OPERATIONAL STATE	• ALL • UP • DOWN • DEGRADED
ALARM STATUS	• ALL • CRITICAL • MAJOR • MINOR • WARNING • CLEARED
EFFECTIVE RATE	• ALL • ODUK • OMS • OCH • STM-N • OC-N • OTU-K • OMSBAND
IMPLEMENTATION STATUS	• ALL • N/A • IN PROGRESS • COMPLETED • FAILED
PROTECTION TYPE	• ALL • UNPROTECTED • PROTECTED • Y CABLE • SNC • OTHER
OLC STATE	• ALL • MAINTENANCE • IN SERVICE

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

IMPLEMENTATION STATUS	• ALL • DEFINED • ALLOCATED • FULLY ALLOCATED • IMPLEMENTED • COMMISIONED
CONNECTION TYPE	• ALL • BROADCAST (INFRA) • INFRASTRUCTURE • LOGICAL LINK • TANDEM
SERVICE STATE	• ALL • IN SERVICE • OUT OF SERVICE • MAINTENANCE • AUTOMATIC IN SERVICE

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: For additional navigation options for 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 or if you want to reset a customized view of the data table to its default

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

display, refer to the26.9 “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 7.66 “Manage Columns on Infrastructure Connections page” (p. 1004) for more details.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.66 Manage Columns on Infrastructure Connections page

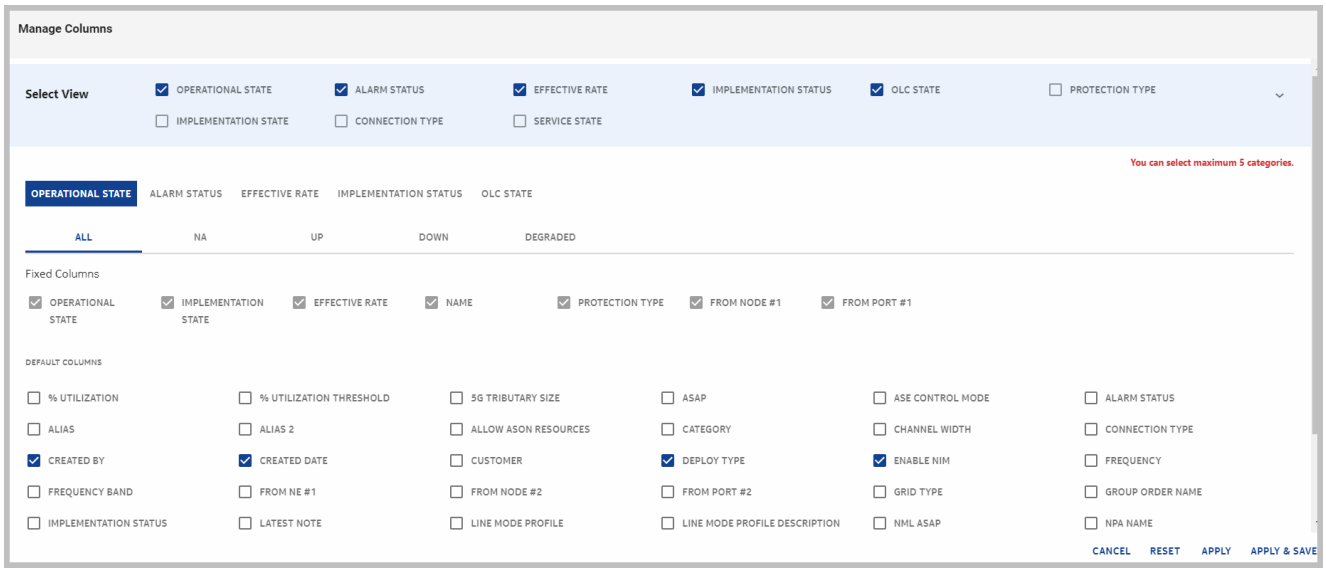
Task

1

Click **MANAGE COLUMNS** icon on top right corner on **Infrastructure Connections** page.

Result: The system displays **Manage Columns** page.

Figure 7-183 Infrastructure Connections- Manage Columns



2

The user can choose a maximum of five view types in the**Select View** panel.

Result: The systems displays the chosen 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 **Fixed Columns**. The system displays optional columns under sub type tab.

4

Click one of view sub type tab. Choose optional columns that appear on the data table along with the fixed columns. See 7.79 “Infrastructure Connections columns” (p. 1054) for more details on the attributes.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

Click **APPLY & SAVE** to save the changes and apply the modifications on data table in physical connections page. Alternatively, click **RESET** to reset 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

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.67 Manage the inventory view of Services

When to use

Use this task to view a list of services.

Task

Complete the following steps to view a list of services:

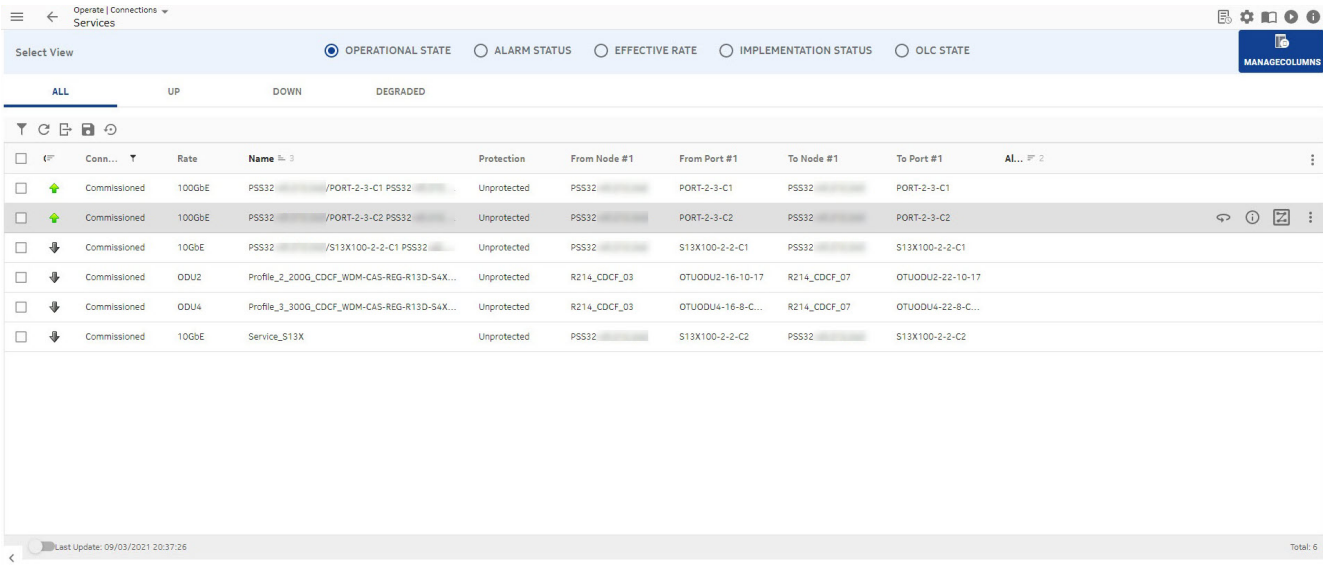
1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Services

Result: The system displays a data table that lists all of the services.

Figure 7-184 Connections – Services



2

From the **Select View** panel, select one of the following options to change the view.

View types	Sub types

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

OPERATIONAL STATE	• ALL • UP • DOWN • DEGRADED
ALARM STATUS	• ALL • CRITICAL • MAJOR • MINOR • WARNING • CLEARED
EFFECTIVE RATE	• ALL • ODU4 • ODU3E2 • ODU3 • ODU2 • ODU2E • ODU1 • ODU0 • ODUF • OCH • 100GBE • 40GBE • 10GBE • 1GBE • FE • STM-256 • STM-64 • STM-16 • STM-1 • OC-768 • OC-192 • OC-48 • OC-12 • OC-3

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

IMPLEMENTATION STATE	• ALL • N/A • IN PROGRESS • COMPLETED • FAILED
OLC STATE	• ALL • MAINTENANCE • IN SERVICE
PROTECTION TYPE	• ALL • N/A • UNPROTECTED • PROTECTED • Y CABLE • OCHP

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: For additional navigation options for 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: To customize the filters, sorting, column order in a data table, and to save the same 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8

Optional: Click **MANAGE COLUMNS** on top right corner to manage the columns in data table. See 7.68 "Manage data columns on Services page" (p. 1010) for more details.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.68 Manage data columns on Services page

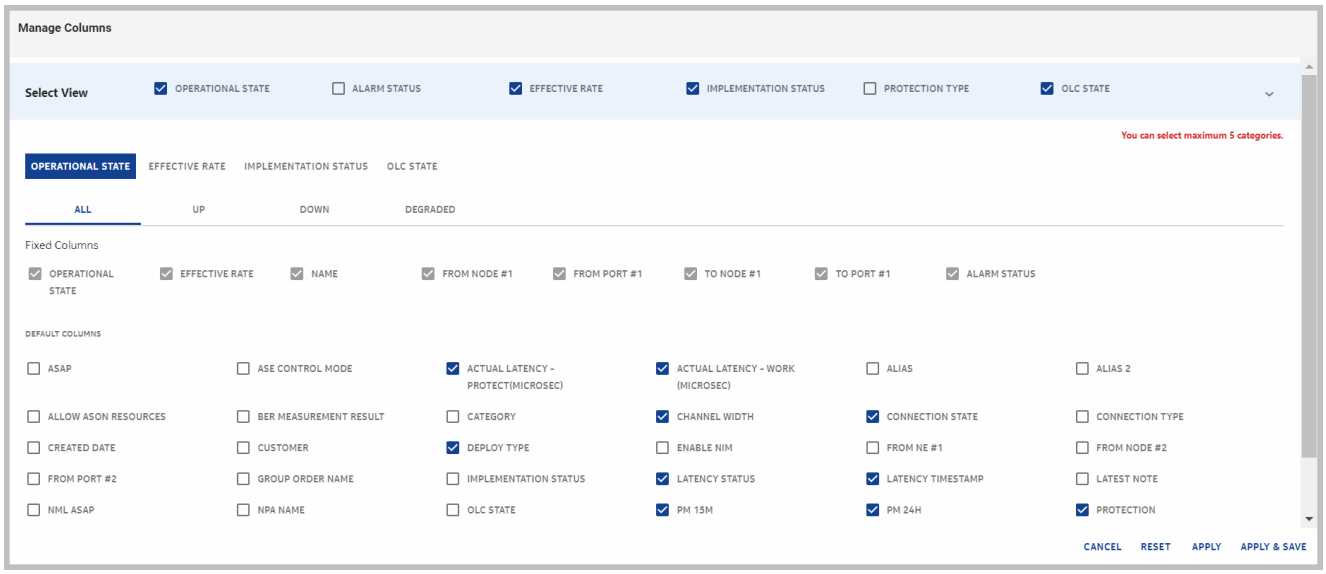
Task

1

Click **MANAGE COLUMNS** on top right corner on **Services** page.

Result: The system displays **Manage Column** page.

Figure 7-185 Services- Manage Columns



2

The user can select a maximum of five view types in **Select View** panel.

Result: The systems displays the chosen 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 **Fixed Columns**. 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 7.80 “Services columns” (p. 1059) for more details on the attributes

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

Click **APPLY & SAVE** to save the changes and apply the modifications on data table in physical connections page. Alternatively, click **RESET** to reset 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

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.69 Set transmission parameters

Create or modify Connection - set transmission parameters

When creating or modifying a connection, setting transmission parameters is best effort.

This means that the order succeeds even if the transmission parameters are not successfully provisioned on the network element. When the transmission parameters are not successfully provisioned on the network element a transmission parameter discrepancy is reported.

For most cases, if even one transmission parameter has an invalid value selected none of the transmission parameters are set on the network element, also valid transmission parameters are not set on the network element.

The user must perform a modify parameters to correct the transmission parameter discrepancy.

Create or modify connection - set transmission parameters - D5X500

For D5X500 OTU4 transmission parameter Trail Trace are not supported from NFM-T for any configuration of D5X500 which is having interworking cases.

For the D5X500 packs, TTI is not settable for the OTU4 for the interworking case, it is settable for the ODU4. Other transmission parameters are settable, not the Trail Trace ones.

For example on D5X500 packs, the user must modify OTU parameter from ODU4 connection under 100GbE. In case of interworking of D5X500 with 2UX200, to set OTU parameters on 2UX it must be modified from OTU connection and for D5X500 it has to be modified from ODU4 trail under 100GbE.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.70 View Failure Analysis for an infrastructure connection or service

When to use

Use this task to view the Failure Analysis window for an infrastructure connection or service from the data table of an infrastructure connection or service.

Related information

The Failure Analysis window provides users with a detailed understanding of the failure that occurred during the routing phases of provisioning, along with information on how to correct the failure.

The Failure Analysis window consists of the following items:

- The name of the attempted connection.

  Example:

  Failure Analysis: MP-132-SITE1/ODU4ODU0-16-3-L1-CH1-1 MP-132-SITE5/ODU4ODU0-16-3-L1-CH1-1 ODU0
- A graphic representation of the attempted connection which minimally includes the from/to nodes.

  The graphic representation illustrates what the routing algorithm has discovered as possible routes through the network up to the point of the failure. If the failure occurs before the routing algorithm can make it through the network, the **From Node** and **To Node** are displayed with a cloud in the middle, which indicates the network. If the routing algorithm has partially made it through the network and has located several partial routes, then the partial routes are displayed. Since most connection requests specify **Auto Server Creation**, both the requested connection and the server routes are displayed.
- Icons to the right of the graphic representation, which users can click on to **Zoom In**, **Zoom Out**, **Reset Position and Zoom Level**, **Toggle Node Labels On/Off**, and **Toggle Link Labels On/Off**.
- An explanation of the **Cause of Failure**, which is located at the higher bottom panel.

  Example:

  Cause of Failure: System cannot allocate photonic channel for trail MP-SITE4/A2325A-1-2-LINE MP-SITE5/A2325A-1-6-LINE OMS and frequency.
- An explanation of the **Correction Action**, which is located at the lower bottom panel.

  Example:

  Correction Action: Please free up a channel with frequency on intermediate trails.

Before you begin

The Failure Analysis window is only available for infrastructure connections or services that are in the **Defined** state and that have an Implementation Status of **Failed**.

You can also access the Failure Analysis window from **Show Failure Analysis** button on the **Progress Bar** when you are creating a connection that has failed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task

Complete the following steps to view the Failure Analysis window for an infrastructure connection or service.

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 infrastructure connections or services.

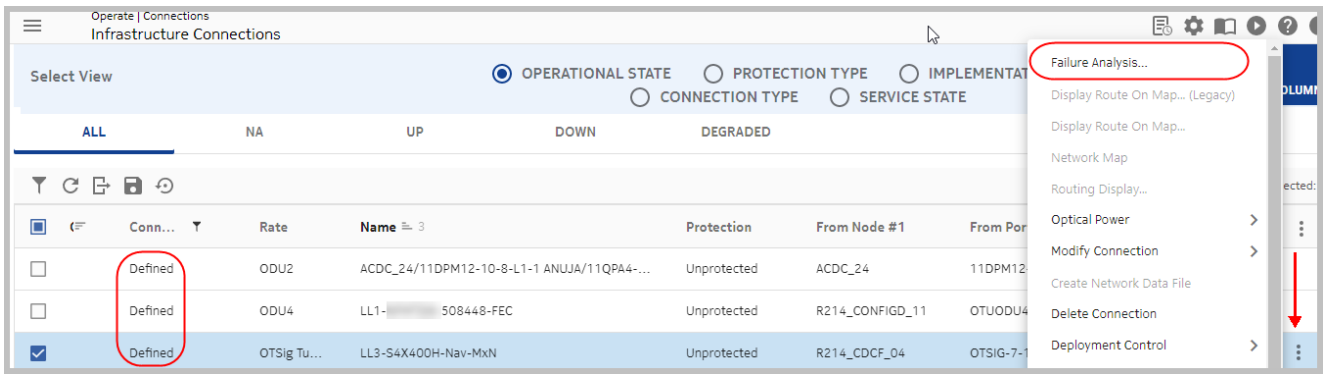
2

Select Defined option from Connection status tab and Click on the **More** icon on the right, **Failed** connection for which you want to view the Failure Analysis and follow this path: **Failure Analysis**.

Example:

The following figure illustrates a **Defined** connection and the location of the **Failure Analysis** option.

Figure 7-186 Connections – Defined infrastructure connection – navigation path to Failure Analysis



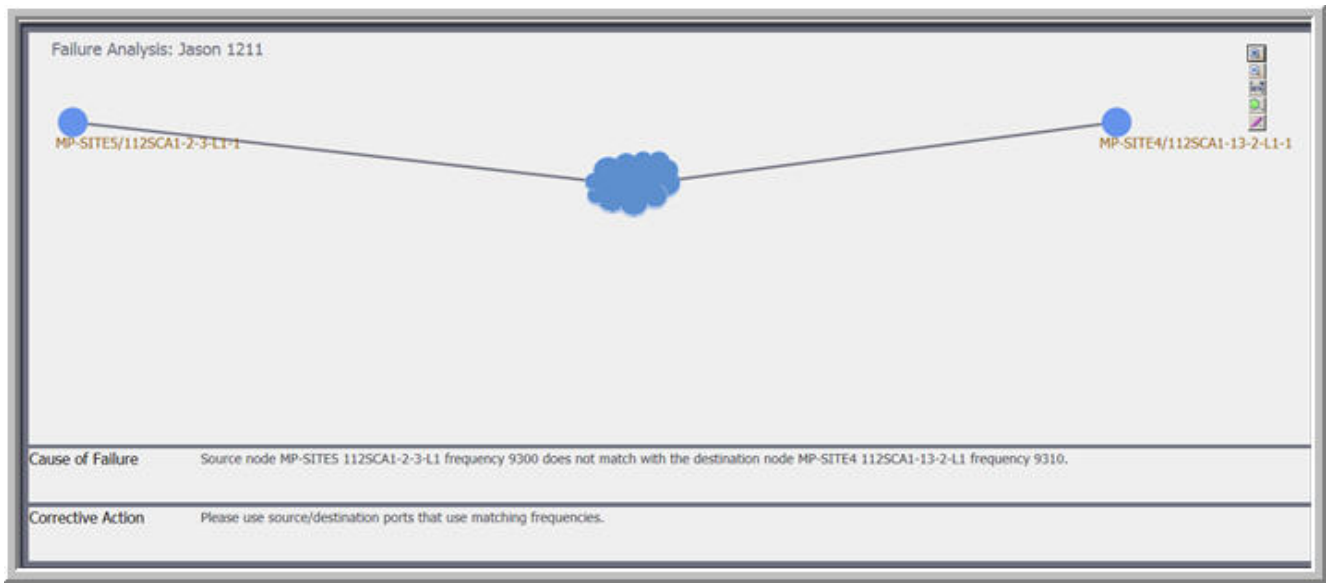
Result: The system opens a new tab and displays the Failure Analysis window for the connection that you selected.

Example:

The following figure illustrates the Failure Analysis window for a **Defined** and **Failed** infrastructure connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

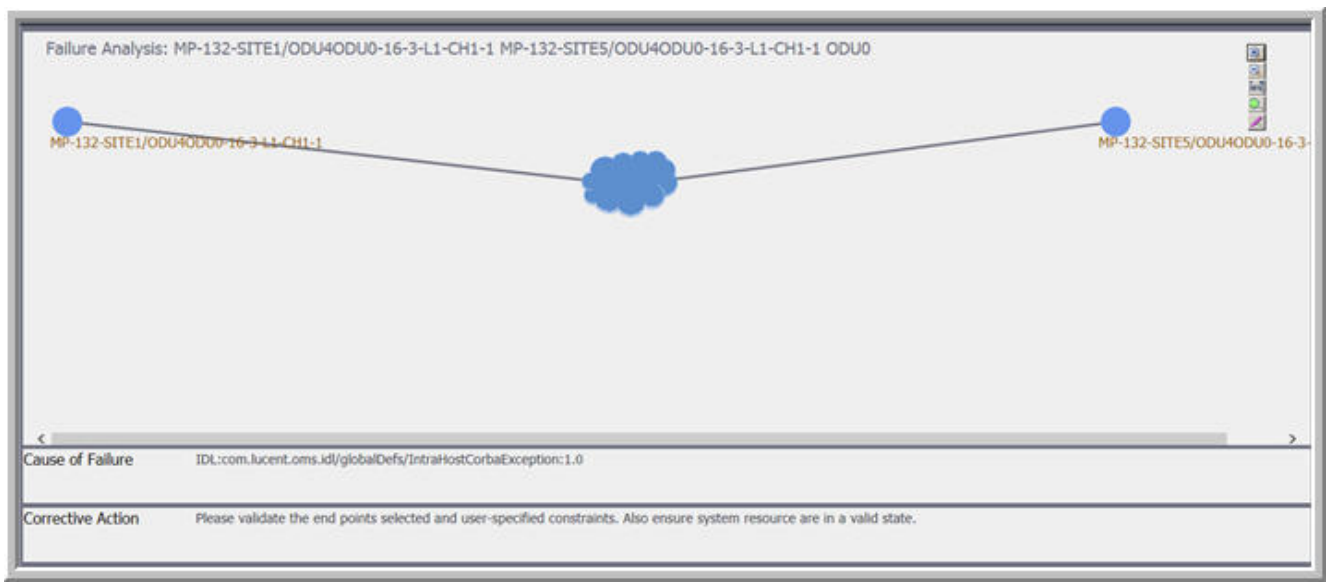
Figure 7-187 Connections – Failure Analysis window – infrastructure connection



Example:

The following figure illustrates the Failure Analysis window for a **Defined** and **Failed** service.

Figure 7-188 Connections – Failure Analysis window – service



END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.71 View Jobs for an infrastructure connection or service

When to use

Use this task to view the jobs for an infrastructure connection or a service.

Before you begin

You can view the jobs 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.

In addition, the system provides a Jobs list for SNC mismatches and Parameter mismatches. Refer to "Task: View the Job List for an SNC Mismatch" (p. 1183) and "Task: View the Job List for an Parameter Mismatch" (p. 1176) for detailed steps. You can also view an inclusive Jobs list from the **ADMINISTER > Jobs** navigation path.

An Important usability note! The system defaults to a display of 15 rows of objects in a data table. Typically, the Services data contains more rows of objects than other data tables. The numerical values that are displayed in the "Total Objects icon" (p. 2276) provides you with the number of rows of objects that are available for viewing. If the "Total Objects icon" (p. 2276) is overlaid with the "Total Objects - Snippet Icon" (p. 2276), you can use the **Remote Filter** to filter the data columns in order to reduce the rows of objects that are displayed in the data table. Refer to 26.4 "Data Table Filtering Icons" (p. 2203) for direction. In addition, to make viewing easier, you can also page through the rows of objects.

Task

Complete the following steps to view the Jobs for an infrastructure connection or a service.

1

Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Infrastructure Connections > 360° View > Clients (tab)

OPERATE > Infrastructure Connections > 360° View > PM Eanbled Points (tab)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

OPERATE > Infrastructure Connections > 360° View > Servers (tab)

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

OPERATE > Protected Connections

OPERATE > Services

OPERATE > Services > 360° View > PM Eanbled Points (tab)

OPERATE > Services > 360° View > Servers (tab)

Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

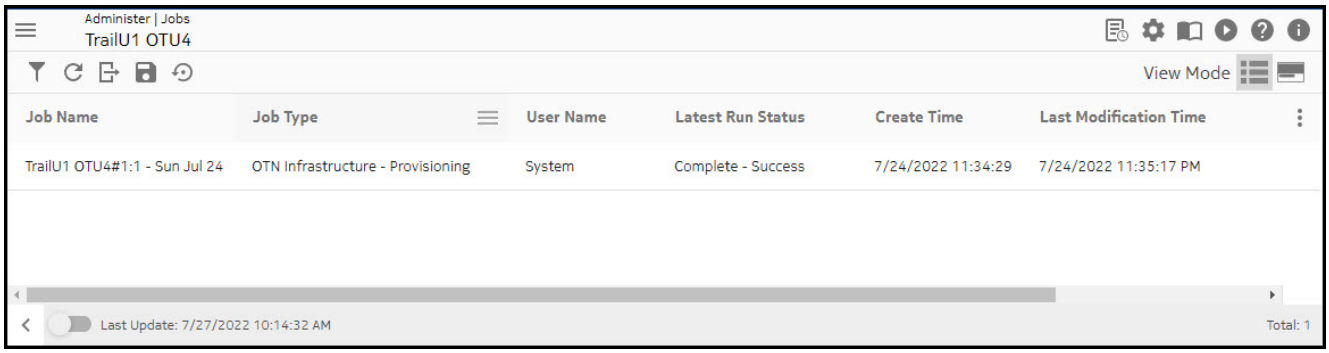
2

Highlight and select the infrastructure connection or service for which you want to view its Jobs and click on the **More** icon on the right of the selected connection row and follow this path: **Jobs**.

Result: The system opens a new browser tab and displays the Jobs window for the selected infrastructure connection or service.

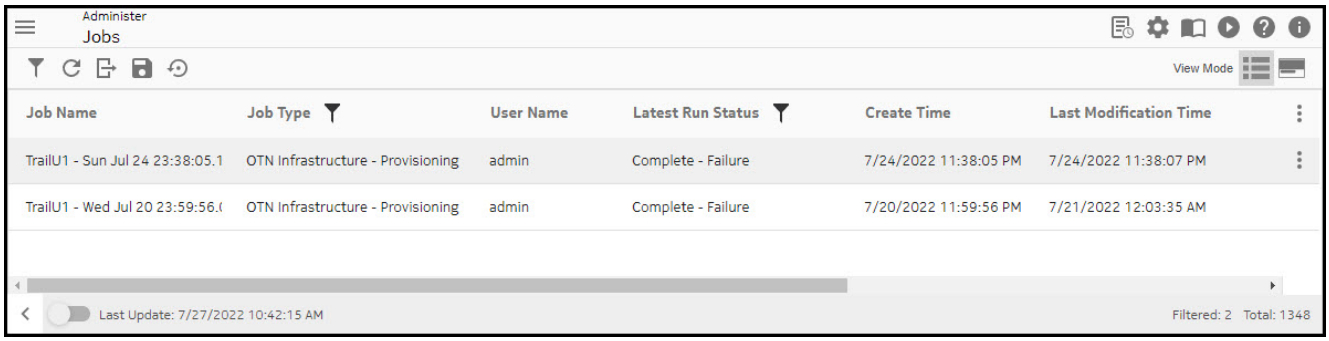
Examples: The following two figures illustrate a completed, successful job for a service and a failed job for a service.

Figure 7-189 Connections – Services – Completed job



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-190 Connections – Services – Failed job



3

Optional: To view the Jobs for the client or server of an infrastructure connection or for the server of a service, highlight and select the infrastructure connection or service, select the **Clients** or **Servers** tab, select the connection, and click on the **More** icon on the right of the selected connection and follow this path: **Jobs**.

Result: The system opens a new browser tab and displays the Job List window for the selected client or server of the infrastructure connection or the server of the service.

4

Optional: Select a job, scroll down to the bottom of the window, and click on one of the following tabs: **Details** or **Job Inventory**.

Result: The system activates the selected tab and the Job List-related information is displayed directly below the data table for the Job List.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.72 View Infrastructure Connections or Services

When to use

Use this task to view a list of infrastructure connections and services.

Before you begin

An Important usability note! The system defaults to a display of 15 rows of objects in a data table. Typically, the Services data contains more rows of objects than other data tables. The numerical values that are displayed in the "Total Objects icon" (p. 2276) provides you with the number of rows of objects that are available for viewing. If the "Total Objects icon" (p. 2276) is overlaid with the "Total Objects - Snippet Icon" (p. 2276), you can use the **Remote Filter** to filter the data columns in order to reduce the rows of objects that are displayed in the data table. Refer to 26.4 "Data Table Filtering Icons" (p. 2203) for direction. In addition, to make viewing easier, you can also page through the rows of objects.

Task

Complete the following steps to view a list of infrastructure connections and services.

1

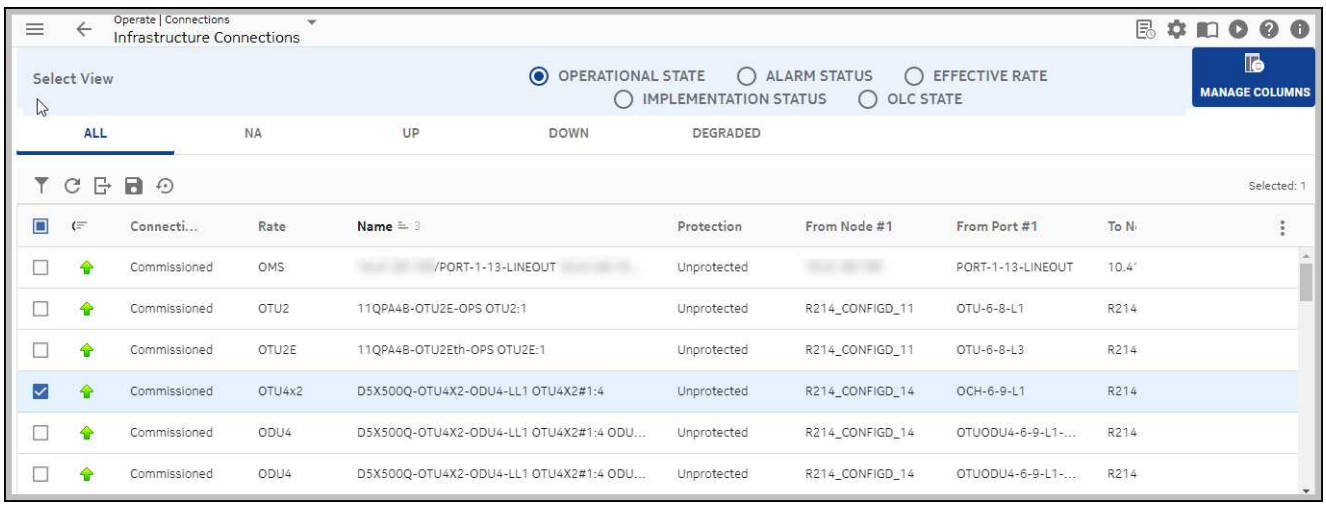
Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

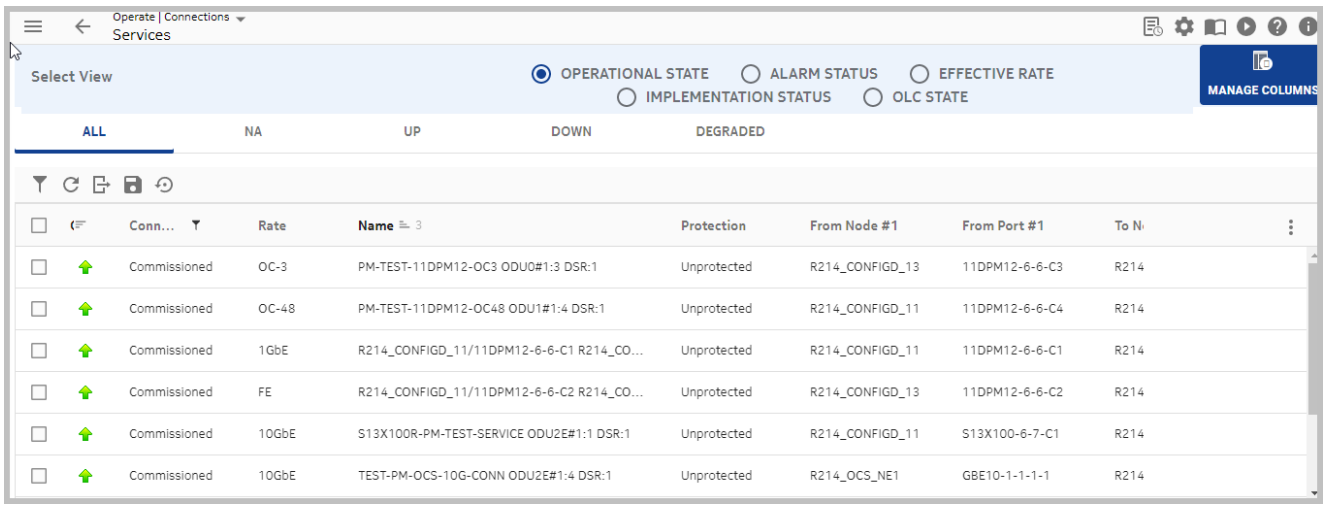
Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

Figure 7-191 Connections – Infrastructure Connections



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-192 Connections – Services



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 user can filter the Infrastructure Connection/Services data table using the **NPA Name** column.

Note: If a Connection crosses more than one NPA and if the user filters on one NPA in the list, then the filtered list shows only the NPA used in the filter for that connection.

4

Optional: For additional navigation options for 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.

6

Optional: To customize the filters, sorting, column order in data table, and to save the same or if you want to reset a customized view of the data table to its default display, refer to the

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

26.9 “Save or reset data table preferences on connections (physical/ infrastructure) and services screen” (p. 2220) task for detailed steps.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.73 View Eline connection on Carrier Ethernet Links and Carrier Ethernet OAM pages in ESM

Overview

When a DSR connection/service is created in OTN, the same connection/service is exported to ESM Carrier Ethernet Links window on a new tab of OTN_Eline. The test suites associated with the connection are available in the Carrier Ethernet OAM window. This is applicable only in 1830 PSD NEs.

Note: The connection must be Eline capable. 1830 PSD supports 1GBE client port rate, for SOAM.
These Eline connections are the connections that run through one of the three supported modes in 1830 PSD and one L2 supported pack.

When to use

Use this task to view the Eline connection on Carrier Ethernet Links and Carrier Ethernet OAM pages in ESM. OAM needs to be supported on the end points of the connections that are created. Deploy OAM entities such as the MD, MA, and MEP on the client ports of the PSDs that are created

Task

Complete the following steps to view the Carrier Ethernet OAM and Carrier Ethernet Links pages in ESM.

1

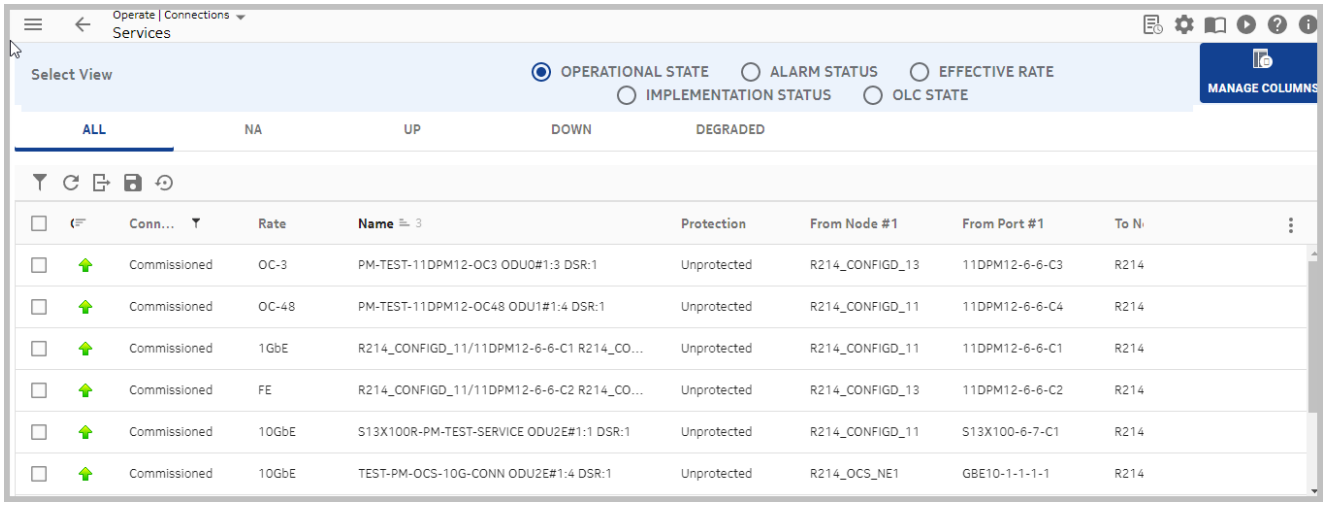
From the NFM-T GUI, follow the navigation path:

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of services.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-193 Connections – Services



2

Select the 1830 PSD NE and click on the **More** icon on the right side of the NE.

3

Do one of the following:

- Select **SOAM Tests** to navigate to the Carrier Ethernet OAM window in ESM.
- Select **SOAM Details** to navigate to the Carrier Ethernet Links window in ESM.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.74 View slots for an infrastructure connection

When to use

Use this task to view the available/unavailable slots for an infrastructure connection.

This task enables you to view the total slots, used slots, and free slots for a selected infrastructure connection.

Task

Complete the following steps to view the available/unavailable slots for an infrastructure connection.

1

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

OPERATE > Infrastructure Connections

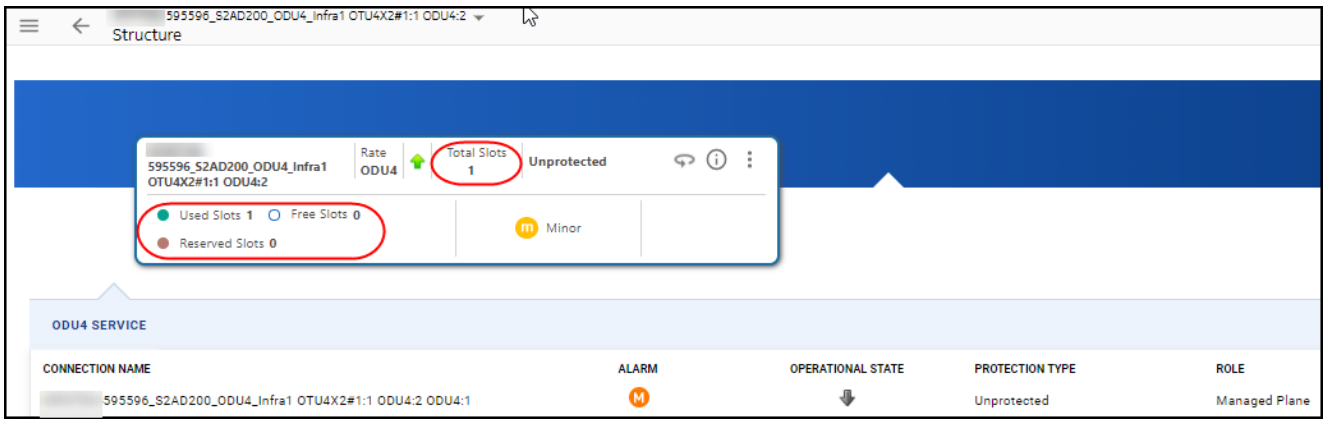
Result: The system displays a data table that lists all of the infrastructure connections.

2

Click on the connection for where you would to view its slots and click on the **More** icon, follow the path **Structure**.

Result: The system displays the **Structure** window and displays the number of total slots, used slots, and free slots for the selected infrastructure connection.

Figure 7-194 Connections – Structure tab – all slots are free



END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.75 1830 PSD Service Testing and BER Monitor

Purpose

The Service Testing feature is used to verify the status of a 10GbE or 1GbE service connection between 1830 PSD NEs. When the feature is enabled, service testing is automatically triggered as a post commissioning operation when a 10GbE/1GbE connection is created. Service testing can also be manually triggered for a connection from the connection list.

Note: NFM-T supports simultaneous testing of a maximum of 10 service connections across multiple users and services.

Service testing includes:

- Injection of a Pseudo-Random Binary Sequence (PRBS) test signal into the line side of the 1830 PSD NE signal path and monitoring of the bit error rate on the receive end.
- Latency measurement

When creating a Service, if enabled on the system preference, service testing is automatically triggered to check the status of the service. This allows testing of the carrier facility prior to establishing live service. The PRBS testing is automatically triggered after commissioning is complete. If PRBS testing successfully completes, latency testing is automatically triggered.

For a commissioned service, the user can manually execute the service testing, to check the status of the service. The service testing is executed based on the system preferences. This allows monitoring of the service after fixing the network problem.

Note: Service testing is performed only if there are no service affecting alarms on the connection. If alarms are present, after the alarms are cleared the user must manually initiate service testing. If the service testing is failed due to service affecting alarm, filter the service affecting alarm from the alarms list of the 1830 PSD connection(s) to view the alarm that caused the failure.

Before you begin

- Since Latency measurement is required as part of Service Level Testing, when creating a Service, make sure the **Compute Latency** check box is selected.
- The system level Service Testing parameter must be enabled.
- The connection rate must be 10GbE or 1GbE when creating a symmetric service.
- All endpoints must be on 1830 PSD NEs of Release 2.0 or higher.
- All endpoints must be on 1830 PSD NEs with a supported system mode. See "Supported system modes for Service Testing" (p. 1027) for the system modes.
- The service connection has a single ODU1/ODU2 server between the 1830 PSD NEs.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

System Preferences setting

Complete the following steps to manage the Test Signal Injection tool from System Preferences. The users with System Administrator privilege can set the following preferences. Note that if the test is in progress, then any change in the preferences are applicable only on next test.

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

   ADMINISTER > **System Preferences**

   Result: The **System Preferences** window is displayed.

2. In the **CONNECTION MANAGEMENT** tab, under **PRBS for PSD** pane, select the options:

Enable Service Testing	Allows the user to enable or disable the service testing. A toggle button with the following options: • **ON** - to enable automatic or manual testing • **OFF** - to disable the testing (default)
Enable inverted PRBS Signal	Allows the user to enable or disable inverted PRBS signal A toggle button with the following options: • **ON** - to enable inverted PRBS signal • **OFF** - to disable inverted PRBS signal (default)
BER Observation Period (HH:MM:SS)	Determines the length of time that BER measurements takes. The observation period can be configured from 5 minutes to 24 hours, where the user is able to adjust the seconds in 5-seconds, 5-minutes, or 1-hour intervals. A time picker is available with initial default value of 15 minutes. Note that the BER observation period is the time that measurements are taken for a direction. If the BER observation period is 15 minutes, measurements for the BER in the A to Z direction are taken for 15 minutes, and measurements for the BER in the Z to A direction are taken for 15 minutes, for a total time of 30 minutes. In R21.4, this field supports the following values: • HH: 0-23 • MM: 0-59 • SS: 0-59
BER Measurement Frequency (MM:SS)	Determines the frequency when BER measurements are taken during the observation period. The interval can be configured from 5 seconds to 55 seconds in 5-seconds intervals and 1 minute to 60 minutes in 1-minute intervals. A time picker is available with initial default value of 30 seconds.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Latency Observation Period (HH:MM:SS)	Determines the length of time that Latency measurements are taken during the observation period. The observation period can be configured from 5 minutes to 24 hours, where the user is able to adjust the seconds in 5-seconds, 5-minutes, or 1-hour intervals. A time picker is available with initial default value of 15 minutes. In R21.4, this field supports the following values: • HH: 0-23 • MM: 0-59 • SS: 0-59
Latency Measurement Frequency (MM:SS)	Determines the frequency at which Latency measurements are taken during the observation period. The interval can be configured from 5 seconds to 55 seconds in 5-seconds intervals and 1 minute to 60 minutes in 1-minute intervals. A time picker is available with initial default value of 30 seconds.
Failure threshold for BER	Specifies the threshold when a Bit Error Rate (BER) measurement fails. If the value of any periodic BER measurement period exceeds the threshold, service testing fails and no further BER or latency measurements are performed even if the observation period is not completed. A text box with the default value of 1.0E-13. Enter the value in `*.*E-**` format, where * is an integer value.
No. of data sets per Service Connection	Specifies the maximum number of data sets which are retained for each connection. When the upper limit is reached the system overwrites the oldest Service Test Results. If the user modifies the number of data sets retained by NFM-T to reduce the number stored per connection, next time the service testing is performed for a connection the system deletes the oldest data sets and inserts the current data set, so that final number of data sets stored for the connection equals the current maximum number. A text box with supported values from 2 to 100. The default value is 10.

3. Click **SUBMIT**.

Supported system modes for Service Testing

Service Testing is supported for the following 1830 PSD system modes:

- 10GBE Client OTU2 network mode
- 10GBE Client OTU2e network mode
- 1GBE Client OTU2 network mode
- 1GBE Client OTU1 network mode

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Supported 1830 PSD configuration for Service Testing

1830 PSD supports the following configuration for service testing:

- Unprotected and SNCP protected 1830 PSD NEs
- L0 Control Plane and Managed Plane 1830 PSS network
- Interworking regression configuration with all 1830 PSS cards with connection rate as 10GbE or 1GbE to create symmetric service.
- All protection configurations within the 1830 PSS network with connection rate as 10GbE or 1GbE to create symmetric service.

  Service testing is not supported for 3-ended Services and 4-ended Services.

Service Testing

Service testing is initiated automatically or manually. The service testing includes PRBS testing and latency measurement. Depending on the **System Preferences** settings, after the service is commissioned, automatic testing is triggered. If the service is already created, user can manually initiate the service testing.

Note: If the **System Preferences** setting is changed, then reload the **Service Connections** browser page before initiating the service testing. In Firefox, clear the cache and then reload the **Service Connections** browser page.

Task: Manually initiate Service Testing

Complete the following steps to perform service testing:

1. From the NFM-T GUI, follow one of these navigation paths:

   OPERATE > Nodes

   OPERATE > Services

   Result: The system displays a data table that lists all of the nodes in the **Nodes** pages and all the services in the **Services** page.
2. If you have navigated from **OPERATE > Nodes**, click on the 360° view icon of the 1830 PSD NE where the service testing needs to be performed and navigate to the **SERVICE CONNECTIONS** tab.
3. Select the 1GbE or 10GbE connection in commissioned state, and click on the **More** icon.
4. Click **Service Testing** > **Perform Testing** to initiate service testing.

   Result: A message is displayed that the PRBS and latency measurement is initiated successfully.

   Note: When the testing is initiated, the OLC state of the service connection in ODU1/ODU2 server connection are changed to maintenance. While testing is in progress, any change to the OLC state is not allowed. When testing successfully completes, the OLC states are changed to in service. If testing fails, the OLC states remain in maintenance.
5. To view the status of the service testing job, perform one of the following:
   - Click **JOBS** to navigate to **Jobs page** and view the status of the
   - From **OPERATE** > **Services** page or **OPERATE** > **Protected Connections** page perform the following:

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Click **MANAGE COLUMNS**, select **TEST STATUS** and click **APPLY & SAVE**.
- View the status under **Test Status** column

- From the **OPERATE** > **Services** page or **OPERATE** > **Protected Connections** page, perform the following:
  - Click on 360° view of the connection.
  - Click the **SERVICE TESTING RESULTS** tab.

  Result: The **Service Testing Result** window is displayed with the information such as, the details of service testing, BER and Latency measurements.

Note: The following actions can be performed when the service testing is in progress. All other actions are not allowed:

- Abort the service testing
- View routing display
- View display route on map
- Add nodes
- View route details
- View timeline
- View jobs

Task: Abort Service Testing

Note: Abort Testing option is enabled only when testing is in progress.

Complete the following steps to abort the service testing:

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

   OPERATE > Services

   Result: The system displays a data table that lists all of the services.
2. Select the 1GbE or 10GbE connection in commissioned state, and click on the **More** icon.
3. Click **Service Testing** > **Abort Testing** to abort the service testing.

   Result: A message is displayed that the abort service testing is initiated successfully.
4. Click **OK**.

   Note: You can perform the abort operation from **OPERATE > Nodes** also.
5. To view the status of the operation, perform the following:
   - Navigate to **OPERATE** > **Services** page or **OPERATE** > **Protected Connections** page.
   - Click **MANAGE COLUMNS**, select **TEST STATUS** and click **APPLY & SAVE**.
   - View the status as *Aborted* under **Test Status** column

Task: View Status of the Service Testing

Complete the following steps to view the status of the service testing:

1. Navigate to **OPERATE** > **Services** page or **OPERATE** > **Protected Connections** page to view the status of the operation.
2. Click **MANAGE COLUMNS**, select **TEST STATUS** and click **APPLY & SAVE**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3. View the status under **Test Status** column

   Test Status column displays the following status:
   - **Success** - Indicates that the service testing is completed and none of the test results exceeded the threshold criteria.
   - **None** - Indicates that the service testing has not been performed in the connection.
   - **In Progress** - Indicates that the service testing is currently in progress for the connection.
   - **Aborted** - Indicates that the service testing was cancelled before completion.
   - **Failed** - Indicates that one or more commands failed and the service testing is not complete.
   - **Maintenance** - Indicates that the service testing was completed, but the test results exceeded the threshold criteria.

Task: View Service Testing Results

Complete the following steps to view the service testing results:

1. From the **OPERATE** > **Services** page or **OPERATE** > **Protected Connections** page, click on 360° view of the connection.
2. Click on **SERVICE TESTING RESULTS** tab.

   Result: The **Service Testing Result** window is displayed with the information such as, the details of service testing, BER and Latency measurements.

   Note: SERVICE TESTING RESULTS tab is not available for aborted tests.

   The following information is available in the **Service Testing Result** window:
   - The status of the service testing
   - The failure reason such as any command execution failed or the bit error rate is greater than the threshold value.
   - BER measurement result with the status of the PRBS testing.

     Note: After the service testing execution, if the value of **Failure threshold for BER** is modified in the **System Preferences**, the BER measurement under **SERVICE TESTING RESULTS** tab displays the modified value.
   - The Details of the BER and latency measurements.

     Note: For a connection with high latency, NFM-T can attempt to measure latency while the measurement is still in progress. When this happens a latency value of -1 is displayed which indicates the measurement was still in progress. In this scenario, to measure the latency, depending on the connection rates, execute the following CLI commands on From Node of immediate ODU2/ODU2e/ODU1 server of the service connection:

     ```
     - show otn odu2p 1 VIRTUAL dm ondemand result
     - show otn odu1p 1 VIRTUAL dm ondemand result
     - show otn odu2ep 1 VIRTUAL dm ondemand result
     ```

     Note: See 25.48 “Service Testing Result Tab” (p. 2158) for more details.
3. Click **EXPORT** to export the details in a PDF format.

Task: View Service Testing Log

Complete the following steps to view the service testing log:

1. From **ADMINISTER**, select **Service Testing Log**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The **Service Testing Log** window is displayed with the information of the connections in which the service testing is performed.

Note: The number of retained test results per connection depends on the value of **No. of data sets per Service Connection** field in **System Preferences**.

2. Click on the 360° view of the connection to navigate to the **SERVICE TESTING RESULTS** page.

   Note: For aborted tests, the 360° view is not available to view the **SERVICE TESTING RESULTS** page.

   Note: After the service testing execution, if the value of **Failure threshold for BER** is modified in the **System Preferences**, the BER measurement under **SERVICE TESTING RESULTS** tab displays the modified value.

3. Select one or more connection and click on the **Export PDF** icon to export the details in a PDF format.

   Note: Export PDF icon is not available if the selected connections have aborted the service testing.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.76 View tabbed topics for an infrastructure connection or service

When to use

Use this task to view the tabbed topics for an infrastructure connection or service.

Before you begin

You can view tabbed topics for a connection clicking on the 360° View icon on the right of the selected object row.

Some tabbed topics are only displayed during certain conditions.

Task

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

1

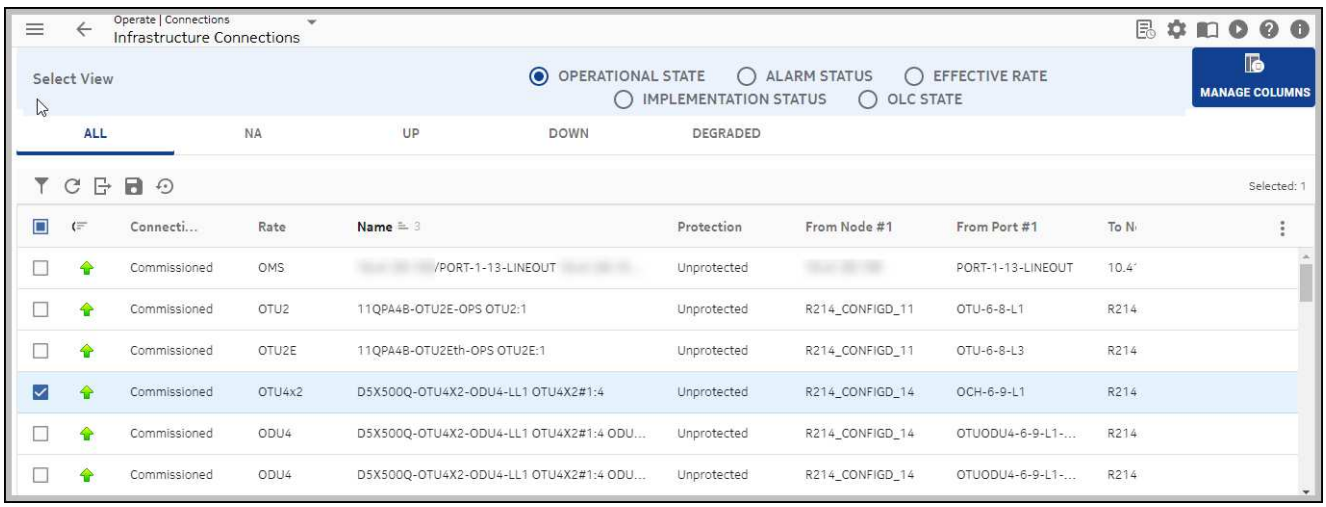
Follow one of the navigation paths from the NFM-T GUI:

OPERATE > Infrastructure Connections

OPERATE > Services

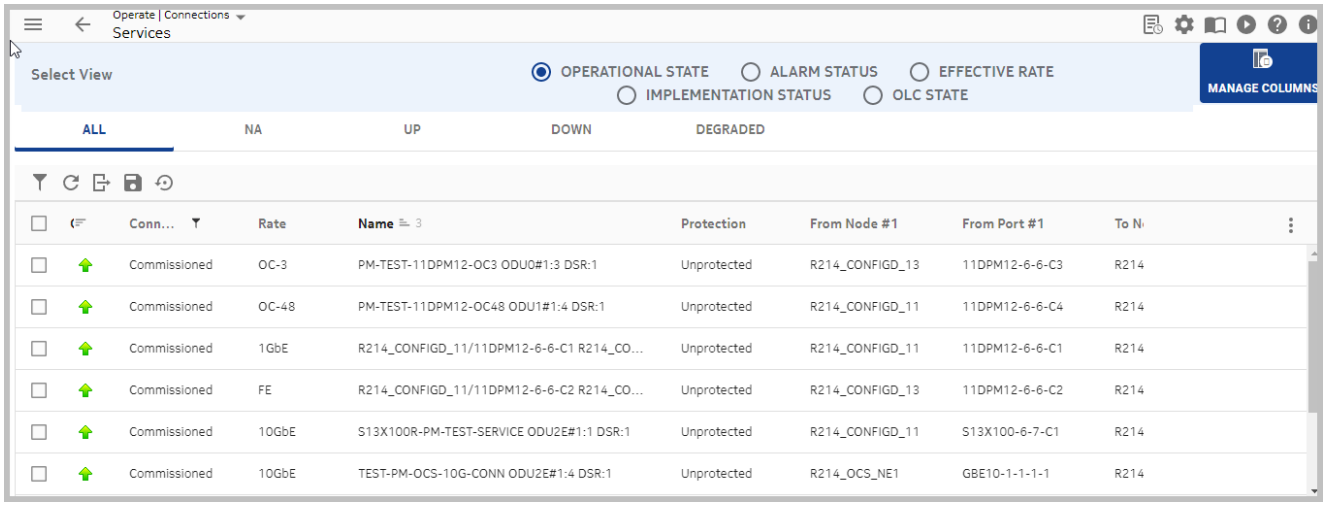
Result: Depending on your selection, the system displays a data table that lists all of the infrastructure connections or services.

