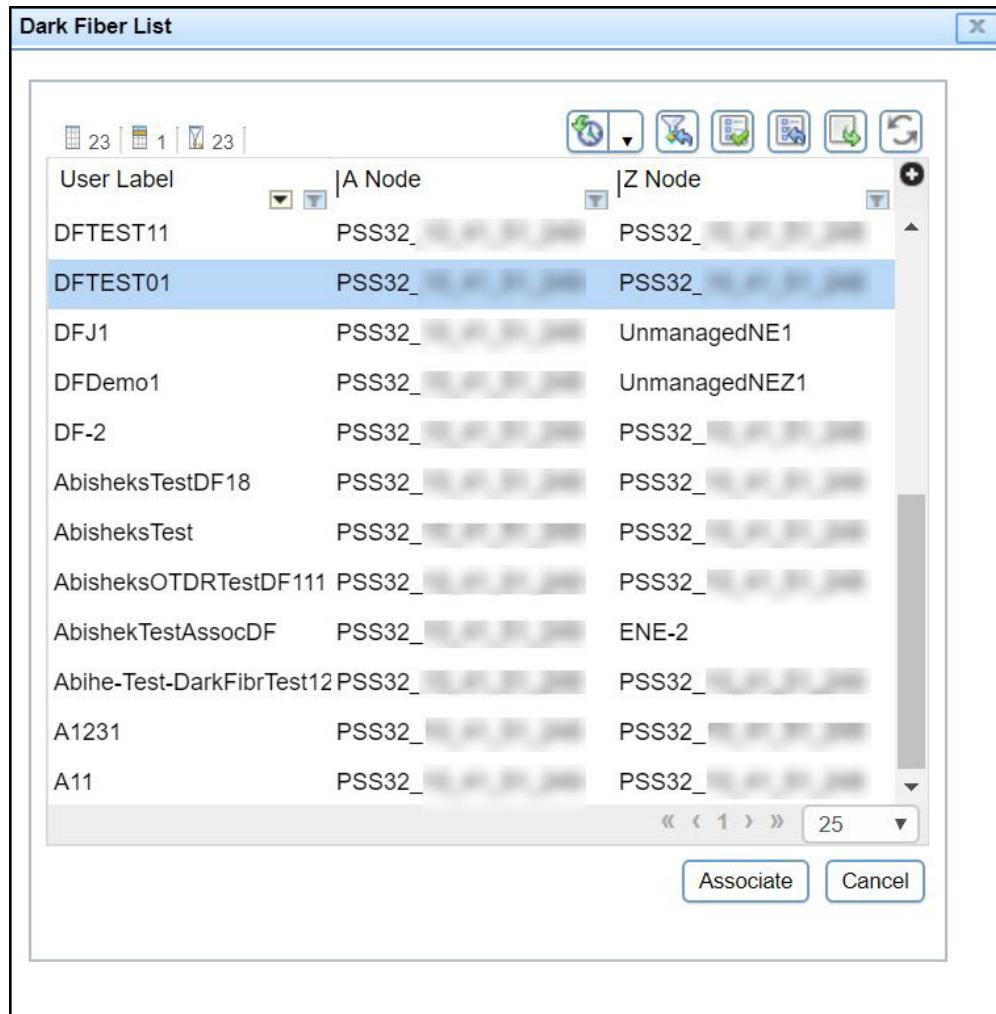
2

Select the connection in the list and click on the **More**  icon.

From the list of actions, select **Dark Fiber > Associate or Disassociate** as required.

Result: The **Dark Fiber List** window is displayed.

Figure 7-67 Dark Fiber List



Note: The **Dark Fiber** option is displayed only in the following conditions:

- If there is an existing dark fiber at the endpoints of the physical connection.
- The physical connection is not associated to an OTDR port.
- The physical connection is not already associated to a dark fiber.

3

Select the dark fiber and click **Associate**.

Result: The status bar displays the success of the association. The dark fiber is associated to the physical connection.

The associated dark fiber is displayed in the corresponding **Dark Fiber** tab of the **360° View** of the connection.

Figure 7-68 Dark Fiber tab

The screenshot shows the 'Dark Fiber' tab selected in the top navigation bar of the '360° View' window. The tab has a red border. Below the tabs, there is a toolbar with icons for notes, PM enabled points, fiber characteristics, end points, misalignment report, and dark fiber. The main area displays a table with two rows of data:

Name	From NE #1	From Port	To NE	To Port
Dark_fiber_with_ENE	Charan_ENE	FakePort_24	R199_OTN_DarkFiber_1	Fakeport_25



Note: A physical connection associated to a dark fiber can be deleted.

END OF STEPS

7.25 Configure alarms of an OTN physical connection

Purpose

Use the subtasks that are in this procedure to manage alarms for physical connections.

Correlate ASAPs to a Connection

By default, once a connection is created, it is assigned the default ASAP. You can correlate an ASAP to a connection from the data table of the connection. If you need to select multiple connections, correlate the same profile to all of the selected connections.

Enable Alarm Reporting

The **Enable Alarm Reporting** feature is based on the connection rate and the role of the port.

Task: Enable Alarm Reporting

The action is enabled only if the reporting is not enabled on the selected physical connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Physical Connections

OPERATE > Infrastructure Connections > 360° View > Clients (tab)

Result: Depending on your selection, the system displays a data table that lists all of the physical connections.

2

Click on the **More**  icon on the physical connection where you want to restore the alarm severities to NE/Node default and follow this path: **Alarms > Enable Alarm Reporting**.

Result: The system displays the message on the bottom part of the window that the request is submitted, and once the request is completed a success message is displayed.

Figure 7-69 Physical Connections – Enable Alarm Reporting Success Message



END OF STEPS

Task: Set Default ASAP

This task allows to restore the alarm severities to NE/Node defaults through ASAP.

The action is enabled only if the ASAP has been previously enabled on the physical connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Physical Connections

OPERATE > Infrastructure Connections > 360° View > Clients (tab)

Result: Depending on your selection, the system displays a data table that lists all of the physical connections.

2

Click on the **More**  icon on the physical connection for which you want to restore the alarm severities to NE/Node default and follow this path: **Alarms > Set Default ASAP**.

Result: The system displays the message on the bottom part of the window that the request is submitted, and once the request is completed a success message is displayed.

3

Once the status changes, refresh the page.

Result: The ASAP is restored to the alarm severities to NE/Node default for the selected connection.

On the NE as part of *Alarm level* Override Severity column values are assigned with **None** severity after the operation.

END OF STEPS

7.26 Configure the service state of an OTN physical connection

When to use

Use this task to configure the service state of an OTN physical connection.

Related information

See the following topics in this document:

- [2.15 “Physical connections” \(p. 220\)](#)

Before you begin

The physical connection to be set to *In Service* must currently be in a *Not In Service* state.

The physical connection to be set to *Not In Service* must currently be in an *In Service* state.

Each time that the service state of a physical connection is put **In Service** or **Not In Service**, the **Service State** column changes to reflect the change.

Note: **Service State** settings are displayed in the data tables for logical and physical connections. The meaning of the **Service State** column and its settings differs for logical and physical connections. For physical connections, the **Service State** column displays whether the connection is **Not in Service**, **In Service**, or **Maintenance**.

Task

Complete the following steps to configure the service state of an OTN physical connection.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

OPERATE > Physical Connections > 360° View > PM Enabled Points (tab)

OPERATE > Physical Connections > 360° View > Structure (tab)

Result: The system displays a data table that lists the OTN physical connections.

2

Highlight and select the connection for which you want to change the service state and click on the **More**  icon, then follow this path: **Deployment Control > Set Service State (in service)** or **Deployment Control > Set Service State (not in service)**.

Result: The system changes the **Service State** column in the data table to reflect the change.

END OF STEPS

7.27 Configure OLC State for connections and services

When to use

Use this procedure to configure OLC state of one or more physical connections, infrastructure connections, and services.

Task

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

OPERATE > Infrastructure Connections

OPERATE > Services

Result: A list of physical connections, infrastructure connections, or services opens based on the selection.

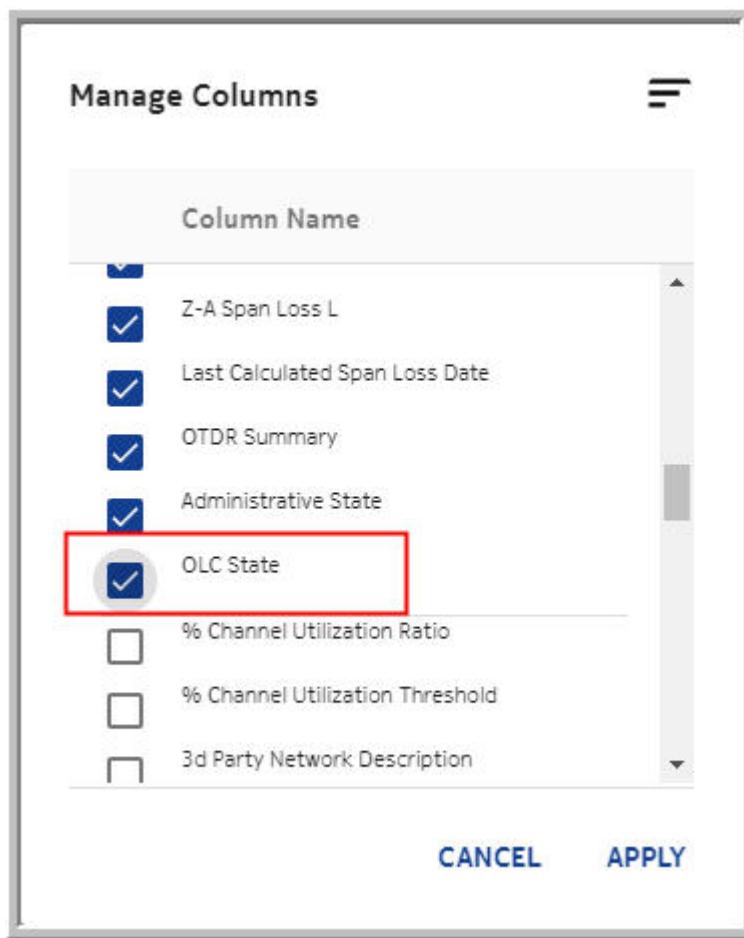
2

Select one or more connections or services from the list, click on the **More**  icon on the physical connection for which you want to set the state to maintenance and follow the path **OLC State > Set to Maintenance**.

Result: A success message appears in the status bar.

3

By default the **OLC State** column is hidden in the table of connections and services. On the top right corner of the table, click on the **More**  icon and select **Manage Columns**.



Result: The **Manage Columns** window is displayed.

4

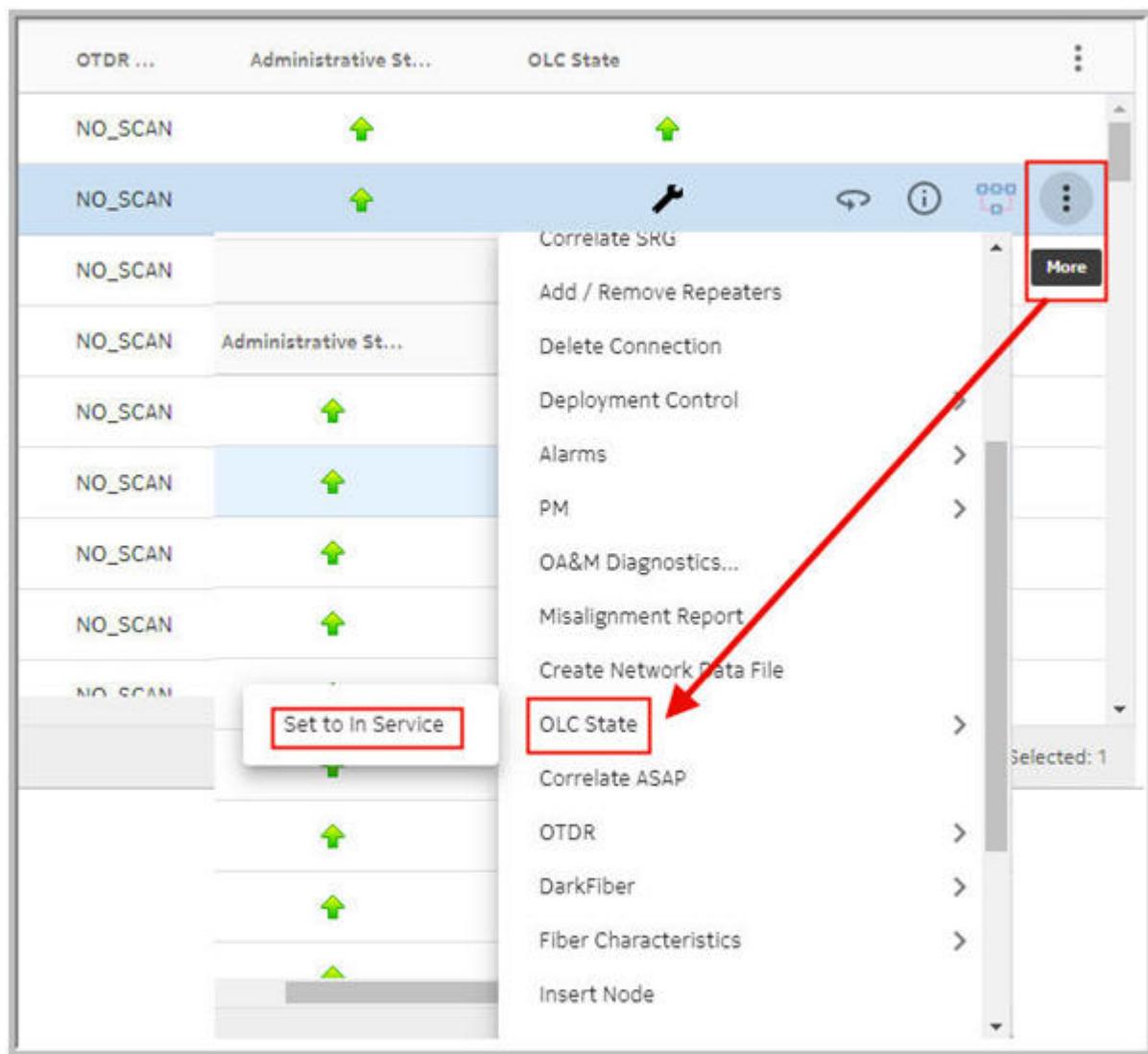
On the **Manage Columns** window, select **OLC State** from the list of columns to be displayed and select **APPLY**.

Result: The OLC State column is displayed with the status for the OLC state.



5

Select one or more connections or services from the list, click on the **More** icon and select **OLC State > Set to In Service** to set the connections or services back in service.



END OF STEPS

7.28 Correlate an OTN physical connection with an SRG

When to use

Use this task to correlate an OTN physical connection with a Shared Risk Group (SRG).

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)
- 6.6 “Correlate a SRG with a Physical Connection” (p. 610)

Before you begin

The SRG must already be created.

The OTN physical connection must belong to a **Defined** NPA. If the NPA is in the **Implemented** state, the operation is available on a TE-link and it will be applied to all physical connections inside the TE link.

Important! The physical connection or TE link that you correlate to one SRG can be correlated to another SRG; meaning, one physical link or one TE link can be correlated to multiple SRGs.

Correlate an OTN physical connection with a Shared Risk Group (SRG) for the following types of connections by using the steps that are provided in this task:

- Physical connections
- PM enabled points of a selected physical connection
- Impacted connections for a selected physical connection
 - Impacted connections are those physical connections that are associated with a selected node and its current operational and alarm state.
- Used ports for a selected physical connection
 - Used ports are those physical connections that are assigned to a port address on a selected node.

Task

Complete the following steps to correlate an OTN physical connection with a Shared Risk Group (SRG).

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

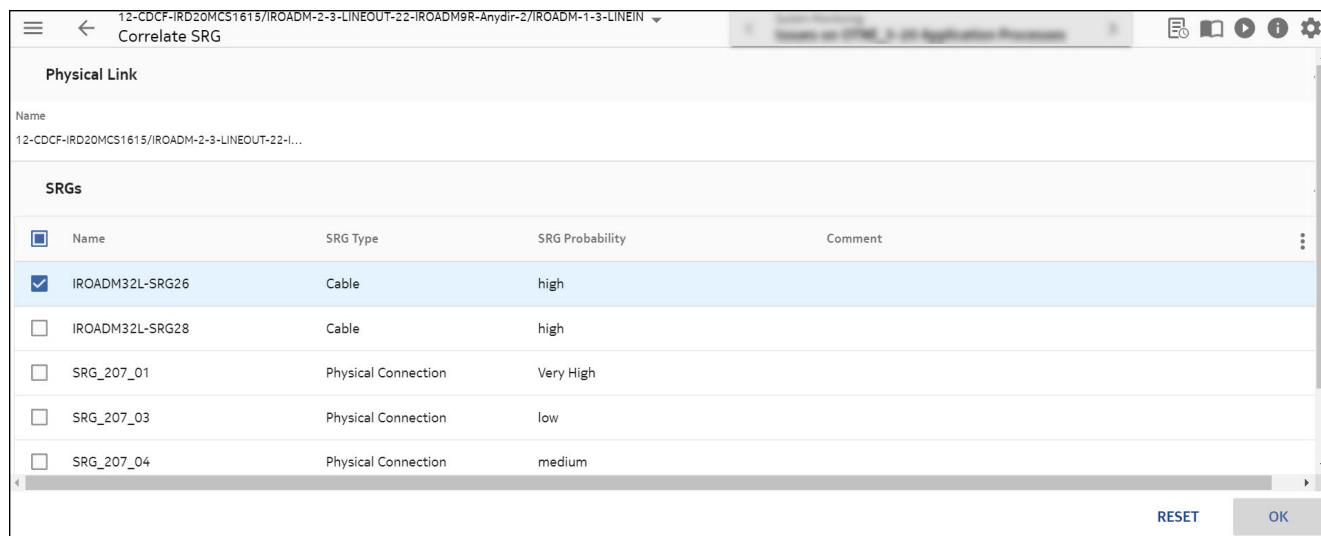
2

Select the connection to correlate an SRG to and click on the **More**  icon on the physical connection where you want to correlate the SRG and follow this path:

Correlate SRG.

Result: The Correlate SRG window is displayed. The name of the connection you selected is displayed in the **Name** field in the Physical Link panel of the window.

Figure 7-70 Correlate SRG window



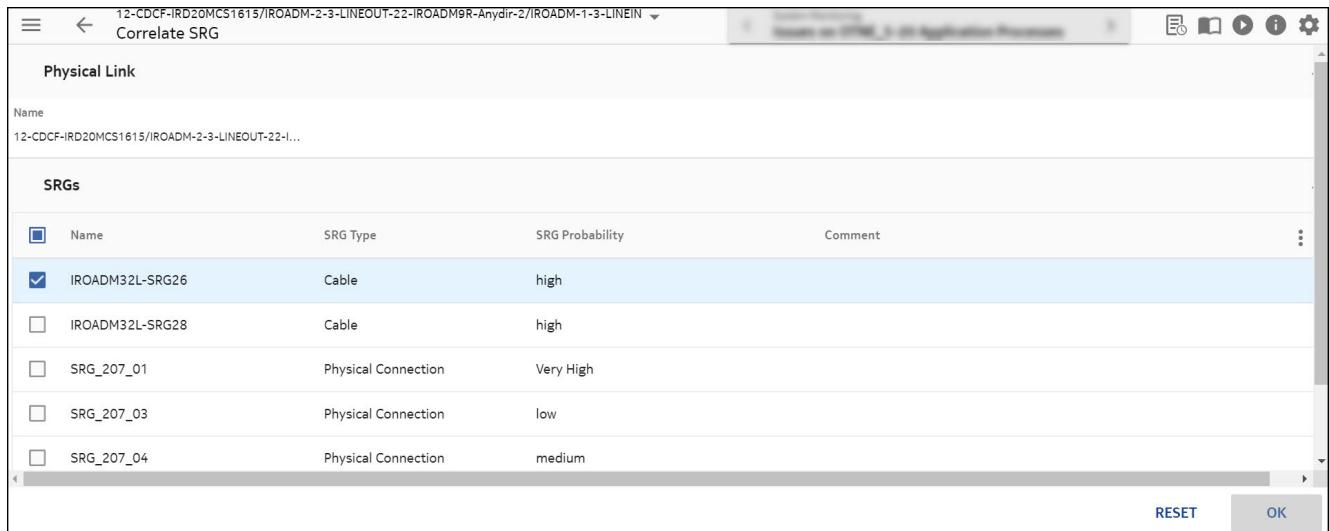
3

In the Shared Risk Group panel of the window, select **SRG**.

4

Click **OK**.

Figure 7-71 Physical Connections – SRG Correlated to the Physical Link



Result: The system displays a Success message at the bottom left of the window:
The physical link and the SRG(s) that you selected are now correlated.

END OF STEPS

7.29 Correlate an OTN physical connection with an ASAP

When to use

Use this task to correlate an OTN physical connection with an Alarm Severity Assignment Profile (ASAP).

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)
- “Alarm Profiles” (p. 649)

Before you begin

By default, once a connection is created, it is assigned the *default ASAP*.

If you need to select multiple connections, you can correlate the same profile to all of the selected connections. Choose up to 150 connections from the connection data table to apply to the alarm profile.

The impact of correlating an ASAP is as follows:

- If the *default ASAP* is changed, existing alarms remain as is and new alarms are raised with new severities as in the *default ASAP*.
- If a user defined ASAP is correlated to a connection, any existing alarms are cleared and they are immediately re-raised with new severities.

If correlation of an ASAP to a connection fails, an error message is displayed.

Correlate an OTN physical connection with an ASAP for the following types of connections by using the steps that are provided in this task:

- Physical connections
- PM enabled points of a selected physical connection
- Impacted connections for a selected physical connection
 - Impacted connections are those physical connections that are associated with a selected node and its current operational and alarm state.
- Used ports for a selected physical connection
 - Used ports are those physical connections that are assigned to a port address on a selected node.

Task

Complete the following steps to correlate an OTN physical connection with an ASAP.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

OPERATE > Physical Connections > 360° View > PM Enabled Points (tab)

OPERATE > Physical Connections > 360° View > Structure (tab)

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

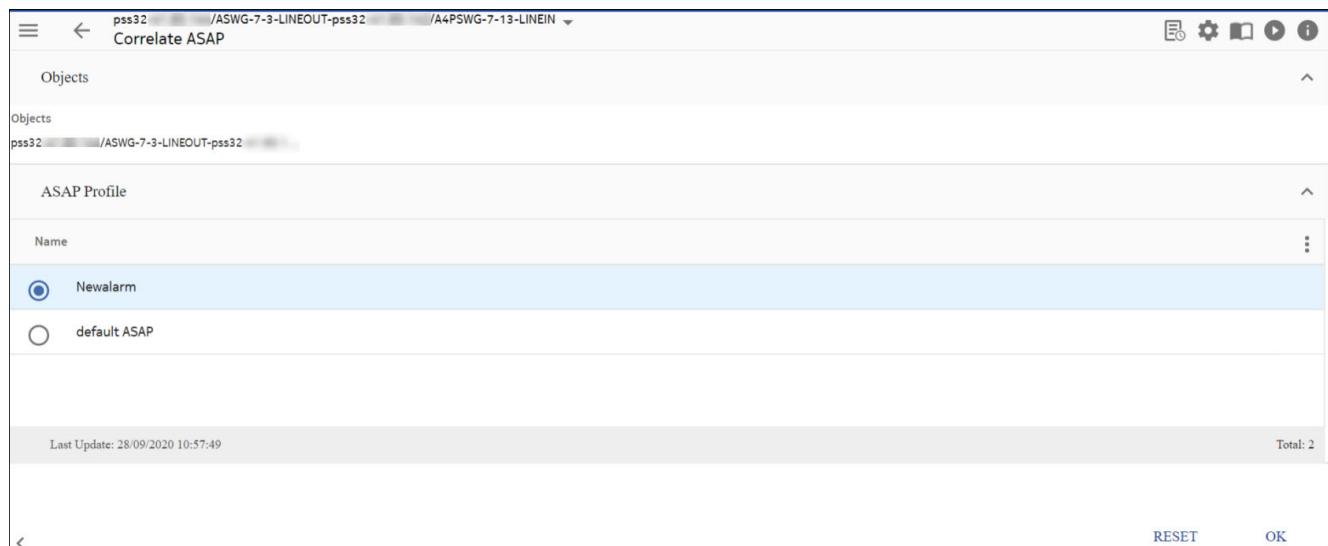
Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Select the connection that you want to correlate to an ASAP, click on the **More**  icon on the right part of the row, and follow this path: **Correlate ASAP**.

Result: The ASAP Correlate window is displayed. The name of the connection you selected is displayed in the **Object** panel of the window.

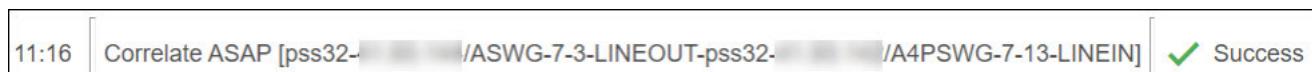
Figure 7-72 Physical Connections – Correlate ASAP window



3

In the **ASAP Panel** of the window, select the ASAPS from the list and click **OK**.

Result: The system displays a message similar to the following at the bottom of the window:



The physical link and the ASAP that you selected are now correlated.

4

Optional: Click **RESET** to reset the selection in the ASAP Profile panel.

END OF STEPS

7.30 Delete the clients of OTN physical connection

When to use

Use this task to delete the clients of an OTN physical connection.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

Delete the clients of an OTN physical connection for the following types of connections by using the steps that are provided in this task:

- Physical connections
- PM enabled points of a selected physical connection
- Impacted connections for a selected physical connection
 - Impacted connections are those physical connections that are associated with a selected node and its current operational and alarm state.
- Used ports for a selected physical connection
 - Used ports are those physical connections that are assigned to a port address on a selected node.

Deleting a physical connection and its client can disrupt traffic.

Task

Complete the following steps to delete (remove) the clients of an OTN physical connection.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections > 360° View > Clients (tab)

OPERATE > Physical Connections >  > Structure

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Highlight and select the client of the OTN physical connection to be deleted.

Important!

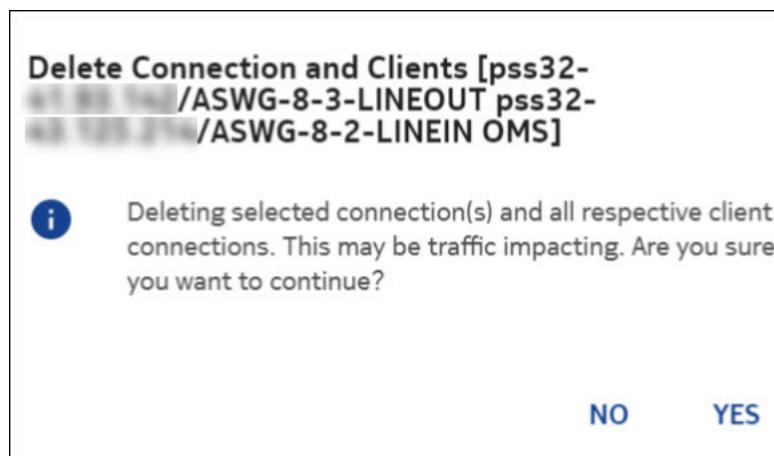
For the **Operate > Nodes > Impacted Connections (tab)** and the **Operate > Nodes > User Ports (tab)**, filter **Type** column in the data table to display physical connections/links.

3

Select the connection, click on the **More**  icon on the right part of the row, and select **Delete Connections and Clients**.

Result: The system informs you that deleting the connection and its clients can affect traffic and asks you if you want to continue.

Figure 7-73 Physical Connections – Delete Connections and Clients – query



4

Click **YES**.

Result: The system deletes the connection and its clients.

END OF STEPS

7.31 Implement/Deimplement an OTN physical connection

When to use

Use this task to implement/deimplement an OTN physical connection.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

The physical connection to be implemented must already be in the **Defined** or **Partially Implemented** state.

The physical connection to be deimplemented must already be in the **Implemented** or **Partially Implemented** state.

Task: Implement a physical connection

Complete the following steps to implement an OTN physical connection.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

OPERATE > Physical Connections > 360° View > PM Enabled Points (tab)

Result: The system displays a data table that lists the OTN physical connections.

2

Highlight and select the connection that you want to implement and click on the **More**  icon on the right part of the row and follow this path: **Deployment Control > Implement**.

Result: The Implementation State field on the data table for the selected physical connection changes from **Defined** to **Implemented**.

END OF STEPS

Task: Deimplement a physical connection

Complete the following steps to deimplement a physical connection.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists the OTN physical connections.

2

Highlight and select the connection that you want to implement and click on the **More** icon on the right part of the row and follow this path: **Deployment Control > Deimplement**.

Result: The system asks the following question:

Figure 7-74 Physical Connections – Deimplement ?

**Physical Connection [pss32 ... /ASWG-7-3-
LINEOUT-pss32 ... /A4PSWG-7-13-LINEIN]**



Deimplementing the Physical Connection will result in the removal of associated OTDR scans. Are you sure you want to continue?

NO YES

3

To continue to deimplement the connection, click **YES**.

Result: The Implementation State field on the data table for the selected physical connection changes from **Implemented** or **Partially Implemented** to **Defined**.

END OF STEPS

7.32 Manage GMRE enabled ASON Link from OTN physical connections

When to use

Use this task to manage ASON links from OTN Physical connections. The user has the option to navigate from the **OPERATE > Physical Connections** page of ASON links, if the physical link (OTS or OPS) is included in NPA.

Before you begin

Ensure that the physical connection links created are assigned to NPA.

Task

Complete the following steps to manage ASON links from OTN Physical connections.

- 1 _____
From the NFM-T GUI, follow this navigation path:
OPERATE > Physical Connections.
- 2 _____
Mouse over the icons on the top left and click on the **Create** icon.
Result: The system displays the Physical Connection Creation window.
- 3 _____
Create an OTS or OPS physical connection. To create a physical connection, see [7.19 “Create an OTN physical connection” \(p. 784\)](#).
- 4 _____
In the **OPERATE > NPA** page, perform the following:
 - **Create NPA:** Mouse over the icons on the top right and click on the **Create NPA** icon. See [10.8 “Create and remove an NPA” \(p. 1443\)](#).
 - **Assign Links to NPA:** Right click the NPA and select **Assign Links to NPA**. See [10.15 “Add links and remove links from ASON” \(p. 1462\)](#).**Result:** The OPS or OTS link created in the physical connections page is assigned to the NPA.
- 5 _____
Navigate to **OPERATE > Physical Connections** page and select the link that is assigned to the NPA.
The **NPA Name** column displays a name, if the NPA is associated to an OTS or OPS physical link; otherwise the **NPA Name** column remains blank.

Result: The **ASON LINK** tab is enabled in the 360° View.

6

Click the **ASON Link** tab.

Result: The ASON link that is associated with the selected Physical Connection in the list is displayed



Note:

- For OPS Physical Connection added to an NPA, the **ASON LINK** tab displays the link as Physical Link in the **Category** column.
- For OTS Physical Connection added to an NPA, the **ASON LINK** tab displays the link as OMSLink in the **Category** column.
- An OTS physical connection with a single ASON Link is either a C Band or L band, whereas an OTS connection with more than one ASON link is a C+L Band.
 - For C Band and L Band, the respective OMS link has to be assigned to NPA.
 - For C + L Band, the user has to individually assign both the OMS links to the NPA.

7

In the **ASON LINK** tab, click on the **More** icon to view the operations supported.

Right click actions	Description
Administrative State	Displays the condition of the ASON link to be Locked, Unlocked, or Shutting Down, Soft Shutting Down, and Synchronize. See 10.27 “Set the ASON administrative state of links” (p. 1504) .
Add Links to ASON/Remove Links from ASON	Allows to add links to ASON or remove links from ASON. See 10.15 “Add links and remove links from ASON” (p. 1462)
Link Maintenance Window	Link Maintenance Window displays the details of TE links. See 10.25 “Perform link maintenance” (p. 1497)
Change ASON WTR	The Wait Time to Restore (WTR) defines the time to wait before the traffic is moved back to the Main path, starting from the Main path restoration. When a failure occurs in ASON, the failed path is switched to an alternative path, called a <i>Spare</i> , to guarantee the traffic. Once the <i>Main</i> path is restored, the traffic is switched from the <i>Spare</i> back to the <i>Main</i> . See 10.18 “Change ASON WTR” (p. 1475)
Modify TCM Defect Raising Time	Manually allows to change the GMRE default value. This option is available in the right-click menu on L1 Logical links and FA-Unterm tunnels. See 10.16 “Modify TCM defect raising time” (p. 1470) .

Right click actions	Description
Auto Restoration	Displays the state of the Automatic Switched Optical Network (ASON) automatic restoration to be Disabled, Enabled, Partially Enabled, or - (a dash, which means that it is not applicable). See 10.20 “Enable or disable auto restoration of links” (p. 1480)
Shared Link	Indicates if the link is sharing a drop port between Managed Plane and Control Plane, a link already supporting MP service is allowed to be added to CP as drop See “Task: Enable/disable shared link” (p. 1467) .
TE-Link Assignment	Provides an option to assign ASON Link and TE-Link parameters. 10.17 “Assign an ASON I-NNI link to a TE Link and SRG” (p. 1473)
Misalignment Report	Displays the Misalignment Report for the selected link. 10.14 “Access and view the misalignment report for a link” (p. 1461)
Jobs	Provides users with the ability to view jobs that are currently in progress or that have completed in the system and to reschedule jobs, delete jobs, and run job histories. 7.126 “Jobs description” (p. 1194)

END OF STEPS

7.33 Move Traffic from a link for L0 Control Plane and MRN

When to use

Use this task to move traffic away from the Physical connections.

The option to move the traffic is available in the **OPERATE > Physical Connections** page for those OTS physical connections that are assigned to NPA. See [7.32 “Manage GMRE enabled ASON Link from OTN physical connections” \(p. 837\)](#)

This functionality moves the traffic away from the selected OTS and the new route is marked as the new Nominal Route for all Subnetwork Connections (SNCs) that were riding on the OTS.

Move Traffic is applicable for L0 Control Plane and Multi-Region Network (MRN).

After the bulk traffic operation, the original link remains in Locked state. The user can decide to either unlock the link or remove the link from NPA.

Before you begin

Ensure that the physical connection links created are assigned to NPA. User can perform moving of bulk traffic on the SNCs which has Nominal Route on the underlying OTS connection.

Task

Complete the following steps to manage Move Traffic from OTS Physical connections.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The Physical Connections page is displayed.

2

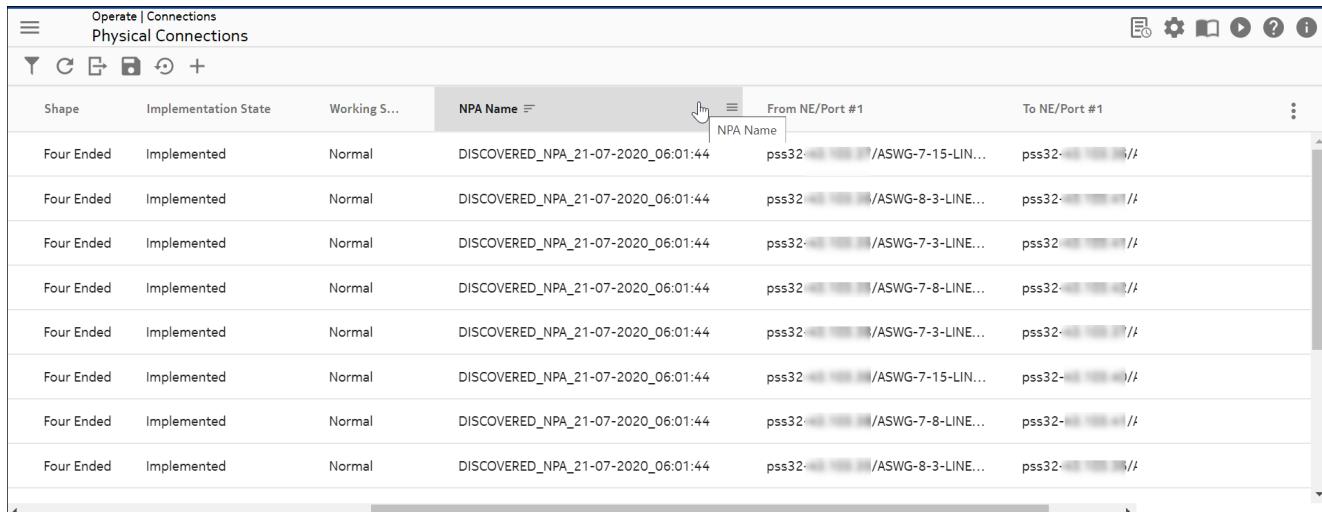
Click the **More**  icon at the right end of the table header and select **Manage Columns**.

3

In the **Manage Columns** window, scroll down and select the check box against **NPA Name** and click **APPLY**.

Result: The **NPA Name** is added to the list of column names.

Figure 7-75 NPA Name

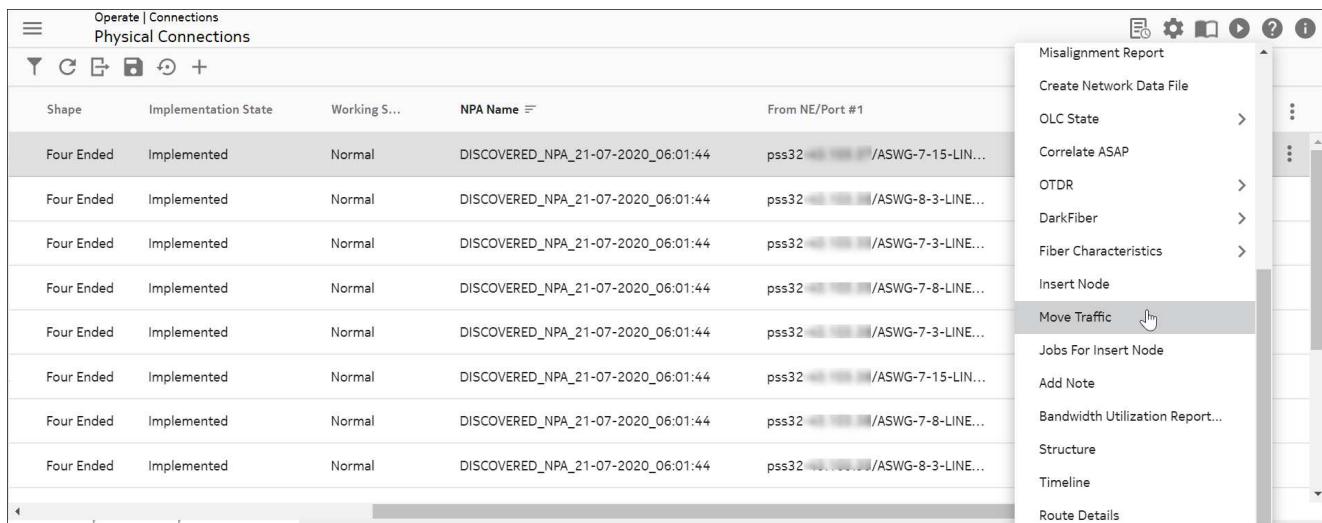


Shape	Implementation State	Working S...	NPA Name	From NE/Port #1	To NE/Port #1
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32 [REDACTED] /ASWG-7-15-LIN...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-3-LINE...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-3-LINE...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-8-LINE...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-3-LINE...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-15-LIN...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-8-LINE...	pss32-[REDACTED] //
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-8-3-LINE...	pss32-[REDACTED] //

4

Select a physical connection that is assigned to NPA and click the More  icon corresponding to the connection, and select **Move Traffic**.

Figure 7-76 Move Traffic selection



Shape	Implementation State	Working S...	NPA Name	From NE/Port #1
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32 [REDACTED] /ASWG-7-15-LIN...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-8-3-LINE...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-3-LINE...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-8-LINE...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-3-LINE...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-15-LIN...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-7-8-LINE...
Four Ended	Implemented	Normal	DISCOVERED_NPA_21-07-2020_06:01:44	pss32-[REDACTED] /ASWG-8-3-LINE...

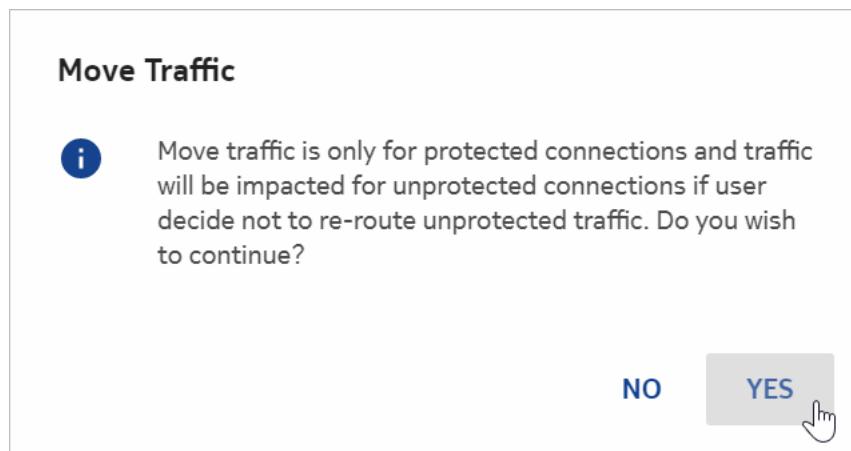
Result: The Move Traffic page is displayed with ASON SNCs riding over.

Figure 7-77 Move Traffic connections

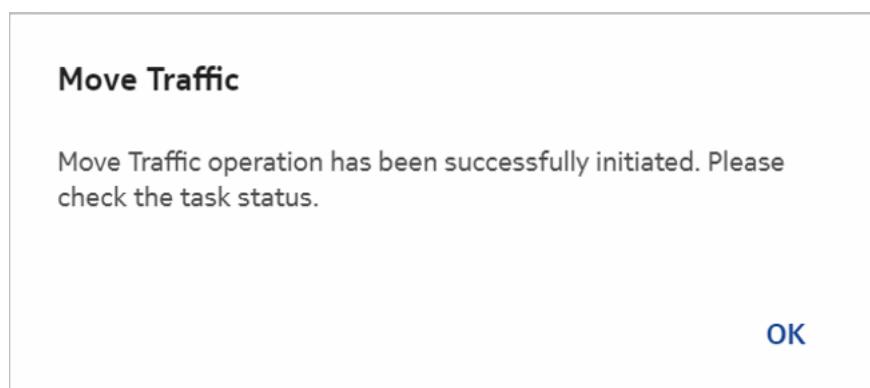


i Note: C - Band navigates to **Client ASON SNCS** page.

- 5 Click the **Move Traffic** button and select **Yes**.



- 6 Click **OK**.



Result: The system displays the **Job Run Details** of the selected job.

Figure 7-78 Move Traffic - Job Run Details

Name	Sub Task	Task Detail	Status	Start Time	End Time
○	GetAsonSncsFromL...	PTP:108020101	Success	2020-08-07 14:26:10	2020-08-07 14:26:10
○	Received Sucessful Respo...	[1] [1] name : EMS value : ...	Success	2020-08-07 14:26:10	2020-08-07 14:26:10
○	setAdminStatePTP...	PTP:107060101	Success	2020-08-07 14:26:10	2020-08-07 14:26:10
○	Received Sucessful Respo...	[1] egressTrafficDescripto...	Success	2020-08-07 14:26:10	2020-08-07 14:26:10
○	Received Sucessful Respo...	[1] egressTrafficDescripto...	Success	2020-08-07 14:26:10	2020-08-07 14:26:10
○	setAdminStatePTP...	PTP:108020101	Success	2020-08-07 14:26:09	2020-08-07 14:26:10



Note:

- icon is to refresh **Move Traffic** page.
- **Refresh** icon is to refresh job run details.
- **Export to CSV file** icon is to export job details to a **.CSV** file.
- **Save Table Preferences** icon is to save data table preferences of job details.
- **Reset Table to Preferences to Default** icon is to save data table preferences and to reset the data tables to its default display.

Alternatively, you can also view the job run details using:

- **ADMINISTER > Jobs**.
- **ADMINISTER > ALL Records**.

Figure 7-79 All Records - User Activity Log

<input type="checkbox"/> Start Time	End Time	Opera...	Action	Object	Stat...	App...	Client Host	⋮
<input type="checkbox"/> 07/08/2020 14:2...	07/08/2020 14:27:10	alcatel	Move Traffic	pss32-43.103.41/AS...	Success	OTN	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:2...	07/08/2020 14:21:22	alcatel	Login History	alcatel	Success	PLATFO...	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:19:51	alcatel	Login History	alcatel	Success	PLATFO...	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:20:48	alcatel	Move Traffic	pss32-43.103.35/AS...	Success	OTN	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:19:38	alcatel	Show ASON SNCs on ...	pss32-43.103.35/AS...	Success	OTN	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:18:35	alcatel	Show ASON SNCs on ...	pss32-43.103.41/AS...	Success	OTN	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:17:56	alcatel	Show ASON SNCs on ...	pss32-43.103.38/AS...	Success	OTN	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:16:59	alcatel	Show ASON SNCs on ...	pss32-43.103.35/AS...	Success	OTN	135.245.130....	
<input type="checkbox"/> 07/08/2020 14:1...	07/08/2020 14:16:23	alcatel	Show ASON SNCs on ...	pss32-41.93.145/AS...	Success	OTN	135.245.130....	

END OF STEPS

7.34 Move Traffic from a link for Managed Plane

When to use

Move Traffic is to reroute all infrastructure connections passing through a selected OTS link. From NFM-T Release 21.12, bulk reroute operation is also available for Managed Plane connections.

For Move Traffic in Control Plane, see [7.33 “Move Traffic from a link for L0 Control Plane and MRN” \(p. 840\)](#)

Bulk move of traffic from a Managed Plane physical connection is initiated from the **OPERATE > Physical Connections** page for that connection. NFM-T calculates the new route or existing reroute to move the trail at OTUk or OTSig layer along with their clients.

Before you begin

- Ensure that the OTS physical connection links are created.
- Alternate route is available for bulk traffic infrastructure connection reroute.

Task

Complete the following steps to manage Move Traffic from OTS Physical connections.

- 1 _____
From the NFM-T GUI, follow this navigation path:
OPERATE > Physical Connections
Result: The Physical Connections page is displayed.
- 2 _____
Select a OTS physical connection and click the **More**  icon corresponding to the connection, and select **Move Traffic**.

Figure 7-80 Move Traffic selection

The screenshot shows the 'Operate | Connections' section under 'Physical Connections'. A context menu is open over a selected connection, with 'Move Traffic' highlighted. Other options in the menu include: PM, OAM&Diagnostics..., Misalignment Report, Create Network Data File, OLC State, Correlate ASAP, OTDR, OTDR (Beta), DarkFiber, Dark Fiber (Beta), Fiber Characteristics, Insert Node, Jobs For Insert Node, Add Note, Bandwidth Utilization Report..., and Structure.

OLC State	WDM Connec...	Name	Shape	Implementation ...	W...
<input type="checkbox"/>	OTS	MP_SITE5/AWBEGR-3-12-LINEOUT-MP_SITE2/RA5P-4-2-LI...	Four Ended	Implemented	
<input type="checkbox"/>	OTS	MP_SITE5/AWBEGR-4-11-LINEOUT-MP_SITE3/RA5P-4-2-LI...	Four Ended	Implemented	
<input type="checkbox"/>	OTS	MP_SITE5/AWBEGR-5-7-LINEOUT-MP_SITE4/RA5P-4-6-LIN...	Four Ended	Implemented	
<input type="checkbox"/>	OTS	OTS-SFD-9-14-OMD-ytan1	Simple	Implemented	
<input type="checkbox"/>	OTS	RW_OTS_A	Simple	Implemented	
<input type="checkbox"/>	OTS	RW_OTS_Z	Simple	Implemented	

Last Update: 09/09/2021 11:39:18

Result: The Move Traffic page is displayed with trails riding over.