Figure 7-195 Connections – Infrastructure Connections



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-196 Connections – Services



2

To view tabbed topics for a connection (Service or Infrastructure), click on the **360° View** icon on the right of the selected connection row.

The available tabs for infrastructure connections are the following:

25.6 “ALARMS Tab” (p. 2066)
25.44 “Servers Tab” (p. 2148)
25.11 “Clients Tab” (p. 2080)
25.42 “Routes Tab” (p. 2145)
25.53 “Structure Tab” (p. 2167)
25.28 “Link Connections Tab” (p. 2117)
25.14 “Command Status tab” (p. 2087)
25.36 “PM Enabled Points Tab” (p. 2135)
25.9 “ASON SNC Tab” (p. 2073)
25.54 “Switched Connections Tab” (p. 2171).

The available tabs for services are the following:

25.6 “ALARMS Tab” (p. 2066)
25.44 “Servers Tab” (p. 2148)
25.42 “Routes Tab” (p. 2145)
25.14 “Command Status tab” (p. 2087)
25.36 “PM Enabled Points Tab” (p. 2135)
25.40 “Private Tunnel Tab” (p. 2142).

Important usability notes:

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

• For infrastructures, the **Command Status** tab is only displayed if the **Implementation Status** of the infrastructure connection is **Implemented**, **Fully Allocated**, or **Partially Allocated**.

• For services, the **Command Status** tab is only displayed if the **Implementation Status** of the service is **Implemented**, **Fully Allocated**, or **Partially Allocated**.

Figure 7-197 Connections – Infrastructure Connections – tab selection

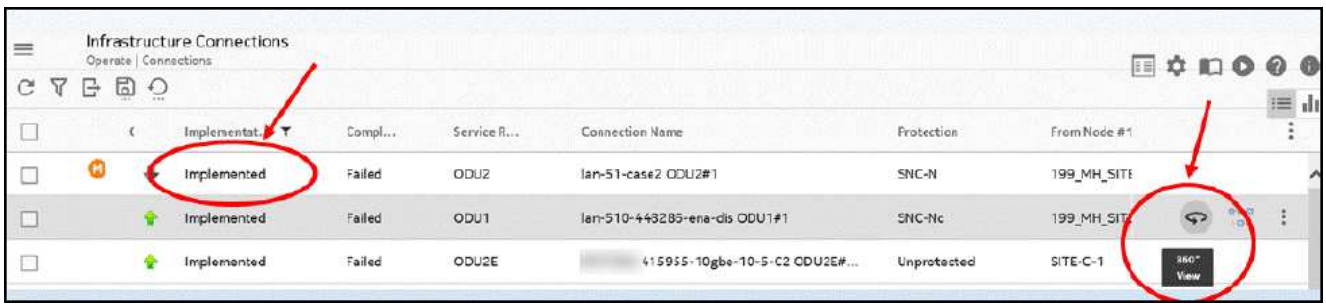
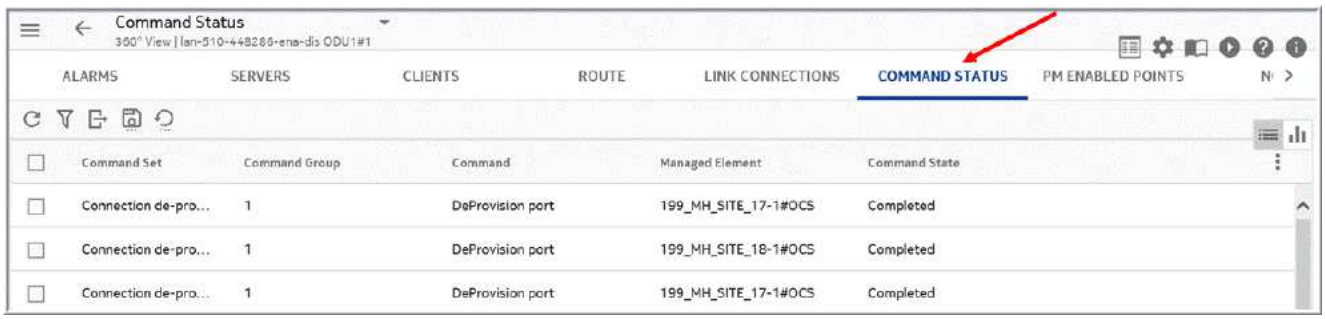


Figure 7-198 Connections – Infrastructure Connections – Command Status



• For infrastructure connections, the **ASON SNC** tabbed topic is only displayed if the **Category** of the connection is **Mixed Plane** or **Control Plane**.

For private tunnel connections, the **Switched Connections** tab is displayed. The **Sc Id** column of the Services page displays the data that is retrieved from the GMRE. Implicit OTU gets created as part of the behavior. For switched connections, the **Category** column displays **ASON Private Tunnel**.

For switched connections, the **Private Tunnel** tab is displayed in the Services connection, in the 360° View. The **Sc Id** column of the Services page displays the data that is retrieved from the GMRE. Implicit OTU gets created as part of the behavior.

• The **Route** tabbed topic offers the option of viewing the information in **Table**, **Graph**, or **Full** format.

• For infrastructure connections, the **Clients** and **Servers** tabbed topics offer the option of viewing the information in **Table** or **Graph** format.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- For services, the **Servers** tabbed topic offers the option of viewing the information in **Table** or **Graph** format.
- From the **Alarms** tabbed topic, you can access the Equipment Manager.

Result: The system activates the tabs and the connection-related information is displayed directly below the data table for the connection or in a new browser window.

Note: If you chose to open a new browser window, click the browser back arrow to return to the original data table.

3

Optional: To view the details of a selected item in a either the top or bottom data table, click on the **i** 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

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.77 View various route displays for an infrastructure connection or service

When to use

Use this task to view the various route displays for a selected infrastructure connection (trail or logical link), a service, the clients and servers of an infrastructure connection, or the servers of a service.

Before you begin

You can view the route of a connection using these graphical displays from the NFM-T GUI:

- You can view the connection in terms of its placement on the Network Map. When you select this view, you see the connection in terms of is neighboring connections. Details regarding the connection are limited. Refer to "Task: Display the route of a connection on the Network Map" (p. 1036).
- You can view the connection on the Routing Display. When you select this view, you see the connection and all of the details regarding the connection. Neighboring connections are not displayed. Refer 7.78 "View the Routing Display of a selected connection " (p. 1042).

Task: Display the route of a connection on the Network Map

Complete the following steps to view the various route displays for a selected infrastructure connection (trail or logical link), a service, the clients and servers of an infrastructure connection, and/or the servers of a service on the Network Map.

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 requested connections.

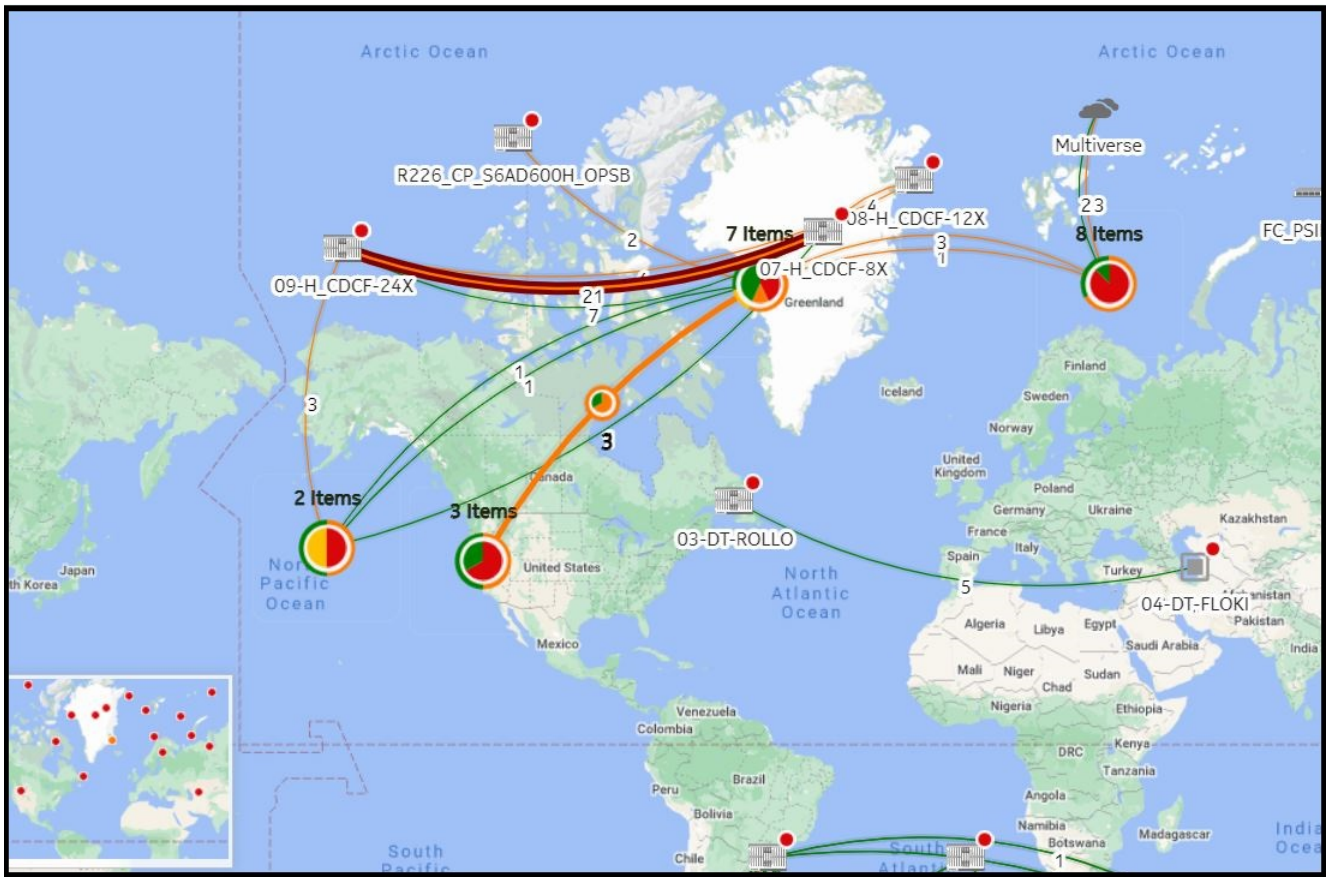
2

Select the connection for which you want to view the route on the Network Map and click on the **More** ⋮ icon and follow this navigation path: **Display on Map > Highlight on Map**.

Result: The system opens a new browser tab and the route of the connection is displayed on the Network Map.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-199 Connection on the Network Map



End of steps

Task: Highlight Physical Route on Network Map

Complete the following steps to view the various route displays for a selected infrastructure connection (trail or logical link), a service, the clients and servers of an infrastructure connection, and/or the servers of a service on the Network Map.

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 requested connections.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

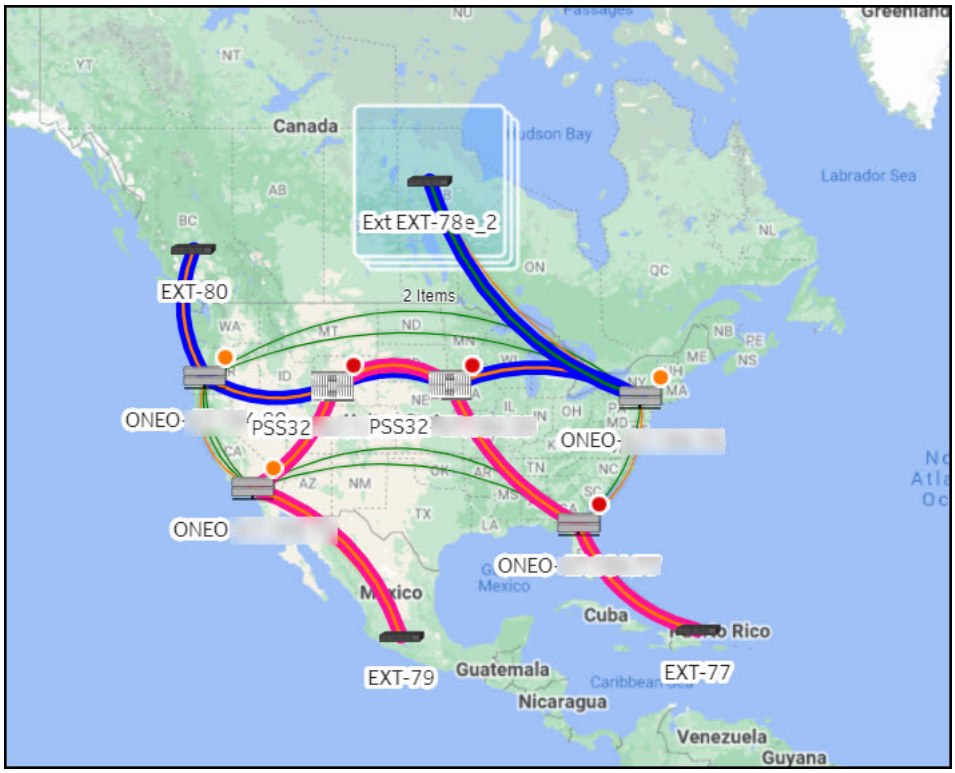
Select one of the element which is in *Commissioned* state from the data table. Click **More icon** and follow this navigation path: **Display on Map > Route at Physical Layer**.

Result: A new network map window is displayed with the physical layer of the connection highlighted.

For a 3-ended and 4-ended connection type the main route and spare route of the physical connection is highlighted.

The Figure 7-200, “Highlight Physical Route on Map” (p. 1037) is an example of a 4-ended connection.

Figure 7-200 Highlight Physical Route on Map



End of steps

Task: Highlight Route at all Layers on Network Map

Complete the following steps to view the various route displays for a selected infrastructure connection (trail or logical link), a service, the clients and servers of an infrastructure connection, and/or the servers of a service on the Network Map.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

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 requested connections.

2

Select one of the element which is in *Commissioned* state from the data table. Click **More icon** and follow this navigation path: **Display on Map > Route at all Layers (all Depths)**.

Result: A new network map window is displayed with the physical layer of the connection highlighted and the **HIGHLIGHT ROUTE** panel for the selection.

Depth of each element is displayed on **Highlight Route** panel. The depth layer selected to navigate from is at the top of the list layers displayed.

3

To view the different layers of the connection, in the **HIGHLIGHT ROUTE** panel select the check box against each layer as required.

a. To change color of any layer, deselect the same.

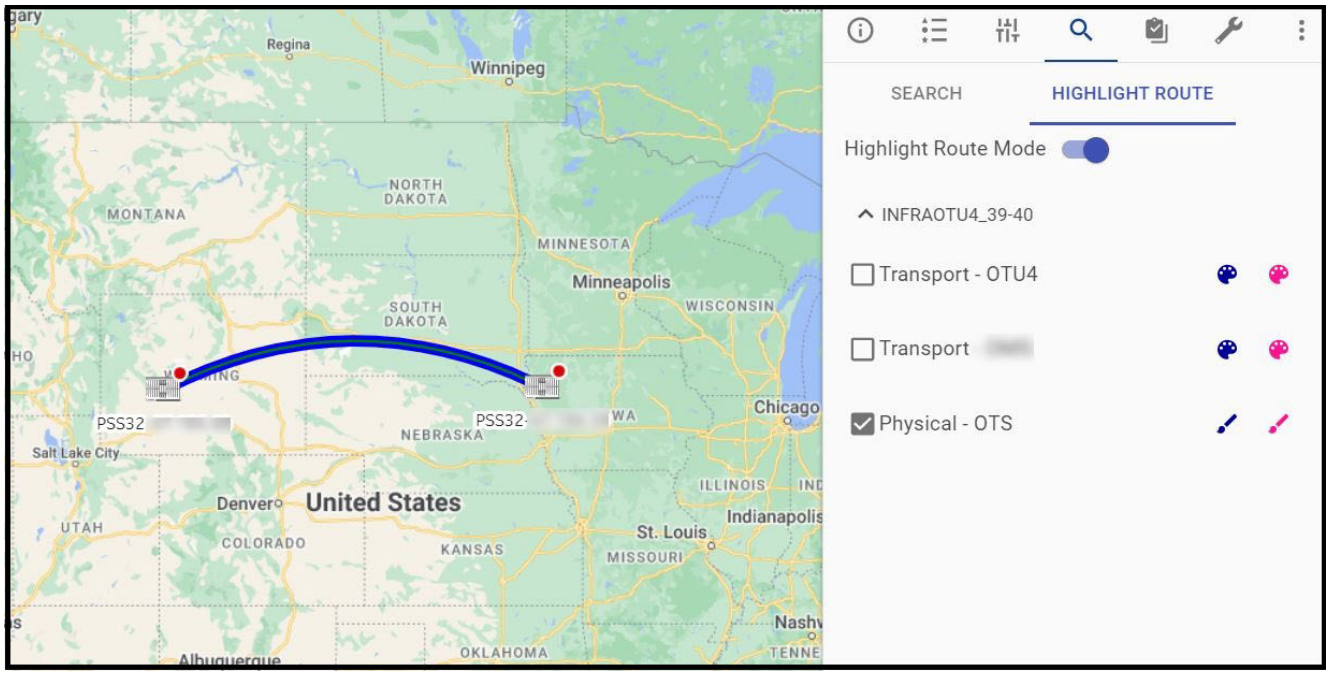
b. Click the icon and select a different color from the color palette.

c. Select the element.

Note: Color selection is disabled once the layer is selected.

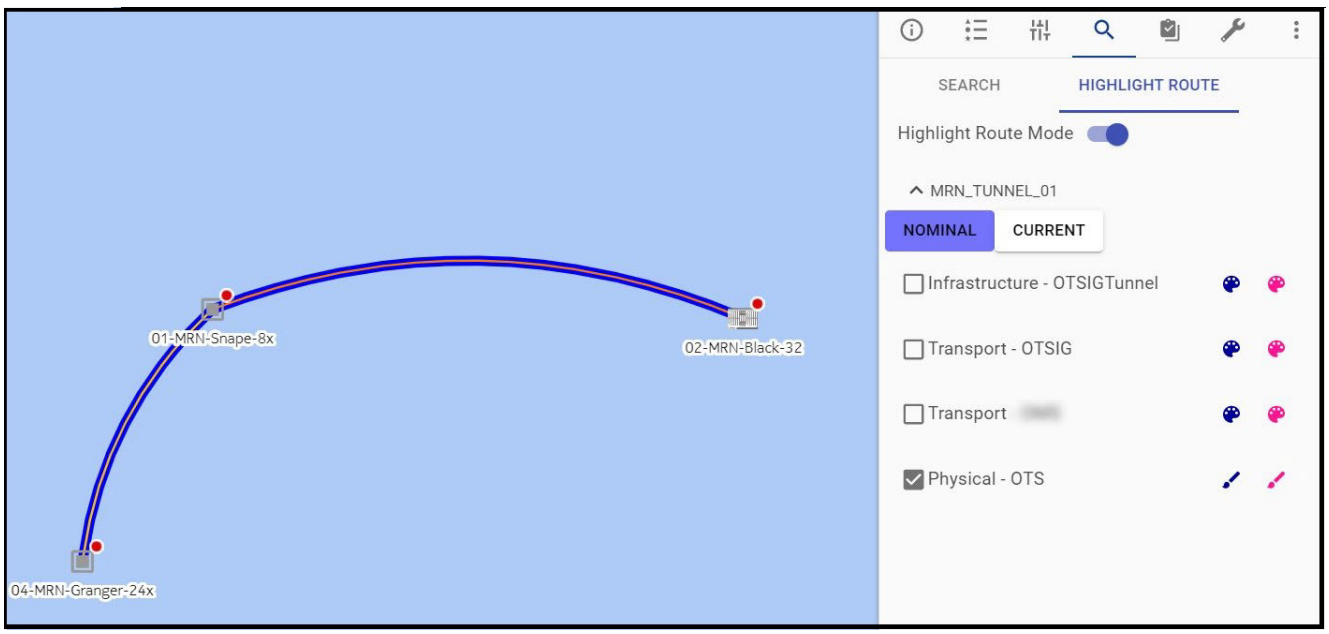
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-201 Display Route [Managed Plane]



Note: In Managed Plane, the network itself does not reroute any connection.

Figure 7-202 Display Route [Control Plane]



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: Control Plane is a part of network that carries signaling traffic and responsible for routing. Control plane can have the following routes has three routes: *Nominal* , *Current*, and *Backup*.

END OF STEPS

Task: Display the route of a connection on the Routing Display

Complete the following steps to view the various route displays for a selected infrastructure connection (trail or logical link), a service, the clients and servers of an infrastructure connection, and/or the servers of a service on the Routing Display.

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 connection for which you want to view the route on the routing display. Click on the **More** icon and follow this navigation path: **Routing Display**. For details see 7.78 "View the Routing Display of a selected connection " (p. 1042).

Result: The system opens a new browser tab and the route of the connection is displayed on the Routing Display

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.78 View the Routing Display of a selected connection

When to use

Use this task to view all the circuit packs involved in the routing of any of the following types of network connections: physical connection, infrastructure connection (trail or logical link), protected connection or a service connection.

Note: Routing display is not available for OPS connections between two external NEs.

Related information

See the following topics in this document:

- 7.86 “View Protected Connections” (p. 1091)

Before you begin

The Routing Display is a high level vision of the connection which allows to display the connection on the maps and connection details. Additionally, the Routing Display, allows the user to display the packs involved in the connection, internal links, physical links including optical lines according to the considered connection. The port alarms displayed, are alarms that may exist at physical layer or at any of the corresponding service or infrastructure layers.

The GMPLS/ASON connections are also displayed from the Routing Display. In this context all the layers (L0 and L1) belonging to the *Nominal route* are displayed. Only ODUk connections at level 0 are displayed in the *Current route*.

At NE level, the packs are displayed in which the IN/OUT ports are configured, connections between ports are displayed in the Routing Display. At port level Loopback option is displayed

The system visualizes the graphical view of the *Implemented* and *Commissioned* connections.

Task: Display a connection on the Routing Display

Complete the following steps to view the Routing Display for a selected physical connection, infrastructure connection (trail or logical link), or a service.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Nodes > Impacted Connections (tab)

OPERATE > Nodes > Used Ports (tab)

OPERATE > Physical Connections

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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

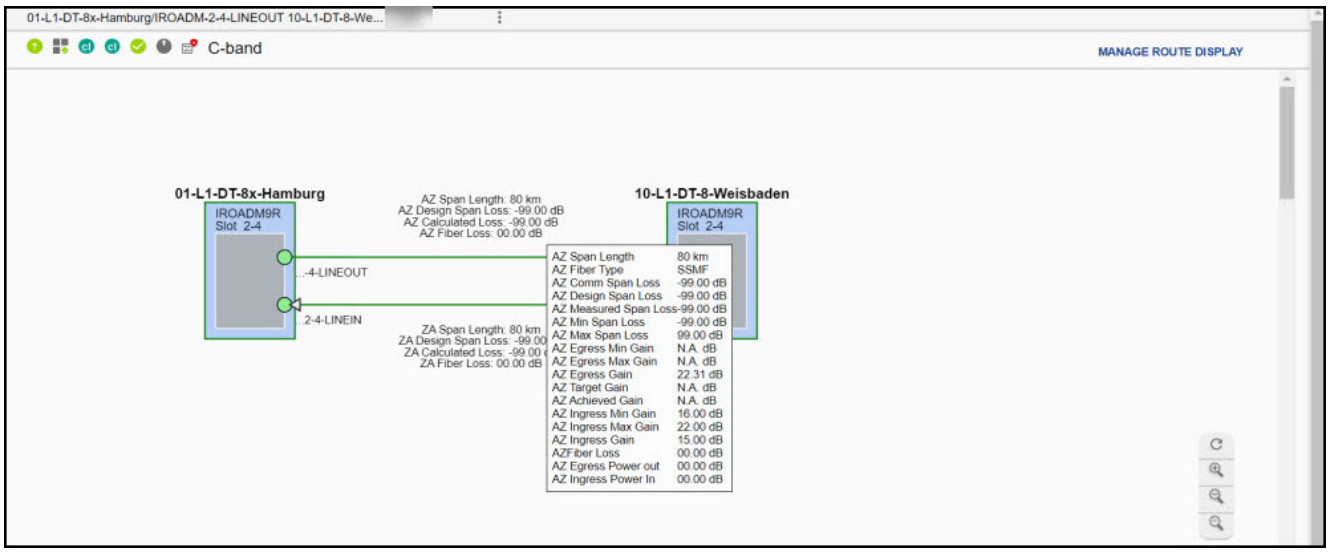
Select the connection for which you want to view the Routing Display, select the routing display icon on the right of the connection row.

OR click on the **More** icon and follow this navigation path: **Routing Display**.

Result: The system opens a new window and the route of the connection is displayed on the Routing Display.

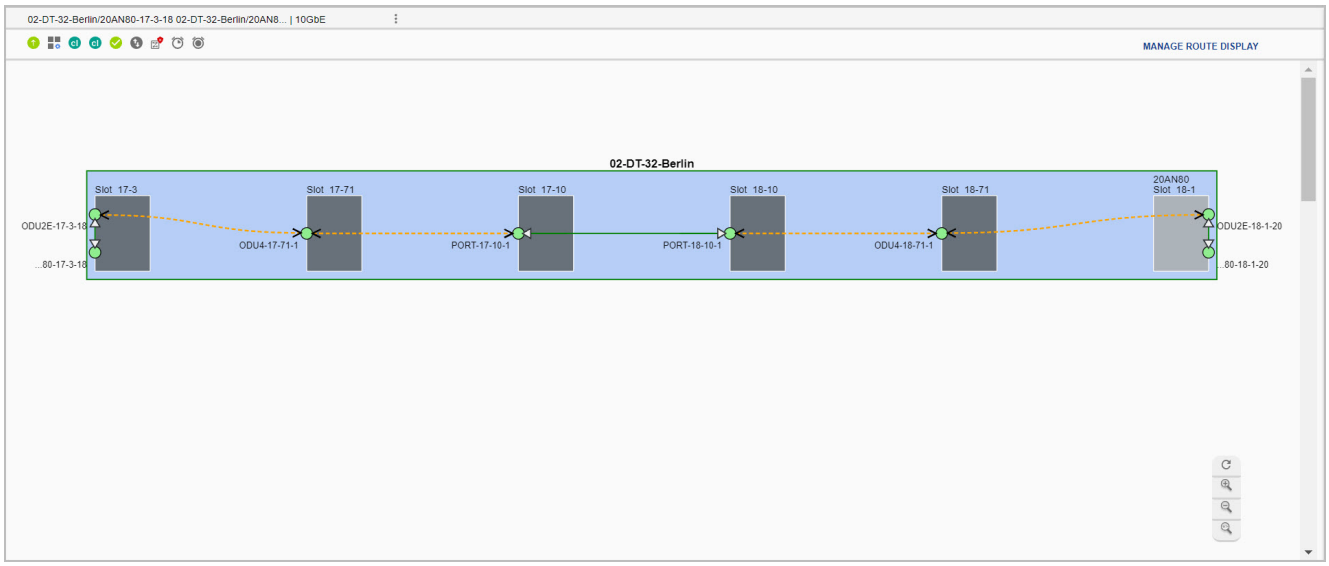
EXAMPLE: The following figures illustrate the Routing Display for an infrastructure connection and related server connection.

Figure 7-203 Routing Display - infrastructure connection with fiber information window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-204 Routing Display - service connection



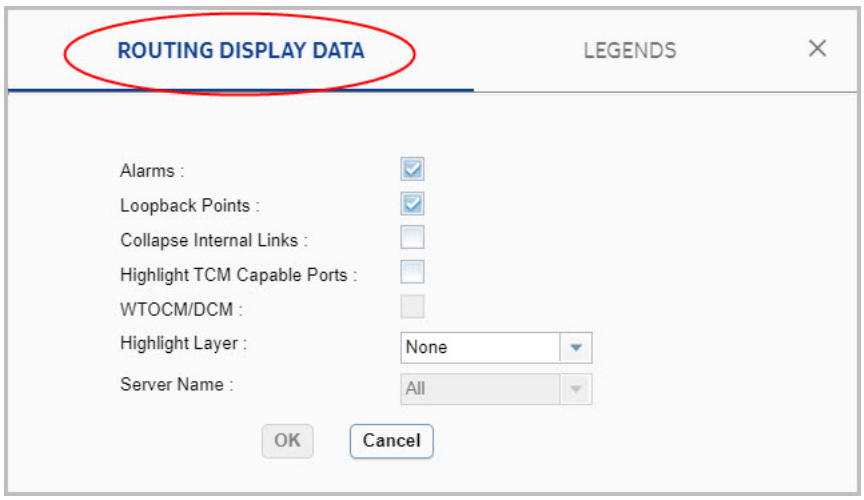
3

Select the **MANAGE ROUTE DISPLAY** button at the top right, a sliding window opens showing the **ROUTING DISPLAY DATA** and **LEGENDS** panels.

The Routing Display view, can be modified by enabling or disabling the following fields in the **ROUTING DISPLAY DATA** panel:

Alarms, **Loopback Points**, **Collapse Internal Links**, **Highlight TCM Capable Ports**, **WTOCM /DCM**, **Highlight Layer** and **Server Name**.

Figure 7-205 Routing Display - Routing Display data panel



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

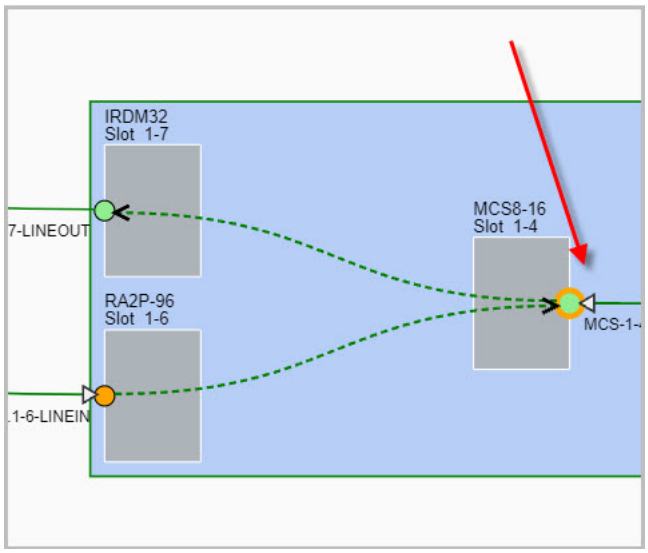
4

The **Alarms** field is checked as default. If checked the alarm associated to each port is visualized.

Alarms check box is checked by default after a refresh or reload of the page.

The displayed port alarms, are the alarms that may exist at physical layer or at any of the corresponding service or infrastructure layers. Ports have the coloring of the alarms on the given port, typically the physical layer. If there are corresponding alarms on the infrastructure or service layer, a ring is added around the port with the color of the alarm at that layer. See 24.4 "Quick Help – The Routing Display Window" (p. 1977) for more information on alarms port.

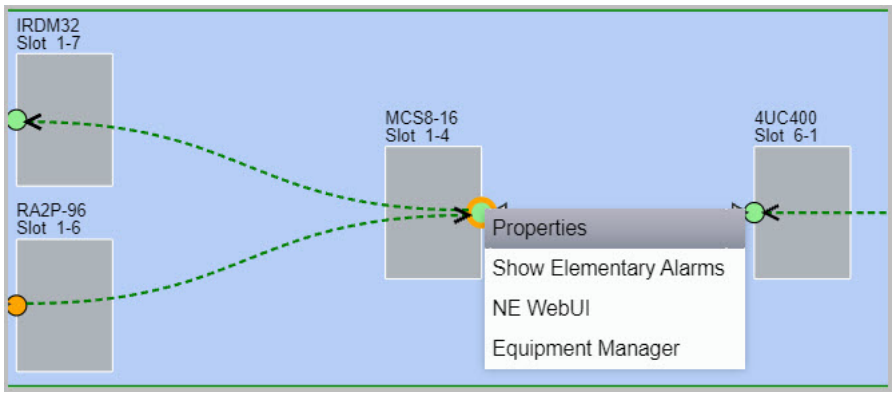
Figure 7-206 Routing Display - infrastructure connection with alarm port



Optional. Right clicking on a port, a list of additional navigation options for that item are displayed, such as **Properties**, **Show Elementary Alarms**, **NE WebUI**, and **Equipment Manager**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

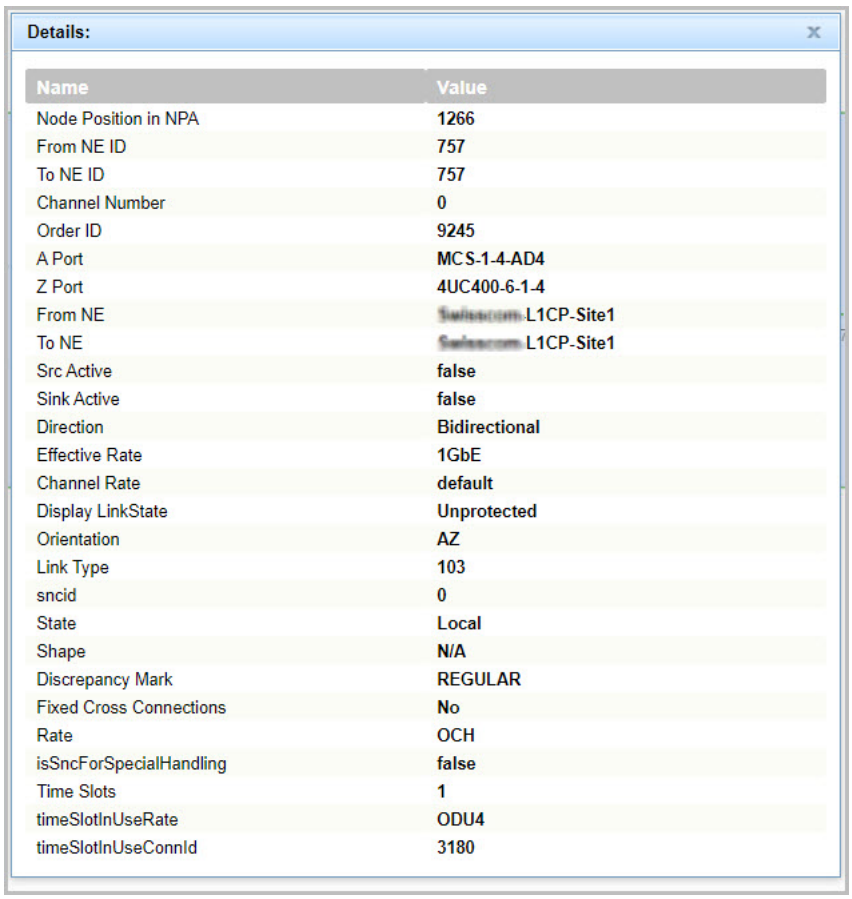
Figure 7-207 Routing Display - Properties



Note : The *Properties* option is available also for connections. Select a connection and right click, the **Details** window of the connection is displayed, which provides the complete information of the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-208 Routing Display - Properties > Details



Details:

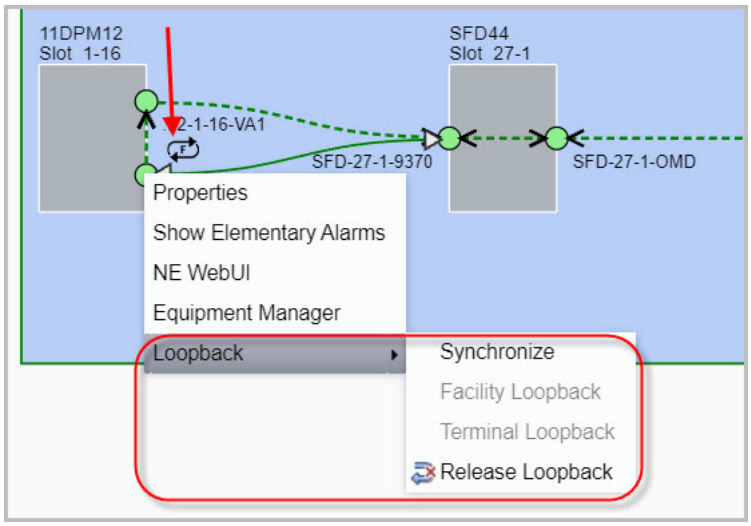
Name	Value
Node Position in NPA	1266
From NE ID	757
To NE ID	757
Channel Number	0
Order ID	9245
A Port	MCS-1-4-AD4
Z Port	4UC400-6-1-4
From NE	[redacted]L1CP-Site1
To NE	[redacted] L1CP-Site1
Src Active	false
Sink Active	false
Direction	Bidirectional
Effective Rate	1GbE
Channel Rate	default
Display LinkState	Unprotected
Orientation	AZ
Link Type	103
sncid	0
State	Local
Shape	N/A
Discrepancy Mark	REGULAR
Fixed Cross Connections	No
Rate	OCH
isSncForSpecialHandling	false
Time Slots	1
timeSlotInUseRate	ODU4
timeSlotInUseConnId	3180

5

The **Loopback Points** field is checked by default. When checked, the loopback icons are displayed near the port in which the option is previously set. The icon displays the direction of the loopback against each port. Moreover, right clicking on the port that supports loopback, you can manage the status of the loopback port, following the commands: **Syncronize**, **Facility Loopback**, **Terminal Loopback**, and **Release Loopback**. See 7.103 “Initiate Facility Loopback Testing on an NE” (p. 1143) to set a loopback port.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-209 Routing Display - Loopback commands



6

The **Collapse Internal links** when checked, allows to hide the XCs packs and relevant connections. The default view of a Node provides a Node view of the connection and a detailed view of the NE, packs, and interconnections between cards. The **Collapse Internal links** checkbox in the Routing Display is auto checked, when **Collapse Internal Links** parameter is enabled in the **Preferences > User > Routing Display tab**. If the **Collapse Internal links** field is checked, then all the internal links are collapsed in the Routing Display. If the **Collapse Internal links** field is unchecked, then all the internal links are expanded and displayed in the Routing Display. See *NFM-T Administration Guide* for more information on the **Preferences > User** tab.

7

The **Highlight TCM Capable Ports** field allows to view the TCM capable ports that are available. TCM can be created either from end ports or intermediate ports through Routing Display. When the **Highlight TCM Capable Ports** checkbox is checked, the **From TCM Port** and **To TCM Port** fields are displayed on the Routing Display. Enter the **From TCM Port** and **To TCM Port** and select **SET TCM PARAMETERS** option to create the TCM from the Routing Display.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-210 Routing Display - Set as To/From TCM Port

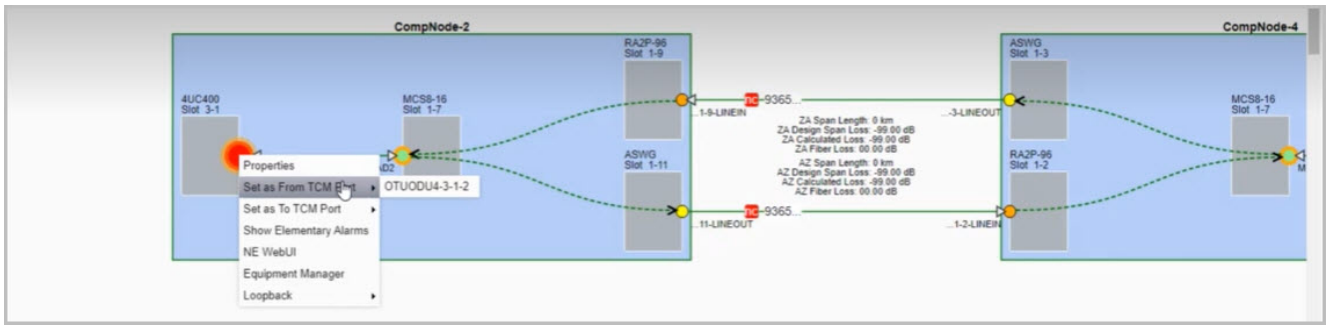
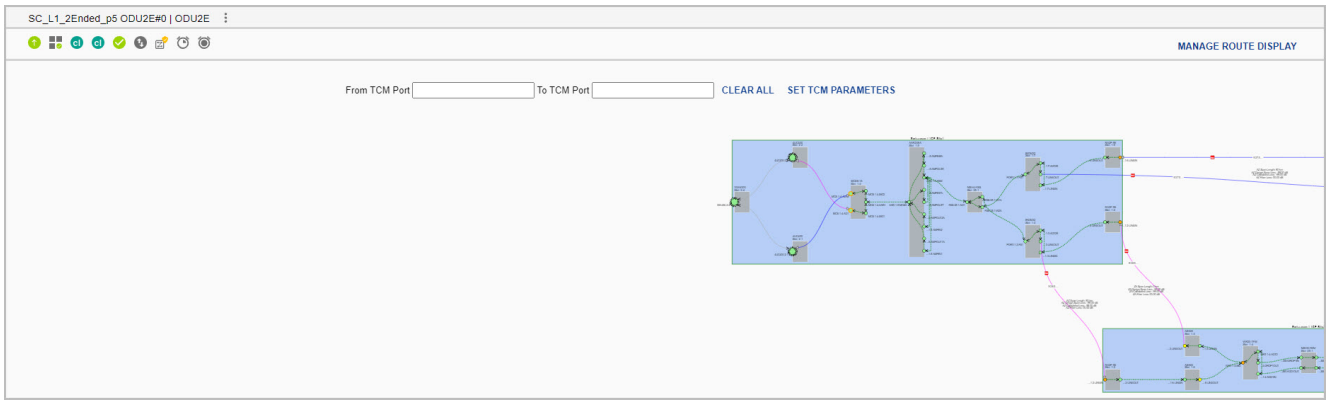


Figure 7-211 Routing Display - set TCM parameters



8

The **WTOCM/DCM** allows to view the WTOCM /DCM packs that are available and provisioned.

9

The **Highlight Layer** allows to highlight a single layer connection for example OTUj or ODUj. Selecting a layer from the drop down menu the layer is highlighted in bold. This option allows to view the termination points of each of the individual layer connections. The default value is *none*.

Selecting a layer, the **Server Name** field is enabled and the server connections are listed in the drop-down menu. Select the server connection to be highlighted on the Routing Display.

10

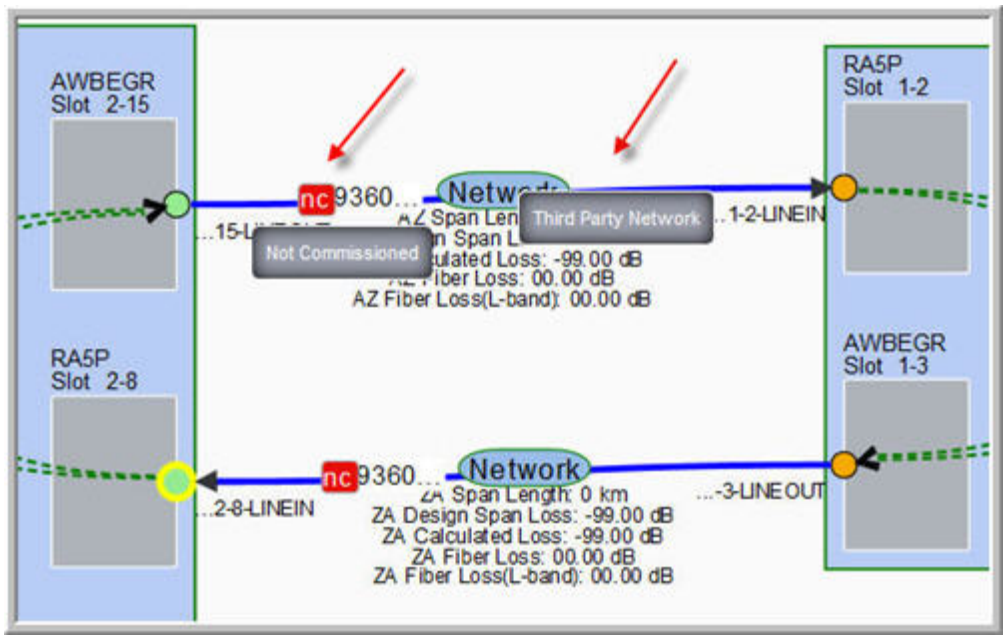
Additionally. Click on the **LEGENDS** panel for an understanding of the end to end routing display symbols. See 24.4 “Quick Help – The Routing Display Window” (p. 1977) for details.

11

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Further information is provided on the status and type of connections using labels. The **Network** label shows when a connection passes through a third-party network, the **nc** label shows a Not Commissioned connection.

Figure 7-212 Routing Display - labels



12

Optionally, right click on the NE in the Routing Display for the following tasks:

Right click actions	Description
Properties	Displays additional parameter information for the selected NE.
Alarms	Opens the **360° View** of the **Nodes** page in another window and the **Alarms** tab is open.
Connections	Opens the **360° View** of the **Nodes** page in another window and the **Used Ports** tab is open.
NE WebUI	Opens the NE ZIC for the selected NE in another window.
Equipment Manager	Displays the NE on the **Equipment Manager** window in another tab.
NE/Node	Displays the **360° View** of the **Nodes** page and opens the **NEs** tab in another window.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Display the Nominal or Current Route of a connection on the Routing Display

Complete the following steps to view the various route displays for a selected infrastructure connection (trail or logical link), a service, the clients and servers of an infrastructure connection, and/or the servers of a service on the Routing Display.

1

From the NFM-T GUI, follow one of these navigation paths:

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

Select the connection for which you want to view the Routing Display, select the routing display icon on the right of the connection row.

OR click on the **More** icon and follow this navigation path: **Routing Display**.

Result: The system opens a new browser tab and the route of the connection is displayed on the Routing Display

3

When the user selects a connection that goes through a *Control Plane* network the Routing Display automatically brings up the full detailed routing display of the current route. The display shows all packs and connections that make up the end to end route, just as is done for *Managed Plane* connections.

The End To End Routing Display might not display internal or photonic cross-connection links for Control Plane connections, when SNC gets re-routed.

Table 7-14 Current and expected behavior for End to End Routing Display in NFM-T R19.9

Scenario (L0 Infrastructure)	Current Route tab	R19.9 expected behavior
No Current Route (Nominal unavailable - Routing Problem, Reroute not possible)	Not available	Internal links with photonic details is displayed in the Nominal Route.
Nominal Route = Current Route (Newly created connection)	Not available	Internal links with photonic details is displayed in the Nominal Route.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-14 Current and expected behavior for End to End Routing Display in NFM-T R19.9 (continued)

Scenario (L0 Infrastructure)	Current Route tab	R19.9 expected behavior
Nominal Route = Current Route (User has modified Nominal Route to match Current Route or performed **Convert Current to Nominal** operation)	Not available	Internal links with photonic details is displayed in the Nominal Route.
Nominal Route ! = Current Route (For existing connections)	Available	Internal links with photonic details will NOT be displayed for Current Route.

4

Nominal route is visualized for all the connections belonging to a *Control Plane*. Both Optical *(Layer 0)* and Electrical *(Layer 1)* are displayed. *Current route* is visualized only for **ODUk** connection at *Layer 0*.

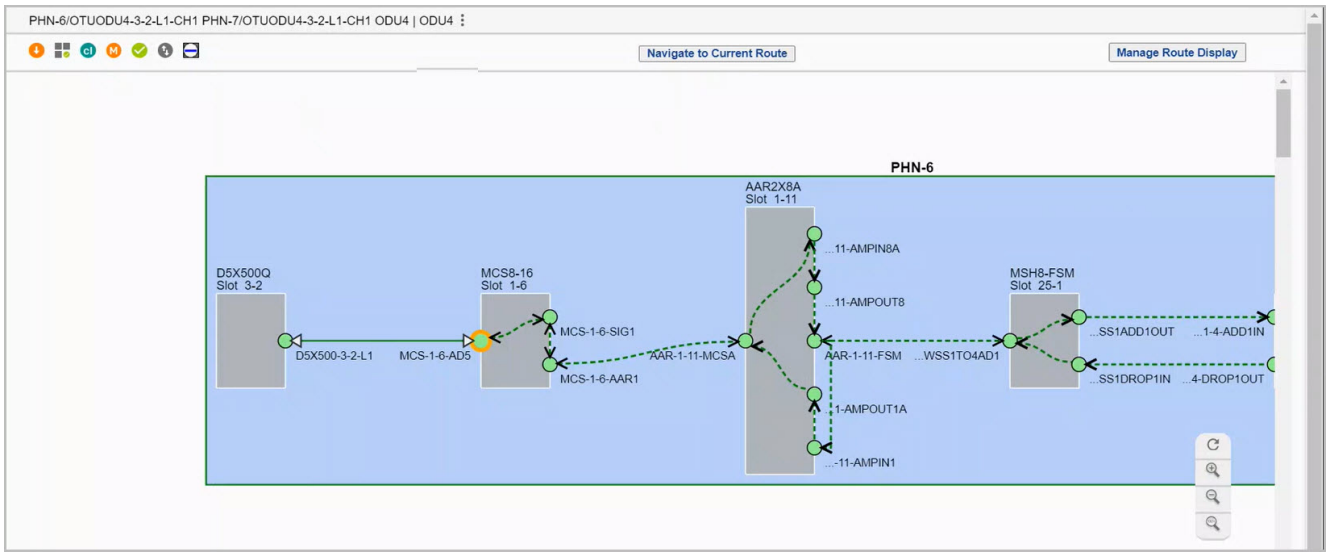
Note: If traffic has switched to a new current route and is no longer following the nominal route, then not all of the original cross-connect information is available on the Route Display for the Nominal Route.

5

Click on the **More** icon on a connection and performing the **Routing Display** command, user can visualize the *Nominal Route* of the connection. To navigate to the *Current Route* select the button on top of the window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-213 Nominal route view



END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.79 Infrastructure Connections columns

Related information

To display the Infrastructure Connections table use the procedure 7.72 "View Infrastructure Connections or Services" (p. 1019).

Each of the data table column can be sorted and filtered, see "Data Tables - React" (p. 2182) and "Sort a single column in a data table" (p. 2187) for details.

For a complete description of the data table and common functions on the data table, see "Data Tables - React" (p. 2182) and "Screens icons" (p. 2241).

Table 7-15 Infrastructure Connections columns description

Column	Description
% Utilization	The **% Utilization** column indicates the percentage of link utilization. It depicts the ratio between the total number of time slots used and the total number of time slots available. Only after the implementation state of the connection is Allocated it is considered for the link utilization calculation. The column can be filtered applying a string filter on the value.
% Utilization Threshold	The **% Utilization Threshold** column indicates the link utilization threshold profile set for the connection. To know more about Link Utilization Profiles, see 22.1 "Link Utilization Profile" (p. 1959). The column can be filtered applying a string filter on the value.
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**. The column can be filtered selecting one or more values.
Alias	The **Alias** displays an alias name that is assigned to the connection. For loopbacks, the **Alias** displays the alias name that is assigned to the connection for which loopbacks have been initiated. See "Connection aliases" (p. 262) If the **Alias** or **Connection Alias** field is left blank, it will be the same as the connection name except for integrated provisioning. For integrated provisioning, the **Alias** will be set to the connection alias of the primary connection. **Note:** The **Alias** is controlled by installation parameters.
Alias 2	The **Alias 2** attribute supports the following: • Text string up to 256 characters, • International character set (for example, circumflex and accents), • UTF-8 encoding. See 7.55 "Manage additional text attribute (Alias) - Infrastructure Connections and Services" (p. 947)
Allow ASON Resources	The **Allow ASON Resources** column displays **Yes** if the managed plane connection uses ASON resources, **No** otherwise. The information is used for the connection creation of HO ODUk trail and ODUk service integrated provisioning of Managed Plane connections. The column can be filtered selecting one of the two values.
ASAP	The **ASAP** displays the Alarm Severity Assignment Profile setting for the connection, which can be **Not Set**, **Enabled**, or **Disable**. The column can be filtered selecting one of the two values.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-15 Infrastructure Connections columns description (continued)

Column	Description
Category	The **Category** of a connection can be **Managed Plane**, **Mixed Plane**, **Control Plane**, **ASON Logical Edge Drop Link**, or **ASON Logical Drop Link**. The NFM-T supports 1830 PSS WDM/photonic and 1830 PSS OCS/switching functions in the Managed Plane, the Control Plane, and the Mixed Plane. The column can be filtered selecting one of the values.
Channel Width	The **Channel Width** column specifies how much bandwidth the connection is using within the available spectrum.
Completion Status	The **Completion Status** displays how the status of the completed operation. The status can be Completed, Failed.
Connection State	For an infrastructure connection or service, the **Connection 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**.
Connection Type	The **Connection Type** field is a drop-down list that displays all available connection type/ shape for the deployed template.
Created By	The **Created By** column displays the entity which created the connection. Possible values are SDH/GMRE, System, System Notify, User.
Created Date	The **Created Date** column displays the date that is associated with the creation of the selected NE.
Customer Name	The **Customer Name** column displays the name of the customer that is assigned to the connection. User-assigned customer names are: **Customer 4**, **Customer 3**, **Customer 2**, **Customer 1**. For auto-discovered connections and system auto-generated connections, the customer name is **None**. **Origin:** Users specify the **Customer Name** in the **Service Description** panel of a template.
Deploy Type	The **Deploy Type** column displays the particular connection request (order). Not all connection requests (orders) support a particular connection. The **Deploy Type** includes the following deployment type indicators: • **Add** indicates that a user has added a new connection to the system. Note that Automatic Routing is only supported for provisioning new connections (**Add** orders). • **Discover** indicates that the system has automatically discovered the connection. • **Delete** indicates that a user has deleted the connection from the system. • **DB Delete** indicates that a user has deleted the connection from the database. • **Reroute** indicates that the connection using a route had to be released, and the connection using the new route was recreated. Reroute is a facet of the Connection Rearrangement feature. • **Reroute with Reinstate** deletes the connection using a route needed to be released, and the connection using the new route was recreated, but the layout of the older connection was stored. During a Reroute with Reinstate, the old route is stored to rollback using the Reinstate. During a Reroute with Reinstate, the original route might cause traffic disruptions. A Reroute is performed on a Reroute with Reinstate order. The older route is purged and the saved time slots are released. Reroute with Reinstate is a facet of the Connection Rearrangement feature. • **Reinstate** indicates that a reroute reverted back 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. Reinstate is a facet of the Connection Rearrangement feature.
Enable NIM	Allows to enable NIM configuration on Infrastructure connections and Services with ODUk service rates. See 7.57 "Manage NIM for a connection" (p. 954). Also allows bulk NIM enabling on multiple connections.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-15 Infrastructure Connections columns description (continued)

Column	Description
Frequency	**Frequency** is a numeric value from **9170** to **9605** in increments of 5 (for example: 9170, 9175, 9180, 9185, ...9600, 9605.) or **N/A** for Wave Keys that are assigned to infrastructures, servers, and clients. For link connections, **Frequency** is only applicable for OCH link connection rates. For rates other than OCH, **NA** is displayed in this field. **Origin:** Users enter **AZ/ZA Wave Key Pairs** in the Wave Key panel when the **Wave Key Assignment** field is **User Selected**. **Note:** When a keyed connection uses Manual Wave Key provisioning users must select the Wave Key values and be aware of the current Wave Key usage in the network to avoid Wave Key collisions. Users must be aware of the Wave Keys assigned by both Manual and Automatic Wave Key assignment since there is a single pool of Wave Key values that is used by both Manual and Automatic assignment.
Frequency Band	The **Frequency Band** column displays a value if the connection manages bandwidth. The value can be 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.
From Node #1 **To Node #1**	The **From Node** and **To Node** columns display the Nodes in which the 2-ended connection originates (**From Node**) and terminates (**To Node**).
From Port #1 **To Port #1**	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**).
Grid Type	
Group Order Name	The Group Order Name column displays the name that is assigned when servers are automatically created, the primary connection (the DSR connection) and the automatically created servers have an automatically assigned group name, which has the format: g-[connection name]
Implementation Status	It displays the implementation status of the connection, for example, **Allocated**, **Fully Allocated**, **Implemented**, **Implementation Failed**, **Partially Allocated**, or **Pending**.
Latest Note	The **Latest Note** column displays the latest note inserted for the selected object.
Line Mode Profile	It indicates the profile number applicable for the OTSig tunnel.
Line Mode Profile Description	It indicates the detailed description of the profile number including the **Payload Rate**, **Baud rate**, and so on.
Name	In general, **Name** is a string of alphanumeric characters that represents the name of the connection, which users supply during connection provisioning in the **Service Definition** panel of a template. The format of the **Name** is controlled by installation parameters. For a link connection, the **Name** is blank if the link connection is not used by a connection that is in the **Implementation Complete** or a **Commissioned** state. For loopbacks, the **Connection Name** is a string of alphanumeric characters that represents the name of the connection for which loopbacks have been initiated.
NPA Name	The **NPA Name** column displays the name of NPA to which a OMS/ODU/DSR is a member or a client of a NPA member. The column is not shown in primary inventory list but can be added customizing the table. The column can be used for filtering the connections on the NPA name. See 26.2 "Data table description" (p. 2182) for details on the data tables. **Note**: If a Connection crosses more than one NPA and if the user filters on one NPA in the list, then the filtered list shows only the NPA used in the filter for that connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-15 Infrastructure Connections columns description (continued)

Column	Description
OLC State	Indicates the OLC (Object Life Cycle) state of the selected infrastructure connection or service. 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 an infrastructure connection or a service, and hence suppress the display of alarms on the infrastructure connection or service that are in maintenance state. See 2.21 "Object Life Cycle (OLC) state" (p. 243) for more information.
OMSP Connection Name	OMSP stands for Optical Multiplex Section Protection and is the protection that protects both, optical amplifiers and transmission fibers. This is the name of the connection with OMSP protection.
Operational State	The **Operational** column (for logical connections) or the **Operational State** column (for SNCs) displays whether the connection is up (in service) or down (out-of-service). Information is displayed in icon format. The **Operational** is an up (green) or down (black) arrow. See "Operational state" (p. 241)
PM 15M and PM 24H	The **PM 15M** and **PM 24H** columns display whether 15 minute and/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). The column displays an icon that identifies the status of the PM on that connection. If it is empty the PM is not enabled, otherwise it can be Started or Start Failed or Stop Failed. **Origin:** Users specify whether 15-minute and/or 24-hour PM data should be collected during connection provisioning in the template **Assurance** panel.
Protection	For logical connections, the **Protection** column displays whether the particular connection is **Unprotected**, **Protected**, or **Segment Protected**. The **Protection** column is not applicable for physical connections. For ASON SNCs, the **Protection** column displays whether the protection method for the subnetwork connection is **D&C SNCP**, **In Rings**, **None**, or **SNCP**.
Rate	The **Rate** column displays the rate of the connection. **Origin:** Users supply the **Service Rate** during connection provisioning in the template **Service Definition** panel. For services this is the **Service Rate** field and for infrastructure connections, this is displayed as the **Rate** field.
Reversion Control Group	Specifies the Reversion Control Group that is associated to the SNC.
Scheduled Jobs	Description of scheduled Jobs.
Server Alarm Status	The **Server Alarm Status column** displays whether the server is alarmed and the severity of the alarm. The **Alarm Synthesis** is: **Minor**, **Critical**, **Major**, or **Cleared**.
Service Name	The **Server Name** column displays the name of the server in a format that combines the NE Name/Port Name/Port Name/Server Rate. For connections without servers, this field is **NA**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-15 Infrastructure Connections columns description (continued)

Column	Description
Service State	The **Service State** is displayed for infrastructure connections and services. The meaning of the **Service State** column differs for infrastructure connections and services. For logical connections, the **Service State** is based on the values of the alarm reporting parameter of the connection endpoints. If all connection endpoints 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 endpoint 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 involved in the endpoints of an infrastructure connection or service are in **Maintenance** state, the connection or service is also in **Maintenance** state. Changing the **Primary State** of an OTUk or ODUk facility on the NE WebUI effects the **Service State** of the corresponding connection or service too. In addition, determinations other than the connection endpoint 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. For an infrastructure connection or service, the **Service State** column displays whether the connection is **Not in Service**, **In Service**, or **Maintenance**.
TCM Enabled	The **TCM Enabled** column displays whether Tandem Connection Monitoring is **Enable**, **NA** (not applicable), or **None**.
Type	For a logical connection, the **Type** column displays whether the connection is a **Service** (service), **Infrastructure** (infrastructure trail), or **Logical Link** (infrastructure logical link). **Origin:** When users select an Infrastructure Connection or Service template they determinate the connection type. In addition, when users select an Infrastructure template and they check the **Logical Link** box in the **Service Definition** panel, they further define the connection type.
TCM ASAP Enabled	The **TCM ASAP Enabled** column displays whether the Tandem Connection Monitoring (TCM) Alarm Severity Assignment Profile is set to **Enable**, **NA** (not applicable), or **None**.
Wave Key	The **Wave Key** column displays, depending on the template/connection type, the Wave Key field is displayed as drop-down list. Values are **Keyed (the default), UnKeyed (Manual), UnKeyed (Auto) or N/A**. The Wave Key column depicts if connection is using wave keys or not.
5G Tributary Size	The **5G Tributary Size** column indicates that the ODUflex is of 5G time slot. The supported values are: • **True**: Applicable for ODUflex connections which is autocreated after 400G service creation. This field is supported for DFM6, DFM6E, and S5AD400H 400G services only. • **N/A**: If the ODUflex is not of 5G timeslot, the **5G Tributary Size** column remains empty or N/A. By default **5G Tributary Size** is not enabled in the UI. To enable **5G Tributary Size**, click **MANAGE COLUMNS** and select **5G TRIBUTARY SIZE** check box and click **APPLY**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.80 Services columns

Related information

To display the Services table use the procedure 7.72 "View Infrastructure Connections or Services" (p. 1019)

Each of the data table column can be sorted and filtered, see "Data Tables - React" (p. 2182) and "Sort a single column in a data table" (p. 2187) for details.

For the complete description of the data table, common functions on the data table, the icons see "Data Tables - React" (p. 2182) and "Screens icons" (p. 2241)

Table 7-16 Services columns description

Column	Description
Actual Latency-PROTECT (microsec)	The computed protected latency in microseconds. Specifies the last successful Latency Measurement (as per user request) on the Protected leg for a protected service
Actual Latency-WORK (microsec)	The computed working latency in microseconds. Specifies the last successful Latency Measurement (as per user request) on the on the Working (Main) for a protected service.
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**.
Alias	The **Alias** displays an alias name that is assigned to the connection. For loopbacks, the **Alias** displays the alias name that is assigned to the connection for which loopbacks have been initiated. See "Connection aliases" (p. 262) If the **Alias** or **Connection Alias** field is left blank, it will be the same as the connection name except for integrated provisioning. For integrated provisioning, the **Alias** will be set to the connection alias of the primary connection. **Note:** The **Alias** is controlled by installation parameters.
Alias 2	The **Alias 2** attribute supports the following: • Text string up to 256 characters, • International character set (for example, circumflex and accents), • UTF-8 encoding. See 7.55 "Manage additional text attribute (Alias) - Infrastructure Connections and Services" (p. 947)
Allow ASON Resources	The **Allow ASON Resources** column displays **Yes** if the managed plane connection uses ASON resources, **No** otherwise. The information is used for the connection creation of HO ODUk trail and ODUk service integrated provisioning of Managed Plane connections.
ASAP	The **ASAP** displays the Alarm Severity Assignment Profile setting for the connection, which can be **Not Set**, **Enabled**, or **Disable**.
Category	The **Category** of a connection can be **Managed Plane**, **Mixed Plane**, **Control Plane**, **ASON Logical Edge Drop Link**, or **ASON Logical Drop Link**. The NFM-T supports 1830 PSS WDM/photonic and 1830 PSS OCS/switching functions in the Managed Plane, the Control Plane, and the Mixed Plane.
Channel Width	The **Channel Width** displays the assigned channel width for the service. The value can be 50Ghz, 62.5Ghz or 75Ghz. The value is assigned at deploy time if the template deployed is an Alien Wavelength template. The channel width value selection is supported only on ENEs or PHN nodes.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-16 Services columns description (continued)

Column	Description
Completion Status	The **Completion Status** displays how the status of the completed operation. The status can be Completed, Failed.
Connection State	For an infrastructure connection or service, the **Connection 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**.
Connection Type	It indicates the type of connection such as physical link.
Created Date	The **Creation Date** column displays the date that is associated with the creation of the selected NE.
Customer	The **Customer** column displays the name of the customer that is assigned to the connection. User-assigned customer names are: **Customer 4**, **Customer 3**, **Customer 2**, **Customer 1**. For auto-discovered connections and system auto-generated connections, the customer name is **None**. **Origin:** Users specify the **Customer Name** in the **Service Description** panel of a template.
Deploy Type	The **Deploy Type** column displays the particular connection request (order). Not all connection requests (orders) support a particular connection. The **Deploy Type** includes the following deployment type indicators: • **Add** indicates that a user has added a new connection to the system. Note that Automatic Routing is only supported for provisioning new connections (**Add** orders). • **Discover** indicates that the system has automatically discovered the connection. • **Delete** indicates that a user has deleted the connection from the system. • **DB Delete** indicates that a user has deleted the connection from the database. • **Reroute** indicates that the connection using a route had to be released, and the connection using the new route was recreated. Reroute is a facet of the Connection Rearrangement feature. • **Reroute with Reinstate** deletes the connection using a route needed to be released, and the connection using the new route was recreated, but the layout of the older connection was stored. During a Reroute with Reinstate, the old route is stored to rollback using the Reinstate. During a Reroute with Reinstate, the original route might cause traffic disruptions. A Reroute is performed on a Reroute with Reinstate order. The older route is purged and the saved time slots are released. Reroute with Reinstate is a facet of the Connection Rearrangement feature. • **Reinstate** indicates that a reroute reverted back 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. Reinstate is a facet of the Connection Rearrangement feature.
Enable NIM	Allows to enable NIM configuration on Infrastructure connections and Services with ODUk service rates. See 7.57 "Manage NIM for a connection" (p. 954). Also allows bulk NIM enabling on multiple connections.
From Node #1 **To Node #1**	The **From Node** and **To Node** columns display the Nodes in which the 2-ended connection originates (**From Node**) and terminates (**To Node**). The columns can be filtered, the filter is a text filter on the node name string.
From Port #1 **To Port #1**	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**).
Group Order Name	The Group Order Name column displays the name that is assigned when servers are automatically created, the primary connection (the DSR connection) and the automatically created servers have an automatically assigned group name, which has the format: g-[connection name]
Implementation Status	It displays the implementation status of the connection, for example, **Allocated**, **Fully Allocated**, **Implemented**, **Implementation Failed**, **Partially Allocated**, or **Pending**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-16 Services columns description (continued)

Column	Description
Latency Status	Specifies the actually reporting about the last user request for Service Latency measurement. The supported values are: • SUCCESS: Delay Measurement test is successful • NOT COMPUTED: Delay Measurement is not yet triggered on the particular service • DMF (Delay Measurement Failure): Delay measurement test is failed on the particular service • NOT SUPPORTED: Delay measurement is not supported n the pack The user can view any failure of the service latency in the NFM-T Jobs page.
Latency Timestamp	The time at which the **Compute Latency** operation was executed on the Network Element NFM-T displays the Timestamp value sent by the Network Element after the time zone conversion.
Latest Note	The **Latest Note** column displays the latest note inserted for the selected object. The **Operational** is an up (green) or down (black) arrow. See 24.9 "Manage Note for a Selected Object" (p. 2002)
Name	In general, **Name** is a string of alphanumeric characters that represents the name of the connection, which users supply during connection provisioning in the **Service Definition** panel of a template. The format of the **Name** is controlled by installation parameters. For a link connection, the **Name** is blank if the link connection is not used by a connection that is in the **Implementation Complete** or a **Commissioned** state. For loopbacks, the **Connection Name** is a string of alphanumeric characters that represents the name of the connection for which loopbacks have been initiated.
NPA Name	The **NPA Name** column displays the name of NPA to which a OMS/ODU/DSR is a member or a client of a NPA member. The column is not shown in primary inventory list but can be added customizing the table. The column can be used for filtering the connections on the NPA name. See 26.2 "Data table description" (p. 2182) for details on the data tables. **Note**: If a Connection crosses more than one NPA and if the user filters on one NPA in the list, then the filtered list shows only the NPA used in the filter for that connection.
OLC State	Indicates the OLC (Object Life Cycle) state of the selected infrastructure connection or service. 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 an infrastructure connection or a service, and hence suppress the display of alarms on the infrastructure connection or service that are in maintenance state. See 2.21 "Object Life Cycle (OLC) state" (p. 243) for more information.
Operational State	The **Operational** column (for logical connections) or the **Operational State** column (for SNCs) displays whether the connection is up (in service) or down (out-of-service). Information is displayed in icon format. The **Operational** is an up (green) or down (black) arrow. See "Operational state" (p. 241)
PM 15M and PM 24H	The **PM 15M** and **PM 24H** columns display whether 15 minute and/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). The column displays an icon that identifies the status of the PM on that connection. If it is empty the PM is not enabled, otherwise it can be Started or Start Failed or Stop Failed. **Origin:** Users specify whether 15-minute and/or 24-hour PM data should be collected during connection provisioning in the template **Assurance** panel.
Protection	For logical connections, the **Protection** column displays whether the particular connection is **Unprotected**, **Protected**, or **Segment Protected**. The **Protection** column is not applicable for physical connections. For ASON SNCs, the **Protection** column displays whether the protection method for the subnetwork connection is **D&C SNCP**, **In Rings**, **None**, or **SNCP**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-16 Services columns description (continued)

Column	Description
Rate	The **Rate** column displays the rate of the connection. **Origin:** Users supply the **Service Rate** during connection provisioning in the template **Service Definition** panel. For services and infrastructure connections, this field is the **Rate** field.
Scheduled Jobs	Show the number of Jobs in the **Scheduled Status**
Server Alarm Status	The **Server Alarm Status column** displays whether the server is alarmed and the severity of the alarm. The **Alarm Synthesis** is: **Minor**, **Critical**, **Major**, or **Cleared**.
Service Name	The **Server Name** column displays the name of the server in a format that combines the NE Name/Port Name/Port Name/Server Rate. For connections without servers, this field is **NA**.
Service State	The **Service State** is displayed for infrastructure connections and services. The meaning of the **Service State** column differs for infrastructure connections and services. For logical connections, the **Service State** is based on the values of the alarm reporting parameter of the connection endpoints. If all connection endpoints 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 endpoint 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 involved in the endpoints of an infrastructure connection or service are in **Maintenance** state, the connection or service is also in **Maintenance** state. Changing the **Primary State** of an OTUk or ODUk facility on the NE WebUI effects the **Service State** of the corresponding connection or service too. 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. For an infrastructure connection or service, the **Service State** column displays whether the connection is **Not in Service**, **In Service**, or **Maintenance**. Service connection's Service State is changed to **Maintenance** when loopback is performed on the end ports of the service. Loopback performed on the Line ports does not change the service connection's Service State.
Type	For a logical connection, the **Type** column displays whether the connection is a **Service** (service), **Infrastructure** (infrastructure trail), or **Logical Link** (infrastructure logical link). **Origin:** When users select an Infrastructure Connection or Service template they determinate the connection type. In addition, when users select an Infrastructure template and they check the **Logical Link** box in the **Service Definition** panel, they further define the connection type.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.81 Infrastructure Connections list further actions

Introduction

Users can select an item in a data table, click on the **More** icon on the right of the item row, and view a list of additional actions for that item.

Note: The selection of available actions depends on the type of the item selected.

Table 7-17 Actions for Infrastructure Connections

Menu item	Second level menu item	Description
Display on Map	Highlight on Map	Displays a new browser tab with only the selected connection highlighted. See 7.77 "View various route displays for an infrastructure connection or service" (p. 1036)
	Route at Physical Layer	Displays a new browser tab with the physical layer of the connection highlighted. See 7.77 "View various route displays for an infrastructure connection or service" (p. 1036)
	Route at all Layers (all Depths)	Displays a new network map tab with the physical layer of the connection highlighted and the **HIGHLIGHT ROUTE** panel for the selection. Depth of each element is displayed on **HIGHLIGHT ROUTE** panel. The depth layer selected to navigate from is at the top of the list layers displayed. See 7.77 "View various route displays for an infrastructure connection or service" (p. 1036)
	Route at all Layers (all Depths) - Legacy	Displays a new network map tab with the selected route highlighted in the legacy display of network map.
Routing Display		The Routing Display is a high level vision of the connection which allows to display the connection on the maps and connection details. Additionally, the Routing Display, allows user to display the packs involved in the connection, internal links, physical links including optical lines according with the considered connection. The port alarms displayed, are alarms that may exist at physical layer or at any of the corresponding service or infrastructure layers. **Note**: The system visualizes the graphical view only of the commissioned connections. See 7.78 "View the Routing Display of a selected connection " (p. 1042)
Optical Power	**Bidirectional Optical Power...**	Displays the bidirectional optical power window. See 17.13 "Optical power visualization" (p. 1818) and 17.14 "Manage optical power of an OTN OTS connection" (p. 1846).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-17 Actions for Infrastructure Connections (continued)

Menu item	Second level menu item	Description
Modify Connection	**Connection and Customer Name ...**	Displays the rename connection window to rename the selected connection. See 7.64 "Rename Connection and Customer Name" (p. 997)
	Parameters	Displays the connection modification window in a new browser tab. See 7.62 "Modify the parameters of a connection" (p. 981)
	Reroute ...	Displays the connection modification window in a new browser tab. See , 7.62 "Modify the parameters of a connection" (p. 981) and 7.63 "Modify Route (Reroute) of a connection" (p. 987) **Note**: Modification of the connection route and modification of the connection parameters should be done in two separate requests.
	Modify Utilization Profile	Allows to modify the link utilization profile for the connection. This is not applicable for OMS, ODUj, and ODUk connections. See 7.38 "Modify Utilization Profile for a physical/infrastructure connection" (p. 881) for more information. See 22.1 "Link Utilization Profile" (p. 1959), to know more about Link Utilization Profiles.
Rename Connection		Displays the rename connection window to rename the selected connection. See 7.64 "Rename Connection and Customer Name" (p. 997)
Enable NIM		Allows to enable NIM configuration on Infrastructure connections and Services with ODUk service rates. See 7.57 "Manage NIM for a connection" (p. 954). Also allows bulk NIM enabling on multiple connections.
Disable NIM		Allows to disable NIM configuration on Infrastructure connections and Services with ODUk service rates. See 7.57 "Manage NIM for a connection" (p. 954). Also allows bulk NIM disabling on multiple connections.
Alarms	**Enable Alarm Profile**	This action is based on the connection rate and the role of the port. 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. See 7.53 "Manage alarms for a connection" (p. 924)
	Disable Alarm Reporting	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 **None** for disabled case, **NA** (Not Applicable). for *Set Default ASAP* case. • The connection rate must be one of the following: OTU1, OTU2, OTU3, ODU1, ODU2, ODU3, DSR, STMnRS, or OCnRS **Note**: No alarms are reported by the NE for this connection until *Enable Alarm Profile* is selected. See 7.53 "Manage alarms for a connection" (p. 924)
	Set Default ASAP	This action allows to restore the alarm severities to NE/Node defaults through ASAP. See "Task: Set Default ASAP" (p. 933)
Create Network Data File		Displays the Network Data Files window, to create a new file. See 20.2 "Network data files description" (p. 1932).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-17 Actions for Infrastructure Connections (continued)

Menu item	Second level menu item	Description
Delete Connection		Allows to delete a connection, the operation can be traffic impacting, so a confirmation box is displayed to confirm the operation. See 7.51 "Delete a commissioned connection" (p. 919)
Delete Connection and Clients		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.
Deployment Control	Allocate, Implement, Deimplement, Commission (In Service), Complete Stop, Complete Order, Abort Order Processing, Move Forward One Command Set, Move Backward One Command Set, Delete from NFM-T	The available deployment actions depend on the connection selected and its state. See 7.49 "Control the deployment of a connection" (p. 915) for information about single deployment action,
Jobs		Displays the Jobs page with the connection related jobs and job's information. See 7.71 "View Jobs for an infrastructure connection or service" (p. 1016)
Add Note		This function allows the users to add a note or comment to a selected infrastructure or service. See 24.9 "Manage Note for a Selected Object" (p. 2002).
	Modify PM	Menu item enabled if the performance monitoring is enabled on the connection. It displays the PM modification window in a new browser tab. See 7.53 "Manage alarms for a connection" (p. 924).
	Clear PM Bin	The Clear PM Bin operation is used to reset the current PM counter bins. The Clear PM Bin operation is applicable to all the Infrastructure connections and Services, irrespective of the 15-min or 24-hr PM being enabled. The Clear PM Bin option will be disabled, if PM is not supported. See Manage PM for a Connection in the *NFM-T Service Assurance Guide*.
OA&M Diagnostics		The system opens a new browser tab and displays the OA&M Diagnostics window. The window has the traditional NFM-T 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 Perform PM-Related OA&M Diagnostics on a Connection in the *NFM-T Service Assurance Guide*
OLC State		Allows the user to configure the OLC State of the selected infrastructure connection or service to **Maintenance** or **In Service**. See 2.21 "Object Life Cycle (OLC) state" (p. 243).
Correlate ASAP		Allows to correlate an ASAP to the connection. See "Task: Correlate a commissioned connection to an ASAP" (p. 925)
Schedule Job		Opens the ASON Reversion job window and allows to create a job for the selected connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-17 Actions for Infrastructure Connections (continued)

Menu item	Second level menu item	Description
Bulk Modify PM	Enable/Disable	Allows to enable/disable Modify PM option on multiple Infrastructure connections and Services. See Bulk Modify PM Settings for multiple Infrastructure Connections and Services. Not supported for OMS Service types.
Structure		Displays the structure window fro the selected connection. See 25.53 "Structure Tab" (p. 2167)
Timeline		Timeline displays the activities and additional information of a selected object. It resembles a social media timeline of activities that are performed on the NEs and connections pages of NFM-T. See 24.10 "Manage Timeline" (p. 2009).
Route Details		Displays the full route details in a new window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.82 Services list further actions

Introduction

Users can select an item in a data table, click on the **More** icon on the right of the item row, and view a list of additional actions for that item.

Note: The selection of available actions depends on the type of the item selected.

Table 7-18 Actions for Services

Menu Item	Second Level Menu Item	Description
Display on Map	Highlight on Map	Displays a new browser tab with only the selected service highlighted. See 7.77 "View various route displays for an infrastructure connection or service" (p. 1036)
	Route at Physical Layer	Displays a new browser tab with the physical layer of the service highlighted. See 7.77 "View various route displays for an infrastructure connection or service" (p. 1036)
	Route at all Layers (all Depths)	Displays a new network map tab with the physical layer of the service highlighted and the **HIGHLIGHT ROUTE** panel for the selection. Depth of each element is displayed on **HIGHLIGHT ROUTE** panel. The depth layer selected to navigate from is at the top of the list layers displayed. See 7.77 "View various route displays for an infrastructure connection or service" (p. 1036)
	Route at all Layers (all Depths) - Legacy	Displays a new network map tab with the selected route highlighted in the legacy display of network map.
Routing Display		The Routing Display is a high level vision of the connection which allows to display the connection on the maps and connection details. Additionally, the Routing Display, allows the user to display the packs involved in the connection, internal links, physical links including optical lines according with the considered connection. The port alarms displayed, are alarms that may exist at physical layer or at any of the corresponding service or infrastructure layers. **Note**: The system visualizes the graphical view only of the commissioned connections. See 7.78 "View the Routing Display of a selected connection " (p. 1042)
Optical Power	**Bidirectional Optical Power...**	Displays the bidirectional optical power window. See 17.13 "Optical power visualization" (p. 1818) and 17.14 "Manage optical power of an OTN OTS connection" (p. 1846).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-18 Actions for Services (continued)

Menu Item	Second Level Menu Item	Description
Modify Connection	**Connection and Customer Name ...**	Displays the rename connection window to rename the selected connection. See
	Parameters	Displays the connection modification window in a new browser tab. See
	Reroute ...	Displays the connection modification window in a new browser tab. See 7.62 "Modify the parameters of a connection" (p. 981) and 7.63 "Modify Route (Reroute) of a connection" (p. 987) **Note**: Modification of the connection route and modification of the connection parameters should be done in two separate requests.
	Modify Utilization Profile	Allows to modify the link utilization profile for the connection. This is not applicable for OMS, ODUj, and ODUk connections. See 7.38 "Modify Utilization Profile for a physical/infrastructure connection" (p. 881) for more information. See 22.1 "Link Utilization Profile" (p. 1959), to know more about Link Utilization Profiles.
Clone Connection		It replicates the properties of the existing service.
Alarms	**Enable Alarm Profile**	This action is based on the connection rate and the role of the port. 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. See 7.53 "Manage alarms for a connection" (p. 924)
	Disable Alarm Reporting	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 **None** for disabled case, **NA** (Not Applicable). for *Set Default ASAP* case. • The connection rate must be one of the following: OTU1, OTU2, OTU3, ODU1, ODU2, ODU3, DSR, STMnRS, or OCnRS **Note**: No alarms are reported by the NE for this connection until *Enable Alarm Profile* is selected. See 7.53 "Manage alarms for a connection" (p. 924)
	Set Default ASAP	This action allows to restore the alarm severities to NE/Node defaults through ASAP. See "Task: Set Default ASAP" (p. 933)
Create Network Data File		Displays the Network Data Files window, to create a new file. See 20.2 "Network data files description" (p. 1932).
Delete Connection		Allows to delete a connection, the operation can be time consuming, hence a confirmation box is displayed to confirm the operation. See 7.51 "Delete a commissioned connection" (p. 919)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-18 Actions for Services (continued)

Menu Item	Second Level Menu Item	Description
Deployment Control	Allocate, Implement, Deimplement, Commission (In Service), Complete Stop, Complete Order, Abort Order Processing, Move Forward One Command Set, Move Backward One Command Set, Delete from NFM-T	The available deployment actions depend on the connection selected and its state. See 7.49 "Control the deployment of a connection" (p. 915) for information about single deployment action,
Jobs		Displays the Jobs page with the connection related jobs and job's information. See 7.71 "View Jobs for an infrastructure connection or service" (p. 1016)
Add Note		This function allows the users to add a note or comment to a selected infrastructure or service. See 24.9 "Manage Note for a Selected Object" (p. 2002).
	Modify PM	Menu item enabled if the performance monitoring is enabled on the connection. It displays the PM modification window in a new browser tab. See 7.53 "Manage alarms for a connection" (p. 924).
	Clear PM Bin	The Clear PM Bin operation is used to reset the current PM counter bins. The Clear PM Bin operation is applicable to all the Infrastructure connections and Services, irrespective of the 15-min or 24-hr PM being enabled. The Clear PM Bin option will be disabled, if PM is not supported. See Manage PM for a Connection in the *NFM-T Service Assurance Guide*.
OA&M Diagnostics		The system opens a new browser tab and displays the OA&M Diagnostics window. The window has the traditional NFM-T 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 Perform PM-Related OA&M Diagnostics on a Connection in the *NFM-T Service Assurance Guide*
Service State	In Service (IS) Out of Service (OOS) Automatic In Service (AINS)	Allows to change the Service state. An error message is displayed if the operation cannot be fulfilled.
OLC State	**Set to Maintenance...**	Allows the user to configure the OLC State of the selected infrastructure conenction ot service to **Maintenance** or **In Service**. See 2.21 "Object Life Cycle (OLC) state" (p. 243).
Correlate ASAP		Allows to correlate an ASAP to the connection. See "Task: Correlate a commissioned connection to an ASAP" (p. 925)
Schedule Job		Opens the ASON Reversion job window and allows to create a job for the selected connection.
Bulk Modify PM	Enable/Disable	Allows to enable/disable Modify PM option on multiple Infrastructure connections and Services. See Bulk Modify PM Settings for multiple Infrastructure Connections and Services. Not supported for OMS Service types.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-18 Actions for Services (continued)

Menu Item	Second Level Menu Item	Description
Timeline		Timeline displays the activities and additional information of a selected object. It resembles a social media timeline of activities that are performed on the NEs and connections pages of NFM-T. See 24.10 "Manage Timeline" (p. 2009).
Compute Latency		Computes the amount of time taken by a signal in traveling from the AEnd to the ZEnd for a service. **Note:** The **Compute Latency** function is only available for NE R11.1 or greater. 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). The supported cards are: • D5X500Q, S13X100R/E, 11DPM8, 11QPA4B, 12P120, 20MX80, 30AN300, 4AN400, 10AN10GC, 1AN100G, 20P200, 8P20, 1UD200, PSD R1.1 • S6AD600H from 1830 PSS PHN NE R14.0 • S5AD400H from 1830 PSS PHN NE R14.0 • SFM6 from 1830 PSI-M NE R6.0.8 Latency can be computed for no more than ten services at a time. The success/failure of the Compute Latency operation is logged in the Jobs page and User Activity Log.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.83 Resize ODUFlex Bandwidth

Introduction

The ODUflex adjustment provides the capability to size the bandwidth to a desired rate. This feature allows user to select a flexible rate client service connection and resize the bandwidth from the NFM-T GUI as a single operation.

As part of the resize operation, the user can increase or decrease the bandwidth. This procedure avoids the deletion and recreation of ODUflex services connections. The increase and decrease bandwidth imply a change in the time slot of the related services connections.

The bandwidth adjustment is applicable to existing route only. When increasing the bandwidth, if the current route cannot accommodate the wider bandwidth the request will fail and an error message will be displayed.

The Resize ODUflex Bandwidth is applicable on ODUFlex clients with GFP-F Encapsulation Mode.

The Resize ODUflex Bandwidth is applicable for Managed Plane, Control Plane, and Mixed Plane connections.

In Managed Plane, the ODUflex Bandwidth Resize operation is performed on the ODUj server connection from infrastructure connection list.

For mixed plane connections where the ODUflex connection is in the control plane, the ODUflex Bandwidth Resize operation is performed on the DSR client connection from service connection list.

Note:

- For protected managed plane connections with more than one ODUflex server (for example, Y-cable or OPSB protected), the user must resize the bandwidth on each ODUj server connection independently.
- For protected mixed plane connections with more than one ODUflex server (for example, Y-cable or OPSB protected), resizing the ODUflex bandwidth on the service connection resizes the bandwidth of all ODUflex servers.
- Y-cable or OPSB protected not supported for mixed plane and for end to end protected connection resize will on service layer for mixed plane(where 2 unprotected SNC present)

Bandwidth adjustment is applicable only with end points and connection route containing the supported NE/pack types mentioned in “Supported cards” (p. 1072).

During resize operation, alarms raised by NE are displayed in NFM-T, under the OLCS MT category.

Impact on the L2 services

This feature helps to check and validate the presence of Ethernet (L2) clients on top of the ODUFlex connections (DSR). For a given DSR, when bandwidth decrease operation is in progress, then the L2 service creation/modification is not allowed for L2 services using the same DSR.

When an Ethernet (L2) client connection is present, increase bandwidth is allowed. If ODUFlex is in progress during Ethernet service modification or creation, then an error message is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

When an Ethernet (L2) client is present, decrease bandwidth is allowed if the CIR of the Ethernet client connection is less than or equal to the decreased bandwidth.

ODUflex resize is not supported for L2 packs present in ASON domain.

Supported cards

Resize ODUFlex Bandwidth is supported in 1830 PSS and 1830 PSD Network Elements.

The following 1830 PSS cards supports Resize ODUFlex Bandwidth as end packs

- 4AN400
- 10AN1T
- 10AN400
- 4MX200
- 30AN300
- 20AN80
- 20AX200
- 20MX80
- 30SE300
- 6SE300
- 5MX500
- 20P200
- S13X100R

The following cards supports Resize ODUFlex Band width within the route.

- 4AN400
- 10AN1T
- 10AN400
- 4MX200
- 30AN300
- 20AN80
- 20AX200
- 20MX80
- 2UC400/2UC400E
- 4UC400
- 8UCIT
- 1UX100
- 2UX200
- 5MX500

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Before you begin

- To minimize the service interruption time when resizing a connection with SNCP protection, the connection should have the working path as the active path.
- As part of the resize request of an SNCP protected connection, NFM-T will lockout protection before executing the resize and will clear the protection switch after the resize is complete.
- A force lockout of protection is required because resizing an SNCP protected configuration will cause transient protection switch conditions and may not preserve the previous selector positions. When the protection path is the active path, the service interruption period will be longer as there will be a service interruption when the force lockout of protection is performed.
- As part of resize for packet switch configuration, create a packet switch card with uplink and packet cards. If the Equipment Manager window, If BP1 is empty or ILKN, the user can use slot 1 to slot 20 for oduflex connection. If BP1 is OTL4.10, slots 11 to 20 are applicable.

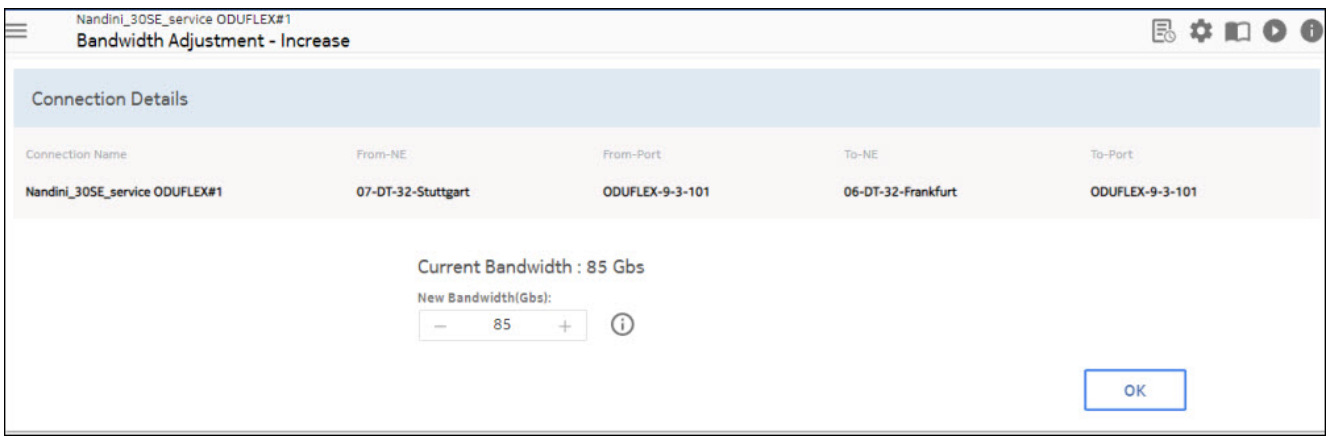
Bandwidth Adjustment window

The **Bandwidth Adjustment - Increase** or **Bandwidth Adjustment - Decrease** window displays the current bandwidth that is set during the creation of ODUflex connection or service. Click the plus or minus icon in the **New Bandwidth (Gbs)** field to increase or decrease the bandwidth.

The **Bandwidth Adjustment - Increase** page provides an option to increase the bandwidth by clicking the plus icon. **Bandwidth Adjustment - Decrease** provides an option to decrease the bandwidth by clicking the minus icon.

The valid values are 1.25 to 18.75 Gbs where the granularity increases or decreases by a default value of 1.25 Gbs. The maximum valid values are based on the selected end ports.

Figure 7-214 Bandwidth Adjustment - Managed Plane



Parameter	Description
Connection Name	Specifies the name of the connection or service
From-NE	Specifies the NE on the A end

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Parameter	Description
From-Port	Specifies the port on the A end
To-NE	Specifies the NE on the z end
To-Port	Specifies the port on the z end
Current Bandwidth	Specifies the current bandwidth that is set during the creation of ODUflex service or connection. The user can set the new bandwidth in the **New Bandwidth (Gbs)** field. The Increase bandwidth window allows only to increase the bandwidth and the Decrease Bandwidth window allows to decrease the bandwidth. The user cannot increase or decrease the bandwidth from the same window at the same time.

When increasing the bandwidth of an ODUflex service or connection for each channelized end port, the user must select the correct number of time slots based on the increased ODUflex bandwidth (for example, if the ODUflex bandwidth is increased from 1.25 Gbs to 2.5Gbs then two time slots must be selected for each channelized end port) or the resize will fail.

When decreasing the bandwidth of an ODUflex service or connection, the user is not required to select timeslots for each channelized end port because the system will choose which time slots to remove.

When increasing the bandwidth, if one or more connection endpoint is channelized, the **Bandwidth Adjustment** window displays additional parameters. This is application only for Managed Plane and Control Plane connections.

Note:

- The resize bandwidth operation fails if there is an inconsistent connection associated to it.
- Failure of the resize bandwidth operation will auto rollback and set the connection back to the original bandwidth using a cancel request. If the cancel fails, the order remains in implementation failed state.
- Resize is not allowed if the ODUflex connection is an inconsistent connection.
- Resize is not allowed if any Network Element in the route does not support the resize operation.
- Resize is not allowed if any pack in the route does not support the resize operation
- Resize is only allowed for ODUflex connections using GFP encapsulation.
- For Control Plane connections, resize maintains the current route. When increasing the bandwidth if the current route does not have sufficient capacity the resize will fail.
- For Control Plane connections, resize is not allowed if ASON SNC is in Rerouted state.
- When an Ethernet (L2) client is present, decrease bandwidth is not allowed if the CIR of the Ethernet client connection is less than or equal to the decreased bandwidth. An error message will be displayed indicating that the Service Level Agreement (SLA) would be violated.
- The Network Element automatically adjusts the value of Burst Threshold as part of the resize operation and NFM-T will reset the connection value of the transmission parameter to “Use NE Values”. After the resize is complete, the user can perform a modify parameters request to adjust the value if needed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Resize is not supported when TCM is enabled on the connection. The user must remove the TCM enabled on the service , perform resize and enable the TCM.
- Resize is not supported when Test Mode is enabled on ASON SNC. The user must disable the Test Mode, perform resize and enable test mode
- Resize is supported from R14.0 GMRE active release version for Control Plane connections

ODUFlex Bandwidth Adjustment for the ODUj and ODUk connections

Complete the following steps to adjust the ODUFlex bandwidth on a Managed Plane, Control Plane or Mixed Plane connection

ODUFlex Bandwidth Adjustment for Managed Plane connection

1

From the NFM-T GUI, follow one of the navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services > SERVERS(tab)

Result: The list of infrastructure connections are displayed.

2

Click **MANAGE COLUMNS** icon on the top right corner to manage the columns in data table. See 7.66 “Manage Columns on Infrastructure Connections page” (p. 1004) for more details.

Result: The system displays **Manage Column** page.

3

Select **CREATED BY** from the list of **DEFAULT COLUMNS** and click **APPLY & SAVE**.

Select System to create system created connections so that the ODUflex connections are included in the list

4

Select or sort the connection with **CREATED BY** as **System** and with the **Rate** as **ODUflex**

5

Select or sort the connection with the **Rate** as **ODUflex** , click the **More** icon and select **Modify Connection > Increase Bandwidth** or **Modify Connection > Decrease Bandwidth**.

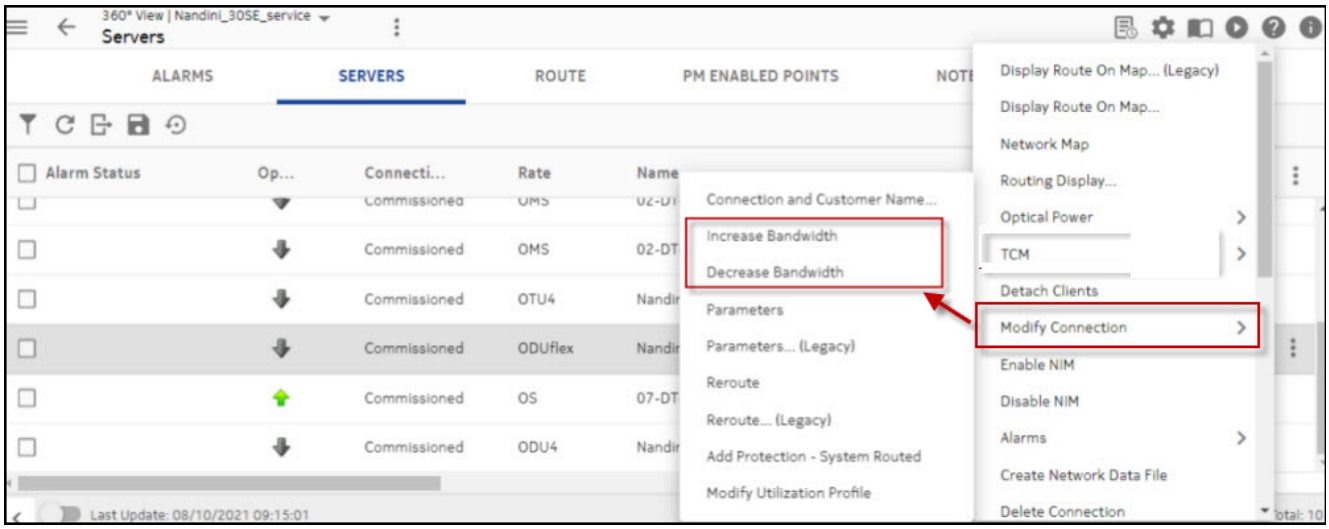
The **Increase Bandwidth** or **Decrease Bandwidth** option is enabled if

- the connection rate is ODUflex for Managed Plane connections
- the immediate client connection of the ODUflex connection is a Flexible Rate Client
- ASON Routed is unchecked for Managed Plane connection

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Protection is checked for protected connections and services.
- all endpoints are on one of the pack types listed below or are on an ENE connected to one of the pack types listed
- the connection is in *Commissioned* state.

Figure 7-215 **Increase Bandwidth** or **Decrease Bandwidth** for Managed Plane connections



Result: Bandwidth Adjustment - Increase or **Bandwidth Adjustment - Decrease** window is displayed. To know more about these windows, see "Bandwidth Adjustment window" (p. 1073).

6

Increase or decrease the bandwidth and click **OK**.

Result: A confirmation message is displayed indicating the connection is moved to *Commissioned*.

The **Rate** column in the Infrastructure Connections page is appended with the currently bandwidth that is set.

Navigate to **OPERATE > Infrastructure connections > 360° View > LINK CONNECTIONS (tab)** which displays the number of ODU0 time slots that is occupied. You can view the ODU0 time slots from the **Structure** window.

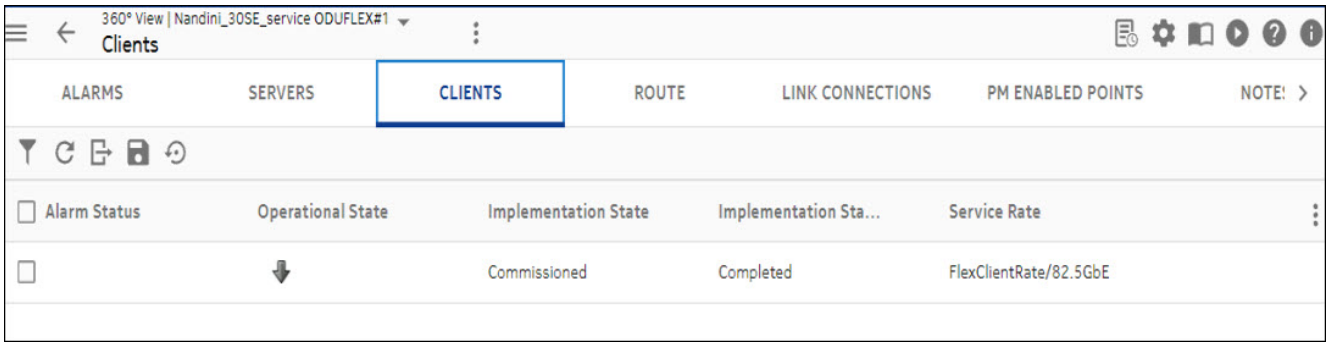
7

Navigate to the **Clients** tab of the associated connection to view the services with the associated bandwidth. To view the Ethernet level view, navigate to **OPERATE > Ethernet Service Manager**.

For more information, see *NFM-T Ethernet Services Manager Guide*.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-216 Clients tab with Flex Client Rate



ODUflex Bandwidth for Control Plane and Mixed Plane connection

8

From the NFM-T GUI, follow one of the navigation paths:

OPERATE > Services

Result: The list of services are displayed.

9

Click **MANAGE COLUMNS** icon on the top right corner to manage the columns in data table. See 7.66 "Manage Columns on Infrastructure Connections page" (p. 1004) for more details.

Result: The system displays **Manage Columns** page.

10

Select **Category** and **Deploy Type** from the list of **DEFAULT COLUMNS** and click **APPLY & SAVE**.

11

Navigate to **OPERATE > ASON > SNCs**. Select a connection, click the **360° View** icon, and **ROUTES** tab

Result: The Nominal and Current routes are displayed. Ensure that the time slot of **Nominal Route** is equal to the time slot of the **Current Route** for that particular ODUk service.

12

Select or sort the connection with the **Rate** as **FlexibleClientRate**, click the **More** and select **Modify Connection > Increase Bandwidth** or **Modify Connection > Decrease Bandwidth**.

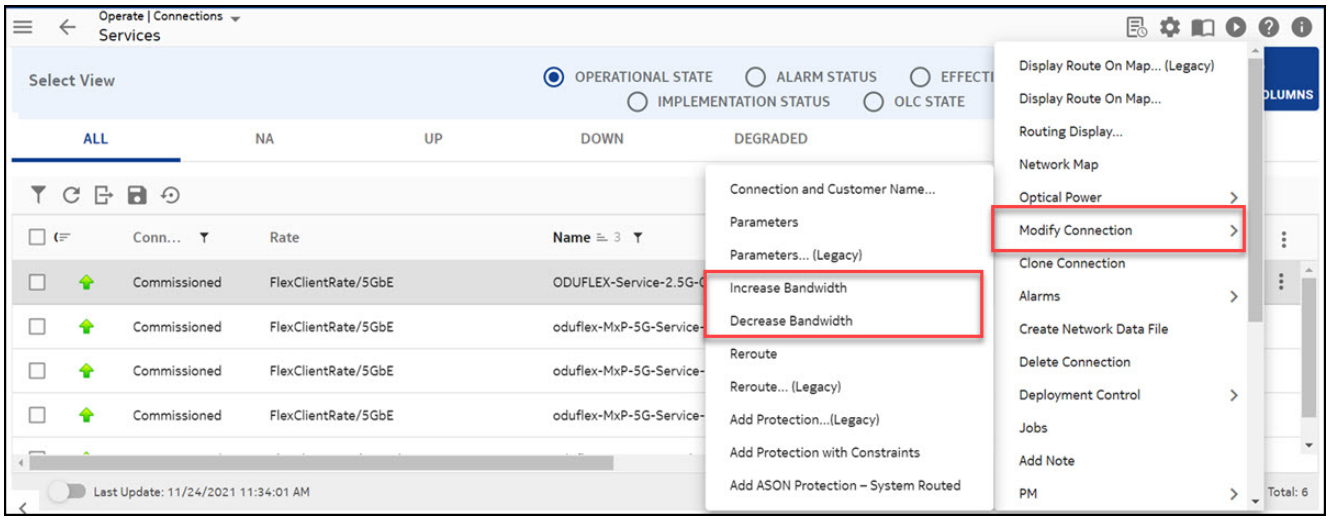
The **Increase Bandwidth** or **Decrease Bandwidth** option is enabled if

- the connection rate is **FlexibleClientRate** for Control and Mixed Plane connections

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- ASON Routed is checked for Control Plane connection
- Protection is checked for protected connections and services.
- all endpoints are on one of the pack types listed below or are on an ENE connected to one of the pack types listed
- the connection is in *Commissioned* state.

Figure 7-217 **Increase Bandwidth** or **Decrease Bandwidth** for Control Plane connections



Result: The **Bandwidth Adjustment - Increase** or **Bandwidth Adjustment - Decrease** window is displayed. To know more about the **Bandwidth Adjustment** window, see "Bandwidth Adjustment window" (p. 1073).

13

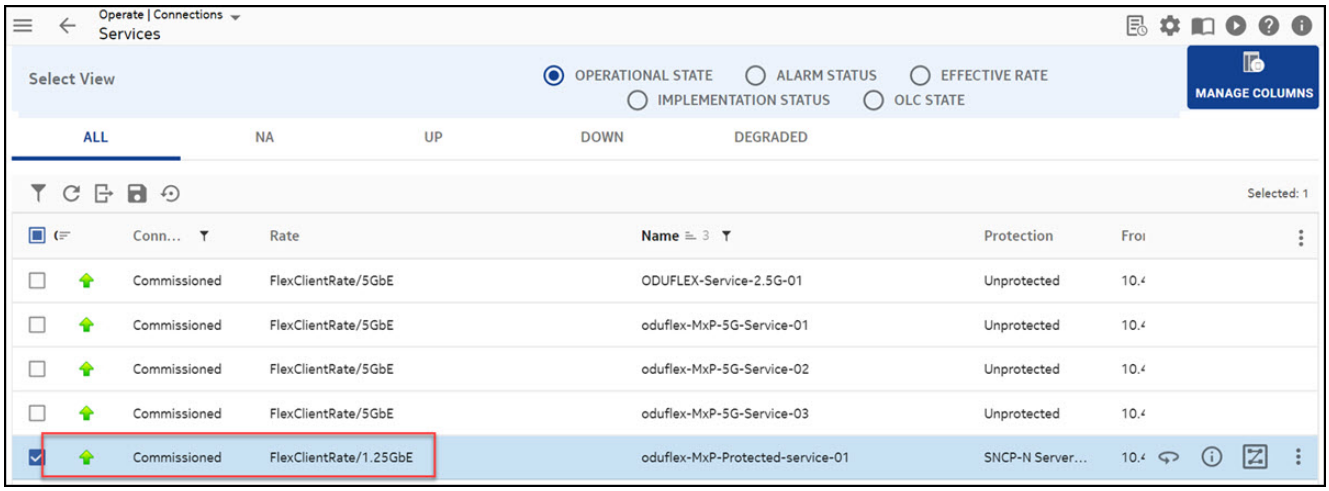
Increase or decrease the bandwidth and click **OK**.

Result: A confirmation message is displayed indicating the connection is moved to *Commissioned*.

The **Rate** column in the Services page is appended with the currently bandwidth that is set.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-218 Rate after Decrease Bandwidth operation



14

For Control Plane connections, navigate to the **OPERATE > ASON SNCs**

The Configuration State is moved to Implemented and Working State to Normal.

15

Select the connection and click the **360° View** icon. Select **ROUTES** tab and check the time slots.

The current route will be equal to nominal route.

When increasing the bandwidth if the current route does not have sufficient capacity the resize will fail.

16

To verify the change in time slots during ODUflex bandwidth, click the **Open link** icon, **360° View > Client ASON SNCs** or **Client ASON SNCs - Structure**.

The ODUFlex resize functionality in Control Plane is not supported for 1830 PSS OCS NEs.

In case of SNCP/PRC SNC , user has to reconfigure SNC as Unprotected source based restoration or guaranteed restoration before executing the ODUflex resize.

This feature is not supported for 3-ended and for 4-ended SNCs.

A new alarm Rate Mismatch is raised for ODUFlex resize.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

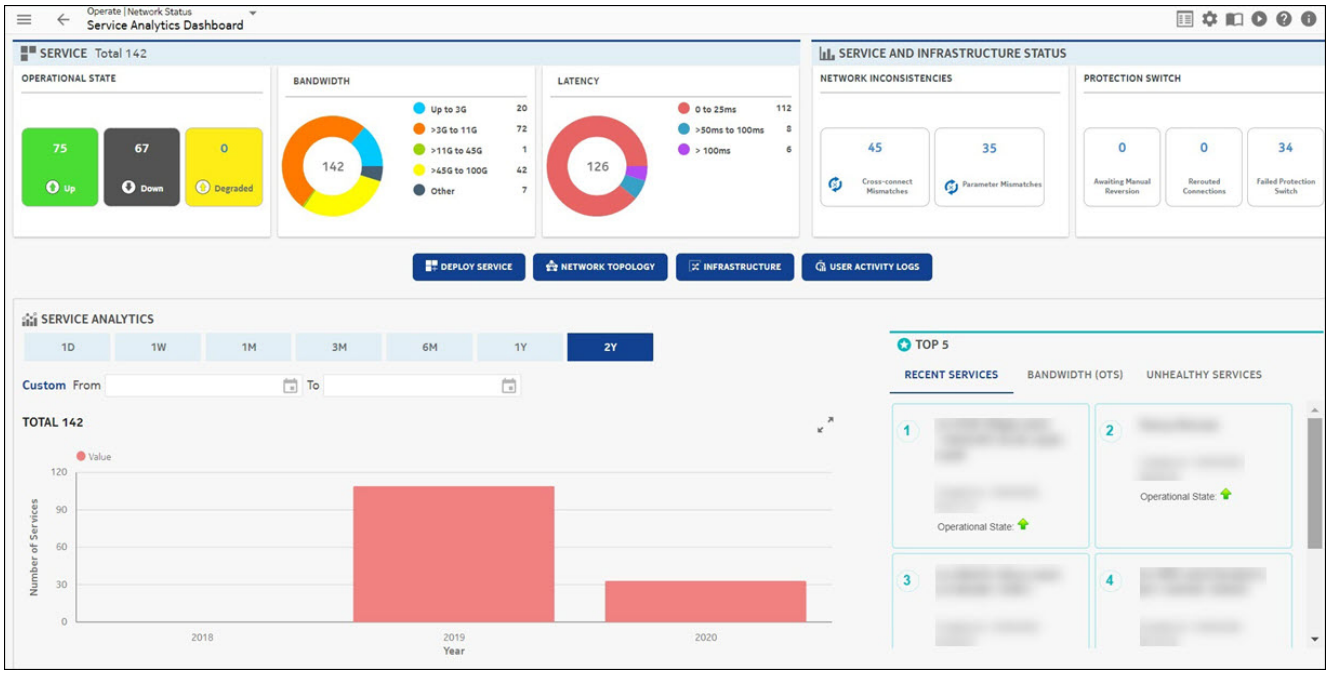
7.84 Service Analytics Dashboard

Overview

The Service Analytics Dashboard provides a summary of services fulfilled, service health, service fulfilment analytics, and infrastructure and physical connections information. To view the Service Analytics Dashboard, from the NFM-T GUI, navigate to **OPERATE > Network Status > Service Analytics Dashboard** .