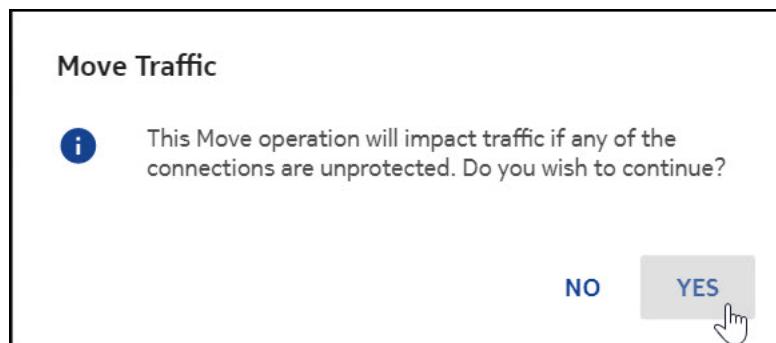
Figure 7-81 Move Traffic connections

The screenshot shows the 'Move Traffic' page with a message: 'Trails riding over - MP_SITE5/AWBEGR-5-7-LINEOUT-MP_SITE4/RA5P-4-6-LINEIN : C-Band L-Band'. A blue 'MOVE TRAFFIC' button is visible at the bottom right.

Note: C-Band or L-Band navigates to Impacted Trail page.

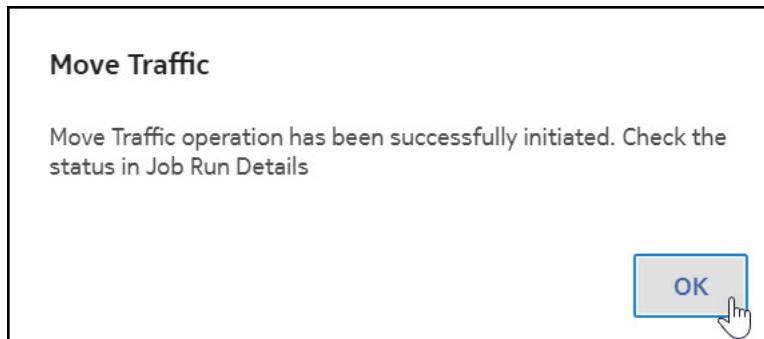
3

Click the **MOVE TRAFFIC** button and select **Yes**.



4

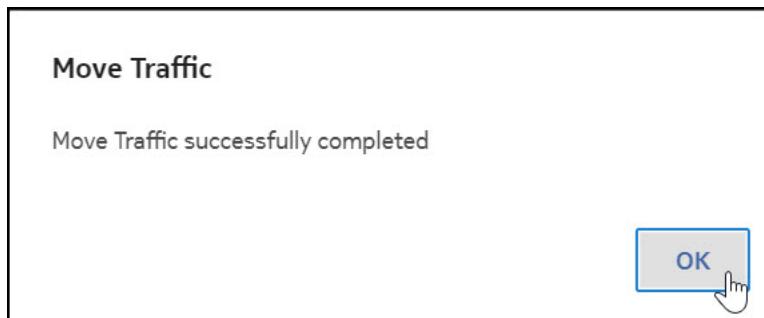
Click **OK** for checking the job run details status.



Result: A successful Move Traffic message is displayed.

5

Click **OK**.



Result: The system displays the **Job Run Details** of the selected job.

Figure 7-82 Move Traffic - Job Run Details

The screenshot shows the 'Move Traffic' job run details in the Nokia NFM-T interface. The main content area displays a table of tasks with columns: Name, Task Detail, Status, Start Time, End Time, S., and more. The tasks listed are:

Name	Task Detail	Status	Start Time	End Time	S.
Move traffic in managed plane away from original physical Link	Reroute connection (1/1) for RW_MT_OCHP_S2S4_...	Failure	09/09/2021 15:06:05	09/09/2021 15:06:05	
Move traffic in managed plane away from original physical Link	Skip Reroute (3R connection) for :RW_3R_L_Tunne...	Success	09/09/2021 15:06:05	09/09/2021 15:06:05	
Move traffic in managed plane away from original physical Link	Moving Traffic for MP_SITE5/AWBEGR-5-7-LINEOU...	Success	09/09/2021 15:06:03	09/09/2021 15:06:03	

The footer of the interface shows the progress bar and status message: 'Move Traffic [MP_SITE5/AWBEGR-5-7-LINEOUT-MP_SITE4/RA5P-4-6-LINEIN] Success'.



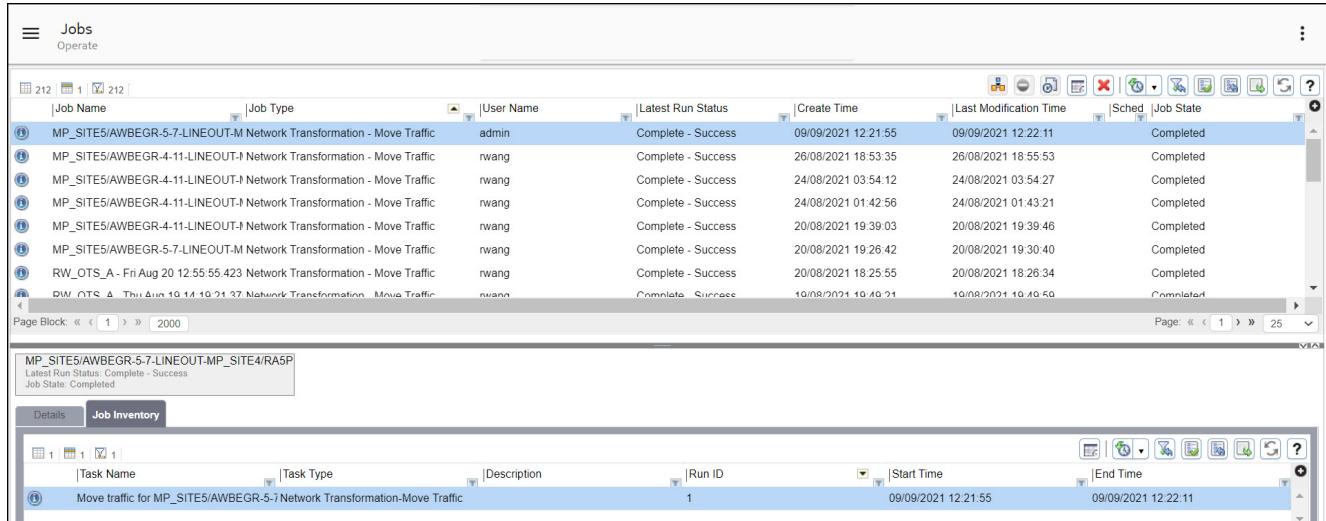
Note:

- **Filter** icon allows to setup a data set filter on the displayed table.
- **Refresh** icon is to refresh job run details.
- **Export to CSV file** icon is to export job details to a .CSV file.
- **Save Table Preferences** icon is to save data table preferences of job details.
- **Reset Table to Preferences to Default** icon is to save data table preferences and to reset the data tables to its default display.

Alternatively, you can also view the job run details using:

- **ADMINISTER > Jobs.**
- **ADMINISTER > ALL Records.**

Figure 7-83 Jobs-User Activity Log



The screenshot shows the 'Jobs' section of the Nokia NFM-T interface. At the top, there is a toolbar with various icons. Below it is a table with columns: Job Name, Job Type, User Name, Latest Run Status, Create Time, Last Modification Time, Sched, and Job State. The table lists several completed jobs, mostly related to 'Network Transformation - Move Traffic'. A specific job entry is highlighted: 'MP_SITE5/AWBEGR-5-7-LINEOUT-M Network Transformation - Move Traffic' by user 'admin' on 09/09/2021 at 12:21:55, with a status of 'Complete - Success'. Below the table, there is a message box showing details for this job: 'MP_SITE5/AWBEGR-5-7-LINEOUT-MP_SITE4/RAS5P', 'Latest Run Status: Complete - Success', and 'Job State: Completed'. At the bottom of the interface, there are tabs for 'Details' and 'Job Inventory', and another table showing task details for the selected job.



Note: Move Traffic operation in Managed Plane is not applicable for the following connections:

- Connections terminated on either of the end terminals of the given OTS.
- 3R connections on the nodes at the end terminals of the OTS link.
- In the OTS link, if there are connections that are not commissioned.

END OF STEPS

7.35 Manage repeaters for an OTN OTS physical connection

When to use

Use this multi-task procedure to manage repeaters for an OTN OTS physical connection.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

Before you associate a repeater to an OTN physical connection, the repeater must be added to the management system. Refer to Add a Node/NE procedure in the *NFM-T NE Management Guide* for details.

User can also refer to this procedure, to add a 1830 SLTE to the network. Users can add 1830 SLTEs using the Add 1830 SLTE Information procedure in the *NFM-T NE Management Guide*.

User can also refer to this procedure, to add a GenericNE_RedC to the network. See Add RA3P Information procedure in the *NFM-T NE Management Guide*.

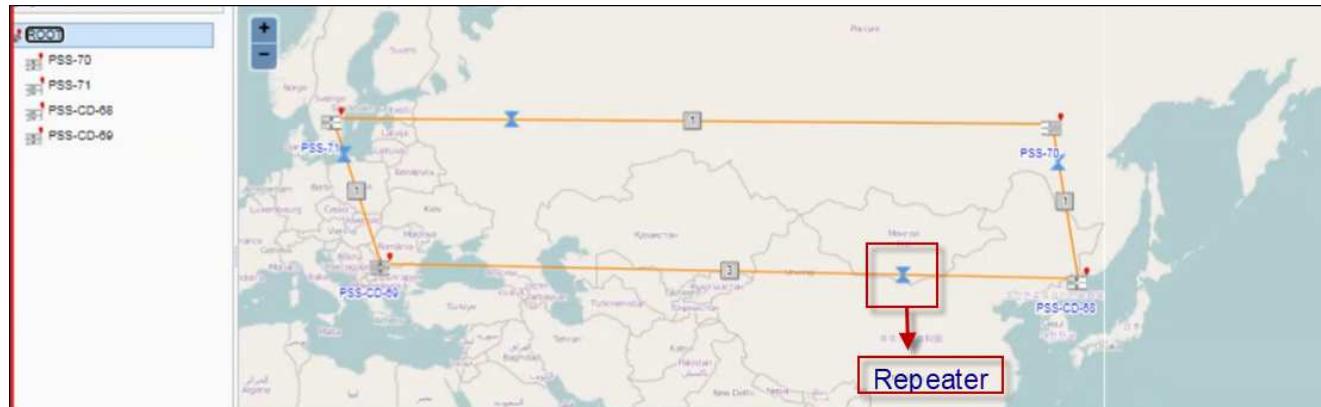
They can manually associate the 1830 STLE or GenericNE_RedC NE to an amplifier port and to a transmit/receive direction through OTS physical connection ports using the subtasks provided in this procedure.

Users can readily identify 1830 SLTE or GenericNE_RedC on the Physical Connections data table by customizing the data table to list the **Repeater** column. From the Physical Connections data table, users can then navigate to the 1830 SLTE ZIC. A unique double triangle icon on the Network Map and the Routing Display makes the OTS physical connections to 1830 SLTEs or GenericNE_RedC readily visible.



Note: Routing Display support is not available for GenericNE_RedC.

Figure 7-84 Physical Connections – Manage Repeaters – Repeater on the Network Map



Task: Associate a repeater to an OTS physical connection

Complete the following steps to add a repeater to an OTS physical connection.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

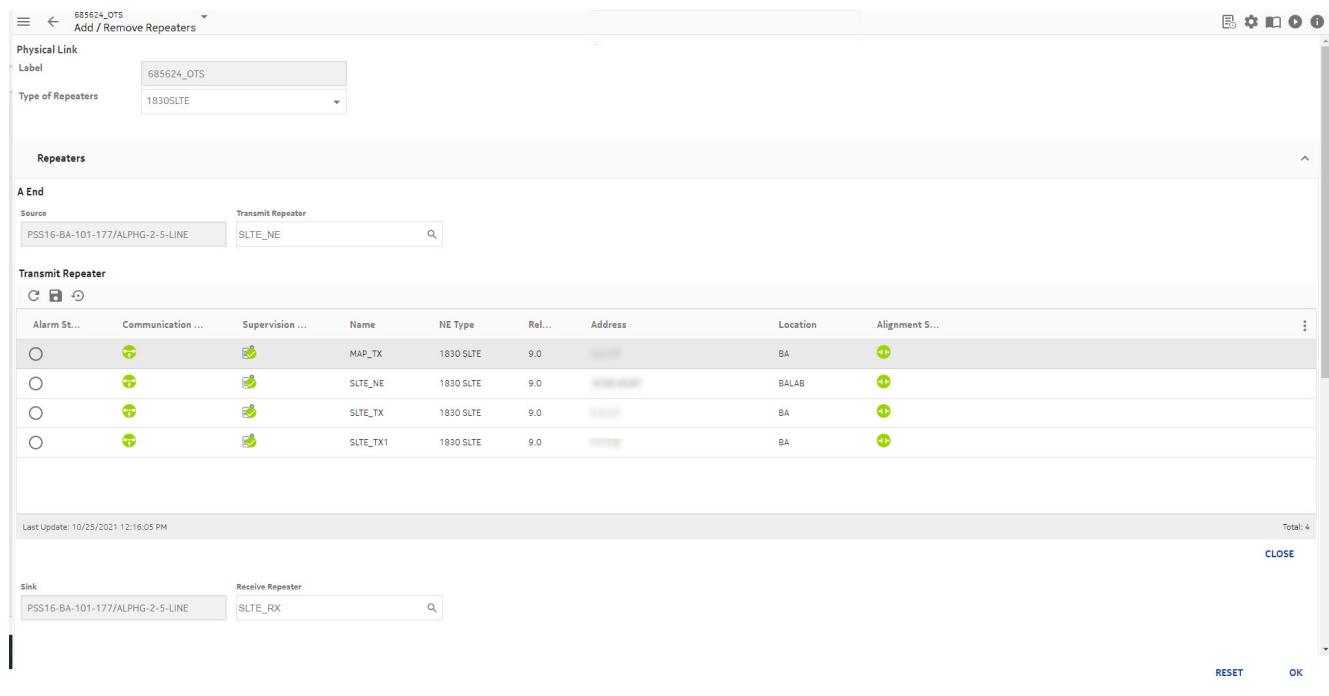
Result: The system displays a data table that lists all of the requested connections.

2

Highlight and select the OTS physical connection for which you want to add a repeater, click on the **More**  icon on the OTS physical connection, and select **Add/Remove Repeaters**.

Result: The system displays the **Add/Remove Repeaters** window. The **Name** is populated with the name of the OTS physical connection that you selected. The **Type of Repeaters** field is populated based on the NE selected. The **A/Z Port** fields are populated with the respective port names.

Figure 7-85 Physical Connections – manage repeaters – Add/Remove Repeaters window



3

Select the type of repeaters in the **Type of Repeaters** field. The available options are 1830SLTE, 1830LX, and GenericNE_RedC.

4

Perform one of the following steps:

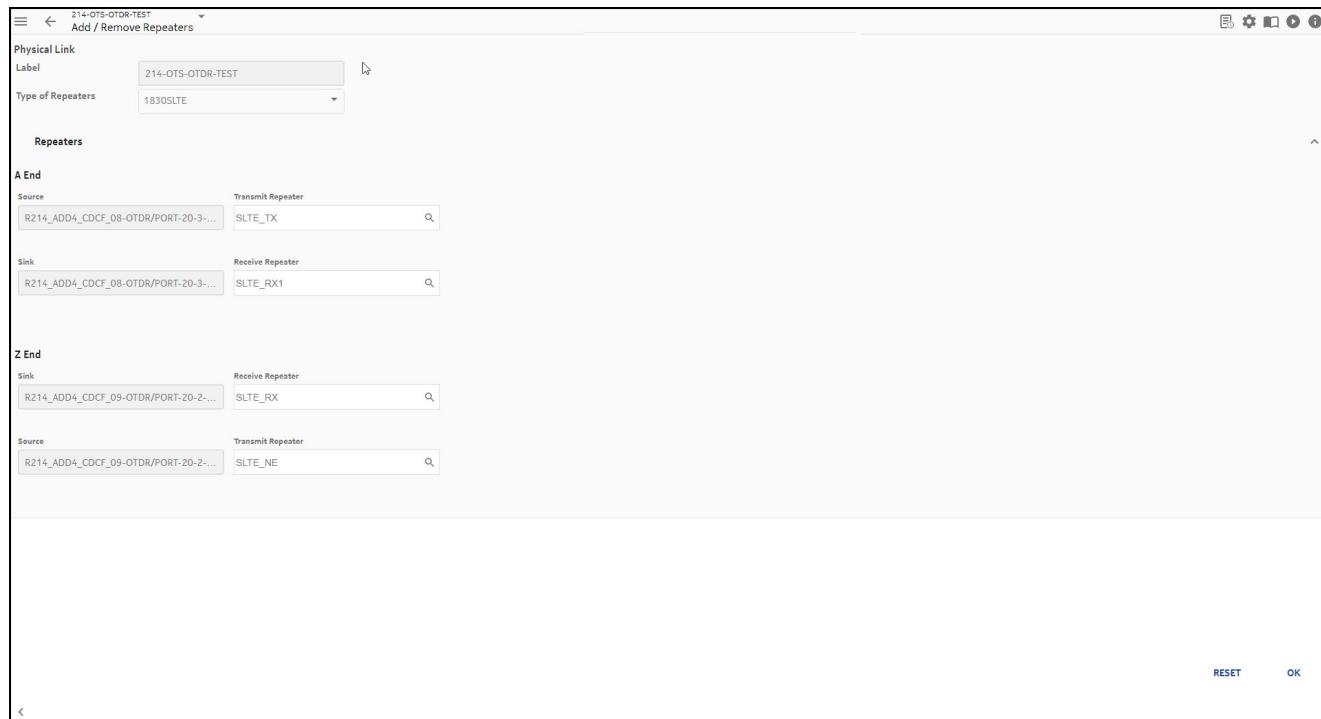
If...	then...
you have selected 1830SLTE in the Type of Repeaters field	Go to Step 5
you have selected 1830LX in the Type of Repeaters field	Go to Step 9
you have selected GenericNE_RedC in the Type of Repeaters field	Go to Step 13

5

To select the repeaters for the **A End** and **Z End** port transmit and receive fields, click on the search icon to the right of the **SLTE Transmit Repeater** and **SLTE Receive Repeater** fields.

Result: The system displays the **Repeater Selection** window with the 1830 SLTE repeaters.

Figure 7-86 Physical Connections – 1830SLTE manage repeaters – Repeater Selection window



6

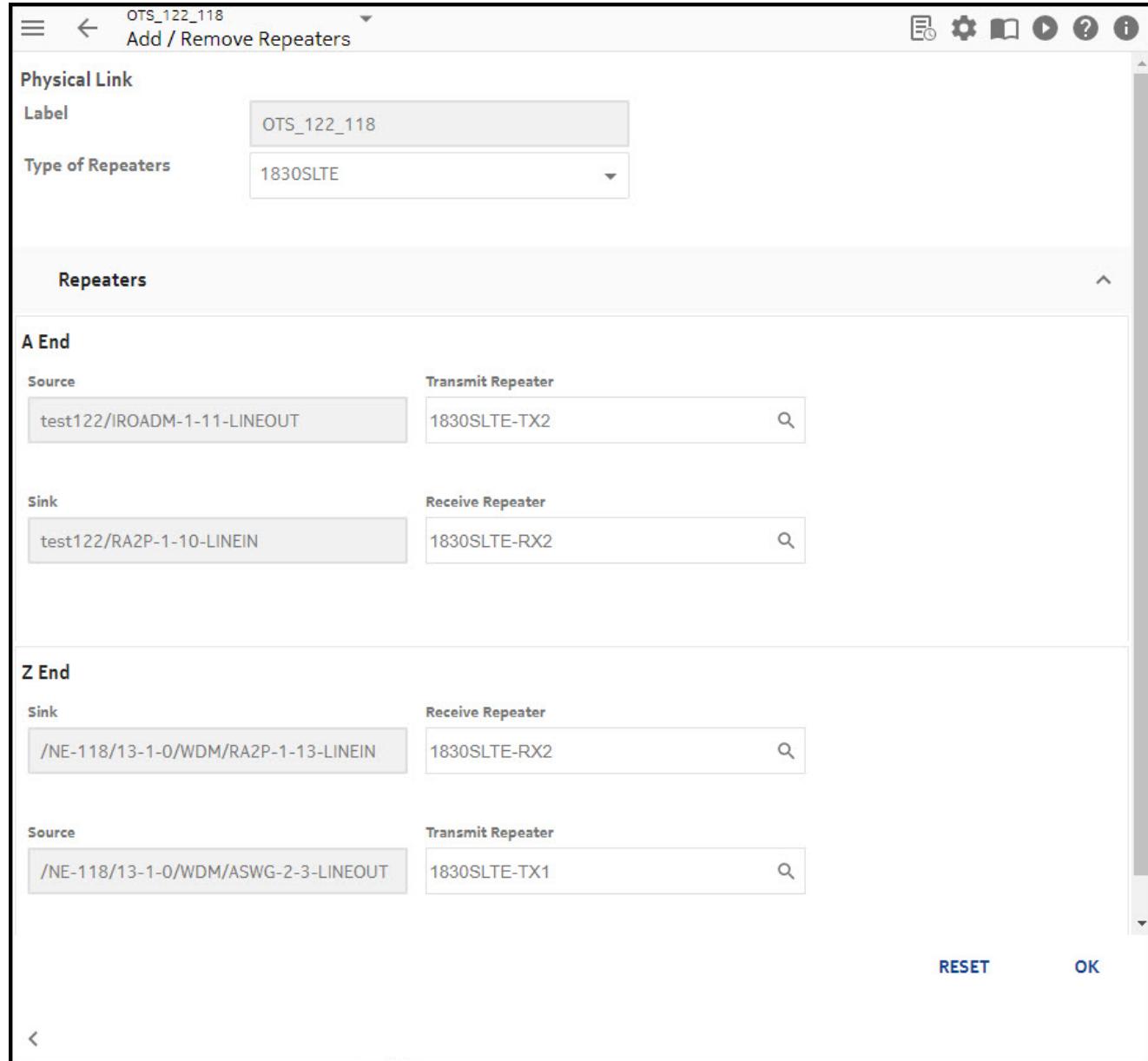
From the **Repeater Selection** window, click the appropriate repeater to populate the **SLTE Transmit Repeater** and **SLTE Receive Repeater** fields for the **A End** and **Z End**. The user can select either one of the end points to add the repeater.

7

Click **Select**.

Result: The system adds the selected repeaters to the **SLTE Transmit Repeater** and **SLTE Receive Repeater** for the **A End** and **Z End**.

Figure 7-87 Physical Connections – 1830SLTE manage repeaters – repeater selected – field populated



8

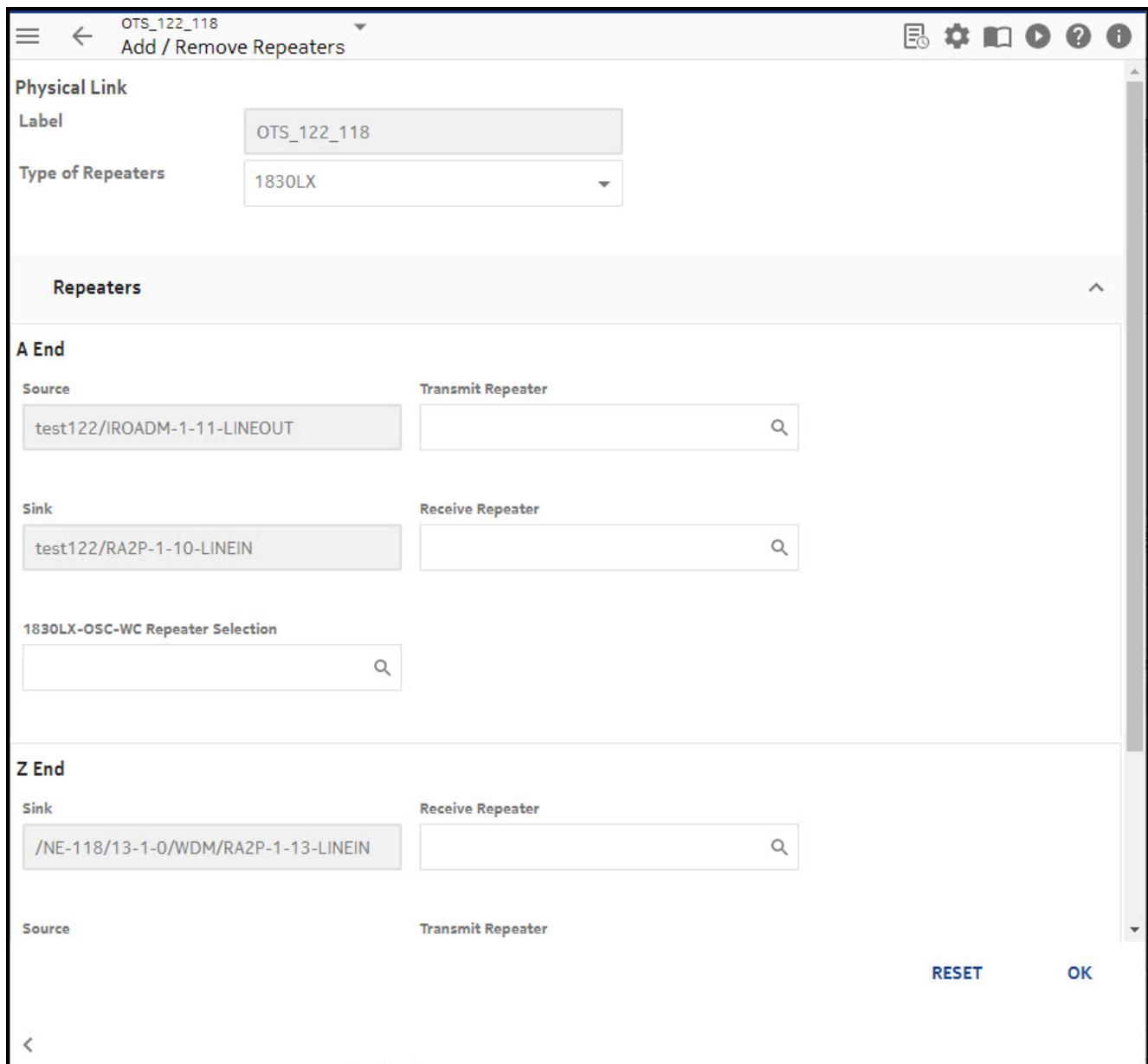
To deploy, go to [Step 16](#)

9

To select the repeaters for the **A End** and **Z End** port transmit and receive fields, click the search icon to the right of the **LX Transmit Repeater**, **LX Receive Repeater**, **1830LX-OSC-WC A End**, and **1830LX-OSC-WC Z End** fields.

Result: The system displays the **Repeater Selection** window with the 1830 LX repeaters.

Figure 7-88 Physical Connections – 1830LX manage repeaters – Repeater Selection window



10

From the Repeater Selection window, click the appropriate repeater to populate the **LX Transmit Repeater**, **LX Receive Repeater**, **1830LX-OSC-WC A End**, and **1830LX-OSC-WC Z End** fields for the **A End** and **Z End**. The user can select either one of the end points to add the 1830 LX repeater.

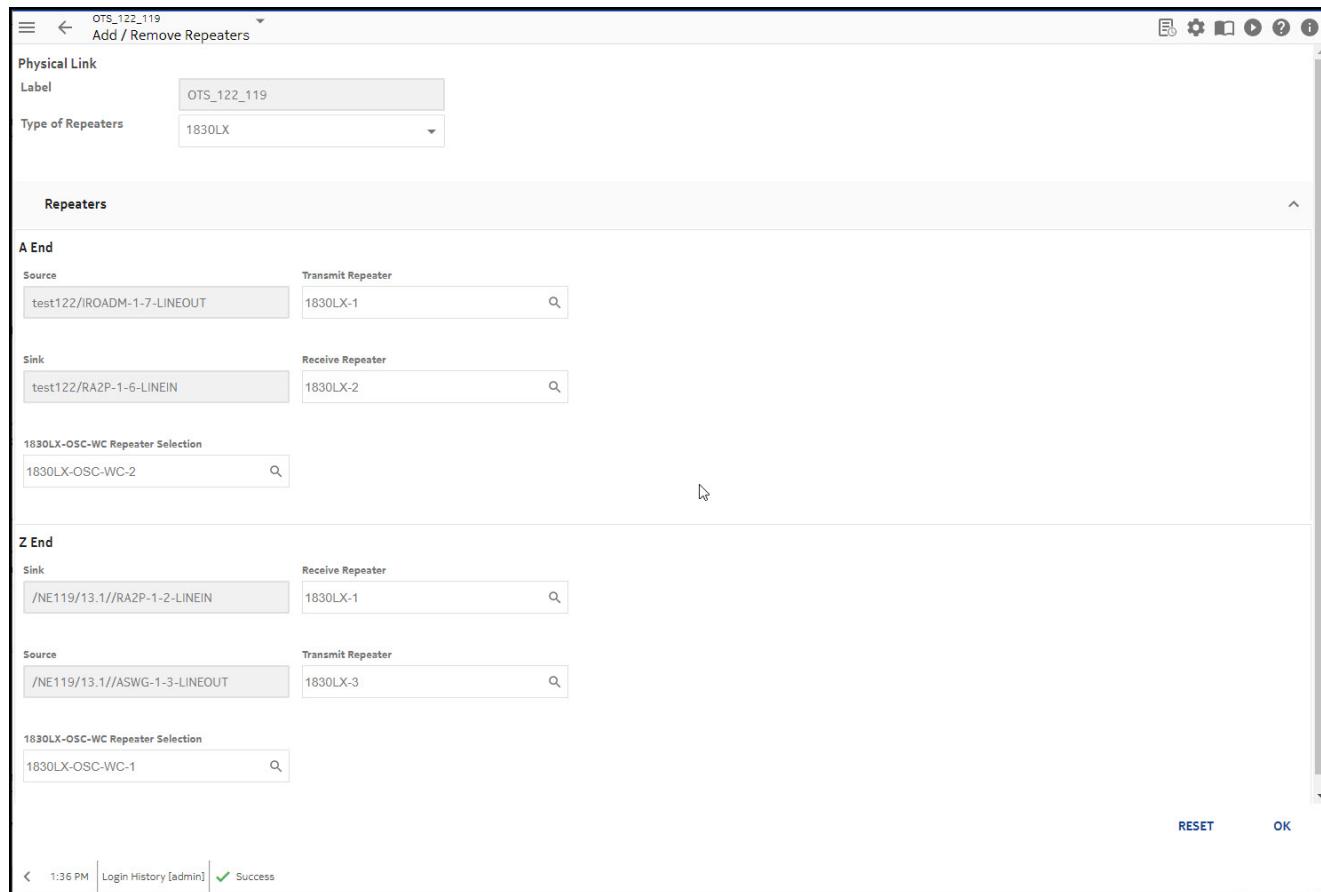
Note: While selecting 1830 LX OSC-WC, make sure the 1830 LX repeaters are selected.

11

Click **Select**.

Result: The system adds the selected repeaters to the **LX Transmit Repeater** and **LX Receive Repeater** for the **A End** and **Z End**.

Figure 7-89 Physical Connections – 1830 LX manage repeaters – repeater selected – field populated



12

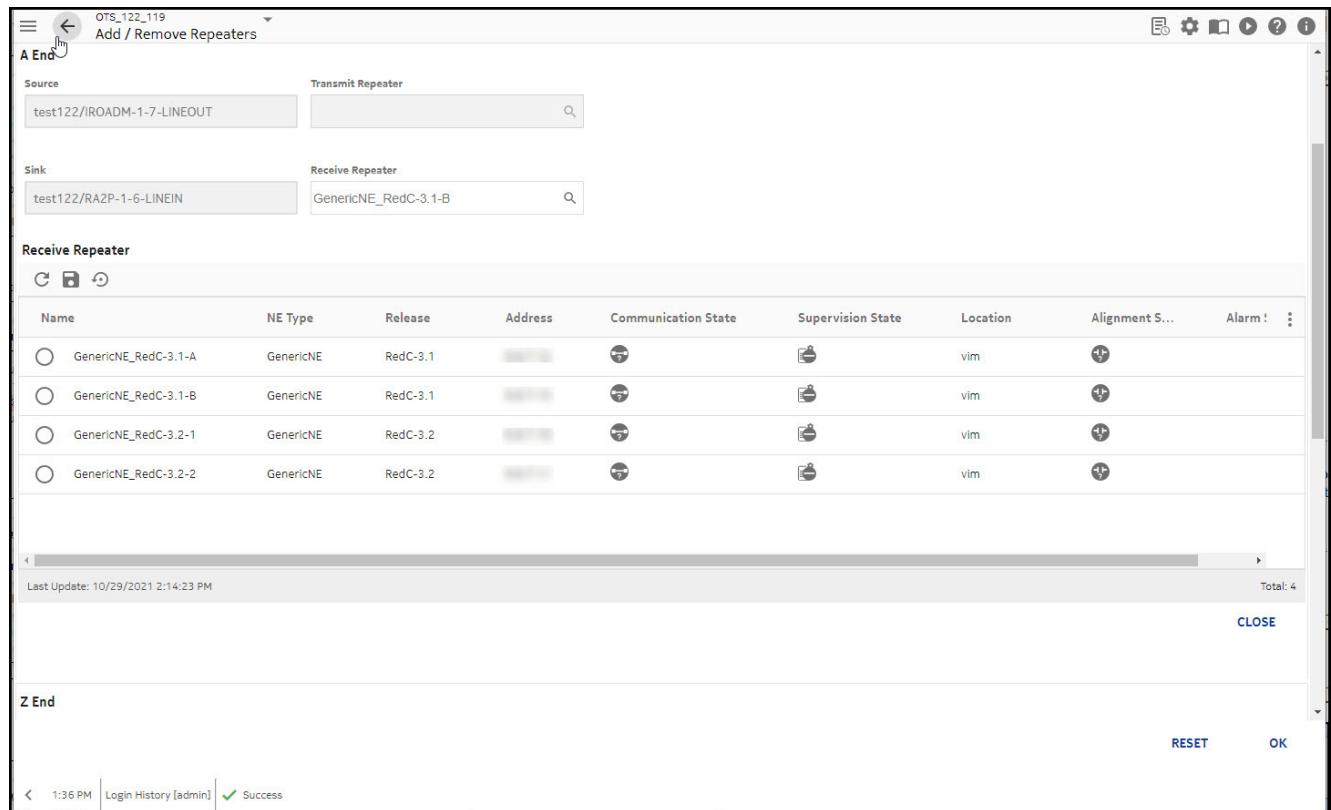
To deploy, go to [Step 16](#).

13

To select the repeaters for the **A End** and **Z End** port transmit and receive fields, click the **Search** icon to the right of the **RedC Receive Repeater** fields.

Result: The system displays the **Repeater Selection** window with the RedC repeaters.

Figure 7-90 Physical Connections – GenericNE_RedC manage repeaters – Repeater Selection window



14

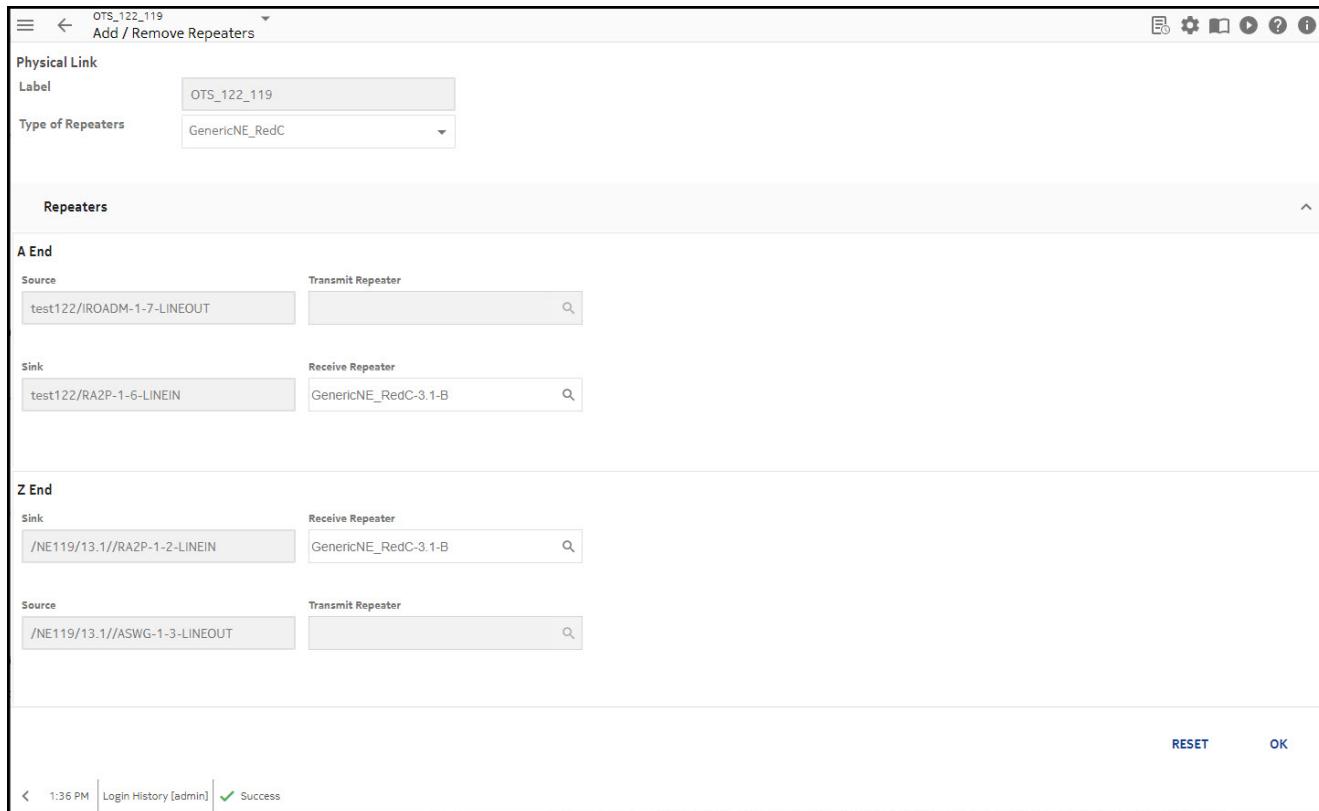
From the **Repeater Selection** window, click the appropriate repeater to populate the **RedC Receive Repeater** fields for the **A End** and **Z End**. The user can select either one of the end points to add the GenericNE_RedC repeater.

15

Click **Select**.

Result: The system adds the selected repeaters to the **RedC Receive Repeater** for the **A End** and **Z End**.

Figure 7-91 Physical Connections – GenericNE_RedC manage repeaters – repeater selected – field populated



16

Click **Deploy**.

Result: The system adds the repeater that you selected to the port A/Z end points for the selected connection.

END OF STEPS

Task: Remove a repeater to an OTS physical connection

Complete the following steps to remove a repeater to an OTS physical connection.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

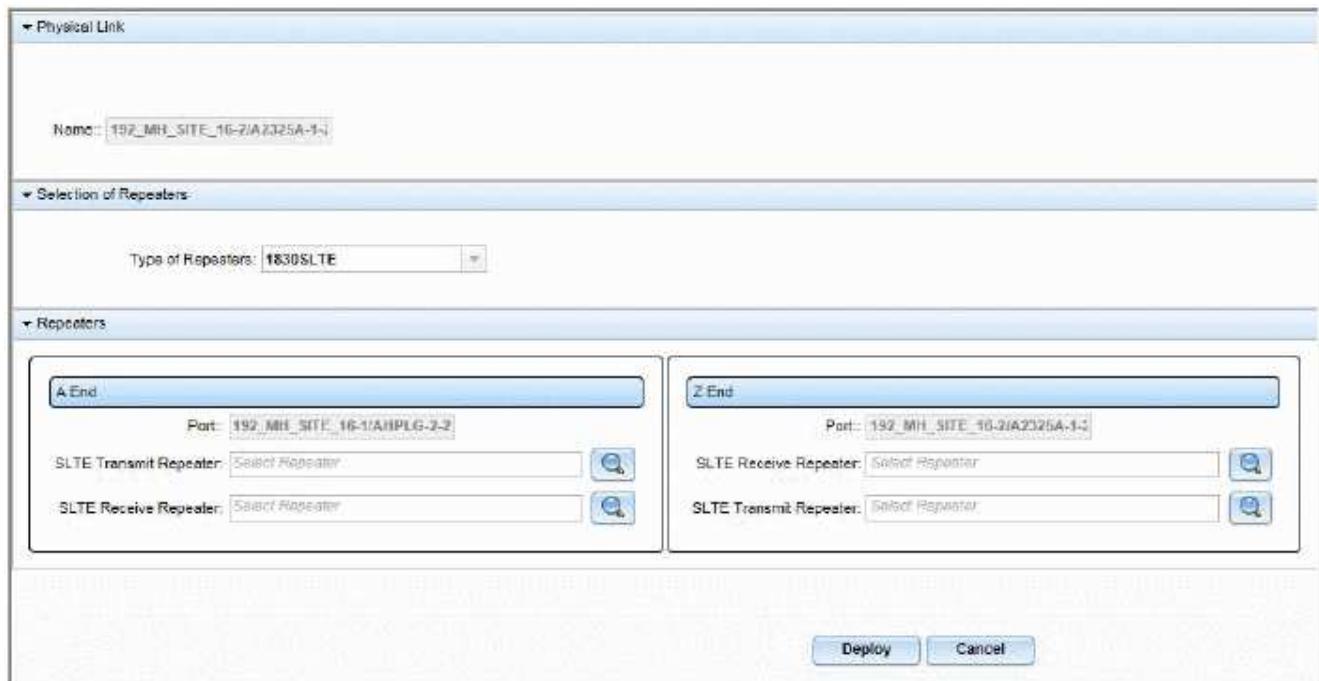
Result: The system displays a data table that lists all of the requested connections.

2

Highlight and select the OTS physical connection for which you want to remove a repeater, Click on the **More**  icon on the right part of the row and select **Add/Remove Repeaters**.

Result: The system displays the **Add/Remove Repeaters** window. The **Name** is populated with the name of the OTS physical connection that you selected. The **Type of Repeaters** field is populated based on the NE selected. The **A/Z Port** fields are populated with the respective port names.

Figure 7-92 Physical Connections – manage repeaters – Add /Remove Repeaters window



3

Select the type of repeaters in the **Type of Repeaters** field. The available options are 1830SLTE, 1830LX, and GenericNE_RedC..

4

Perform one of the following steps:

If...	then...
you have selected 1830SLTE in the Type of Repeaters field	Go to Step 5
you have selected 1830LX in the Type of Repeaters field	Go to Step 6
you have selected GenericNE_RedC in the Type of Repeaters field	Go to Step 7

5

To remove the repeaters for the **A End** and **Z End** port transmit and receive fields, manually delete the values populated in the **SLTE Transmit Repeater** and **SLTE Receive Repeater** fields and click **Deploy**.

Result: The system removes the repeater that you selected from the port A/Z end points for the selected connection.

6

To remove the repeaters for the **A End** and **Z End** port transmit and receive fields, manually delete the values populated in the **LX Transmit Repeater**, **LX Receive Repeater**, **1830LX-OSC-WC A End**, and **1830LX-OSC-WC Z End** fields, and click **Deploy**.

Result: The system removes the repeater that you selected from the port A/Z end points for the selected connection.

7

To remove the repeaters for the **A End** and **Z End** port transmit and receive fields, manually delete the values populated in the **RedC Receive Repeater** fields, and click **Deploy**.

Result: The system removes the repeater that you selected from the port A/Z end points for the selected connection.

END OF STEPS

Task: View a repeater associated with an OTS physical connection on the data table

Complete the following steps to view a list of OTS physical connections that are associated with repeaters.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists all of the requested connections.

2

On the top right corner, click **Manage Columns**

Search for **Repeater**, and select the **Repeater** check box. Click **APPLY**.

Figure 7-93 Physical Connections – manage repeaters – customize data table to view repeaters

Manage Columns					
ALL	DOWN	UP	DEGRADED		
<input checked="" type="checkbox"/> OPERATIONAL STATE	<input checked="" type="checkbox"/> NAME	<input checked="" type="checkbox"/> FROM NE/PORT #1	<input checked="" type="checkbox"/> TO NE/PORT #1	<input checked="" type="checkbox"/> ALARM STATUS	
<input type="checkbox"/> % HIGH UTILIZATION THRESHOLD	<input type="checkbox"/> % LOW UTILIZATION THRESHOLD	<input type="checkbox"/> % UTILIZATION	<input type="checkbox"/> 3D PARTY NETWORK DESCRIPTION	<input type="checkbox"/> 3D PARTY NETWORK NAME	<input type="checkbox"/> A-Z SPAN LOSS C
<input type="checkbox"/> A-Z SPAN LOSS L	<input type="checkbox"/> ASAP	<input type="checkbox"/> ASAP NAME	<input type="checkbox"/> ASELL STATUS	<input type="checkbox"/> ACCESS CONTROL DOMAIN	<input type="checkbox"/> ADMINISTRATIVE STATE
<input type="checkbox"/> BAND	<input type="checkbox"/> CLIENT SIGNAL TYPE	<input type="checkbox"/> CLUSTER	<input type="checkbox"/> COLOR PROFILE ID	<input type="checkbox"/> COLOR PROFILE NAME	<input type="checkbox"/> COLORS BITS
<input type="checkbox"/> COMMISSIONED STATUS	<input type="checkbox"/> DARK FIBER ASSOCIATED	<input type="checkbox"/> DEFINITION TIME	<input type="checkbox"/> DIRECTION	<input type="checkbox"/> FIBER ROUTE ASSOCIATED	<input type="checkbox"/> FLEX GRID CAPABLE
<input type="checkbox"/> FROM NE/PORT #2	<input type="checkbox"/> GRID TYPE	<input checked="" type="checkbox"/> IMPLEMENTATION STATE	<input type="checkbox"/> LAST CALCULATED SPAN LOSS DATE	<input type="checkbox"/> LATENCY (MICROSEC.)	<input type="checkbox"/> LATEST NOTE
<input type="checkbox"/> LINK TYPE	<input type="checkbox"/> NPA NAME	<input type="checkbox"/> OLC STATE	<input type="checkbox"/> OTDR SCAN STATUS	<input type="checkbox"/> OTDR SUMMARY	<input type="checkbox"/> OTDR SUPPORTED
<input type="checkbox"/> PM 15M	<input type="checkbox"/> PM 24H	<input type="checkbox"/> PROTECTION	<input type="checkbox"/> RX FREQUENCY	<input checked="" type="checkbox"/> REPEATER	<input type="checkbox"/> SRG PRESENT
<input type="checkbox"/> SERVICE STATE	<input checked="" type="checkbox"/> SHAPE	<input type="checkbox"/> SPAN TYPE	<input type="checkbox"/> TX FREQUENCY	<input type="checkbox"/> TO NE/PORT #2	<input type="checkbox"/> UTILIZATION PROFILE
<input checked="" type="checkbox"/> WDM CONNECTION TYPE	<input checked="" type="checkbox"/> WORKING STATE	<input type="checkbox"/> Z-A SPAN LOSS C	<input type="checkbox"/> Z-A SPAN LOSS L	<input type="checkbox"/> INTERSHELF	

CANCEL RESET APPLY APPLY & SAVE

Result: The system adds the **Repeater** column to the currently displayed data table.

3

Scroll down the data table list to view which physical connections have the **Repeater** column checked.