Figure 7-219, “Service Analytics Dashboard” (p. 1080) shows the Service Analytics Dashboard.

Figure 7-219 Service Analytics Dashboard



Service

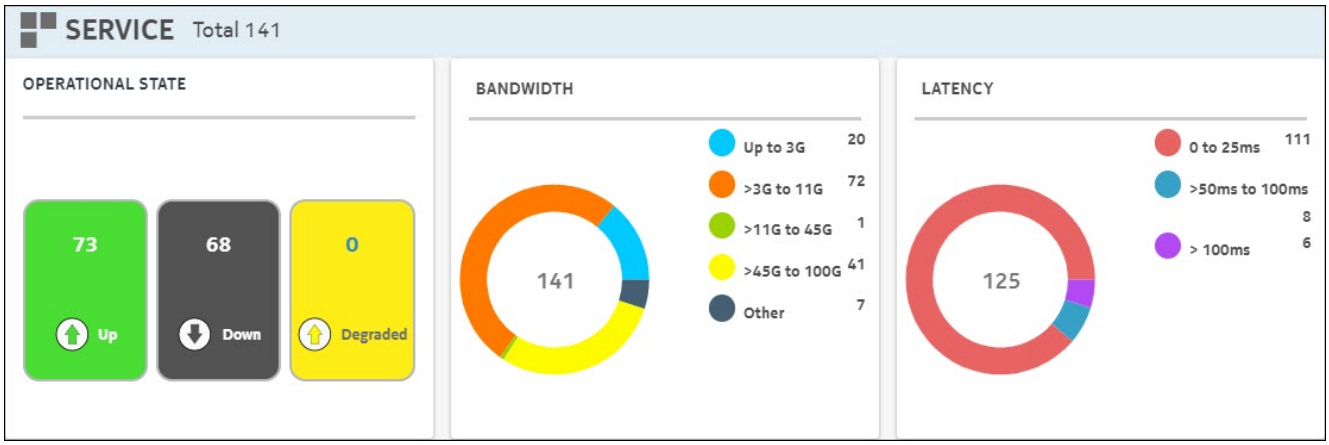
The **SERVICE** panel of the dashboard shows the summary of Operational State, Bandwidth, and Latency.

The **SERVICE** panel of the dashboard provides the number of services that are in a **Commissioned** state from the **OPERATE > Services** list. Total in the title bar indicates the total number of services that are in the **Commissioned** state. Click **Total** to navigate to the **Services** that are in **Commissioned** state.

Figure 7-220, “Service” (p. 1081) shows the **SERVICE** panel of the Service Analytics Dashboard.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-220 Service



Operational state

The **OPERATIONAL STATE** panel categorizes the services that are in **Commissioned** state by the Operational state values **UP**, **DOWN**, and **DEGRADED**. Click the icons to navigate to the list of services that are in **UP**, **DOWN**, and **DEGRADED** state respectively.

Bandwidth

The **BANDWIDTH** panel categorizes the services in **Commissioned** state by the service rate. This is represented using a donut chart and a total count of services is available at the center of the donut chart. Click the various categories available next to the donut chart to navigate to the **OPERATE > Services** list. The services list is filtered by the service rates in the interval represented by the segment of the chart. The **Other** category shows the count of services where the service rate is not available.

Table 7-19, “Bandwidth rate grouping” (p. 71) indicates the rate grouping for various rates.

Table 7-19 Bandwidth rate grouping

Group	Rate
Up to 3G	1GbE, FE, STM-16, STM-16MS, OC-48, STM-4, STM-4MS, OC-12, STM-1, STM-1MS, OC-3, FC200, FC100, FlexClientRate/(1.25GbE, 2.5GbE), ODU1, ODU0, HDSDI, SDSDI, 3GSDI, DVBASI, CBR2G5
>3G to 11G	10GbE, STM-64, STM-64MS, OC-192, FC1200, FC800, FC400, FlexClientRate/(3.75GbE, 5GbE, 6.25GbE, 7.5GbE, 8.75GbE,10.0GbE), ODU2E, ODU2

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-19 Bandwidth rate grouping (continued)

Group	Rate
>11G to 45G	40GbE, STM-256, OC-768, FlexClientRate/ 40GbE, ODU3E2, ODU3, FC1600
>45G to 100G	100GbE, ODU4
>100G	400G, 200G
Other	OMS, OCH, OCHT, ODUflex, DSR, DDR

Latency

The **LATENCY** panel categorizes the services that are in **Commissioned** state by latency using a donut chart and provides a total count at the center of the donut chart. This is an on-demand based latency for a limited set of cards. For a service, latency value is the sum of the delays for all the ODU supporting the service. Click the various categories available next to the donut chart to navigate to the services with latency within the specified range. Latency is available on terminated ODU paths with interworking source and destination cards that support Latency and Delay Measurements (DM).

Following are the **LATENCY** grouping categories:

- **0 to 25 ms**
- **> 25 to 50 ms**
- **> 50 to 100 ms**
- **> 100 ms**

Note: The dashboard panel for Operational State, Bandwidth, Latency, Network Inconsistencies, and Protection Switch is updated every 15 minutes to reflect recent data.

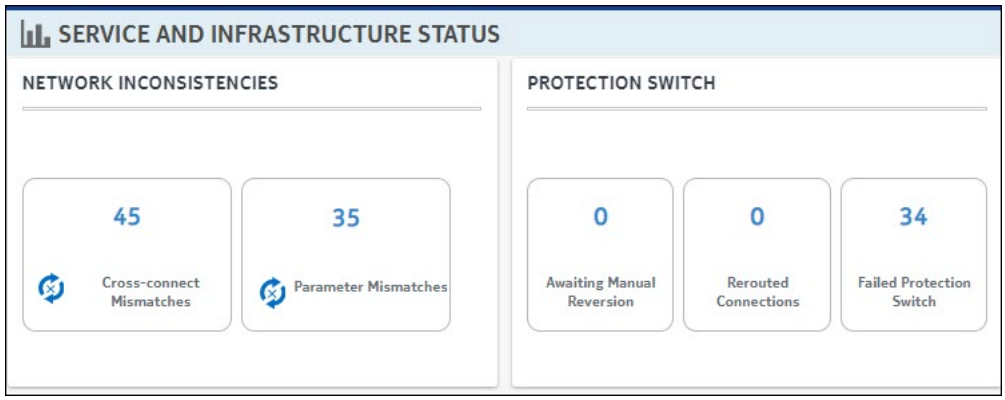
Service and infrastructure status

The **SERVICE AND INFRASTRUCTURE STATUS** panel of the dashboard provides the summary of Network Inconsistencies and Protection Switch.

Figure 7-221, “Service and infrastructure status” (p. 1083) shows the **SERVICE AND INFRASTRUCTURE STATUS** section of the Service Analytics Dashboard.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-221 Service and infrastructure status



Network inconsistencies

The **NETWORK INCONSISTENCIES** panel categorizes services and infrastructure connections by **Cross-Connect Mismatches** and **Parameter Mismatches**. Click **Cross-Connect Mismatches** or **Parameter Mismatches** to navigate to the **Network Inconsistencies** window and view the list of services and infrastructure that are not in sync with the network due to missing SNC cross-connects and mismatched parameters, respectively.

Protection switch

The **PROTECTION SWITCH** panel categorizes services and infrastructure connections by the **Awaiting Manual Reversion**, **Rerouted Connections**, and **Failed Protection Switch** status.

Table 7-20, “Protection switch category” (p. 73) indicates the **PROTECTION SWITCH** categories and provides the filters used to define the categories.

Table 7-20 Protection switch category

Category	Navigation path
Awaiting Manual Reversion	Navigates to **OPERATE > Protected Connections** where the connections listed have the values: • Revertive Mode: Manual • Active Route: Protection • Alarm Status: Clear
Rerouted Connections	Navigates to **OPERATE > Protected Connections** where the connections listed have the value - Active Route: Protection

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-20 Protection switch category (continued)

Category	Navigation path
Failed Protection Switch	Navigates to **OPERATE > Protected Connections** where the connections listed have the value - Operational State: Down

Navigation Buttons

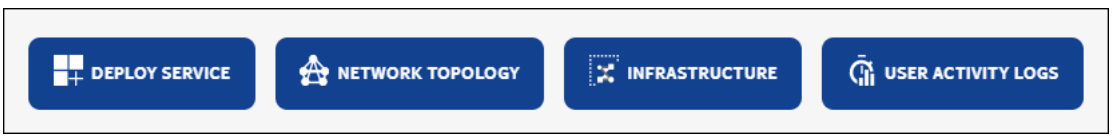
The **Navigation Buttons** panel of the dashboard shows the navigation buttons for the **DEPLOY SERVICE**, **NETWORK TOPOLOGY**, **INFRASTRUCTURE**, and **USER ACTIVITY LOGS**.

Table 7-21 Navigation Buttons

Navigation Button	Destination
DEPLOY SERVICE	Navigates to the **DEPLOY > New Service/Infrastructure Connection** template window.
NETWORK TOPOLOGY	Navigates to the **OPERATE > Network Map** page.
INFRASTRUCTURE	Navigates to the **OPERATE > Infrastructure Connections** page.
USER ACTIVITY LOGS	Navigates to the **ADMINISTER > All Records** page.

Figure 7-222, “Navigation Buttons” (p. 1084) shows the **Navigation Buttons** section of the Service Analytics Dashboard.

Figure 7-222 **Navigation Buttons**



Service Analytics

The **SERVICE ANALYTICS** panel of the dashboard provides service fulfilment history. The data in the bar chart refers to the services that are in **Commissioned** state. Select a bar from the bar chart to navigate to a list of connections created during the time interval specified by the bar. The data is retrieved from the **Services** page of the NFM-T and filtered by created date. Hover over the cursor on any specific bar to view the total number of services on the bar. The total number of services for the selected time duration is displayed at the top of the chart on the left hand side.

The granularity on the X-axis depends on the selection such as 1D, 1W, 1M, and so on. See Table 7-22, “Time Period and X-axis Representation” (p. 97) for more details.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

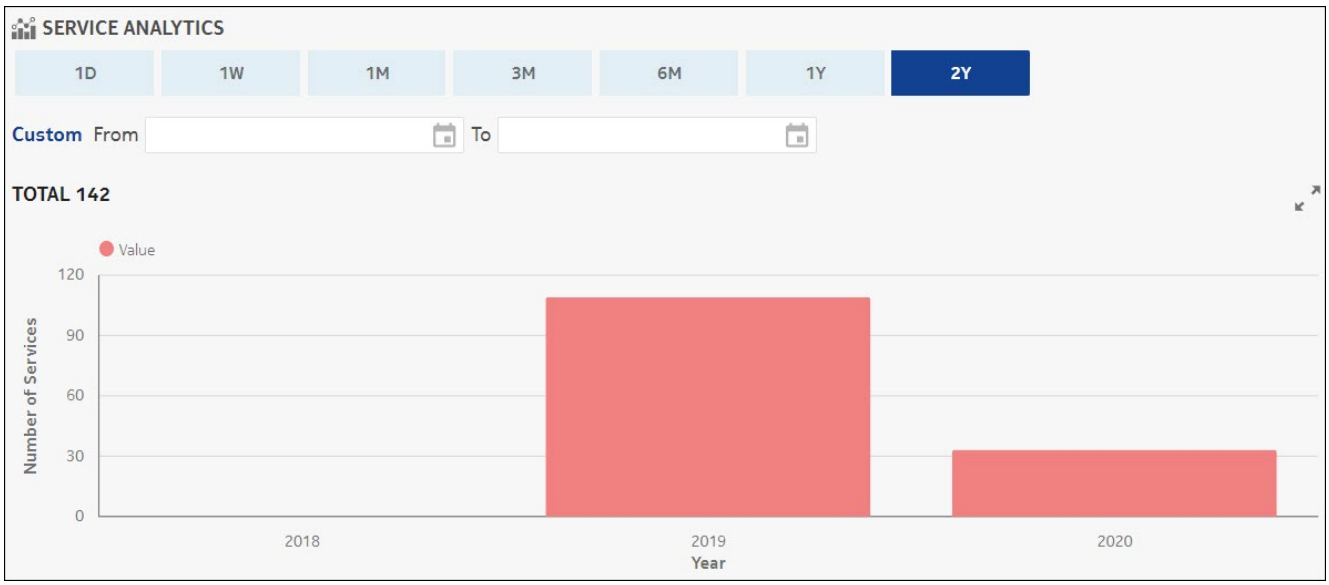
A user has the flexibility to customize the selection using the **Custom** option and specify the **From** and **To** date.

Table 7-22 Time Period and X-axis Representation

Time period	X-axis representation
1D	Per hour basis
1W	Per day basis
1M	Per day basis
3M and above	Per week basis
1Y and above	Per month basis
2Y and above	Per year basis

Figure 7-223, “Service Analytics” (p. 1085) shows the **SERVICE ANALYTICS** section of the Service Analytics Dashboard.

Figure 7-223 Service Analytics



Note: The dashboard panel for Service Analytics panel refreshes when the user selects the items to view.

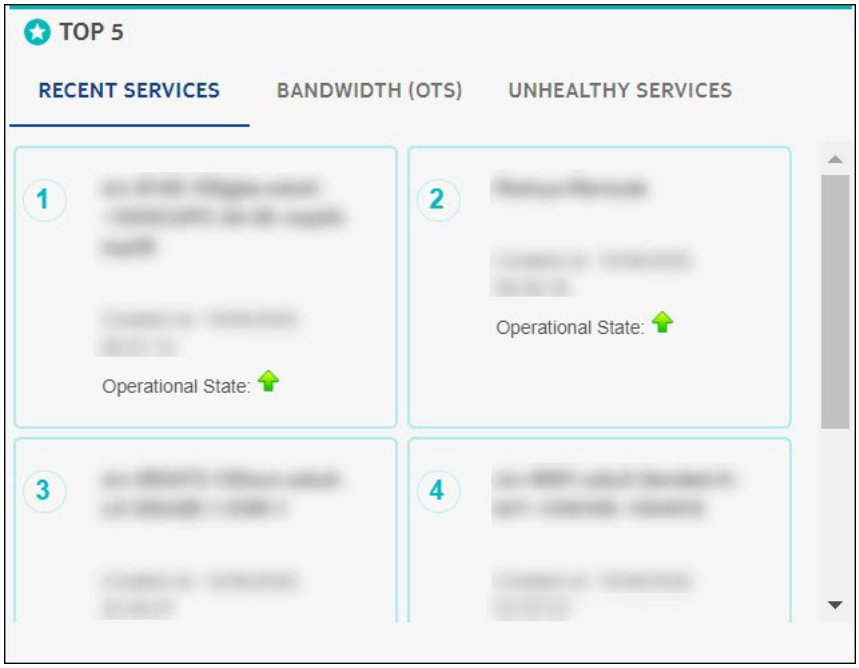
Top 5

The **TOP 5** panel of the dashboard provides the list of top five **RECENT SERVICES**, **BANDWIDTH (OTS)**, and **UNHEALTHY SERVICES**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

The following figure shows the **TOP 5** section of the Service Analytics Dashboard.

Figure 7-224 Top 5



Recent Services

The **RECENT SERVICES** tab provides a rolling list of the top five recently created services in a **Commissioned** state from the **OPERATE > Services** list. Click the panel to view the details of the service and navigate to the 360^0 View for that service.

Bandwidth (OTS)

The **BANDWIDTH (OTS)** tab provides a list of the top five physical connections with the highest bandwidth utilization. These physical connections indicates the availability in the network when the user tries to provision a service. Click the panel to navigate to the **Bandwidth Utilization Report** filtered for the top five connections.

Note: As a prerequisite for **BANDWIDTH (OTS)**, a utilization threshold must be set for the physical connections.

Unhealthy services

The **UNHEALTHY SERVICES** tab provides a list of top five unhealthy services that are in a **Commissioned** state. Unhealthy Services is measured as the number of times a service has Operational State as **DOWN** over a fixed period of time for example, 30 days. Click the panel to view the details of the service and navigate to the 360^0 View of the service.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: The dashboard panel for Top 5 panel refreshes when the user selects the items to view.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Protected Connections

7.85 Manage Protected Connections

Purpose

Use this task to manage a selected protected connection.

When an infrastructure connection is selected in the Protected Connection List the NFM-T GUI enables users to perform the same actions from the **OPERATE > Protected Connections** navigation path as it does from the **OPERATE > Infrastructure Connections** path.

When a service connection is selected in the Protected Connection List the NFM-T GUI enables users to perform the same actions from the **OPERATE > Protected Connections** navigation path as it does from the **OPERATE > Service Connections** path.

Task

Complete the following step to manage a selected protected connection.

1

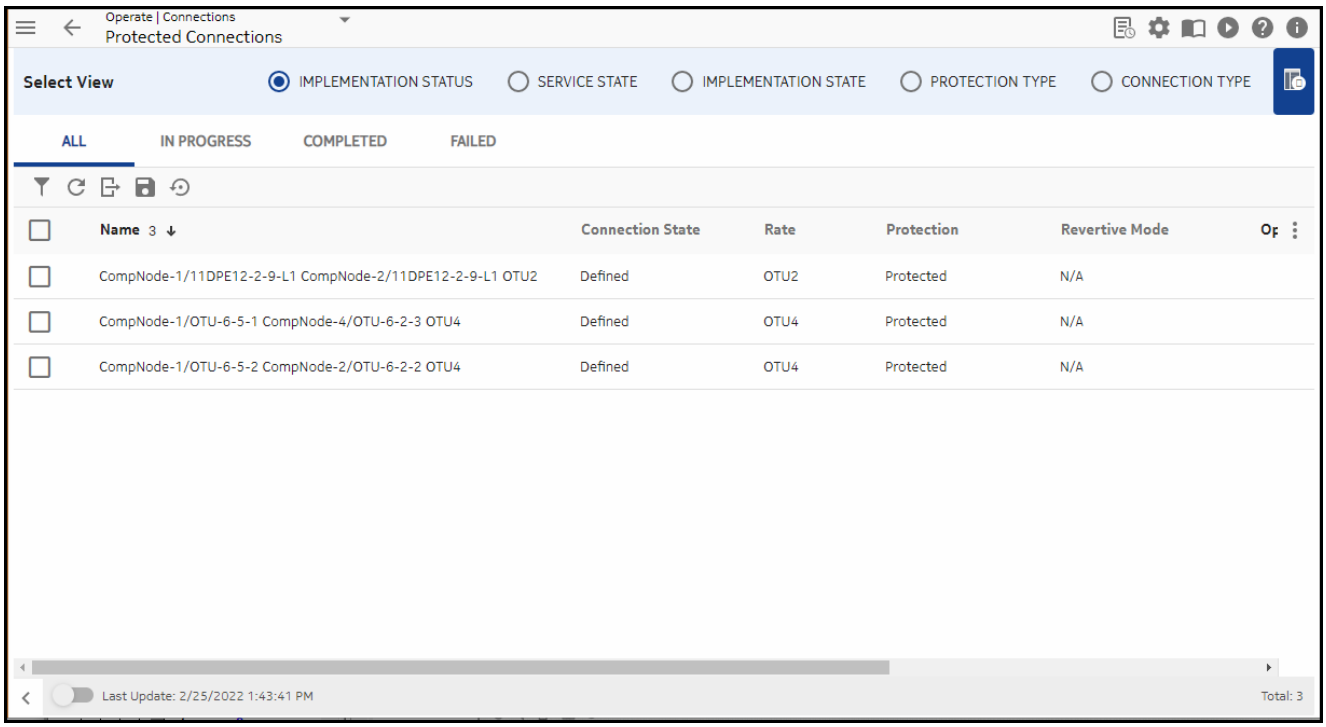
From the NFM-T GUI, follow this navigation path:

OPERATE > Protected Connections

Result: The system displays the Protected Connections data table.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-225 Protected Connections – Data Table



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window and return to the main page.

See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the Manage Columns window.

3

If the protected connection is an infrastructure connection, go to Step 4.

If the protected connection is a service connection, go to Step 5.

4

Select a protected infrastructure connection; and, depending on the type of infrastructure connection (infrastructure or logical link) that is selected and its current state, perform one of the following commands:

- **Alarms**
- **Correlate ASAP**
- **Delete Connection**
- **Deployment Control**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- **Service State**
- **Display Route on Map**
- **Jobs**
- **Manage Protection Group**
- **Modify Connection > Modify Parameters...**
- **Network MAP**
- **OA&M Diagnostics**
- **OLC State**
- **Optical Power**
- **PM > Modify PM**
- **Routing Details**
- **Routing Display**
- **Service Testing**
- **TCM**
- **Timeline**

5

Select a protected service connection; and, depending on its current state, perform one of the following commands:

- **Alarms**
- **Correlate ASAP**
- **Delete Connection**
- **Deployment Control**
- **Disable Service State**
- **Display Route on Map**
- **Enable Service State**
- **Jobs**
- **Manage Protection Group**
- **Modify Connection...**
- **Modify Parameters...**
- **NIM**
- **OA&M Diagnostics**
- **Compute Latency**
- **Routing Display**
- **TCM**
- **Timeline**

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.86 View Protected Connections

Purpose

Use this task to view the data table list and the end to end view of a Protected Connection.

Task

Complete the following step to view the Protected Connections data table list and a Protected Connection end to end view.

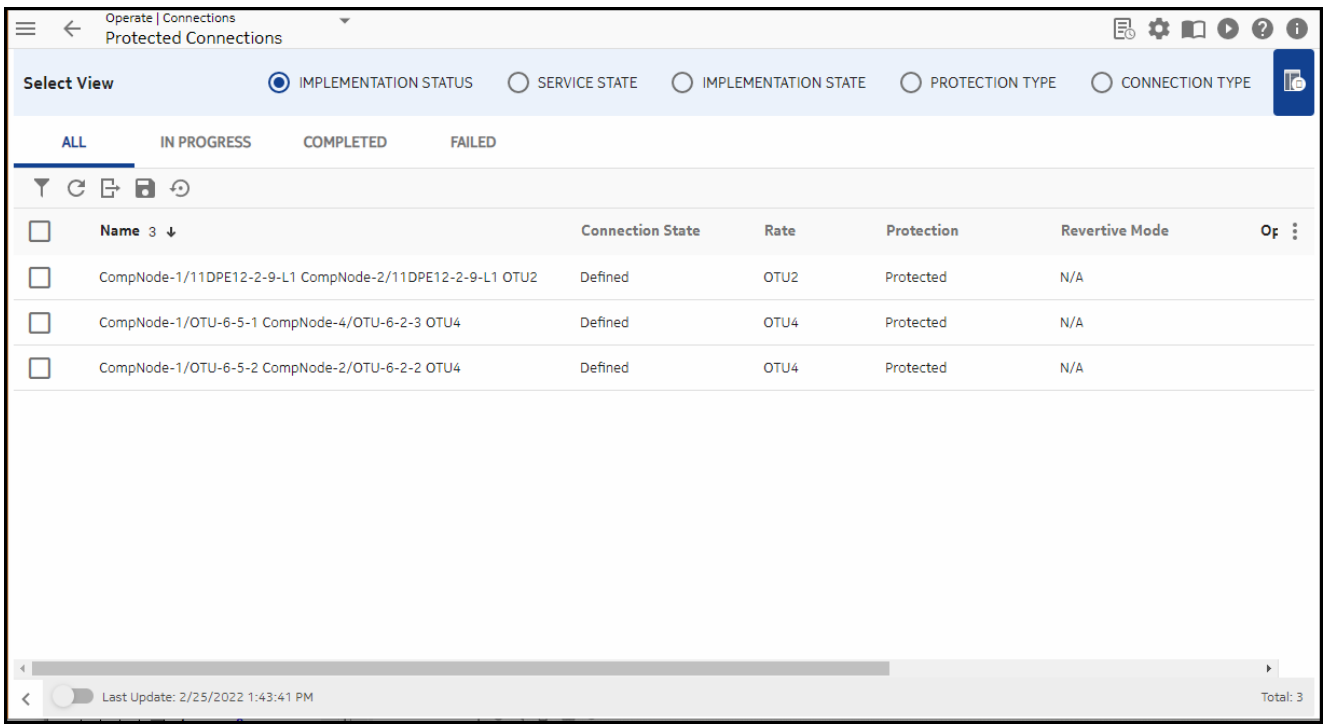
1

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

OPERATE > Protected Connections

Result: The system displays the Protected Connections data table.

Figure 7-226 Protected Connections – data table



Control Plane and Mixed Plane connections For Control Plane and Mixed Plane Connections where the protection group is in the control plane domain, navigate to the **ASON SNC** tab of the connection to request a protection switch action. For control plane and

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

mixed plane connections, the **Routing Display** displays the nominal route of the control plane connection with a distinct identification to indicate that it is the **Nominal Route**.

A connection with SNCP Protection can have managed plane SNCP on the network side, managed plane SNCP protection on the client side, control plane SNCP protection or a combination of these types. When a connection has more than one type of SNCP protection the value of Protection displayed to the user has the following precedence

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

The **Protection** field in the Protected Connection List for a connection with protection in the control plane displays the type of ASON Sub-Network protection with valid value **SNCP-N**.

The Protection field in the Protected Connection List for a connection with protection in the managed plane can have following values: Y-Cable, OPSB, OPSA, E-SNCP, SNC-I, SNC-N, SNC-Nc, SNCP and OMSP.

SNCP protection in the managed plane can have following values: E-SNCP, SNC-I, SNC-N, SNC-Nc and SNCP. For most packs (such as, 10xANY10G, 20P200, 12P120) the values SNC-I, SNC-N, SNC-Nc and SNCP are possible.

If a circuit pack does not support the SNC Type, the value *SNCP* is displayed. For older legacy packs on 1830 PSS which do not support setting the SNC Type, for example, 11QPA4, the value *E-SNCP* is displayed. If a connection is stopped in the planned state, it may not be possible to determine the type of protection because the route of the connection has not been determined. In this case the system displays a value of **SNCP** or **Protected**.

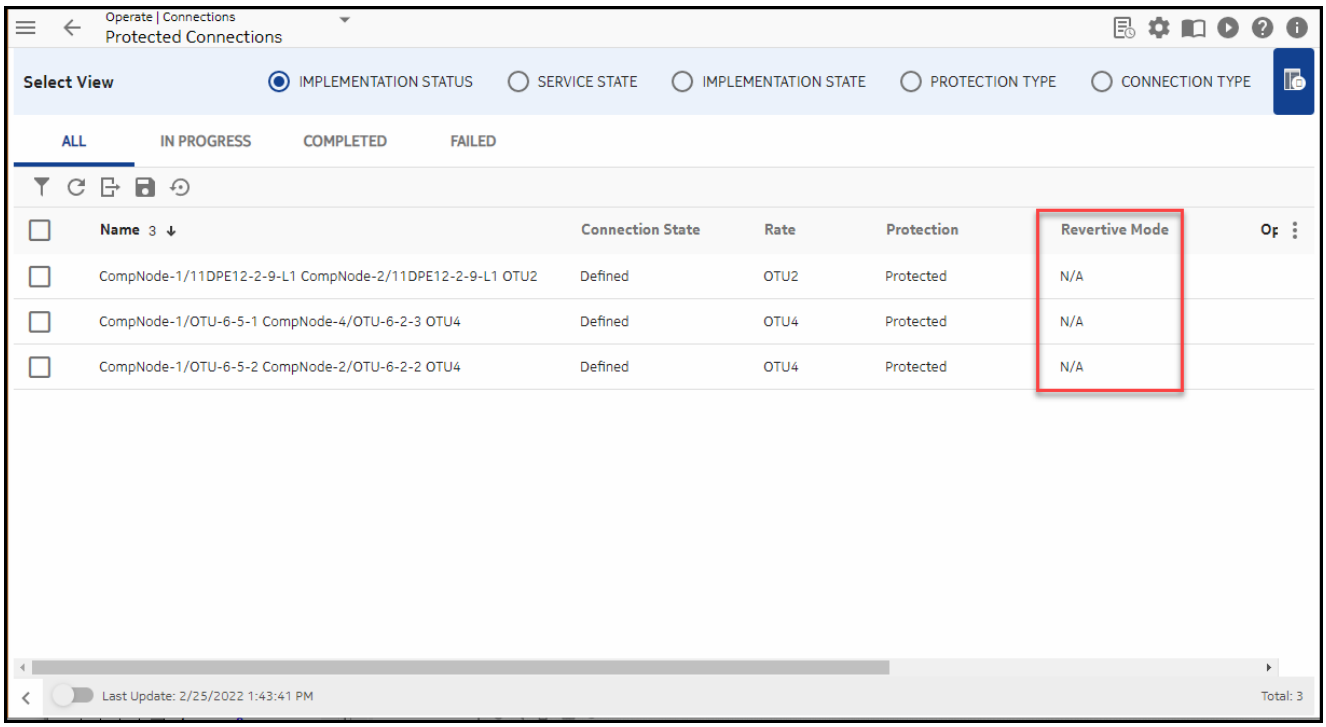
Note: 12P120 supports the following protections types provided by OPSA packs:

- OCHP. Note, only keyed service is supported for OCHP.
- OMSP
- OLP
  OPSA/OLP pack does not support add and remove protection.
  OMSP is not supported for CDC-F configurations.

Revertive Mode field The value of Revertive Mode column is the connection level value of the parameter. Revertive mode field values can be enabled, disabled, automatic, soft automatic, manual and N/A or blank. For former releases of the supported nodes, this value is not managed, N/A is displayed in the column.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-227 Protected Connections – Revertive Mode field



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window, once you have made the changes.

See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the **Manage Columns** window.

3

On the main page, click the **More** icon on the protected connection row for which you want to visualize the end to end view and follow the path: **Routing Display**

Result: The system opens a new tab and displays the Routing Display for the selected protected connection.

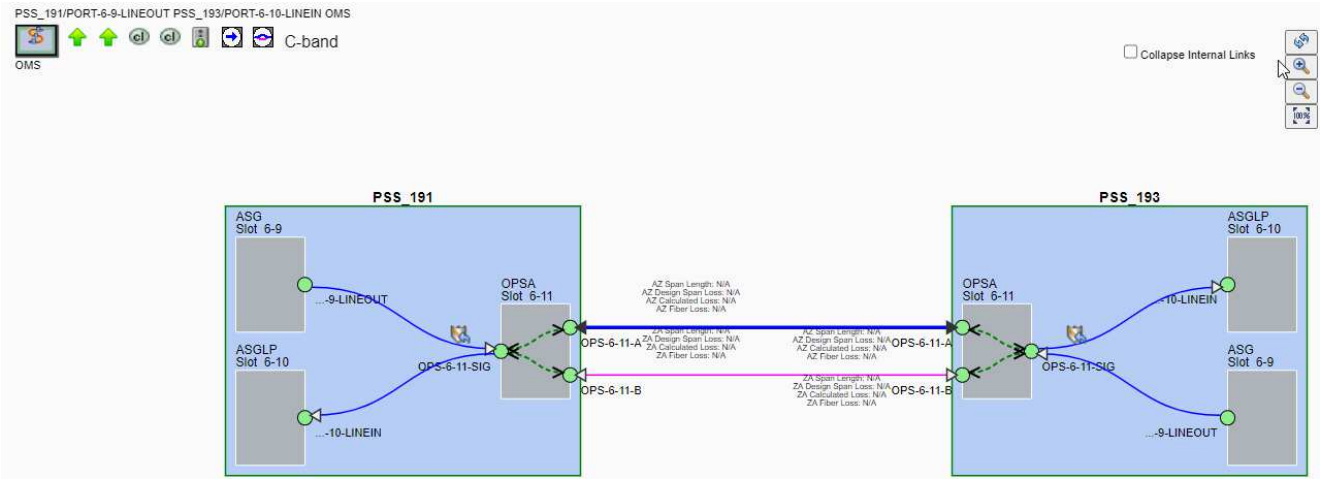
The *working* and *protection* paths are highlighted with different color; **blue** for the working path and **purple** for the protection path.

Note: The active route (*working* or *protection*) is shown in bold in the Managed Plane and not shown in bold in the Control Plane. The user can navigate to the **ASON > SNCs** and SNCP tab in the **360° View** and manually synchronize the SNCP to see the switch position.

The following image shows an example of an end to end view of a protected connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

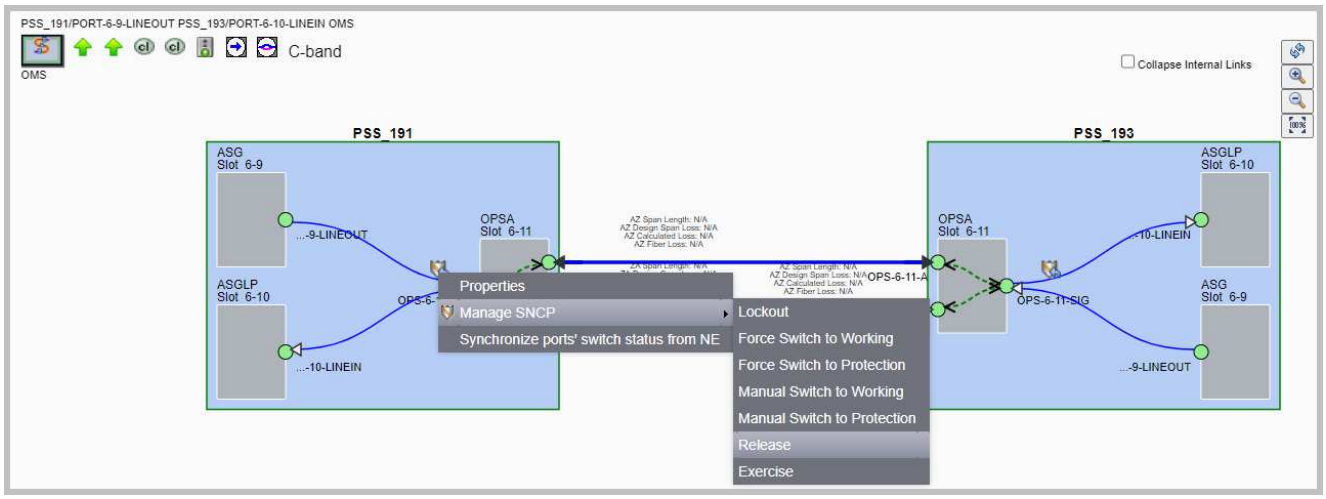
Figure 7-228 Protected Connections – Routing Display view



4

Moreover, right clicking on the Protection Group icon and following the path **Manage SNCP** you can execute the following commands: **Synchronize Switch Position, Lockout**, **Force Switch to Working**, **Force Switch to Protection**, **Manual Switch to Working**, **Manual Switch to Protection**, **Release** and **Exercise**. See 7.90 "Perform protection switching" (p. 1106) and 7.91 "Perform Force Switch Operation" (p. 1112) for details. Selecting **Update all ports' protection switch status from NE** you can synchronize the ports status with NE.

Figure 7-229 Protected Connections – switch commands



End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.87 View tabbed topics for a protected connection

Purpose

Use this task to view tabbed topics for a selected protected connection.

Task

Complete the following steps to view tabbed topics for a selected protected connection.

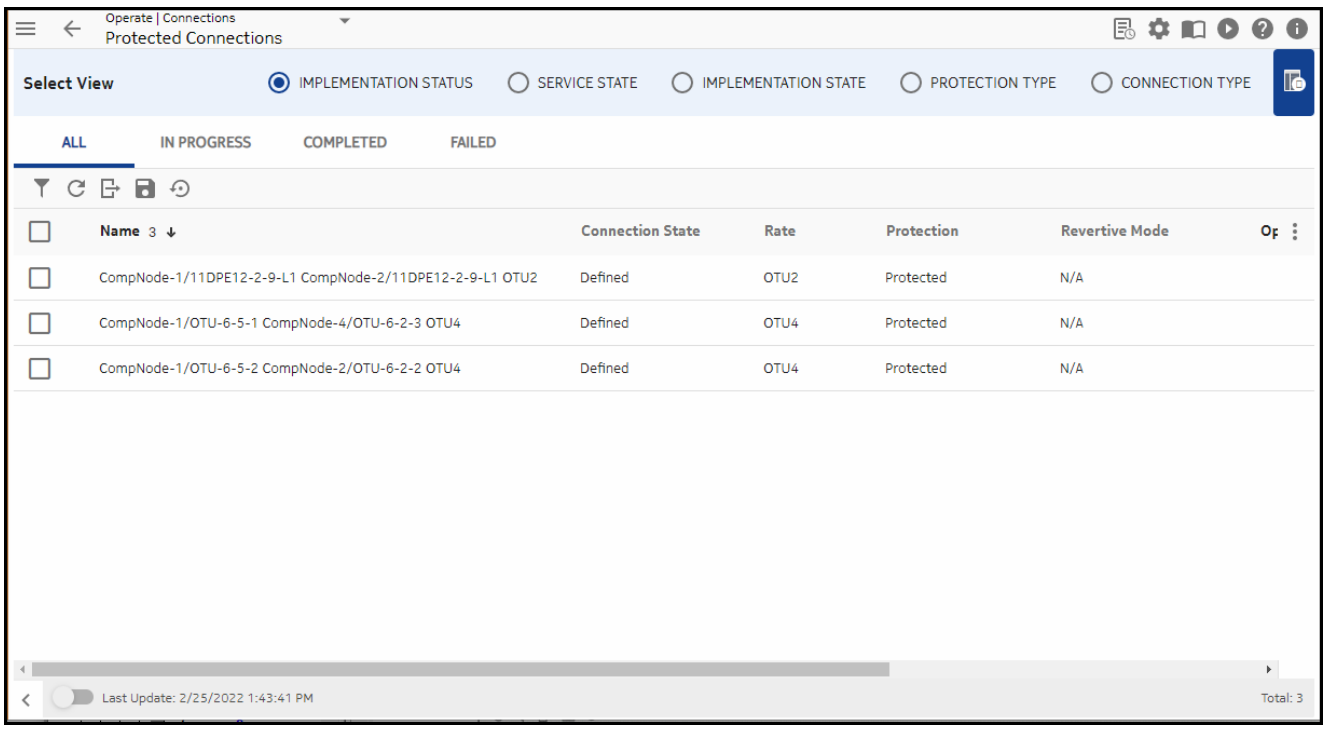
1

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

OPERATE > Protected Connections

Result: The system displays the Protected Connections data table.

Figure 7-230 Protected Connections – data table



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window, once you have made the changes.

See 26.7 “Manage data columns” (p. 2213) for a detailed description and usage of the **Manage Columns** window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

On the main page, select a protected connection, and click the **360° View** icon.

The available tabs for protected infrastructure connections are the following:

25.6 “ALARMS Tab” (p. 2066)
25.44 “Servers Tab” (p. 2148)
25.11 “Clients Tab” (p. 2080)
25.42 “Routes Tab” (p. 2145)
25.28 “Link Connections Tab” (p. 2117)
25.36 “PM Enabled Points Tab” (p. 2135)
25.9 “ASON SNC Tab” (p. 2073)
25.38 “Protection Tab” (p. 2140)
25.37 “PGs Tab” (p. 2139)

The available tabs for protected services are the following:

25.6 “ALARMS Tab” (p. 2066)
25.44 “Servers Tab” (p. 2148)
25.42 “Routes Tab” (p. 2145)
25.36 “PM Enabled Points Tab” (p. 2135)
25.38 “Protection Tab” (p. 2140)
25.37 “PGs Tab” (p. 2139)

Result: The system activates the selected tab and related information is displayed directly below the Protected Connections data table.

4

If you select a Control Plane or Mixed plane connection, the **ASON SNC** tab is enabled. User requested protection switch operations for L1 control plane connections is from the **ASON SNC** tab.

For detailed information and actions of **ASON SNC** tab, see NFM-T ASON Guide.

END OF STEPS

Revertive Mode value

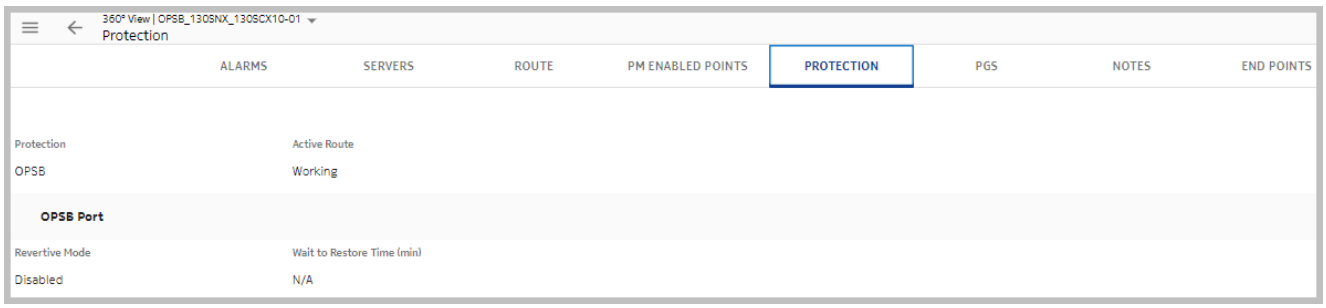
If you click the **Protection** tab, the **Revertive Mode** value is displayed in the corresponding field. See the example in the figure below.

The Protection for a connection in the Protected Connection List can be of type: Y-Cable, OCHP, OPSB, OPSA, E-SNCP, SNC-I, SNC-N, SNC-Nc, SNCP and OMSP.

An SNCP protected connection can have managed plane SNCP network protection, control plane SNCP protection, managed plane client SNCP protection or a combination of these types.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-231 Protected Connections - Revertive Mode OPSB



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.88 OTN Protected Connections data columns

Description

Column	Description
Active Route	Displays values of Working and Protection • For connections with more than one protected segment the value of the **Active Route** field is calculated using only the **From End** and **To End** Network Protection groups. • For connections with client and network protection, the value of the **Active Route** field is calculated using only the network protection.
Additional info	The **Additional info** column displays additional information about topics that are related to an object.
Alarm Status	Displays whether the node/NE is alarmed and the severity of the alarm. The Alarm Synthesis is: **Minor**, **Critical**, **Major**, or **Cleared**.
ASAP	The **ASAP** displays the Alarm Severity Assignment Profile setting for the connection, which can be **Not Set**, **Enabled**, or **Disable**.
Category	The **Category** of a connection can be **Managed Plane**, **Mixed Plane**, **Control Plane**, **ASON Logical Edge Drop Link**, or **ASON Logical Drop Link**. The NFM-T supports 1830 PSS WDM/photonic and 1830 PSS OCS/switching functions in the Managed Plane, the Control Plane, and the Mixed Plane. or External, Shared, Managed Plane, Control Plane, Mixed Plane, ASON Logical Link, ASON Implicit Server, ASON Logical Edge Drop Link, ASON MRN Un-terminated Tunnel, ASON MRN Terminated Tunnel, Edge HO Trail, ASON Edge HO Trail, All (default value).
Completion Status	The **Completion Status** column displays the completion status of the connection.
Connection Alias	The **Connection Alias** displays an alias name that is assigned to the connection. **Note:** The **Connection Alias** is controlled by installation parameters.
Connection Name	Specifies the connection name
Customer Name	The **Customer Name** displays the name of the customer that is assigned to the connection. User-assigned customer names are: **Customer 4**, **Customer 3**, **Customer 2**, **Customer 1**. For auto-discovered connections and system auto-generated connections, the customer name is **None**. **Origin:** Users specify the **Customer Name** in the **Service Description** panel of a template.
Created Date	The **Created Date** column displays date of the creation of the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Column	Description
Deploy Type	The **Deploy Type** column displays the particular connection request (order). Not all connection requests (orders) support a particular connection. The **Deploy Type** includes the following deployment type indicators: • **Add** indicates that a user has added a new connection to the system. Note that Automatic Routing is only supported for provisioning new connections (**Add** orders). • **Discover** indicates that the system has automatically discovered the connection. • **Delete** indicates that a user has deleted the connection from the system. • **DB Delete** indicates that a user has deleted the connection from the database. • **Reroute** indicates that the connection using a route had to be released, and the connection using the new route was recreated. Reroute is a facet of the Connection Rearrangement feature. • **Reroute with Reinstate** deletes the connection using a route needed to be released, and the connection using the new route was recreated, but the layout of the older connection was stored. During a Reroute with Reinstate, the old route is stored to rollback using the Reinstate. During a Reroute with Reinstate, the original route might cause traffic disruptions. A Reroute is performed on a Reroute with Reinstate order. The older route is purged and the saved time slots are released. Reroute with Reinstate is a facet of the Connection Rearrangement feature. • **Reinstate** indicates that a reroute reverted back 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. Reinstate is a facet of the Connection Rearrangement feature.
Frequency	The **Frequency** column displays a numeric value from **9170** to **9605** in increments of 5 (for example: 9170, 9175, 9180, 9185, ...9600, 9605.) or **N/A** for Wave Keys that are assigned to infrastructures, servers, and clients. For link connections, **Frequency** is only applicable for OCH link connection rates. For rates other than OCH, **NA** is displayed in this field. **Origin:** Users enter **AZ/ZA Wave Key Pairs** in the Wave Key panel when the **Wave Key Assignment** field is **User Selected**. **Note:** When a keyed connection uses Manual Wave Key provisioning users must select the Wave Key values and be aware of the current Wave Key usage in the network to avoid Wave Key collisions. Users must be aware of the Wave Keys assigned by both Manual and Automatic Wave Key assignment since there is a single pool of Wave Key values that is used by both Manual and Automatic assignment.
From End Active Route	Includes values of Working and Protection. The **From End Active Route** is the value for the first network protection group found in the route starting from the **From End** of the connection and may not be on the end node For L1 control plane the **From End Active Route**value is from whichever route (nominal or current) that is currently active
From End Switch Reason	The **From End Switch Reason**is the value for the first network protection group found in the route starting from the **From End** of the connection and may not be on the end node For L1 control plane **From End Switch Reason** value is from whichever route (nominal or current) that is currently active.
From Node #1 **From Node #2** **To Node #1** **To Node #2**	The **From Node #1** and **To Node #1** columns display the nodes where the 2-ended connection originates (**From Node #1**) and terminates (**To Node #1**). The **From Node #2** and **To Node #2** columns display the nodes where the 3-ended or 4-ended connection originates (**From Node #2**) and terminates (**To Node #2**).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Column	Description
From Node/Port #1 **To Node/Port #1** **From Node/Port #2** **To Node/Port #2**	The **From Node/Port** and **To Node/Port** columns display the Nodes and ports in which the 2-ended connection originates (**From Node**) and terminates (**To Node**).
From Port #1 **From Port #2** **To Port #1** **To Port #2**	The **From Port #1** and **To Port #1** columns display the names of the nodes 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 names of the nodes where the 3-ended or 4-ended connection originates (**From Port #2**) and terminates (**To Port #2**).
Group Order Name	
Implementation State	Displays whether the connection is Implemented, Commissioned, or Allocated
NML ASAP	The **NML ASAP** displays the Alarm Severity Assignment Profile setting for the connection at NML level, which can be **Not Set**, **Enabled**, or **Disable**.
Operational State	When the operational state of a connection is changed, the system dynamically updates the value of the operational state in the connection list
Order Number	The **Order Number** column displays a unique alphanumeric string that identifies the connection being made. The **Order Number** is system generated. The **Order Number** can also be used as a link to an external inventory or order management system.
PM 15M **PM 24H**	The **PM 15M** and **PM 24H** columns display whether 15 minute and/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.
Protection	Values supported are Y-Cable, OPSB, OPSA, OPSA server protected, E-SNCP, SNC-I, SNC-N, SNC-Nc, SNCP-N, SNC-N server protected, SNC-I server protected, SNCP-N server protected, OMSP, OMSP server protected. When protection is at the connection level, the protection type reflects the type of protection (e.g. Y-Cable, OPSB, SNCP, OPSA, OMSP). When protection is at the immediate server level the protection type is of type server protection. For DSR connections with SNCP protection at the HO ODUk server level, the protection type of both the LO ODUk and DSR client connections is the type of server protection
Provisionable Wave Key	The **Provisionable Wave Key** column displays, depending on the template/connection type, the Provisionable Wave Key field is displayed as drop-down list. Values are **Keyed** (the default - a managed service in which Wavelength Tracker is enabled), **UnKeyed** (a managed service in which Wavelength Tracker is disabled), or **N/A** (not applicable/valid for the connection). **Origin:** Users supply the **Provisionable Wave Key** assignment during connection provisioning in the **Additional Information** panel of the template. 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Column	Description
Revertive Mode	The **Revertive Mode** column displays the revertive mode value for the selected protected connection. Possible values for the Revertive Mode column are enabled, disabled, automatic, soft automatic, manual and N/A or blank. The Revertive Mode field does not apply for OMSP and OLP connections. If the Revertive Mode parameter does not apply for the connection the field is blank or have the value N/A. This column allows the user to filter and sort the protected connection list by the revertive mode.
Service Rate	Displays the effective rate of the connection • For OCH connections the value of the Effective Rate is equal to the connection rate • For DSR connections the Effective Rate is equal to the Signal Type of the connection • For DSR connections between 11QPE24 Line ports the Effective Rate is equal to 10GbE • For OS connections the Effective Rate is equal to the Signal Type of the connection • For OTS connections the value of the Effective Rate shall be equal to the connection rate • For OTUk connections the value of Effective Rate shall be based on the bit rate of the Line Ports • For ODUk connections with one or more end point on a PSS-64 Network Element the Effective Rate shall be equal to the connection rate. • For ODUk connections with one or more end points on an I/O card on the PSS32S shelf on an 1830 PSS Network Element the Effective Rate is equal to the connection rate. • For ODUk connections with all endpoints on 1830 PSS/PSS-1/PSS-4 Network Elements except connections with one or more end points on a 10AN10G pack the value of Effective Rate is based on the bit rate of the Client/Line Ports.
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 endpoints. If all connection endpoints 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 endpoint 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 endpoint 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 path connections with Y-cable protection, the alarm Reporting parameter of the OT client ports determines the Service State and not the connection endpoints. • For path connections with OPSB Protection, the alarm Reporting parameter of the OT client ports determines the Service State and not the connection endpoints. • 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 endpoints. For physical connections, the **Service State** column displays whether the connection is **Not in Service** or **In Service**.
Synced Switch Data with Network	Syncs the protection switch data for a specific connection with the NE
TCM ASAP Enabled	The **TCM ASAP Enabled** column displays whether the Tandem Connection Monitoring (TCM) Alarm Severity Assignment Profile is set to **Enable**, **NA** (not applicable), or **None**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Column	Description
TCM Enabled	The **TCM Enabled** column displays whether Tandem Connection Monitoring is **Enable**, **NA** (not applicable), or **None**.
To End Active Route	Include valid values of Working and Protection The **To End Active Route** is the value for the first network protection group found in the route starting from the To End of the connection and may not be on the end node. For L1 control plane the To End Active Route values shall be from whichever route (nominal or current) that is currently active.
To End Switch Reason	The **To End Switch Reason**is the value for the first network protection group found in the route starting from the **To End** of the connection and may not be on the end node. For L1 control plane, the **To End Switch Reason** values is from whichever route (nominal or current) which is currently active.
Type	specifies the type of connection

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.89 Perform Synchronize Switch Position

When to use

Use this task to perform synchronization of Switch event for protected connections.

Ensure that the connection is protected.

Ensure that the Implementation State of a protected connection is in Implemented or Commissioned state.

You can manage MSP/SNCP 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

Note: In NFM-T R21.12, the switch reason for protection switching and synchronize switch position operations for 1830 PSI-CL end points is not reflected in NFM-T. However, correct details are reflected on the 1830 PSI-CL NE.

Task

Complete the following steps to perform synchronization of Switch events for protected connections.

1

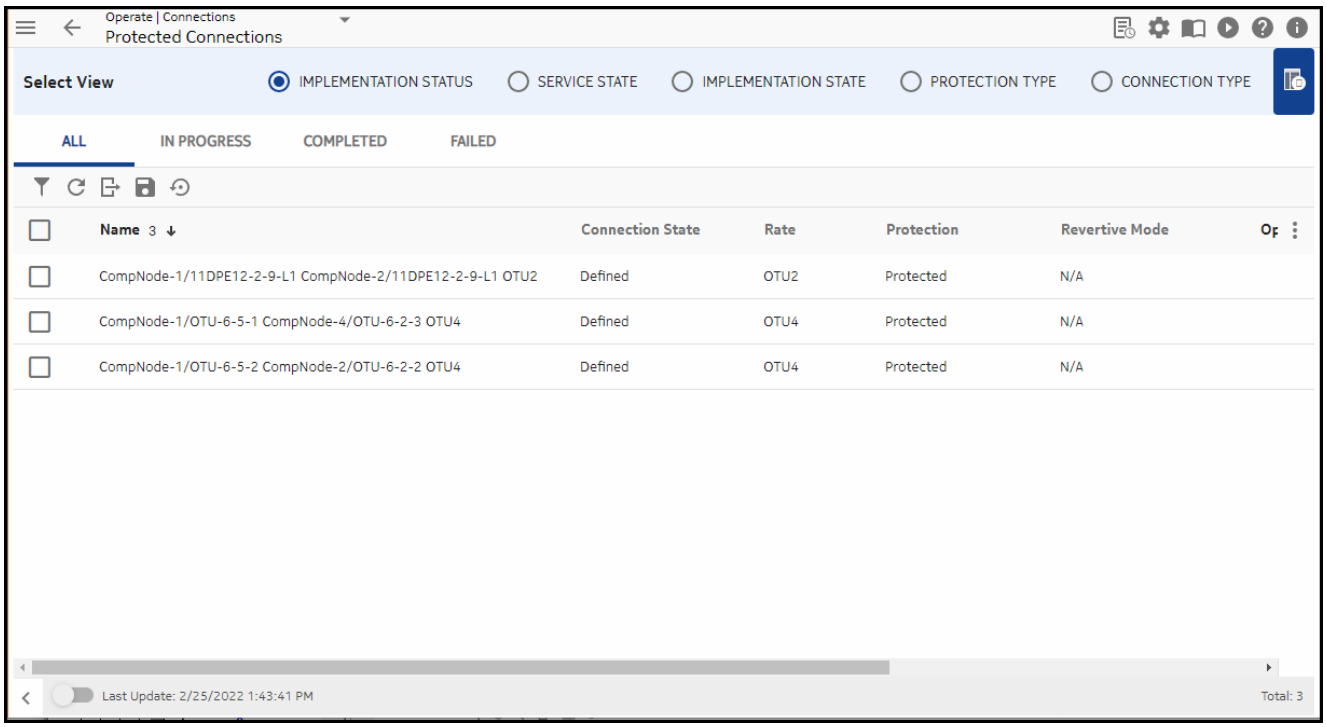
From the NFM-T GUI, follow this navigation path:

OPERATE > Protected Connections

Result: The system displays the Protected Connections data table.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-232 Protected Connections – data table



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window, once you have made the changes.