Figure 7-94 Physical Connections – manage repeaters – Repeater column – view repeaters

W..	Name	Shape	Implementation ...	From NE/...	To NE/Port #1	Repeater
OTS	PSS32 /OPS-3-30...	Simple	Implemented	PSS32	PSS32 /OPS-3...	<input checked="" type="checkbox"/>
OTS	PSS32 /IROADM-2...	Four Ended	Implemented	PSS32	PSS32 /IROADM...	<input checked="" type="checkbox"/>
OTS	PSS32 /IROADM-3...	Simple	Implemented	PSS32	PSS32 /OPS-3...	
OTS	PSS32 /IROADM-2...	Four Ended	Implemented	PSS32	PSS32 /IROADM...	
OTS	PSS32 /AHPHG-1...	Simple	Implemented	PSS32	PSS32 /AHPH...	
OPS	SF_CI	Four Ended	Implemented	PSS32	PSS32 /SFD-1...	
OPS	SF_Ex	Four Ended	Implemented	PSS32	PSS32 /SFD-4...	
OPS	SF_OT_Ex	Four Ended	Implemented	PSS32	PSS32 /PORT-1...	

END OF STEPS**Task: View a repeater associated with an OTS physical connection on the Routing Display**

Complete the following steps to view the repeater that is associated with an OTS physical connections on the Routing Display.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists all of the requested connections.

2

On the top right corner of the table, click on the **More** icon and select **Manage Columns**.

Search for **Repeater**, and select the **Repeater** check box. Click **APPLY**.

Figure 7-95 Physical Connections – manage repeaters – customize data table to view repeaters

The screenshot shows the 'Manage Columns' interface. The 'ALL' tab is active. Under 'Fixed Columns', several checkboxes are checked: 'OPERATIONAL STATE', 'NAME', 'FROM NE/PORT #1', 'TO NE/PORT #1', and 'ALARM STATUS'. In the 'DEFAULT COLUMNS' section, there are two columns of checkboxes. The second column contains a checkbox for 'REPEATER', which is checked and highlighted with a red border. At the bottom right of the dialog are buttons for 'CANCEL', 'RESET', 'APPLY', and 'APPLY & SAVE'.

Result: The system adds the **Repeater** column to the currently displayed data table.

3

Scroll down the data table list to view which physical connections have the **Repeater** column checked.

Example: In the following figure, the Repeater is illustrated within the red box.

Figure 7-96 Physical Connections – manage repeaters – Repeater column – view repeaters

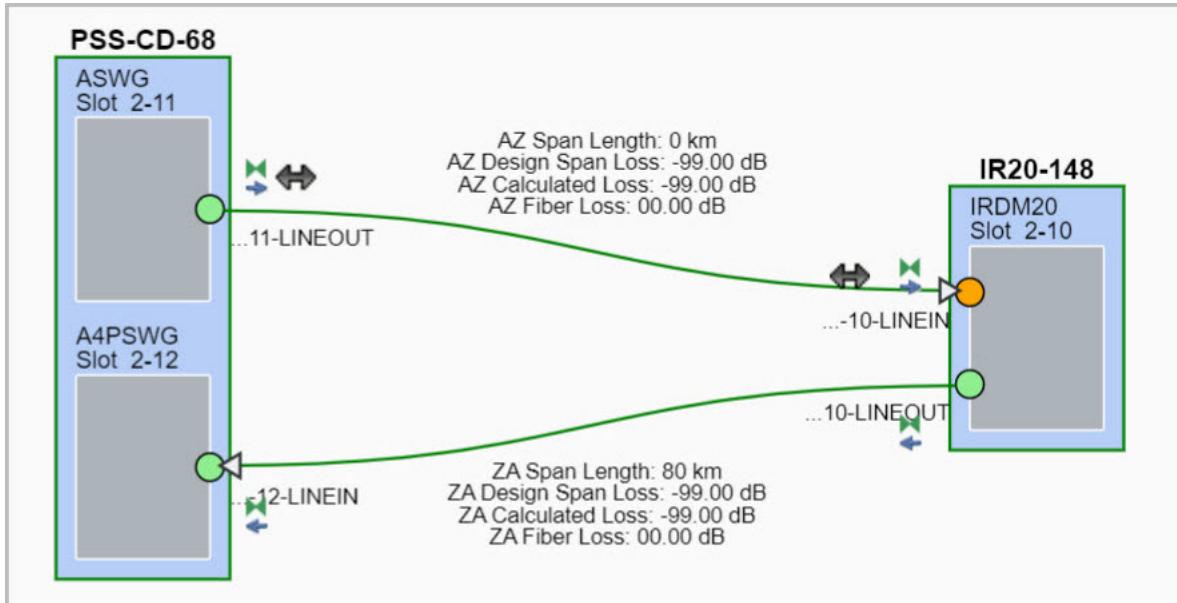
W..	Name	Shape	Implementation ...	From NE/...	To NE/Port #1	Repeater
<input type="checkbox"/>	OTS PSS32 /OPS-3-30...	Simple	Implemented	PSS32	PSS32 /OPS-3...	<input checked="" type="checkbox"/>
<input type="checkbox"/>	OTS PSS32 /IROADM-2...	Four Ended	Implemented	PSS32	PSS32 /IROADM...	<input checked="" type="checkbox"/>
<input type="checkbox"/>	OTS PSS32 /IROADM-3...	Simple	Implemented	PSS32	PSS32 /OPS-3...	
<input type="checkbox"/>	OTS PSS32 /IROADM-2...	Four Ended	Implemented	PSS32	PSS32 /IROADM...	
<input type="checkbox"/>	OTS PSS32 /AHPHG-1...	Simple	Implemented	PSS32	PSS32 /AHPH...	
<input type="checkbox"/>	OPS SF_CI	Four Ended	Implemented	PSS32	PSS32 /SFD-1...	
<input type="checkbox"/>	OPS SF_Ex	Four Ended	Implemented	PSS32	PSS32 /SFD-4...	
<input type="checkbox"/>	OPS SF_OT_Ex	Four Ended	Implemented	PSS32	PSS32 /PORT-1...	

4

Select one of the OTS physical connections in which the **Repeater** column is checked and select the **Routing Display** icon.

Result: The system displays the Routing Display for the selected OTS physical connection.

Figure 7-97 Physical Connections – manage repeaters – repeater on the Routing Display



In the routing display, 1830 SLTE and 1830 LX repeaters are displayed as brownie icon along with the direction (TX/RX) and the 1830 LX OSC-WC is displayed as bidirectional icon, as displayed in the following figure.

Important! Once a repeater is removed, the repeater/icon is no longer displayed on the Routing Display.

END OF STEPS

Task: View a repeater associated with an OTS physical connection on the Network Map

Complete the following steps to view the repeater that is associated with an OTS physical connections on the Routing Display

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Network Map

Result: The system displays the Network Map.

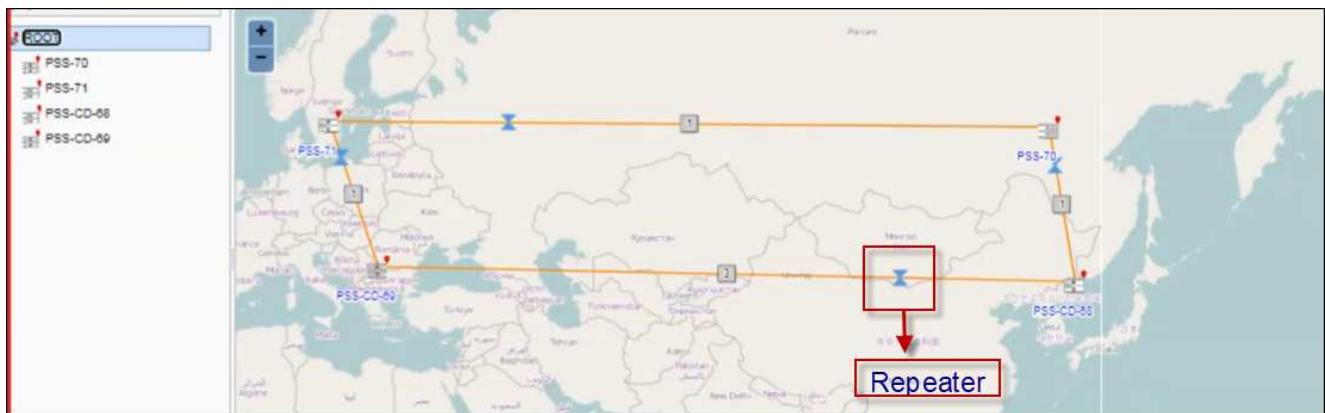
2

Using the left tree, navigate to the particular node/repeater on the tree.

Result: The system adjusts the Network Map to display the particular node/repeater that you selected.

Example: In the following figure, the node/repeater is illustrated within the red boxes.

Figure 7-98 Physical Connections – manage repeaters – repeater on the Network Map (Legacy)



Important! Once a repeater is removed, the repeater/icon is no longer displayed on the Network Map.

END OF STEPS

Task: View a repeater associated with an OTS physical connection from the physical connection list

Complete the following steps to view the 1830LX, 1830LX OSC-WC, and GenericNE_RedC repeaters associated to an OTS physical connections, from the Physical Connection list.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays the Physical Connections window.

2

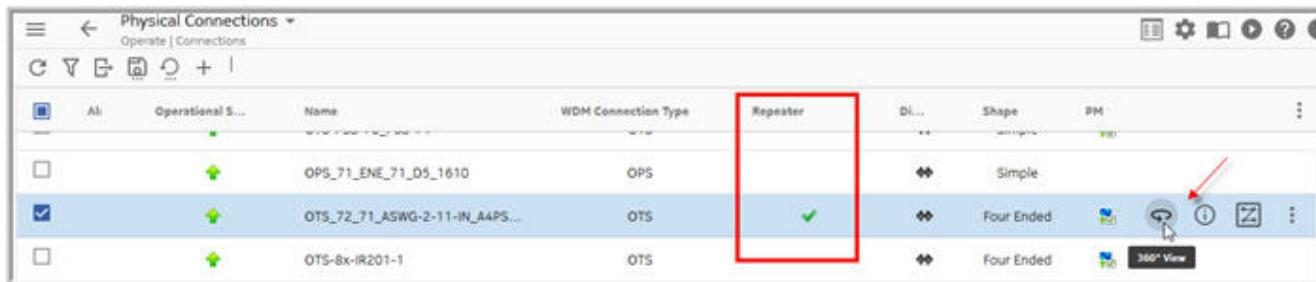
Click **Manage Columns**.

From the list check **Repeaters** and click **Apply** to add the column of the available repeaters to the list.

3

Select the **OTS** link of which you want to display the repeater and click on **360° View** icon.

Figure 7-99 Physical Connections – manage repeaters – Physical Connections list



Result: The system displays the **360° View** window with all the available tabs.

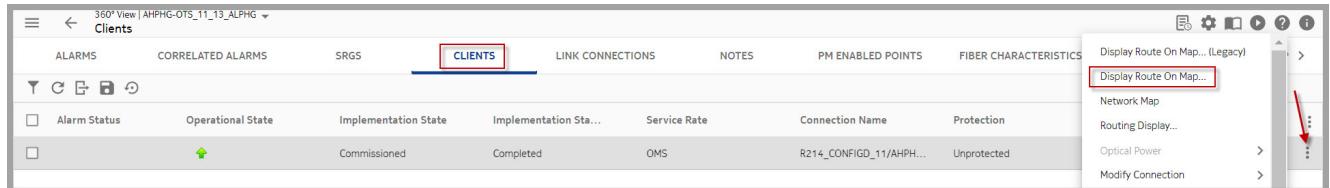
4

In the **Clients** tab select the OMS connection.

5

Click on the **More** icon and select the command: **Display Route on Map...**

Figure 7-100 Physical Connections – manage repeaters – clients - Display Route on Map

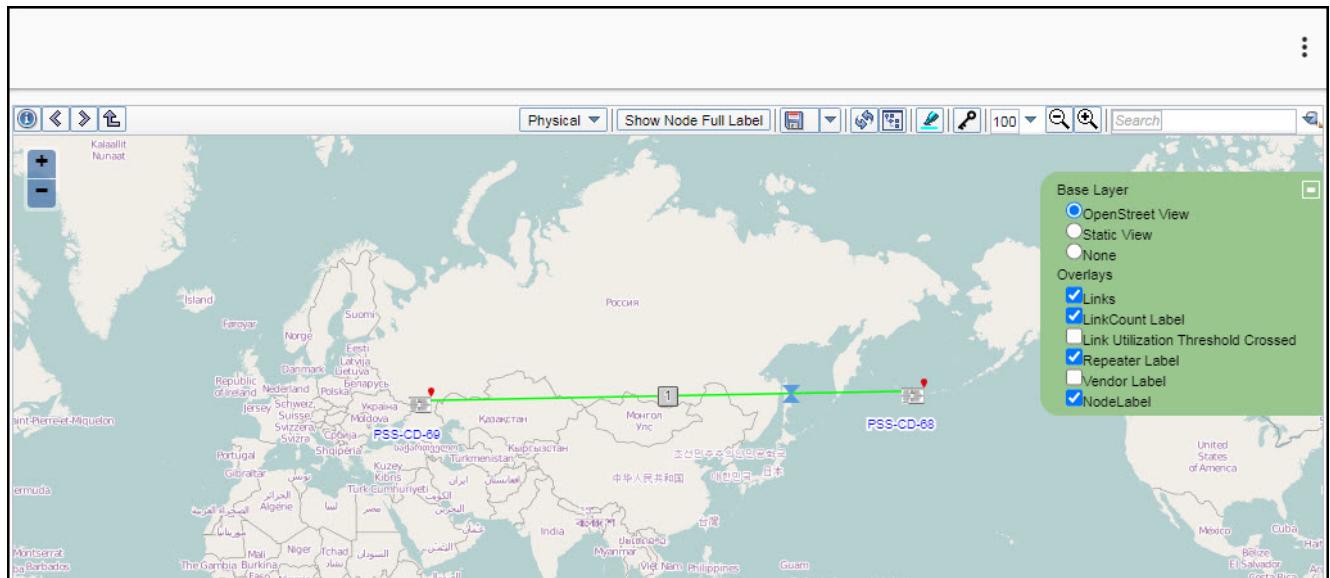


Result: The system displays the Network Map window.

6

Click the plus icon on the right side of the map and select **Repeater Label** to display the repeater on the map.

Figure 7-101 Physical Connections – manage repeaters – Network Map



END OF STEPS

7.36 Manage third party vendor networks for a physical connection

When to use

Use this multi-task procedure to manage third party vendor networks for an OTN physical connection.

Related information

When optical traffic is carried over a third party vendor network, you can associate that traffic with a physical connection. Once you associate a physical connection with a third party vendor network, you can then view this link on the Physical Connections data table, the Routing Display, and the Network Map.

In addition, see the following topic in this document: [2.15 “Physical connections” \(p. 220\)](#).

Before you begin

The physical connection must be created and must be listed in the OTN Physical Connections data table.

Task: Associate a Third Party Vendor Network with an OTN physical connection

Complete the following steps to associate a third party vendor network with an OTN physical connection.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

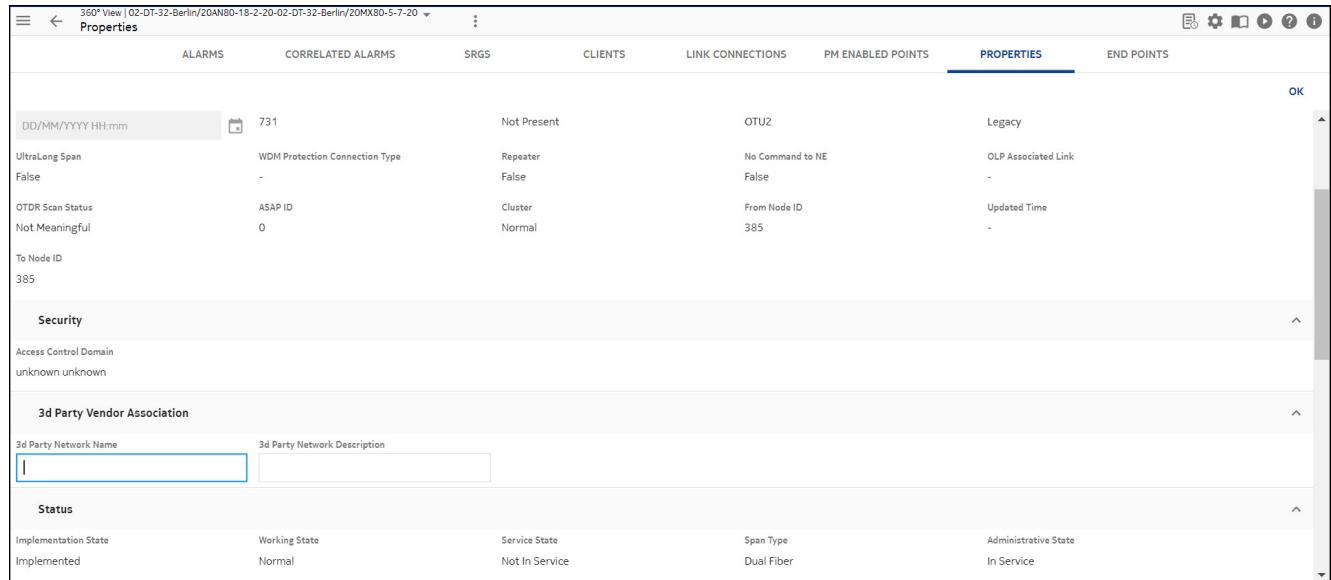
Result: The system displays a data table that lists all of the requested connections.

2

Select the OTN physical connection with which you want to associate a third party vendor network and click the **360° View**  icon, then select the **PROPERTIES** tab.

Result: The system activates the **PROPERTIES** tab.

Figure 7-102 Physical Connections – associate Third Party Vendor Network – window and properties tab

**3**

Scroll down the page up to the **3d Party Vendor Association** panel.

4

In the **3d Party Network Name** field, enter a name to identify the third party vendor network.

5

In the **3d Party Network Description** field, enter wording that describes the third party vendor network.

6

Click the **OK** icon, which is located to the upper right of the **PROPERTIES** tab.

Result: The system saves the third party vendor network information that you have added and displays the information in the **3d Party Network Name** and **3d Party Network Description** columns of the Physical Connections data table.

END OF STEPS

Task: Remove a Third Party Vendor Network association from an OTN physical connection

Complete the following steps to remove a third party vendor network association from an OTN physical connection.

-
- 1 From the NFM-T GUI, follow this navigation path:
OPERATE > Physical Connections
Result: The system displays a data table that lists all of the requested connections.
 - 2 Highlight and select the OTN physical connection with which you want to remove its third party vendor network association and click on the **360° View**  icon, then select the **PROPERTIES** tab.
 - 3 Scroll down the page up to the **3d Party Vendor Association** panel.
 - 4 In the **3d Party Network Name** field, manually swipe the text that appears in the field and press the **Delete** button on your keyboard.
Result: The system removes the content and restores a blank field.
 - 5 In the **3d Party Network Description** field, manually swipe the text that appears in the field and press the **Delete** button on your keyboard.
Result: The system removes the content and restores a blank field.
 - 6 Click the **OK** icon, which is located to the upper right of the **PROPERTIES** tab window.
Result: The system removes the third party vendor network information from the **3d Party Vendor Association** panel and from the **3d Party Network Name** and **3d Party Network Description** columns of the Physical Connections data table.

END OF STEPS

Task: View a list of third party vendor networks that are associated with an OTN physical connection

Complete the following steps to view a list of third party vendor networks that are associated with an OTN physical connection.

- 1 From the NFM-T GUI, follow this navigation path:
OPERATE > Physical Connections
Result: The system displays a data table that lists all of the requested connections.

2

Click on the three dots icon that is located in the upper right corner of the data table, then select **Manage Columns....** Search for **3d Party Network Name** and **3d Party Network Description**, and check the boxes for **3d Party Network Name** and **3d Party Network Description**.

Result: The system adds the **3d Party Network Name** and **3d Party Network Description** columns to the currently displayed data table.

END OF STEPS

Task: View a Third Party Vendor Network that is associated with an OTN physical connection on the Network Map

Complete the following steps to view a third party vendor network is associated with an OTN physical connection on the Network Map.

1

From the NFM-T GUI, follow this navigation path:

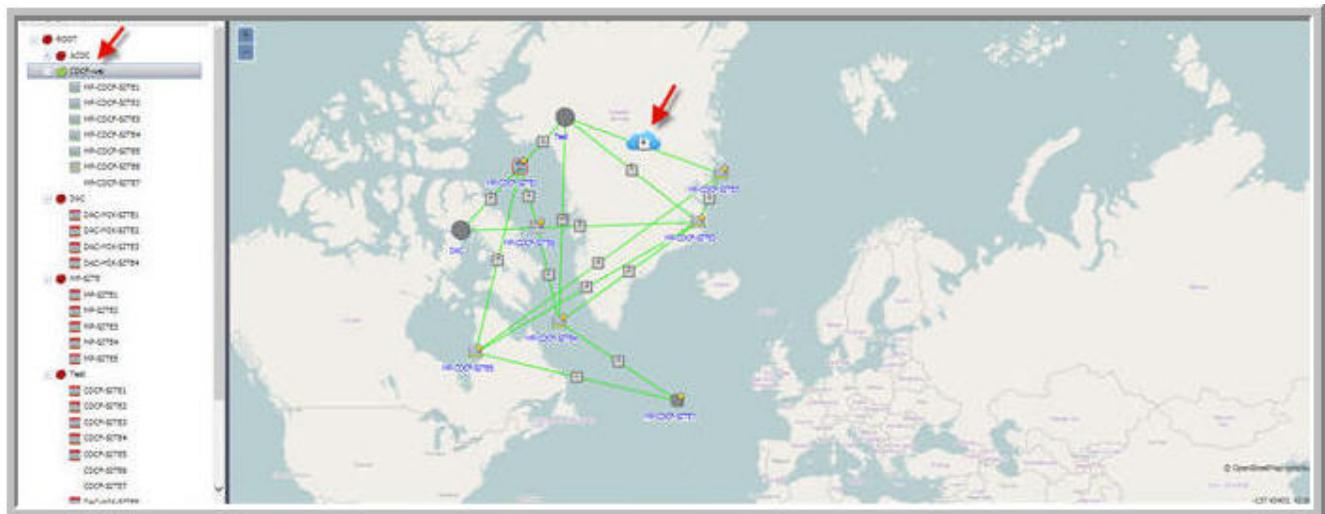
OPERATE > Network Map

Result: The system displays the Network Map. The system displays all nodes and connections. Third party vendor networks are identified by a blue cloud icon.

2

In the appropriate subnetwork, look for the blue cloud icon.

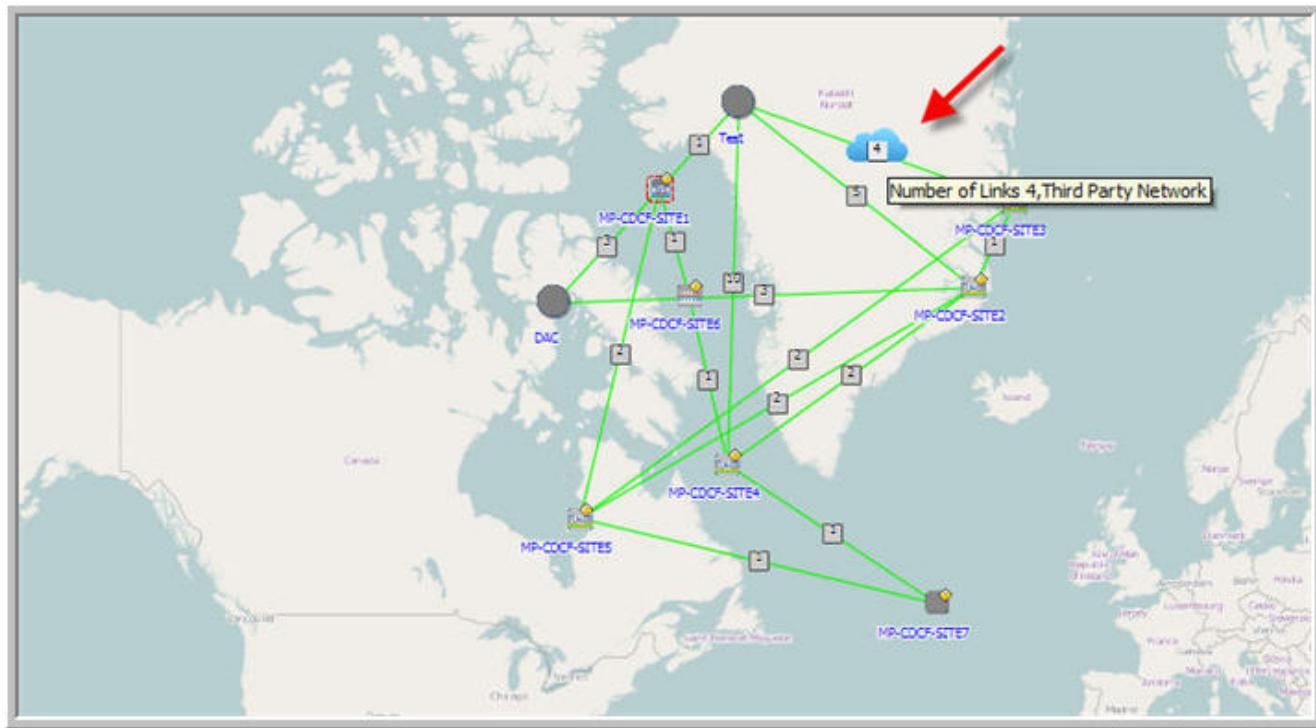
Figure 7-103 Physical Connections – Third Party Vendor Network – Network Map (Legacy)



3

Optional: Mouse over the **Third Party Vendor Network** icon to reveal the number of links in the network.

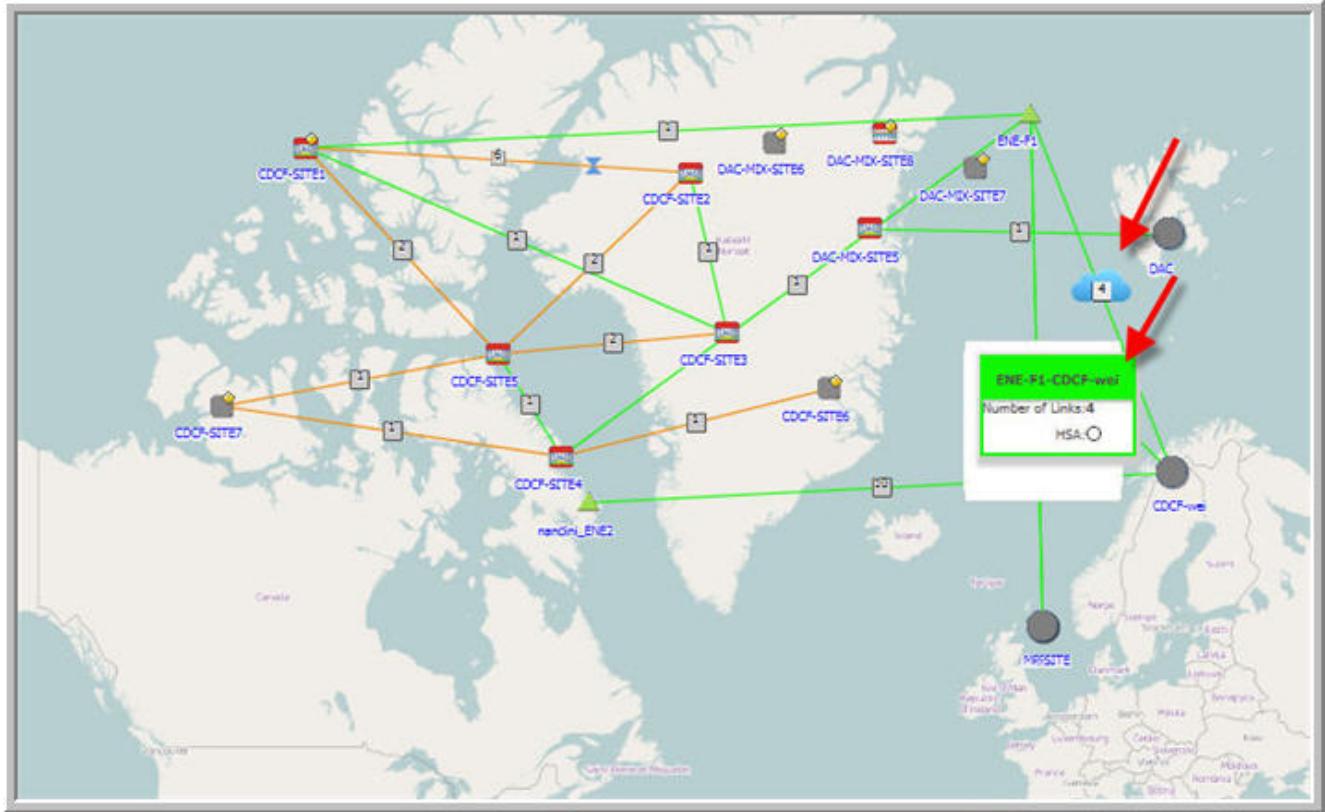
Figure 7-104 Physical Connections – Third Party Vendor Network – Network Map – Number of Links (Legacy)



4

Optional: Click on the **Third Party Vendor Network** icon to display vendor details.

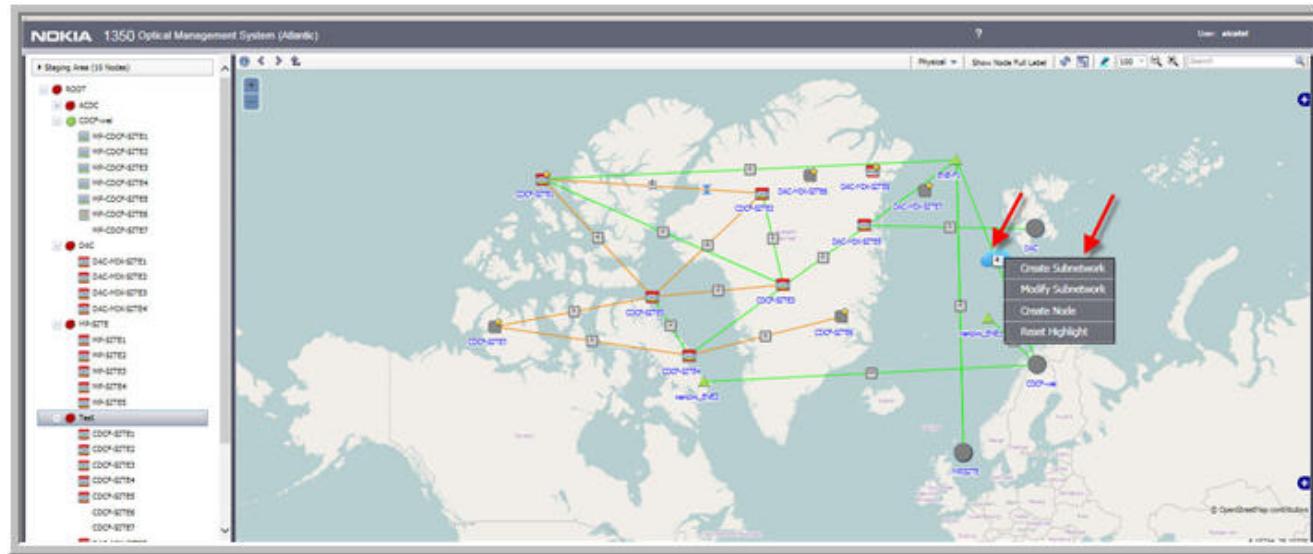
Figure 7-105 Physical Connections – Third Party Vendor Network – Network Map – details (Legacy)



5

Optional: Right click on the **Third Party Vendor Network** icon to display actions.

Figure 7-106 Physical Connections – Third Party Vendor Network – Network Map – Right Click Actions (Legacy)



Result: The system enables you to **Create Subnetwork**, **Modify Subnetwork**, **Create Node**, or **Reset Highlight**.

6

Optional: Click on the **Third Party Vendor Network** icon to associated physical connections.

Result: The system opens a new browser tab and displays the associated physical connections.

END OF STEPS

Task: View a Third Party Vendor Network that is associated with an OTN physical connection on the Routing Display

Complete the following steps to view a third party vendor network that is associated with an OTN physical connection on the Routing Display.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists all of the requested connections.

2

Optional: To determine if a physical connection is associated with a third party vendor network, Click on the three dots icon that is located in the upper right corner of the data table, then select **3d Party Network Name** and **3d Party Network Description**, and check the boxes for **3d Party Network Name** and **3d Party Network Description**.

Result: The system adds the **3d Party Network Name** and **3d Party Network Description** columns to the currently displayed data table.

3

Select a connection that is known to be associated with a third party vendor network and click the **Route Details**.

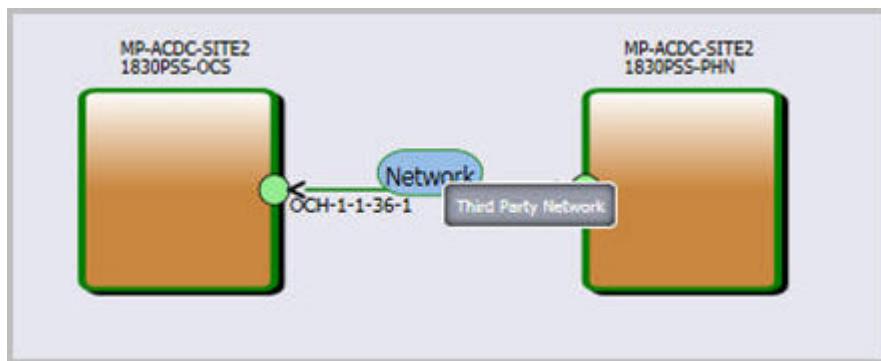
Result: The system activates the **Route Details**.

4

In **Routes**, select the **Graph** tab.

Result: The system opens a new browser tab and displays the selected connection on the Routing Display. The selected connection is indicated by the word **Network**.

Figure 7-107 Physical Connections – associate Third Party Vendor Network – Routing Display

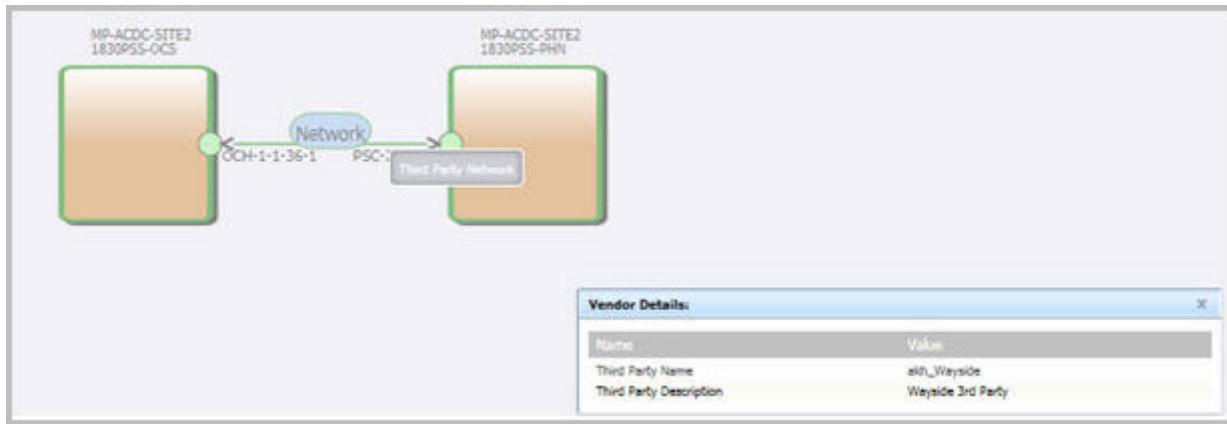
**5**

Optional: Mouse over the **Network** icon to reveal the **Third Party Network** pop-up.

6

Optional: Click on the **Network** icon to display **Vendor Details** details.

Figure 7-108 Physical Connections – associate Third Party Vendor Network – Routing Display – Vendor Details



END OF STEPS

7.37 Modify the fiber characteristics of an OTN physical connection

When to use

Use this task to modify the fiber characteristics of an OTN physical connection.

Related information

If the fiber length and fiber type values for a physical connection are present in the EPT file during the commissioning process of a new network or sub-network, the same values are configured for the connection in the process of commissioning the new network. See [11.4 “OTS fiber characteristics configuration using CPB” \(p. 1603\)](#).

Before you begin

The physical connection must be created and displayed on the data table for physical connections.

Task

Complete the following steps to modify fiber characteristics of an OTN physical connection.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

Result: The system displays a data table that lists the OTN physical connections.

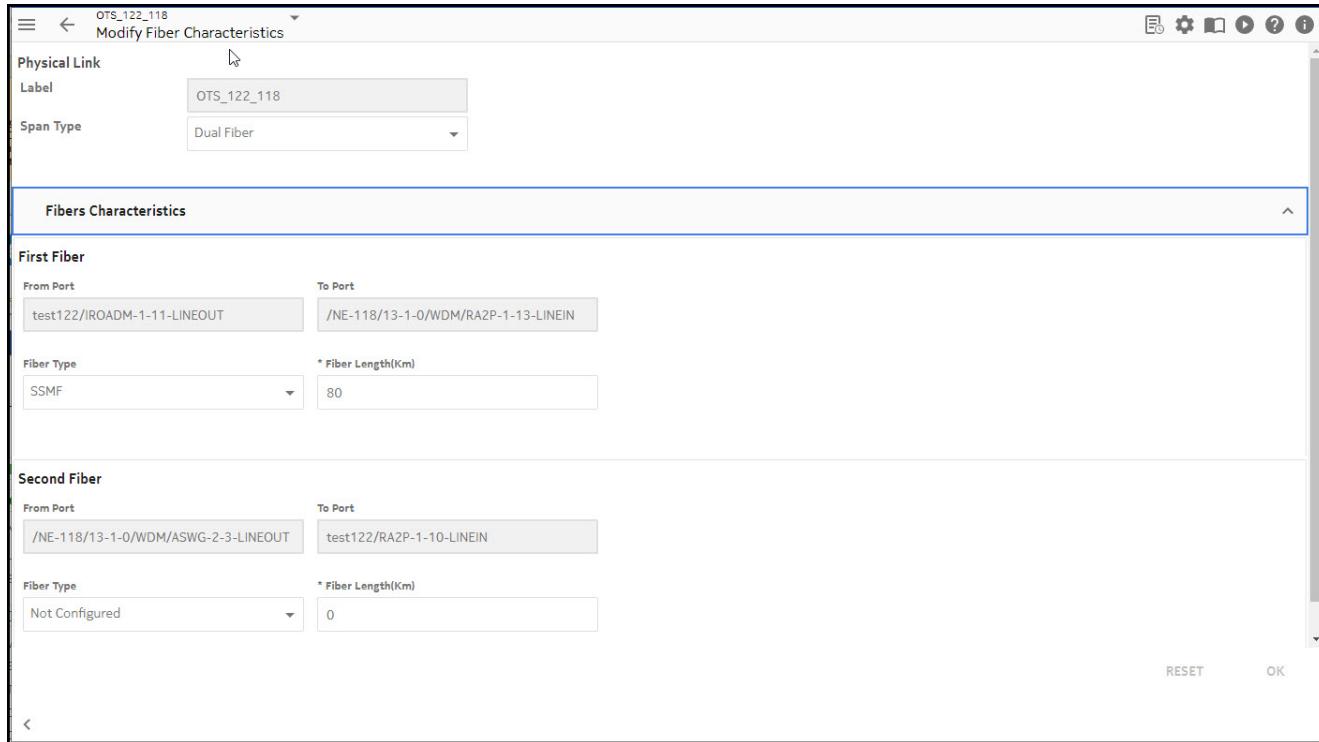
2

Select the connection and click on the **More**  icon on the right part of the row and follow this path: **Modify Fiber Characteristics**

Result: The system displays the **Modify Fiber Characteristics** window for the selected physical connection.

Refer to the following example:

Figure 7-109 Physical Connections – Modify Fiber Characteristics

**3**

In the **Fiber Type** drop-down list, select an appropriate fiber type.

4

In the **Fiber Length (Km)** drop-down list, enter the length of the fiber rounded to the nearest Km.

5

Click **Deploy**.

Result: The system makes the requested change and outputs a request submitted and then a success message at the bottom of the window.

6

Additionally: All fiber characteristics are resumed in the **Fiber Characteristics section**, click on the 360° View icon.

END OF STEPS

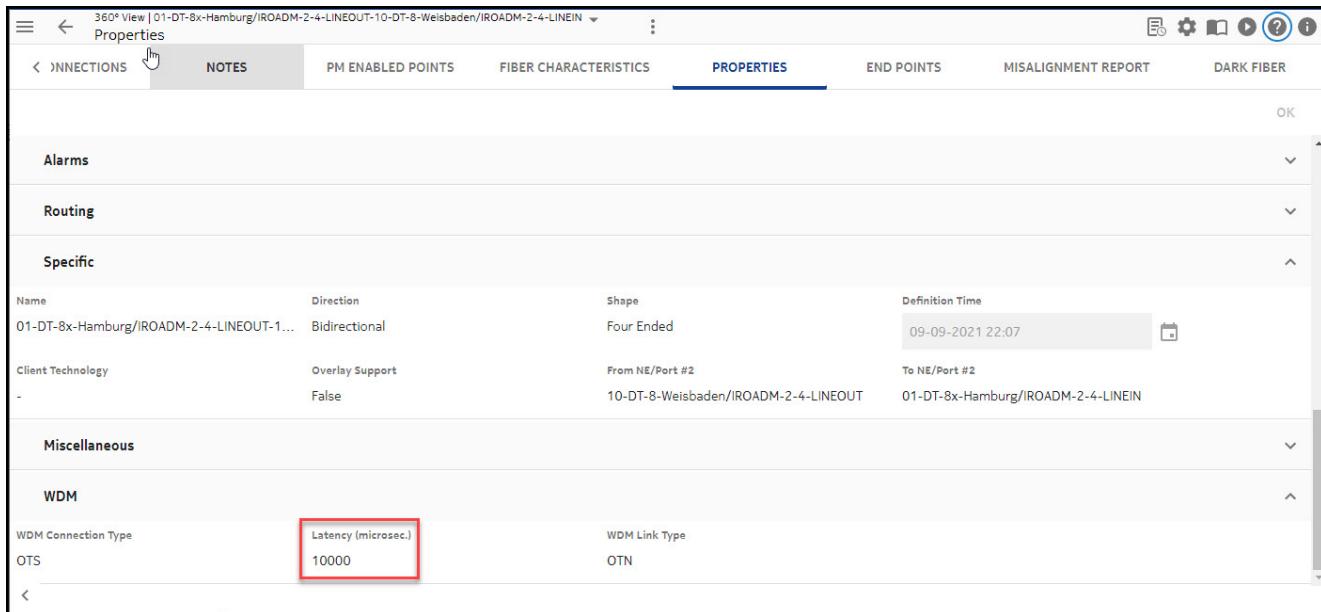
Correlation of fiber length with physical link latency

The physical link Latency is calculated on the physical links from the fiber length set in the **Fiber Characteristics** panel and the value of Latency parameter can be seen in the **PROPERTIES** tab under **OTN PHYSICAL CONNECTIONS** tab.

To view the **Latency (microsec.)** on the NFM-T GUI, navigate to the following path :

OPERATE > Physical Connections > OTN PHYSICAL CONNECTIONS tab > **360° View > PROPERTIES** tab

Figure 7-110 Properties



The same Latency value is displayed from the **Properties** icon on a configured OTN physical connection.

Properties: 01-DT-8x-Hamburg/IROADM-2-4-LINEOUT-10-DT-8-Weisbaden/IROADM-2-4-LINEIN

NA	NA	0	
OTHER PROPERTIES			
Operational State Up	Name 01-DT-8x-Hamburg/IROADM-2-4-LIN...	From NE/Port #1 01-DT-8x-Hamburg/IROADM-2-4-LIN...	To NE/Port #1 10-DT-8-Weisbaden/IROADM-2-4-LI...
Alarm Status Cleared	PM 15m Started	PM 24h Started	Protection Unprotected
Service State Not In Service	Administrative State In Service	OLC State In Service	Cluster Normal
Colors Bits 0000.0000.0000.0000.0000.0000.0...	Latency (microsec.) 10000	From NE/Port #2 10-DT-8-Weisbaden/IROADM-2-4-LI...	Access Control Domain unknown unknown
OTDR Supported False	To NE/Port #2 01-DT-8x-Hamburg/IROADM-2-4-LIN...	Latest Note	ASAP Enabled
% Low Utilization Threshold 50	% High Utilization Threshold 80	Repeater False	% Utilization -
ASELL Status NA	Utilization Profile DEFAULT		
LATENCY			
ASON			
CLOSE			



Note: Latency parameter is not editable and is updated based on the calculation using a formula based on the average length of the fiber set at the A-Z and Z-A end points or using existing REST API interface for direct update of latency value on physical link. If the fiber length is not set during fiber configuration, then the system configures a default value of 10000 micro seconds. The fiber length value is also set from REST API interface and the CPB application.

7.38 Modify Utilization Profile for a physical/infrastructure connection

When to use

Use this task to modify the link utilization profile for a Physical or Infrastructure connection.

Related information

Refer to [22.1 “Link Utilization Profile” \(p. 1959\)](#).

Task: To modify Utilization Profile for a physical/infrastructure connection

Perform the following steps to modify the utilization profile of a physical or infrastructure connection:

1

From the NFM-T GUI, follow one of the following navigation paths:

- To modify a physical connection, **OPERATE > Physical Connections**.
- To modify an infrastructure connection, **OPERATE > Infrastructure Connections**.

Result: Depending on the selection, the system displays a data table listing the requested connections.

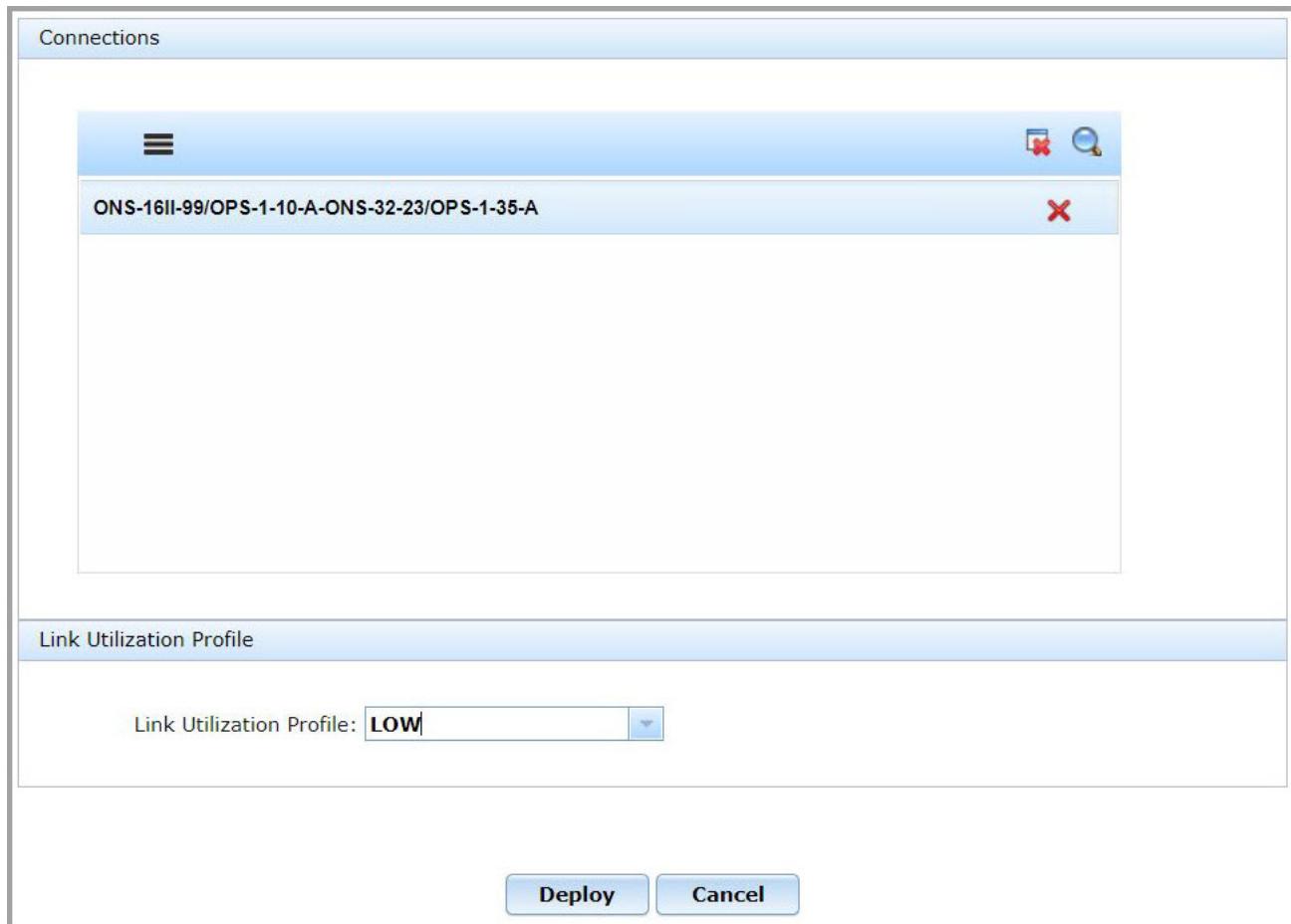
2

Select a connection from the list and click on the **More**  icon:

- For a physical connection, select **Modify Utilization Profile**.
- For an infrastructure connection, select **Modify Connection > Modify Utilization Profile**.