See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the **Manage Columns** window.

3

On the main page, select a protected connection from the list of protected connections and click the **More** icon on the right of the connection row and follow the path **Manage Protection Group > Synchronize Switch Position** from the menu options.

Result: The system displays a confirmation message about the initiation of Synchronize Switch Position.

The Synchronize Switch Position action retrieves the current protection switch data of a specific connection from the network element.

The system performs an automatic synchronization when communication is reestablished after a loss of communication with a Network Element.

Note: On demand and scheduled Protection Switch Event synchronization can be initiated by a user for a single Network Element or for the entire Network.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

On demand Protection Switch Event synchronization can be initiated by a user for a single connection from the Protected Connection List.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.90 Perform protection switching

Purpose

Use this task to perform force switch operation for protected connections.

The connection must be in the protected state.

Perform a Force Switch operation for the following types of protected connections that are in Managed Plane 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

If you have selected a Control Plane or Mixed Plane connection, the system displays a message that the Protecting switching can be performed only from the **ASON SNC** page.

Note: In NFM-T R21.12, the switch reason for protection switching and synchronize switch position operations for 1830 PSI-CL end points is not reflected in NFM-T. However, correct details are reflected on the 1830 PSI-CL NE.

Task: Perform force switch for the selected protected connection

Complete the following step to perform force switch for the selected protected connection.

1

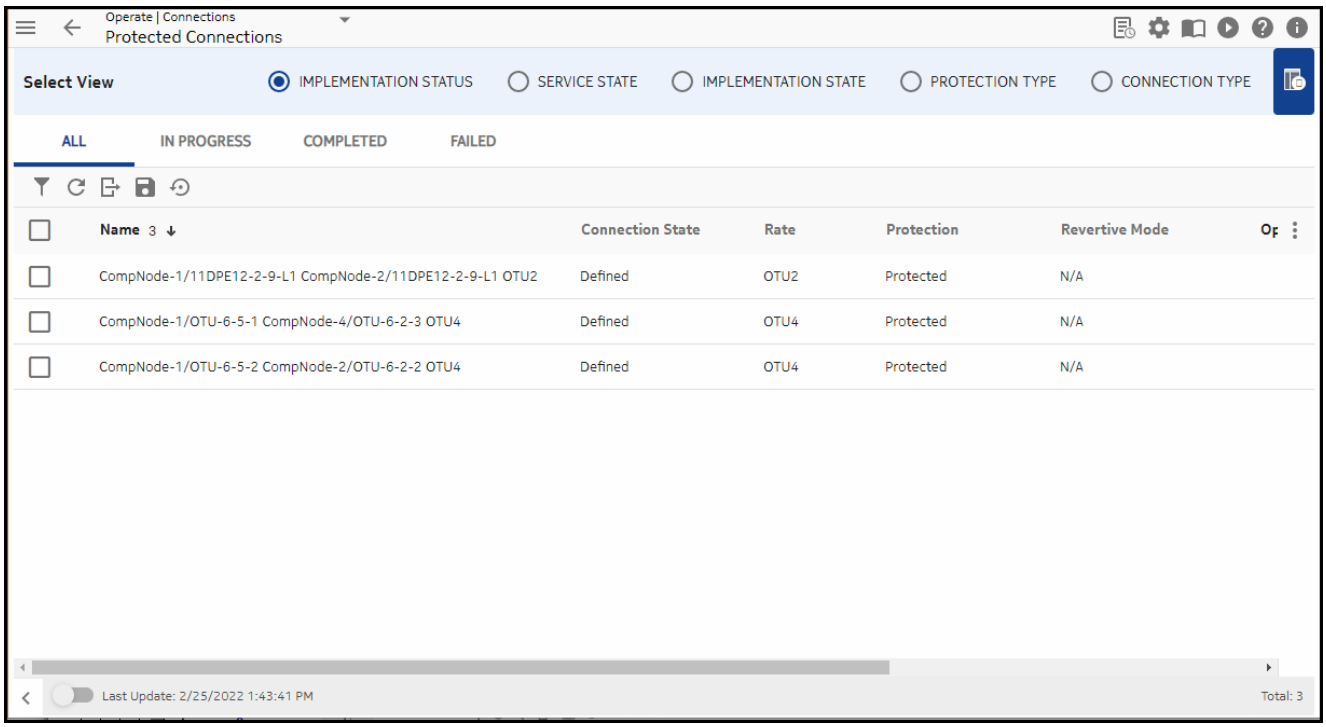
From the NFM-T GUI, follow this navigation path:

OPERATE > Protected Connections

Result: The system displays the Protected Connections data table.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-233 Protected Connections – data table



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window, once you have made the changes.

See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the **Manage Columns** window.

3

On the main page, select a protected connection from the list of protected connections and click the **More** icon on the right of the connection row and follow the path to **Manage Protection Group > Force Switch to Working**, **Force Switch to Protection**, **Manual Switch to Working**, or **Manual Switch to Protection** from the menu options.

Result: The system displays a confirmation message that this operation is traffic impacting.

4

Click **OK**.

Result: The system displays a success message.

The commands are sent to the NE and the response is notified in the NFM-T GUI.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Control Plane and Mixed Plane connections For Control Plane and Mixed Plane Connections where the protection group is in the control plane domain, navigate to the **ASON SNC** tab of the connection to request a protection switch action. For control plane and mixed plane connections, the **Routing Display** displays the nominal route of the control plane connection with a distinct identification to indicate that it is the **Nominal Route**.

The following types of **Protection Switch** operations are supported for the **Main** and **Spare** path for the **Control Plane** connections:

- Synchronize
- Force Active: Main, Spare, and Per Direction (Main A-Z, Main Z-A, Spare A-Z, and Spare Z-A)
- Manual Active: Main, Spare, and Per Direction (Main A-Z, Main Z-A, Spare A-Z, and Spare Z-A)
- Release: All and Per Direction (A-Z and Z-A)

END OF STEPS

Task: Multiple selection of Y-Cable protected service connections for protection switching

The NFM-T allows to select multiple Y-Cable protected service connections and perform protection switching operation.

Perform the following steps to select multiple Y-Cable service connections and perform the protection switching operation.

1

From the NFM-T GUI, navigate to one of the following paths:

- **OPERATE > Services**
- **OPERATE > Protected Connections**
- **OPERATE > Infrastructure Connection**
  Select the required infrastructure connection from the list, click the corresponding **360^0 View > CLIENTS** tab.
- **OPERATE > Nodes**
  Select the required node, click the corresponding **360^0 View > IMPACTED CONNECTIONS** tab.

2

Select multiple Y-Cable protected service connections from the list that are in a **Commissioned** state.

Note: Multiple selection of Y-Cable protected service connections for protection switching is supported for a maximum of 150 service connections. If the selection exceeds the maximum limit of 150 connections, the system displays the following error message:

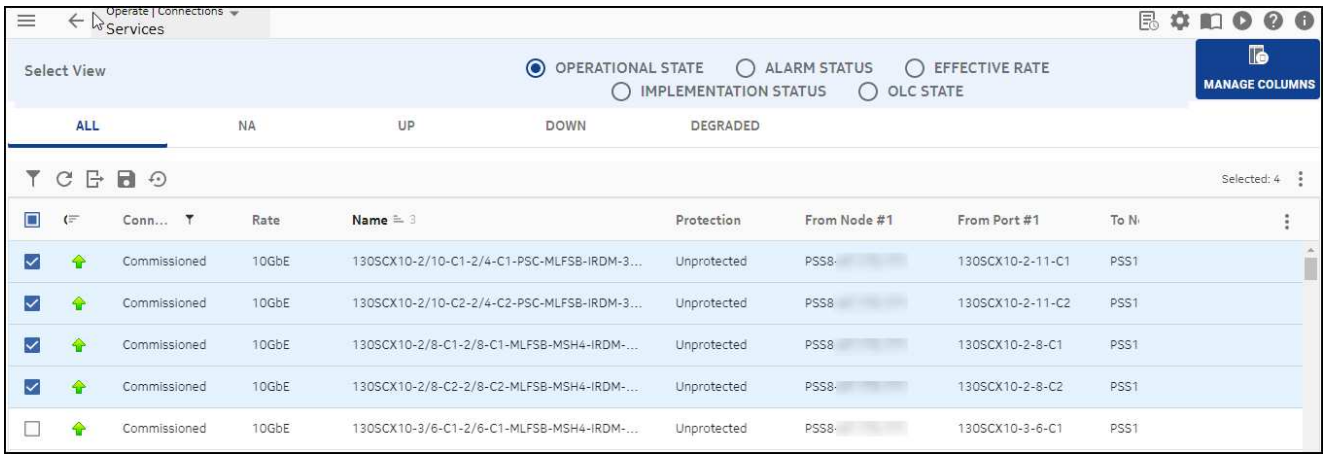
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

```
Number of selected items exceeds limit of 150. Please reduce the
selection size.
```

3

Click the **More** icon at the top right hand side as shown in the following figure.

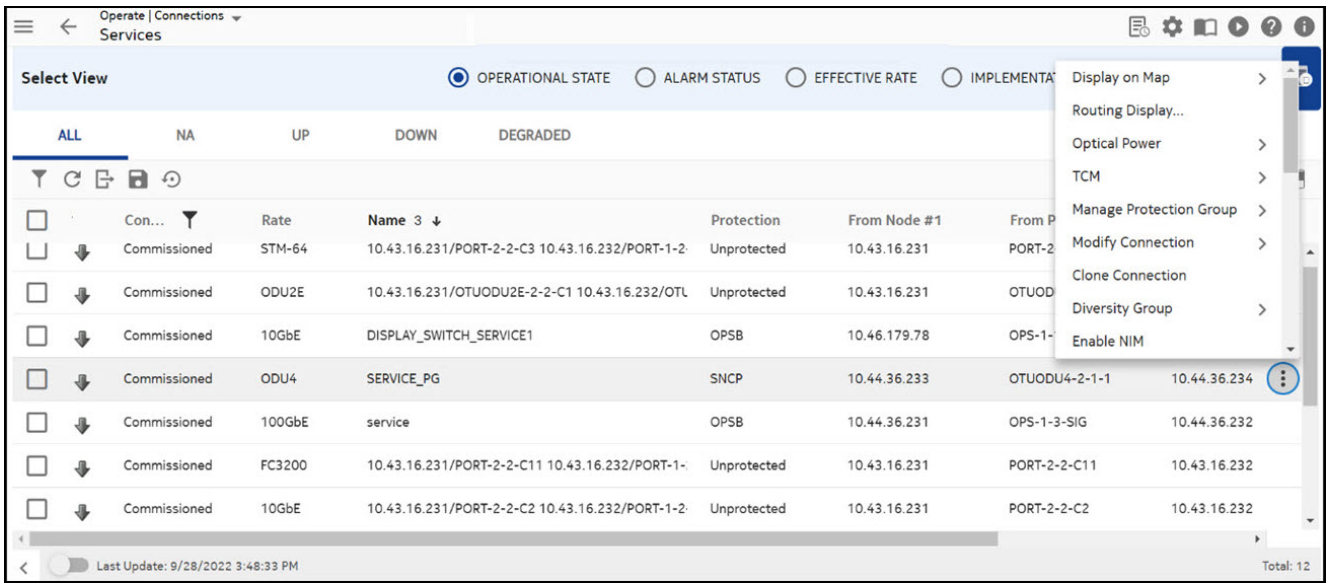
Figure 7-234 Services – data table – More option



4

Select **Manage Protection Group**.

Figure 7-235 Services – Manage Protection Group



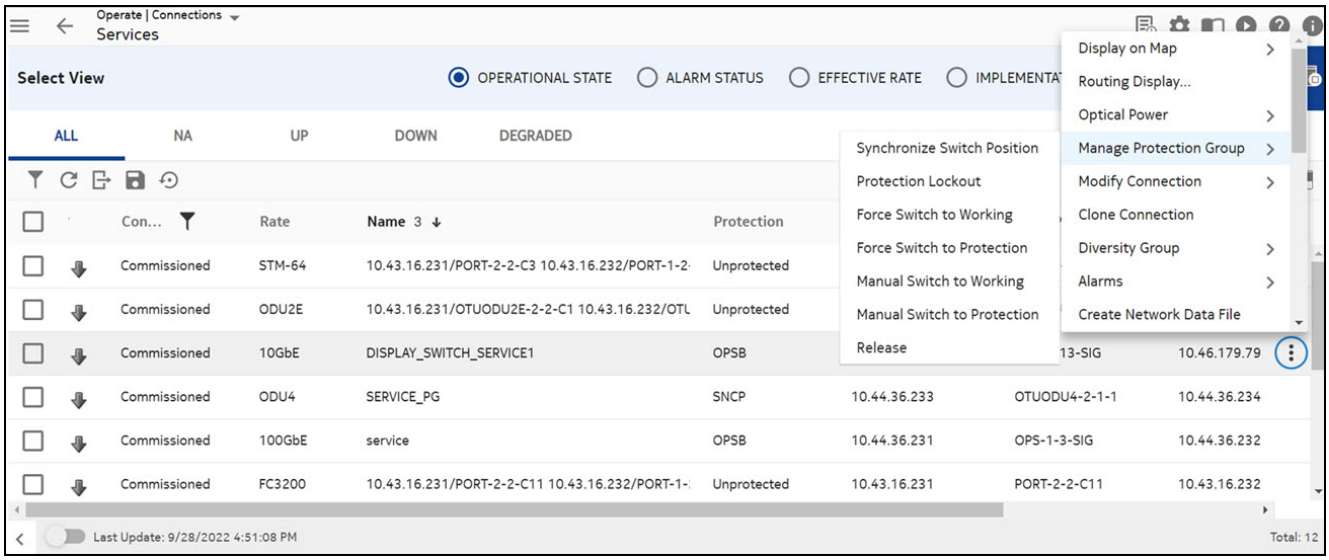
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: All the selected connections must be service connections with Y-Cable protection type in **Commissioned** state. If you select connections with protection type other than Y-Cable or Y-Cable protected connections that are in **Non-Commissioned** state, the **Manage Protection Group** option is disabled.

5

Select the required protection switching operation from the list of protection switching options as shown in the following figure.

Figure 7-236 Services – protection switching operations



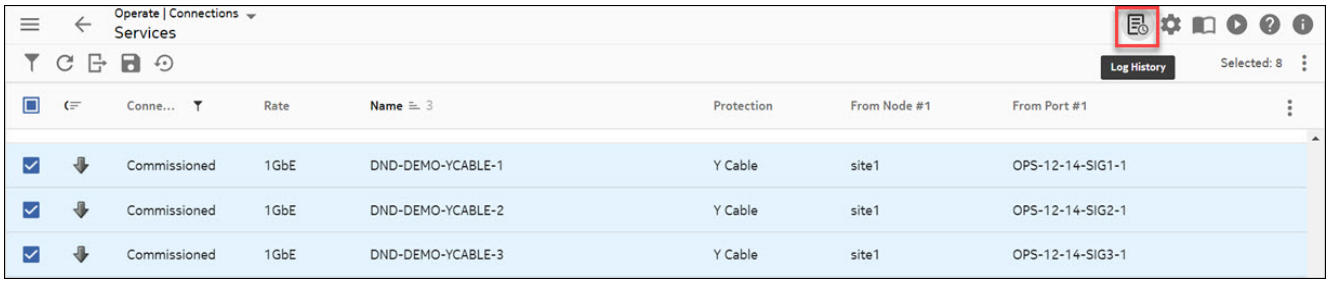
Result: The protection switching operation is applied to the selected list of Y-Cable protected service connections.

6

Click the **Log History** icon as shown in the following figure to view the status of the protection switch operation.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-237 Services – Log History



Result: The **Log History** includes an entry for each connection indicating if the protection switch request succeeded or failed. If the protection switch request for a connection fails, the reason for failure is available in the **Log History**.

7

Optional: Navigate to the **ADMINISTER > Jobs** page for the failed connections to view the **Run History** and take necessary action.

Reference: To view the REST call for multiple selection of Y-Cable protected service connections for protection switching, see *NFM-T REST API Documentation*.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.91 Perform Force Switch Operation

Purpose

Use this task to perform force switch operation for protected connections.

The connection must be in the protected state.

Perform a Force Switch operation for the following types of protected connections that are in Managed Plane 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

Task

Complete the following step to perform force switch of the selected protected connection.

1

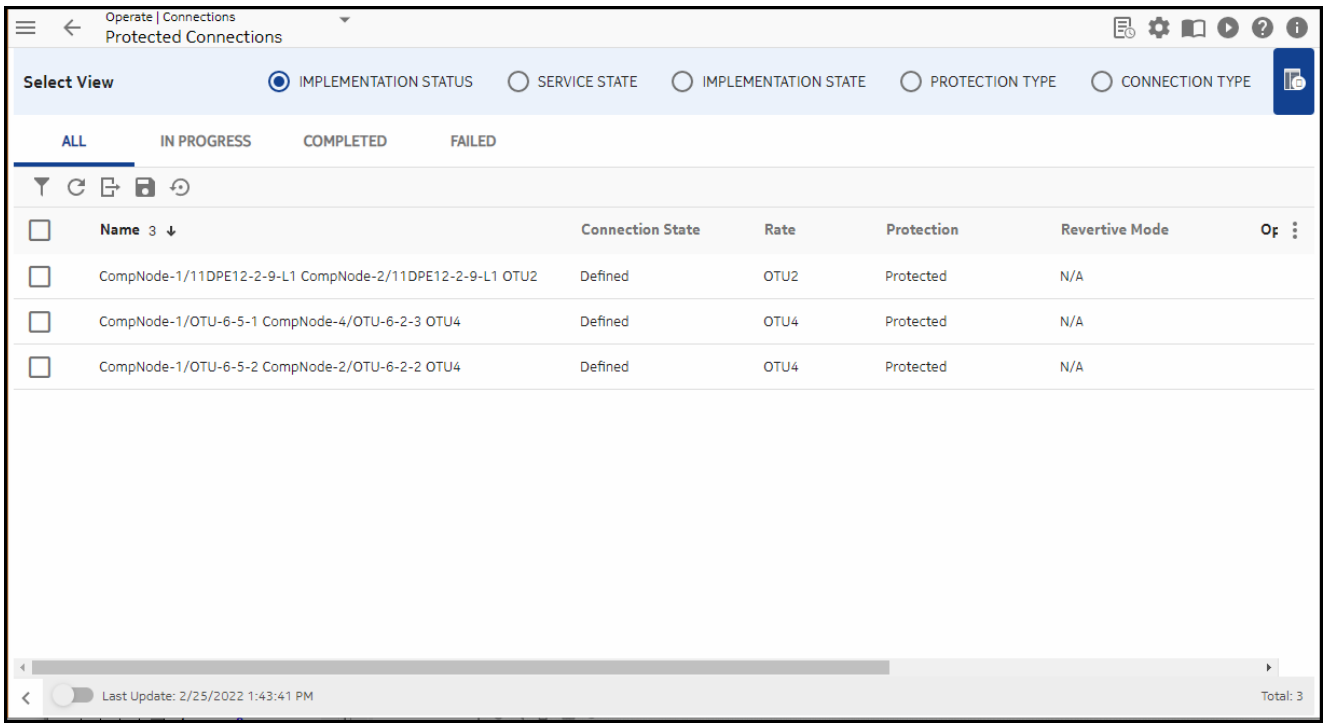
From the NFM-T GUI, follow this navigation path:

OPERATE > Protected Connections

Result: The system displays the Protected Connections data table.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-238 Protected Connections – Data Table



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window, once you have made the changes.

See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the **Manage Columns** window.

3

On the main page, select a protected connection from the list of protected connections and click the **More** icon on the right of the connection row and follow the path to **Manage Protection Group > Force Switch to Working** or **Force Switch to Protection** from the menu options.

Result: The system displays a confirmation message that this operation is traffic impacting.

4

Click **OK**.

Result: The system displays a success message.

The commands are sent to the NE and the response is notified in the NFM-T GUI.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.92 Manage OPSA protection with revertive mode

Purpose

Use this task to enable or disable the reveritive mode of an OPSA protection.

Before you begin

With the previous NE releases, the OPSA protection was *not revertive* type. With 1830 PSS R10.0, the OPSA *revertive* protection support is added.

When *revertive* OPSA protection is selected, traffic is restored to the working route after a switch reason is cleared. In the case of clearing a command (such as, Lockout, Forced Switch, Manual Switch) this happens immediately. In the case of clearing a defect, after expiration of the wait to restore time, protected traffic is switched back to the working route if the defect is no longer present on the OPSA/OLP

Revertive OPSA switching is only supported when the OPSA is positioned between the OT and two SFD/CLS channel ports.

The OPSA card supports three protection modes: OCHP, OMSP and OLP. Revertive OPSA4 protection is only supported for **OCHP** mode.

Revertive OPSA protection is supported by the NE for PSS-32, PSS-8 and PSS-16II shelves, equipped with the following packs 260SCX2, 130SCX10 and 130SNX10.

Note: OPSA protection applies to **OTUk**, **OCH** protected connections and **ODUk** protected connection created with auto server connection.

Task

Complete the following steps to manage an OPSA protection with revertive mode.

1

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

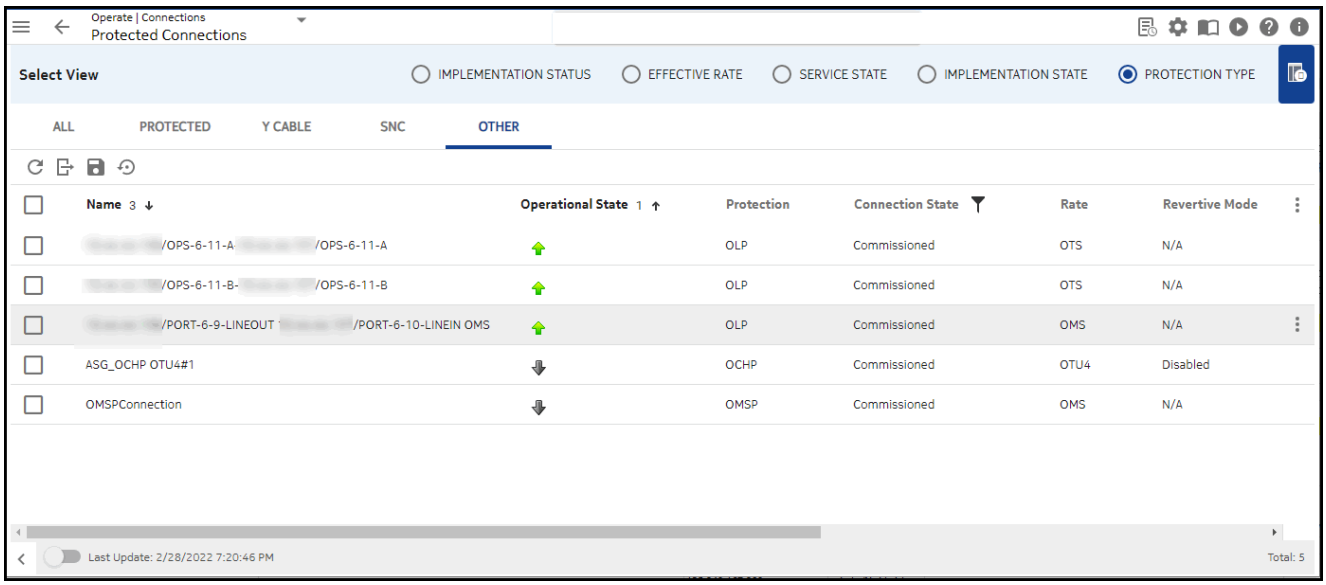
OPERATE > Protected Connections

OPERATE > Infrastructure Connections

Result: The system displays the data table with the related connections.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-239 Protected Connections: OPSA/OLP table list



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window and return to the main page.

See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the Manage Columns window.

3

From the main page, select an OPSA/OLP protected connection from the list and click the **More** icon on the right of the connection row and follow the path **Modify Parameters** from the menu options

Important ! The connection must have one of the following status: *Defined*, *Implemented* or *Commissioned*.

Result: The Service Definition window is displayed.

4

In the **Advanced Settings** panel, expand the **OPSA/OLP** pane.

5

Set the **Opsa Revertive Mode** field. Select **Enable** if you want the traffic is restored to the working route after switch; otherwise select **Disable**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

6

If the **Revertive Mode** is enabled, users can then specify the **Wait to Restore Time (min)**. Which is a period of time that must elapse after a recovered fault before traffic is restored to the working route.

The Network Wait to Restore Time (min) field is displayed as a drop-down list. Values are **1** to **20** minutes. The default is **5** minutes.

7

Click **Apply**.

8

Additionally The OPSA/OLP parameters are visible in the **Protection** and **OPSA** data table tabs.

Clicking the OPSA protected link in the list, the **Protection** tab is populated with information about the connection itself.

Note: OPSA/OLP tab is displayed only if the OPSA connection is created on NEs with rel 10.0 and above.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

TCM on Infrastructure Connections and Services

7.93 Create TCM in Control Plane and Managed Plane connections

Purpose

Use this task to create TCM on an infrastructure connection or service in Control Plane and Managed Plane connections.

Create the TCM on an infrastructure connection (trails and logical links) and service from the data table list when the TCM is enabled.

Link connection and cross connection TCM are enabled on a connection, based on the connection supported by 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, and 1830 PSS 8X shelves, and Managed Plane connection on 1830 PSS 32 for 260SCX2 service pack.

In Control Plane, TCM is applicable for L1 & L0 & MRN connections.

Note: TCM is not supported for Control Plane terminated connections.

The connection must be in the **Implemented** and **Commissioned** state.

TCM must not already be **Enabled** for the connection. The TCM status must be **None**.

Important! The PM parameters specified during the infrastructure connection or service provisioning differs from the parameters specified for TCM.

Important! In NFM-T R21.12, when a TCM trail is created, the TCM PM is enabled by default. Once TCM PM is enabled it cannot be disabled from NFM-T. When a TCM trail is deleted, TCM PM will be removed. There is no modify TCM PM for the connection as well as the TCM trail.

Task: Create TCM from data table List

Complete the following steps to create TCM for an infrastructure connection or service from a data table list.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, use the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as a column of the table.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: The TCM status is by default **NONE** for TCM supported connections. Once enabled, the status is updated as **Enabled**.

3

Select a TCM supported connection in which the **TCM Enabled** field is **None**.

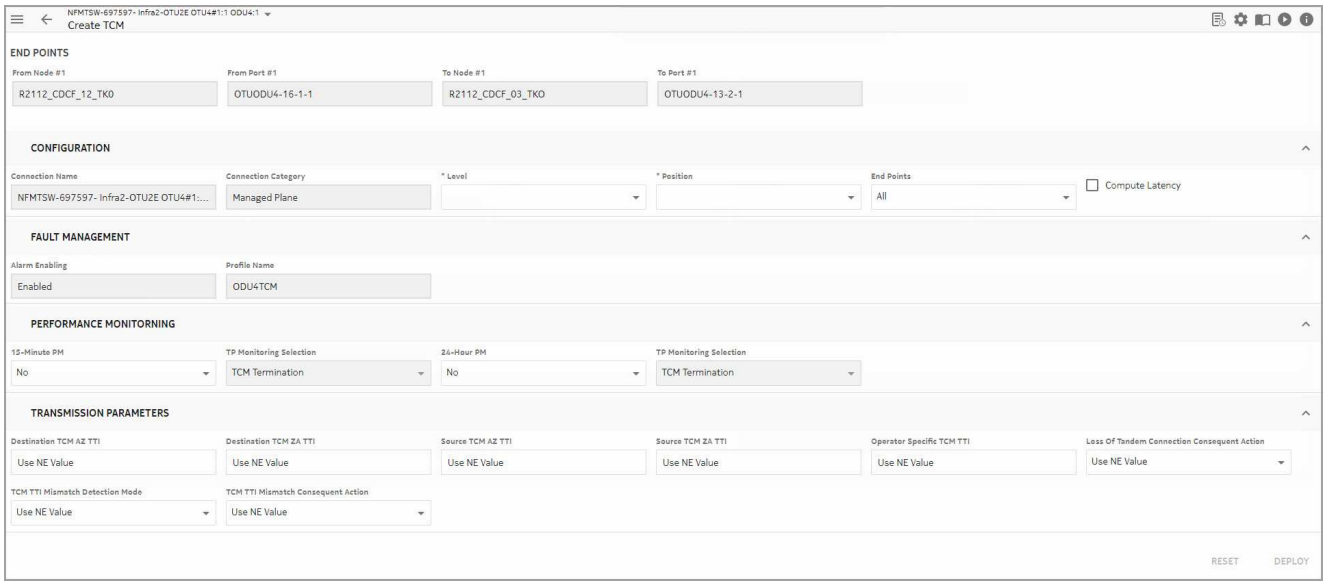
Note: TCM Enabled field status changes to **Enabled** after the creation of TCM.

4

Click the **More** icon on the right of the connection row, follow this path: **TCM > Create TCM**.

Result: The Create TCM window is displayed. Depending on the selection, fields are pre-populated.

Figure 7-240 TCM – Create TCM window



5

In the **CONFIGURATION** panel of the window, configure the following:

- The **Connection Name** and **Connection Category** fields are pre-populated.
- **For link based and cross-connection based connection:** The selected NE/port information is pre-populated in the **From Node #1** and **To Node #1** fields and in the **From Port #1** and the **To Port #1** fields.

  Note: OCS endpoints are not displayed for link connections.
- **For a protected connection:** The selected NE/port information is pre-populated in the **From Node #1**, **From Node #2** and **To Node #1**, **To Node #2** fields . Also the information is pre-populated in the **From Port #1**, **From Port #2**, **To Port #1**, and **To Port #2** fields.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- In the **Level** field, select a value from the drop-down. The available values are in the range from **1** to **6.**
- In the **Position** field, select a value from the drop-down. The available values are in the range from **1** to **3.**
- The **END POINTS** field is pre-populated.
- Select the **Compute Latency** checkbox to calculate the delay measurement after the TCM creation on endpoints of TCM trail.

Note: Currently, the TCM TPs validations are not implemented, user needs to enter correct inputs.

6

In the **FAULT MANAGEMENT** panel of the window, the **Alarm Enabling** field and **Profile Name** are pre-populated.

Note: By default, FM profile is enabled for all TCM trails.

7

In the **PERFORMANCE MONITORING** panel of the window, based on the connection, specify the PM parameters:

Change the **15-Minute PM** and the **24-Hour PM** fields to **Yes** or **No**.

The **TP Monitoring Selection** drop-down is set to **TCM Termination** and set to disabled.

Important! The PM parameters specified during the infrastructure connection or service provisioning differs from the parameters specified for TCM.

8

In the **TRANSMISSION PARAMETERS** panel of the window, based on the connection, configure the following:

- In the **Destination TCM AZ TTI**, **Destination TCM ZA TTI**, **Source TCM AZ TTI**, **Source TCM ZA TTI**, and **Operator Specific TCM TTI** fields, select a value from the drop-down.
- In the **Loss of Tandem Connection Consequent Action**, **TCM TTI Mismatch Detection Mode**, **TCM TTI Mismatch Consequent Action** fields, select a value from the drop-down.

9

Click **DEPLOY**.

Result: The TCM parameters are set for the selected infrastructure connection or service.

Note: For Control Plane terminated connections, a validation message is displayed.

Note: Click **RESET** to reset the values.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.94 Create TCM in Mixed Plane connection

Purpose

Use this task to create TCM on service in Mixed Plane Connection.

You can create TCM on services from the data table list when the TCM is enabled.

Link connection and cross connection TCM are enabled on a connection, based on the connection supported by 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, and 1830 PSS 8X shelves, and Managed Plane connection on 1830 PSS 32 for 260SCX2 service pack.

The connection must be in the **Implemented** and **Commissioned** state.

To create TCM, the TCM status must be **None**.

Important! The PM parameters specified during the service provisioning differs from the parameters specified for TCM.

Task: Create TCM from data table List

Complete the following steps to create TCM for an infrastructure connection or service from a data table list.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, use the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

Select a TCM supported connection in which the **TCM Enabled** field is **None**.

Note: TCM Enabled field status changes to **Enabled** after the creation of TCM.

4

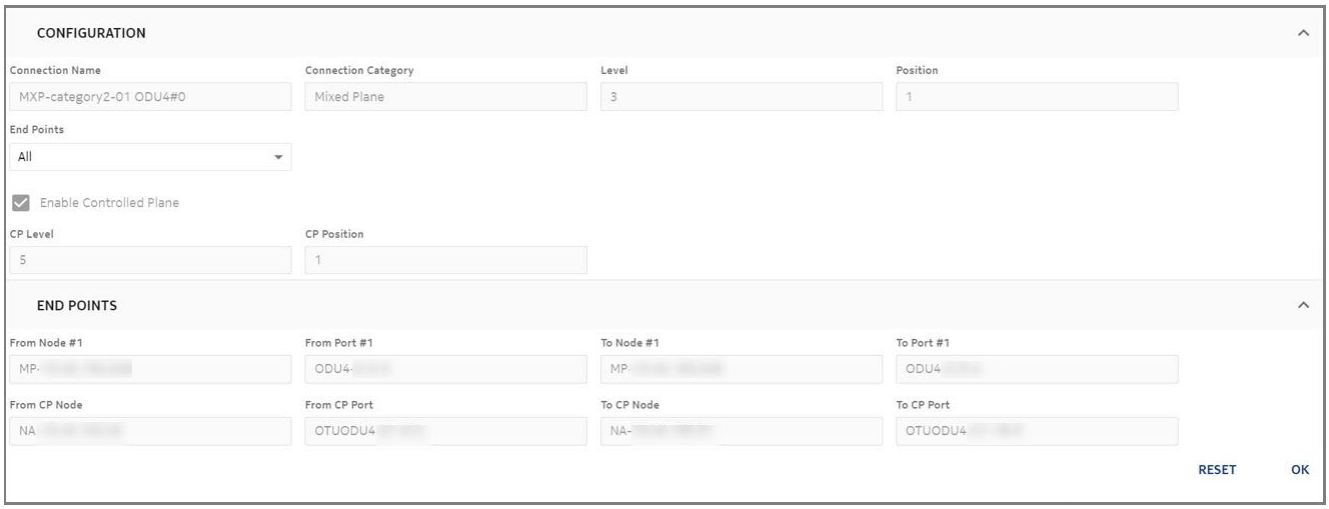
Click the **More** icon on the right of the connection row, follow this path: **TCM > Create TCM**.

Result: The Create TCM window is displayed. Depending on the selection, some fields are pre-populated.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

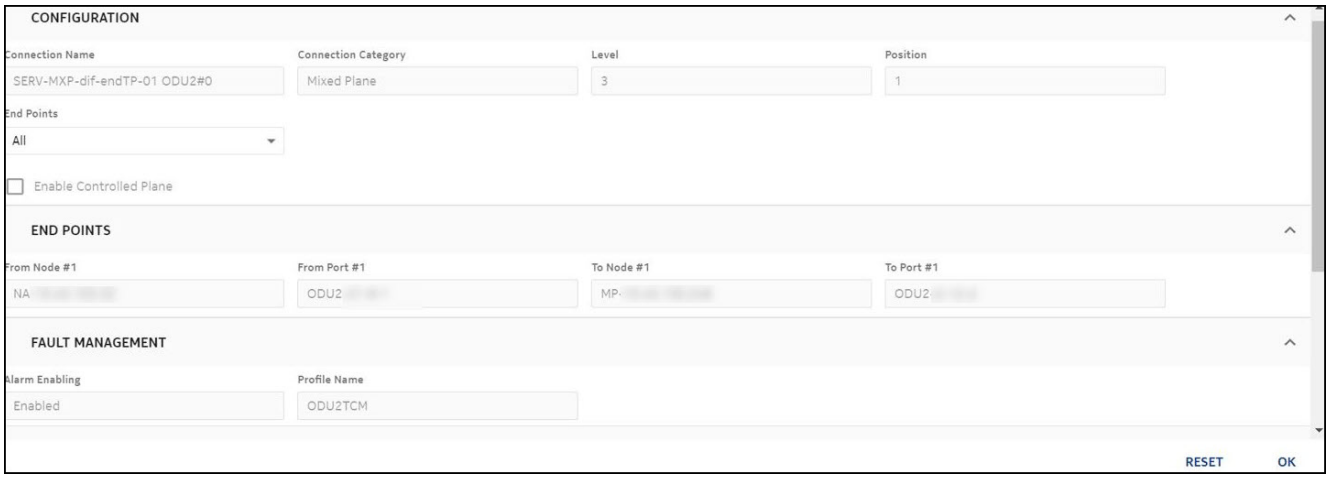
Figure 7-241 TCM – create TCM window- end TPs at external nodes

Figure 7-242 TCM – create TCM window- L1 network with extension on both sides



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-243 TCM – create TCM window- L1 network with extension on one Side and co-incident on another side



5

Configure the following:

End TPs as External nodes

In the **CONFIGURATION** panel of the window:

- The **Connection Name** and **Connection Category** fields are pre-populated.
- The **Level** and **Position** are pre-populated as **N/A**, as TCM is not supported for external nodes.
- The **END POINTS** field is pre-populated.
- The **Enable Controlled Plane** checkbox disabled for modification. If the *To TP* of end-to-end connection and ASON SNC are different, then **Enable Controlled Plane** checkbox is checked.
- The **CP Level** is pre-populated as **5** for ASON boundary connection.

  Note: NFM-T has set the value to 5. You will be able to create TCM with other values from the NE.

  The **CP Position** is pre-populated as **3** for Mixed Plane end-to-end connection.

In the **END POINTS** panel of the window:

- The end-to-end external node information are pre-populated in the **From Node #1**, **From Node #2**, **To Node #1**, and **To Node #2** fields.
- ASON SNCs nodes and ports information are pre-populated in the **From CP Node**, **From CP Port**, **To CP Node**, and **To CP Port** fields.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

L1 network with extension on both sides

In the **CONFIGURATION** panel of the window:

- The **Connection Name** and **Connection Category** fields are pre-populated.
- The **Level** and **Position** are pre-populated.
- The **END POINTS** field is pre-populated.
- The **Enable Controlled Plane** checkbox disabled for modification. If the *To TP* of end-to-end connection and ASON SNC are different, then **Enable Controlled Plane** checkbox is checked.
- The **CP Level** is pre-populated as **5** for ASON boundary connection.

  Note: NFM-T has set the value to 5. You will be able to create TCM with other values from the NE.

  The **CP Position** is pre-populated as **3** for Mixed Plane end-to-end connection.

In the **END POINTS** panel of the window:

- The node information are pre-populated in the **From Node #1**, **From Node #2**, **To Node #1**, and **To Node #2** fields.
- ASON SNCs nodes and ports information are pre-populated in the **From CP Node**, **From CP Port**, **To CP Node**, and **To CP Port** fields.

L1 network with extension on one side and co-incident on another side

In the **CONFIGURATION** panel of the window:

- The **Connection Name** and **Connection Category** fields are pre-populated.
- The **Level** and **Position** are pre-populated.
- The **Enable Controlled Plane** checkbox disabled for modification. If the *From TP* of end-to-end connection and ASON SNC are same, then **Enable Controlled Plane** checkbox is unchecked.
- The **END POINTS** field is pre-populated.
- The **Enable Controlled Plane** checkbox is unchecked, and disabled for modification.

In the **END POINTS** panel of the window:

- The node information are pre-populated in the **From Node #1**, **From Node #2**, **To Node #1**, and **To Node #2** fields.

6

In the **FAULT MANAGEMENT** panel of the window, the **Alarm Enabling** field and **Profile Name** are pre-populated.

Note: FM profile is enabled for all TCM trails.

7

In the **PERFORMANCE MONITORING** panel of the window, depending on the connection, specify the PM parameters:

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Change the **15-Minute PM** and the **24-Hour PM** fields to **Yes** or **No**.

The **TP Monitoring Selection** drop-down is set to **TCM Termination** and set to disabled.

Important! The PM parameters specified during the infrastructure connection or service provisioning differs from the parameters specified for TCM.

8

In the **TRANSMISSION PARAMETERS** panel of the window, depending on the connection, configure the following:

- In the **Destination TCM AZ TTI**, **Destination TCM ZA TTI**, **Source TCM AZ TTI**, **Source TCM ZA TTI**, and **Operator Specific TCM TTI** fields, select a value from the drop-down.
- In the **Loss of Tandem Connection Consequent Action**, **TCM TTI Mismatch Detection Mode**, **TCM TTI Mismatch Consequent Action** fields, select a value from the drop-down.

9

Click **OK**.

Result: The TCM parameters are set for the selected service.

Note: For Control Plane terminated connections, a validation message is displayed.

Note: Click **RESET** to reset the values.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.95 Create TCM from end or intermediate ports from Routing Display

Purpose

Use this task to create TCM on from end or intermediate ports from Routing Display. You can create TCM on services from the data table list when the TCM is enabled.

Task: Create TCM from end or intermediate ports

Complete the following steps to create TCM from end or intermediate ports from the Routing Display page.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPETATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, use the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

Verify that the **TCM Enabled** column displays **None**.

4

Select a TCM enabled connection, click the **Routing Display** icon on the right of the connection row.

Result: The **Routing Display** page is displayed.

5

Click **MANAGE ROUTE DISPLAY**. The **ROUTING DISPLAY DATA** panel is displayed. Select **Highlight TCM Capable Ports** checkbox and click **OK**.

Result: The TCM capable ports are highlighted.

Optional: Select the **LEGENDS** tab in the **ROUTING DISPLAY DATA** panel to view the colour identification conventions for the entities.

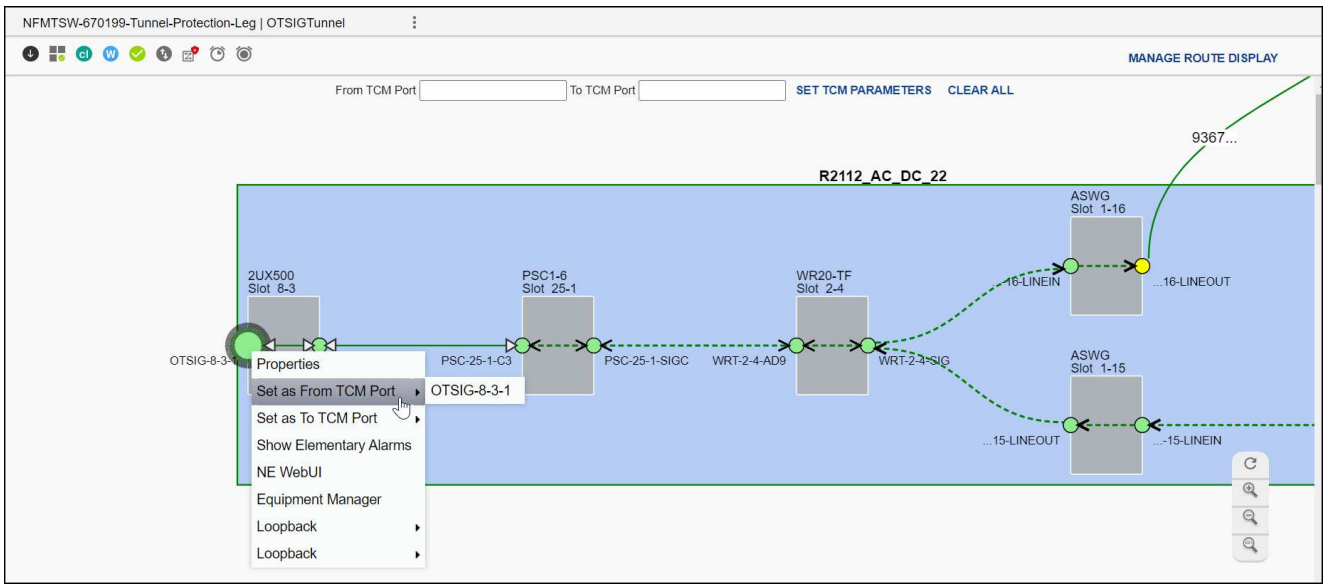
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

6

For A end TCM port, right click the highlighted intermediate port for A end, then select **Set as From TCM Port** and click the port. The **From TCM Port** field is populated with the selected value.

Similarly, select Z end point TCM port, right click the highlighted port, then select **Set as To TCM Port** and click the port. Select **CLEAR ALL** to clear the values.

Figure 7-244 TCM highlighted ports



7

Click **SET TCM PARAMETERS**.

Result: The **Create TCM** page is displayed.

8

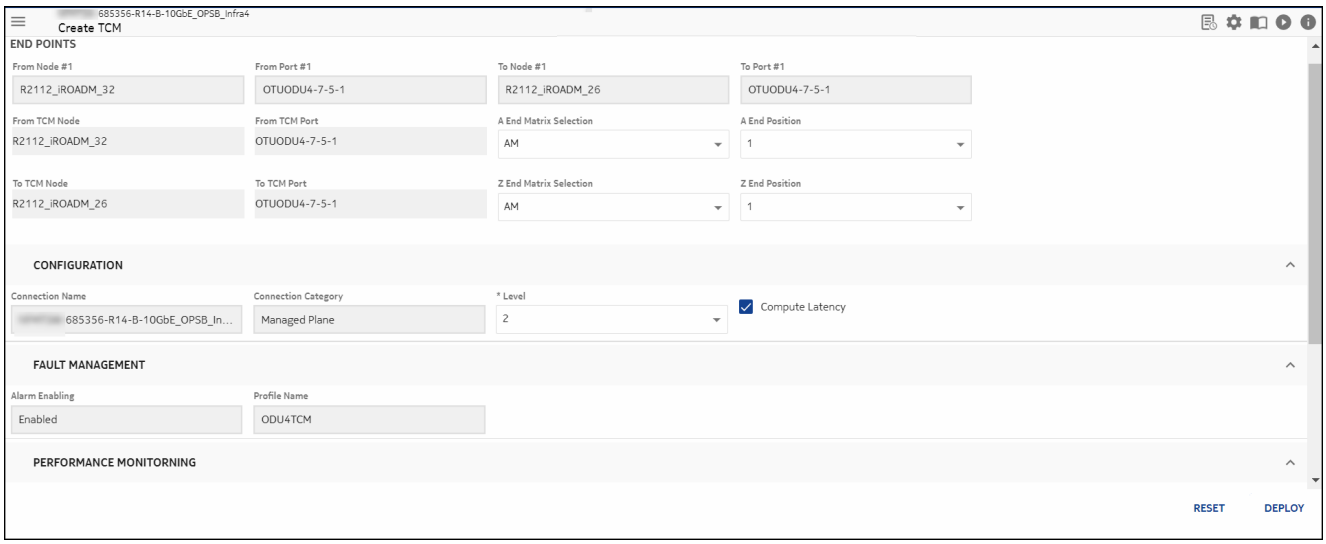
In the **END POINTS** panel, configure End Matrix and End Position, the other fields are displayed with the values automatically populated.

For more information about creating TCM, see 7.93 “Create TCM in Control Plane and Managed Plane connections” (p. 1117).

Result:

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-245 Create TCM - Routing Display



Note: Routing operations such as Modify Route or Add or Remove Connection may impact the TCM trails if the route is changed. Hence, if the original service has one or more TCM trails in the middle of the route, the user will be prompted to remove the intermediate TCM trails first, and then perform the routing operation.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.96 Navigating to TCM 360º View

Purpose

Use this task to navigate to TCM 360º View from the data table that lists all of the configured connections.

Task: Navigate to TCM 360º View

Complete the following steps to navigate to TCM 360º View.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, click the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

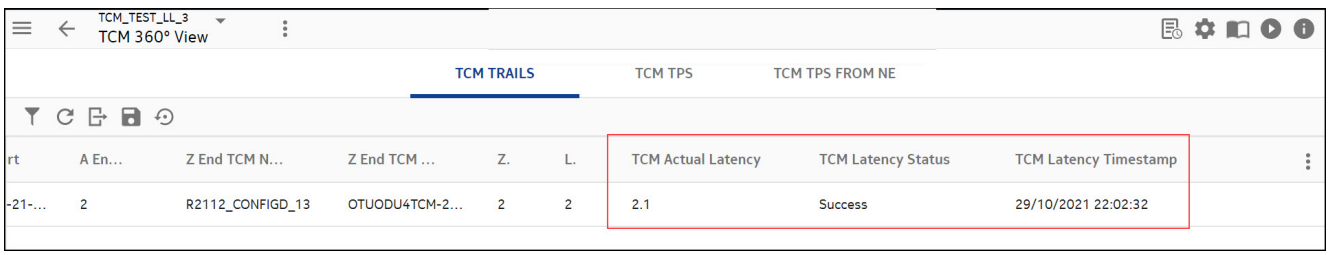
Verify that the **TCM Enabled** column displays **Enabled**.

4

Select a TCM enabled connection, click the **More** icon on the right of the connection row, follow this path: **TCM > TCM 360º View**

Result: The **TCM 360º View** page is displayed. **TCM Actual Latency**, **TCM Latency Status**, and **TCM Latency Timestamp** values are populated.

Figure 7-246 TCM 360º View



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.97 TCM TPs from the NE

When to use

Use this task to retrieve TCM Termination Points (TPs) from the NE for an infrastructure connection or service. When TCMs are created from ZIC/NE , the TCM TPs are retrieved through **TCM TPS FROM NE**, but trails are not recoverable.

Before you begin

The infrastructure connection can be a trail or a logical link.

The infrastructure connection or service must be in the **Implemented** and **Commissioned** state.

For the **TCM Enabled** field, the following values are displayed on the connection list:

- TCM is **Enabled** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has been created.
- TCM is **None** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has not been created for the connection.
- TCM is not applicable (**N/A**) if the NE is not an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, or the layer rate is DSR/OMS.
- When TCMs are created from the ZIC/NE , the TCM tps are retrieved through **TCM TPS FROM NE**, but the trails are not recoverable.

Task: Retrieve TCM TPs from NE

Complete the following steps to retrieve TCM TPs from the NE for an infrastructure connection or service from a data table list.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPETATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, use the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

Verify that the **TCM Enabled** column displays **Enabled**.

4

Select a TCM enabled connection, click the **More** icon on the right of the connection row, follow this path: **TCM > TCM 360º View > TCM TPS FROM NE (tab)**

Result: The system retrieves the TCM TPs from the NE and displays in the window.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.98 View TCM and TCM ASAP Enabled connections

When to use

Use this task to view if the TCM and TCM Alarm Severity Assignment Profile (ASAP) are enabled for an infrastructure connection or service.

Before you begin

The infrastructure connection can be a trail or a logical link.

The infrastructure connection or service must be in the **Implemented** and **Commissioned** state.

For the **TCM Enabled** field, the following values are displayed on the connection list:

- TCM is **Enabled** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has been created.
- TCM is **None** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has not been created for the connection.
- TCM is not applicable (**N/A**) if the NE is not an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, or the layer rate is DSR/OMS.

Note: The TCM ASAP is always enabled by default. The following values are displayed on the connection list:

- If TCM is **Enabled**, the **TCM ASAP Enabled** field on the connection list displays **Enabled**.
  TCM is **Enabled** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has been created.
- If TCM is **None**, the **TCM ASAP Enabled** field on the connection list displays **None**.
  TCM is **None** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has not been created for the connection.
- If TCM is **Not Applicable**, the **TCM ASAP Enabled** field on the connection list displays **N/A**.
  TCM is not applicable (**N/A**) if the NE is not an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, or the layer rate is DSR/OMS.

Task: View TCM and TCM ASAP Enabled connections

Complete the following steps to view if the TCM and TCM Alarm Severity Assignment Profile (ASAP) are enabled for an infrastructure connection or service.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections

2

In the Infrastructure Connections page, use the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

Verify that the **TCM Enabled** and **TCM ASAP Enabled** columns display **Enabled**.

4

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.

5

Optional: If you have customized the data table and you want to save your display preferences and/or if you want to reset a customized view of the data table to its default display, refer to the 26.8 "Save data table preferences and reset data table preferences to default" (p. 2218) task for detailed steps.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.99 Show TCM TPs

When to use

Use this task to show the TCM Termination Points (TPs) for an infrastructure connection or service.

Before you begin

The infrastructure connection can be a trail or a logical link.

The infrastructure connection or service must be in the **Implemented** and **Commissioned** state.

For the **TCM Enabled** field, the following values are displayed on the connection list:

- TCM is **Enabled** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has been created.
- TCM is **None** if the NE is an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, and TCM has not been created for the connection.
- TCM is not applicable (**N/A**) if the NE is not an 1830 OCS NE, 1830 PSS 24X, 1830 PSS 12X, or 1830 PSS 8X shelf, or connection is not Managed Plane on 1830 PSS 32 for 260SCX2 service pack, or the layer rate is DSR/OMS.

Task: Show TCM TPs from a data table list

Complete the following steps to show TCM TPs for an infrastructure connection or service from a data table list.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, use the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

Verify that the **TCM Enabled** column displays **Enabled**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

4

Select a TCM enabled connection, click the **More** icon on the right of the connection row, follow this path: **Show TCM TPs**.

Result: The system displays the TCM TPs in the window.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.100 Delete TCM trail

When to use

Use this task to delete a TCM trail.

Task: Delete TCM from Data Table List

Complete the following steps to delete TCM trail on an infrastructure connection or service from a data table list.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

In the Infrastructure Connections page, click the **More** icon in the upper right part of the data table and select **MANAGE COLUMNS** to add the **TCM Enabled** column to the data table.

Result: The newly added column is displayed as the last column of the table.

Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

Verify that the **TCM Enabled** column displays **Enabled**.

4

Select a TCM enabled connection, click the **More** icon on the right of the connection row, follow this path: **TCM > TCM 360º View**

Result: The **TCM 360º View** page is displayed.

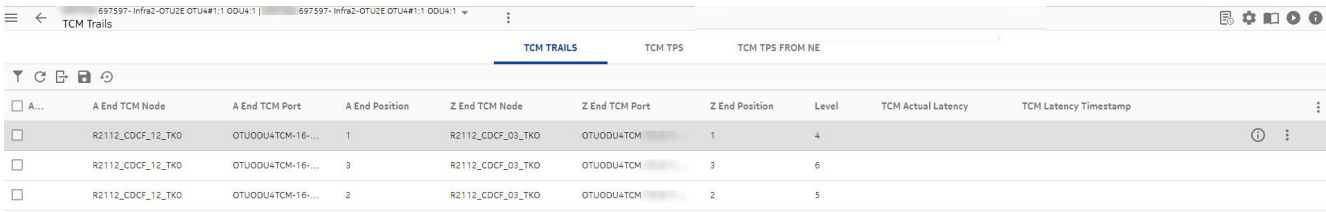
5

Click the **TCM TRAILS** tab.

Result: The system displays a data table that lists all of the TCM trails.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

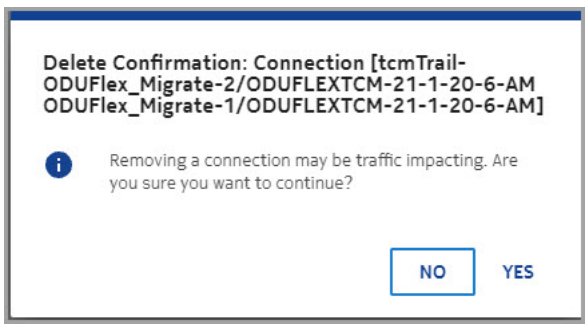
Figure 7-247 TCM trails



6

To delete a TCM trail, click the **More** icon on the right of the connection row, and click **Delete TCM Trail**.

Figure 7-248 TCM Trail - Delete Confirmation



Result: A **Delete Confirmation** window opens. Click **YES** to delete the TCM trail.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.101 TCM on-demand latency measurement

When to use

Use this task to create on-demand latency measurement from the TCM trail list for an infrastructure connection or service. User can create/configure multiple TCM layer over the network.

On-demand latency is to calculate the delay measurement after the TCM creation either at A and Z end points or at the intermediate ports on ODUk connections.

This feature is supported on Control Plane, Mixed Plane, and Managed Plane connections.

Before you begin

Ensure that the TCM is created for an infrastructure connection or service. See 7.93 “Create TCM in Control Plane and Managed Plane connections” (p. 1117)

Task: Calculating on-demand latency measurement

Complete the following steps to calculate on-demand latency measurement from the TCM trail list.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > Infrastructure Connections

OPERATE > Services

Result: Depending on your selection, the system displays a data table that lists all of the configured connections.

2

Click the **MANAGE COLUMNS** icon on top right corner and enable **TCM ENABLED** checkbox. Select **APPLY** to include the column in data table.

Result: The newly added column is displayed in the table.

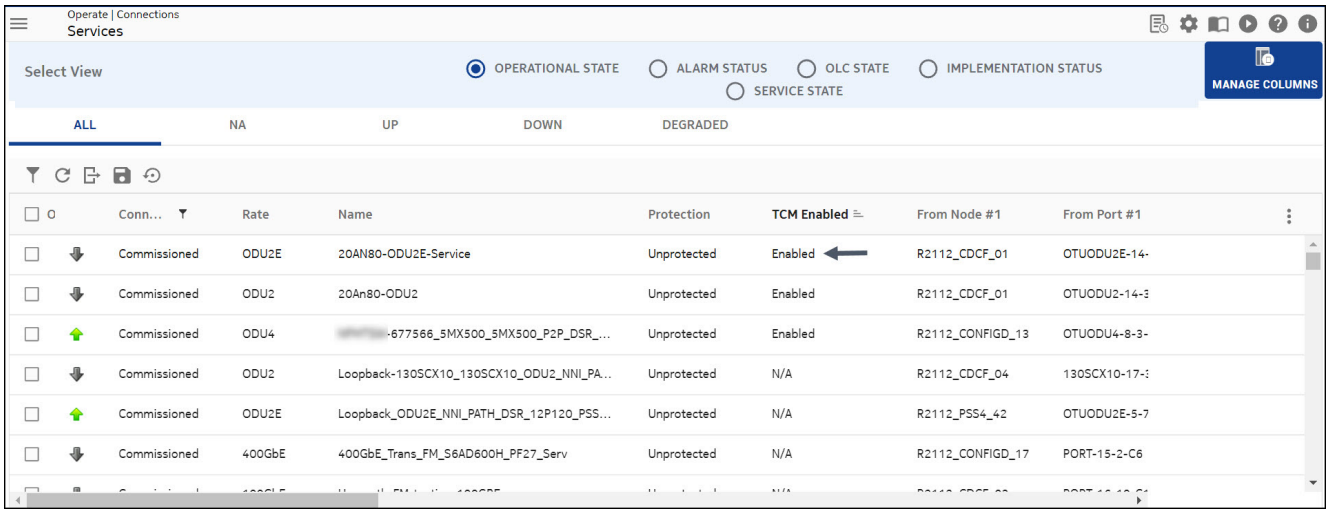
Note: The **TCM Enabled** column displays **Enabled**, **None**, or **N/A**.

3

Select a TCM supported connection in which the **TCM Enabled** column is **Enabled**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-249 TCM Enabled - Enabled



4

Click the **More** icon on the right of the connection row, follow this path:

TCM > TCM 360º View

Result: The TCM 360 view page is displayed.

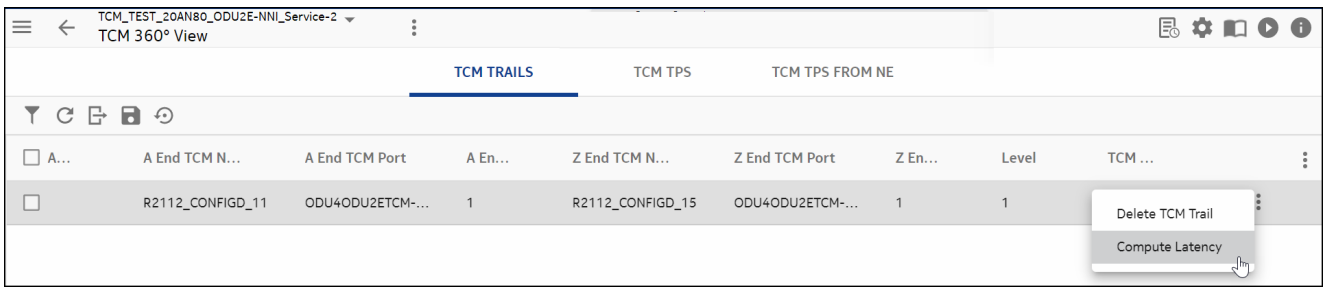
5

Click the **TCM TRAILS** tab.

6

Select a TCM trail connection, click the **More** icon the right of the connection row, and select **Compute Latency**.

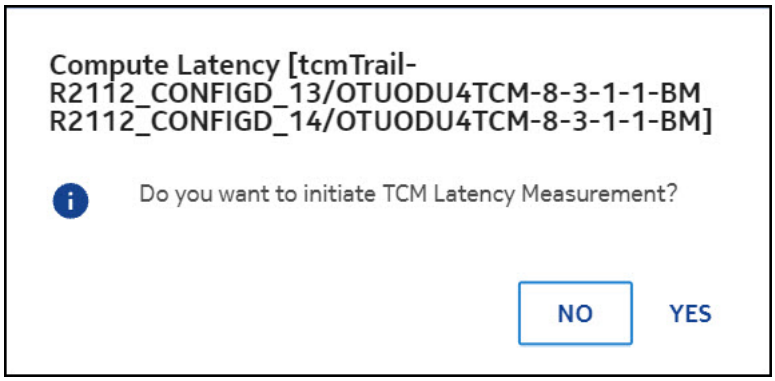
Figure 7-250 TCM trail - Compute Latency



Result: A confirmation window to initiate TCM latency measurement is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-251 TCM latency measurement - Confirmation

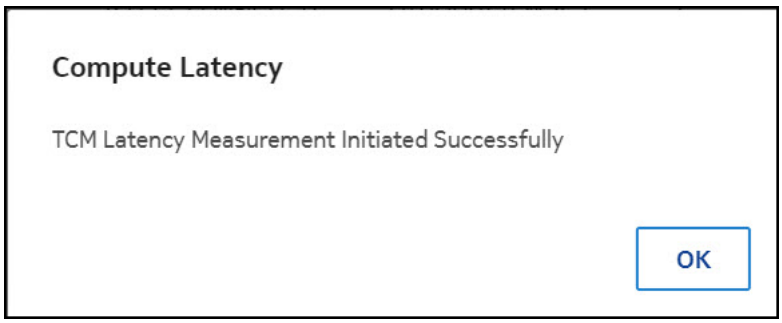


7

Click **YES**.

Result: A compute latency window for initiation of successful TCM latency measurement is displayed.

Figure 7-252 Compute Latency Initiation



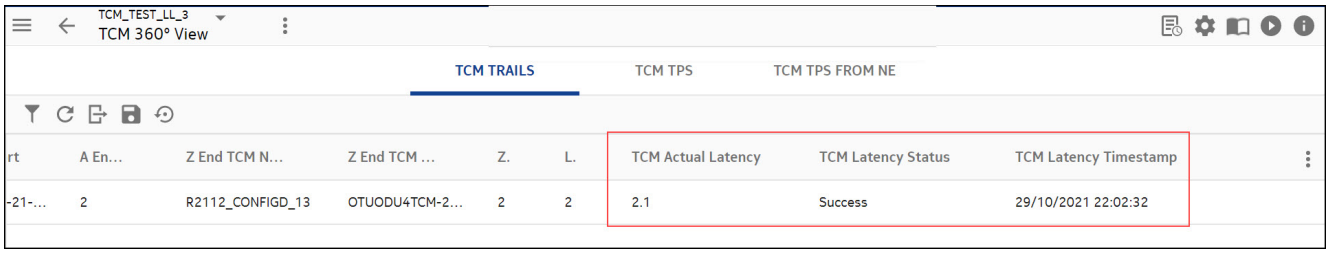
8

Click **OK**.

Result: The on-demand latency measurement is calculated. **TCM Actual Latency**, **TCM Latency Status**, and **TCM Latency Timestamp** values are updated.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-253 TCM Latency



9

Optional: To view the log and status of the on-demand latency, navigate to **ADMINISTER > Jobs**

Optional: To view the status, whether the operation is initiated or failed, navigate to **ADMINISTER > All Records**

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Ethernet Service Manager

7.102 Access the Ethernet Service Manager

Description

For information and tasks that are related to the Ethernet Service Manager, refer to the *OTN Ethernet Service Manager Guide*, which is the companion document to the *OTN Guide*.

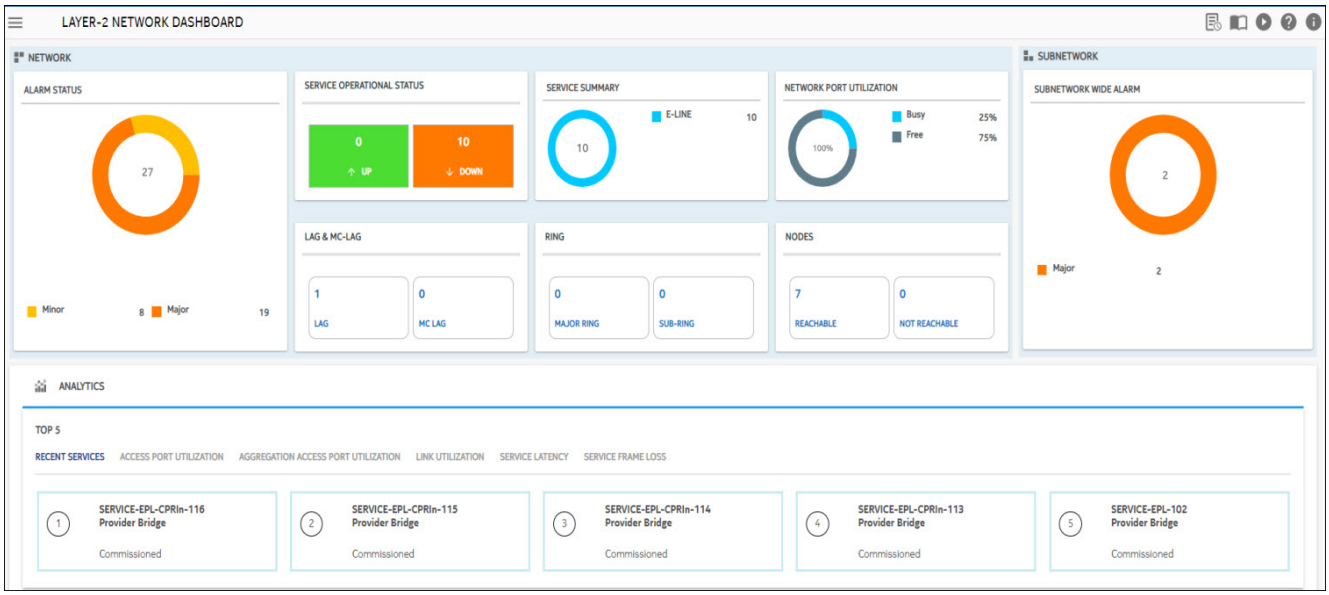
The Ethernet Service Manager is a feature of the NFM-T OTN application of the NFM-T management system. This task only enables you to access the ESM. For ESM related information and tasks, refer to the *OTN Ethernet Service Manager Guide*.

To access the Ethernet Service Manager follow this navigation path from the NFM-T GUI:

OPERATE > Ethernet Service Manager...

The system opens the ESM in a new tab and displays the Ethernet Service Manager dashboard.

Figure 7-254 ESM – dashboard



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Looped back connections

7.103 Initiate Facility Loopback Testing on an NE

When to use

Use this task to initiate Facility Loopback testing on the required NE port.

Before you begin

The NFM-T OTN supports loopbacks only for the optical transponder circuit packs (OT packs) of directly managed NEs.

In this task, the incoming received signal must be connected to the transmitter in the return direction.

A Routing Display for a DSR, OTUk, or OS connection must be open.

Supported NE

NFM-T supports loopback on 1830 PSS (R14.0 onwards), WaveLite, and 1830 ONE NEs.

Supported NE shelf types:

- 1830 PSS4
- 1830 PSS8, PSS8X
- 1830 PSS12x
- 1830 PSS16, PSS16II
- 1830 PSS24X
- 1830 PSS32
- 1830 PSS36
- 1830 PSS64
- 1830 PSI-M
- 1830ONE-Agg
- 1830ONE-Hub
- WaveLite

Task:

Complete the following steps to initiate a Facility Loopback on the required NE port.

1

From a related data table list (connection, Node/NE, looped back connection), select the appropriate connection; and depending your current location in the system:

- Right click and select the **Routing Display** icon

  Result: The Routing Display that meets your criteria is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Right click the **Port** icon of the OT port and follow the path: **Loopback > Facility Loopback**.

Result: For testing on the client or line port of a WDM OTU port, the system outputs the following pop-up message:

```
Facilty Loopback [port ID]
All services on this port will be impacted. Do you wish to continue?
```

Note: NFM-T throws a warning message when **Facility Loopback** is configured on a client port or line port enabled with GCC.
1830 PSS NEs
`Warning: You are about to configure a loopback and all services on [port-ID] will be impacted. This includes GCC interruption, which may cause loss of communication with remote NE. Continue?.`
WaveLite NE
`Loopback cannot be activated on [port-ID] until GCC (In-Band Admin Status) is disabled.` This warning is displayed in *Equipment Manager* and *Routing Display* windows.

3

Select **OK** to continue.

Result: The Facility Loopback for the selected port is successfully sent to the NE. The system outputs a pop-up message similar to the following:

```
Success
Facility Loopback: Maintenance Operation for port on NE completed
successfully.
```

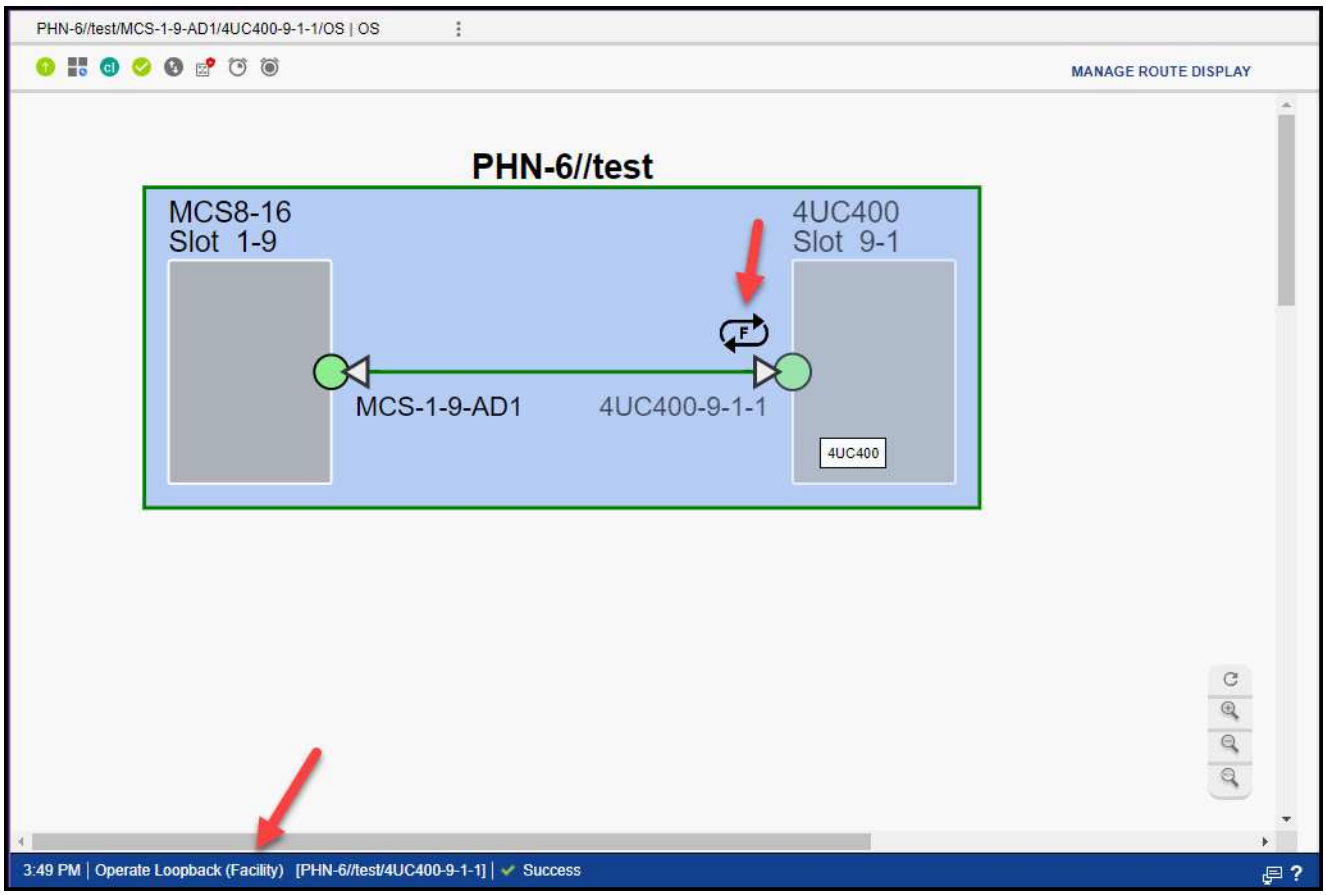
4

Click **Close** to remove the pop-up Success message.

Result: The system displays the loopback icon, which indicates that the incoming received signal is connected to the transmitter in the return direction along with a ✓ Success message at the bottom of the window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-255 Looped Back Connections – Facility Loopback successful execution



5

Optional: To release the connection from the loopback status, right click the **Port** icon of the OT port and follow the path **Loopback > Release Loopback**.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.104 Initiate Terminal Loopback testing on an NE

When to use

Use this task to initiate Terminal Loopback testing on the required NE port.

Before you begin

The NFM-T OTN supports loopbacks only for the optical transponder circuit packs (OT packs) of directly managed NEs.

A Routing Display for a DSR, OTUk, or OS connection must be open.

In this task, the entire signal that is transmitted is connected to the associated incoming receiver on an NE.

Supported NE

NFM-T supports loopback on 1830 PSS R14.0 onwards and WaveLite NEs.

Supported NE shelf types:

- 1830 PSS4
- 1830 PSS8, PSS8X
- 1830 PSS12x
- 1830 PSS16, PSS16II
- 1830 PSS24X
- 1830 PSS32
- 1830 PSS36
- 1830 PSS64
- 1830 PSI-M
- 1830ONE-Agg
- 1830ONE-Hub
- WaveLite

Task

Complete the following steps to initiate Terminal Loopback testing on an NE port.

1

From a related data table list (connection, Node/NE, looped back connection), select the appropriate connection; and depending your current location in the system, do one of the following:

- Right click and select **Routing Display**

  Result: The Routing Display that meets your criteria is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Right click the **Port** icon of the OT port and follow the path: **Loopback > Terminal Loopback**.

Result: For testing on the client or line port of a WDM OTU port, the system outputs the following pop-up message:

```
Terminal Loopback [port ID]
All services on this port will be impacted. Do you wish to continue?
```

Note: NFM-T throws a warning message when **Facility Loopback** is configured on a client port or line port enabled with GCC.
1830 PSS NEs
`Warning: You are about to configure a loopback and all services on [port-ID] will be impacted. This includes GCC interruption, which may cause loss of communication with remote NE. Continue?.`
WaveLite NE
`Loopback cannot be activated on [port-ID] until GCC (In-Band Admin Status) is disabled.` This warning is displayed in *Equipment Manager* and *Routing Display* windows.

3

Select **OK** to continue.

Result: The Terminal Loopback for the selected port is successfully sent to the NE. The system outputs a pop-up message similar to the following:

```
Success
Terminal Loopback: Maintenance Operation for port on NE completed
successfully.
```

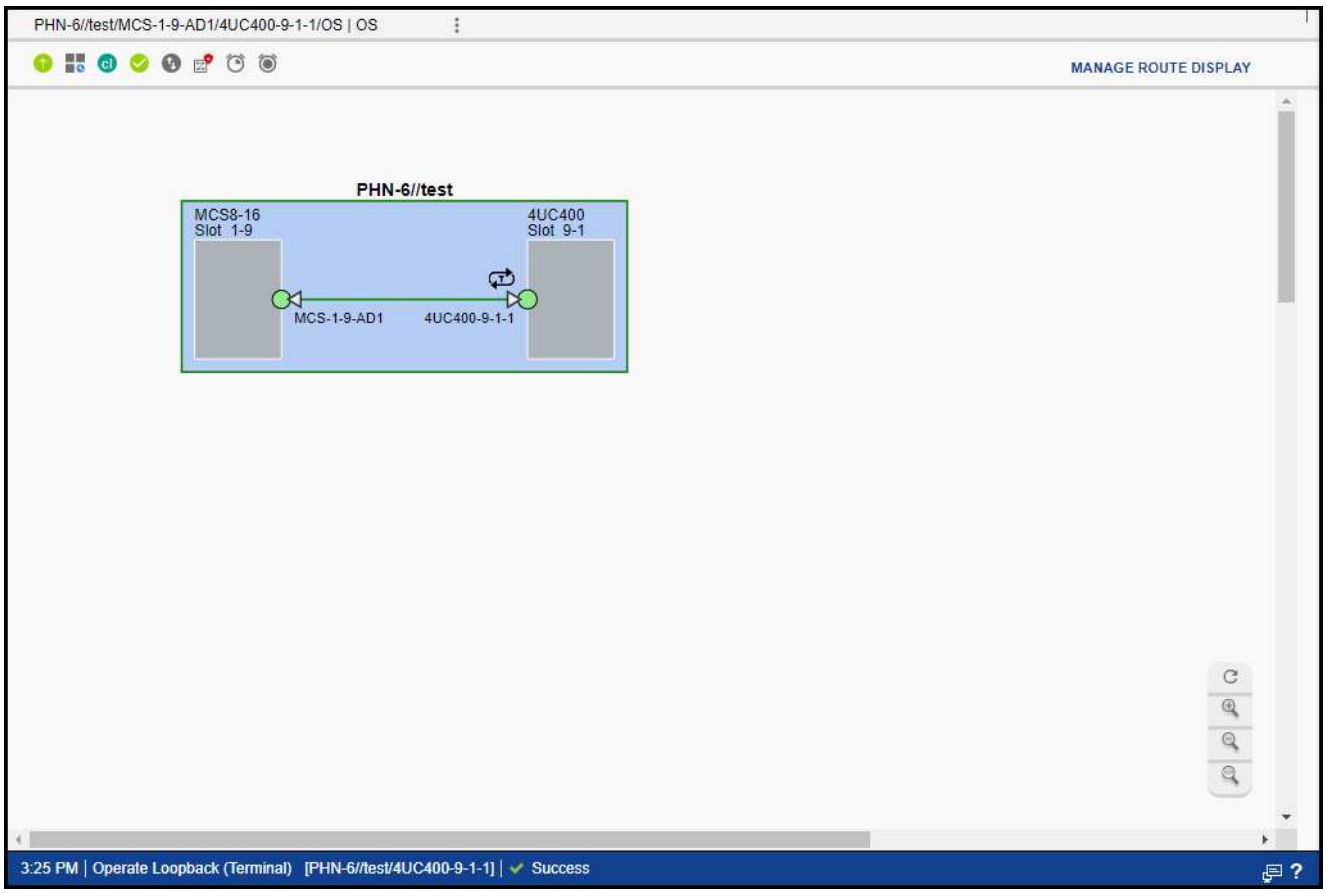
4

Click **Close** to remove the pop-up Success message.

Result: The system displays the loopback icon, which indicates that the incoming received signal is connected to the transmitter in the return direction along with a ✓ Success message at the bottom of the window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-256 Looped Back Connections – Terminal Loopback successful execution



5

Optional: To release the connection from the loopback status, right click the **Port** icon of the OT port and follow the path **Loopback > Release Loopback**.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.105 Release the loopback on a connection

When to use

Use this task to release the loopback on a connection.

Before you begin

This task is applicable for the 1830 PSS family of NEs.

Release the loopback on a connection from the loopback data table or from the Routing Display.

Task, Method 1: Release the loopback on a connection from the loopback data table

Complete the following steps to release the loopback on a connection from the Loopback Connection data table.

1

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

Operate > Looped Back Connections

Result: The system displays the Loopback Connection data table.

2

From the Loopback Connection data table, right click on a connection where loopbacks have been enabled and follow this path: **Release Loopback**.

Result: The system outputs a pop-up message similar to the following:

```
Success
Release Loopback: Maintenance Operation for port on NE completed
successfully.
```

3

Click **Close** to remove the pop-up Success message.

Result: The system removes the display of the loopback icon on the Routing Display and outputs a ✓ Success message at the bottom of the Looped Back Connections data table window.

END OF STEPS

Task, Method 2: Release the loopback on a connection from the Routing Display

Complete the following steps to release the loopback on a connection from the Routing Display.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

1

From a related data table list (connection, NE, looped back connection), select the appropriate connection; and depending your current location in the system, do one of the following:

- Right click and select **Routing Display**

  Result: The Routing Display that meets your criteria is displayed.

2

To release the connection from the loopback status, right click the **Port** icon of the OT port and follow the path **Loopback > Release Loopback**.

Result: The system outputs a pop-up message similar to the following:

```
Success
Release Loopback: Maintenance Operation for port on NE completed
successfully.
```

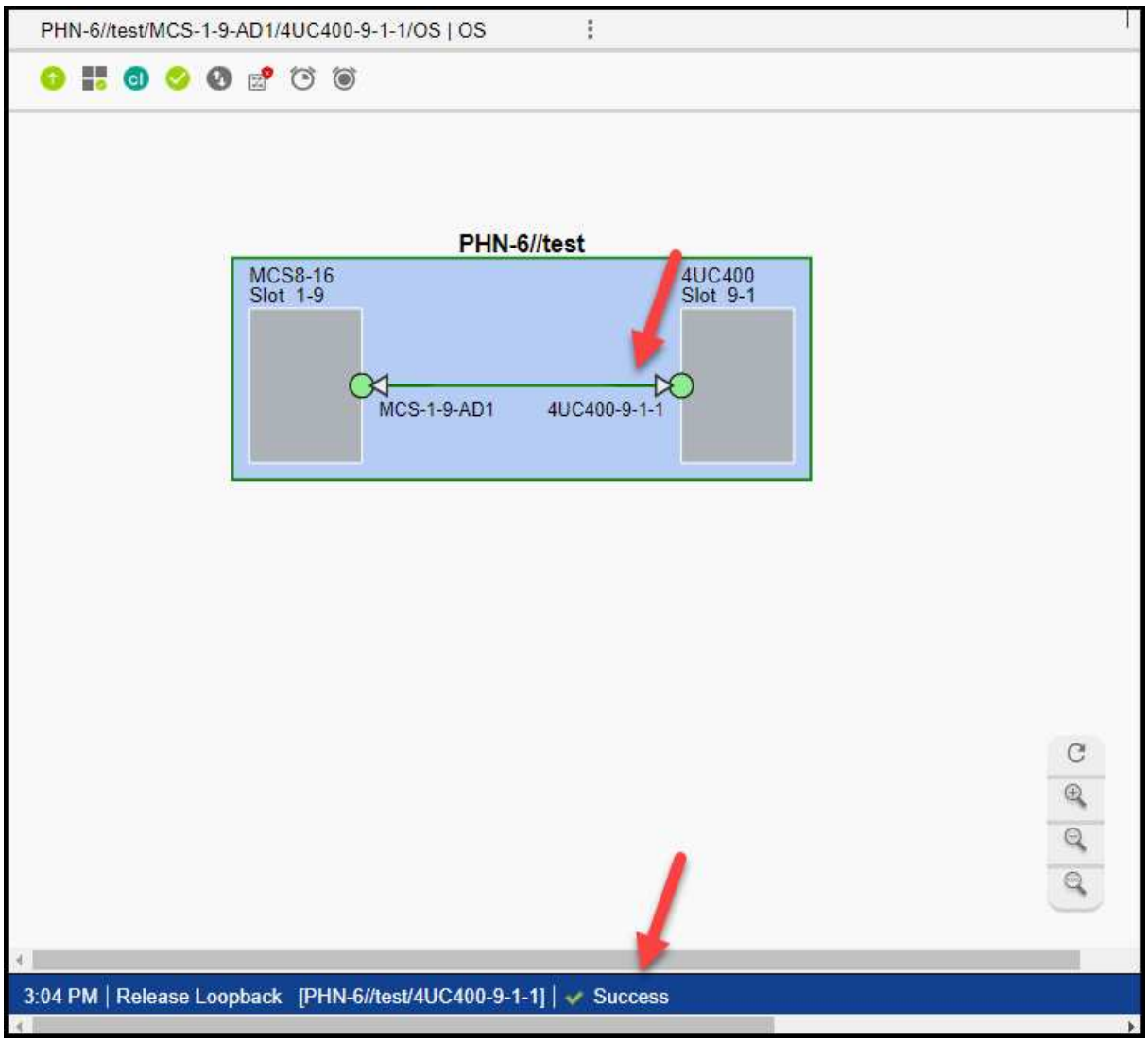
3

Click **Close** to remove the pop-up Success message.

Result: The system removes the display of the loopback icon on the Routing Display and outputs a ✓ Success message at the bottom of the window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-257 Loopback Connections – Release Loopback successful execution



End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.106 Synchronize loopback status on an NE

When to use

Use this task to synchronize loopback status on an NE.

Before you begin

A Routing Display must be open.

Task

Complete the following steps to synchronize the loopback status on an NE.

1

From a related data table list (connection, Node/NE, looped back connection), select the appropriate connection; and depending your current location in the system, do one of the following:

Click the **More** ⋮ icon at the end of the selected row and select **Routing Display**

Result: The Routing Display that meets your criteria is displayed.

2

Right click the **Port** icon to synchronize the loopback and follow the path:

Loopback > Synchronize

Result: The system outputs a pop-up message that is similar to the following:

```
Success
Synchronize: Synchronize Loopback Successfully done.
```

In addition, the system outputs a ✓ Success message at the bottom of the window.

3

Click **Close** to remove the pop-up Success message.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.107 View Looped Back Connections

When to use

Use this task to view the looped back connection list for the 1830 PSS family of NEs.

Before you begin

This task is applicable for the 1830 PSS family of NEs.

Note: The looped back connections data must be manually refreshed, they are not automatically refreshed.

Task

Complete the following steps to view the looped back connection list for the 1830 PSS family of NEs.

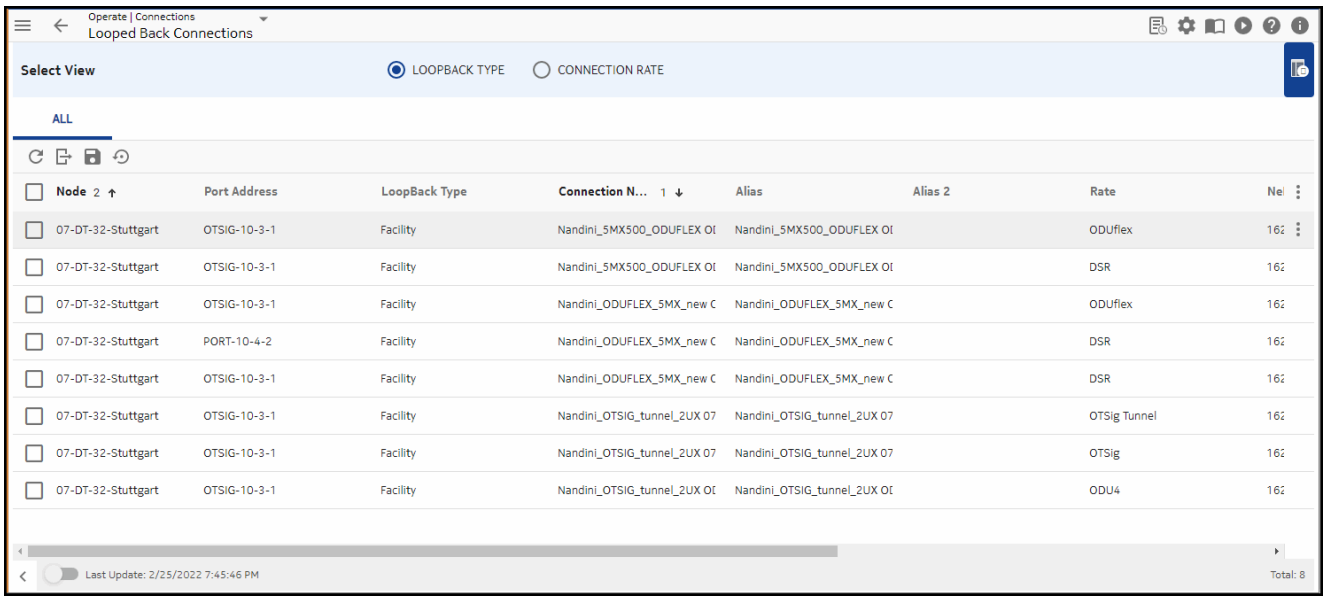
1

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

OPERATE > Looped Back Connections

Result: The system displays the Loopback Connection data table.

Figure 7-258 Looped Back Connections – data table



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Optional: To view the details of a selected object 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:

- "Sort a single column in a data table" (p. 2187)
- 26.7 "Manage data columns" (p. 2213)

4

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.

5

Optional: If you have customized the data table and you want to save your display preferences or if you want to reset a customized view of the data table to its default display, refer to the 26.8 "Save data table preferences and reset data table preferences to default" (p. 2218) task for detailed steps.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.108 View tabbed topics for a Looped Back Connection

When to use

Use this task to view tabbed topics for a looped back connection.

Task

Complete the following steps to view tabbed topics for a looped back connection.

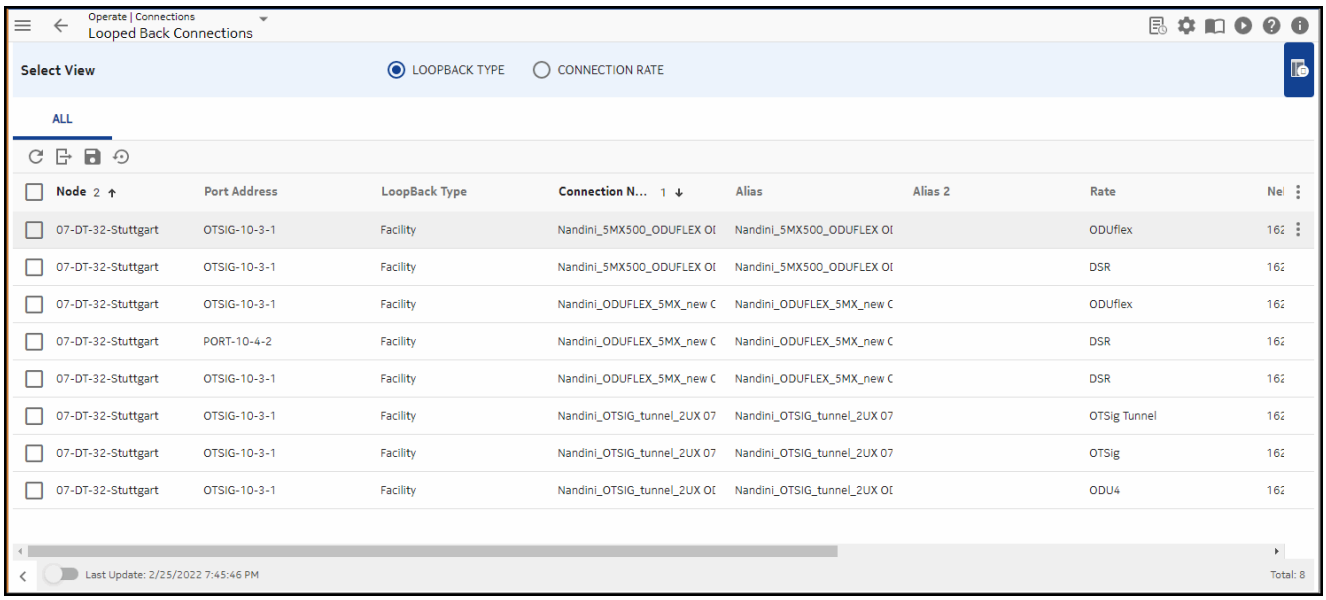
1

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

OPERATE > Looped Back Connections

Result: The system displays the Loopback Connection data table.

Figure 7-259 Looped Back Connections – Data Table



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click **Apply** to close the window and return to the **OPERATE > Looped Back Connections** page.

See 26.7 “Manage data columns” (p. 2213) for a detailed description and usage of the Manage Columns window.

Note: The **Looped Back Connections** page has three views in the Select View area.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

You can view tabbed topics for a connection. Hover over the **More** icon at the end of the selected row and selec the **360° View** icon..

Result: The related 360^0 View window is displayed.

4

The available tabs are: **ALARMS**, **SERVERS**, **ROUTE**, and **PM ENABLED POINTS**.

Important Usability Notes:

• The tabbed topics for looped back connections are the same tabbed topics that are displayed for infrastructure connections. All detailed tasks 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 loopback related information is displayed directly below the data table for the looped back connection.

5

Optional: To view the details of a selected item in a either the top or bottom data table, click on the **i** icon.

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

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Network Inconsistencies

7.109 Inconsistent connections description

Inconsistent connection definition

An *inconsistent connection* is a **Commissioned** or **Implemented** connection in which the NFM-T OTN view of the connection is *inconsistent* with the NE level view of the connection.

Inconsistent connection types

Inconsistent connections is the collective term that is used for the following types of inconsistent connections:

- Inconsistent services
- Inconsistent infrastructure connections

Inconsistent connection acknowledgment

You can acknowledge inconsistent infrastructure connections or services that have SNC Mismatches, parameter Mismatches, or ASAP Mismatches. You cannot acknowledge Download Disable Mismatches. You can acknowledge more than one inconsistent connection simultaneously.

The following guidelines apply to the order in which inconsistent connections are acknowledged:

- When you acknowledge an infrastructure connection or service from the SNC Mismatches list, if the connection appears on both the SNC Mismatches list and the Parameter Mismatches list, only the SNC Mismatches list connection is acknowledged. The Parameter Mismatches list connection remains unacknowledged.
- When you acknowledge an infrastructure connection or service from the SNC Mismatches list, if the connection appears on the SNC Mismatches list, the Parameter Mismatches list, and the ASAP Mismatches list, only the SNC Mismatches list connection is acknowledged. The Parameter Mismatches list and ASAP Mismatches connections remain unacknowledged.
- When you acknowledge an infrastructure connection or service from the Parameter Mismatches list, if the connection appears on the Parameter Mismatches list, the ASAP Mismatches list and the SNC Mismatches list, only the Parameter Mismatch list connection is acknowledged. The SNC Mismatches list and the ASAP Mismatches list connections remain unacknowledged.
- When you acknowledge an infrastructure connection or service from the ASAP Mismatches list, if the connection appears on the ASAP Mismatches list, the Parameter Mismatches list and the SNC Mismatches list, only the ASAP Mismatch list connection is acknowledged. The SNC Mismatches list and the Parameter Mismatches list connections remain unacknowledged.

Inconsistent connection events

Inconsistent infrastructure connections and inconsistent services can occur during one of the following events:

- 7.110 “ASAP Mismatches” (p. 1159)
- 7.111 “Download Disable Mismatches” (p. 1160)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- 7.112 “Parameter Mismatches” (p. 1161)
- 7.114 “SNC Mismatches ” (p. 1164)

Inconsistent connection user interaction

Users can view all inconsistent connections. With some inconsistent connections, users can Acknowledge or Restore the connections.

NFM-T has a restriction: if a connection is inconsistent due to a missing Double Add/Drop (Bi) cross connection, it cannot be restored by NFM-T. The NFM-T restores any other missing cross connection but skips the missing Double Add/Drop (Bi) cross connections. The system returns an error message: *Cannot Restore Inconsistent Connection due to inconsistent Double Add/Drop (Bi) cross connections. Inconsistencies due to missing Double Add/Drop (Bi) cross connections must be resolved using the WebUI*.

Refer to the following procedures for a detailed explanations and steps:

- 7.116 “Manage ASAP Mismatches” (p. 1167)
- 7.117 “Manage Download Disabled Mismatches” (p. 1171)
- 7.118 “Manage Parameter Mismatches” (p. 1173)
- 7.120 “Manage SNC Mismatches” (p. 1179)
- 7.122 “Manage Uncorrelated Cross Connections” (p. 1186)

Inconsistent connections table columns

To display the Inconsistent Connections table use the procedures listed in “Inconsistent connection user interaction” (p. 1158), then select the item in the drop-down list on the top right part of the window: SNC Mismatches, Parameter Mismatches, Download Disabled Mismatches, ASAP Mismatches, Uncorrelated Cross connections to display the required data table.

Column	Description
Connection Name	The name of the connection
Type	The type of the connection, Service or Infrastructure.
Service Rate	The service rate, for example ODU4, OTU2, ...
Protection	Can be Protected or Unprotected.
Mismatch Detect Date	The date where the mismatch has been detected.
Acknowledge Date	The date when the mismatch has been acknowledge, empty if it is not acknowledged.
Acknowledge User	The user that has acknowledged the mismatch, empty if it is not acknowledged.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.110 ASAP Mismatches

ASAP Mismatches definition

ASAP Mismatches, which are *Alarm Severity Assignment Profile Mismatches*, are those inconsistent connections in which the ASAPs that are associated with a **Commissioned** or **Implemented** connection differ from the ASAPs that are provisioned for the NE.

ASAP Mismatches deletion/reclassification

Inconsistent connections that have ASAP Mismatches are automatically reclassified in the NFM-T OTN in these situations:

- If a user resolves an inconsistent connection by using **Manual Disable** and **Manual Enable** actions and these actions result in no discrepancies between the NE ASAP values and the connection values, then the inconsistent connection is automatically removed from the ASAP Mismatches list.
- When an audit of the ASAP is triggered on an NE and discrepancies do not exist between the NE ASAP values and the connection values, the inconsistent connection is automatically removed from the ASAP Mismatches list.
- If a request to remove the ASAP Mismatched connection has moved to the **Commissioned** state, the inconsistent connection is automatically removed from the NFM-T OTN.

ASAP Mismatches user interaction

Users can view, acknowledge, and restore ASAP Mismatches. In addition, users can disable alarm reporting for ASAP Mismatches. Refer to the 7.116 “Manage ASAP Mismatches” (p. 1167) task for detailed steps and to 7.109 “Inconsistent connections description” (p. 1157) for a detailed description.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.111 Download Disable Mismatches

Download Disable Mismatch definition

Download Disable Mismatches are those **Commissioned** or **Implementation Complete** inconsistent connections that have commands that have not been implemented because one or more than one NE in the connection has been set to Download Disable.

Download Disable Mismatches deletion/reclassification

Download Disable Mismatches are automatically reclassified in the NFM-T OTN in these situations:

- If a Download Disable NE becomes download enabled, and all un-implemented commands for a connection are no longer disabled, the inconsistent connection is automatically removed from the Download Disable list. If any command sent to the NE as a result of enabling the download for a NE fails, the connection is added to the SNC Mismatches list and/or the Parameter Mismatches list, as required.
- If any command that is sent to the NE as a result of enabling the download for a NE fails, the connection is added to the SNC Mismatches list and/or the Parameter Mismatches list and/or the ASAP Mismatches list, as required.

Download Disable Mismatches user interaction

Users can view Download Disable Mismatches; refer to the 7.117 “Manage Download Disabled Mismatches” (p. 1171) task for detailed steps. Users cannot acknowledge or restore Download Disable Mismatches.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.112 Parameter Mismatches

Parameter Mismatches definition

Parameter Mismatches are those inconsistent connections in which the connection parameters that are associated with a **Commissioned** or **Implementation Complete** connection are different from the parameters that are provisioned for the NE.

The NFM-T OTN support for Parameter Mismatches is as follows:

- For infrastructures or services, Parameter Mismatches are supported only when the applicable port parameters, which are those port parameters that are supported through port notification, are modified. The applicable port parameters are based on the NE and the port type of the connection endpoints.
- The parameter mismatch for the client signal type parameter is supported only if the parameter is set during the corresponding service provisioning. If the signal type is set during internal link provisioning, then the signal type Mismatch is not supported for those services that are created.
- For infrastructures or services, some parameters displayed in the Transmission parameter panel are cross connection parameters. For example: ASE Noise Insertion. The Parameter Mismatches are shown as Transmission parameters on cross connection parameters and are not supported on the NFM-T OTN. The network values for cross connection parameters can be viewed for a cross connection via the Network Elements Cross Connection list.
- For 3-ended and 4-ended connections, discrepancies are reported for From Port and To Port.
- For OPSB and Y-cable protected connections, discrepancies are only reported for the working ports.

Parameter Mismatches deletion/reclassification

Parameter Mismatches are automatically reclassified in the NFM-T OTN in these situations:

- If an inconsistent connection is resolved at the NE level, the NFM-T OTN is notified of the newly-modified parameters. If the NFM-T OTN finds that no discrepancies exist between the NE (port) values and the connection values, the inconsistent connection is automatically removed from the Parameter Mismatches list.
- If a **Remove** or **DB Remove** request for an inconsistent connection is moved to the **Commissioned** state, the inconsistent connection is automatically removed from the NFM-T OTN.

Parameter Mismatches user interaction

From the Parameter Mismatches screen, users can view and acknowledge parameter mismatches for **Commissioned** or **Implementation Complete** connections in which *transmission* parameter Mismatches exist between the connection that is stored in the NFM-T OTN and the values that are provisioned in the NEs. The users cannot restore parameter Mismatches. In addition, users can view the Job List for parameter Mismatches. Refer to the 7.118 “Manage Parameter Mismatches” (p. 1173) task for detailed explanations and steps and to 7.109 “Inconsistent connections description” (p. 1157) for a detailed description.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

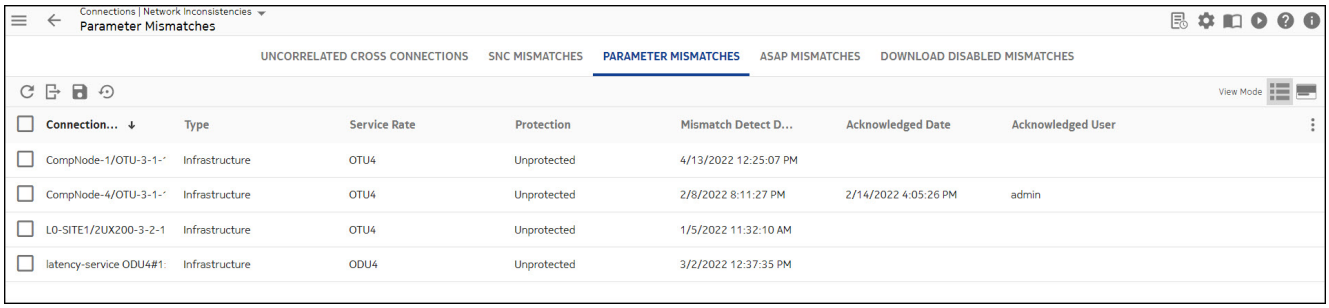
7.113 Show Parameter Mismatches

Purpose

The show Mismatches feature displays all the discrepancies of the parameter.

Show Parameter Mismatches

Figure 7-260 Parameter Mismatches



1. From the NFM-T GUI, navigate to **OPERATE > Network Inconsistencies.** By default, the uncorrelated cross connections tab is displayed.
2. Select **Parameter Mismatches** tab.
3. Select a connection, Click the **More** icon and click **Show Mismatches**.

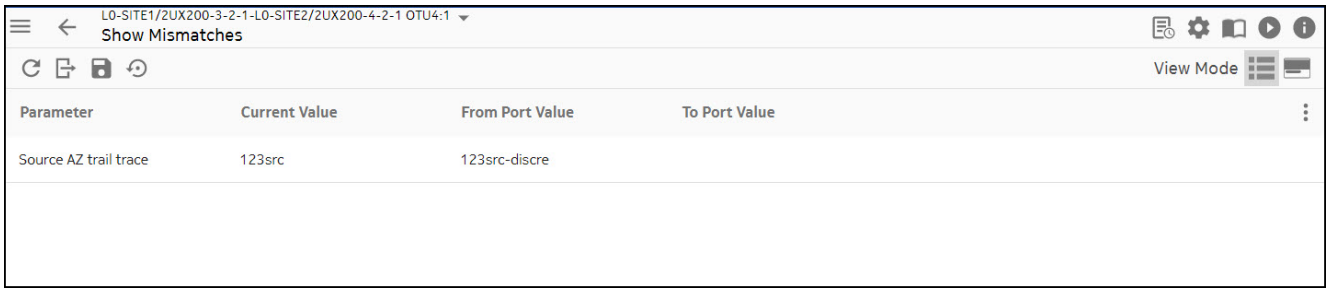
   The Show Mismatches window displays four columns:

Column Headings	Description
Parameter	Name of each transmission parameter.
Current Value	A value set by the user during creation.
From Port Value	A value set on NE From end point.
To Port Value	A value set on NE to end point.

The Show Mismatches window displays all transmission parameters for which there is a discrepancy. When the network value is different from the connection value for a port, the network value is shown. When the network value is the same as the current value, the port value is blank.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-261 Show Mismatches - Displaying Parameter



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.114 SNC Mismatches

SNC Mismatches definition

An *SNC Mismatch*, which is a *subnetwork connection Mismatch*, is a type of inconsistent connection in which one of the following events occur:

- A cross-connection is associated with a **Commissioned** or **Implemented** connection that is not provisioned in the NE.
- An OCH, ODUk, DSR, or OC-n/STM-n Multiplex Section connection is established using automatic or manual routing when an OS topological link that is associated with a **Commissioned** or **Implemented** connection is discovered or rearranged outside of the NFM-T OTN and is not provisioned in the NE.

Important! An inconsistent connection *does occur* for an OCH, ODUk, DSR, or OC-n/STM-n MS connection that is established using automatic or manual routing when an OS topological link between an OMU/ODU, OTU/OUPSR, OTU/OMU/ODU, OUPSR/OMU/ODU, or ODC/OTU/OMU/ODU that is associated with a **Commissioned** or **Implemented** connection is disconnected or rearranged outside of the NFM-T OTN application. However, an inconsistent connection *does not occur* when an OS topological link between TDM NEs and WDM NEs (both compatible optics and no compatible optics cases) is disconnected.

SNC Mismatches deletion/reclassification

Inconsistent connections that have SNC Mismatches are automatically reclassified in the NFM-T OTN in the following situations:

- If an inconsistent connection is resolved at the NE level, the NFM-T OTN is notified of the newly created cross connection. If the NFM-T OTN has a newly created cross connection whose end ports and shape match those of the inconsistent connection, and if all of the inconsistent cross connections and OS topological links in that connection are accounted for, the inconsistent connection is automatically removed from the SNC Mismatches list.
- If an inconsistent connection is resolved at the NE level, the NFM-T OTN is notified of the newly created OS topological link. If the NFM-T OTN has a newly-created OS topological link whose end ports and shape match those of the inconsistent connection, and if all of the inconsistent cross connections and OS topological links in that connection are accounted for, the inconsistent connection is automatically removed from the SNC Mismatches list.
- If a **Remove** or **DB Remove** request of an inconsistent connection is moved to the **Commissioned** state, the inconsistent connection is automatically removed from the NFM-T OTN.

SNC Mismatches restoration

SNC Mismatches can be restored by creating the missing cross connections to restore the inconsistent connection in the network to match the management system database. When performing a restore, the NFM-T OTN does not attempt to create missing OS connections.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

The NFM-T OTN determines all of the cross connections that need to be created to restore an inconsistent connection.

Restoring inconsistent connections is not supported for the following:

- If any port in any cross connection to be restored is being used in another, different, or existing active or partial cross connection.

  Exception! However, if all existing cross connections are uncorrelated and use the same ports as the inconsistent cross connection, the **Restore** function is allowed.
- If a connection has a disconnected order in the **Implemented** or **Commissioned** deployment state.

Refer to the "Task: Restore an SNC Mismatch" (p. 1181) task for detailed steps.

SNC Mismatches user interaction

Users can view, acknowledge, and restore SNC Mismatches and view ASON SNCs. In addition, users can view the Job List for SNC Mismatches. Refer to the 7.120 "Manage SNC Mismatches" (p. 1179) task for detailed explanations and steps and to 7.109 "Inconsistent connections description" (p. 1157) for a detailed description.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.115 Uncorrelated Cross Connections

Uncorrelated Cross Connection definition

An *Uncorrelated Cross Connection* is an connection within a managed NE that internally connects one logical port on an NE to one or more logical ports on the same NE; but, it is not associated with a connection that is provisioned in the NFM-T OTN.

Uncorrelated Cross Connection functional overview

An Uncorrelated Cross Connection is a cross connection that is not associated with a connection that is provisioned in the NFM-T OTN. Uncorrelated Cross Connections exist on the NE and are created outside the NFM-T OTN, for example, by using the ZIC.

An Uncorrelated Cross Connection can occur in any of the following scenarios:

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

If an Uncorrelated Cross Connection becomes a part of a connection that is either Implemented, Completed or Commissioned, the management system automatically reclassifies the Uncorrelated Cross Connection as correlated.

The management system does not display cross connections that are found on the NFM-T OTN, but are not found on the NE. These cross connections cause an inconsistent connection to exist. Refer to 7.109 “Inconsistent connections description” (p. 1157) for details.

User interaction with Uncorrelated Cross Connections

Users can view a list of Uncorrelated Cross Connections in data table format. In addition, users can remove Uncorrelated Cross Connections. Refer to the 7.122 “Manage Uncorrelated Cross Connections” (p. 1186) task for details and to 7.109 “Inconsistent connections description” (p. 1157) for a detailed description..