Result: The system displays the **Modify Utilization Profile** window.

Figure 7-111 Modify Utilization Profile window



3

In the connections panel, select the connection to be modified.

To include connections to the modification list:

- Click the search (**Select items from List**) icon.
Result: The physical connections window is displayed.
- Use the **Search** option to find the required connection, select the connection, and click **Add**.
Result: The connections are added to the modification list.

4

In the **Link Utilization Profile** panel, select the profile threshold from the drop-down. See [22.1 “Link Utilization Profile” \(p. 1959\)](#), to know in detail about Link Utilization Profiles.

5

Click **Deploy**.

Result: The system modifies the **% Utilization Threshold**, displays a success message in the status bar at the bottom of the connections window.

END OF STEPS

7.39 Rename an OTN physical connection or/and of its port on an ENE

When to use

Use this task to modify the label of an OTN physical connection and/or of its port that is on an ENE.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

The physical connection must be created and displayed on the data table for physical connections.

The Modify Labels window provides you with the current label that is used to identify the physical connection and it provides you with the A and Z node and port names.

Task

Complete the following steps to modify the label of an OTN physical connection and/or of its port that is on an ENE.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists the OTN physical connections.

2

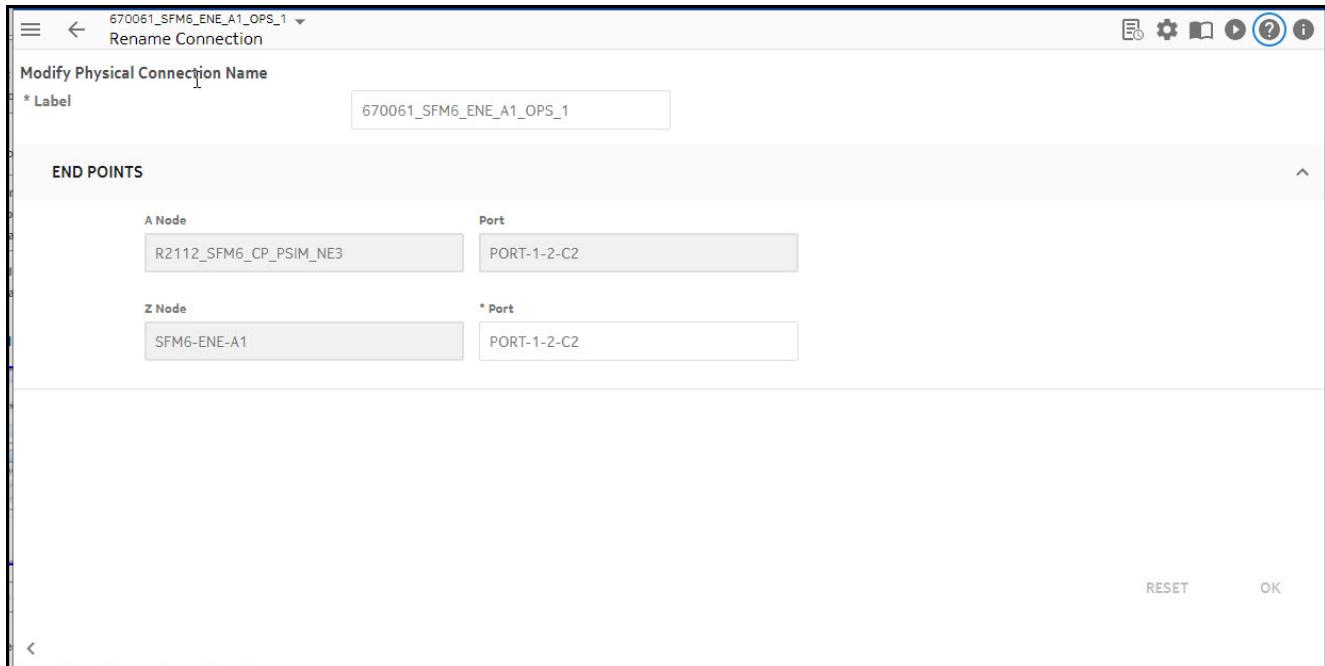
Select the connection and click on the **More**  icon and follow this path: **Rename Connection**.

Result: The system displays the **Rename Connection** window for the selected physical connection.

Refer to the following example:

Rename an OTN physical connection or/and of its port on an ENE

Figure 7-112 Physical Connections – Rename Connection



3

In the **Label** field, change the name of the label that is used to identify the physical connection. For more information on the label, see [7.19.9 “Physical connection User Label” \(p. 804\)](#)

4

Click **OK**.

Result: The system makes the requested change and outputs a request submitted and then a success message at the bottom of the main window.

Figure 7-113 Physical Connections – Rename Connection – Success



END OF STEPS

7.40 View a misalignment report for an OTN physical connection

When to use

Use this task to view a misalignment report for an OTN physical connection.

Related information

See the following topics in this document:

- “Three dots more... icon” (p. 2196)
- 2.15 “Physical connections” (p. 220)

Before you begin

You view a misalignment report for an OTN physical connection for the following types of connections by using the steps that are provided in this task:

- Physical connections
- PM enabled points of a selected physical connection
- Impacted connections for a selected physical connection
 - Impacted connections are those physical connections that are associated with a selected node and its current operational and alarm state.
- Used ports for a selected physical connection
 - Used ports are those physical connections that are assigned to a port address on a selected node.

If the selected physical connection does not have any misaligned objects, the system responds with the following message:

No results found.

Task

Complete the following steps to view a misalignment report for an OTN physical connection.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Physical Connections

OPERATE > Node > Impacted Connections (tab)

OPERATE > Node > Used Ports (tab)

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Click on the **More**  icon on the physical connection for which you want to view its not aligned objects and follow this path: **Misalignment Report**.

Result: The system displays a data table that lists the misaligned objects for the selected physical connection.



Note: The misalignment report displays data only for objects involving ASON SNC links for Control Plane connections.

END OF STEPS

7.41 View Physical Connections

Purpose

Use this task to view a list of physical connections.

Task

Complete the following steps to display the list of physical connections.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists the physical connections.

Figure 7-114 Physical Connections – Physical Connections data table

A..	Operational S...	Name	WDM Connection Type	Di...	Shape	P...	P...	From NE/	...
<input type="checkbox"/>		LO_CBAND_NODE4/11QPA4-1-5...	OPS	↔↔	Simple			LO_CBAN	
<input type="checkbox"/>		OPS-RETEST-3	OPS	↔↔	Simple			LO_CBAN	🔗 ⓘ ⓘ
<input type="checkbox"/>		am2625physical8	OTS	↔↔	Simple	🕒	🕒	LO_CBAN	
<input type="checkbox"/>		LO_CBAND_NODE2/ASWG-7-3-LIN...	OTS	↔↔	Four Ended	🕒	🕒	LO_CBAN	
<input type="checkbox"/>		OCS-OTS	OTS	↔↔	Simple	🕒	🕒	SF-NE1/5	
<input type="checkbox"/>		OTS_8p_s13x	OTS	↔↔	Simple	🕒	🕒	10.41.85	
<input type="checkbox"/>	🕒	PSS32-42.37.6/AWBILA-1-B-LINE...	OTS	↔↔	Four Ended			PSS32-4...	
<input type="checkbox"/>		singlefibre-ots	OTS	↔↔	Simple	🕒	🕒	10.41.85	
<input type="checkbox"/>		YCABLE-OTS1	OTS	↔↔	Simple	🕒	🕒	SF-NE1/5	...

2

Optional: To view the details of a selected connection in the data table, refer to “[View additional attributes for a selected item in a data table](#)” (p. 2194).

3

Optional: To manipulate the view of the data table, refer to the following for direction:

- “[Sort a single column in a data table](#)” (p. 2187)
- “[Manage the columns displayed in a data table](#)” (p. 2192)

The column **ASON NPA Name** can also be used to sort and filter the OTN Physical Connection list. **ASON NPA Name** column is not shown in primary inventory list but can be added customizing the table view.

4

Optional: To perform additional actions on a selected connection in the data table, refer to the following for direction: “[Three dots more... icon](#)” (p. 2196).

5

Optional: To export the contents of the data table that is currently displayed to a **.CSV** file, refer to the [26.6 “Export a Data Table to a .csv File” \(p. 2209\)](#) task for detailed steps.

If you export data to **.CSV** file, the column **ASON NPA Name** is included in the output file.

6

Optional: If you have customized the filters, sorting or column order in data table and you want to save the same and/or if you want to reset a customized view of the data table to its default display, refer to the [26.9 “Save or reset data table preferences on connections \(physical/infrastructure\) and services screen” \(p. 2220\)](#) task for detailed steps.

END OF STEPS

Observations

Some exceptions in the physical connections list:

- When the 2-Ended Split Bi OPS connection is created for single fiber scenario, a single OPS connection of shape *Four Ended* is displayed in the **Physical connections** list, while in the **Impacted connections** list and **Affected Clients** list, two Uni-directional connections of service rate OS are displayed.
- In case OPS creation is involving SFC to OT pack, the RX frequency column has only one frequency updated. If the user assigns frequency from NE user interface, the port synchronization action is mandatory to reflect the same in physical connections page. During DB delete scenarios of single fiber OPS, it is necessary to perform a port synchronization followed by path synchronization for single fiber connections.

7.42 View the 360° tabs for a physical connection

When to use

Use this task to view the tabbed topics for an OTN physical connection.

Task

Complete the following steps to view the tabbed topics for an OTN physical connection.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Physical Connections

Result: The system displays a data table that lists the OTN physical connections.

Figure 7-115 Physical Connections – OTN data table

Oper...	WDM Conn...	Name	Shape	Implementation ...	Working State	From NE/Port #1	To NE/Port #2	...
<input type="checkbox"/>		OTS	30-CDCFIRD20-PSI-8L/OPS-1-8...	Simple	Implemented	Normal	30-CDCFIRD20-PSI-8L/OPS-1-8-A	27-iROADM
<input type="checkbox"/>		OTS	44-IRDM32-PSG32/OPS-1-17-A-1...	Simple	Implemented	Normal	44-IRDM32-PSG32/OPS-1-17-A	12-CDCF-I
<input type="checkbox"/>		OTS	AlienWavelengthbank_OTS	Four Ended	Implemented	Normal	06-CDCF-IRD20-MCS816/iROADM...	12-CDCF-I
<input type="checkbox"/>		OTS	MP_OTS_WDM-PRO2-CAS-R13-F...	Simple	Implemented	Normal	06-CDCF-IRD20-MCS816/AHPLG...	07-C-F-V
<input type="checkbox"/>		OTS	MP_OTS_WDM-PRO2-CAS-R13-F...	Simple	Implemented	Normal	MP_OP_Node-24/AHPLG-18-6-LINE	12-CDCF-I
<input type="checkbox"/>		OTS	MP_OTS_WDM-PRO2-CAS-R13-F...	Simple	Implemented	Normal	06-CDCF-IRD20-MCS816/AHPLG...	07-C-F-WR
<input type="checkbox"/>		OTS	MP_OTS_WDM-PRO2-CAS-R13-F...	Simple	Implemented	Normal	12-CDCF-IRD20MCS1615/AHPLG...	24-CDC-F-

2

To view the tabbed topics for a physical connection select a physical connection in the data table and click on the **360° View** icon.

Figure 7-116 Physical Connections – tabbed topics

NE	NE Severity	Port	NE SA/NSA	Alarm Type	NE Probable Cause	Time Raised	NML Probable
44-IRDM32-PSS32	C	OPSA-1-17	Service Affecting	Primary	Card missing	10/12/2021 9:33:24 AM	
44-IRDM32-PSS32	C	OPSA-1-17	Service Affecting	Primary	Card missing	10/12/2021 9:33:24 AM	
12-CDCF-IRD20MCS1615	C	OPSA-1-17	Service Affecting	Primary	Card missing	10/12/2021 3:46:01 PM	
12-CDCF-IRD20MCS1615	C	OPSA-1-17	Service Affecting	Primary	Card missing	10/12/2021 3:46:01 PM	
44-IRDM32-PSS32	C	IRDM32-1-14	Service Affecting	Primary	Card missing	10/12/2021 9:33:24 AM	
12-CDCF-IRD20MCS1615	C	IRDM20-1-15	Service Affecting	Primary	Card missing	10/12/2021 3:46:01 PM	
44-IRDM32-PSS32	C	OPSA-1-17	Service Affecting	Primary	Card missing	10/12/2021 9:33:24 AM	
12-CDCF-IRD20MCS1615	C	OPSA-1-17	Service Affecting	Primary	Card missing	10/12/2021 3:46:01 PM	

The available tabbed topics are the following:

- [25.6 “ALARMS Tab” \(p. 2066\)](#)
- [25.16 “Correlated Alarms Tab” \(p. 2093\)](#)
- [25.51 “SRGs Tab” \(p. 2164\)](#)
- [25.11 “Clients Tab” \(p. 2080\)](#)
- [25.42 “Routes Tab” \(p. 2145\)](#)
- [25.28 “Link Connections Tab” \(p. 2117\)](#)
- [25.31 “Notes Tab” \(p. 2123\)](#)
- [25.7 “ASON Links Tab” \(p. 2069\)](#)
- [25.36 “PM Enabled Points Tab” \(p. 2135\)](#)
- [25.23 “Fiber Characteristics Tab” \(p. 2105\)](#)
- [25.39 “Properties Tab” \(p. 2141\)](#)
- [25.19 “End Points Tab” \(p. 2098\)](#)
- [25.18 “Dark Fiber Tab” \(p. 2097\)](#)

Important usability notes:

- The **Fiber Characteristics** tabbed topic is only displayed for OTS physical connections. The system provides information for all supported amplifier configurations.
- The icons and right click functions that are provided with the **SRGs** tabbed topic are the same icons and right click functions that are provided when you access this object directly from the **OPERATE > Network Profiles > Shared Risk Groups** navigation path. All detailed tasks for SRGs can be found in the [“Shared Risk Group \(SRG\)” \(p. 603\)](#) section.

-
- The data table that is displayed for the **Clients** tabbed topic lists both infrastructure and service connections. If you click on an infrastructure or service connection in the data table, the system changes the icons and functions according to your selection. All detailed tasks for **Clients** can be found in the “[Infrastructure Connections and Services](#)” (p. 913) section.

- From the **Alarms** tabbed topic, you can access the Equipment Manager.

Result: The system activates the tabs and the connection-related information is displayed in a new window.

Note: To return to the original data table, click the back arrow at the top left of the data table screen.

3

Optional: To view the details of a selected OTN item, click on the **i** icon.

Result: The system displays detailed information for the selected item.

END OF STEPS

7.43 Physical Connections list further actions

Users can select an item in a data table, click on the **More**  icon, and view a list of additional navigation and action options for that item.



Note: The selection of the following menus depend from the type of the selected object, depending on the type some of the described items may be disabled for the object selected.

From the physical connections List, selecting an object, in this case a physical connection, the user can access different Actions that are possible for the selected object.

Menu item	Second level menu item	Description
Routing Display		Shows the physical connection routing display. The Routing Display is the graphical representation of the connections. Moreover, helps to view all the circuit packs involved in the routing of physical connection. See 7.78 "View the Routing Display of a selected connection" (p. 1042)
Optical Power	A to Z Ingress/Egress Power	Activate the window displaying Ingress/Egress A/Z power and allowing adjustments. See 17.14 "Manage optical power of an OTN OTS connection" (p. 1846)
	Z to A Ingress/Egress Power	
	Export to Excel	Export the Optical Power data in Excel sheet. See 17.14 "Manage optical power of an OTN OTS connection" (p. 1846)
Rename Connection		The physical connection label can be modified. See 7.39 "Rename an OTN physical connection or/and of its port on an ENE" (p. 884)
Modify Utilization Profile		Allows to modify the utilization profile. Applicable only for OTS connections. See 7.38 "Modify Utilization Profile for a physical/infrastructure connection" (p. 881) .
Modify Fiber Characteristics		The Fiber Characteristics are available only for OTS physical connections. See 7.37 "Modify the fiber characteristics of an OTN physical connection" (p. 877)
Correlate SRG		Allows to correlate the physical connection to a Shared Risk Group. A single physical connection may belong to several SRGs in different sections. See 7.28 "Correlate an OTN physical connection with an SRG" (p. 827)
Add/Remove Repeaters		Allows to add or remove a repeater which can be a line amplifier or a standalone NE that functions as a repeater. See 7.35 "Manage repeaters for an OTN OTS physical connection" (p. 850)
Delete Connection		Deletes the physical connection in NFM-T and the NE. When there is a synchronization operation, the deleted connection is not rediscovered.
Deployment Control	Implement/Deimplement	See 7.31 "Implement/Deimplement an OTN physical connection" (p. 835)
	Delete from NFM-T	Deletes the OPS/OTS physical connection from the NFM-T database and not from the NE. When there is a synchronization operation, the deleted connection is rediscovered from the NE by executing the external link discovery operation. See 7.23 "Delete OTS and OPS connections from NFM-T" (p. 815)
	Set Service State (In Service/Not In Service)	Allows to set the service state.

Menu item	Second level menu item	Description
Alarms	Set Default ASAP	This action allows to restore the alarm severities to NE/Node defaults through ASAP. See "Task: Set Default ASAP" (p. 820)
	Enable Alarm Reporting	Enables the reporting of alarms on the selected physical connection. See 7.53 "Manage alarms for a connection" (p. 924)
PM	Modify PM	Modifies the PM settings for a physical connection. See Manage PM for an OTN Physical Connection in the <i>NFM-T Service Assurance Guide</i> .
	Clear PM Bin	Removes the PM bin counters for the selected Physical Connection. See Manage PM for an OTN Physical Connection in the <i>NFM-T Service Assurance Guide</i> .
OA&M Diagnostics ...		The system opens a new browser tab and displays the OA&M Diagnostics window. The window has the traditional MW-INT Routing Display of the selected connection on the top and Summary and Real-Time panels on the bottom, which display PM data for a subset of the ports that are related to the connection. By default, the end points of the connection are displayed. See 24.5 "Quick Help – The OA&M Diagnostics Window" (p. 1990)
Misalignment Report		The system displays a data table that lists the misaligned objects for the selected physical connection.
Create Network Data File		Allows to generate a network data file for the selected physical connection. See "Task: Create Network Data Files" (p. 1936)
OLC State	Set To Maintenance	Allows the user to configure the OLC state of a physical connection to in service or maintenance.
	In Service	See 2.21 "Object Life Cycle (OLC) state" (p. 243) .
Correlate ASAP		By default, once a connection is created, it is assigned the default ASAP. You can correlate a different ASAP to a connection, the ASAP should be previously created. See 7.29 "Correlate an OTN physical connection with an ASAP" (p. 830)
OTDR	Baseline	Associate ports, delete association and scan Optical Time Domain Reflectometers (OTDR), OTDRM (Metro-optimized OTDR), and MON-OTDR cards.
	Troubleshoot	See 17.6 "Manage an OTDR Scan for an OTN OTS Physical Connection" (p. 1734) , for more information.
	Scan Now	
	Configure	
	Jobs	
Dark Fiber	Associate	Allows to associate or disassociate the physical connection to a dark fiber in the NE. This option is available only for OTS connections. See 7.24 "Associate/Disassociate dark fiber to physical connection" (p. 817) , for more details.
	Disassociate	See "Managing Dark Fibers" (p. 1804) , to know about dark fibers.
Fiber Characteristic	Import Fiber Route	Allows the user to create association of multiple fiber routes using a single KML file. See 17.8 "Manage fiber cut localization" (p. 1781)
	Delete Fiber Route	Allows the user to delete the single fiber associated to the physical connection. See 17.8 "Manage fiber cut localization" (p. 1781)
	Display Fiber Route on Map	Displays the Fiber Route on Network Map. See 17.8 "Manage fiber cut localization" (p. 1781)

Menu item	Second level menu item	Description
Insert Node		Inserts a node in the network.
Jobs for Insert Node		Opens the Job page with the node option for the selected physical connection.
Add Note		Allows the user to add notes for the selected object. See 24.9 "Manage Note for a Selected Object" (p. 2002)
Structure		Display the structure window of the selected connection.
Timeline		Display the activities performed on a specific date and time.
Route Details		Display the full Route details in a new window.

7.44 Physical Connections table columns

Description

To display the OTN Physical Connections table use the procedure [7.41 “View Physical Connections” \(p. 888\)](#)

Column	Description
% Utilization	The % Utilization column indicates the percentage of link utilization. It depicts the ratio between the total number of channels used and the total number of channels available. By default, the system assumes that the total number of channels available per band is 96. This field is displayed only when clients are created on the physical link. Only after the implementation state of the connections are Allocated it is considered for the link utilization calculation.
% Utilization Threshold	The % Utilization Threshold column indicates the link utilization threshold profile set for the connection. See 22.1 “Link Utilization Profile” (p. 1959) , to know more about Link Utilization Profiles.
3d Party Network Name	The 3d Party Network Name column displays a name to identify the third party vendor network.
3d Party Network Description	The 3d Party Network Description column displays a wording that describes the third party vendor network.
Access Control Domain	The Access Control Domain column displays the <AnodeACD> <ZnodeACD> values, that is the Node A access control domain value and the Node Z access control domain value, these two value can be different, so the connection is seen in the list but if the user does not belong to the Node A or Node Z control domain, no action is allowed on this connection. A user can see an object, for example the Connection, if one end belongs to the user's domain. A user may act on the object only if both ends belong to that user's domain.
Administrative State	If the ports involved in the end points of a physical connection are in Maintenance state, the physical connection is also in Maintenance Administrative state. See <i>NFM-T NE Management Guide</i> for more information about NE objects administrative state.
Alarm Status	The Alarm Synthesis column displays whether the node/NE is alarmed and the severity of the alarm. The Alarm Synthesis is: Minor , Critical , Major , or Cleared .
Alignment State	The Alignment State column displays icons that indicate whether the NE MIB and its image in the OS are aligned or not. The icons are status indicators; the system displays the status indicator when the icon is moused over. If an icon is not present in the column, the Alignment State is not known. The Alignment State includes the following status indicators: <ul style="list-style-type: none">• Transient: the system is performing a MIB Align Upwards operation. No operation can be done on the node/NE.• Aligned: the NE MIB and its image in the OS are the same.• Misaligned: the NE MIB and its image in the OS are not identical and eventually, the NE has to be re-configured.
ASAP	The ASAP displays the Alarm Severity Assignment Profile setting for the physical connection, which can be Not Set or Enabled .
ASAP Name	The ASAP Name displays the name of the Alarm Severity Assignment Profile to be default ASAP or the actual name of the ASAP.

Column	Description
ASON AutoRestoration	The ASON Auto Restoration column displays the state of the Automatic Switched Optical Network (ASON) automatic restoration to be Disabled , Enabled , Partially Enabled , or - (a dash, which means that it is not applicable).
ASON Administrative State	The Administrative State column displays the condition of the ASON link to be Locked , Unlocked , or Not Applicable . This parameter defines if the ASON link can be used by ASON to carry traffic.
ASON WTR	The ASON WTR column displays Automatic Switched Optical Network (ASON) wait time to restore (WTR) in minutes. The default is 60 .
A-Z Span Loss and Z-A Span Loss	Span Loss is the Quality of Service (QoS) alarm and is applicable only for ports of the Line Driver pack/amplifier pack (OTS rate).
Client Signal Type	The Client Signal Type of a physical connection can be the rate of the client signal or a -, which means that the client signal type is not meaningful or is unknown.
Colors Bits	The Color Bits column displays the Color representation in bits format, for example 0000.0000.0000.0000.0000.0000
Color Profile Name	The Color Profile Name column displays the color that is allocated to a Physical Connection. If the color profile is allocated, the color profile is displayed (Red , Green ...). If the color profile is not allocated, NoColor is displayed. NoColor is a neutral profile that does not contain any (zero, 0) colors. AllColors is a profile that is used for exclusions.
Commissioned Status	The Commissioned Status column displays whether the physical connection is Commissioned , Not Commissioned , or Not Applicable .
Current Frequency	The Current Frequency of a physical connection or ASON SNC is expressed as a number of cycles.
Dark Fiber Associated	The Dark Fiber Associated column displays a check mark, if the connection is associated to a dark fiber. A blank table cell indicates that the selected physical connection is not associated to any dark fiber. See 7.24 "Associate/Disassociate dark fiber to physical connection" (p. 817) .
Definition Time	The Definition Time column displays the date and time on which the physical connection or ASON link has been created.
Direction	The Direction is the direction of the physical connection, which is expressed as an arrow icon. When users mouse over the arrow icon, the Direction is displayed. For example: bidirectional .
Flex Grid Capable	The Flex Grid Capable columns displays if the connection is flexgrid capable, the values can be: Yes, No or Undefined. When the flex-grid capability can be determined, the values can only be Yes or 'No' When NFM-T is unable to determine whether an OTS link is flexgrid capable or not, Flex Grid Capable field is displayed as <i>Undefined</i> . This typically happens when the OMS link is not commissioned. The Flex Grid Capable connection parameter is only set when OMS is moved to commissioned state.
From NE and To NE	The To/From NE column displays the NEs in which the 2-ended connection originates (From NE) and terminates (To NE).
From Port 1/2 and To Port 1/2	The From Port 1 and To Port 1 columns display the ports where the 2-ended connection originates (From Port 1) and terminates (To Port 1). The From Port 2 and To Port 2 columns display the ports where the 3-ended or 4-ended connection originates (From Port 2) and terminates (To Port 2).

Column	Description
Implementation State	For an infrastructure connection or service, the Implementation State column displays whether the connection is Implemented , Commissioned , Allocated , Fully Allocated , or Defined . For a physical connection, the Implementation State column displays whether the connection is Implemented or Partially Implemented .
Last Calculated Span Loss Date	The Last Calculated Span Loss Date column displays the last date of the calculation of the Span Loss, that is the Quality of Service (QoS) alarm and is applicable only for ports of the Line Driver
Latency (microsec.)	The Latency (microsec.) column displays the time in microseconds for the selected physical connection. The latency is the time taken to deliver a packet from the source to the receiver, it includes propagation delay (the time taken for the electrical or optical signals to travel the distance between the two points) and processing delay. The default is 10000 micro seconds.
Link Type	The Link Type column displays the type of the link to be Legacy , Internal Link (i-nni) , or drop link .
NPA Name	The NPA Name column displays the NPA name in case the category of the Physical Connections is Control Plane. If the Physical Connection category is Managed Plane, no value is displayed in the corresponding column. The column is not shown in primary inventory list but it can be added on-demand per user customization. The column can be used for filtering the connections on the NPA name. The NPA Name column displays a name, if the NPA is associated to an OTS or OPS physical link; else the NPA Name column remains blank. See 26.2 "Data table description" (p. 2182) for details on the data tables.
OLC State	Indicates the OLC (Object Life Cycle) state of the selected physical connection. The values can be Maintenance and In Service . By default, the OLC State is In Service. This option allows the user to filter out alarms based on OLC state of a physical connection and hence suppress the display of alarms on physical connections in maintenance state. See 2.21 "Object Life Cycle (OLC) state" (p. 243) for more information.
OTDR Scan Status	The OTDR Scan Status column provides three status indicators <ul style="list-style-type: none"> An open symbol indicates that upcoming OTDR scans have not been scheduled. A green filled symbol indicates that an OTDR schedule exists and that the last scan was successful or has not yet been triggered. A red filled symbol indicates that the last OTDR scan that was run has failed. See 17.6 "Manage an OTDR Scan for an OTN OTS Physical Connection" (p. 1734)
OTDR Supported	The OTDR Supported column provides the following status indicators: <ul style="list-style-type: none"> A green check mark indicates that OTDR scans are supported on the selected physical connection. A blank table cell indicates that OTDR scans are not supported on the selected physical connection.
OTDR Summary	The OTDR Summary column provides the following status indicators: <ul style="list-style-type: none"> A red filled symbol indicates that there is a Fiber cut against the Baseline data. A yellow filled symbol indicates that there is no Baseline scan data. A white filled symbol indicates that there are no Fiber cuts.
PM 15m and PM 24h	The PM 15M and PM 24H columns display whether 15 minute or 24 hour performance monitoring data is being collected for the particular connection. Information is displayed as a check mark (is being collected) or empty box (is not being collected). Origin: Users specify whether 15-minute and/or 24-hour PM data should be collected during connection provisioning in the template Assurance panel.

Column	Description
RX Frequency and TX Frequency	The RX Frequency and TX Frequency indicates the Receive and Transmit frequency of the physical connection. Note: In case of single fiber, two frequencies appear in the RX Frequency and TX Frequency columns.
Service State	The Service State is displayed for logical and physical connections. The meaning of the Service State column differs for logical and physical connections. For logical connections, the Service State is based on the values of the alarm reporting parameter of the connection end points. If all connection end points have the alarm reporting parameter ON or if they have the primary state parameter set to IS-NR, IS-ANR, or OOS-AU, the Service State of the connection is ON . If any connection end point has the alarm reporting parameter OFF or if they have the primary state parameter set to OOS-MA or OOS-AUMA, the Service State of the connection is OFF . The Service State is NA for internal connectivities. In addition, determinations other than the connection end point regarding the Service State include the following: <ul style="list-style-type: none"> When a connection endpoint is on a black box, the alarm reporting parameter or the OT port that is connected to the black box determines the Service State and not the connection end point. For path connections with Y-cable protection, the alarm Reporting parameter of the OT client ports determines the Service State and not the connection end points. For path connections with OPSB Protection, the alarm Reporting parameter of the OT client ports determines the Service State and not the connection end points. For path connections with OPS protection, the alarm Reporting parameter of the OT/SVAC/MVAC client ports determines the Service State and not the connection end points. For physical connections, the Service State column displays whether the connection is Not in Service , In Service , or Maintenance .
Shape	For physical connections, the Shape of a physical connection can be simple or four ended .
Span Type	The Span Type column displays the type of the configuration fiber which can be Single Fiber or Dual Fiber . See 5.10 "Transmission over fiber" (p. 560)
SRG Present	The Srg present column displays whether Shared Risk Groups are Present or Not Present for the particular physical connection or ASON link.
WDM Connection Type	The WDM Connection Type column displays whether the physical connection is an OPS or an OTS connection.
Working State	The Working State column displays whether the working state of the NE or physical connection is Normal , Failed to Implement , Failed to Deimplement , or Failed to Assign Ports . For ASON SNCs, the Working State column displays one of the numerous working states of the selected ASON SNC.

Import Physical Connections and Nodes from CSV file

7.45 Import from CSV function

General

NFM-T supports import of CSV file to create a new Physical Connection or a new Node.

An option of downloading a CSV template file is provided from the **ADMINISTER > Import physical network > Import Physical Connections and Nodes** window. You can download a CSV template file and create a physical connection or a Node by importing the CSV template file from your local system.

Related import procedure are:

- [7.46 “Import Physical Connections from CSV file” \(p. 901\)](#)
- [7.47 “Import CSV Template file to Create a Node\(s\)” \(p. 907\)](#)

7.46 Import Physical Connections from CSV file

Description

NFM-T supports import of CSV file to create a new Physical Connection.

- The downloaded CSV template file is a sample file for reference. You can either use this file or the format and the parameters of the sample CSV template file to create a CSV file to import and create a new physical connection.
- This feature is supported only for bi-directional OPS and OTS physical connections involving real NEs or external NEs.
- As part of this feature, Network Access Domain (NAD) and Functional Access Domain (FAD) validations are also performed by system while importing the template, the nodes involved in the physical connection should belong to same user domain.

Following are the supported physical connection types and scenario for the import operation:

The supported physical connection types for the import operations are as follows:

- Physical connections between GMRE and non-GMRE nodes
- Physical connections between nodes in different EML domains
- Bidirectional OTS connections.
- Bidirectional OPS connections – inter compound PHN-OCS, PHN-ENE, OCS-ENE, PHN-PHN, OCS-OCS
- Cluster OPS connections
- Dangling OPS connections
- Physical connections template downloaded on one NFM-T server and uploaded to another NFM-T server

The result of the import operation of the physical connections is available under the Jobs page, Log History, and UAL.



Note: There is no specific parameter in the downloaded template for cluster and dangling OPS connections but they are the same as for normal OPS bidirectional connections.

Download physical connection CSV template

This feature allows you to download the existing Physical connections in a CSV template file which is further imported on the **Import Physical Connections and Nodes** window to create a new Physical Connection.

Download physical connection CSV template

Complete the following steps to download the Physical connection CSV template:

1

From the NFM-T GUI, navigate to:

ADMINISTER > Import physical network

Result: Import Physical Connections and Nodes window is displayed.

Figure 7-117 Import Physical Connections and Nodes window



2

In the **Import Physical Connections and Nodes** window, select the **Download Template** check box and click **Download Template Files**.



Result: The **Nes** and the **PhysicalConns** CSV template files are downloaded into your local system.

3

Browse and open the **PhysicalConns** CSV template file to add the parameters to create a CSV file, that is imported to create a new physical connection.

Figure 7-118 Physical connection template

```

IdClass,Tag,aPort,aNode_guiLabel,aNodeENE,allPathCost,clientSignalType,interfaceType,userLabel,WDMconnectionType,technologyDomain,WDMconnectionIwType,zPort,zNode
16,"CMD_WIZTYPE_createConn","AAA/ARHLG-1-4-LINE","AAA","false",20,"ClientSignalType_meaningful",",","AAA/ARHLG-1-14-LINE-BBB/AHPLG-1-7-LINE","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS042241/T24PS1-1-3-X1","TPS042241","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_042241-042242","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116001/T24PS1-1-3-X1","TPS116001","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116001-116002","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116003/T24PS1-1-3-X1","TPS116003","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116003-116004","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116005/T24PS1-1-3-X1","TPS116005","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116005-116006","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116007/T24PS1-1-3-X1","TPS116007","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116007-116008","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116009/T24PS1-1-3-X1","TPS116009","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116009-116010","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116011/T24PS1-1-3-X1","TPS116011","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116011-116012","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116013/T24PS1-1-3-X1","TPS116013","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116013-116014","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116015/T24PS1-1-3-X1","TPS116015","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116015-116016","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116017/T24PS1-1-3-X1","TPS116017","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116017-116018","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116019/T24PS1-1-3-X1","TPS116019","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116019-116020","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116021/T24PS1-1-3-X1","TPS116021","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116021-116022","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116023/T24PS1-1-3-X1","TPS116023","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116023-116024","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116025/T24PS1-1-3-X1","TPS116025","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116025-116026","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116027/T24PS1-1-3-X1","TPS116027","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116027-116028","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116029/T24PS1-1-3-X1","TPS116029","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116029-116030","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116031/T24PS1-1-3-X1","TPS116031","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116031-116032","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116033/T24PS1-1-3-X1","TPS116033","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116033-116034","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116035/T24PS1-1-3-X1","TPS116035","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116035-116036","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116037/T24PS1-1-3-X1","TPS116037","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116037-116038","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116039/T24PS1-1-3-X1","TPS116039","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116039-116040","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116041/T24PS1-1-3-X1","TPS116041","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116041-116042","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116043/T24PS1-1-3-X1","TPS116043","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116043-116044","WdmPortType_ops","
16,"CMD_WIZTYPE_createConn","TPS116045/T24PS1-1-3-X1","TPS116045","false",20,"ClientSignalType_eth100GbE",,UNI-Ethernet,"LINK1_116045-116046","WdmPortType_ops","

```

4

Use the downloaded CSV template file to create a new physical connection.

END OF STEPS

Create new physical connection from CSV template file

Use the downloaded CSV template, to modify or add the parameters for the new Physical Connection and import the CSV file on the **Import Physical Connections and Nodes** window.

i Note: Before importing the CSV template file, open the downloaded CSV template file in a notepad or wordpad application to verify and ensure that the file structure to be imported, is in correct format. This ensures that the parameter values to be imported in system are in executable format.

```
IdClass,PH_comments,PH_neGroupId,PH_neType,PH_subType,PH_operation,PH_address,PH_acd,PH_partnerAddress,PH_userName,PH_password,PH_secondaryIPAddress,PH_location,PH
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V2C","ftp","ps32-","01-Aragon","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","snmp","ps32-","01-HOMELANDER","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V2C","ftp","ps32-","02-Bilbo","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","snmp","ps33-","02-STARGATE","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V2C","snmp","ps33-","03-A-TRAIN","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","[REDACTED]","AMN-ASON","V2C","ftp","ps32-","03-Frodo","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V2C","ftp","ps32-","04-Gimli","13.0.4","nms_snmp","nms_snmp",""
3,"",102,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V4","ftp","ps32-","05-Gollum","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V2C","ftp","ps32-","06-Isildur","13.0.4","nms_snmp","nms_snmp",""
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMN-ASON","V2C","ftp","ps32-","07-Samwise","13.0.4","nms_snmp","nms_snmp",""
```

Complete the following steps to import the Physical Connection creation template:

1

From the NFM-T GUI, navigate to:

ADMINISTER > Import physical network

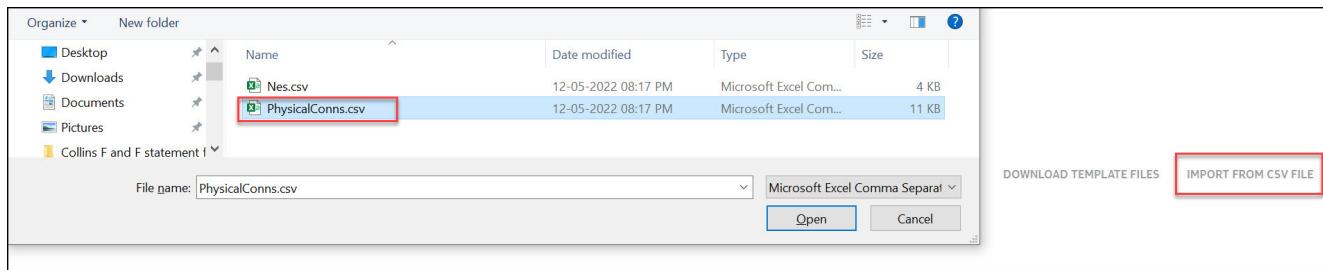
Result: Import Physical Connections and Nodes window is displayed.

Figure 7-119 Import Physical Connections and Nodes window



2

Click ↑ next to Select a file and select the **PhysicalConns** template to be imported and click **Import From CSV File**.



Result: xx.csv Import From CSV File is In-Progress, Check Jobs from Status message is displayed.

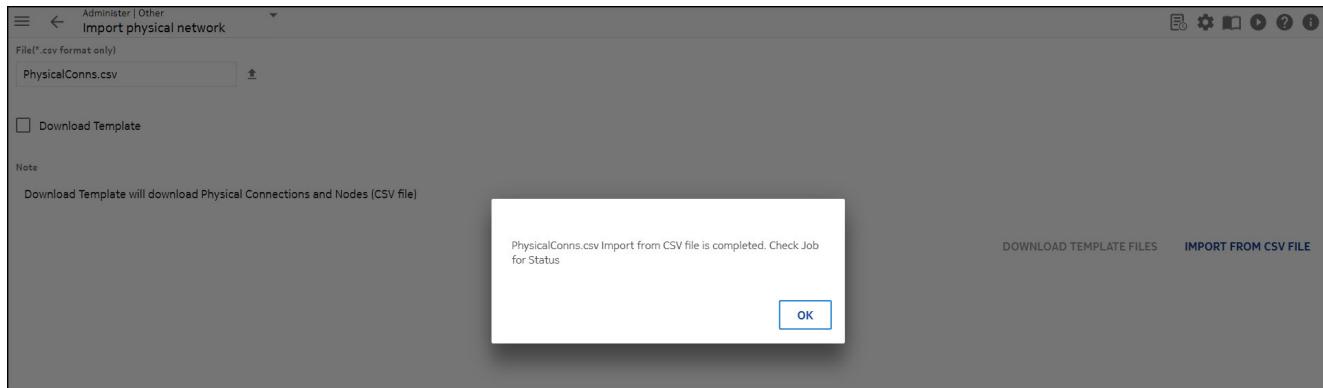


Figure 7-120 Jobs page

Job Name	Job Type	User Name	Latest Run Status	Create Time	Last Modification Ti...	Schedule	Next Run	⋮
SSAD_ENE2_OPS - Thu May 12	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:24 PM	5/12/2022 8:33:25 PM			⋮
SSAD_ENE1_OPS - Thu May 12	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:23 PM	5/12/2022 8:33:25 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:23 PM	5/12/2022 8:33:25 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:22 PM	5/12/2022 8:33:25 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:22 PM	5/12/2022 8:33:24 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:21 PM	5/12/2022 8:33:24 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:21 PM	5/12/2022 8:33:24 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:20 PM	5/12/2022 8:33:24 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:20 PM	5/12/2022 8:33:24 PM			⋮
ENE-test2_CP-NODE1-10.47.1	Physical Connection - Create	admin	Complete - Failure	5/12/2022 8:33:20 PM	5/12/2022 8:33:23 PM			⋮

3

After Physical connection is created, start the supervision.

4

From the NFM-T GUI, navigate to **ADMINISTER > User Activity Log > All Records** to check all records log for the physical connection created.

Figure 7-121 Add physical connection All Records log

Administrator User Activity Log All Records								
Start Time	End Time	Opera...	Action	Object	Stat...	App...	Client Host	⋮
10/5/2020 ...	10/5/2020 7:25:46 PM	alcatel	Create External Netw...	DemoEne3	Failed	OTN	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 7:22:17 PM	alcatel	Create External Netw...	DemoEne4	Success	OTN	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 7:22:16 PM	alcatel	Create External Netw...	DemoEne3	Success	OTN	10.10.10.100	⋮
<input checked="" type="checkbox"/> 10/5/2020 ...	10/5/2020 4:19:50 PM	admin	Add Node	User Label : DemoPHN	Success	EML	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 2:24:57 PM	admin	Delete Node	User Label : DemoPHN	Success	EML	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 2:13:13 PM	admin	Add Node	User Label : DemoPHN	Success	EML	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 12:22:44 PM	admin	Create External Netw...	DemoEne2	Success	OTN	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 12:22:44 PM	admin	Create External Netw...	DemoEne1	Success	OTN	10.10.10.100	⋮
10/5/2020 ...	10/5/2020 12:15:42 PM	admin	Add Node	User Label : DemoGe...	Success	EML	10.10.10.100	⋮

5

Click Log History  icon on the top right on the Physical Connections page, to view the log history.

END OF STEPS

7.47 Import CSV Template file to Create a Node(s)

Description

NFM-T supports CSV file import in the system to create a new Node.

- The downloaded CSV template file is a sample file for reference. Either use this file or the format and the parameters of the sample CSV template file to create a CSV file to import and create a new node.
- As part of this feature, Network Access Domain (NAD) and Functional Access Domain (FAD) validations are also performed by system while importing the template , the nodes involved in the physical connection should belong to same user domain.

From the NFM-T GUI, navigate follow the path **ADMINISTER > Import physical network**



Note: This feature is supported only for bi-directional OPS and OTS physical connections involving real NEs or external NEs.

The following types of NEs support import of CSV template to create a Node:

- 1830 PSS
- 1830 PSS-4
- 1830 ONE-Agg
- 1830 ONE-mROADM
- 1830 TPS
- External

CSV Template download to Import a Node(s)

This allows you to download the existing Nodes in CSV template file that is imported from the **Import Physical Connections and Nodes** window to create new Node.

Download Template in CSV format to create a Node(s)

Complete the following steps to download the Node creation template in CSV format:

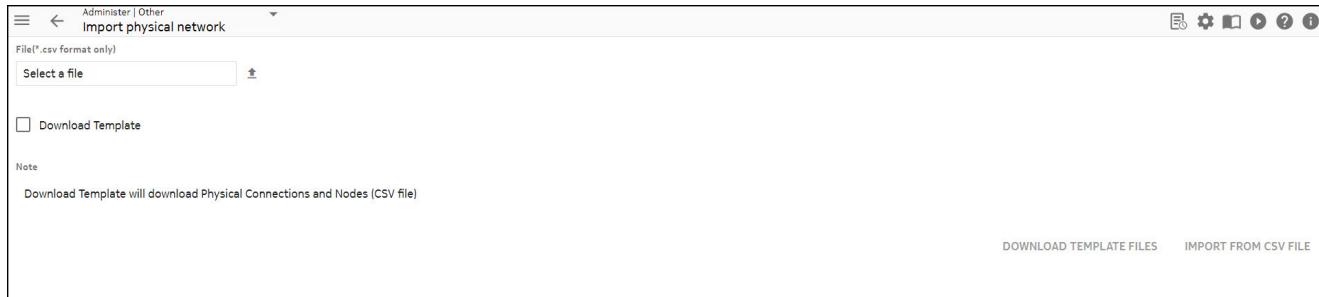
1

From the NFM-T GUI, navigate to:

ADMINISTER > Import physical network

Result: **Import Physical Connections and Nodes** window is displayed.

Figure 7-122 Import Physical Connections and Nodes window



2

In the **Import Physical Connections and Nodes** window, select the **Download Template Physical Connections and Nodes (CSV file)** check box and click **Download Template Files**.



Result: The **Nes** and the **PhysicalConns** CSV files are downloaded into your local system.

3

Browse and open the CSV file to view and modify the parameters to create a new Node.

Figure 7-123 NEs template

idClass,comments,neGroupId,neType,subType,operation,address,acd,partnerAddress,user_name,password,location,snmpVersion,usmUser,ssh2pubKey,TID,userLabel,version,sy
3,"",102,"1830PSS","EHN",add,"","unknown","","admin",<password>,102,"V2C","","","",pss32 .60,"PM-0060","11.1","SNMP","nms_snmp","nms_snmp","","","
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .60,"PM-0062","11.1","FTP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","unknown","","admin",<password>,102,"V2C","","","",pss32 .63,"PM-0063","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .63,"PM-0064","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","unknown","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0065","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0070","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0074","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0076","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0077","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","unknown","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0079","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","unknown","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0081","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0088","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",102,"1830PSS","EHN",add,"","PM","","admin",<password>,102,"V2C","","","",pss32 .65,"PM-0091","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",205,"1830PSS","EHN",add,"","PM","","admin",<password>,205,"V2C","","","",pss32 .65,"PM-0479","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",205,"1830PSS","EHN",add,"","PM","","admin",<password>,205,"V2C","","","",pss32 .65,"PM-0482","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",205,"1830PSS","EHN",add,"","PM","","admin",<password>,205,"V2C","","","",pss32 .65,"PM-0485","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",205,"1830PSS","EHN",add,"","PM","","admin",<password>,205,"V2C","","","",pss32 .65,"PM-0486","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",205,"1830PSS","EHN",add,"","PM","","admin",<password>,205,"V2C","","","",pss32 .65,"PM-0487","11.1","SNMP","nms_snmp","nms_snmp","","",""
3,"",205,"1830PSS","EHN",add,"","PM","","admin",<password>,205,"V2C","","","",pss32 .65,"PM-0488","11.1","SNMP","nms_snmp","nms_snmp","","",""

4

Use the downloaded CSV files to create a new node.



Note: Cluster associations are not supported while importing a node template.

END OF STEPS

Create a new node from the CSV template file

Use the downloaded CSV template to modify or add the parameters for the new Node(s) and import the template on the **Import Physical Connections and Nodes** window.



Note:

- Before importing the CSV template file, open the downloaded CSV template file in a notepad or wordpad application to verify and ensure that the file structure to be imported, is in correct format. This ensures that the parameter values to be imported in system are in executable format.

In the template file to be imported, perform the following mandatory actions for the NE types and attributes. Modification of other parameters is optional

Attribute / NE Types	Action
For <password> attribute	Modify <password> values with actual credentials in (") by opening the CSV template file in a notepad or wordpad
For 1830 PHN, 1830 TPS, 1830 ONE and External NE types	Add “PH_” prefix to the headers
For OCS NE types	Add “OCS_” prefix to the headers
For compound node(s)	Combine the data for OCS and PHN NEs details in a single row

- Add prefix for all the other attributes, except **IdClass**.

Figure 7-124 NEs template after modification

```

IdClass,PH_comments,PH_neGroupId,PH_neType,PH_subType,PH_operation,PH_address,PH_acd,PH_partnerAddress,PH_userName,PH_password,PH_secondaryIPAddress,PH_location
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","pss32","01-Aragon","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","snmp","pss32","01-HOMELANDER","13.0.4","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","pss32","02-Bilbo","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","snmp","pss32","02-STARLIGHT","13.0.4","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","snmp","pss32","03-A-TRAIN","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","ftp","pss32","03-Frodo","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","pss32","04-Gimli","13.0.4","nms_snmp","nms_snmp",
3,"",102,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V4","ftp","pss32","05-Gollum","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","pss32","06-Isildur","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","","07-Samwise","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","","201-Aragon","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","snmp","","201-HOMELANDER","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","","202-Bilbo","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","TAKEOVER-ASON","V2C","snmp","","202-STARLIGHT","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","","203-Frodo","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","ftp","","204-Gimli","13.0.4","nms_snmp","nms_snmp",
3,"",102,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V4","snmp","","205-Gollum","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","snmp","","206-Isildur","13.0.4","nms_snmp","nms_snmp",
3,"",101,"1830PSS","PHN",add,"","unknown","","admin","","AMX-ASON","V2C","snmp","","207-Samwise","13.0.4","nms_snmp","nms_snmp"

```

Complete the following steps to import the Node creation template:

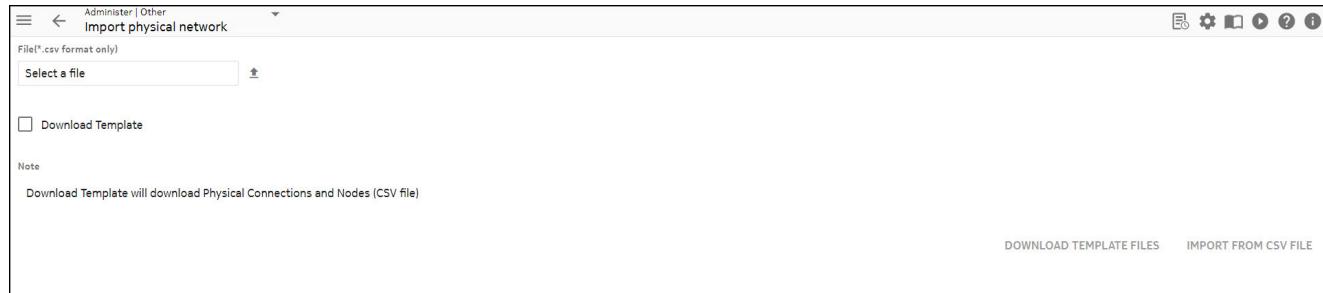
1

From the NFM-T GUI, navigate to:

ADMINISTER > Import physical network

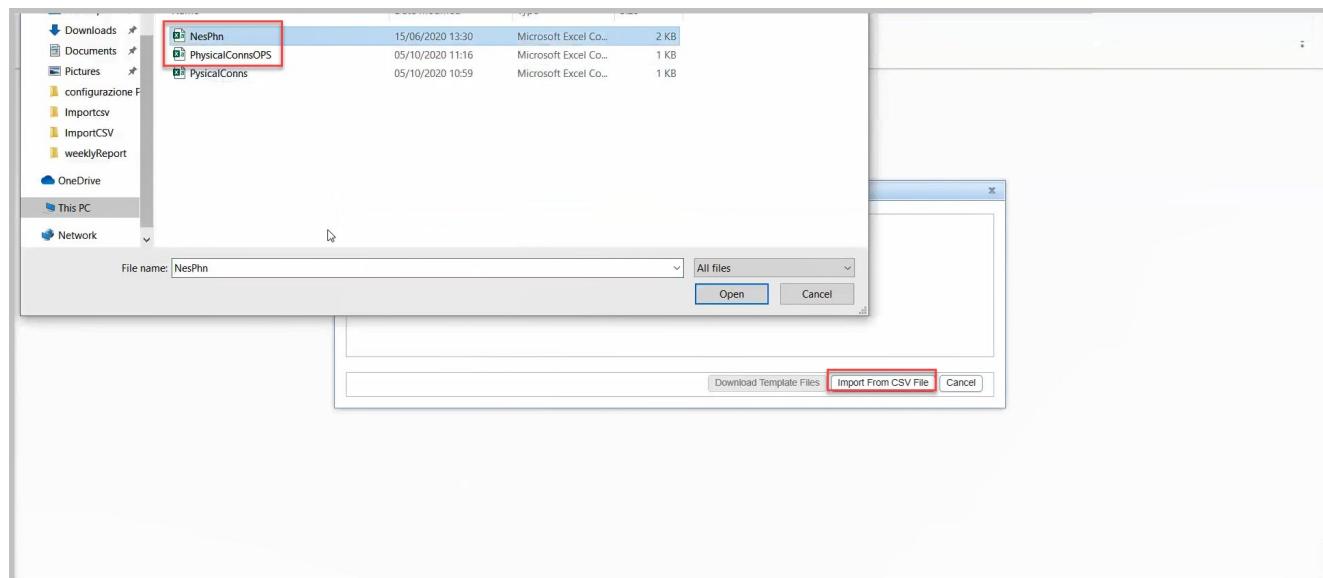
Result: Import Physical Connections and Nodes window is displayed.

Figure 7-125 Import Physical Connections and Nodes window



2

Click **Choose Files** and select the Nes template to be imported and click **Import From CSV File**.



Result: xx.csv Import From CSV File is In-Progress, Check Jobs from Status message is displayed.

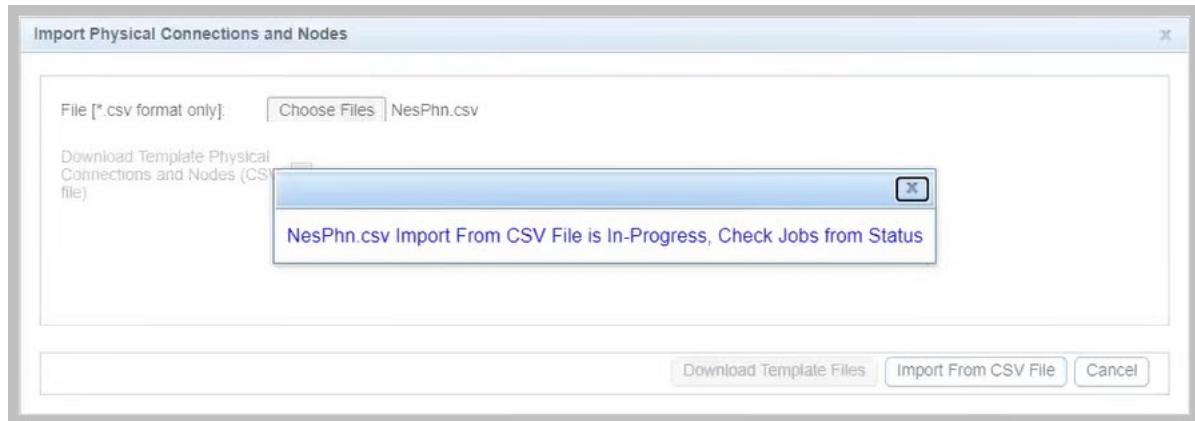


Figure 7-126 Jobs page

Job Name	Job Type	User Name	Latest Run Status	Create Time	Job State	⋮
NokDC1 - Sat Apr 02 04:09:16.965 UTC 2022	Node Management - Create	admin	Complete - Success	4/2/2022 9:39:16 AM	Completed	⋮
Troubleshoot_Job_10_42_324	DF OTDR Scan - Schedule	admin	In-Progress	2/21/2022 10:42:50 AM	In-Progres	⋮
NE-LO-SITE5 - Sat Apr 02 04:00:26.827 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:26 AM	Completed	⋮
NE-LO-SITE4 - Sat Apr 02 04:00:25.187 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:25 AM	Completed	⋮
NE-LO-SITE3 - Sat Apr 02 04:00:23.896 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:23 AM	Completed	⋮
NE-LO-SITE2 - Sat Apr 02 04:00:21.210 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:21 AM	Completed	⋮
NE-LO-SITE1 - Sat Apr 02 04:00:17.425 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:17 AM	Completed	⋮
NE-pss32-45.150.198 - Sat Apr 02 04:00:16.679 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:16 AM	Completed	⋮
NE-CompNode-7 - Sat Apr 02 04:00:15.803 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:15 AM	Completed	⋮
NE-CompNode-5 - Sat Apr 02 04:00:15.017 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:15 AM	Completed	⋮
NE-CompNode-4 - Sat Apr 02 04:00:11.315 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:11 AM	Completed	⋮
NE-CompNode-2 - Sat Apr 02 04:00:07.059 UTC 2022	Paths - Sync	Ason	Complete - Success	4/2/2022 9:30:07 AM	Completed	⋮

3

After a Node(s) is created, start the supervision.

4

From the NFM-T GUI, navigate to **ADMINISTER > User Activity Log > All Records** to check all records log for the created Node.

Figure 7-127 Add node All Records log

Start Time	End Time	Opera...	Action	Object	Stat...	App...	Client Host	⋮
05/10/2020 12:5...	05/10/2020 12:51:04	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 12:4...	05/10/2020 12:49:50	admin	Add Node	User Label : DemoPHN	Success	EML	[REDACTED]	⋮
05/10/2020 11:3...	05/10/2020 11:30:11	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:2...	05/10/2020 11:23:20	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:1...	05/10/2020 11:22:39	admin	Deimplement	testOPS	Failed	NPR	[REDACTED]	⋮
05/10/2020 11:1...	05/10/2020 11:16:17	admin	Session expired	Selected Session	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:1...	05/10/2020 11:10:33	admin	Implement	testOPS	Failed	NPR	[REDACTED]	⋮
05/10/2020 11:0...	05/10/2020 11:09:58	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:0...	05/10/2020 11:08:48	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:0...	05/10/2020 11:07:38	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:0...	05/10/2020 11:07:46	admin	Delete Physical Conn...	testOPS	Failed	NPR	[REDACTED]	⋮
05/10/2020 11:0...	05/10/2020 11:06:02	admin	Login History	admin	Success	PLATFO...	[REDACTED]	⋮
05/10/2020 11:0...	05/10/2020 11:05:30	admin	Delete Physical Conn...	testOTS	Success	NPR	[REDACTED]	⋮

5

Click Log History  icon on the top right on the Nodes page, to view the log history.

END OF STEPS

Infrastructure Connections and Services

7.48 Overview

Purpose

This section provides users with information required to understand how to setup connection and services on the NFM-T.

Contents

7.48 Overview	913
7.49 Control the deployment of a connection	915
7.50 Clone a connection	918
7.51 Delete a commissioned connection	919
7.52 Delete a commissioned infrastructure and clients	922
7.53 Manage alarms for a connection	924
7.54 Clear ASAP inconsistencies on a connection	936
7.55 Manage additional text attribute (Alias) - Infrastructure Connections and Services	947
7.56 Manage protection groups (MSP/SNCP) for a protected connection	952
7.57 Manage NIM for a connection	954
7.58 Manage protection for a connection in Managed Plane and Control Plane	960
7.59 Manage protection for a Mixed Plane service	968
7.60 Manage the service state of connection	975
7.61 Manage 3R for Managed Plane connections	978
7.62 Modify the parameters of a connection	981
7.63 Modify Route (Reroute) of a connection	987
7.64 Rename Connection and Customer Name	997
7.65 Manage the inventory view of Infrastructure Connections	1000
7.66 Manage Columns on Infrastructure Connections page	1004
7.67 Manage the inventory view of Services	1006
7.68 Manage data columns on Services page	1010
7.69 Set transmission parameters	1012

7.70 View Failure Analysis for an infrastructure connection or service	1013
7.71 View Jobs for an infrastructure connection or service	1016
7.72 View Infrastructure Connections or Services	1019
7.73 View Eline connection on Carrier Ethernet Links and Carrier Ethernet OAM pages in ESM	1022
7.74 View slots for an infrastructure connection	1024
7.75 1830 PSD Service Testing and BER Monitor	1025
7.76 View tabbed topics for an infrastructure connection or service	1032
7.77 View various route displays for an infrastructure connection or service	1036
7.78 View the Routing Display of a selected connection	1042
7.79 Infrastructure Connections columns	1054
7.80 Services columns	1059
7.81 Infrastructure Connections list further actions	1063
7.82 Services list further actions	1067
7.83 Resize ODUFlex Bandwidth	1071
7.84 Service Analytics Dashboard	1080

7.49 Control the deployment of a connection

Purpose

Use this task to control the deployment of a selected connection.

An *order* is the administrative data that is associated with your provisioning request, which the system creates to track your provisioning request through its life cycle, from its initial entry, to its implementation, to its possible service termination. Orders are assigned numbers, which are displayed on the data table for the infrastructure or service.

Through order and configuration state management, track the progress of the provisioning request (an order) and perform actions on a particular request.

You can manage the deployment state of the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- PM enabled points of a selected service or infrastructure connection
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

Depending on the existing deployment state of the connection and depending on the connection type, the configuration state that can be managed include, but is not limited, to the deployment states that are listed in the following table. Deployment states that are not specific to the connection that you select are either greyed-out or not displayed on the list.

Table 7-12 Deployment control for Infrastructure Connections and Services

Deployment control for Infrastructure Connections and Services	
Depending on the state of a particular provisioning request (order), NFM-T GUI Deployment Control includes the following states:	
Deployment control state	Meaning
Abort Order Processing	Stops the processing of a current order that is processing normally, which can cause a discrepancy between the network and the NFM-T OTN. The final Deploy State of the order varies, depending on when and where the abort occurred during processing.
Allocate	Specifies that the object is fully defined, but provisioning commands have not been sent.
Commission (In Service)	Specifies the allocated and implemented object should be put into service.
Complete Order	Performs all actions and validations that are needed to move an order to its final step.
Complete Step	Re-attempts to complete a failed current step of the order.

Table 7-12 Deployment control for Infrastructure Connections and Services (continued)

Deployment control for Infrastructure Connections and Services	
Depending on the state of a particular provisioning request (order), NFM-T GUI Deployment Control includes the following states:	
Deployment control state	Meaning
Cancel	Stops the order before it goes to the Commission (In Service) step; undoes all of the steps that have already been completed or partially completed; and, deletes the order from the system and from its appearance on the data table.
Delete Connection from NFM-T	Deletes the connection from the NFM-T database for Managed Plane and Control Plane connections. This option is not supported for MRN connections.
Delete Connection and Clients from NFM-T	Deletes the connections and its associated client connections from the database.
Deimplement	Specifies that an object that is currently in the Implement state should be deimplemented.
Implement	Specifies that the object has been implemented, but it is not yet available for end-customer use. This action enables additional testing to be performed.
Force delete	Accomplishes the same thing as Delete , except if any failure occurred in completing the commands, the order is still deleted.
Force Commission (In Service)	Accomplishes the same thing as Commission (In Service) , except if any failure occurred in completing the commands, the order is still commissioned.
Force Complete Order	The Force Complete Order request accomplishes the same action as Complete Order , except if any failure occurred in completing the commands, the order is still moved to its final step.
Force Complete Step	Accomplishes the same action as Complete Step , except if any failure occurred in completing the commands, the order step is still completed.
Force Deimplement	Accomplishes the same action as Deimplement , except if any failure occurred in completing the commands, the order step is still deimplemented.
Force Implement	Accomplishes the same action as Implement , except if any failure occurred in completing the commands, the order step is still implemented.
Move Backward One Command Set	Specifies to undo all actions in one command set of the implementation process.
Move Forward One Command Set	Specifies to complete all actions in the next set of the implementation process.

Task

Complete the following steps to control the deployment of a selected connection.

1

From the NFM-T GUI, follow one of the navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Depending on the type of connection and the existing Deploy State and Deploy Status of the connection, click on the **More**  icon of the selected connection, and follow the path **Deployment Control**, and select one of the options displayed. (See [Table 7-12, “Deployment control for Infrastructure Connections and Services” \(p. 915\).](#))

Result: Depending on your selection, the system changes the deployment state to reflect your selection and/or outputs a message.

END OF STEPS

7.50 Clone a connection

Purpose

Use this task to Clone a connection from a data table.

Select an already Deployed Service, involving the same A-Z Nodes of interest, the Deploy Form is automatically populated, not for the service end Ports. User can select the new Ports but can use all the other already populated parameters.

Task

Complete the following steps to delete a commissioned connection from a data table.

1

From the NFM-T GUI, follow the navigation paths:

OPERATE > Services

Result: The system displays a data table that lists all of the requested connections.

2

Select the service that you want to clone, click on the **More**  icon at the right end of the row and follow the path **Clone Connection**.

Result: The system displays the Clone Connection window.

3

Select the **From Port #1** and **To Port #1** values on the already From Node #1 and To Node #1 already populated.

4

Click the **CONTINUE** button to proceed in the creation.

5

Click **DEPLOY**.

Result: The system deploys the connection. Use the progress bar, toaster, or the Jobs list to view the completed action.

END OF STEPS

7.51 Delete a commissioned connection

Purpose

Use this task to delete a commissioned connection from a data table.

Delete a commissioned connection for the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- PM enabled points of a selected service or infrastructure connection
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

The connection to be deleted must be in the **Implementation State** of **Commissioned**. When you delete a connection, it can affect traffic.

To delete a connection from the data table in the **Implementation State** of **Defined**, **Allocated**, or **Partially Allocated**, use the **Deployment Control Cancel** option. Refer to the [7.49 “Control the deployment of a connection” \(p. 915\)](#) task for details.

The **Delete Connection** command does not support the following categories of connections: ASON logical link, ASON implicit server, Control Plane, Mixed Plane, ASON MRN terminated tunnel, ASON MRN unterminated tunnel, and ASON edge HO trail.

For the 1UD200, 260SCX2, 2UC400, and D5X500 circuit packs, the manual deletion of an ODU4 connection that has a server OTU4x2 infrastructure connection does not trigger the automatic deletion of the OTU4x2 infrastructure connection unless the ODU4 connection is the last ODU4 client connection for the OTU4x2. The manual deletion of the last ODU4 client connection of the OTU4x2 infrastructure connection does trigger the automatic deletion of the OTU4x2 connection, even if the ODU4 connection is not the connection that triggered the automatic creation of the OTU4x2.

i Note: From the NFM-T release 20.7 onwards, deleting a connection, the monitored PM points doesn't display the inactive TPs. However, to handle already deleted connections Inactive Monitored PM points, please contact the NFM-T Support team.

i Note: When user performs a delete operation with clients for D5X500 in OTU 4x2 mode, this will originate four cases as herewith reported:

- **Case 1:** OTU 4x2 Infra created without any Services on any ODU4.
In this case, *Delete connection and client* deletes both ODU4 and OTU 4x2.
- **Case 2:** OTU 4x2 Infra created with 100GBE Service on both ODU4.

In this case, Delete connection and client deletes only selected ODU4 while second ODU4 deletion delete second ODU4 and OTU 4x2.

- **CASE 3:** OTU 4x2 Infra created with 10GBE Service on any one ODU4.

In this case, *Delete connection and client* on ODU4 which has Service/DSR Riding on it deletes both ODU4 and OTU 4x2.

- **CASE 4:** Infra created with 10GBE Service on any one ODU4.

In this case, Delete connection and client on ODU4, which don't have Service/DSR Riding on it, deletes only selected ODU4 and user has to manually trigger delete for second ODU4 which will delete remaining ODU4 and OTU4x2.

The deletion of a DSR/LO-ODUk connection does not trigger an automatic deletion of the edge HO trail connection unless the DSR/LO-ODUk connection is the last DSR/LO-ODUk client connection for the edge HO trail. The deletion of the last DSR/LO-ODUk client connection of the edge HO trail connection triggers the automatic deletion of the edge HO trail connection even if the DSR/LO-ODUk connection is not the connection that triggered the automatic creation of the edge HO trail.

Task

Complete the following steps to delete a commissioned connection from a data table.

1

From the NFM-T GUI, follow the navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

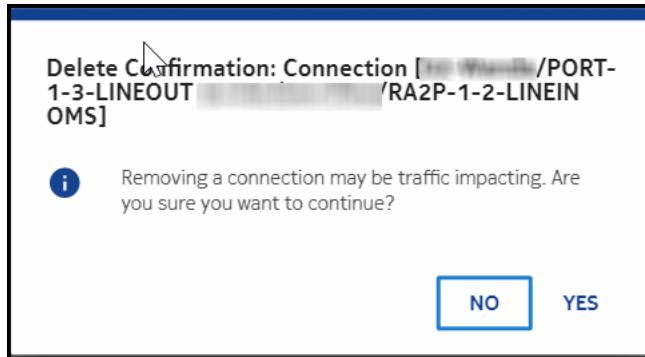
Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Select the commissioned connection that you want to delete, click on the **More**  icon at the right end of the row and follow the path **Delete Connection**.

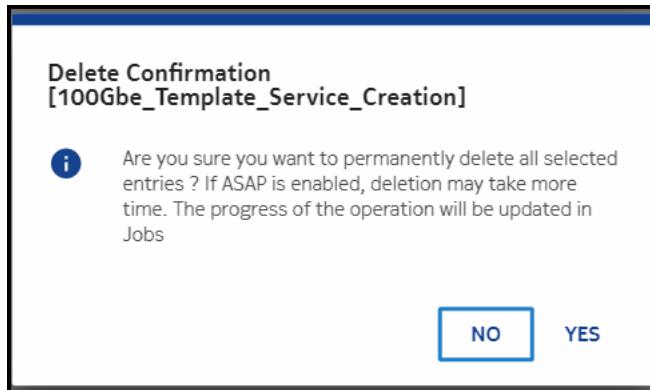
Result: The system outputs a confirmation message with the following warning:

Figure 7-128 Delete confirmation - Infrastructure Connections



Removing a connection may be traffic impacting. Are you sure you want to continue?

Figure 7-129 Delete confirmation - Services or Protected Connections



Are you sure you want to permanently delete all selected entries ? If ASAP is enabled, deletion may take more time. The progress of the operation will be updated in Jobs

3

Click OK.

Result: The system deletes the connection. Use the progress bar, toaster, and/or Jobs list to view the completed action.

END OF STEPS

7.52 Delete a commissioned infrastructure and clients

Purpose

Use this task to delete a commissioned infrastructure connection and its clients from the data table.

Delete a commissioned infrastructure connection with clients for the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Server connections of a selected infrastructure connection
- Server connections of a selected service
- PM enabled points of a selected service or infrastructure connection
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

The connection with clients to be deleted can be an infrastructure connection that has existing client connections. The selected connection must be in the **Commissioned** state.

i **Note:** The user must assign the client rate before deleting an Infrastructure if the ASON SNC has SBR as restoration and is in *Failed NRP* state, in configurations involving 130SLA1 cards on 100GB clear OT.

i **Note:** Delete Connection and Clients from NFM-T and Delete Connection and Clients operation is not supported for Logical link using D5X500/Q/L packs for OTU4x2, OTU4Half and OTU4HalfX5 layer rates if client(s) is(are) riding on any one of the channels.

i **Note:** Delete with clients on a Working Leg TERM (Real Server) connection doesn't delete the Protection Leg TERM Connection. The user has to manually select the option **Delete with Clients** while deleting the Protection Leg trail (LL/Infra) connection or vice-versa.

The **Delete Connection and Clients** command does not support the following categories of connections: ASON logical link, ASON implicit server, Control Plane, Mixed Plane, ASON MRN terminated tunnel, ASON MRN unterminated tunnel, and ASON edge HO trail.

The deletion of a DSR/LO-ODUk connection does not trigger an automatic deletion of the edge HO trail connection unless the DSR/LO-ODUk connection is the last DSR/LO-ODUk client connection for the edge HO trail. The deletion of the last DSR/LO-ODUk client connection of the edge HO trail connection triggers the automatic deletion of the edge HO trail connection even if the DSR/LO-ODUk connection is not the connection that triggered the automatic creation of the edge HO trail.

This task also provides the navigation paths in which you can delete the clients of an infrastructure connection from the **OPERATE > Service > Servers (Tab)** navigation path.

Task

Complete the following steps to delete an infrastructure connection and its clients from the data table.

1

From the NFM-T GUI, follow this navigation path:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

Result: The system displays a data table that lists all of the requested connections.

2

Select the commissioned connection that you want to delete, click on the **More**  icon at the right end of the row and follow the path **Delete Connection and Clients**.

Important!

The connection that you select from the **OPERATE > Services > Servers (Tab)** or the **OPERATE > Nodes > Impacted Connections (Tab)** navigation paths can be an **Infrastructure**, **Logical Link**, or **Physical Link**.

Result: The system outputs a warning and query that is similar to the following:

DB Deleting the selected connection(s) and all client connections.
This action will result in a discrepancy between the network and the application. Are you sure you want to remove the connection(s) from the database?

3

Click **OK**.

Result: The system deletes the connection and its respective client connections. Use the progress bar, toaster, or the Jobs list to view the completed action.

END OF STEPS

7.53 Manage alarms for a connection

When to use

Use the subtasks that are in this procedure to manage alarms for connections.

Related information

Correlate ASAPs to a connection

By default, once a connection is created, it is assigned the *default ASAP*.

You can correlate an ASAP to a connection from the data table of the connection or, for infrastructure connections and services, from the Routing Display.

If you need to select multiple connections, you can correlate the same profile to all of the selected connections. You can choose up to 150 connections from the connection data table to apply to the alarm profile. For Mixed Plane connections, the selection of multiple connections involves sending the selected alarm profile to ASON for the ASON segments on each of the selected connections (if any).

 **Note:** When two ODU4's (OTUX2) are involved, the user has to apply ASAP profiles on individual ODU4 connections.

The impact of correlating an ASAP is as follows:

- If the *default ASAP* is changed, existing alarms remain as *is* and new alarms are raised with new severities as in the *default ASAP*.
- If a user defined ASAP is correlated to a connection, any existing alarms are cleared and they are immediately re-raised with new severities.

If the correlation of an ASAP to a connection fails, an error message is displayed.

Enable Alarm Profile and Disable Alarm Reporting

The **Enable Alarm Profile** feature is based on the connection rate and the role of the port.

The **Disable Alarm Reporting** feature turns off all alarm reporting on the particular connection. It is available on connections that have the following attributes:

- The Alarm Profile is specified as Not Applicable.
- The connection rate must be one of the following: OTU1, OTU2, OTU3, ODU1, ODU2, ODU3, DSR, STMnRS, or OCnRS.

Both the **Enable Alarm Profile** and **Disable Alarm Reporting** features are offered on connections in the **Implemented** state and in which the Alarm Profile is **Not Set also**.

Note: For internal OTS physical connections that the NFM-T OTN creates or discovers, the management system sets the Alarm Severity Assignment Profile (ASAP) and the behavior of the internal OTS physical connection to be consistent with the behavior of the logical connection (infrastructure or service) in regard to the Manual Enable/Disable ASAP and the Routing Display port attributes of the service or infrastructure. For external OTS connections, you must enable or disable the ASAP manually on the physical connection.

Before you begin

You can manage ASAPs for the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- PM enabled points of a selected service or infrastructure connection
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

Task: Correlate a commissioned connection to an ASAP

Important! The connection to correlate to an ASAP must be in the **Commissioned** state.

Complete the following steps to correlate a connection to an ASAP.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

OPERATE > Protected Connections

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Do one of the following:

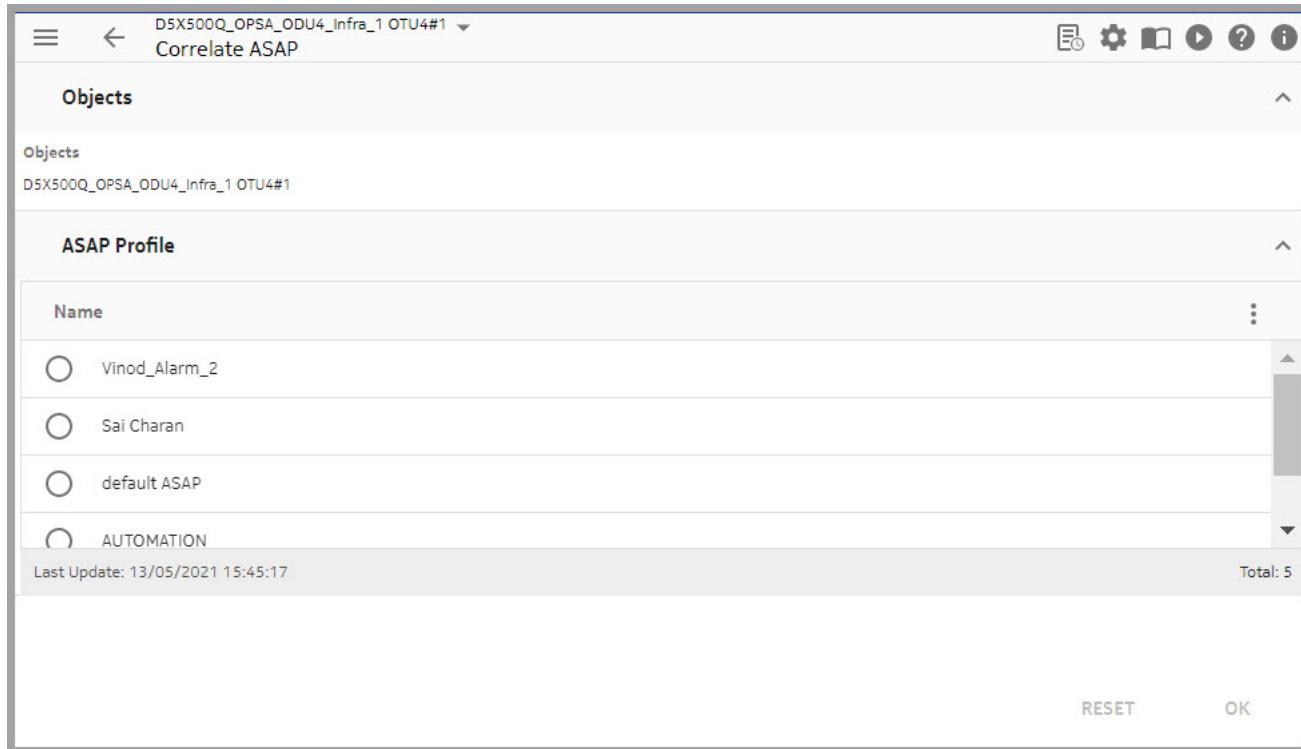
- If you want to correlate a **Commissioned** connection to a network alarm profile from a displayed data table, go to [Step 3](#).
- If you want to correlate a **Commissioned** connection to a network alarm profile from the Routing Display, go to [Step 4](#)

3

From a displayed data table, select the connection for which you want to correlate to an alarm profile, click on the **More**  icon, and follow this navigation path: **Correlate ASAP**.

Result: The system displays the Correlate ASAP window. Go to [Step 6](#).

Figure 7-130 Connections – Correlate ASAP window



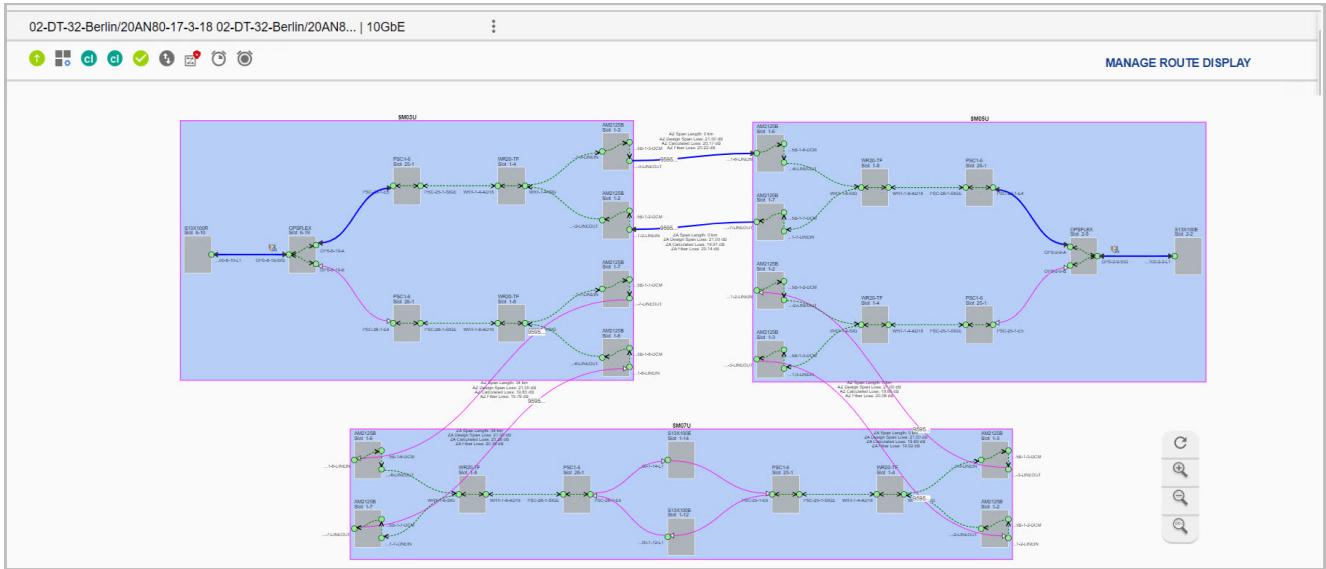
4

From the connection list, select the connection for which you want to correlate to an alarm profile and click on the **More**  icon and then **Routing Display**.

Result: The system opens a new browser tab and the route of the connection is displayed on the Routing Display

Go to the next step.

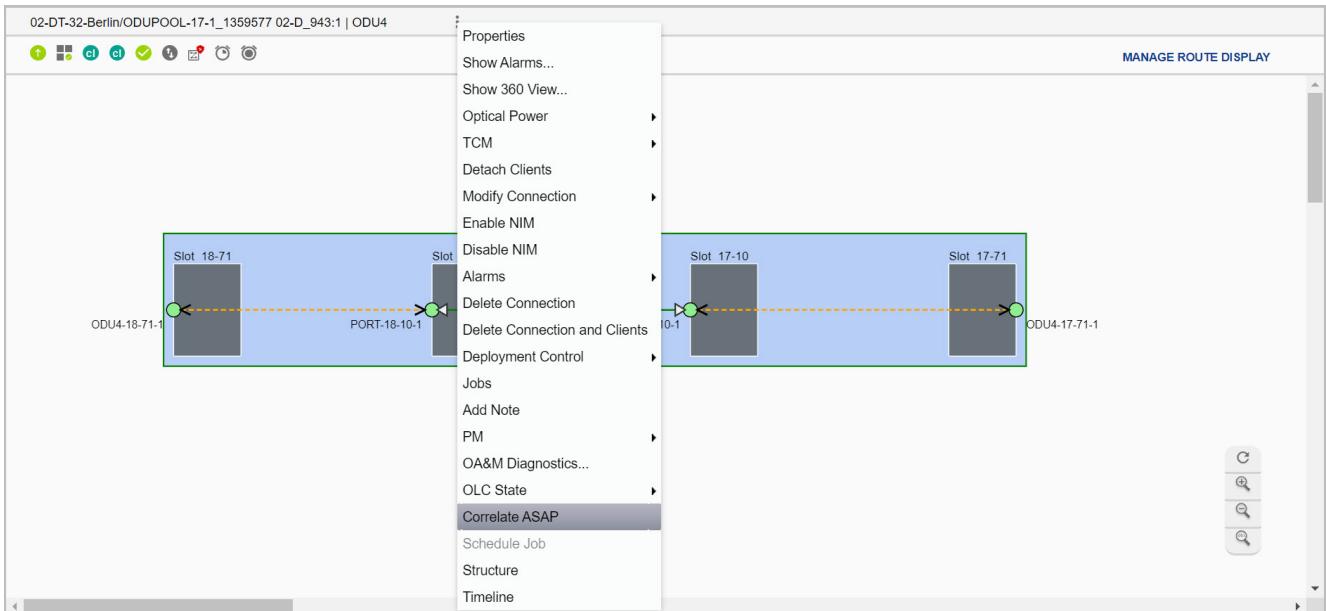
Figure 7-131 Connections – A connection on the Routing Display



5

Right click on the icon for the connection and select **Correlate ASAP**.

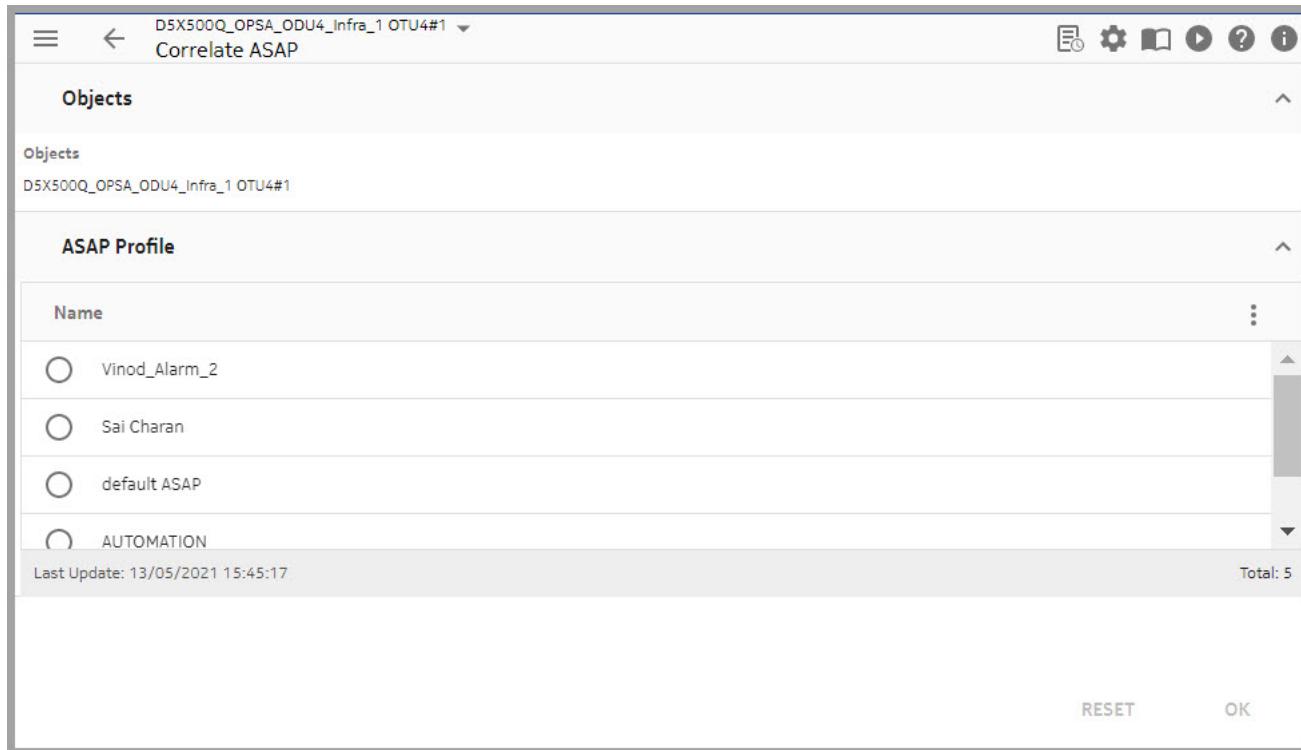
Figure 7-132 Connections – Right Click for Correlate ASAP on the Routing Display



Result: The system displays the Correlate ASAP window. Go to the next step.

i Note: When two ODU4s (OTUX2) are involved, user has to apply ASAP profiles on individual ODU4 connections.

Figure 7-133 Connections – Correlate ASAP window

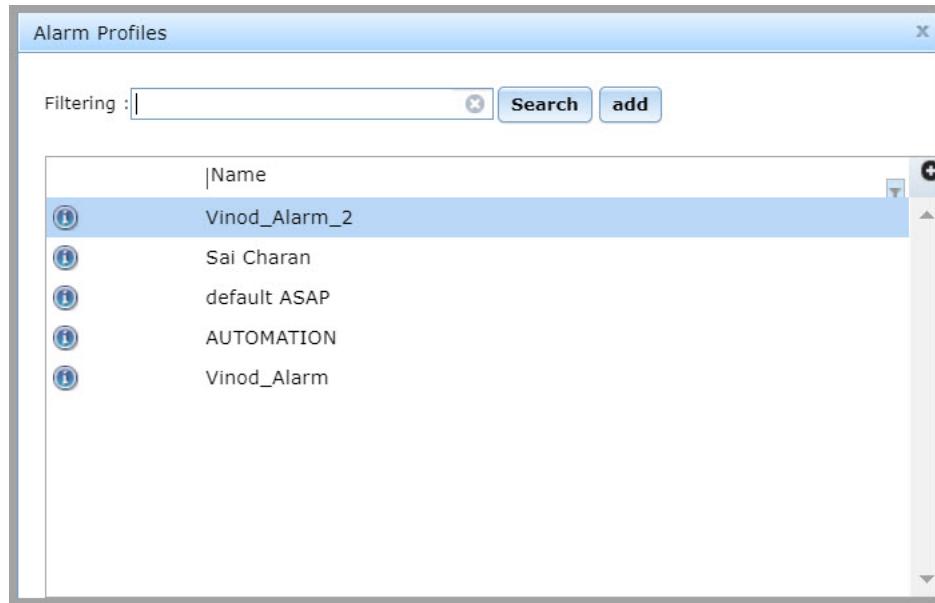


6

In the ASAP Profile pane of the window, select the magnifying glass icon.

Result: The system displays a list of ASAPs.

Figure 7-134 Connections – ASAP list

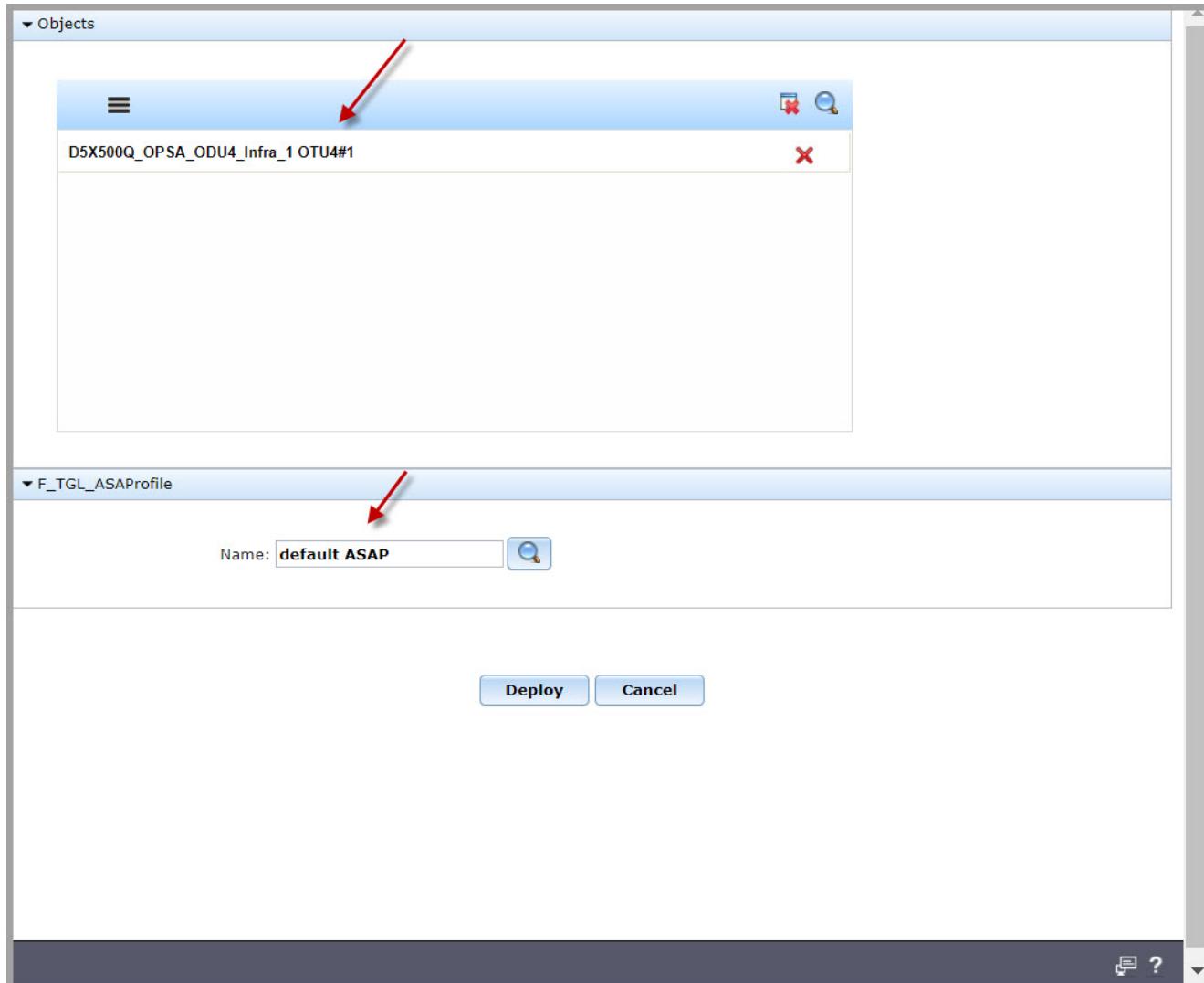


7

Select an ASAP and click **Add**.

Result: The system adds the selected ASAP.

Figure 7-135 Connections – ASAP assigned to the connection



8

Click the **Deploy** button.

Result: The system outputs a success message on the bottom left of the window that is similar to the following:

```
<time stamp>|Update ASAP Connection [<connection ID>]| ✓ Success
```

If the correlation of an ASAP to a connection fails, an error message is displayed.