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.116 Manage ASAP Mismatches

When to use

Use this task to manage Alarm Severity Assignment Profile (ASAP) Mismatches.

Before you begin

Follow these guidelines before you begin any of the tasks in this procedure:

• Before you attempt to acknowledge an ASAP Mismatch, refer to "Inconsistent connection acknowledgment" (p. 1157) for a detailed explanation of the order in which inconsistent connections are acknowledged:

• Alarm reporting must have already been enabled for the ASAP Mismatch.

• You can only restore one inconsistent connection at a time.

Task: Acknowledge ASAP Mismatches

Important! Before you attempt to acknowledge an ASAP Mismatch, refer to "Inconsistent connection acknowledgment" (p. 1157) for a detailed explanation of the order in which inconsistent connections are acknowledged:

Complete the following steps to acknowledge ASAP Mismatches.

1

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

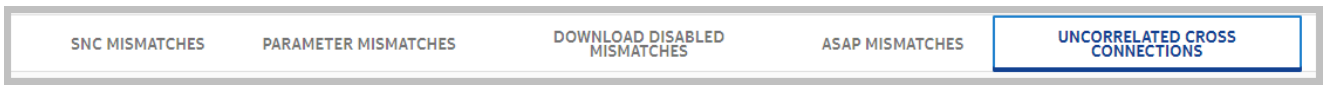
OPERATE > Network Inconsistencies

Result: The system displays the data table list for SNC Mismatches.

2

Select the **ASAP Mismatches** item from TAB, which is located to the upper left part of the data table.

Figure 7-262 Network Inconsistencies – Left Tabs



Result: The system displays the data table that you selected.

3

Select the required connection, Click on **more** icon on the right end of the selected row, and follow the path: **Actions > Acknowledge**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: You can acknowledge more that one item at one time; however, if any item that you highlight *does not* have a status of Unacknowledged, the Acknowledge action is not available. In this case, if the action is allowed, you have to Click on **more** icon on the left upper side of the screen.

Result: When the acknowledgement is completed, the **Acknowledged Date** and **Acknowledged User** fields are updated when you refresh the data table.

END OF STEPS

Task: Disable Alarm Reporting for an ASAP Mismatch

Important! Alarm reporting must have already been enabled for the ASAP Mismatch.

Complete the following steps to disable alarm reporting for an ASAP Mismatch.

1

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

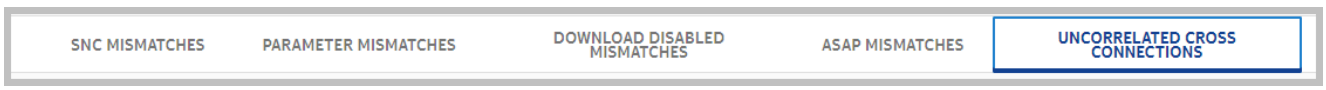
OPERATE > Network Inconsistencies

Result: The system displays the data table list for SNC Mismatches.

2

Select the **ASAP Mismatches** item from TAB, which is located to the upper left part of the data table.

Figure 7-263 Network Inconsistencies – Left Tabs



Result: The system displays the data table list for **ASAP Mismatches**.

3

Select the required connection, Click on **more** icon on the right end of the selected row, and follow the path: **Alarms > Disable Alarm Reporting**.

Result: The system displays outputs a message similar to the following:

```
Disable Alarm Reporting <connection name>
Disabling ASAPs for the connetion could take several minutes to
complete. Do you want to continue?
```

4

Click on **OK**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The system disables alarm reporting for the selected connection.

END OF STEPS

Task: Restore an ASAP Mismatch

Important! You can only restore one inconsistent connection at a time.

Complete the following steps to restore an ASAP Mismatch.

1

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

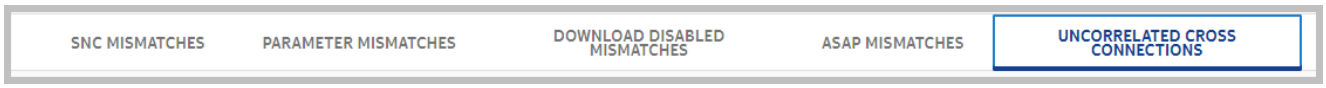
OPERATE > Network Inconsistencies

Result: The system displays the data table list for SNC Mismatches.

2

Select the **ASAP Mismatches** item from the drop-down list, which is located to the upper left part of the data table.

Figure 7-264 Network Inconsistencies – Left Tabs



Result: The system displays the data table list for **ASAP Mismatches**.

3

Select the required connection, Click on **more** icon on the right end of the selected row, and follow the path: **Restore**.

Result: If system validations are passed, a confirmation message is displayed. If you confirm the request, the selected item is restored. If the restore is successful, and you refresh the data table list, the restored connections *do not* appear.

Warning! After a restore successfully completes, do not attempt to remove any remaining Uncorrelated Cross Connections that share the same ports as the restored cross connection without first performing a database synchronization operation.

END OF STEPS

Task: View an ASAP Mismatch

Complete the following steps to view a data table list of ASAP Mismatches.

1

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

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

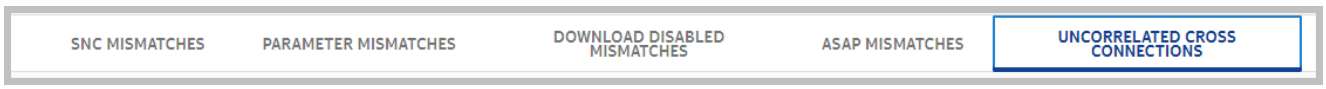
OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

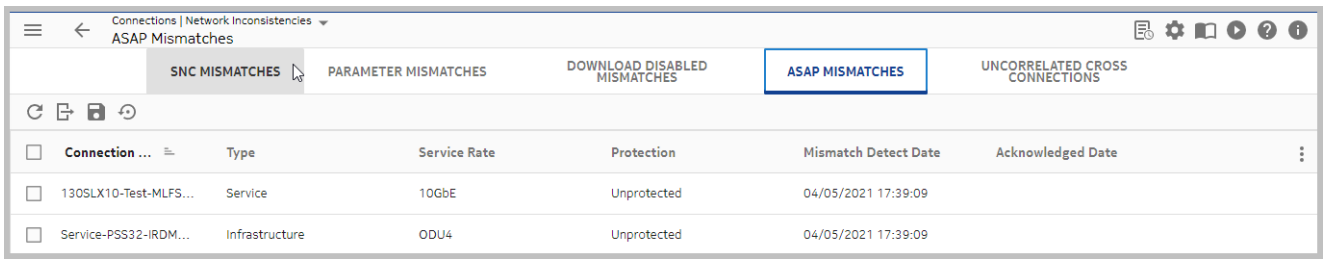
Select the **ASAP Mismatches** item from the TAB.

Figure 7-265 Network Inconsistencies – Left Tabs



Result: The system displays the ASAP Mismatches data table list.

Figure 7-266 Network Inconsistencies – ASAP Mismatches



END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.117 Manage Download Disabled Mismatches

When to use

Use this task to manage Download Disabled Mismatches.

Before you begin

An inconsistent infrastructure connection or service must exist in the NFM-T OTN application.

Task: View Download Disabled Mismatches

Complete the following steps to view a data table list of Download Disabled Mismatches.

1

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

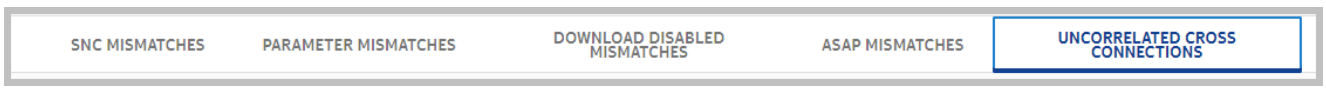
OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

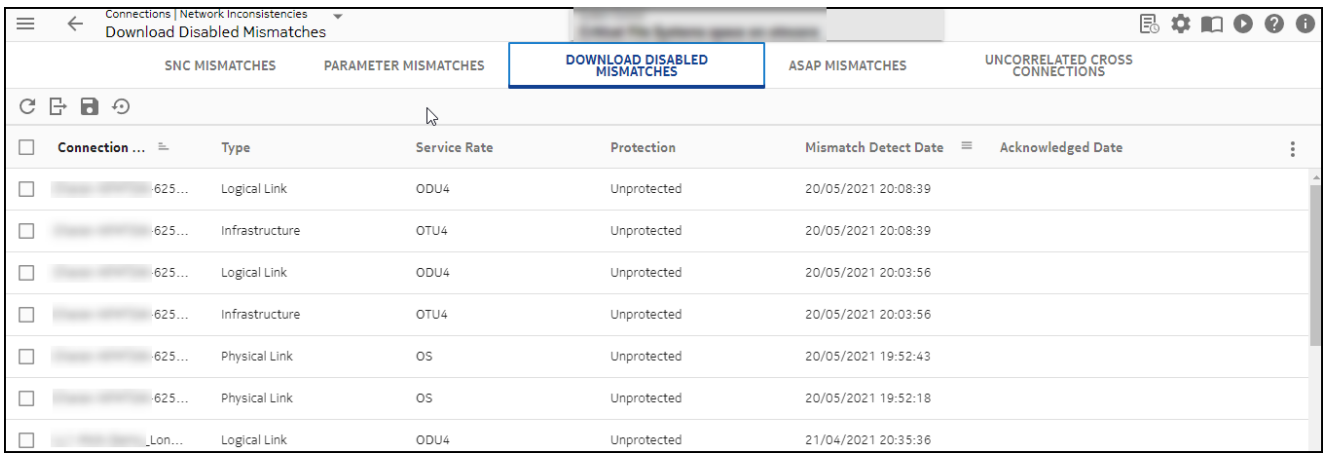
Select the **Download Disabled Mismatches** item from TAB.

Figure 7-267 Network Inconsistencies – Left tabs



Result: The system displays the data table list that you selected.

Figure 7-268 Network Inconsistencies – Download Disable Mismatches



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.118 Manage Parameter Mismatches

When to use

Use this task to modify an infrastructure connection or service that has a parameter Mismatch.

Before you begin

You can only modify inconsistent connections that are parameter Mismatches. You cannot modify inconsistent connections that are SNC Mismatches, ASAP Mismatches, and/or Download Disabled Mismatches.

Task: Acknowledge Parameter Mismatches

Important! Before you attempt to acknowledge a Parameter Mismatch, refer to "Inconsistent connection acknowledgment" (p. 1157) for a detailed explanation of the order in which inconsistent connections are acknowledged:

Complete the following steps to acknowledge Parameter Mismatches.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Select the **Parameter Mismatches** item from the TAB.

Result: The system displays the data table that you selected.

3

Select the required connection, Click on **more** icon on the right end of the selected row, and follow the path: **Actions > Acknowledge**.

Note: You can acknowledge more that one item at one time; however, if any item that you highlight *does not* have a status of Unacknowledged, the Acknowledge action is not available. In this case, if the action is allowed, you have to Click on **more** icon on the left upper side of the screen.

Result: When the acknowledgement is completed, the **Acknowledged Date** and **Acknowledged User** fields are updated when you refresh the data table.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task: Modify an Infrastructure Connection or Service with a Parameter Mismatch

Complete the following steps to modify an infrastructure connection or service that has a parameter Mismatch.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Select the **Parameter Mismatches** item from the TAB.

Result: The system displays the data table list for **Parameter Mismatches**.

3

Select the connection, Click on **more** ⋮ icon on the right end of the row, and follow the path **Modify Connection > Parameters**.

Result: The system displays the Modify Connection window, which is the template from which the connection was created.

4

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).

• The system determines which parameters you can modify based on the type of connection that you select.

• You can modify many of the Transmission Parameters; but, your ability to modify a transmission parameter can depend on the particular transmission parameter that you are trying to modify, on the current Implementation State of the connection, and on whether one or more end points have been changed.

5

Click **Deploy**.

Result: The system makes the requested changes.

END OF STEPS

Task: View Parameter Mismatches

Complete the following steps to view a list of Parameter Mismatches.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

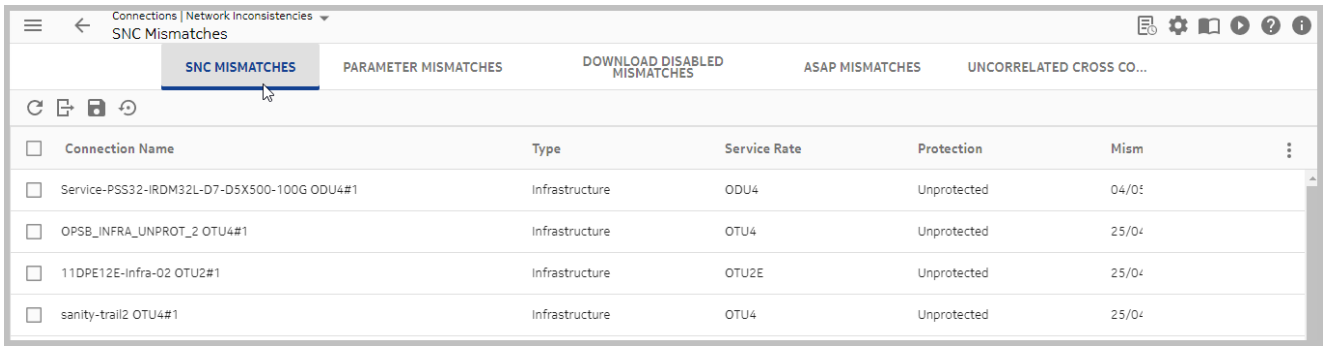
1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

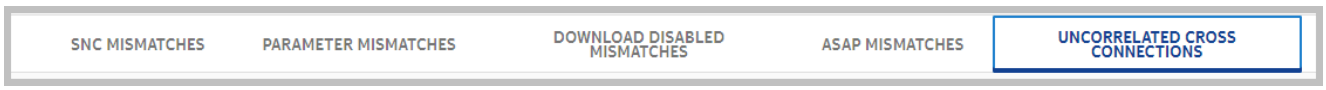
Figure 7-269 Network Inconsistencies – SNC Mismatches



2

Select the **Parameter Mismatches** item from the TAB.

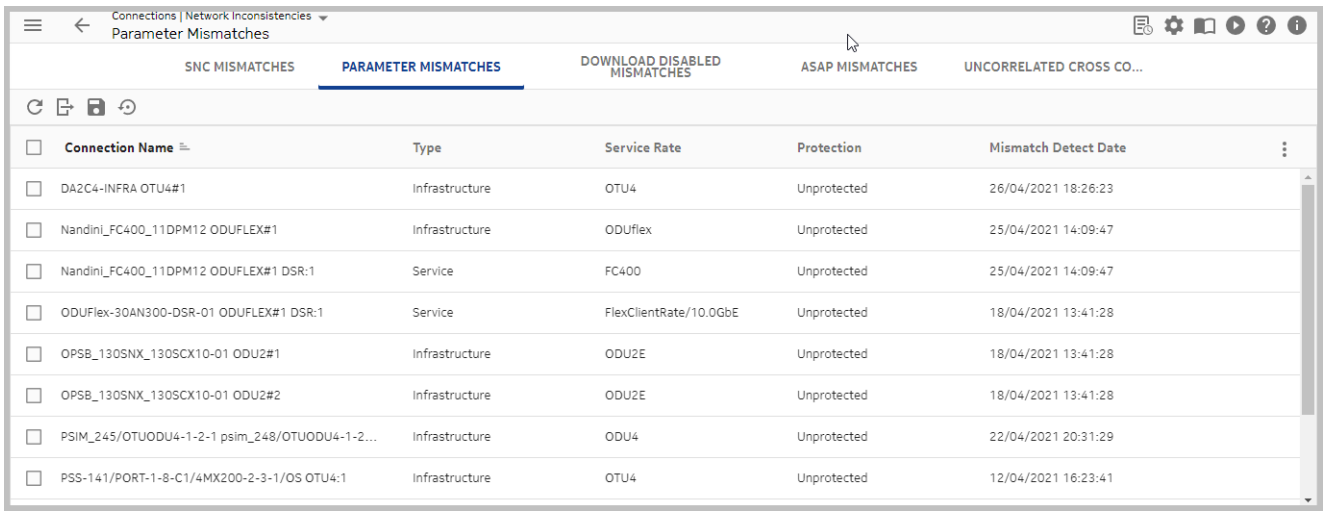
Figure 7-270 Network Inconsistencies – Left tabs



Result: The system displays the data table list that you selected.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-271 Network Inconsistencies – Parameter Mismatches



END OF STEPS

Task: View the Job List for an Parameter Mismatch

Complete the following steps to view the Job List for a parameter Mismatch.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Select the **Parameter Mismatches** item from the TAB.

Result: The system displays the **Parameter Mismatches** data table.

3

Select the parameter Mismatch; and mouse over and select the **Schedule jobs** icon.

Result: The system opens a new browser window and displays the Job List for the selected parameter Mismatch.

4

Optional: Select a job, scroll down to the bottom of the window, and click on one of the following tabs: **Details** or **Job Inventory**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The system activates the selected tab and the Job List related information is displayed directly below the data table for the Job List.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.119 Parameter Mismatches list further actions

Parameter Mismatches list further actions

Users can select an item in a data table, Click on **more** icon on the right end of the item row, and view a list of additional navigation 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 Parameter Mismatches List, selecting an object, in this case a Parameter, the user can access different Actions that are possible for the selected object.

Menu Item	Description
Failure Analysis ...	The system displays the failure analysis with cause of failure and corrective action in a new tab, see 7.70 "View Failure Analysis for an infrastructure connection or service" (p. 1013)
Acknowledge	The Acknowledge action starts and is logged in the log panel. The result of the action is displayed in the bottom of the window in the message area. If the operation is successful the fields Acknowledge Date and Acknowledge User are updated in the list. See "Inconsistent connection acknowledgment" (p. 1157)
Show Mismtaches	Show Mismatches feature displays all the discrepancies of the parameter
Modify Parameters ...	The Path Creation window of the selected connection opens and allows to modify the connection parameters. See 7.62 "Modify the parameters of a connection" (p. 981)
Add Note	A window is open displaying the connection selected and a note can by typed and saved. See 24.9 "Manage Note for a Selected Object" (p. 2002)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.120 Manage SNC Mismatches

Before you begin

Controlling the Deployment of a Selected SNC Mismatch

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, you can track the progress of your provisioning request (an order) and your can perform actions on a particular request.

You can manage the deployment state of SNCs (infrastructure connections). Depending on the existing deployment state of the SNC, the configuration state that can be managed can 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 7-23 Deployment Control for SNCs

Deployment Control for SNCs	
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.
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 database.
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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 7-23 Deployment Control for SNCs (continued)

Deployment Control for SNCs	
Depending on the state of a particular provisioning request (order), NFM-T GUI Deployment Control includes the following states:	
Deployment Control State	Meaning
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: Acknowledge an SNC Mismatch

Important! Before you attempt to acknowledge an SNC Mismatch, refer to "Inconsistent connection acknowledgment" (p. 1157) for a detailed explanation of the order in which inconsistent connections are acknowledged:

Complete the following steps to acknowledge SNC Mismatches

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Select the required connection, Click on **more** ⋮ icon on the right of the connection row, and follow the path: **Actions > Acknowledge**.

Note: You can acknowledge more that one item at one time; however, if any item that you highlight *does not* have a status of Unacknowledged, the Acknowledge action is not available.

Result: When the acknowledgement is completed, the **Acknowledged Date** and **Acknowledged User** fields are updated when you refresh the data table.

END OF STEPS

Task: Control the Deployment of an SNC Mismatch

Important! To understand order processing and the deployment control of an SNC Mismatch, read Before you begin "Before you begin" (p. 1179).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Complete the following steps to control the deployment of a selected SNC.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Depending on the existing Deploy State and Deploy Status of the SNC, Click on **more** icon on the right of the connection row, and follow the path **Deployment Control**, and select one of the options displayed. See Table 7-23, “Deployment Control for SNCs” (p. 1179).

Result: Depending on your selection, the system changes the deployment state to reflect your selection and/or outputs a message.

END OF STEPS

Task: Restore an SNC Mismatch

Important! You can only restore one inconsistent connection at a time.

Complete the following steps to restore an SNC Mismatch.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Select the required connection, Click on **more** icon on the right of the connection row, and follow the path: **Restore**.

Result: If system validations are passed, a confirmation message is displayed. If you confirm the request, the selected item is restored. If the restore is successful, and you refresh the data table list, the restored connections *do not* appear.

Warning! After a restore successfully completes, do not attempt to remove any remaining Uncorrelated Cross Connections that share the same ports as the restored cross connection without first performing a database synchronization operation.

END OF STEPS

Task: View an ASON SNC

Important! The SNC (infrastructure connection) must exist in the NFM-T OTN application.

Complete the following steps to view an ASON SNC for a selected SNC Mismatch.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

1

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

OPERATE > Network Inconsistencies

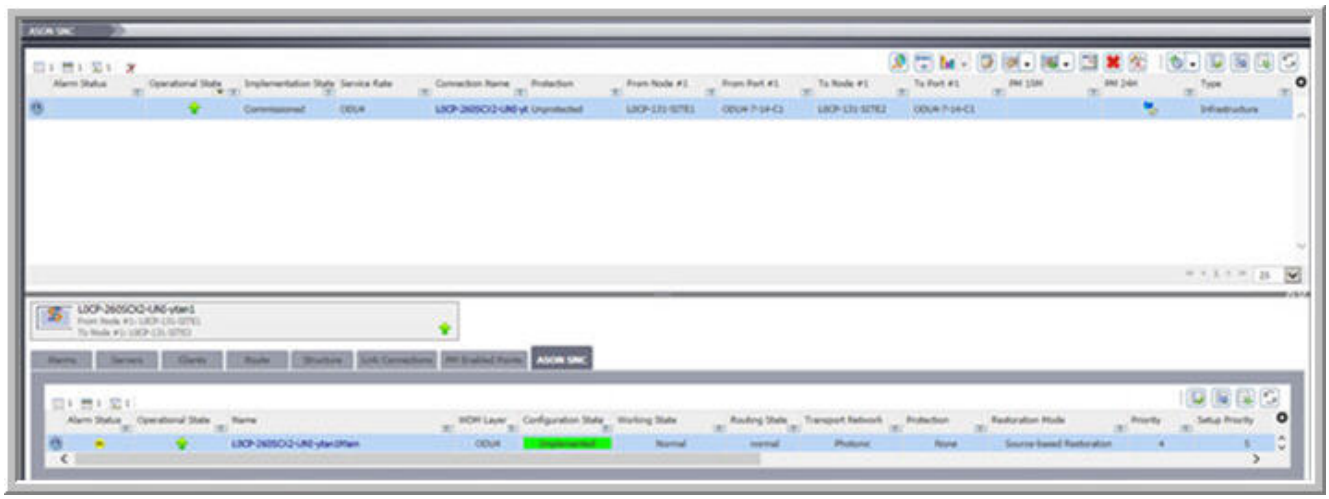
Result: The system displays the data table list as default.

2

Right click on an SNC and select **ASON SNC**.

Result: The system opens a new tab and displays the ASON SNC for the selected SNC Mismatch.

Figure 7-272 Network Inconsistencies – SNC Mismatches – ASON SNC



END OF STEPS

Task: View an SNC Mismatch on the Routing Display

Important! The SNC (infrastructure connection) must exist in the NFM-T OTN application.

Complete the following steps to view a selected SNC Mismatch on the Routing Display.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Select the required connection, Click on **more** icon on the right of the connection row, and follow the path: **Routing Display**.

Result: The system displays the Routing Display for the selected SNC.

End of steps

Task: View the Job List for an SNC Mismatch

Complete the following steps to view the Job List for an SNC Mismatch.

1

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

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

Select the required connection, Click on **more** icon on the right of the connection row, and follow the path: **Schedule jobs** icon.

Result: The system opens a new browser window and displays the Job List for the selected parameter Mismatch.

3

Optional: Select a job, scroll down to the bottom of the window, and click on one of the following tabs: **Details** or **Job Inventory**.

Result: The system activates the selected tab and the Job List-related information is displayed directly below the data table for the Job List.

End of steps

Task: View SNC Mismatches

Complete the following steps to view a data table list of SNC Mismatches.

1

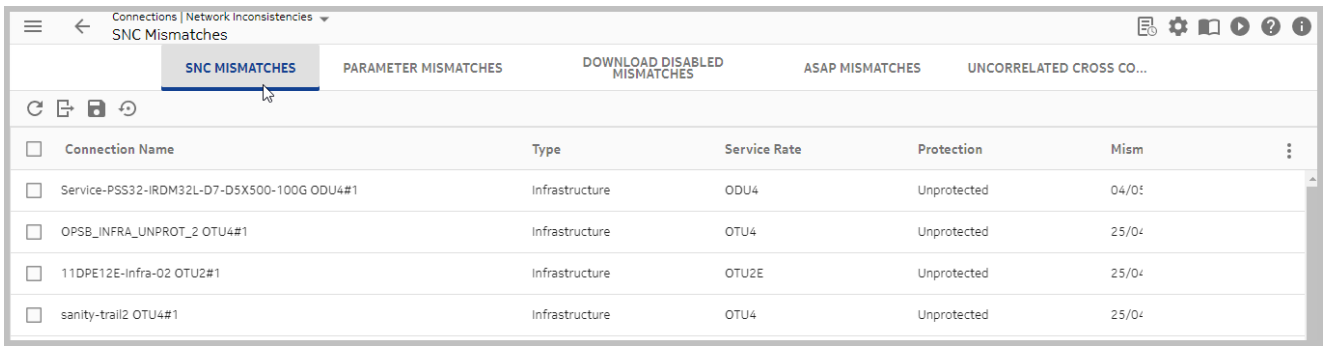
From the NFM-T GUI, follow this navigation path:

OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-273 Network Inconsistencies – SNC Mismatches



END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.121 SNC Mismatches list further actions

SNC Mismatches list further actions

Users can select an item in a data table, Click on **more** icon on the right end of the item row, and view a list of additional navigation 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 SNC Mismatches List, selecting an object, in this case a Subnetwork Connection, the user can access different Actions that are possible for the selected object.

Menu Item	Second Level Menu Item	Description
Acknowledge		The Acknowledge action starts and is logged in the log panel. The result of the action is displayed in the bottom of the window in the message area. If the operation is successful the fields Acknowledge Date and Acknowledge User are updated in the list. See "Inconsistent connection acknowledgment" (p. 1157)
Restore		The Restore action starts and the result of the action is displayed in the bottom of the window in the message area. SNC Mismatches can be restored by creating the missing cross connections to restore the inconsistent connection in the network to match the management system database. See "SNC Mismatches restoration" (p. 1164) and "Task: Restore an SNC Mismatch" (p. 1181)
Routing Display		This function displays the Routing Display of the SNC.
Deployment Control	Allocate, Implement, Deimplement, Commission (In Service) Complete Step, Complete Order, Cancel, Abort Order Processing, Move Forward one Command Set, Move Backward one Command Set	See the table Table 7-23, "Deployment Control for SNCs" (p. 1179)
	Delete from NFM-T Delete Connection and Clients from NFM-T	A confirmation message is displayed to avoid genarating discrepancies on the system, deleting the connection from database.
Add Note		A window is open displaying the connection selected and a note can by typed and saved. See 24.9 "Manage Note for a Selected Object" (p. 2002)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.122 Manage Uncorrelated Cross Connections

Task: Remove Uncorrelated Cross Connections

Complete the following steps to remove an Uncorrelated Cross Connection.

1

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

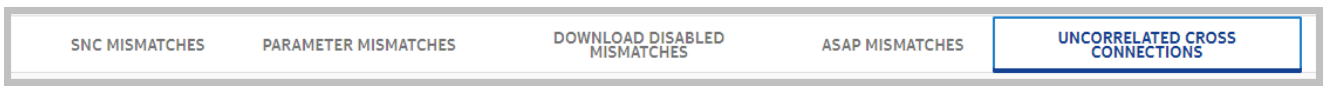
OPERATE > Network Inconsistencies

Result: The system displays the data table list as default.

2

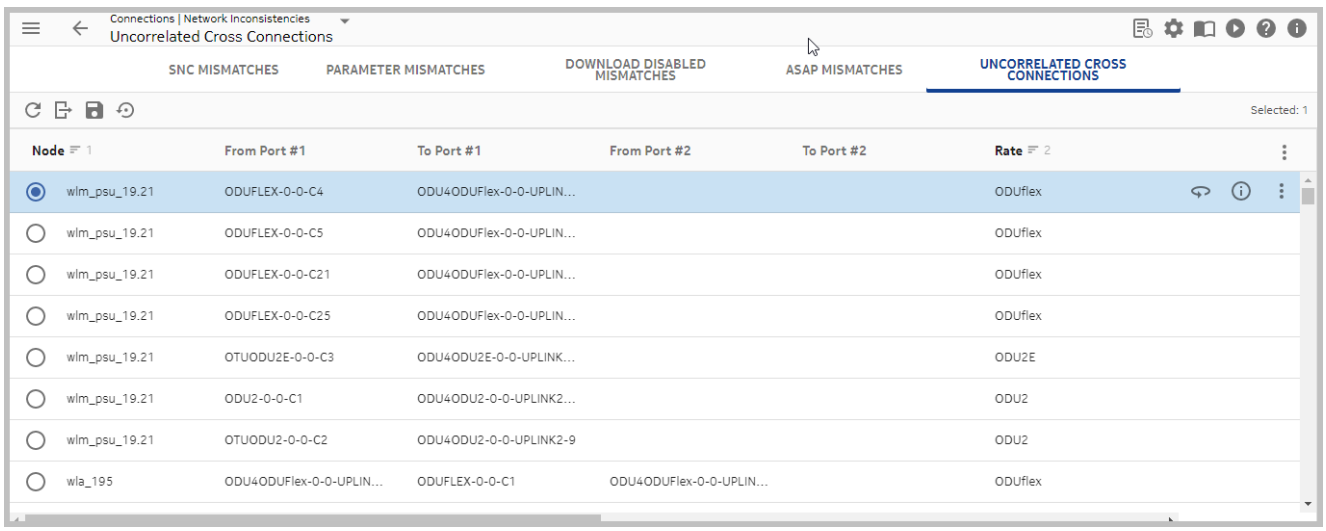
Select the **Uncorrelated Cross Connection** item from the TAB.

Figure 7-274 Network Inconsistencies – left tabs



Result: The system displays the data table list of Uncorrelated Cross Connections.

Figure 7-275 Network Inconsistencies – Uncorrelated Cross Connections



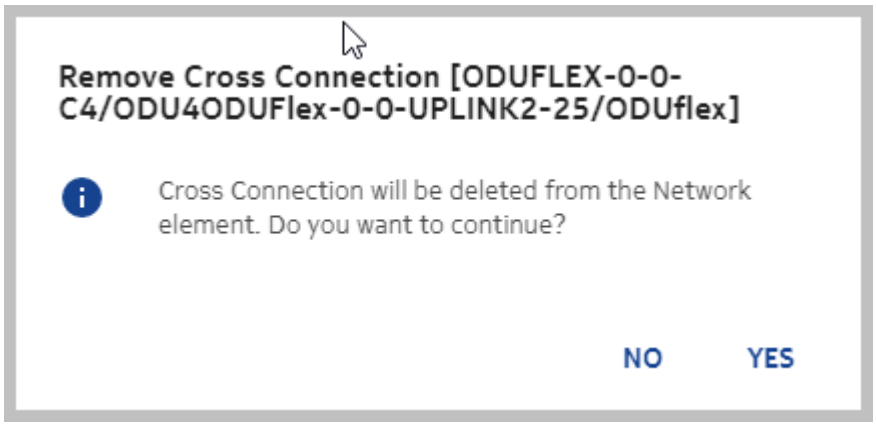
3

Select the Uncorrelated Cross Connection. Click on **more** icon on the right of the connection row, and follow the path **Remove Cross Connection**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The system outputs a query similar to the following:

Figure 7-276 Network Inconsistencies – uncorrelated cross connections – remove query



4

Select **Yes**.

Result: The system outputs a **SUCCESS** message, similar to the message in the following figure.

Figure 7-277 Network Inconsistencies – uncorrelated cross connections – remove Successful

END OF STEPS

Task: View Uncorrelated Cross Connections

Complete the following steps to view a list of Uncorrelated Cross Connections.

1

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

OPERATE > Network Inconsistencies

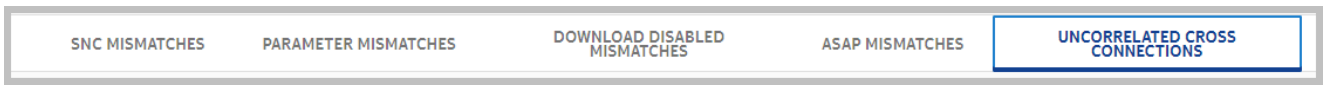
Result: The system displays the data table list as default.

2

Select the **Uncorrelated Cross Connection** item from the TAB.

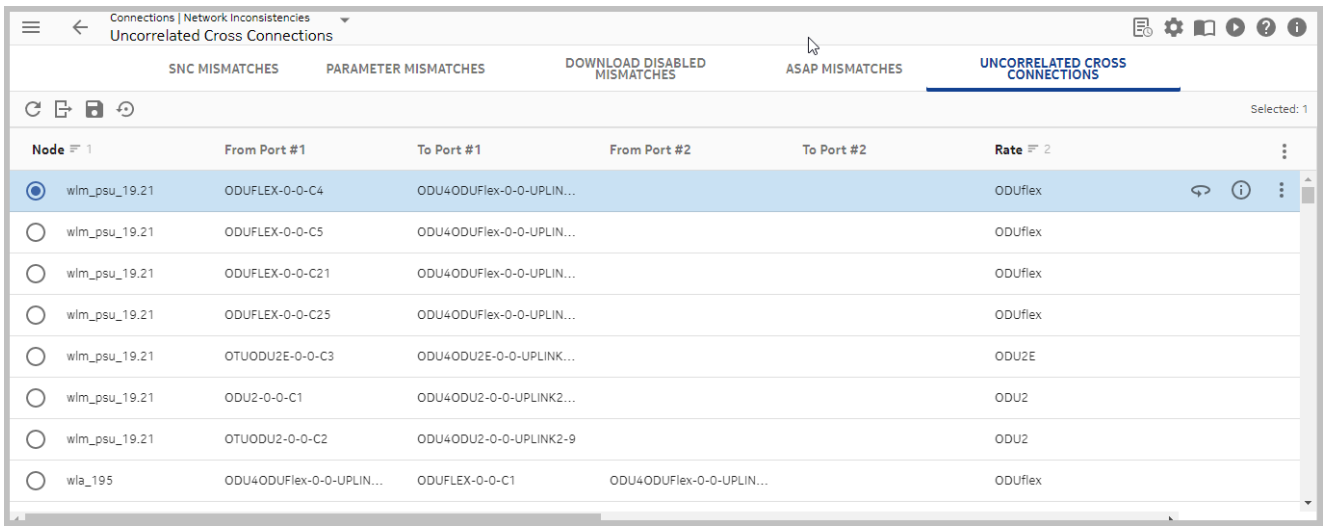
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-278 Network Inconsistencies – left tabs



Result: The system displays the data table list of Uncorrelated Cross Connections.

Figure 7-279 Network Inconsistencies – uncorrelated cross connections



3

Optional: From the initially displayed data table list, right click on an item and select **Properties**.

Result: The Details window for the selected item is displayed.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.123 Uncorrelated Cross Connections list further actions

Uncorrelated Cross Connections list further actions

Users can select an item in a data table, Click on **more** icon on the right end of the item row, and view a list of additional navigation 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 Uncorrelated Cross Connections List, selecting an object, in this case a Uncorrelated Cross Connection, the user can access different Actions that are possible for the selected object.

Menu Item	Description
Properties	The selected cross connection properties window is displayed. See "Inconsistent connection acknowledgment" (p. 1157)
Remove Cross Connection	A confirmation message is displayed advising that the cross connection will be deleted from the NE. See 7.122 "Manage Uncorrelated Cross Connections" (p. 1186)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Wavelength Usage Report

7.124 Wavelength Usage Report description

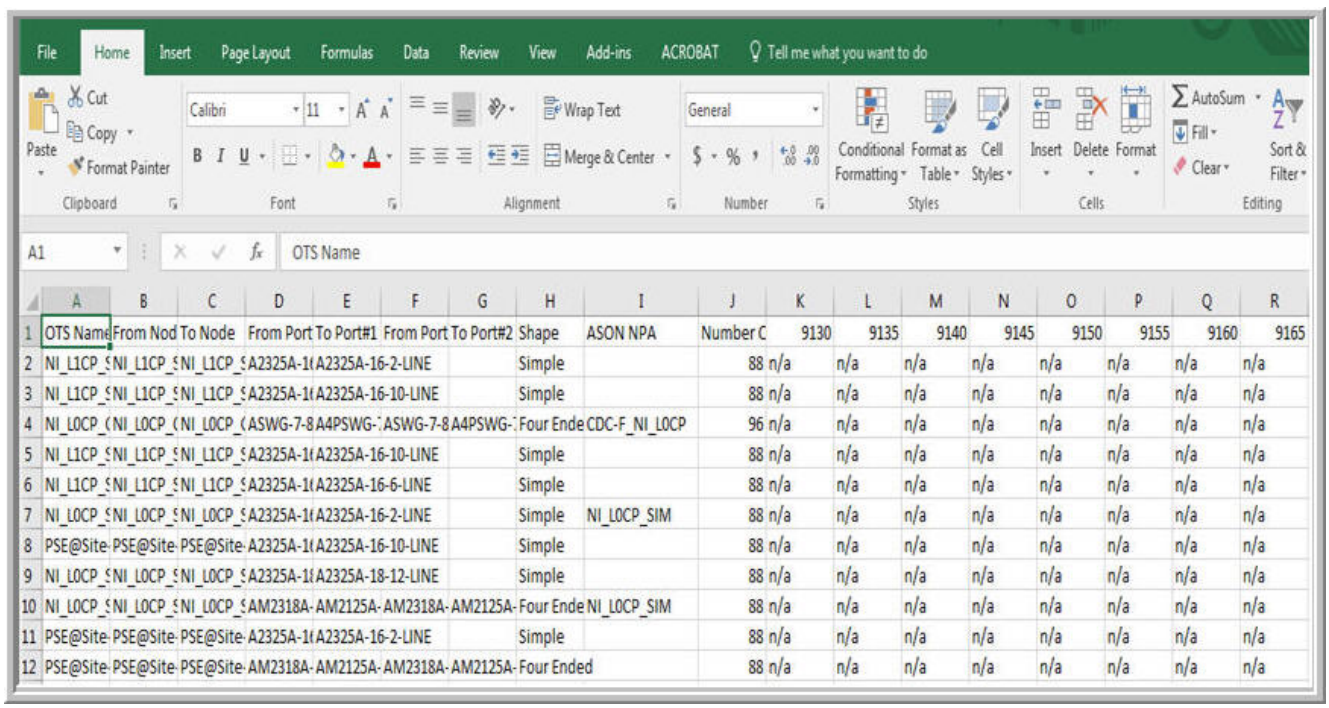
Wavelength Usage Report definition

The *Wavelength Usage Report* displays available and used wavelengths on OTS spans between the nodes. It can be used as a reference for determining the available wavelengths for a new service turn-up across an optical network.

Wavelength Usage Report format

The Wavelength Usage Report is a generated in **.CSV** format. It can be opened immediately or saved to the user's PC.

Figure 7-280 Wavelength Usage Report – Top Portion of the Report



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	OTS Name	From Nod	To Node	From Port	To Port#1	From Port	To Port#2	Shape	ASON NPA	Number C	9130	9135	9140	9145	9150	9155	9160	9165
2	NI_L1CP_S	NI_L1CP_S	NI_L1CP_S	A2325A-1(	A2325A-16-2-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
3	NI_L1CP_S	NI_L1CP_S	NI_L1CP_S	A2325A-1(	A2325A-16-10-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
4	NI_L0CP_(	NI_L0CP_(	NI_L0CP_(	ASWG-7-8	A4PSWG-:	ASWG-7-8	A4PSWG-:	Four Ende	CDC-F_NI_L0CP	96	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
5	NI_L1CP_S	NI_L1CP_S	NI_L1CP_S	A2325A-1(	A2325A-16-10-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
6	NI_L1CP_S	NI_L1CP_S	NI_L1CP_S	A2325A-1(	A2325A-16-6-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
7	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	A2325A-1(	A2325A-16-2-LINE			Simple	NI_L0CP_SIM	88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
8	PSE@Site-	PSE@Site-	PSE@Site-	A2325A-1(	A2325A-16-10-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
9	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	A2325A-1(	A2325A-18-12-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
10	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	AM2318A-	AM2125A-	AM2318A-	AM2125A-	Four Ende	NI_L0CP_SIM	88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
11	PSE@Site-	PSE@Site-	PSE@Site-	A2325A-1(	A2325A-16-2-LINE			Simple		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
12	PSE@Site-	PSE@Site-	PSE@Site-	AM2318A-	AM2125A-	AM2318A-	AM2125A-	Four Ended		88	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

The Wavelength Usage Report columns are as follows:

- **Column A:** Name of OTS Span between nodes.
- **Column B/C:** The From Node end port of OTS and To Node (**From Node**)
- **Column D/E:** The To Node end point of OTS (**To Node**)
- **Column F:** Specifies the From Port #
- **Column G:** Specifies the To Port #

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

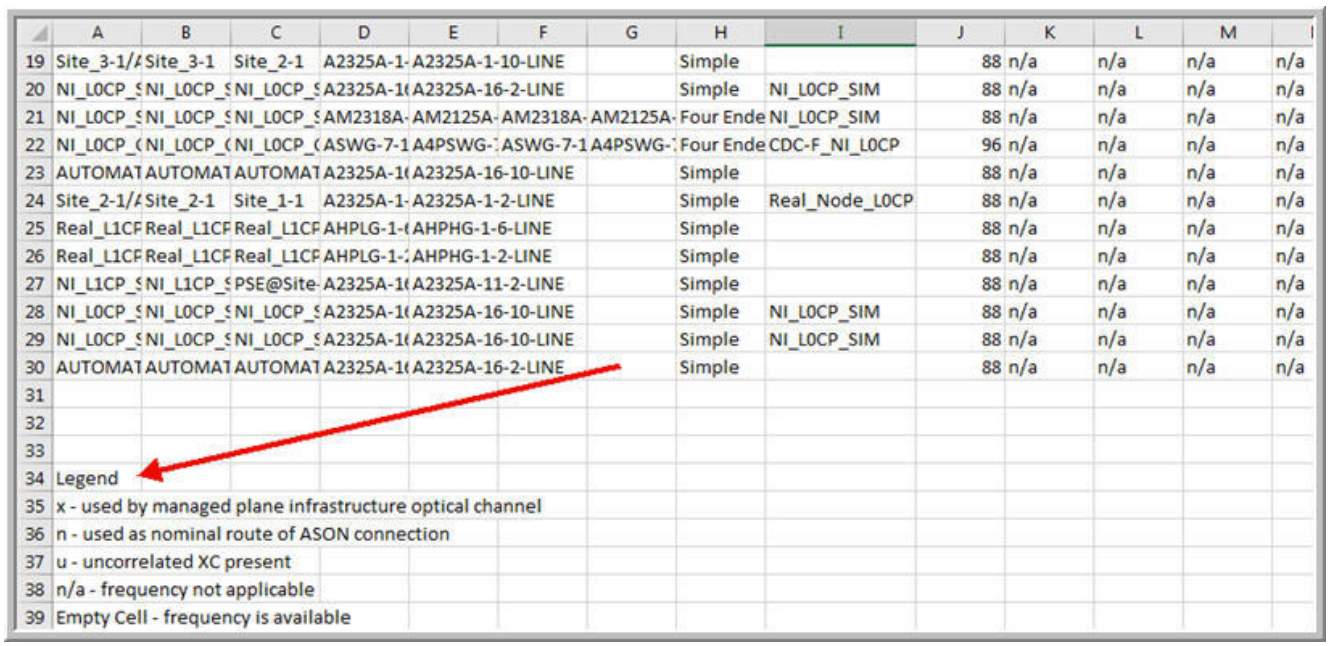
- **Column H:** Shape of the particular OTS connection that can be supported by the OTS span. This information is derived from hardware capability of adjacent nodes.
- **Column I:** The name of ASON NPA to which the OTS/OMS belongs. For Control Plane links, ASON NPA field is auto-populated with the name, L0_GMRE that specifies the ASON NPA that the OTS or OMS belongs to. If the link is a Managed Plane link, the field is blank.
- **Column J:** The number of channels, which are based on number of LCs of the OTS/OMS. The Wavelength Usage Report supports **44**, and **88**, and **96** channels

  These columns in the port are fixed with values from 9605 to 9130 and do not change regardless of number of wavelengths applicable to a given OTS.

  Note The report generated will only have OTS with OMS trail present in **Commissioned** state, and is applicable for Non CWDM links only.
- **Column K:** These columns in the port are fixed with values from 9605 to 9130, and do not change regardless of number of wavelengths applicable to a given OTS.

The bottom of the Wavelength Usage Report provides the following legends:

Figure 7-281 Wavelength Usage Report – Legend – bottom portion of the report



	A	B	C	D	E	F	G	H	I	J	K	L	M	
19	Site_3-1/4	Site_3-1	Site_2-1	A2325A-1-	A2325A-1-10-LINE			Simple		88	n/a	n/a	n/a	n/a
20	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	A2325A-1(	A2325A-16-2-LINE			Simple	NI_L0CP_SIM	88	n/a	n/a	n/a	n/a
21	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	AM2318A-	AM2125A-	AM2318A-	AM2125A-	Four Ende	NI_L0CP_SIM	88	n/a	n/a	n/a	n/a
22	NI_L0CP_(	NI_L0CP_(	NI_L0CP_(	ASWG-7-1	A4PSWG-7	ASWG-7-1	A4PSWG-7	Four Ende	CDC-F_NI_L0CP	96	n/a	n/a	n/a	n/a
23	AUTOMAT	AUTOMAT	AUTOMAT	A2325A-1(	A2325A-16-10-LINE			Simple		88	n/a	n/a	n/a	n/a
24	Site_2-1/4	Site_2-1	Site_1-1	A2325A-1-	A2325A-1-2-LINE			Simple	Real_Node_L0CP	88	n/a	n/a	n/a	n/a
25	Real_L1CF	Real_L1CF	Real_L1CF	AHPLG-1-(	AHPHG-1-6-LINE			Simple		88	n/a	n/a	n/a	n/a
26	Real_L1CF	Real_L1CF	Real_L1CF	AHPLG-1-2	AHPHG-1-2-LINE			Simple		88	n/a	n/a	n/a	n/a
27	NI_L1CP_S	NI_L1CP_S	PSE@Site-	A2325A-1(	A2325A-11-2-LINE			Simple		88	n/a	n/a	n/a	n/a
28	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	A2325A-1(	A2325A-16-10-LINE			Simple	NI_L0CP_SIM	88	n/a	n/a	n/a	n/a
29	NI_L0CP_S	NI_L0CP_S	NI_L0CP_S	A2325A-1(	A2325A-16-10-LINE			Simple	NI_L0CP_SIM	88	n/a	n/a	n/a	n/a
30	AUTOMAT	AUTOMAT	AUTOMAT	A2325A-1(	A2325A-16-2-LINE			Simple		88	n/a	n/a	n/a	n/a
31														
32														
33														
34	Legend													
35	x - used by managed plane infrastructure optical channel													
36	n - used as nominal route of ASON connection													
37	u - uncorrelated XC present													
38	n/a - frequency not applicable													
39	Empty Cell - frequency is available													

Wavelength Usage Report usage

The following scenarios explain typical usages of the Wavelength Usage Report

- **When a new service must be deployed between two sites:**

  To determine how to fiber transponders (especially to static filters) prior to service turn up, generate the report and check the frequencies that are available on the end-to-end route between sites.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- **When performing maintenance on a link/node or temporary reroute traffic around a failure:**

  Users must first determine the availability of the wavelengths or blocks of spectrum on alternative routes between the source and the destination. Users then reroutes or re-provision existing wavelength services via alternative routes and put them on available wavelengths according to Wavelength Usage Report.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.125 Manage Wavelength Usage Report

When to use

Use this task to generate, view, and save the User Activity Log into **.CSV** file format.

Related information

This feature supports the scenario where there is no planning tool for allocating wavelengths in the network.

Before you begin

Ensure that the OTS network topology is being fully inventoried and can be seen in Map view or Physical Connections list.

Task

Complete the following step to generate and download the Wavelength Usage Report in **.CSV** file format.

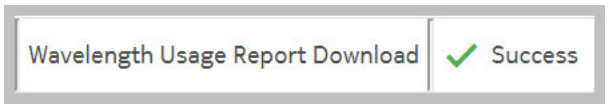
1

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

OPERATE > Wavelength Usage Report

Result: A success message is displayed at the bottom left of the page and the system downloads the Wavelength Usage Report.

Figure 7-282 Wavelength Usage Report – Download notification



2

The file is saved to **Downloads** directory.

3

Navigate to the directory where the CSV file is saved and double click to open the CSV file.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Jobs

7.126 Jobs description

Jobs definition

Jobs is a NFM-T OTN feature that 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.

Jobs functional description

The system provides a Jobs list for infrastructure connections and their clients and servers and for services and their servers. These jobs can be accessed from an inclusive Jobs list from the **ADMINISTER > Jobs** navigation path.

As a filtering mechanism and to avoid navigation path changes, the system also enables users to view the Jobs list for infrastructure connections and their clients and servers from the **OPERATE > Infrastructure Connections** navigation path and for services and their servers from the **OPERATE > Services** navigation path. Refer to 7.71 "View Jobs for an infrastructure connection or service" (p. 1016) for detailed steps.

In addition, the system provides a Jobs list for SNC matches and parameter matches from the **OPERATE > Network Inconsistencies** navigation path. Refer to "Task: View the Job List for an Parameter Mismatch" (p. 1176) and "Task: View the Job List for an SNC Mismatch" (p. 1183) for detailed steps.

Jobs list properties

The Jobs list provides users with the user name (**otn**), type, and state. In addition, the data and time are also provided for when the job was created, was last run, and was last updated. The date and time are also provided for the next run and the scheduled run.

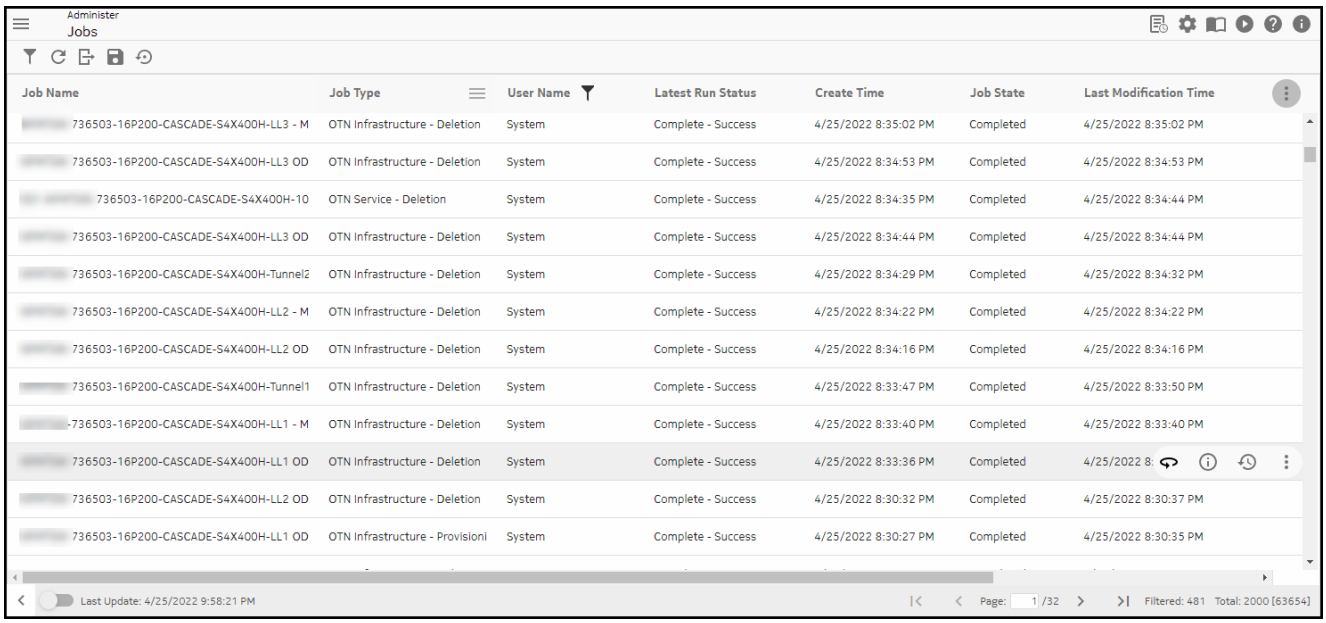
User interaction with Jobs

To access the Jobs data table and visualize the jobs list, follow the path:

ADMINISTER > Jobs

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-283 Jobs – Data Table



From the Jobs list the user can do the following actions:

Delete a Job

To delete a Job, select the job in the list and click the **More** icon at the end of the selected row and select **Delete** from the pop-up menu that is displayed. A confirmation box is displayed, click **Yes** to delete the job.

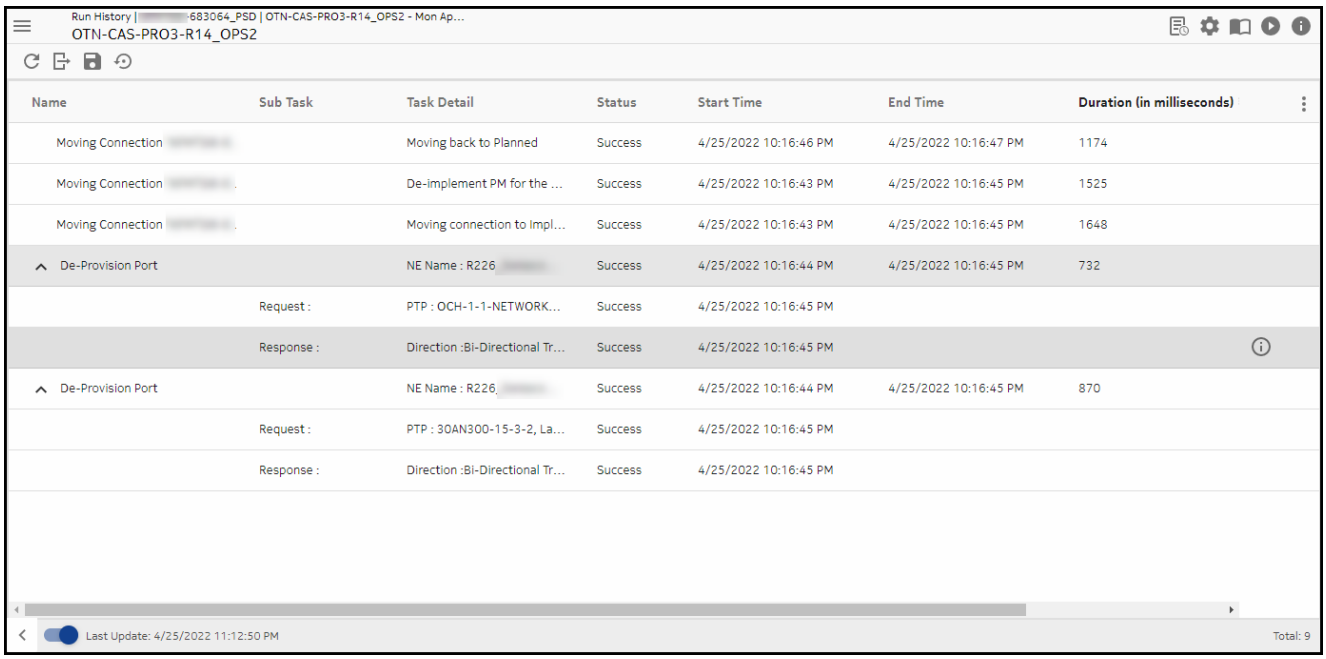
Run the history for a job

Select a job in the list and hover over the **More** icon at the end of the selected row and select the **Run History** icon.