END OF STEPS

Task: Disable Alarm Reporting

Important! The **Disable Alarm Reporting** feature turns off all alarm reporting on the particular connection. It is available on connections in which Alarm Profile is specified as **Not Applicable** and connections with rates of OTU1, OTU2, OTU3, ODU1, ODU2, ODU3, DSR, STMnRS, or OCnRS. The connection must be in the **Implemented** state. The **Disable Alarm Reporting** feature can take several minutes to implement.

Complete the following steps to disable alarm reporting on a selected connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

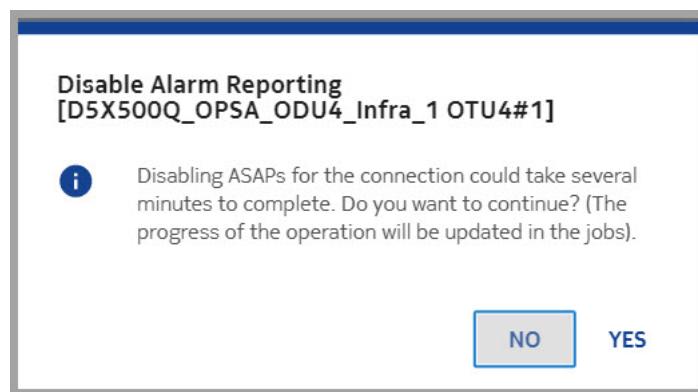
Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

2

Click on the connection for which you want to disable alarm reporting, click on the **More** icon on the right of the selected row, and follow this path: **Alarms > Disable Alarm Reporting**.

Result: The system displays the following query window:

Figure 7-136 Connections – Disable Alarm Reporting [connection] query window



3

To continue to disable the ASAP on the selected connection, click **Yes**.

Result: The system displays a message similar to the following at the bottom of the window:

Figure 7-137 Connections – Disable alarm reporting success message



4

Once the status changes, refresh the page.

Result: The ASAP is disabled for the selected connection.

END OF STEPS

Task: Enable Alarm Profile

Important! The **Enable Alarm Profile** feature is based on the connection rate and the role of the port. The connection must be in the **Implemented** state. The **Enable Alarm Profile** feature can take several minutes to implement.

Complete the following steps to enable the alarm profile on a selected connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

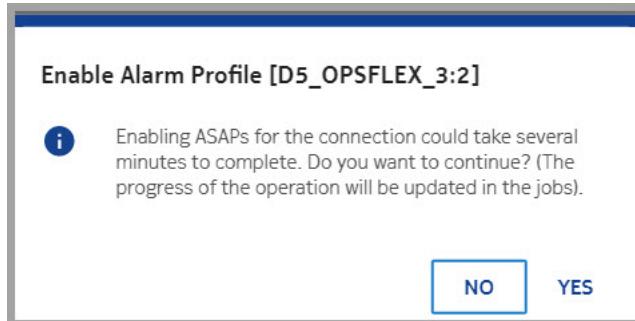
Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

2

Click on the **Implemented** connection to enable the alarm profile, mouse over the icons on the right of the row, click the **More**  icon, and follow this path **Alarms > Enable Alarm Profile**.

Result: The system displays the following query window:

Figure 7-138 Connections – Enable Alarm Profile [connection] query window

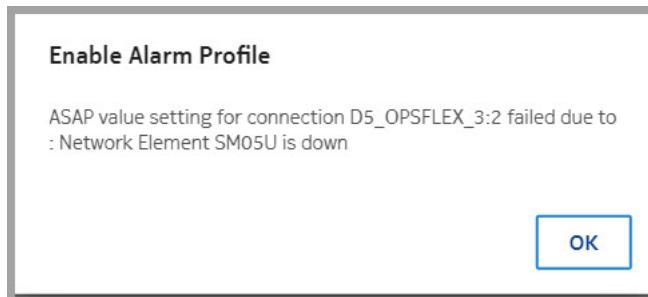


3

To continue to enable the ASAP on the selected connection, click **Yes**.

Result: The system displays a message similar to the following at the bottom of the window:

Figure 7-139 Connections – Enable Alarm reporting success message



4

Once the status changes, refresh the page.

Result: The ASAP is enabled for the selected connection.

END OF STEPS

Task: Set Default ASAP

This task allows to restore the alarm severities to NE/Node defaults through ASAP.

The action is enabled only if the ASAP has been previously enabled on the infrastructure or service.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

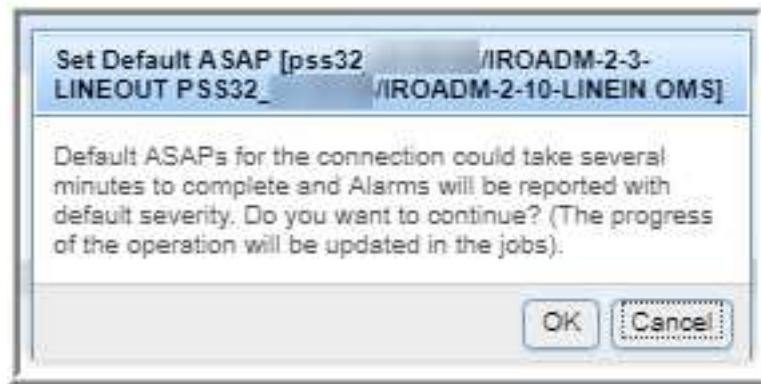
Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

2

Click on the connection for which you want to restore the alarm severities to NE/Node default, mouse over the icons on the right of the row, click the **More**  icon, and follow this path **Alarms > Set Default ASAP**.

Result: The system displays the following query window:

Figure 7-140 Connections – Set Default ASAP [connection] Query Window

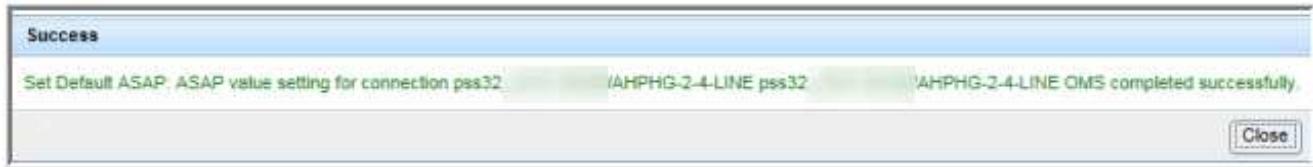


3

To continue to set the default ASAP on the selected connection, click **OK**.

Result: The system displays a message similar to the following on the window:

Figure 7-141 Connections – Set Default ASAP success message



4

Once the status changes, refresh the page.

Result: The ASAP is restored to the alarm severities to NE/Node default for the selected connection.

END OF STEPS

7.54 Clear ASAP inconsistencies on a connection

Overview

There are three approaches to clear a Connection marked as inconsistent in **ASAP Mismatches** tab:

1. By resetting the override severity value of an alarm to the previous severity (for example: severity assigned during **Enable ASAP** operation) value on NE and the user should perform ASAP synchronization on the NE on which severity is changed.
2. By performing **Disable ASAP** operation on the connection marked as ASAP Inconsistent.
3. By performing **Set To Default** operation on the connection marked as ASAP Inconsistent.



Note: ASAP synchronization on the NE, has to be performed only in the Approach 1, to clear the ASAP inconsistencies. In the other two approaches, ASAP inconsistencies are cleared automatically.

Task: Clearing the ASAP inconsistency by resetting the ASAP override severity value to the previous severity

Complete the following steps to clear the ASAP inconsistency by resetting the ASAP override severity value to the previous severity.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

2

Click on the **Implemented** connection to enable the alarm profile, mouse over the icons on the right of the row, click the **More :** icon, and follow this path **Alarms > Enable Alarm Profile**.

Result: The system displays a message that Enabling ASAPs for the connection could take several minutes to complete. Do you want to continue?

3

To continue to enable the ASAP on the selected connection, click **Yes**.

Result: The system displays a message **Enable ASAP xxx Success**.

4

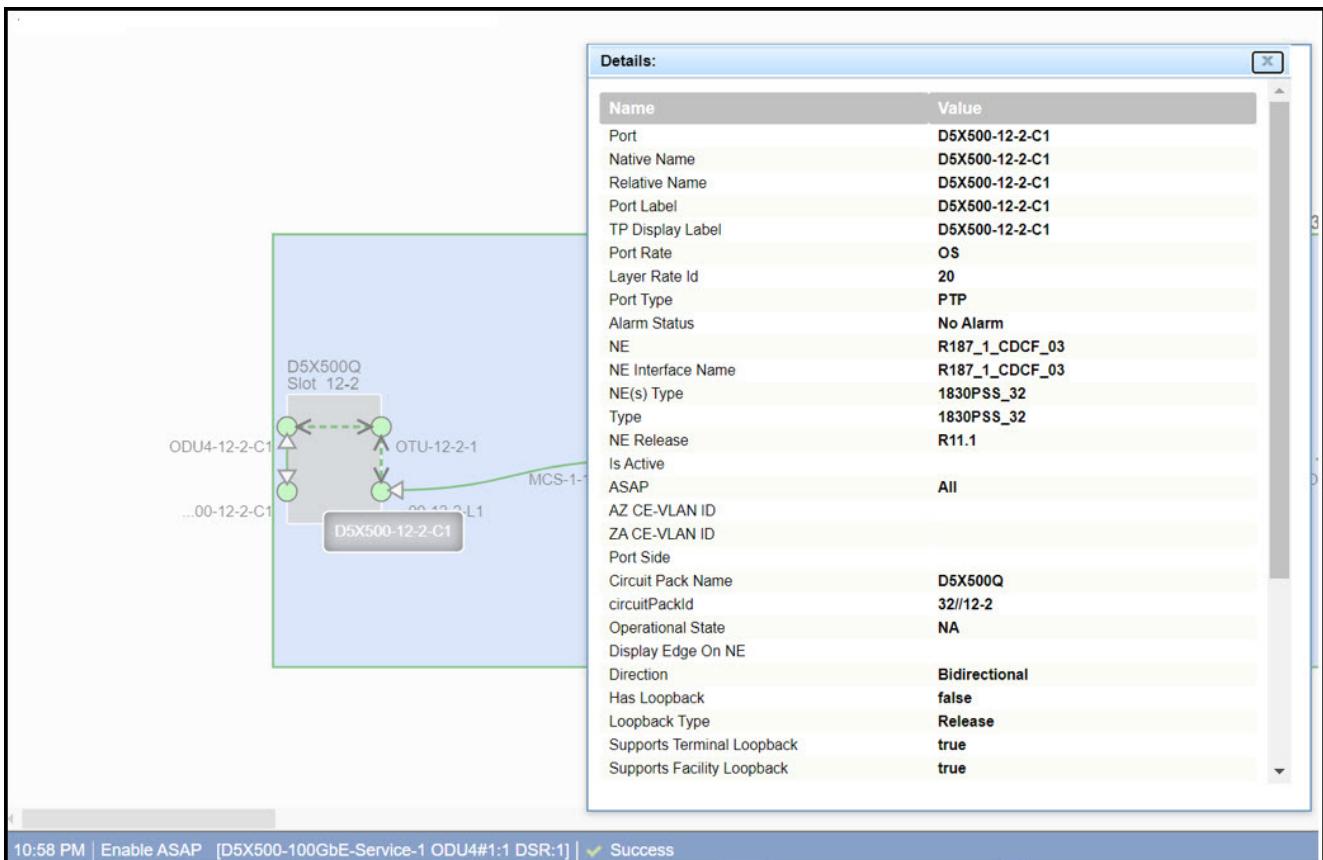
Once the status changes, refresh the page.

Result: The ASAP is enabled for the selected connection.

5

Navigate to **More**  icon, and follow the path **Routing Display** to check the enabled ASAP.

Figure 7-142 Enable ASAP

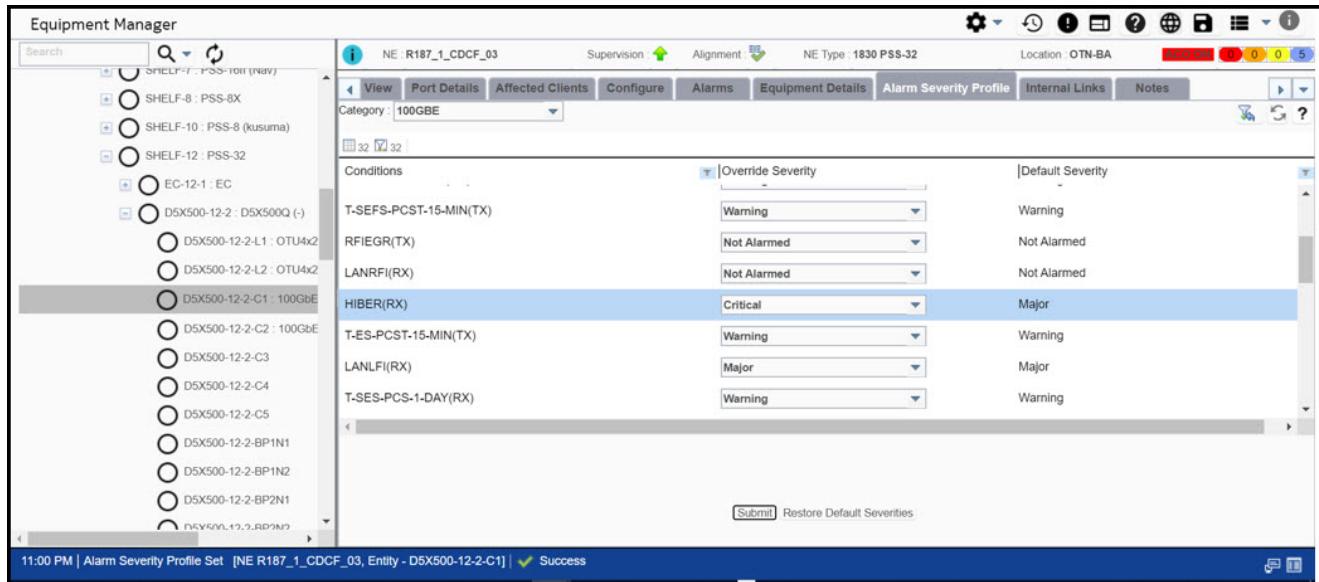


Result: The ASAP is enabled for the connection and the status bar displays **Enable ASAP: xxx Success** and in the Routing Display, the ASAP details is displayed as **All**.

6

Navigate to **OPERATE > Equipment Manager**, select the card and navigate to **Alarm Severity Profile** tab, then change the ASAP override severity from **Major** to **Critical**. Select from the drop-down and click **Submit**.

Figure 7-143 Change Override Severity



Result: The ASAP severity is changed to the new value.

7

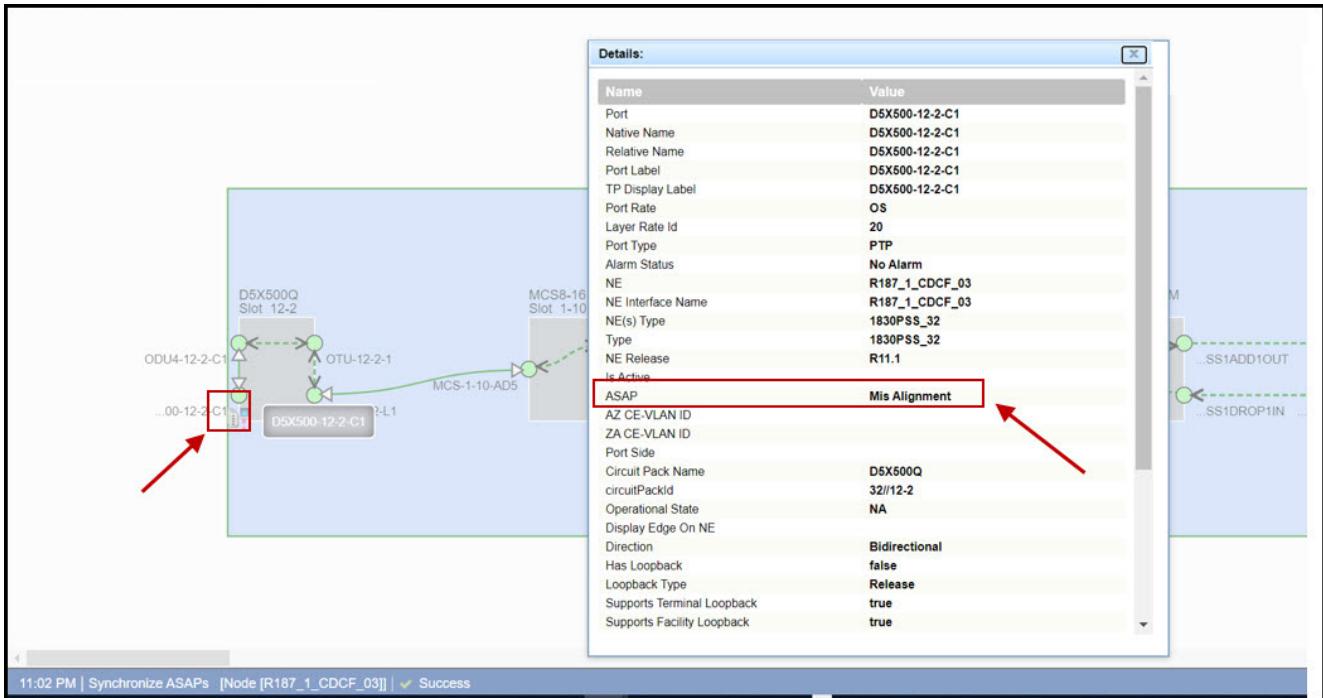
Navigate to **OPERATE > Nodes**, and click the **More** icon, and follow this path, **Synchronization > ASAP** to perform the ASAP synchronization.

Result: The Nodes are synchronized.

8

Click the **More** icon, and follow this path, **Routing Display** to validate the ASAP inconsistency in End-End Routing Display.

Figure 7-144 Validate ASAP inconsistency in Routing Display



Result: The ASAP inconsistency is reported in the Routing Display and the ASAP details is displayed as **Mis Alignment**.

9

Navigate to **OPERATE > Network Inconsistencies**, select the **ASAP MISMATCHES** tab to validate the ASAP inconsistency.

Result: The port and the connection on which the ASAP override severity was performed is displayed.

Figure 7-145 ASAP mismatches tab

SNC MISMATCHES	PARAMETER MISMATCHES	DOWNLOAD DISABLED MISMATCHES	ASAP MISMATCHES	UNCORRELATED CROSS CO...
<input checked="" type="checkbox"/> Connection Name	Type	Service Rate	Protection	Mismatch Detect Dat
<input checked="" type="checkbox"/> D5X500-100GbE-Service-1 ODU4#1:1 DSR:1	Service	100GbE	Unprotected	8/10/2020 11:02:00

10

Navigate to **OPERATE > Equipment Manager**, select the card and navigate to **Alarm Severity Profile** tab, then reverse the ASAP override severity changes from **Critical** to **Major**. Select from the drop-down and click **Submit**.

Figure 7-146 Reverse the ASAP severity to the previous severity

Condition	Override Severity	Default Severity
T-SEFS-PCST-15-MIN(TX)	Warning	Warning
RFIEGR(TX)	Not Alarmed	Not Alarmed
LANRFI(RX)	Not Alarmed	Not Alarmed
HIBER(RX)	Major	Major
T-ES-PCST-15-MIN(TX)	Warning	Warning
LANLF(RX)	Major	Major
T-SES-PCS-1-DAY(RX)	Warning	Warning
T-SES-PCS-1-DAY(TX)	Warning	Warning

11

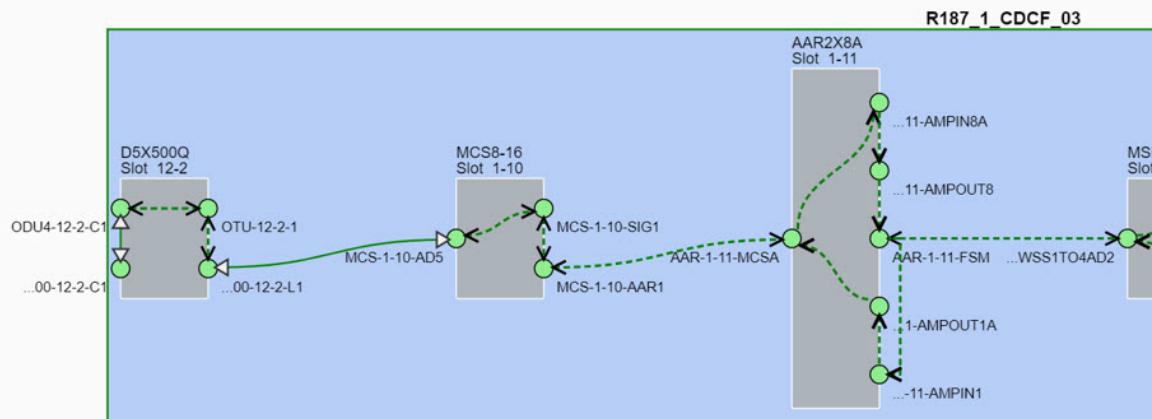
Navigate to **OPERATE > Nodes**, and click the **More** icon, and follow this path, **Synchronization > ASAP** to perform the ASAP synchronization.

Result: The Nodes are synchronized.

12

Click the **More** icon, and follow this path, **Routing Display** to validate the ASAP inconsistency in End-End Routing Display.

Figure 7-147 Validate ASAP inconsistency in Routing Display



Result: The ASAP inconsistency reported in the Routing Display is cleared.

13

Navigate to **OPERATE > Network Inconsistencies**, select the **ASAP MISMATCHES** tab to validate the ASAP inconsistency.

Result: No connection is displayed which indicates the ASAP inconsistency is cleared.

Figure 7-148 ASAP mismatches tab

END OF STEPS

Task: Clearing the ASAP inconsistency by disabling the ASAP

Complete the following steps to clear the ASAP inconsistency by disabling the ASAP:

1

Follow the steps from [Step 1](#) to [Step 9](#) in “[Task: Clearing the ASAP inconsistency by resetting the ASAP override severity value to the previous severity](#)” (p. 936) and then continue with [Step 2](#).

2

Click on the connection for which you want to disable alarm reporting, click on the **More** icon on the right of the selected row, and follow this path: **Alarms > Disable Alarm Reporting**.

Result: The system displays the message **Disabling ASAPs for the connection could take several minutes to complete. Do you want to continue?**

3

To continue to disable the ASAP on the selected connection, click **Yes**.

Result: The system displays a message **Disable Alarm Reporting: ASAP value setting for connection xxx completed successfully.**

Figure 7-149 Disable ASAP



4

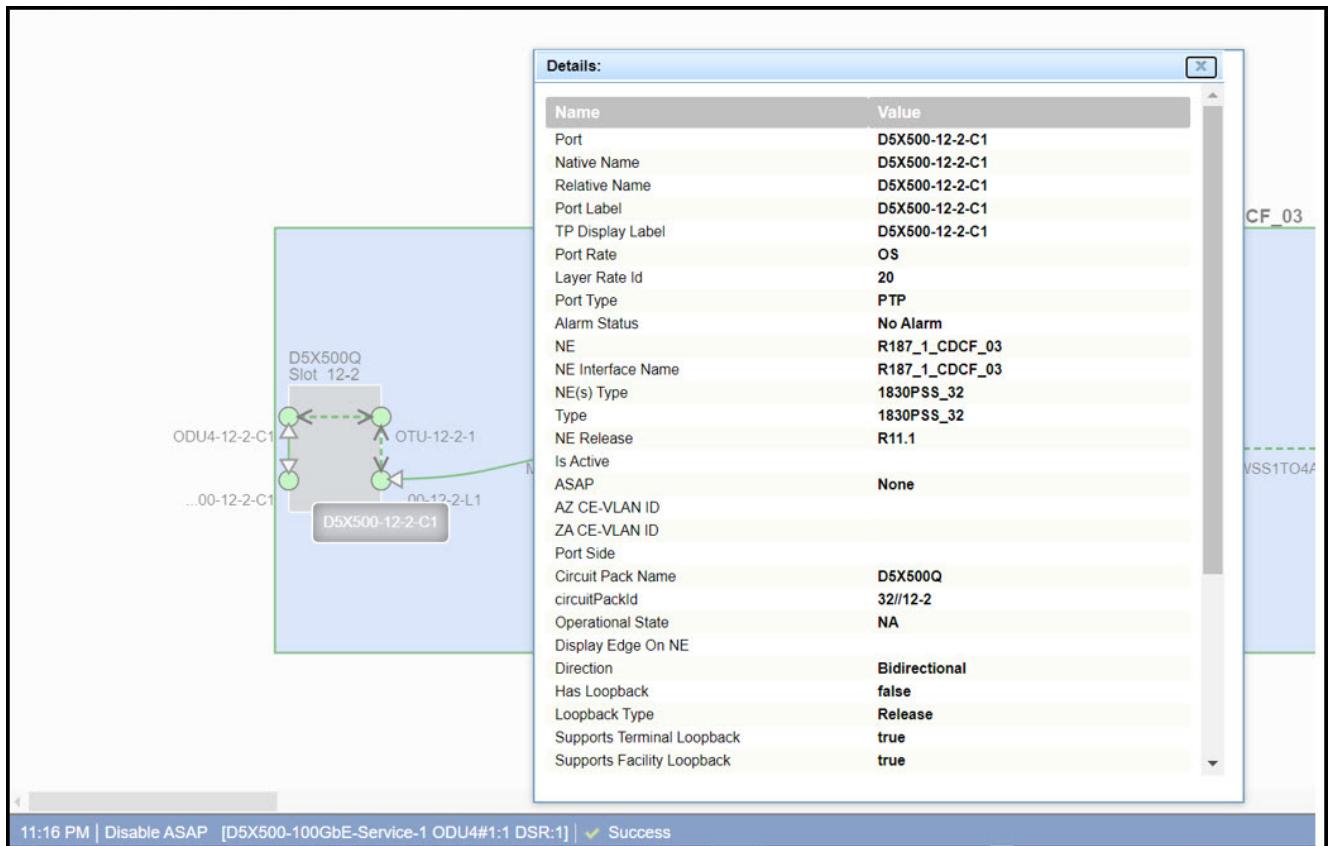
Once the status changes, refresh the page.

Result: The ASAP is disabled for the selected connection.

5

Click the **More** icon, and follow this path, **Routing Display** to validate the ASAP inconsistency in End-End Routing Display.

Figure 7-150 Validate ASAP inconsistency in Routing Display



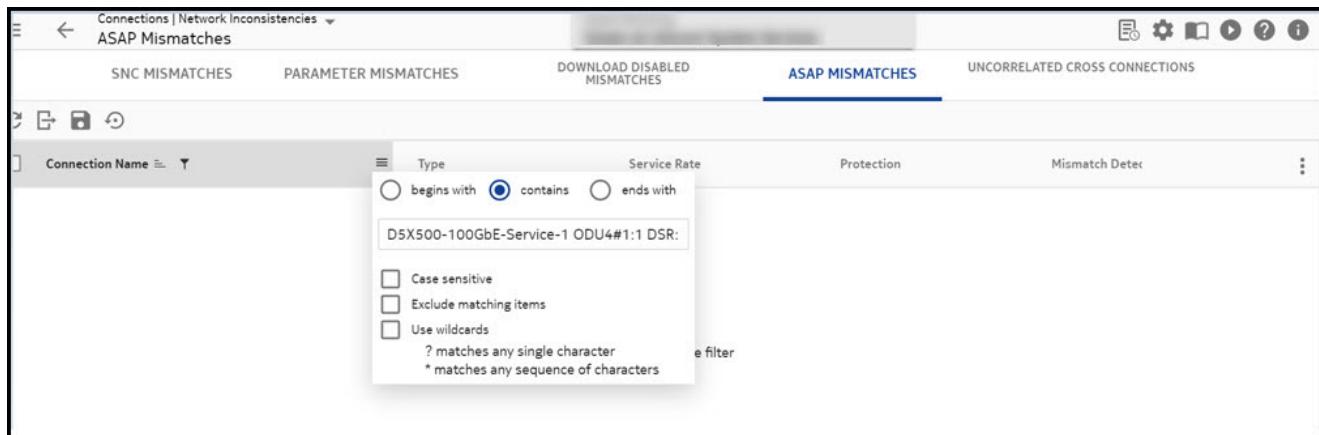
Result: The ASAP inconsistency reported in the Routing Display is cleared and the ASAP details is displayed as **None**.

6

Navigate to **OPERATE > Network Inconsistencies**, select the **ASAP MISMATCHES** tab to validate the ASAP inconsistency.

Result: No connection is displayed which indicates the ASAP inconsistency is cleared.

Figure 7-151 ASAP mismatches tab



END OF STEPS

Task: Clearing the ASAP inconsistency by setting the ASAP to default

Complete the following steps to clear the ASAP inconsistency by setting the ASAP to default value.

1

Follow the steps from [Step 1](#) to [Step 9](#) in “[Task: Clearing the ASAP inconsistency by resetting the ASAP override severity value to the previous severity](#)” (p. 936) and then continue with [Step 2](#).

2

Click on the connection for which you want to restore the alarm severities to NE/Node default, click the **More**  icon, and follow this path **Alarms > Set Default ASAP**.

Result: The system displays the message Default ASAPs for the connection could take several minutes to complete and Alarms will be reported with default severity. Do you want to continue? (The progress of the operation will be updated in the jobs)

3

To continue to set the default ASAP on the selected connection, click **OK**.

Result: The system displays a message Set Default ASAP: ASAP value setting for connection xxxx completed successfully.

Figure 7-152 Connections – Set Default ASAP success message



4

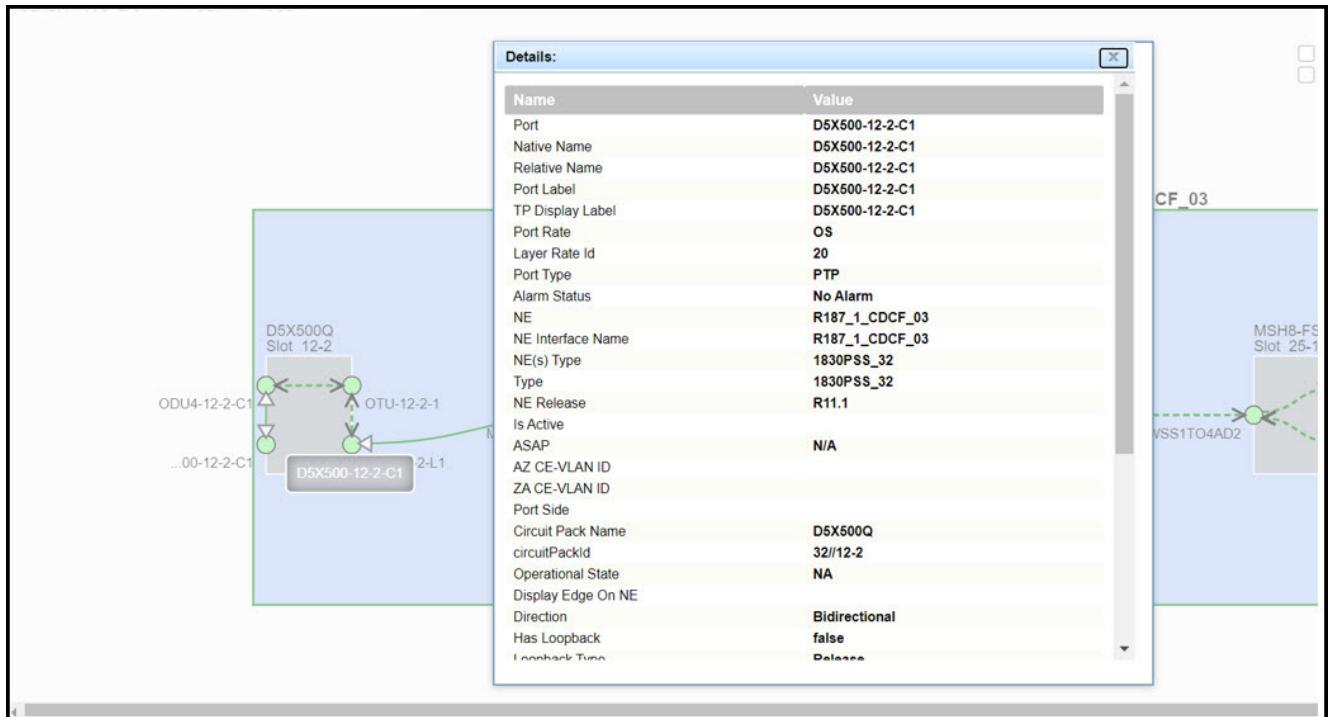
Once the status changes, refresh the page.

Result: The ASAP is restored to the alarm severities to NE/Node default for the selected connection.

5

Click the **More**  icon, and follow this path, **Routing Display** to validate the ASAP inconsistency in End-End Routing Display.

Figure 7-153 Validate ASAP inconsistency in Routing Display



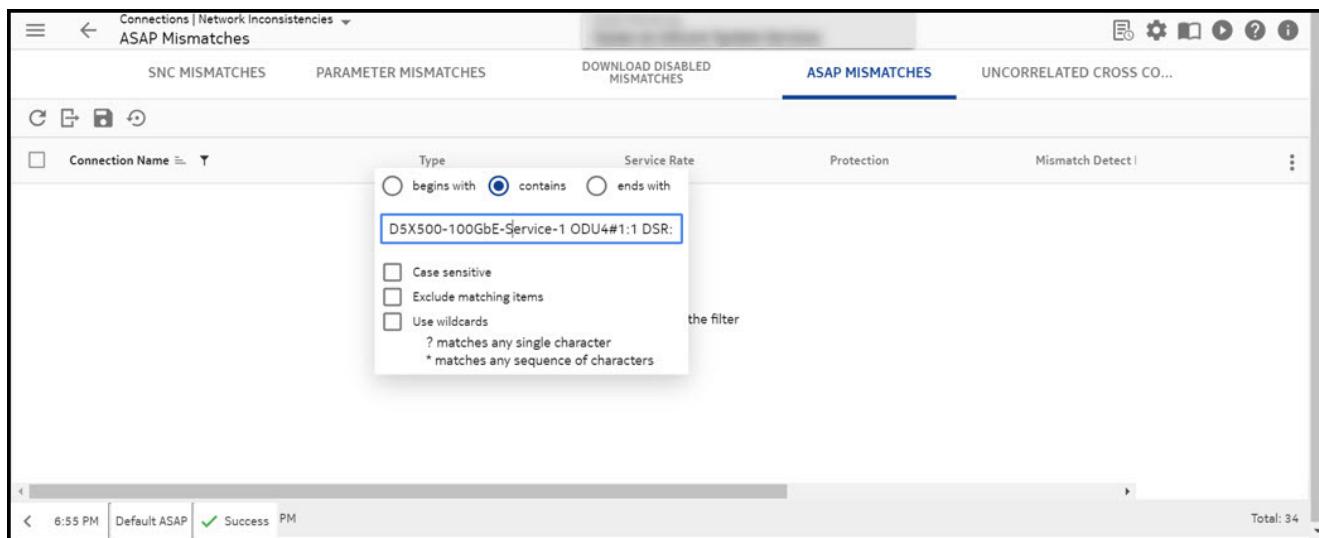
Result: The ASAP inconsistency reported in the Routing Display is cleared and the ASAP details is displayed as **N/A**.

6

Navigate to **OPERATE > Network Inconsistencies**, select the **ASAP MISMATCHES** tab to validate the ASAP inconsistency.

Result: No connection is displayed which indicates the ASAP Inconsistency is cleared.

Figure 7-154 ASAP mismatches tab



END OF STEPS

7.55 Manage additional text attribute (Alias) - Infrastructure Connections and Services

Task: Enable Alias 2 attribute

By default, the additional text attribute **Alias 2** is hidden in the Infrastructure Connections and Services window.

Complete the following steps to enable and view the **Alias 2** attribute in the **Infrastructure Connections and Services** window.

1

From the NFM-T GUI, follow one of the following navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: The corresponding **Infrastructure Connections** or **Services** data table is displayed.

2

Click the **More**  icon at the right end of the table header, click **Manage Columns** and select **Alias 2**.

Figure 7-155 Manage Columns - Infrastructure Connections

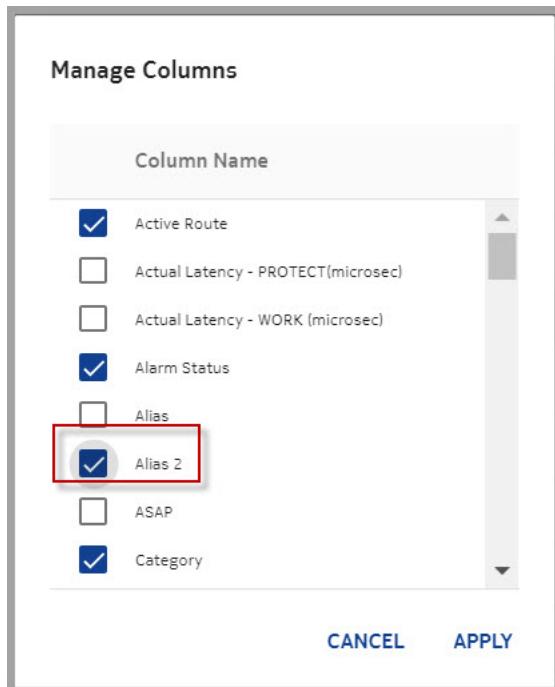


Figure 7-156 Manage Columns - Services

3

Click **APPLY**.

Result: The **Alias 2** is added to the list of column names.

END OF STEPS

Add Connection Alias 2 attribute

1

From the NFM-T GUI, navigate to **DEPLOY** and click **New Service/Infrastructure Connection**.

Result: The New Service/Infrastructure Connection page is displayed with templates for Infrastructure, Service, and MultiLayer Service.

2

Select the ODUk or OTSiG Tunnel infrastructure template.

Result: Default parameters of this template are displayed on the right-hand side.

3

Click **Deploy**  button on the selected template.

Result: Connection window is displayed with **DEPLOY RULES** section selected by default.

For complete steps to add the value in the **Connection Alias 2** attribute, see [8.5 “Deploy a Managed Plane Connection” \(p. 1271\)](#)

END OF STEPS

Task: View Connection Alias 2 attribute in a data table

Complete the following steps to view the **Connection Alias 2** attribute in the data table.

1

From the NFM-T GUI, follow one of the following navigation paths:

OPERATE > Infrastructure Connections > Properties 

OPERATE > Services > Properties 

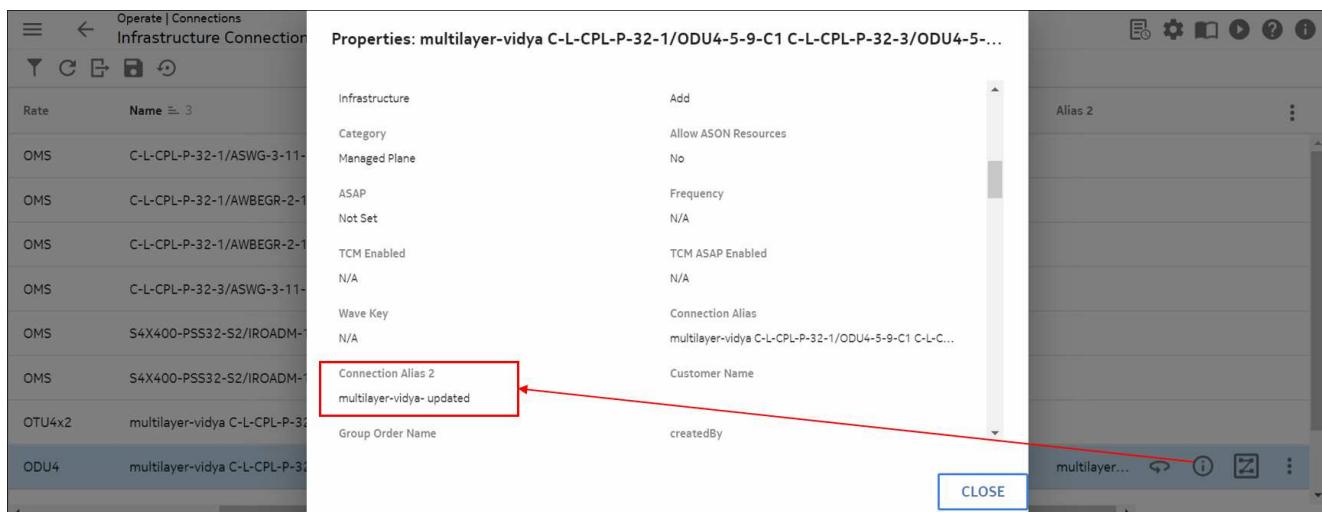
OPERATE > Infrastructure Connections > 360° View > SERVERS (tab)

OPERATE > Infrastructure Connections > 360° View > CLIENTS (tab)

OPERATE > Services > 360° View > SERVERS (tab)

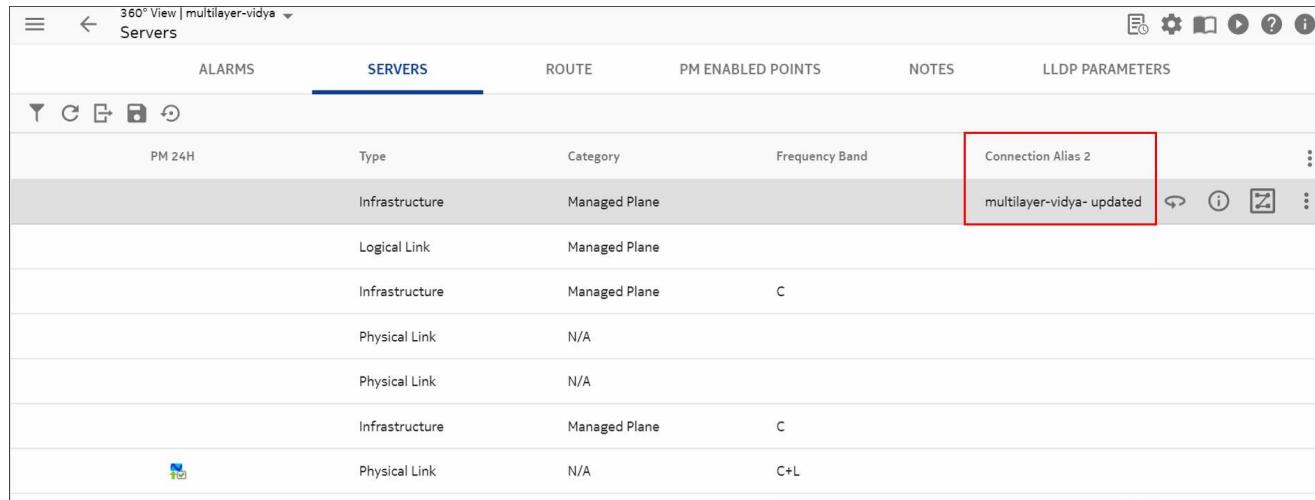
The following figure represents the **Properties** window.

Figure 7-157 Properties - Connection Alias 2



The following figure represents the **360° View** window.

Figure 7-158 360° View - Connection Alias 2



PM 24H	Type	Category	Frequency Band	Connection Alias 2	⋮
	Infrastructure	Managed Plane		multilayer-vidya- updated	
	Logical Link	Managed Plane			
	Infrastructure	Managed Plane	C		
	Physical Link	N/A			
	Physical Link	N/A			
	Infrastructure	Managed Plane	C		
	Physical Link	N/A	C+L		

Result: Based on the selection, the system displays a data table that lists **Connection Alias 2** attribute.

END OF STEPS

Modify Connection Alias 2 attribute

1

From the NFM-T GUI, follow one of the following navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: The corresponding **Infrastructure Connections** or **Services** data table is displayed.

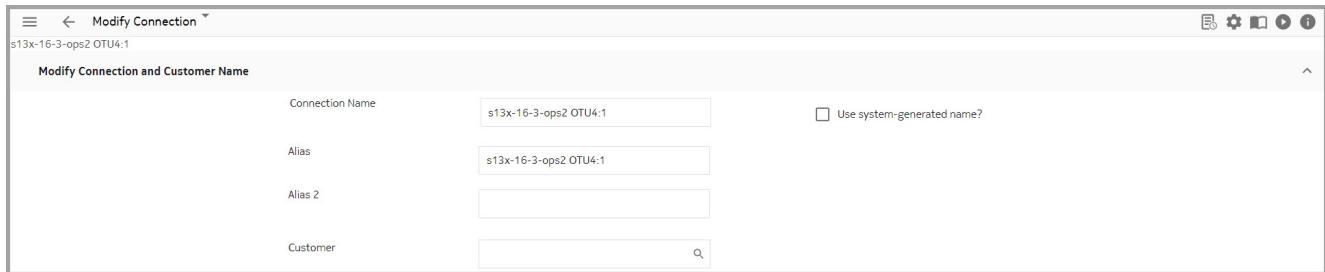
2

Select the connection from the list and click the corresponding **More** icon.

3

Select **Modify Connection > Connection and Customer Name**.

Figure 7-159 Rename Connection - Connection Alias 2



Result: The **Rename Connection And Customer Name** window is displayed.

4

Rename the value in the **Connection Alias 2** field as required.

5

Click **Apply** or **OK**. Alternatively, click **Cancel** to terminate the operation.

Result: The system displays a data table that lists the modified text value in **Alias 2** attribute column.

END OF STEPS

7.56 Manage protection groups (MSP/SNCP) for a protected connection

Purpose

Use this task to manage protection groups (MSP/SNCP) for a protected connection.

The connection must be in the protected state. The options that are available to manage protected connections are **Synchronize Switch Position**, **Protection Lockout**, **Force Switch to Working**, **Force Switch to Protection**, **Manual Switch to Working**, **Manual Switch to Protection**, **Release**, or **Exercise**.

Exercise is cleared automatically at the end of the Exercise routine or the required switch completion time, whichever is sooner. Exercises the protocol for a protection switch of the specified channel, unless a request of equal or higher priority is in effect, by issuing an Exercise request for that channel and checking the response on the APS channel.

You can manage protected for the following types of protected connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Impacted connections of a selected service or infrastructure connection.
Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state
- Used ports of a selected service or infrastructure connection.
Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

Task

Complete the following steps to manage protection groups (MSP/SNCP) for a protected connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

OPERATE > Protected Connections

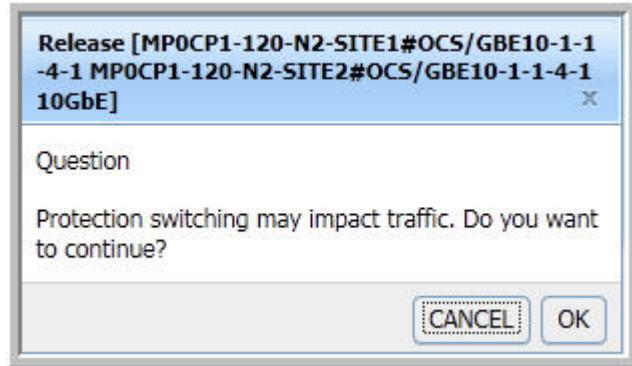
Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Click on a protected connection for which you want to manage protection groups (MSP/SNCP), mouse over the icons on the right of the row, click the **More**  icon, and follow this path **Manage Protection Group**, and select one of the options displayed.

Result: The system outputs a query box informing you that protection switching might impact traffic.

Figure 7-160 Connections – Manage Protection Group – query



3

Click OK.

Result: The system processes your selection and changes the protection switching status to the option that you selected.

END OF STEPS

7.57 Manage NIM for a connection

Purpose

Use this multi-task procedure to enable or disable Non-intrusive Monitoring (NIM) for a connection.

You can manage NIM for the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- PM enabled points of a selected service or infrastructure connection
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

You can enable or disable NIM for ODU4, ODU3e2, ODU3, ODU2e, ODU2, ODU1, or ODU0 infrastructure connections (trails, and logical links) and services in the Managed Plane if the connection is in the **Implemented** or **Commissioned** Deploy State.

Non-intrusive Monitoring, or *NIM*, is a method for reporting defects and performance monitoring (PM) for intermediate services on non-terminated Add/Drop and through connections.

The enable or disable NIM function is available for connections that are listed as Managed Plane, Mixed Plane, and Logical Drop Link in the **Category** column of the connections data table. The enable or disable NIM function is not available for connections that are categorized as **Control Plane**, **ASON Implicit Server**, **ASON MRN Terminated Tunnel** or **ASON MRN Unterminated Tunnel** on the connections data table.

The following NIM guidelines apply:

- For ODUk connections, Ingress NIM is enabled for all connection termination points (CTPs on 1830 PSS OCS NEs).
For ODUk connections, Ingress NIM is not enabled for all FTPs on 1830 PSS OCS NEs.
- For ODUk connections, Egress NIM is enabled for all unterminated connection endpoints and unterminated reliable ports on 1830 PSS OCS NE except:
Egress NIM is not enabled for ports that are cross connected to the ODUPOOL.
Egress NIM is not enabled for ports that are not cross connected if the Infrastructure is a Logical Link.
- For ODUk connections, Ingress NIM is enabled for all CTPs on 260SCX2 circuit packs on 1830 PSS NEs.
For ODUk connections, Ingress and Egress NIM is not enabled for FTPs on 260SCX2 circuit packs on 1830 PSS NEs.

- For ODUk connections, Ingress and Egress NIM is enabled for all CTPs on 1UD200 circuit packs on 1830 PSS NEs.
- For ODUk connections, Ingress and Egress NIM is enabled for all CTPs on 20P200 circuit packs on 1830 PSS NEs, which includes CTPs on BP ports.
For ODUk connections, Ingress and Egress NIM is not enabled for FTPs on 20P200 circuit packs.
- For ODUk connections, Ingress and Egress NIM is enabled for all CTPs on 8P20 circuit packs on 1830 PSS NEs, which includes CTPs on BP ports and virtual plane ports.
For ODUk connections, Ingress NIM is not enabled for FTPs on 8P20 circuit packs. Egress NIM is not supported.
- Ingress NIM and Egress NIM are enabled for all CTPs on 2UC400 and 4UC400 circuit packs.
- Ingress NIM and Egress NIM is enabled for all CTPs on 30AN400 and 4AN400 circuit packs.
Ingress NIM is not enabled for FTPs on 30AN400 and 4AN400 circuit packs.
- For ODUk connections, Ingress NIM is enabled for all CTPs on the Virtual Plane in the route.
For ODUk Connections, Ingress NIM is not enabled for FTPs on the Virtual Plane in the route.
- For ODUk connections, Ingress NIM is enabled for all CTPs on the Preset Plane in the route.
For ODUk connections, Ingress NIM is not enabled for FTPs on the Preset Plane in the route.
- When creating an ODU4 infrastructure connection with one or more endpoints on a D5X500 circuit pack, Ingress and Egress NIM is enabled for all connection termination points that are on D5X500 circuit packs.
Ingress and Egress NIM are not enabled for FTPs or *fake* connection termination points on D5X500 packs.
- For connections that have a **Category of Mixed Plane or Logical Drop Link**, the OTN manager sets Ingress and Egress NIM for ports within the Managed Plain domain. The ASON manager sets Ingress and Egress NIM for for ASON boundary ports or ports within the Control Plain domain.
- Alarm Monitoring is enabled for all ports for which Ingress or Egress NIM is enabled.
- Ingress and Egress NIM cannot be set when creating an infrastructure connection that is a logical link.

Bulk NIM Enable or Disable

You can enable or disable NIM on multiple infrastructure connections (trails, and logical links) and services in the Managed Plane for ODUk service rates and if the connection is in the **Implemented** or **Commissioned** Deploy State.



Note: Implementation status should not be **Defined** and the completion status should always be **Completed**.

Bulk NIM is not available if any non supported connection is selected in the bulk combination.

Task: Disable NIM

Complete the following steps to disable NIM on a connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

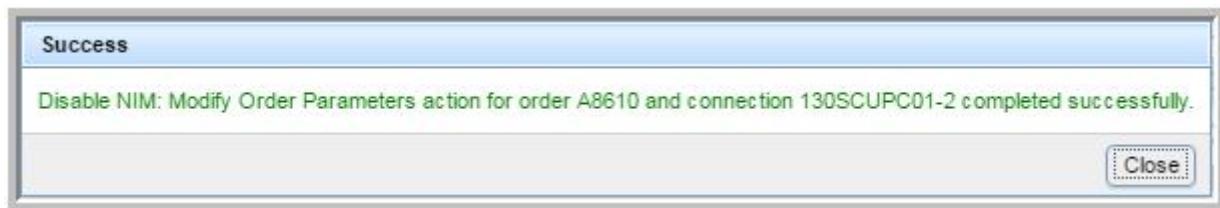
Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Select the **Implemented** or **Commissioned** connection to disable NIM, click on the **More**  icon and follow this path: **Disable NIM**.

Result: NIM is disabled for the selected connection. A success message is displayed for the action.

Figure 7-161 Disable NIM - Success message



END OF STEPS

Task: Enable NIM

Complete the following steps to enable Non-Intrusive Monitoring (NIM) for a connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

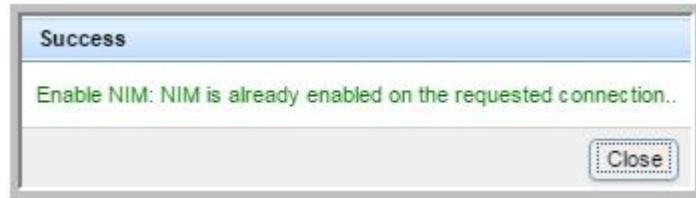
Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Click on a protected **Implemented** or **Commissioned** connection to enable NIM, mouse over the icons on the right of the row, click the **More**  icon, and follow this path **Enable NIM**.

Result: NIM is enabled for the selected connection. A success message is displayed for the action.

Figure 7-162 Enable NIM - Success message



END OF STEPS

Task: Bulk NIM Enable or Disable

Complete the following steps to enable/disable NIM for multiple connections.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

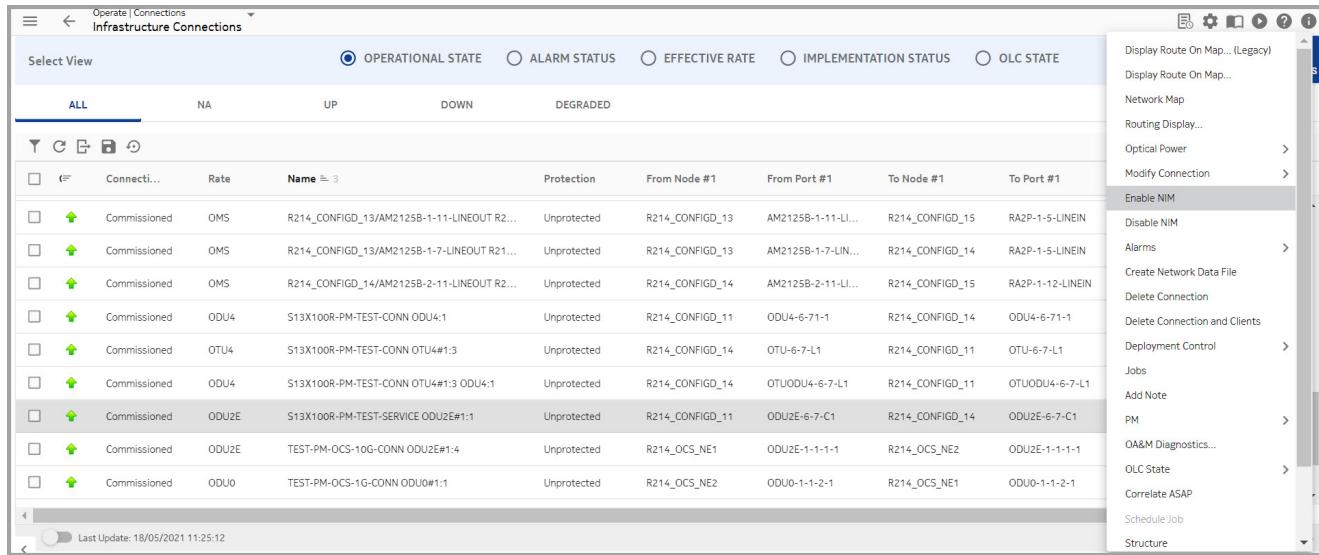
2

Select multiple connections with implementation state as **Commissioned** or **Implemented** connection to enable or disable NIM, mouse over the icons on the top left of the window, click the **More**  icon, and follow this path: **Enable NIM** or **Disable NIM**.



Note: The Enable or Disable NIM is supported only for ODUk service rates.

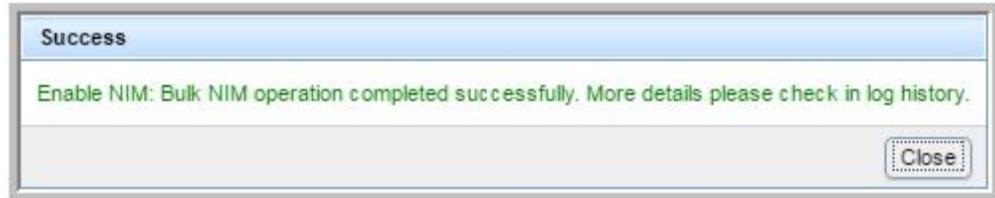
Figure 7-163 Bulk Enable NIM



Result: NIM is enabled or disabled for the selected connections. A success message is displayed for the appropriate action enable or disable.

For example:

Figure 7-164 Bulk Enable NIM - Success message



3

To view the details, navigate to **ADMINISTER > Jobs > Run History**.

Figure 7-165 Bulk Enable NIM - Run History

Run History: PSS4-BA-03/11QCE12X-3-7-X1-PSS8-BA-01/11QCE12X-1-5-X3 OTU2:1 ODU2:1 - Wed Jun 07 17:55:46 IST 2017						
OTN Infrastructure-Modification: PSS4-BA-03/11QCE12X-3-7-X1-PSS8-BA-01/11QCE12X-1-5-X3 OTU2:1 ODU2:1						
Result Details						
Task Name	Sub Task	Task Detail	Status	Remarks	Start Time	End Time
Nim enable		Nim enable	Success		2017-06-07 17:55:46	2017-06-07 17:55:46

END OF STEPS

7.58 Manage protection for a connection in Managed Plane and Control Plane

When to use

Use this task to manage the protection status of a connection.

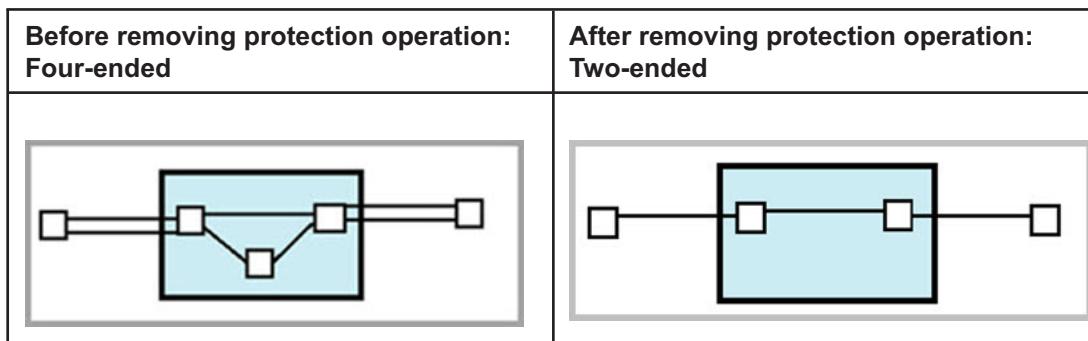
To add protection with user specified routes for Managed Plane, the user has to use the menu option **Modify Connection > Reroute**, see [7.63 “Modify Route \(Reroute\) of a connection” \(p. 987\)](#).

Related information

To change the role of a routing constraint from *service* to *protection* or from *protection* to *service*, go to [7.63 “Modify Route \(Reroute\) of a connection” \(p. 987\)](#) task and note “*Route constraints*” (p. 992).

Add protection - System Routed option uses soft reroute and adds protection to the service without service interruption, but it will calculate the route automatically without considering user constraints.

i **Note:** For a Mixed Plane connection, end points cannot be modified for a Control Plane SNC while adding or removing protection. For example, if the end points of the Control Plane SNC changes from four-ended to two-ended after removing the protection, then the configuration is not supported.



Before you begin

You can manage the protection status of the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service

To change the protection state of a connection, the connection must be in **Commissioned** Implementation State.

Add Protection and Remove Protection are not available for edge HO trails or ASON edge HO trails.

Task: Add Protection to an existing unprotected commissioned connection

Complete the following steps to add protection to an existing unprotected Commissioned connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the selected connections.

2

Optional: To view the protection that is currently assigned to the connection, look at the **Protection** column in the data table to determine if the connection is listed as **OMSP**, **Protected**, or **Unprotected**.

Note: If the **Protection** column is not visible on the data table, click the **More**  icon that is located in the upper right corner of the data table to customize the columns that are displayed in the data table. By checking or unchecking the column headings that are available for display, you can customize your views. Check the **Protection** column then repeat this step.

3

Depending on the type of connection and the existing **Protection** and deployment state of the connection, do one of the following:

Click on a connection, mouse over the icons on the right of the row, click the **More**  icon, and follow this path **Modify Connection** and select **Add Protection**.

Important considerations

- The **Add Protection** option is not available for Control Plane connections or for DSR connections if the ODUk server is a Control Plane connection. The **Add Protection - System Routed** option is not available for Control Plane connections, or for DSR connections that have an ODUk Control Plane server, or for DSR connections if the ODUk server is a Control Plane connection.
- **Add Protection** is not available for Y-cable protected services, Y-cable OPSB protected services, OMS connections with OPSB protection, edge HO trails, and ASON edge HO trails.
- You cannot **Remove Protection** for a connection that has one or more endpoints on a 112SDX11 circuit pack in OTL4.4 mode. These requests must be performed on each individual OTL4.4 connection.

Result: Depending on your selection, the system displays the appropriate deployed template for the connection.

4

Click the **Deploy** button.

Result: If protection type can be added to the connection type selected, the system outputs a message similar to the following in the Add Protection dialog window:

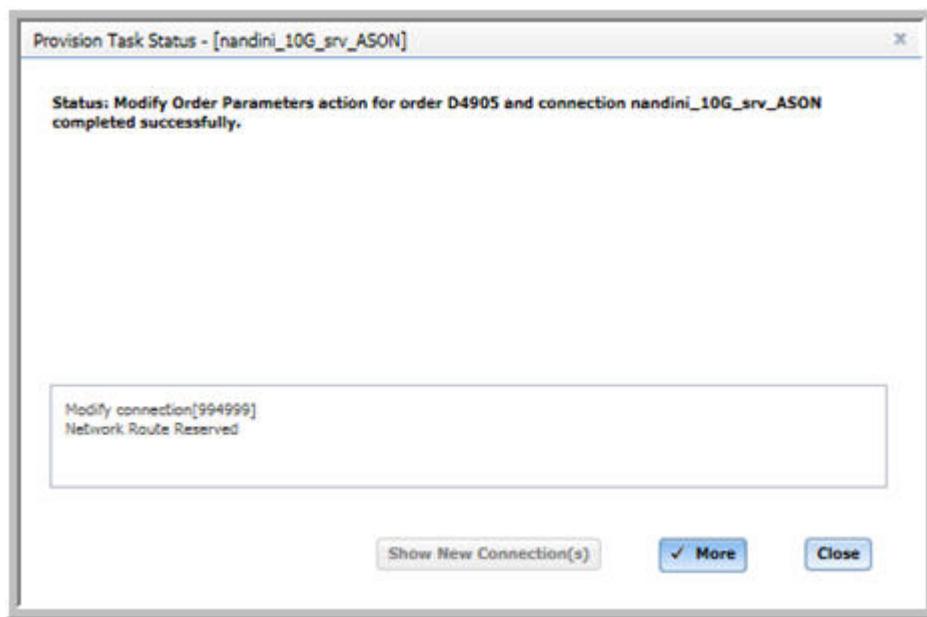
Warning! The modify connection request may cause traffic disruption.
Do you still want to continue?

5

Click on **OK**.

Result: The system displays the Provision Task Status window to inform you of the success or failure of the modification request.

Figure 7-166 Connections – Modify Connection – Add Protection – Provision Task Status window – Success



END OF STEPS

Task: Remove Protection from an existing protected commissioned connection

Complete the following steps to remove protection from an existing protected Commissioned connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the selected connections.

2

Optional: To view the protection that is currently assigned to the connection, look at the **Protection** column in the data table to determine if the connection is listed as **OMSP**, **Protected**, or **Unprotected**.

Note: If the **Protection** column is not visible on the data table, click the **More**  icon that is located in the upper right corner of the data table to customize the columns that are displayed in the data table. By checking or unchecking the column headings that are available for display, you can customize your views. Check the **Protection** column then repeat this step.

3

Depending on the type of connection and the existing **Protection** and deployment state of the connection, do one of the following:

Click on a connection, mouse over the icons on the right of the row, click the **More**  icon, and follow this path **Modify Connection** and select **Remove ASON Protection - Retain Working Path**, or **Remove ASON Protection - Retain Protection Path**.

Important Considerations

- The **Remove Protection...** option is not available for Control Plane connections or for DSR connections if the ODUk server is a Control Plane connection. The **Remove Protection - Retain Main** and **Remove Protection - Retain Spare** options are not available for Control Plane connections, or for DSR connections that have an ODUk Control Plane server, or for DSR connections if the ODUk server is a Control Plane connection.
- **Remove Protection** is not available for Y-cable protected services, Y-cable OPSB protected services, OMS connections with OPSB protection, edge HO trails, and ASON edge HO trails.
- You cannot **Remove Protection...** for a connection that has one or more endpoints on a 112SDX11 circuit pack in OTL4.4 mode. These requests must be performed on each individual OTL4.4 connection.

To perform **Remove ASON Protection – Retain Protection Path** operation for a Protected connection there are two scenarios:

- If the **Revertive Mode** is set to *Manual*, perform **Switch to Nominal** to remove the **Spare Route** from the **Current Route**. In this scenario, **Ready to revert** alarm is triggered by GMRE.
- If the **Revertive Mode** is set to *Automatic*, GMRE removes the **Spare Route** from the **Current Route**.

Result: Depending on your selection, the system displays the appropriate deployed template for the connection.

4

Click the **Deploy** button.

Result: If protection type can be removed from the connection type selected, the system outputs a message similar to the following in a dialog window:

Warning! The modify connection request may cause traffic disruption.
Do you still want to continue?

5

Click on **OK**.

Result: The system displays the Provision Task Status window to inform you of the success or failure of the modification request.

END OF STEPS

Task: Add or Remove protection with single click

Use this function to add or remove protection using dedicated menu items and without specifying any constraints. This function applies to Control Plane and Managed Plane.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

Important Consideration

Add or Remove protection is applicable only for the following connections.

- Connections in Commissioned state.
- Electrical L1 services (DSR) and ODUj trails.
Note: The function is not applicable for photonic trails, as they only support OPSA protection which is fixed with hardware connectivity
- 2-Ended connections
- Paths ending on NE with packs supporting Add/Drop SNCP.

 **Note:** The function is not applicable for Muxponders, transponders that does not fully support flexible SNCP switching.

Add or Remove protection is applicable only for the following protection types.

- *Unprotected:* If the connection is unprotected and supports network SNC protection. The system finds a protected route automatically that is diverse from the working leg. System tries to find an end to end protected route or segment protected route based on the switching capability of the nodes involved in working path.
- *SNCP/SNC-N Protected:* If the connection is SNC/SNC-N protected, the system automatically removes the leg specified by user to find unprotected route.



Note: Add Protection only works for SNCP, not for SNC/N. An SNC/N protection can be removed, but when the protection is added back, it will be SNCP type.

Result: Depending on your selection, the system displays a data table that lists all of the selected connections.

2

Select the connection from the list, click the More icon, and follow this path **Modify Connection**.

Result:

If	Then
Selected connection is Unprotected	the menu item displayed is Add Protection - System Routed or Add Protection System Routed : Enable on ODUj Unprotected connection
Selected connection is Protected	the menu items displayed are Remove Protection - Retain Working and Remove Protection - Retain Protection

Figure 7-167 Add or Remove Protection - remove menu items

The screenshot shows the 'Operate | Connections Infrastructure Connections' view. The main area displays a table of connections with columns: ALL, NA, UP, DOWN, and DEGRADED. A context menu is open over a row for a connection named '11STMM10_OPS OTU2:1'. The menu path 'Modify Connection' is visible, followed by a submenu with options: 'Connection and Customer Name...', 'Parameters', 'Parameters... (Legacy)', and 'Reroute'. The 'Reroute' option is highlighted with a red box. The right side of the screen shows a vertical toolbar with various icons and a list of actions: Display Route On Map..., Network Map, Routing Display..., Optical Power, Modify Connection, Alarms, Create Network Data File, Delete Connection, Delete Connection and Clients, Deployment Control, Jobs, Add Note, PM, OA&M Diagnostics..., OLC State, Correlate ASAP, Schedule Job, Structure, and Structure (Legacy). The status bar at the bottom indicates 'Last Update: 17/05/2021 16:42:00'.

3

Select the corresponding menu item.

Result: The system submits the request and sends a message.

The function sets by default the restoration type as soft. If soft restoration is not supported by the underlying configuration, the system returns an error message.

If the request is remove protection on a protected connection that has Double add drop XC, the system returns an error. Converting Double add drop to simple cross connection is traffic impacting and is not supported with this Remove Protection operation. If you try to remove protection for an SNC/N protection type, an error message is displayed as you can see in the figure below.

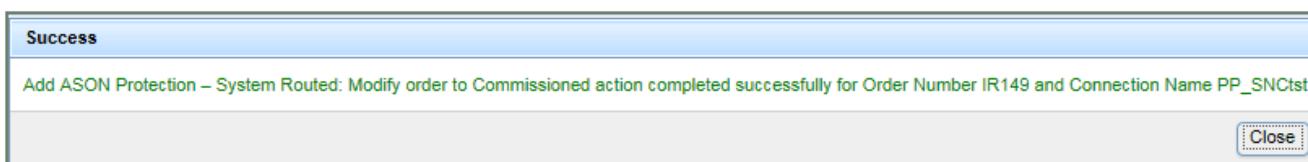
Figure 7-168 Add or Remove Protection - error message

Log History					
Status	Command	Target Objects	Start Time	End Time	
Failed	Remove Protection	connName : Jason_XX_100G_SNC	2/14/2018 5:29:32 PM	2/14/2018 5:29:33 PM	
Remove Protection with soft rearrange is not supported for the connection with double AddDrop XC. Use hard rearrange using modify route to remove protection.					
Success	Get Fiber Characteristics	SITE21-1/A2325A-1-10-LINE-SITE	2/14/2018 5:27:22 PM	2/14/2018 5:27:26 PM	
Success	Get Fiber Characteristics	SITE20-1/A2325A-1-6-LINE-SITE2	2/14/2018 5:27:11 PM	2/14/2018 5:27:22 PM	
Success	Create Connection	Jason_XX_100G_SNCN_DSR	2/14/2018 5:21:54 PM	2/14/2018 5:22:28 PM	
Activate	Create Entity	NE - SITE21-1, NE Type : 1830pss	2/14/2018 5:20:27 PM		
Activate	Create Entity	NE - SITE20-1, NE Type : 1830pss	2/14/2018 5:20:21 PM		
Activate	Create Entity	NE - SITE21-1, NE Type : 1830pss	2/14/2018 5:19:53 PM		
Activate	Create Entity	NE - SITE20-1, NE Type : 1830pss	2/14/2018 5:19:50 PM		
Success	Create Connection	connName : Jason_XX_LL4	2/14/2018 5:18:20 PM	2/14/2018 5:18:53 PM	
Activate	Internal Topology Link Create	NE SITE23-1, aEnd SFD-33-1-948I	2/14/2018 5:16:57 PM		

4

When the operation is terminated a message box is displayed with the operation result.

Figure 7-169 Add ASON Protection - result box example



Add Protection - System Routed: A single click action that finds automatically a route diverse with the working route.

Remove Protection - Retain Working: A single click action in which the system drops the designated protection route.

Remove Protection - Retain Protection: A single click action in which the system drops the designated working route.

5

Click **Close** button to close the box.

END OF STEPS

7.59 Manage protection for a Mixed Plane service

When to use

Use this task to add or remove the protection status for an end to end service in mixed plane connection in L1 GMPLS/MRN.

For managing protection in Managed Plane and Control Plane, see [7.58 “Manage protection for a connection in Managed Plane and Control Plane” \(p. 960\)](#)

Related information

The supported scenarios for managing protection in Mixed Plane are as follows:

- Managed Plane (MP) to Managed Plane (MP) service passing through Control Plane (CP) domain

The symmetric configuration where both the end points are in MP. The add protection is created as a different ASON SNC which is not overlapping with the working path, also known as segmented protection.

- Managed Plane (MP) to Control Plane (CP)

An asymmetric configuration where one end point is MP and another end point is in CP.

- Managed Plane (MP) to Control Plane (CP) with open SNCP

Open SNCP is a protected service configuration with a 3-ended bidirectional ASON SNC connection SNCP protected in an L1 GMPLS domain, where the protection is opened when entering GMPLS and closed outside of GMPLS.

i **Note:** Network 1 is always the working port and Network 2 is always the protection port, this is fixed behavior on the 1830 PSD NE.

Before you begin

You can manage the protection status of the following types of connections:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service

To change the protection state of a connection, the connection must be in **Commissioned** Implementation State.

Add Protection and Remove Protection are not available for edge HO trails or ASON edge HO trails.

Task: Add Protection to an existing unprotected commissioned connection

Complete the following steps to add protection to an existing unprotected Commissioned connection.

1

Follow the navigation path from the NFM-T GUI:

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the selected connections.

2

Optional: To view the protection that is currently assigned to the connection, look at the **Protection** column in the data table to determine if the connection is listed as **SNCP-N**, **SNCP-N Server Protected**, **SNCP-Nc Server Protected**, **Server Protected**, **Protected**, or **Unprotected**.

Note: If the **Protection** column is not visible on the data table, click the **MANAGE COLUMNS** icon on top right corner to manage the columns in data table.

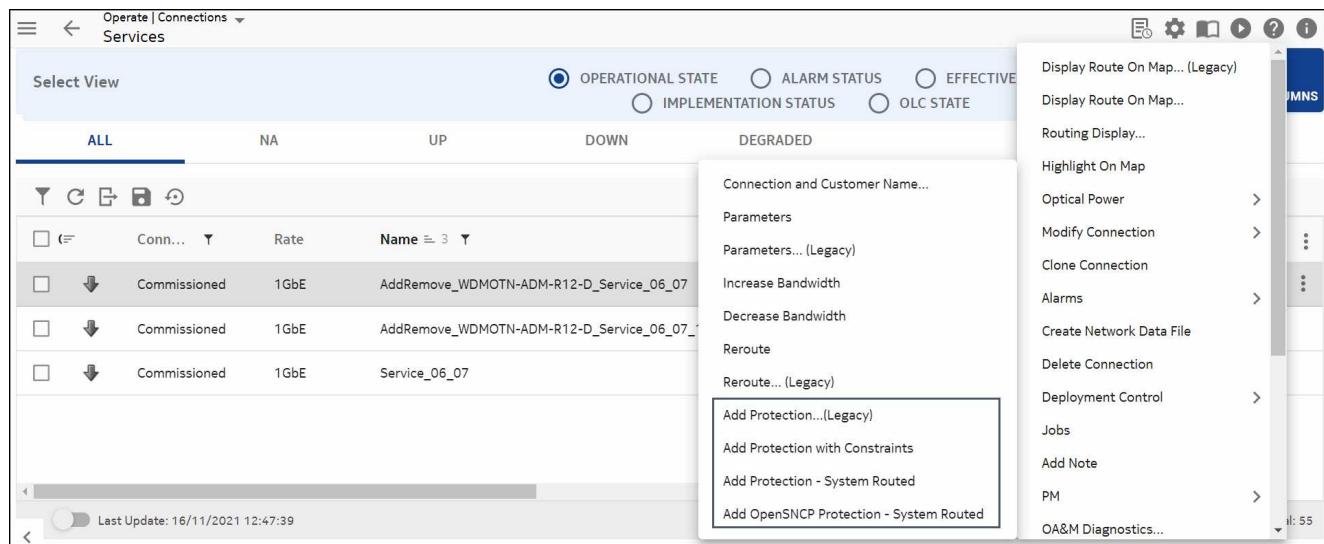
3

Depending on the type of connection and the existing **Protection** and deployment state of the connection, do one of the following:

Select the connection and click the corresponding **More**  icon, and follow this path **Modify Connection** and select one of the following:

- **Add Protection - (Legacy)**
- **Add Protection with Constraints**
- **Add Protection - System Routed**
- **Add OpenSNCP Protection - System Routed**

Figure 7-170 Add Protection - Mixed Plane



Important considerations

- The **Add Protection with Constraints** option provides the user to add full route constraints for the protection path only. No change of the main path or constraints is allowed.
- For SNCP, the connection shape can be changed from 2 ended to 3 ended bidirectional. The default Open SNCP status will be set to true. Connection shape can be changed by selecting **Connection Shape** drop down, select 3 ended Z bi and provide TO **NODE#2** and TO **PORT#2** details on UI along with full route constraints.
- The **Add Protection - System Routed** option provides an automatic end-to-end add protection route by the system. This option is not available for Control Plane connections, or for DSR connections that have an ODUk Control Plane server, or for DSR connections if the ODUk server is a Control Plane connection. This option can be used for Open SNCP by manually checking the Open SNCP checkbox. This option is a single click add protection system routed which is used to add protection resulting in open SNCP
 - The **Add Open SNCP Protection - System Routed** option provides an automatic end-to-end add protection route by the system. Open SNCP option is enabled by default.

Result: Depending on your selection, the system displays the appropriate deployed template for the connection.

In the **Add Protection with Constraints** option, the included link connection constraint is added as Protection. **REMOVE** button is enabled for removing the protection path, whereas **REMOVE ALL** button is disabled.

Figure 7-171 Add Protection with Constraints - Remove

Type	Constraint	Role	Name	Frequency	Channel
Link	Include	Service	8UC1T_22_23_Tunnel_1 ODU4:2		5
Link	Include	Service	8UC1T_22_23_Tunnel_1 ODU4:2		6
Link	Include	Service	8UC1T_22_23_Tunnel_1 ODU4:2		7
Link	Include	Service	8UC1T_22_23_Tunnel_1 ODU4:2		8
Link	Include	Service	8UC1T_22_23_Tunnel_1 ODU4:2		9
<input checked="" type="checkbox"/> Link	Include	Protection	OPS_22_ENE_1 OTU2:1 ODU2:1	NA	4

Last Update: 28/09/2021 23:06:45 Total: 9

INCLUDE SERVICE PROTECTION REMOVE REMOVE ALL

BACK CONTINUE DEPLOY SAVE CONSTRAINT TEMPLATE

4

Click the **Deploy** button.

Result: **DEPLOY** section is displayed. As the deployment progresses, the progress bar increases in percentage and the states move from **Defined > Allocated > Implemented > Commissioned**. Once the deployment is successful a success message is displayed at the bottom of the section.

5

Optional: Click **SHOW NEW CONNECTION(S)** to view the new connection.

Click **ROUTING DISPLAY** view the end-to-end routing display for the connection.

Click **JOBs** to view the log and status of the connection.

6

Optional: Click **SHOW FAILED CONNECTION(S)** to view the deployed connection.

i Note: In case of an error during any of the states, red color is displayed in the progress bar and the state at which the error occurs. Also, an error message is displayed.

END OF STEPS

Task: Remove Protection from an existing protected commissioned connection

Complete the following steps to remove protection from an existing protected Commissioned connection.

1

Follow the navigation path from the NFM-T GUI:

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the selected connections.

2

Optional: To view the protection that is currently assigned to the connection, look at the **Protection** column in the data table to determine if the connection is listed as **SNCP-N**, **SNCP-N Server Protected**, **SNCP-Nc Server Protected**, **Protected**, or **Unprotected**.

Note: If the **Protection** column is not visible on the data table, click the **MANAGE COLUMNS** icon on top right corner to manage the columns in data table.

3

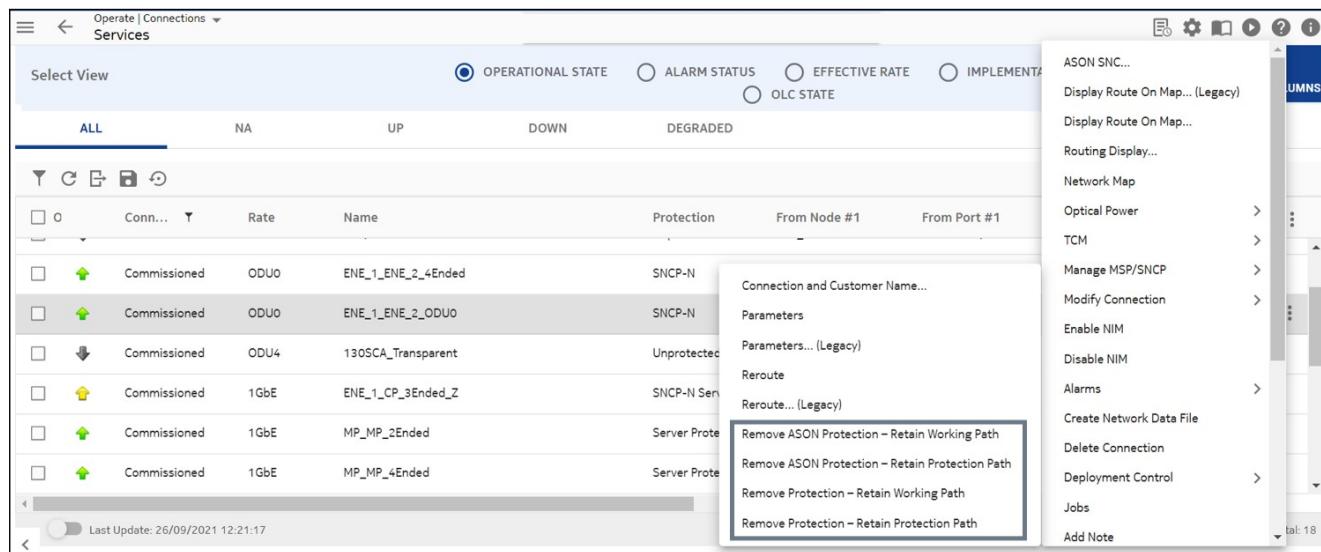
Depending on the type of connection and the existing **Protection** and deployment state of the connection, do one of the following:

Select the connection and click the corresponding **More**  icon, and follow this path **Modify Connection** and select one of the following:

- **Remove ASON Protection - Retain Working Path**

- Remove ASON Protection - Retain Protection Path
- Remove Protection - Retain Working Path
- Remove Protection - Retain Protection Path

Figure 7-172 Remove Protection - Mixed Plane



Important considerations

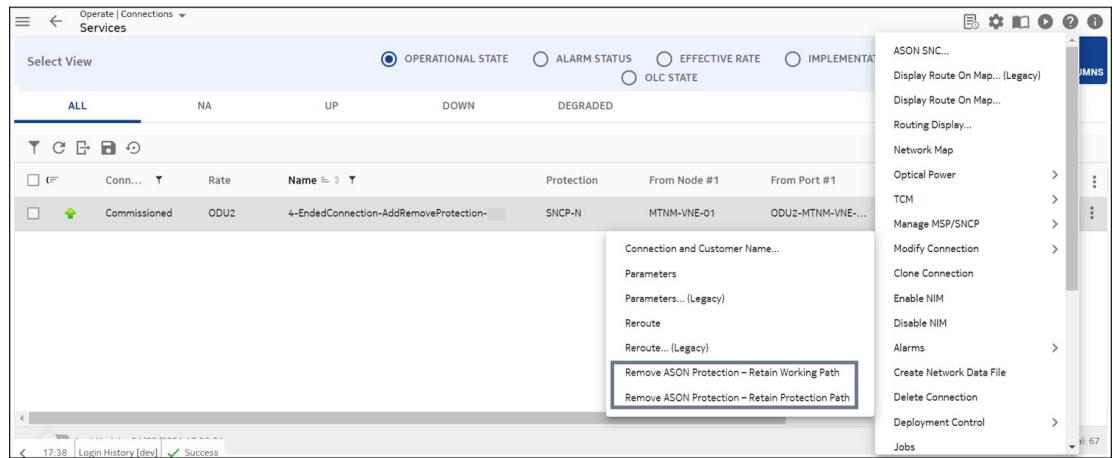
To perform **Remove ASON Protection – Retain Protection Path** operation for a Protected connection there are two scenarios:

- If the **Revertive Mode** is set to *Manual*, perform **Switch to Nominal** to remove the **Spare Route** from the **Current Route**. This is a mandatory step. In this scenario, **Ready to revert** alarm is triggered by GMRE.
- If the **Revertive Mode** is set to *Automatic*, GMRE removes the **Spare Route** from the **Current Route**.
- **Remove Protection - Retain Working Path** option, in which the system drops the designated protection route.
- **Remove Protection - Retain Protection Path** option, in which the system drops the designated working route.

Result: A confirmation window for removing protection is displayed.

- If ASON SNC belongs to a 3-ended or 4-ended mixed plane connection, then end-to-end Remove protection is not supported. Remove ASON protection without open SNCP is only supported. The options are **Remove ASON Protection - Retain Working Path** and **Remove**

ASON Protection - Retain Protection Path as shown in the following figure:



- For a connection with 3-ended or 4-ended ASON SNC, in case, a user views the option: **Remove Protection - Retain Working Path** and **Remove Protection - Retain Protection Path** then by clicking the option, the message is displayed: User cannot perform Remove Protection if ASON SNC is 3 or 4 Ended, Try Remove ASON Protection.
- For OPEN SNCP Mixed plane connection, **Remove Protection - Retain Working Path** is supported.

4

Click **YES**.

Result: The system removes the protection depending on the selection.

5

Navigate to **ADMINISTER > Jobs** or **ADMINISTER > All Records** page to view the log and status of the connection

END OF STEPS

Note:

For an I-shaped SNCs configuration, after performing **Modify Connection > Add Protection with Constraints** or **Modify Connection > Add Protection - System Routed** two unprotected ASON SNCs get created:

- <Connection Name>#0Main
- <Connection Name>#0Spare

When user performs **Modify Connection > Remove ASON Protection – Retain Protection Path** then:

- <Connection Name>#0Main is removed.

-
- <Connection Name>#0Spare is retained.

Again, if user performs **Modify Connection > Add Protection with Constraints** or **Modify Connection > Add Protection - System Routed** then the retained spare label gets appended. The modified ASON SNCs are as follows:

- <Connection Name>#0Spare
- <Connection Name>#0Spare1

7.60 Manage the service state of connection

When to use

Use this task to manage the service state of a connection.

Before you begin

You can enable or disable the service state of the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- PM enabled points of a selected service or infrastructure connection
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

Important! The **Service State** parameter and its setting differs for logical connections (infrastructures and services) and physical connections. The **Service State** of a logical connection is based on the values of the alarm reporting parameter of the connection end points. If all connection end points have the alarm reporting parameter **ON** or if they have the primary state parameter set to **IS-NR**, **IS-ANR**, or **OOS-AU**, the **Service State** of the connection is **ON**. If any connection end point has the alarm reporting parameter **OFF** or if they have the primary state parameter set to **OOS-MA** or **OOS-AUMA**, the **Service State** of the connection is **OFF**. The Service State is **NA** for internal connectivities.

If the ports that are part of the endpoints of an infrastructure connection or service are set to **Maintenance** state, the **Service State** for the infrastructure connection or service is also set to **Maintenance** state.

In addition, determinations other than the connection end point regarding the **Service State** include the following:

- When a connection endpoint is on a black box, the alarm reporting parameter or the OT port that is connected to the black box determines the **Service State** and not the connection endpoint.
- For service connections with Y-cable protection, the alarm reporting parameter of the OT client ports determines the **Service State** and not the connection endpoints.
- For service connections with OPSB Protection, the alarm reporting parameter of the OT client ports determines the **Service State** and not the connection endpoints.
- For service connections with OPS protection, the alarm reporting parameter of the OT/SVAC/MVAC client ports determines the **Service State** and not the connection endpoints.

Both the **Enable Service State** and **Disable Service State** features are not available for connections with a category value of Control Plane, ASON MRN unterminated tunnel, or ASON MRN terminated tunnel, ASON logical link, and ASON implicit server, and an ASON edge HO trail.

Task: Disable the service state

Complete the following steps to disable the service state of a connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

OPERATE > Protected Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Depending on the connection, click on the **More :** icon on the connection to disable the service state and follow this path: **Disable Service State**.

Result: The system disables the service state of the selected connection and outputs a message that is similar to the following:

Figure 7-173 Connections – Disable Service State – message



END OF STEPS

Task: Enable the service state

Complete the following steps to enable the service state of connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

OPERATE > Protected Connections

OPERATE > Services

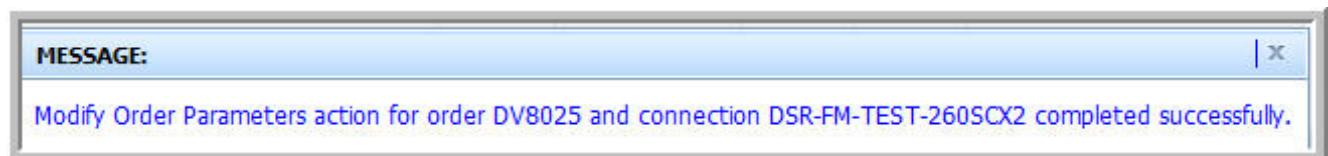
Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Depending on the connection, click on the **More :** icon on the connection for which you want to enable the service state and follow this path: **Enable Service State**.

Result: The system enables the service state of the selected connection and outputs a message that is similar to the following:

Figure 7-174 Connections – Enable Service State – message



END OF STEPS

7.61 Manage 3R for Managed Plane connections

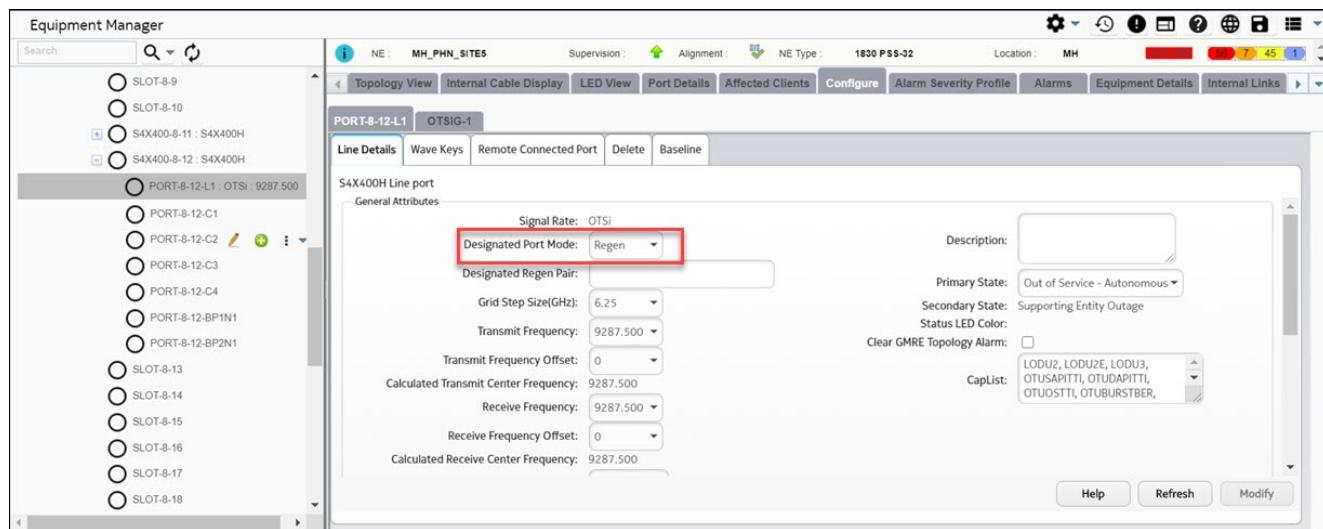
Purpose

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. Managing 3Rs for Managed Plane connection includes the create 3R, add 3R as a routing constraints while modifying a route, and remove 3R. It is also supported for the OTSig Tunnel.

Before you begin

By default, the **Designated Port Mode** for the OTSi is set to **Add/Drop**. As a prerequisite, for the unidirectional 3R, from the Equipment Manager **Configure** tab, ensure that the **Designated Port Mode** is set to **Regen**.

Figure 7-175 OTSi – Designated Port Mode – Regen



Use these tasks to manage 3Rs for Managed Plane connections.

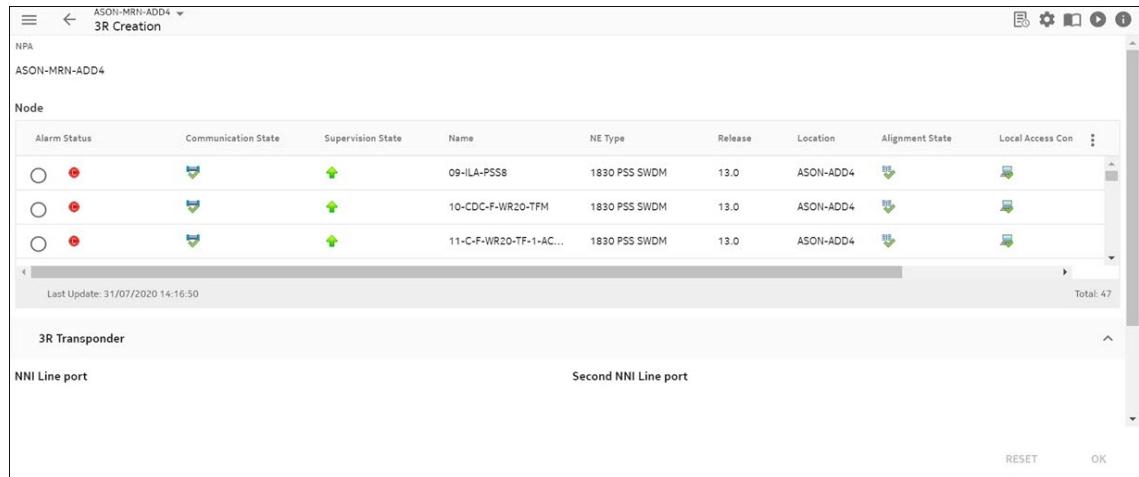
Note: The system supports the allocation by means of automatic routing or through manual routing. With automatic routing, the 3R must be used only if there are no alternative paths without 3R.

Task: Create a 3R for Managed Plane connection

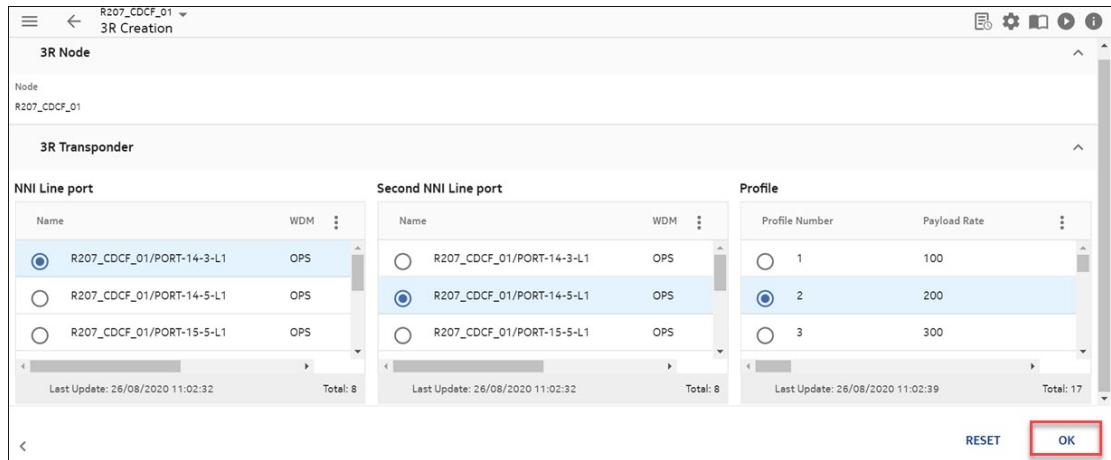
Complete the following steps to create a 3R for Managed Plane connections from the **NODES** page for S4X400H card.

1. From the NFM-T GUI, navigate to **OPERATE > NODES**.
2. Select a node, click the corresponding **360° View > 3R** tab.
3. Click the **Create** icon on the top left of the window. The system displays the **3R Creation**

window as shown in the following figure.



4. In the **3R Transponder** panel, configure the following fields as shown in the following figure:
 - In the **NNI Line port** field, select a port to add it to the 3R Transponder panel.
 - In the **Second NNI Line port** field, select a port to add it to the 3R Transponder panel.
 - In the **Profile** field, select a profile to add it to the 3R Transponder panel.



5. Click **OK**. The system creates a 3R and is added to the 3R tab for the selected Node and listed in **Allocated** state.

Task: Remove a 3R for Managed Plane connection

Complete the following steps to remove a 3R for Managed Plane connections from the **NODES** page for S4X400H card.

1. From the NFM-T GUI, navigate to **OPERATE > NODES**.
2. Select a node, click the corresponding **360° View > 3R** tab.

-
3. Select the 3R, click the corresponding **More**  icon and then select **Remove**. The selected 3R is removed from the system.



Note: Refer to the [8.11.12 “Task: To Modify the route of OTSig Tunnel” \(p. 1337\)](#) section to modify a route of an OTSig tunnel and add 3R as a routing constraint.

7.62 Modify the parameters of a connection

When to use

Use this task to modify the parameters to modify the parameters of a connection.

Before you begin

When you modify the parameters of a connection, you are actually modifying the template from which the connection was created. The system determines which parameters can be modified.

NIM is supported for all the OCS packs and all new PHN packs which have Client-Line modelling (including PSS24x supported packs). NIM Enabling is supported on all ODUj infrastructure and services. NIM is supported on both symmetric configurations and asymmetric configurations including protected configurations.

In the *Modify Parameters* screen, the **Connection Name** and **Connection Alias**, the **Customer Name** fields are disabled and cannot be modified, to modify these fields use the task [7.64 “Rename Connection and Customer Name” \(p. 997\)](#). A tooltip is displayed that suggest the use of the **Rename Connection** function.

You can modify the parameters of the following types of connections by using the steps that are provided in this task:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- Impacted connections of a selected service or infrastructure connection
Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

i **Note:** *Transmission Parameters settings are not supported for Mixed Plane and Control Plane connections.*

Important provisioning consideration when modifying OTU4/OTL4.4 connections: For OTL4.4 connections, the Transmission Parameters and Assurance panels are disabled and the Wave Keys panel is enabled. For OTU4 connections with one or more endpoints on the 112SDX11 pack and server OTL4.4 connections, the Transmission Parameters and Assurance panels are enabled and the Wave Keys panel is disabled. For OTU4 connections with one or more endpoints on the 112SDX11 pack that do not have server OTL4.4 connections, the Transmission Parameters, Assurance, and Wave Keys panels are enabled.

Important provisioning consideration when modifying OTUK parameters for OPSA with 3R:

When you modify the Transmission Parameters (such as TTI) of an OTUk connection that is a server in the *working path* of an OPSA protected ODUk connection, the system automatically updates the parameters on the OTUk connection that is the server in the protection path that

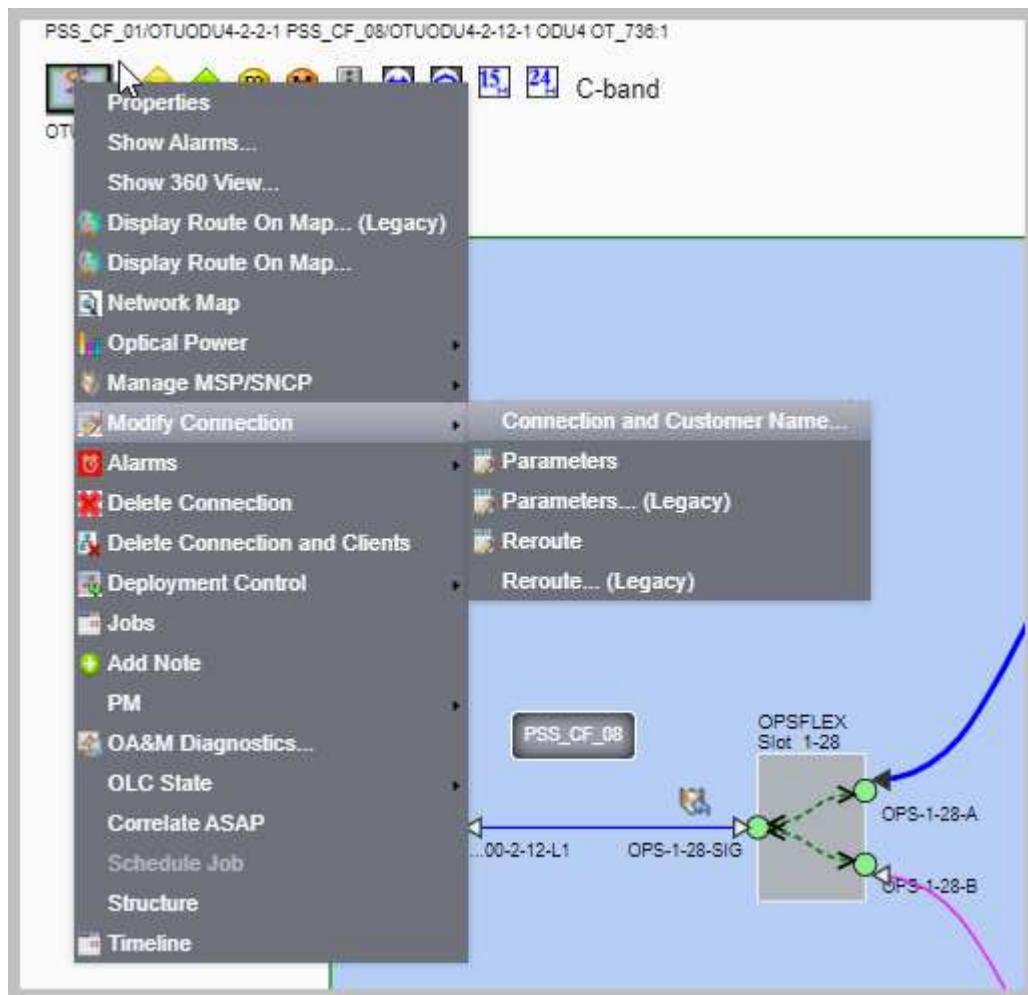
shares the same connection endpoint. And conversely, when you modify the transmission parameters (such as TTI) of an OTUK connection that is a server in the *protection path* of an OPSA protected ODUK connections, the system automatically updates the OTUK connection that is the server in the working path that shares the same connection endpoint.

Important! Use separate **Modify Connection - Reroute** and **Parameters** requests if the modification of the connection route and the connection parameters are needed.

Example: If a connection needs to be rerouted and the parameters of this connection need to be changed, then use two steps:

1. Click on the **More** icon on the connection, select **Modify Connection > Reroute ...**, make changes in the connection route, and then **Deploy** the change.
2. Click on the **More** icon on the connection, select **Modify Connection > Parameters...**, make the necessary changes in the parameters, and then **Deploy** the change.

Figure 7-176 Modify Connection - Menu selection



Task

Complete the following steps to modify the parameters of a connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

OPERATE > Protected Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

Highlight and select the connection for which you want to modify parameters and click on the **More**  icon on the right of the connection row and follow this path: **Modify Connection > Parameters**

Result: The system displays the **Modify Connection** window.



Note:

- During the modification of the connection, If connection name is empty and if system generated name is not selected, then system displays an error message.
- During the modification of the connection, the deployment is successful if the **Customer Name** is left blank.

3

Make the necessary changes to suit your installation. For detailed explanations of each template field, refer to [7.5 “Advanced Settings field descriptions for deploy Best Practices templates” \(p. 708\)](#).

Important provisioning considerations!

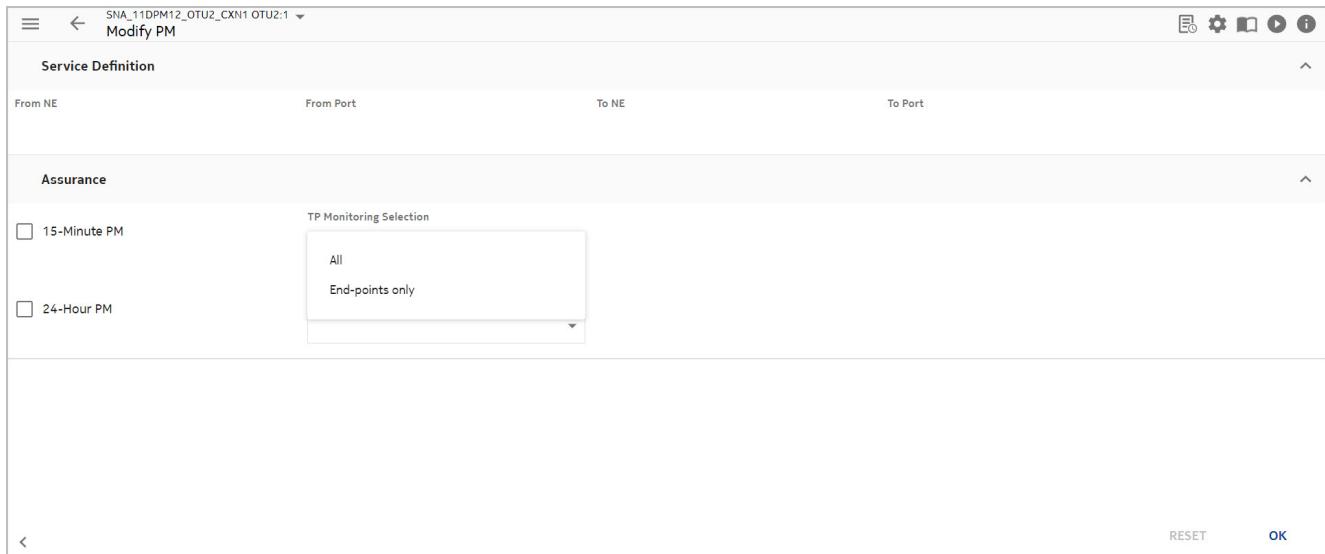
- The system determines which parameters you can modify based on the type of connection that you select, the particular transmission parameter that you are trying to modify, the current **Implementation State** of the connection, and whether one or more end points have been changed.
- In the Service Definition, you can modify the **Transmission Mode** parameter if the connection rate is OTU4x2 or OTU4 and at least one connection endpoint is on a D5X500 card, a 4UC400, or a 2UC400 pack.

Note: The **Transmission Mode** parameter cannot be edited for a Modify Transmission Parameters request. For details, refer to [“Transmission Mode” \(p. 701\)](#).

- When changing an end point, if you select an unassigned port on an 1830 PSS OCS NE as the new endpoint, if the pluggable module for the port is already equipped, the pluggable module drop-down list for the port contains only the equipped pluggable module. If you select an unassigned port on an 1830 PSS OCS NE as the new endpoint, if the pluggable module for the port is not already equipped, the pluggable module drop-down list for the port contains all possible pluggable modules. Third party pluggable modules are supported and are identified on the drop-down list as **USER**.
 - You can modify the **SNC Protection** parameters if the **ASON Routed** check box on the Service Definition panel is checked and the connection shape is one of the supported bi-directional shapes. Network protection can be specified for all connection shapes; client protection can only be specified for connections in which the connection shape is other than 2-ended. **SNC-I** is only displayed for the Client Protection Type field if all connection endpoints are on 1830 PSS OCS NEs and black boxes. **SNC-Nc** is only displayed for the Network Protection Type and Managed Plane Network Protection Type fields if all connection endpoints are on 11DPM8 packs and black boxes. **ODUk Path Adaptation** is only displayed for the Client Protected Protection Method and Client Protecting Protection Method fields if all connection endpoints are on 1830 PSS OCS NEs and black boxes. Depending on the current values and the current **Implementation State**, some fields are read-only. For other details, refer to “[SNC Protection](#)” (p. 717).
 - Newly created services the **ASON Restoration** from *Source-based Restoration* to *Guaranteed Restoration* without service removal. To change the **ASON Restoration** for already setup services L0 ASON SNC in previous releases of NFM-T from Source-based Restoration to Guaranteed Restoration you have to remove and re-create the service.
 - When you modify the **Frequency**, the system validates if the connection consists of one link connection or the connection type is a tandem connection. If the system fails the validation, change the **Frequency** field to the original value and retry the request.
 - You can only change manual Wave Keys when a **Rearrange** of the connection changes the frequency of the connection. Therefore, for all other instances, use **Modify Parameters** to change the manual Wave Keys.
 - Because rekeying is not supported during a **Rearrange**, use **Modify Parameters** to rekey a connection. For a **Rearrange** without frequency change, if you want to rearrange the connection without allowing duplicate wave keys for the frequency, first rearrange the connection and then use **Modify Parameters** to rekey the connection. For a **Rearrange** without frequency change, if you want to rearrange the connection and allow duplicate wave keys for the frequency, first use **Modify Parameters** to rekey the connection with duplicates, then **Rearrange** the connection. For a **Rearrange** with frequency change, the wave keys must change since the frequency is changing. When you rearrange the connection, if you want to allow duplicate wave keys for the frequency, choose **Duplicates Allowed** for the AZ Wave Keying Preference and/or ZA Wave Keying Preference.
- For OTL4.4 connections, the Transmission Parameters and Assurance panels are disabled and the Wave Keys panel is enabled. For OTU4 connections with one or more endpoints on the 112SDX11 pack and server OTL4.4 connections, the Transmission Parameters and Assurance panels are enabled and the Wave Keys panel is disabled. For OTU4 connections with one or more endpoints on the 112SDX11 pack that do not have server OTL4.4 connections, the Transmission Parameters, Assurance, and Wave Keys panels are enabled.

4

In the **Assurance** tab, the fields are not editable. To modify the PM attributes, right-click on a connection, select **PM > Modify PM**.

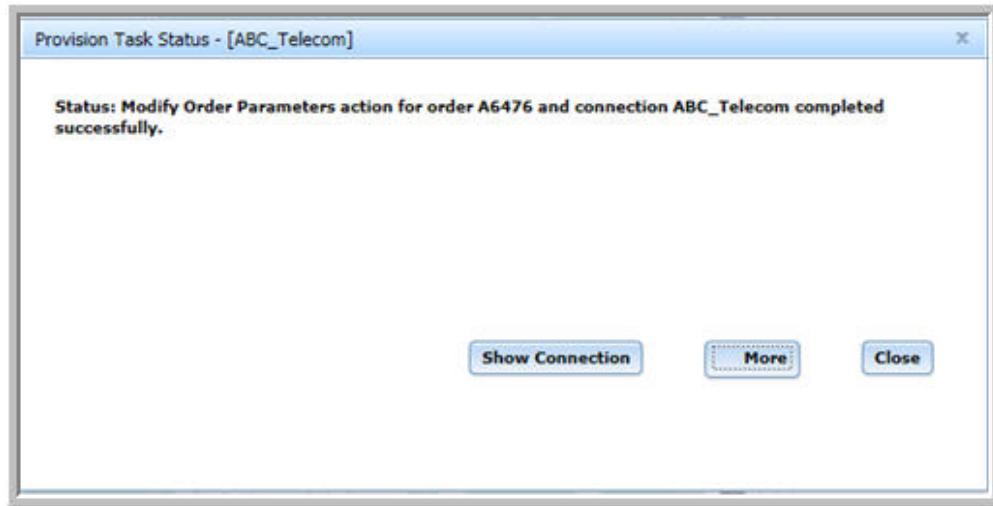


5

Click **Deploy**.

Result: The system makes the requested changes and outputs a message window similar to the following:

Figure 7-177 Connections – Infrastructure Connections – modify parameters – Provision Task Status



6

Optional: To view connection details for the connection that you just modified in data table format, click on **Show Connection**.

Result: The system opens the data table and displays the modified connection.

END OF STEPS

7.63 Modify Route (Reroute) of a connection

Description

This function allows the user to change the path route of a connection without having to fully define the new route. The user can specify automatic routing and add constraints so that the new route is directed towards the path requested. You can provide a partial set of **INCLUDE** or **EXCLUDE** constraints as input.

The Managed Entity for L0 Control plane connection is the ODUk and only that entity can be modified. For Edge HO Trails, HO Aggregated trails that leave the managed domains cannot be rearranged as it will have implications on far-end of the trail for which NFM-T does not have control.

i Note: In an L1 Mixed plane scenario, the user is not allowed to modify the route of the end-to-end ODUk Connection. This implies, changing the end points of the ASON SNC in Control plane domain. The L1 ASON SNC end points are identified by their location (NE, port), rate and by the time slot. Changing one of these characteristic means changing the end point and the GMRE requires the SNC to be deleted. The new end points are re-assigned as drop and the SNC with new end points are re-provisioned. As a consequence, under this modify route condition, the system displays an error message and the user must perform the delete of the end-to-end ODUk Connection and re-create it.

i Note: Selecting a connection and following the path **Modify Connection > Reroute** allows the action only on the selected layer rate which supports rerouting. Integrated provisioning (multiple layers) is not supported. To perform the modify connection you have to select a connection from the Infrastructure list which is reroutable, for example a Layer 0 ODUk or a Layer 1 ODUj.

i Note: If the connection category of a service is managed plane and its corresponding server is control plane, the **More** options of the control plane connection are disabled if the corresponding SNCs are marked inconsistent. When you perform reroute operation on this managed plane connection, the system displays an error message as shown in the [Figure 7-178, "S4X400H – reroute – error message" \(p. 988\)](#). In this scenario, you must perform DB delete for the connection.

Figure 7-178 S4X400H – reroute – error message



The reroute function with manual routing (Fully Specified Route) supports also Trails, Link connections or a mix of Trails and Link Connections as constraints.

You can access connections from NFM-T in several ways. Some of the key workflows are:

- Infrastructure connections, including infrastructures (trails) and logical links
- Service connections
- Client and server connections of a selected infrastructure connection
- Server connections of a selected service
- Impacted connections of a selected service or infrastructure connection
 - Impacted connections are those infrastructure and service connections that are associated with a selected node and its current operational and alarm state.
- Used ports of a selected service or infrastructure connection
 - Used ports are those infrastructure and service connections that are assigned to a port address on a selected node.

Modify Route task is available from all of these entry points if it is applicable.

Depending on the existing Deploy State and Deploy Status of the connection, the routing modifications that can be made can include, but are not limited to, actions that are listed in the following table. Actions that are not available for the connection that you select are either greyed-out or not displayed on the list.

In the *Modify Parameters* screen, the **Connection Name** and **Connection Alias** fields are disabled and cannot be modified, to modify these fields use the task [7.64 “Rename Connection and Customer Name” \(p. 997\)](#). A tooltip is displayed that suggests the use of the **Rename Connection** function.

Table 7-13 Modify connections for Infrastructure Connections and Services

Modify connections	
You can modify the route of and manage the protection for an infrastructure connection or a service.	
Option	Explanation
Modify Route	<p>When modifying a route, some part of the route must be common between the old and new routes.</p> <ul style="list-style-type: none"> • Reroute deletes the connection using a route that needs to be released, and recreates the connection using the new route. • Reinstate is used to rollback a Reroute with a reinstate order to its original route. Reinstate is available for a commissioned reroute with a reinstate order. With a Reinstate of the original route, traffic disruption might occur. • Reroute with Reinstate deletes the connection using a route that needs to be released, and recreates the connection using the new route, but stores the layout of the older connection so it can be rolled back using a Reinstate. During the Reinstate, the original (older) route might cause traffic disruptions. The older route is purged and the saved time slots are released. • For Control Plane connections, <i>AsonRouted</i> selected, <i>AutoServerCreation</i> selected, the <i>Regenerator ports</i> are displayed in the Routing Constraints panel when you create or modify the route of a ODUk connection. For Managed Plane Connection, <i>AsonRoute</i> not selected, the <i>Regenerator ports</i> are displayed, but not modifiable during modify of a ODUk connection.
Soft *	A Soft is a non-traffic affecting reinstatement of the connection. Soft is executed as a best effort by the system.
Hard *	A Hard is a traffic affecting Reinstate . This is the default reinstatement.

*The system enables you to select whether a request to **Modify Route** is a **Soft** or a **Hard** rearrange. The system makes a best effort to comply with your preferences; that is, the system performs a **Soft Rearrange** if the impacted connection supports that capability. If the impacted connection does not support the capability, the system throws an error. Cancel the connection and change the Rearrange type to **Hard**.

Important! Use separate **Modify Connection > Reroute...** and **Modify Parameters > Parameters...** requests if the modification of the connection route and the connection parameters are needed.

Example: If a connection needs to be rerouted and the parameters of this connection need to be changed, then complete the following two steps:

1. Click on the **More :** icon on the connection, select **Modify Connection > Reroute...**, make changes in the connection route, and then **Deploy** the change.

-
2. Click on the **More**  icon on the connection, select **Modify Parameters > Parameters...**, make then necessary changes in the parameters, and then **Deploy** the change.

This task also provides the navigation paths where you can modify the route of the clients and servers of an infrastructure connection or the servers of a service from the **OPERATE > Infrastructure Connection** or **OPERATE > Services** navigation path. Depending on the connection, the data table that is displayed with the **Clients** or **Servers** tabbed topic provides the same actions and functions as the displayed data table that is displayed for an **Infrastructure Connections** or a **Services**.

Reroute of protected service

When the user does an integrated reroute of the protected service (DSR layer) by changing only few timeslots only on either MAIN or SPARE leg, then the reroute operation fails.

Reroute is allowed with following requisites:

- Changing all the timeslots in both MAIN and SPARE
- Changing all the timeslots in either MAIN or SPARE leg

Modify function - not supported

What is not supported in the Modify Route function is summarized for better convenience:

- The ability to swap the working and protection roles.
- 3R as constraints are not supported. The user cannot change the E2E ODUk through the 3Rs.
- Frequency constraint is not supported. The user cannot type in or change the frequency as a single entry in the input form. However, the user can select a Link Connection on an egressing OMS and use that as a constraint.
- Modulation, Phase Encoding and waveshape cannot be modified via reroute.
- Switching of protected connection roles from service to protection and vice versa is not allowed
- No warning is reported in order summary if rerouted connection uses any of the links of the original connection.

Modify Route flow

When you select the **Modify Route** menu item of a OTUk trail or ODUj trail, following actions can be done.

- The default routing mode when modifying a route is **Auto**, the system can reroute the connection automatically and constraints can be added to redirect the route to the desired path through the network.

In Auto Mode, the user can in addition

- Change the protection type
- Remove some of the Link connections of the original route.

Removed link connections will be available for routing and system finds the shortest path if no constraints are specified.

- Exclude some of the Link connections of the original route.

The list below will be not used in the rerouted connection.

- Selecting **Manual** option implies that all link connections, channels or time slots, must be defined in the constraint table.
- If you want to add protection using the reroute screen with Auto Mode, change the protection type to protected
- If you want to remove protection using the reroute screen with Auto Mode, change the protection type to unprotected and remove the protected leg constraints from Routing constraints panel.
- If you exclude the existing link connections, selecting one or more of the link connections in the right hand Routing Constraint panel and selecting exclude action, then the servers (trail/ infrastructure connections of the link connection) are excluded from the new route.
- Retain some of the Link connections of the original connection as Include
- Add additional include and exclude node, trail, Physical link constraints.

The System tries to find the route using the constraints provided.

Access to the modify the Route (Reroute) of a connection

To access the Modify Connection follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Protected Connections

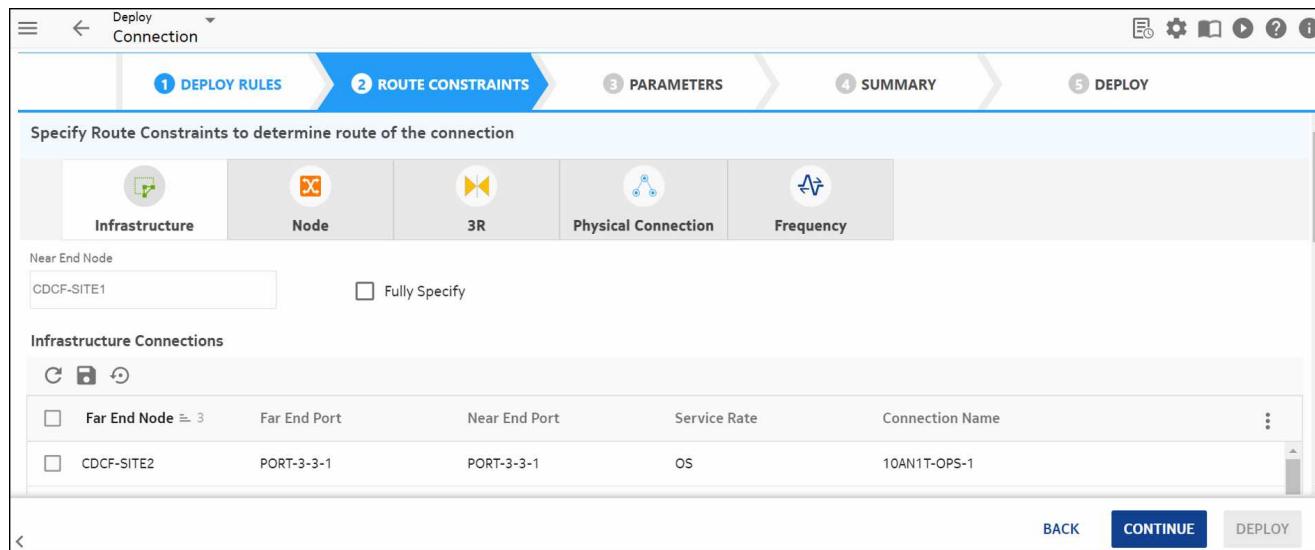
OPERATE > Services

The access to **Modify Connection** depends on the type of connection selected and the existing Deploy State and Deploy Status of the connection. If the **Modify Connection** item is enabled click on the **More**  icon on a connection, follow the path **Modify Connection**, and select **Reroute**.

Note:

The system displays the list of link connection, channels or time slots, used in the original connection in the **ROUTE CONSTRAINTS** tab, see [Figure 7-179, "Connections - Modify Connection - Reroute - Routing Constraints tab" \(p. 992\)](#).

Figure 7-179 Connections - Modify Connection - Reroute - Routing Constraints tab



Service definition

Modification on the **Service Definition** panel are optional and conditional, they depend on the connection selected.

Optional & Conditional:

In the **Service Definition** panel:

- for Cards in 200G Mode (D5X500*, 2UC400,), the Modulation can be modified.
- for Cards in 100G Mode (4UC400) and ODU4s with **Auto Server Creation** enabled, the Modulation can be modified.

For details, refer to [“Transmission Mode” \(p. 701\)](#).

Optional & Conditional: In the **Service Definition** panel, if the connection rate is OTU4x2 or OTU4 and at least one connection endpoint is on a D5X500 card or if the connection rate is ODU4, **Auto Server Creation** is selected, and at least one connection endpoint is on a D5X500 pack, modify the **Phase Encoding** of the **Implemented** connection.

Optional & Conditional: In the **Service Definition** panel, if the connection rate is OTU4x2 or OTU4 and at least one connection endpoint is on a D5X500 card or if the connection rate is ODU4, **Auto Server Creation** is selected, and at least one connection endpoint is on a D5X500 pack, modify the **Phase Encoding** of the **Implemented** connection.

Route constraints

In the **ROUTE CONSTRAINTS** tab, the path that the connection takes through the network can be changed by removing link connections from the routing constraint panel, and by adding new constraints.

In **Auto Routing**, trail, link, Node and Physical link can be added as constraints. In **Manual Routing**, you are allowed to select trail and link connections to be added as constraints.

The constraint role can be changed from *Include* to *Exclude* and vice versa for the constraints that are added. To change the constraint role use the icons,  for *Include* and  for *Exclude*.

The role can be changed from Protection to Service and vice versa for the constraints that are added. To change the role use the icons,  for changing the role to Service and  for change the role to Protection.

The icon  can be used to remove all constraints in one shot.

If the ASON Routed check box has not been selected, in the **Rearrange** field of the **ROUTE CONSTRAINTS** panel, select **Soft** or **Hard**.

If no connection endpoints are changed on the Service Definition panel, the default is **Soft**. If one or more connection endpoints are changed on the Service Definition panel, the default is **Hard**. If the connection rate is OTUk or if the connection category is a terminated ASON MRN tunnel, the default and only option is **Hard**.

Important considerations!

- When rearranging a connection, some part of the route must be common between the old and the new routes. If no part of the route is common, you should create a new connection and delete the old connection. The system makes a best effort to comply with your preferences; that is, the system performs a **Soft** rearrange if the impacted connection supports the capability. If the impacted connection does not support the capability, the system performs a **Hard** rearrange. A **Soft** reinstate is a non-traffic affecting reinstatement of the connection. A **Hard** reinstate is a traffic affecting **Reinstate**.
- **Reroute** fails for a **Soft** rearrange if the **Order Sensitive** parameter is checked.
- If one or more original end ports change (for example, the end port name is changed), the rearrange is always **Hard**. Manually select the **Hard** rearrange for the rearrange to be successful.
- During a **Rearrange**, the system can automatically create and delete an edge HO trail. When you rearrange an ODUK service connection and change an endpoint, if the new endpoint is a channelized endpoint and if it is the first client of an edge HO trail, the system automatically creates the edge HO trail connection. When you rearrange an ODUK service connection and change an endpoint, if the removed endpoint is a channelized port and if it is the last client of an edge HO trail, the system automatically deletes the edge HO trail connection.
- If you select the **Soft** rearrange and the end points of a trail are on a cross-connect switch that supports setting up of SNCP, NFM-T creates SNCP protections. Examples are 20P200 circuit packs in a 24X shelf. A **Soft** rearrange is supported to Add Protection to an unprotected ODUK connection. A **Soft** rearrange is also supported to Remove Protection from a protected ODUK connection. The working leg of the protected cross connection must be retained in the unprotected cross connection. If the protection leg is to remain, then a **Hard** rearrange must be performed.
- For the 112SDX11 circuit pack, **Rearrange** is supported for the OTL4.4 connections, but not for the OTU4 connection. End point change and frequency change are not supported for **Rearrange** of OTL4.4 connections. In addition, you cannot do a **Modify Route** for a connection that has one or more endpoints on a 112SDX11 circuit pack in OTL4.4 mode. These requests must be performed on each individual OTL4.4 connection.

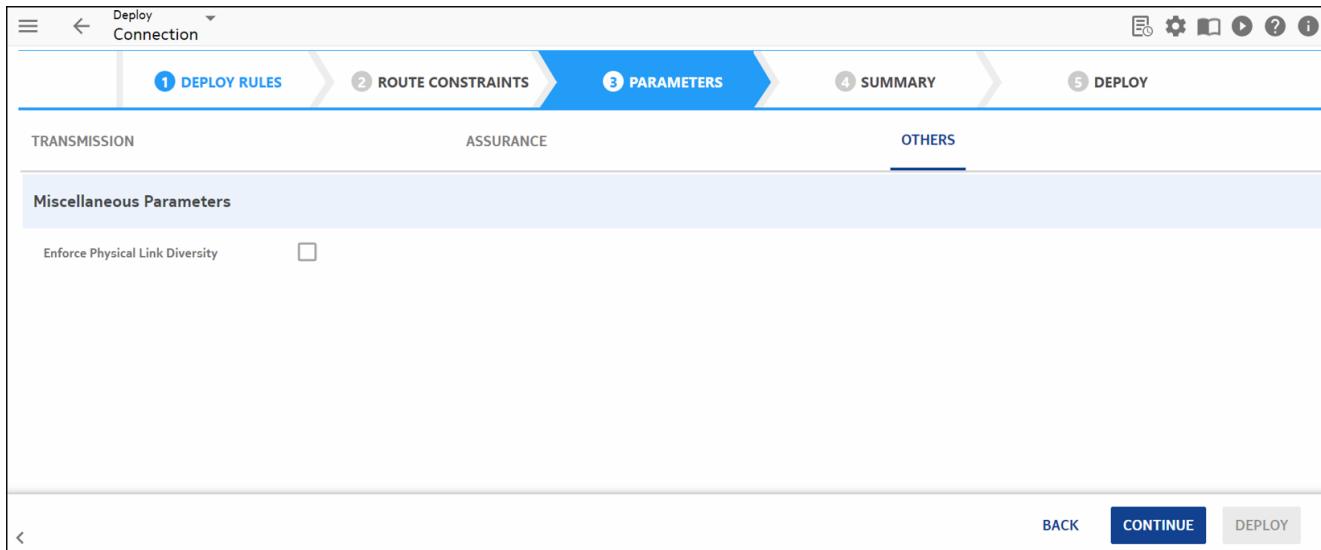
- For a **Rearrange**, the following fields are read only: Rate/Service Rate, ASON Routed, Container, Transmission Mode, Phase Encoding.
- You can only change manual Wave Keys when a **Rearrange** of the connection changes the frequency of the connection. Therefore, for all other instances, use the [7.62 “Modify the parameters of a connection” \(p. 981\)](#) task to change the manual Wave Keys.
- *Optional & Conditional:* For a **Rearrange**, if one or more end points are changed, in the **Service Definition** panel, modify the FEC and, if applicable, any substrate Ethernet fields (the CIR Rate, CBS, EIR, EBS, CE VLAN, S VLAN).
- Because rekeying is not supported during a **Rearrange**, use the [7.62 “Modify the parameters of a connection” \(p. 981\)](#) task to rekey a connection. For a **Rearrange** without frequency change, if you want to rearrange the connection without allowing duplicate wave keys for the frequency, first rearrange the connection and then use the [7.62 “Modify the parameters of a connection” \(p. 981\)](#) task to rekey the connection. For a **Rearrange** without frequency change, if you want to rearrange the connection and allow duplicate wave keys for the frequency, first use the [7.62 “Modify the parameters of a connection” \(p. 981\)](#) task to rekey the connection with duplicates, then **Rearrange** the connection. For a **Rearrange** with frequency change, the wave keys must change since the frequency is changing. When you rearrange the connection, if you want to allow duplicate wave keys for the frequency, choose **Duplicates Allowed** for the AZ Wave Keying Preference and/or ZA Wave Keying Preference.
- **Reroute** is not available for Y-cable protected services, Y-cable OPSB protected services, and OMS connections with OPSB protection. **Reroute** is available for these connections only if they are in the **Defined** state. **Reroute** is not available for edge HO trails and ASON edge HO trails.
- For a channelized service, if the end-points of the last ODUj is changed, the previous parent ODUk trail leaving the domain (Edge HO Trail) is auto-deleted as that is the last client.

If you unchecked the **System Assigned Frequency** field, you can check or uncheck the **CWDM** field. If you checked the **CWDM** field, in the **Wave Length** field, use the drop-down numbered list to specify a CWDM wave length (default 1471).

- For a service connection having more than two nodes and trails, if an OTS link has to be reused between two nodes having unique infrastructure trails, disable the **Enforce Physical Link Diversity** parameter under **PARAMETERS** in **Service Definition** page.

Enforce Physical Link Diversity parameter is disabled only on auto routed ODU trail connection.

Figure 7-180 Enforce Physical Link Diversity



If you want to change the protection role of a routing constraint that is assigned to a routing constraint that appears in the data table, select the routing constraint in the data table and mouse over and select **Change Role to Service** or **Change Role to Protection**.

Using Modify Connection - Reroute to add protection

For protected connections that are physically diverse in segments but not end-to-end, removing protection and adding protection back may not always work.

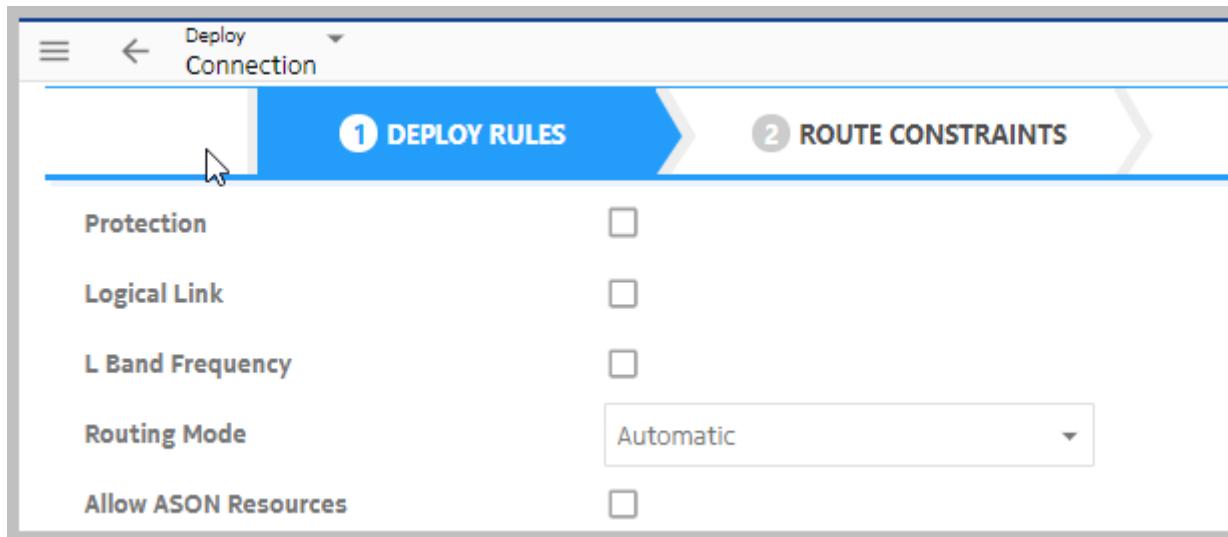
For Add protection to work for segment-protected scenarios, **Enforce Physical Link Diversity** must have been set to false during connection creation.

Add protection for segment-protected scenarios fail, because of insufficient diversity between working and protection paths, if **Enforce Physical Link Diversity** was set to true or is true by default.

To add protection to these segment-protected scenarios, use the modify reroute operation and change protection type to protected (with or without constraints).

Connection Controls

In Deploy tab, select **New Service/Infrastructure Connection**, select Continue at the right bottom corner. Under Deploy rules, navigate to Connection characteristics. The Routing modes has drop down field displays the two values Automatic and Manual. The default value is **Automatic**.



If you select **Automatic** in the Routing field, this implies that the Auto Routing is applied to find the rerouted connection. You can change the route of existing switched connection to new route providing partial constraints with Routing Mode as Automatic. Constraint can be Trail or Link Connection, Node and Physical link.

If you select **Manual** in the Routing field, this implies that you must define all link connections for the rerouted connection.

ASON Routed

Optional & Conditional: If the **ASON Routed** selected, the **ASON** panel is activated.

For a DSR connection, the **ASON** panel is activated only if the TCM Level or Sub-Network Protection Type parameter has been specified in the original connection. All other fields on the ASON panel are read only and are the current values for the ODUk server of the DSR.

Assurance

No fields are editable. Use **Modify PM** menu to modify the PM attributes.

Apply the route modification

To apply and run the route modification done, click the **Deploy** or **Save as Template** buttons.

If you save the template, you can keep this route as a template for other implementations.

7.64 Rename Connection and Customer Name

Purpose

Use this task to rename a Connection, a Service or Infrastructure. This task results in modification of the user label of associated ASON SNCs.

Important notes:

1. The Rename Connection doesn't support integrated provisioning. if a DSR path is renamed, the ODUj doesn't get renamed and also the corresponding ASON SNC.
2. The Rename Connection applies only to NFM-T, the old name persists in GMRE

Task

Complete the following steps to rename a connection.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

OPERATE > Nodes > Used Ports (tab)

OPERATE > Nodes > Service Connections (tab)

OPERATE > Nodes > Infrastructure Connections (tab)

OPERATE > Nodes > Impacted Connection (tab)

OPERATE > Protected Connections

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

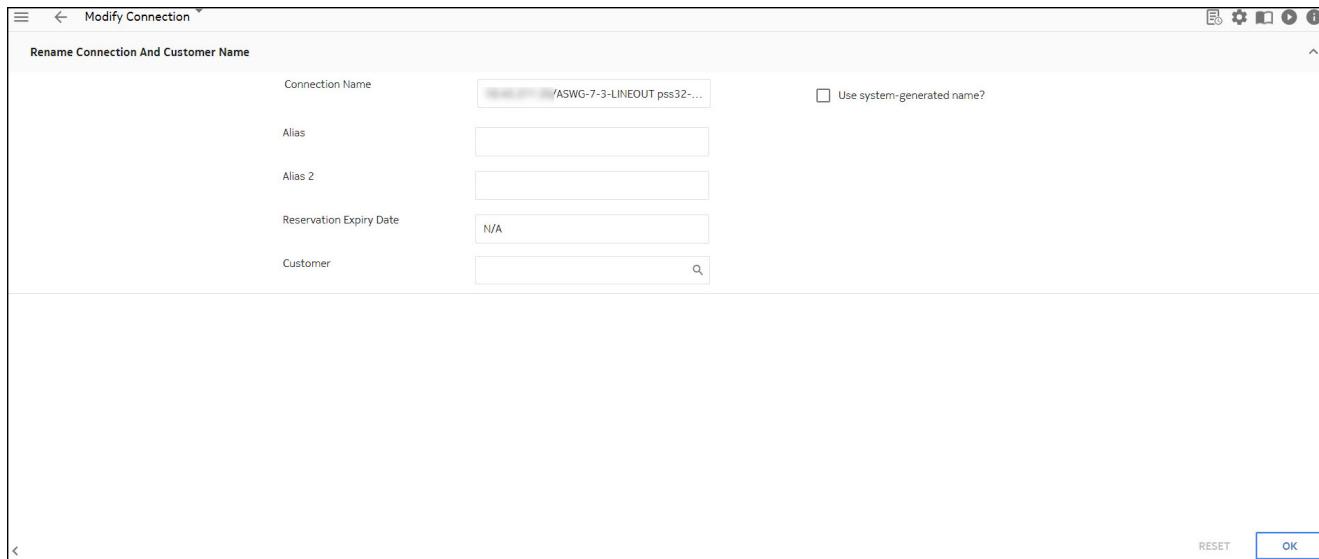
2

Click on the **More**  icon on the connection that you want to rename and follow this path:

Modify Connection > Connection and Customer Name...

Result: The system displays the Rename Connection And Customer Name window.

Figure 7-181 Rename Connection And Customer Name window



3

If required edit the **Connection Name** with a customized name. To use the system generated name check the field **Use system-generated name?**



Note:

- The port based option is used to determine the Connection Name. See [2.26 "Connection names and aliases" \(p. 260\)](#) for more details.
- When **Use system-generated name?** option is selected, service Rate is included as part of the connection name.

Effective rate displayed on the service list is the effective bandwidth used by that connection on a Flexgrid network, so the effective Rate displayed on the service list (for example, FlexClientRate/1.25GbE) may be different from the name that gets generated as connection name, (nodename1)/(portname1) (nodename2)/(portname2) (rate).

For example, MTNM_DT-PSD-009_Ser12/DSR-1-1-CLIENT1 MTNM_DT-PSD-10/DSR-1-1-CLIENT1 *FlexClientRate*.

4

Optional. In the **Alias** and **Alias2** field insert alias for the connection.

5

Optional: Enter appropriate date for **Reservation Expiry Date** field.

6

Optional. In the **Customer** field select a name from the list clicking on the search icon to display the customer name list.

7

Click **OK** to confirm the changes.



Note: If you leave the **Connection Name** blank the port based option is used to determine the Connection Name. See [2.26 “Connection names and aliases” \(p. 260\)](#) for more details.

Result: The system renames the connection. A success message is displayed.

END OF STEPS

7.65 Manage the inventory view of Infrastructure Connections

When to use

Use this task to view a list of infrastructure connections.

Task

Complete the following steps to view a list of infrastructure connections:

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

Result: The system displays a data table that lists all of the infrastructure connections.

Figure 7-182 Connections- Infrastructure Connections

Connecti...	Rate	Name	Protection	From Node #1	From Port #1	To Node #1	To Port #1	All...
Commissioned	OTSig Tu...	OTSIG_PSS6_PSS7_Direct_Profile2_S4X400H_Tu...	Unprotected	SANITY_CDCF_AD...	OTSIG-5-7-1	SANITY_CDCF_AD...	OTSIG-5-7-1	
Commissioned	OTSig Tu...	OTSIG_PSS6_PSS7_Direct_Profile2_S4X400H_Tu...	Unprotected	SANITY_CDCF_AD...	OTSIG-5-8-1	SANITY_CDCF_AD...	OTSIG-5-8-1	
Commissioned	OTSig Tu...	OTSIG_PSS6_PSS7_Direct_Profile3_S4X400H_Tu...	Unprotected	SANITY_CDCF_AD...	OTSIG-5-9-1	SANITY_CDCF_AD...	OTSIG-5-9-1	
Commissioned	OTSig Tu...	OTSIG_PSS6_PSS7_Direct_Profile4_S4X400H_Tu...	Unprotected	SANITY_CDCF_AD...	OTSIG-5-11-1	SANITY_CDCF_AD...	OTSIG-5-11-1	
Commissioned	OTSig Tu...	PSS32 PORT-2-3-1 PSS32-45.212...	Unprotected	PSS32	OTSIG-2-3-1	PSS32	OTSIG-2-3-1	
Commissioned	OMS	R214_CDCF_03/ASWG-1-15-LINEOUT R214_CDCF...	Unprotected	R214_CDCF_03	ASWG-1-15-LINEOUT	R214_CDCF_09	RA2P-1-2-LINEIN	
Commissioned	OMS	R214_CDCF_03/ASWG-1-3-LINEOUT R214_CDCF...	Unprotected	R214_CDCF_03	ASWG-1-3-LINEOUT	R214_CDCF_07	RA2P-1-2-LINEIN	
Commissioned	OMS	R214_CDCF_07/ASWG-1-15-LINEOUT R214_CDCF...	Unprotected	R214_CDCF_07	ASWG-1-15-LINEOUT	R214_CDCF_09	RA2P-1-9-LINEIN	
Commissioned	OMS	SANITY_CDCF_ADD4_PSS_NODE_1/ASWG-1-15-...	Unprotected	SANITY_CDCF_AD...	ASWG-1-15-LINEOUT	SANITY_CDCF_AD...	RA2P-1-2-LINEIN	
Commissioned	OMS	SANITY_CDCF_ADD4_PSS_NODE_1/ASWG-1-3-LI...	Unprotected	SANITY_CDCF_AD...	ASWG-1-3-LINEOUT	SANITY_CDCF_AD...	RA2P-1-2-LINEIN	
Commissioned	OMS	SANITY_CDCF_ADD4_PSS_NODE_1/ASWG-2-3-LI...	Unprotected	SANITY_CDCF_AD...	ASWG-2-3-LINEOUT	SANITY_CDCF_AD...	RA2P-1-2-LINEIN	
Commissioned	OMS	SANITY_CDCF_ADD4_PSS_NODE_2/ASWG-1-15-...	Unprotected	SANITY_CDCF_AD...	ASWG-1-15-LINEOUT	SANITY_CDCF_AD...	RA2P-1-6-LINEIN	

2

From the **Select View** panel, select one of the following options to change the view.

View types	Sub types
------------	-----------