The system displays the history for the selected job.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-284 Jobs – Run History window



View tabbed topics for a Job

Select a job, hover over the **More** icon at the end of the selected row and select the **360° View** icon. The Details window is displayed. Click one of the following tabs: **Details** or **Job Inventory**. The system activates the selected tab and the job-related information is displayed in the Jobs data table.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.127 Jobs table columns

Jobs table

To display the Jobs table, follow this navigation path: **ADMINISTER > Jobs**.

Column	Description
Job Name	For a job, the **Name** column identifies the particular job.
Job Type	The **Job Type** column displays the type of job that the system is executing or has executed. **Example:** OTN Infrastructure Provisioning, OTN Service Provisioning
User Name	The **User Name** column displays the name of the user who initiated the named job that the system that the system is executing or has executed.
Latest Run Status	The **Latest Run Status** column displays the status for the latest run of the named job that the system that the system is executing or has executed to be In Progress, Complete - Success, or Complete - Failure.
Create Time	The **Create Time** column displays the date and time in which the named job has been created. **Example:** 2017-02-26 08:05:05
Last Modification Time	The **Last Modification Time** column displays the date and time in which the status of the named job was last updated. **Example:** 2017-02-26 08:05:05
Schedule	The **Schedule** column displays the date and time in which the named job is scheduled to be run again or a dash (-), which means that a next run is not scheduled.
Next Run	The **Next Run** column displays the date and time in which the named job is to be run again or a dash (-), which means that a next run will not occur.
Job State	The **Job State** column displays the state of the named job that the system that the system is executing or has executed to be In Progress or Completed..
ID	The Job ID.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Schedule Path Synchronization

7.128 Schedule Path Synchronization description

Schedule Path Synchronization definition

The *Schedule Path Synchronization* feature enables users to schedule network connection synchronization using the current data that is available in the NFM-T OTN database.

The typical system behavior is for the NFM-T OTN database to remain in synchronization with a NE by processing notifications from the NE. However, when a connection is created using an external system, if cross connection notifications from the NE do not result in connections being created in the NFM-T OTN, users can discover connections by performing network connection synchronization on demand. With the Schedule Path Synchronization feature, users can schedule network connection synchronization.

Schedule Path Synchronization functional description

Schedule Path Synchronization performs its synchronization by stepping through the NEs on a one-by-one basis. If an NE does not have any uncorrelated cross connections, it is skipped. For all uncorrelated cross connections, Schedule Path Synchronization attempts to discover if the cross connection completes a new connection; and, for each discovered connection, it attempts to discover any client connections. When Schedule Path Synchronization is completed, the Job Status and Logs are updated.

Schedule Path Synchronization intervals

The Schedule Path Synchronization feature supports the following synchronization intervals:

- For *one time intervals*, users can choose the date and time to execute the synchronization.
- For *every N hour intervals*, users can choose the time to execute the synchronization.
- For *daily intervals*, users can choose the day and time to execute the synchronization.
- For *weekly intervals*, users can choose the day of the week, all days, or all days of the week or only the working days of the week and time to execute the synchronization.

For daily, weekly, and hourly scheduled jobs, the system provides the last date/time in which the synchronization was executed and the overall success/failure status of the synchronization.

User interaction with Path Synchronization

To manage Path Synchronization, you can perform the following actions:

- 7.130 “Schedule or Reschedule Path Synchronization ” (p. 1201)
- 7.131 “View the Path Synchronization job ” (p. 1205)
- 7.129 “Delete the last Scheduled Path Synchronization request” (p. 1199)
- 7.132 “Abort Path Synchronization ” (p. 1207)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.129 Delete the last Scheduled Path Synchronization request

When to use

Use this task to delete the last scheduled path synchronization request.

Before you begin

The Schedule Path Synchronization window must display a scheduled synchronization request.

Task

Complete the following steps to delete the last scheduled path synchronization request.

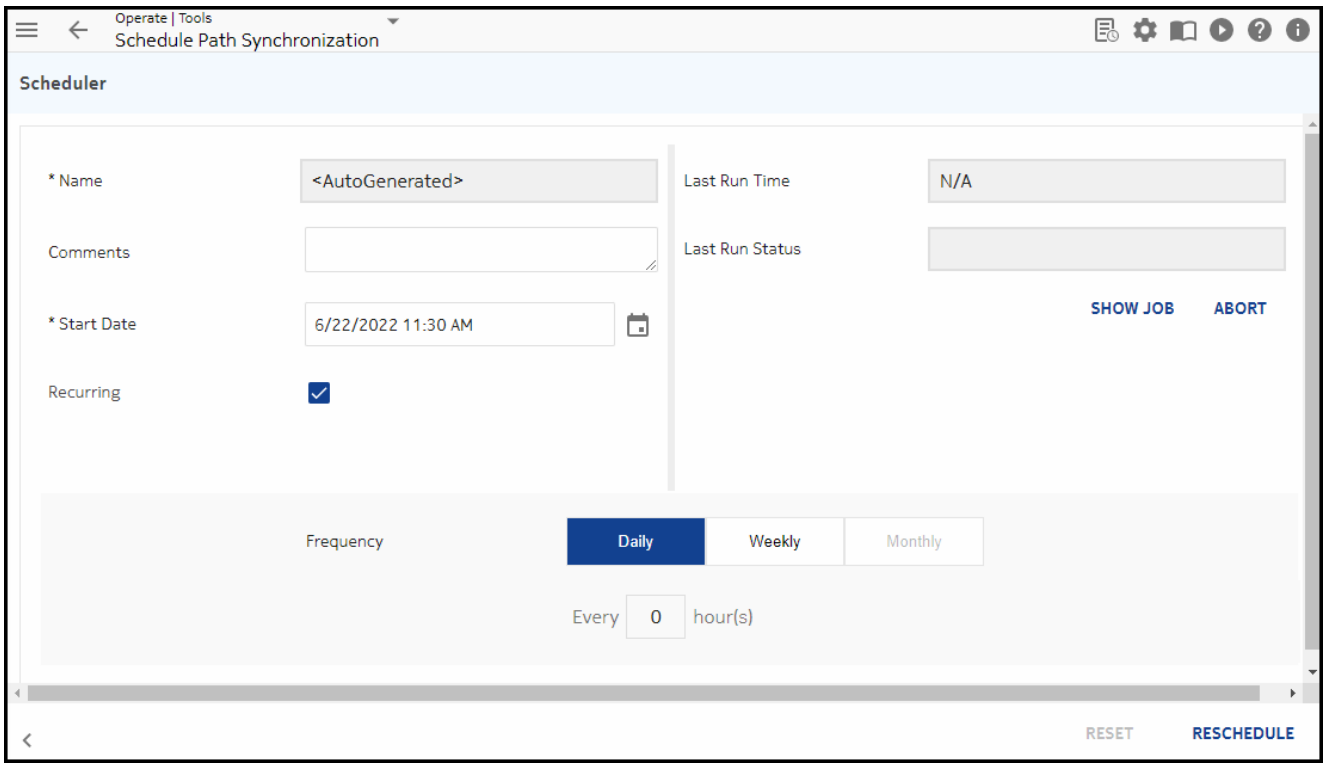
1

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

Operate > Tools > Schedule Path Synchronization

Result: The system displays the Schedule Path Synchronization page. The **Last Run Time** field shows the date and time in which the last path synchronization was scheduled. The **Last Run Status** field shows the status.

Figure 7-285 Schedule Path Synchronization – default window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Click **SHOW JOB**.

Result: The Jobs page is displayed.

3

Select the job you want to delete, click the **More** icon at the end of the selected row and select **Delete** from the pop-up menu that appears.

Result: The system deletes the scheduled path synchronization job and outputs a success message similar to the following:

```
Success.
Delete Job Complete.
```

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.130 Schedule or Reschedule Path Synchronization

When to use

Use this task to schedule or reschedule path synchronization.

Before you begin

To reschedule a path synchronization, the job must currently exist.

Task: Schedule Path Synchronization

Complete the following steps to schedule path synchronization.

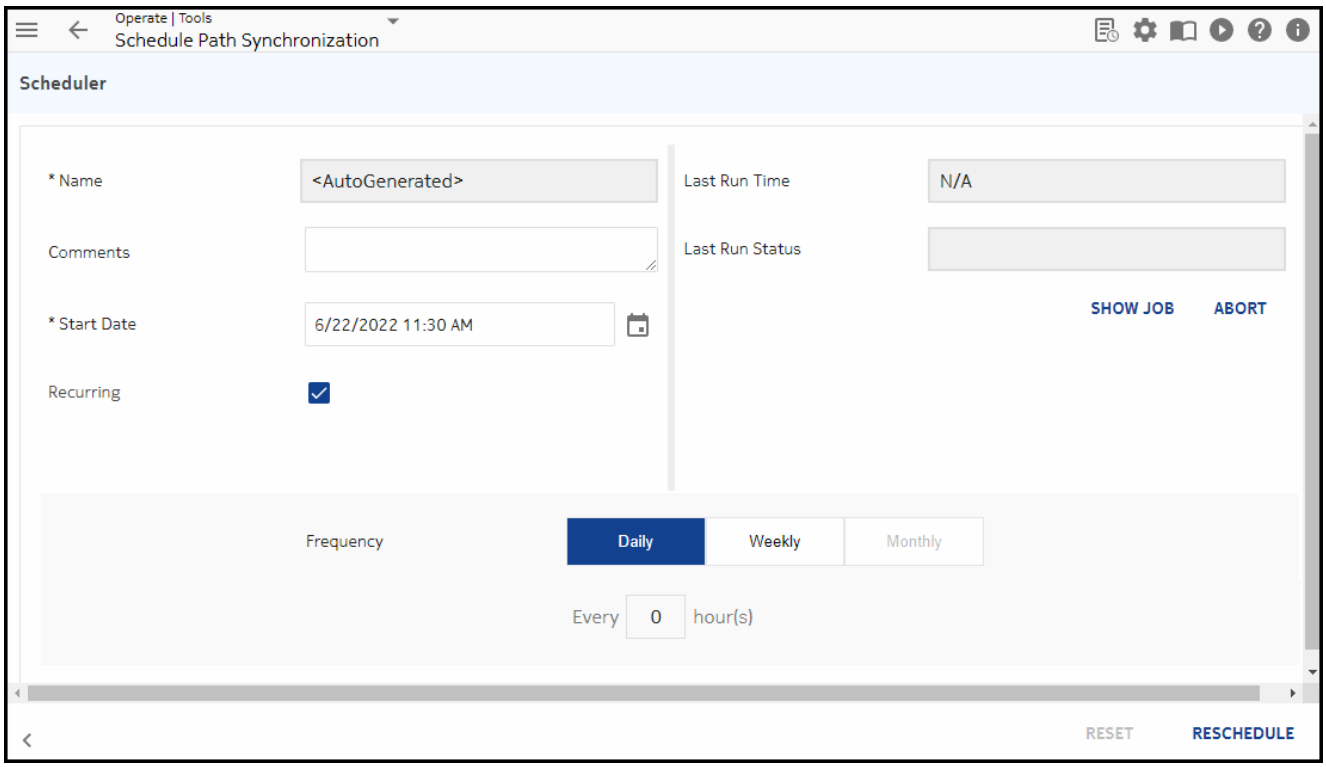
1

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

Operate > Tools > Schedule Path Synchronization

Result: The system displays the Schedule Path Synchronization page. The **Last Run Time** field shows the date and time in which the last path synchronization was scheduled. The **Last Run Status** field shows the status.

Figure 7-286 Schedule Path Synchronization – default window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Click the **Calendar** icon next to the **Start Date** field, and select a date and time from the calendar that is displayed.

3

To run the path synchronization one time, clear the **Recurring** check box.

4

To run the path synchronization in a recurring manner, select the **Recurring** checkbox and do one of the following:

a. To run the path synchronization daily at fixed intervals, click the **Daily** option in the **Frequency** list and enter a number from **1** to **23** in the **Every** field; where: **1** to **23** are the hours in the day.

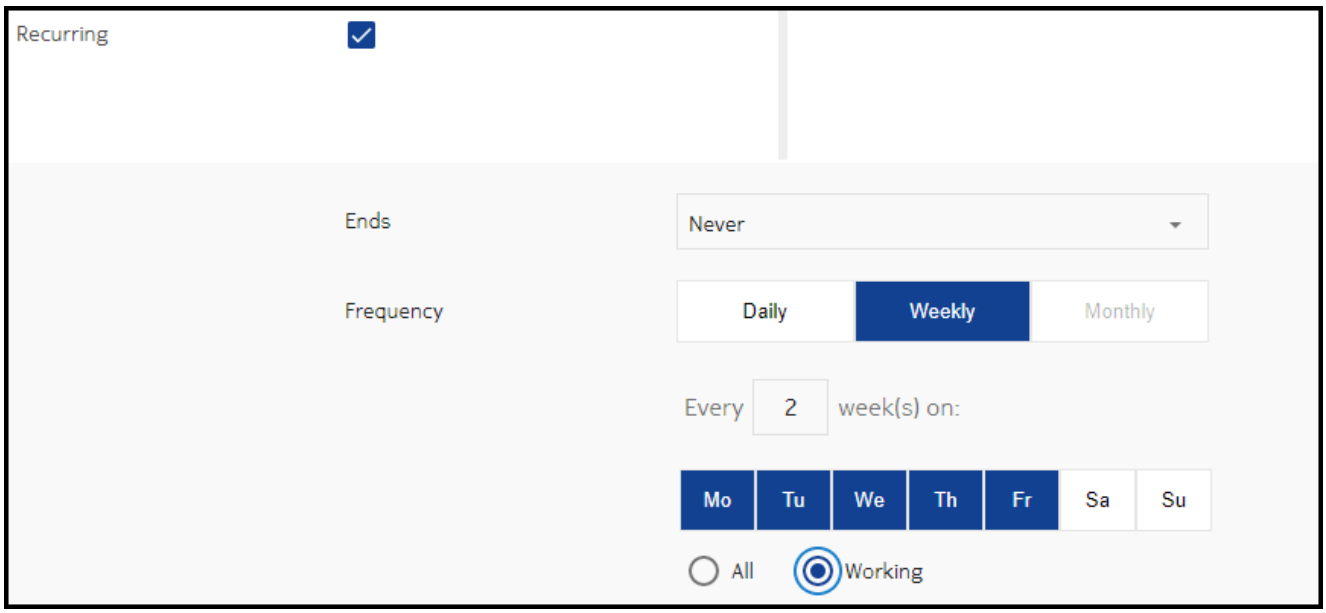
Note: Enter **0** in the **Every** field, to run the path synchronization once daily.

Figure 7-287 Schedule Path Synchronisation - Recurring > Daily option

b. To run the path synchronization weekly, click the **Weekly** option in the **Frequency** list and enter the number that represents the weekly interval in the **Every** field. Select the day or days of the week that the synchronization is to be run. See Figure 7-288, “Schedule Path Synchronisation - Recurring > Weekly option” (p. 1203)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-288 Schedule Path Synchronisation - Recurring > Weekly option



Select **All** to select all days of the week. Select **Working** to select only the working days of the week.

5

Click **RESCHEDULE**.

Result: The system schedules the path synchronization and displays a success message in the status bar at the bottom of the page.

Note: The **Monthly** option is not applicable for schedule path synchronization.

6

Click **RESET** to reset the settings and reschedule the path synchronization job.

END OF STEPS

Task: Reschedule Path Synchronization

Complete the following steps to reschedule path synchronization from the Jobs page.

1

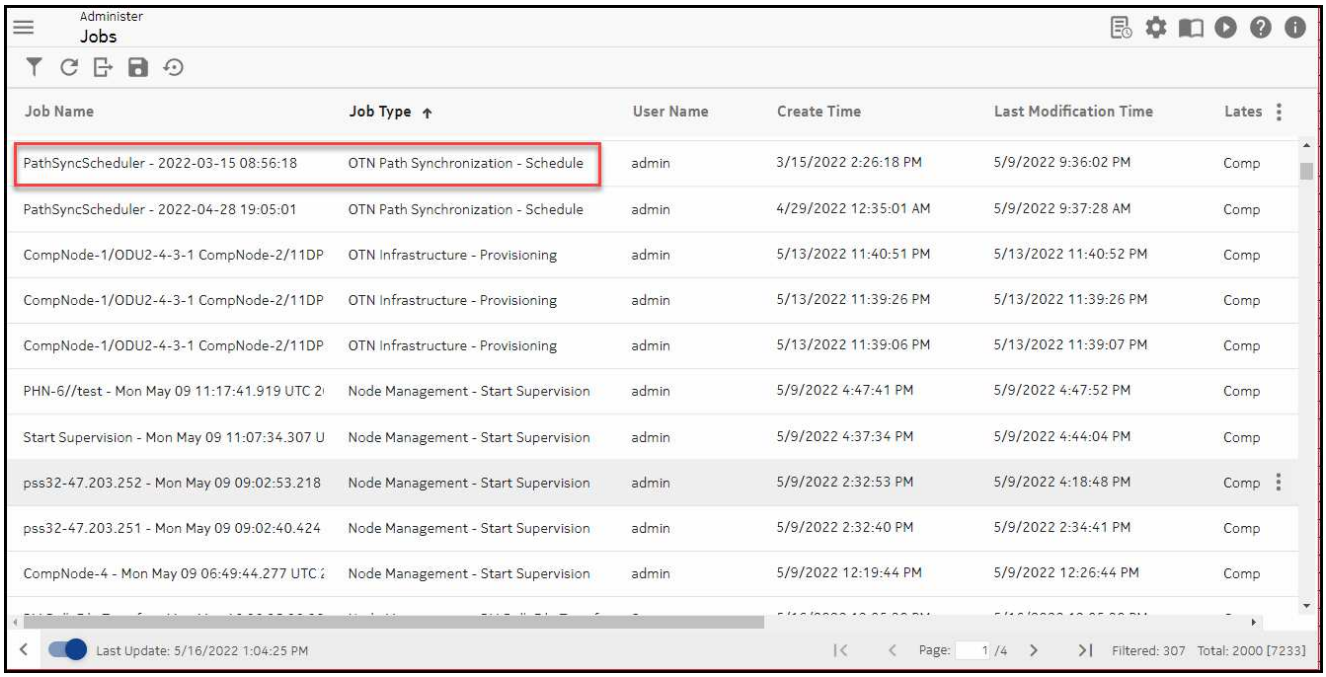
From the NFM-T GUI, follow the navigation path to open the Jobs page.

Operate > Tools > Schedule Path Synchronization. Click **SHOW JOB** on the Schedule Path Synchronization page

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The system displays the Jobs page, which shows the list of jobs submitted. See Figure 7-289, “Jobs page ” (p. 1203)

Figure 7-289 Jobs page



2

Select the job you want to reschedule, click the **More** icon at the end of the selected row and select **Reschedule** from the pop-up menu that appears. See “Actions on a scheduled job” in the OTN guide.

Result: The system reschedules the path synchronization and outputs a success message, which is similar to the following:

```
Path Synchronization with Frequency Type <Once/Hourly/Daily/Weekly> is
Successfully Rescheduled.
```

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.131 View the Path Synchronization job

When to use

Use this task to view the path synchronization job.

Before you begin

The Schedule Path Synchronization page must display a scheduled synchronization request.

Task

Complete the following steps to view the path synchronization job.

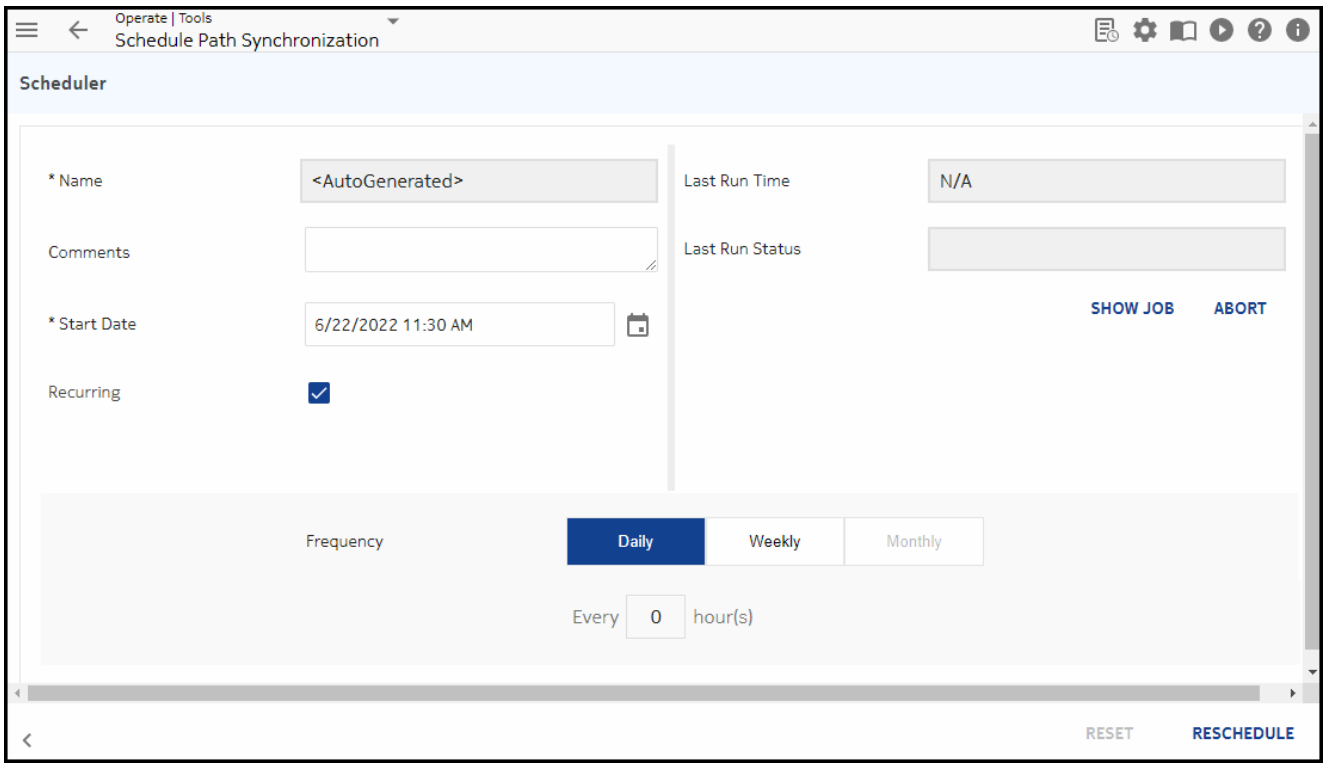
1

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

Operate > Tools > Schedule Path Synchronization

Result: The system displays the Schedule Path Synchronization page. which shows the date and time in which the last path synchronization was scheduled in the**Last Run Time** field and the status in the **Last Run Status** field.

Figure 7-290 Schedule Path Synchronization – default window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

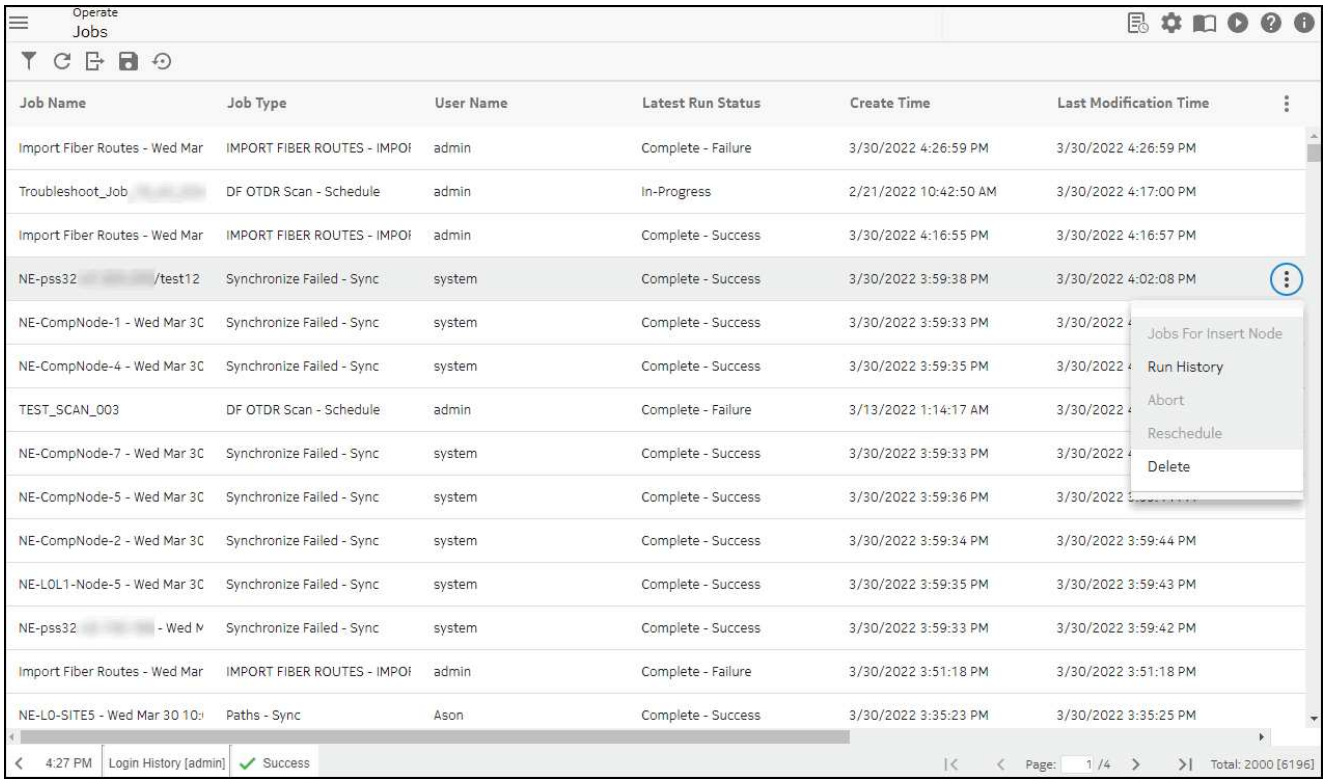
2

Click **SHOW JOB**, located in the right panel of the page.

Result: The system displays the Jobs window.

Example: The following figure illustrates the path synchronization job that has been scheduled.

Figure 7-291 Schedule Path Synchronization – Jobs window



3

Select a job and view details. See “Actions on a scheduled job” in the OTN guide.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.132 Abort Path Synchronization

When to use

Use this task to abort the path synchronization.

Task:

Complete the following steps to abort path synchronization from the Jobs page.

1

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

Operate > Tools > Schedule Path Synchronization. Click **SHOW JOB** on the Schedule Path Synchronization page

Result: The system displays the Jobs page, which shows the list of jobs submitted.

2

Select the job you want to abort, click the **More** icon at the end of the selected row and select **Abort** from the pop-up menu that appears. See “Actions on a scheduled job” in the OTN guide.

Result: The system aborts the path synchronization. The job is aborted but the ongoing synchronization process on the current NE will not be aborted.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Flex Framer 3 (FF3) pool handling

7.133 Overview

Purpose

In 1830 PSS R13.1/ NFM-T R21.4, the full flexibility of supported ODU rates is up to the maximum of 190 ODU cross-connects. Some cards have resource restrictions for lower order OTU or OTSig switching. A large number of low level ODU connections are set, then available cross-connect resources may exhaust before the spare channels on the links are used. It appears that there are spare channels available, but those are not available because of the cross-connect limit. The HO-ODU, which is mapped to a OTU or OTSig is associated to a chip called **Flex Framer 3 (FF3)**, which is used as a 500G mapper device. FF3 creates the resource restrictions. FF3 supports 500G of network capacity and maximum of 190 ODU cross-connects.

The cards that use FF3 technology:

- 4UC1T (4 ports)
- 8UC1T (8 ports)
- 10AN1T (10 ports)
- 2UX500 (2 ports)

Contents

7.133 Overview	1208
7.134 Flex Framer 3 (FF3) pool handling	1209

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7.134 Flex Framer 3 (FF3) pool handling

FF3 Mode

The possible value for the FF3 mode are **Managed Plane (MP)**, **Control Plane (CP)**, and **Managed Plane Control Plane (MPCP)**. The default value on 1830 PSS R13.1 NE is MP. For cards that are migrated from 1830 PSS R13.0.4 (NFM-T R20.11) to 1830 PSS R13.1 (NFM-T R21.4), the default value is MPCP. The same value of FF3 mode is applicable for both the pools.

- When FF3 mode is MP, on that ODU Channel pool, shared pool can only be used by MP services whereas private pool can be used by CP services belonging to CP server in that pool.
- When FF3 mode is CP, on that ODU Channel pool, shared pool can only be used by CP services whereas private pool can be used by MP services belonging to MP server in that pool.
- When FF3 mode is MPCP, on each ODU4 server it is possible to have only 38 clients.

FF3 Mode	MP	CP	MPCP
Private Pool	GMRE can use private pool on servers that are assigned to GMRE	Managed Plane connections can use private pool	Number of clients on each ODUk is 38
Shared Pool	Reserved for MP	Reserved for CP	

Two settings that are managed by the system:

- FF3 mode setting on the NE
- Link assignment request/command sent to GMRE

During tunnel creation, similar to link assignment, the FF3 mode is set first, followed by MRN creation commands to GMRE. If FF3 mode setting fails, MRN creation requests will not be sent to GMRE. During link assignment, if setting of FF3 mode fails, link assignment also fails. The same is applicable for MRN tunnel creation.

For example:

- Scenario 1: Link Assignment to NPA

  When the first link (drop link assignment or i-nni link assignment) is assigned to NPA, the default value of FF3 mode is MP and there is no shared pool used, then the system will send a command to change the FF3 mode to CP as part of link assignment.
- Scenario 2: MRN Tunnel Creation

  When the first MRN tunnel is created, the default value of FF3 mode is MP and there is no shared pool used, then the system will send a command to change the FF3 mode to CP as part of MRN tunnel creation.
- Scenario 3: Link Unassignment / MRN Tunnel Deletion

  During unassignment, if it is the last tunnel/link being deleted, FF3 mode must be set to MP.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Private and Shared Pool

190 cross-connects available in the FF3 are shared across private and shared pools.

Private Pool: Ten cross-connects per OTU and OTSig tunnel.

Shared Pool: 140 cross-connects shared across the five OTU and OTSig tunnels.

Note: The 190 available cross-connects are distributed across the five OTU and OTSig tunnels that terminate on the cards (8UC1T, 10AN1T, and 4UC1T) in the following manner:

- 10 cross-connects are fixed for each OTU and OTSig tunnel if the card is in the **MP** or **CP** mode
- 140 cross-connects can be used by any of the OTU and OTSig tunnels.

If the card is in **MPCP** mode, then each OTU and OTSig tunnel is allotted 38 cross-connects.

The connection created (MP or CP) set the card mode and thus control the shared pool.

Table 7-24 Managed / control Plane: FF3 mode and maximum capacity/group details

Managed / Control Plane	FF3 Mode	Maximum Capacity/ Group
NFM-T R21.4	CP	186 channels
NFM-T R21.4	MP	186 channels
NFM-T R20.11	MPCP	38 channels/ OTU4

Discovery: Discovery of connection from the network will inventory in NFM-T and increment the count. All the connections on the NE are discovered.

Deletion: A service is deleted from a shared pool before decreasing from the private pool on the server.

Migration from 1830 PSS R13.0.4 to 1830 PSS R13.1

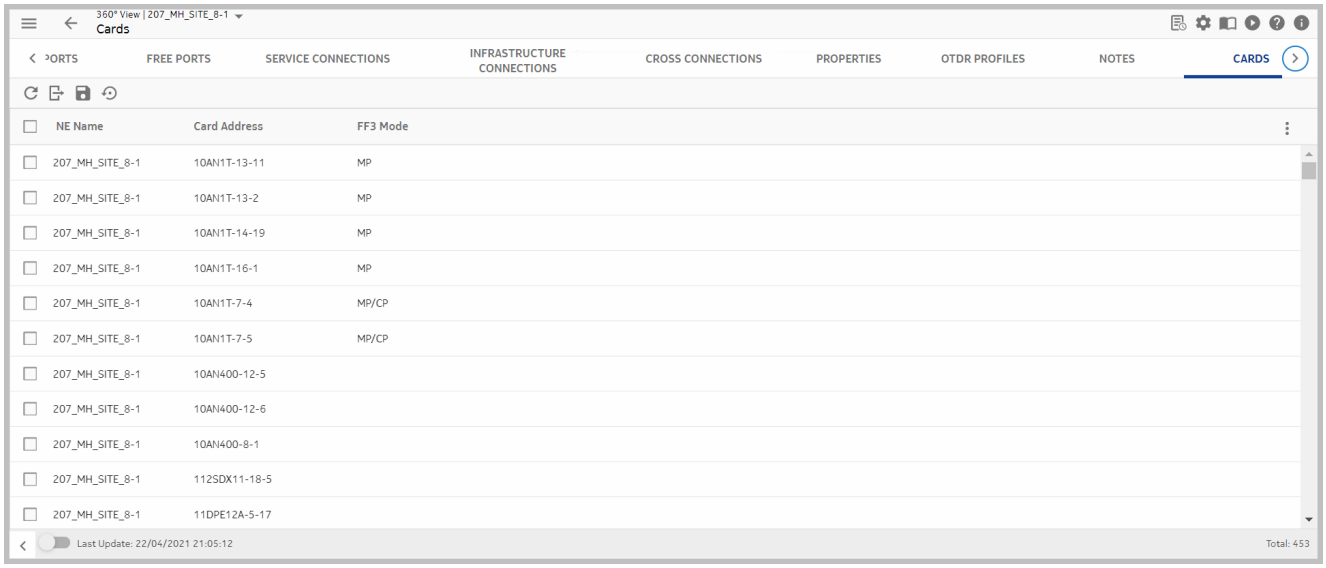
A port synchronization is required for a NE after it is upgraded to 1830 PSS R13.1 for the inventory of ODU channel pool. The port synchronization will be triggered by NFM-T when the version of the NE changes. After the port sync is completed, NFM-T triggers auto migration service. NFM-T migration service identifies the ODU channel pools that are eligible for FF3 mode, then changes to either MP or CP. After the migration is completed, user can check the status of each card for which mode change is set on the **ADMINISTER > Jobs** page.

Complete the following steps to view FF3 mode of the cards:

1. **Operate > Nodes > 360º View > NEs > [Select an NE] > 360º View** or **Operate > NEs > 360º View**
2. Click the **Cards** tab.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 7-292 360º view - Cards tab



Migration from NFM-T 20.11 to NFM-T 21.4

- If there are no cross-connects then, no ODU containers are used for the traffic. The ODU pool can be switched to flexible mode and the segmentation defined in NFM-T 20.11 is removed which defines 140 ODU containers for each FF3. The card mode is marked as MP or CP if the traffic already defined is pure MP or CP. The configuration of card mode is possible through a manual command raised by user for each card.
- If the ODUPool is used for MP traffic and the Flexible ODUPool is applicable in NFM-T R21.4, then ODU pool can be used only for MP traffic and the card mode can only be MP. Then the same is valid in case the traffic is GMPLS in 1830 PSS 13.0.4/ NFM-T R20.11
- If the Pseudo Shared Containers in the ODU pool have been used for MP and GMPLS traffic the flexible ODU Pool cannot be applied after the migration. The card mode will remain MPCP and each port will have only 38 ODU containers forever. To enable the flexible ODU pool management, the ODU pool has to be free

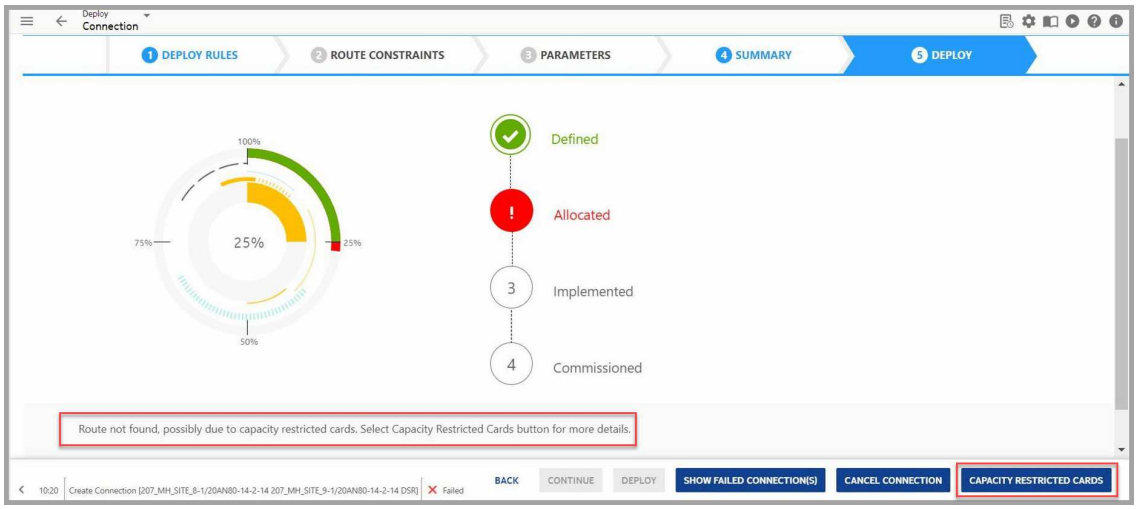
Example scenario: restrictions seen during MRN Tunnel creation

Restrictions seen during MRN Tunnel creation

1. Create an MRN tunnel. See the task for MRN tunnel creation for more details: “Task: To create MRN Terminated Tunnel ” (p. 1399)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2. If the capacity is exhausted, the following error message is displayed.

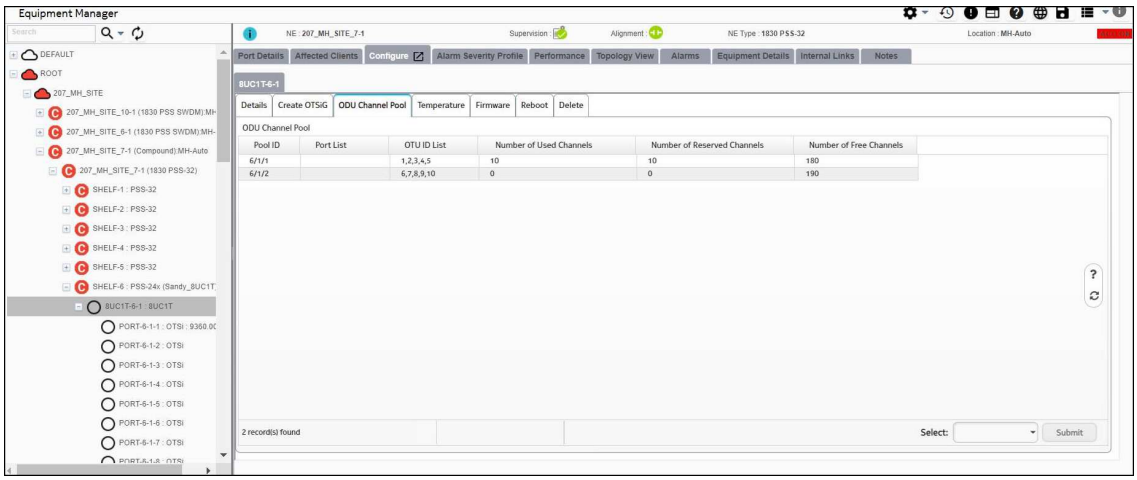


3. Click **CAPACITY RESTRICTED CARDS** button. **CAPACITY RESTRICTED CARDS** page is displayed.

4. From the **Capacity Restricted Cards** page, navigate to **Equipment Manager** by clicking the **More** icon ⋮ and selecting **Equipment Manager**.
5. On the **Equipment Manager** window, check the pool usage on **ODU Channel Pool** sub-tab

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

under **Configure** tab.



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8 Deploy Connections

8.1 Overview

Purpose

This chapter provides the information on using the **New Service/Infrastructure Connection** templates.

Contents

8.1 Overview	1215
Deploy a new service or infrastructure connection with template	1216
8.2 Overview	1216
8.3 Service or infrastructure connection template	1217
8.4 New service/infrastructure connection	1219
8.5 Deploy a Managed Plane Connection	1271
8.6 Deploy an L0 Control Plane Connection	1278
8.7 Deploy a Connection with Routing Constraints	1286
8.8 Deploy a Service	1294
8.9 Deploy 1:N Broadcast Connection	1301
8.10 Create an end to end ODUFlex service	1310
8.11 Manage an OTSig Tunnel	1314
8.12 Deploy a Disjoint Service	1344
8.13 Create ASON hairpin service	1351
8.14 Interworking configuration in OTN for ADD4 cards	1355

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Deploy a new service or infrastructure connection with template

8.2 Overview

Purpose

This section provides information on the New Service or Infrastructure Connection templates and different scenarios where we use this template.

Contents

8.2 Overview	1216
8.3 Service or infrastructure connection template	1217
8.4 New service/infrastructure connection	1219
8.5 Deploy a Managed Plane Connection	1271
8.6 Deploy an L0 Control Plane Connection	1278
8.7 Deploy a Connection with Routing Constraints	1286
8.8 Deploy a Service	1294
8.9 Deploy 1:N Broadcast Connection	1301
8.10 Create an end to end ODUFlex service	1310
8.11 Manage an OTSig Tunnel	1314
8.12 Deploy a Disjoint Service	1344
8.13 Create ASON hairpin service	1351
8.14 Interworking configuration in OTN for ADD4 cards	1355

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.3 Service or infrastructure connection template

Overview

NFM-T provides the new improved, simplified, and predefined set of best practices templates for provisioning a logical connection. These logical connections include infrastructure connection for trails and logical links, and service templates.

Each best practices template is specific to a technology and connection type, and each template provides a combination of parameters needed to create a working service.

Best practices templates are system owned templates and cannot be modified.

The templates are located at **DEPLOY** > **New Service/Infrastructure Connection**. The *New Service/Infrastructure Connection* page lists all the available templates.

The templates are broadly divided into three categories:

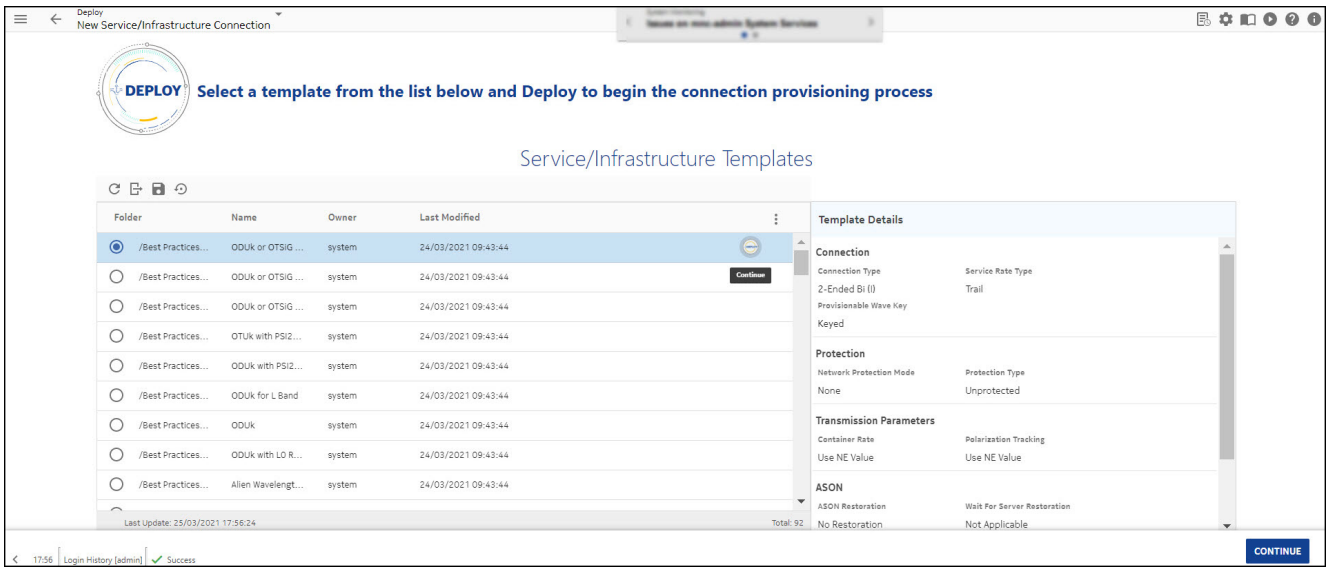
- Infrastructure Trail
- Service
- MultiLayer Service

Using these templates you can create an *ODUk or OTSiG Tunnel*, *ODUk*, *Y-cable Protected STM-N*, or many more connections.

Select a template to view the **Template Details** on the right-side of the template list.

The New Service/Infrastructure Connection Templates figure shows the template window.

Figure 8-1 New Service/Infrastructure Connection Templates page



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

References

For more information on *New Service/Infrastructure Connection Templates*, see the following topics:

- “Deploy Rules” (p. 1220)
- “Route Constraints” (p. 1244)
- “Parameters” (p. 1250)
- “Summary” (p. 1263)
- “Deploy” (p. 1266)
- 8.5 “Deploy a Managed Plane Connection” (p. 1271)
- 8.6 “Deploy an L0 Control Plane Connection” (p. 1278)
- 8.7 “Deploy a Connection with Routing Constraints” (p. 1286)
- 8.8 “Deploy a Service” (p. 1294)

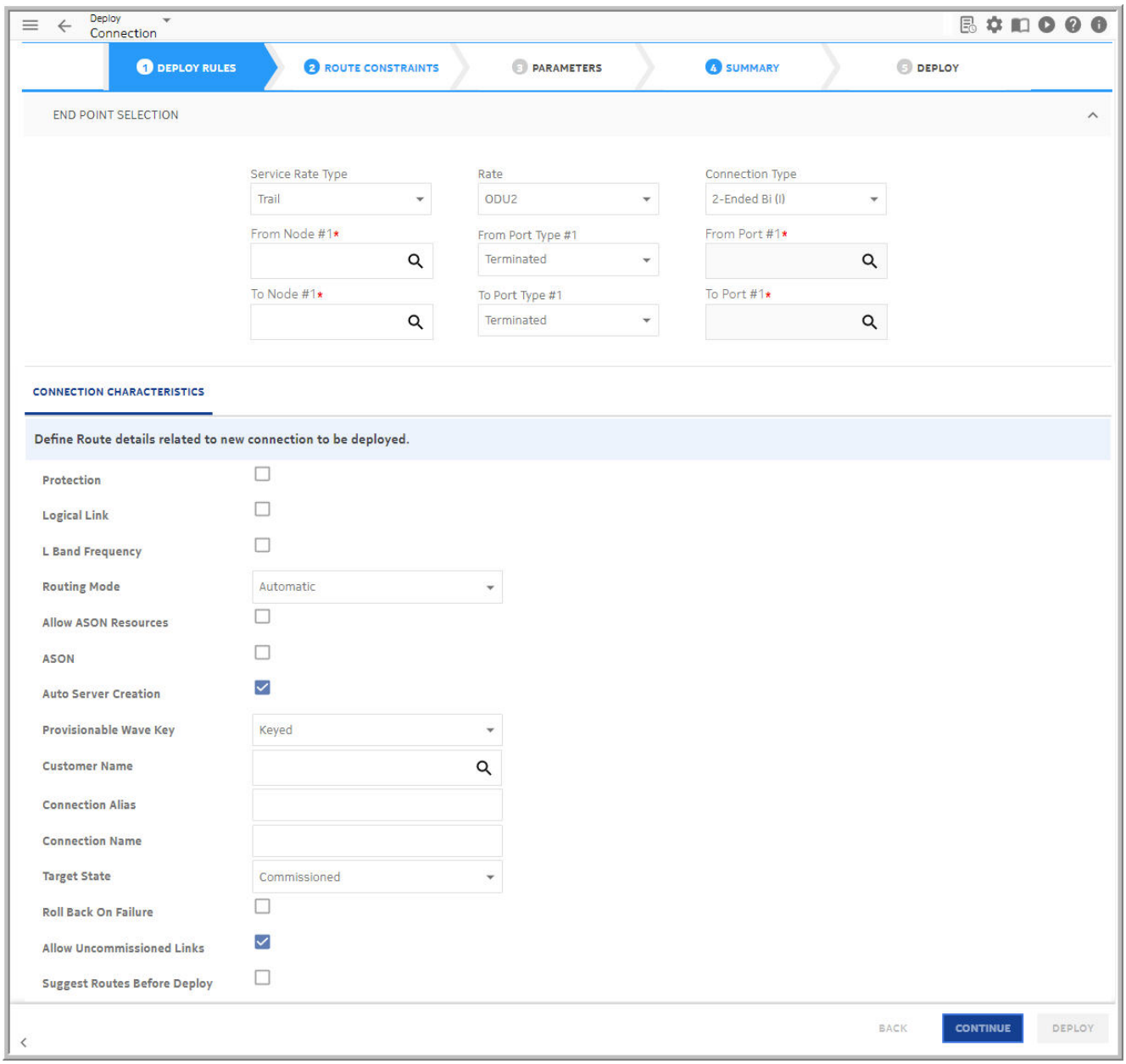
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.4 New service/infrastructure connection

Overview

To create a connection, select a template from the *Service/Infrastructure Templates* list and click **Deploy** button or **CONTINUE** button. The *Connection* window is displayed.

Figure 8-2 Connection Window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

The *Connection* window is divided into five sections: DEPLOY RULES, ROUTE CONSTRAINTS, PARAMETERS, SUMMARY, and DEPLOY.

By default **DEPLOY RULES** section is selected.

Note: If the user creates a logical link, an OCI alarm is visible and it is cleared as soon as service is created on this new logical link.

Deploy Rules

DEPLOY RULES section is divided into **END POINT SELECTION** panel and depending on the selected *Signal Rate*, it is further divided into:

- **CONNECTION CONTROL**
- **OPTICAL LINE CHARACTERISTICS** (displayed when **Rate** is set to `OTSig Tunnel`)
- **ADDITIONAL DROP PORTS** (displayed when **Connection Type** is set to `1-N Broadcast Uni(Experimental)`)
- **YCABLE** (displayed for Y cable)
- **OPSB**

END POINT SELECTION Panel

Set the service rate type, signal rate, connection type, node name, port name, and port type using the **END POINT SELECTION** panel.

The following parameters are set from the **Deploy Rules** section.

Table 8-1 DEPLOY RULES Section Parameters

Parameter	Description	Supported Values
Service Rate Type	This parameter defines the type of connection, for example, a trail or an Ethernet connection.	• Trails for infrastructure connection • SONET or MultiLayerSONET for SONET service connection • Optical, CBR, MultiLayerOptical, or MultiLayerCBR for Transparent service connection • Data or MultiLayerData for Data service connection • Ethernet, SubrateEthernet, or MultiLayerEthernet for Ethernet service connection • SDH or MultiLayerSDH for SDH services

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-1 DEPLOY RULES Section Parameters (continued)

Parameter	Description	Supported Values
Rate	This parameter defines the type of signal rate, for example, ODUk or OTSig Tunnel.	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 templates, or SDH. For more information on supported signal rate values, see Table 7-2, "Service definition – containers – service rates and container options" (p. 688)
Connection Type	This parameter defines the connection shapes of infrastructure connections or services as bidirectional (bi) shape or unidirectional (uni) shape.	• 2 Ended Bi (I) • 2 Ended Split (Bi) • 3 Ended A Bi (Y) • 3 Ended Z Bi (Y) • 4 Ended Bi (X) • 1-N Broadcast Uni • 4 Ended Open Add/Drop • 1-N Broadcast Uni(Experimental)
From Node #<number>	This parameter defines the node at the A-end of the connection. As per the value of **Connection Type** the number of **From Node #<number>** parameters increases.	Select the node for deployment by clicking the search icon and selecting the node from the list displayed. Or type the node name in the text box (if you know which node to use), a list matching the typed name is displayed under the text box, select the node from that list.
From Port #<number>	This parameter defines the port name of the node at the A-end used to create a connection.	Select the node for deployment by clicking the search icon and selecting the node from the list displayed. Or type the node name in the text box (if you know which node to use), a list matching the typed name is displayed under the text box, select the node from that list.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-1 DEPLOY RULES Section Parameters (continued)

Parameter	Description	Supported Values
To Node #<number>	This parameter defines the node at the Z-end of the connection. As per the value of **Connection Type** the number of **To Node #<number>** parameters increases.	Select the node for deployment by clicking the search icon and selecting the node from the list displayed. Or type the node name in the text box (if you know which node to use), a list matching the typed name is displayed under the text box, select the node from that list.
To Port #<number>	This parameter defines the port name of the node at the Z-end used to create a connection.	Select the node for deployment by clicking the search icon and selecting the node from the list displayed. Or type the node name in the text box (if you know which node to use), a list matching the typed name is displayed under the text box, select the node from that list.
From Port Type #<number>	This parameter determines if a UNI or NNI port is created when an MDL port is selected as the connection endpoint in regards to the **From Node #<number>**	Supported values are Terminated (default value) or UnTerminated. **NOTE:** • For 3-ended Y connections and for 4-ended X connections, multiple From Port Type #<number> fields are displayed, depending on the display of the From Port #<number> field. • When DSR connections are automatically discovered (through application notification or Auto Discovery), the From/To Port Type #<number> parameter is set for all connection endpoints. • If the From Port Type #<number> 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 cards. • Ports on 103SCEC cards are displayed for connections with service rate of 100 GbE, 40 GbE, and 10 GbE. • 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-1 DEPLOY RULES Section Parameters (continued)

Parameter	Description	Supported Values
To Port Type #<number>	This parameter determines if a UNI or NNI port is created when an MDL port is selected as the connection endpoint in regards to the **To Node #<number>**.	Supported values are Terminated (default value) or UnTerminated. **NOTE:** • 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.

For more information on these parameters, see 7.4 "Service definition field descriptions for deploy Best Practices templates" (p. 688)

CONNECTION CHARACTERISTICS tab

Define the route details related to a new service, infrastructure, or physical connection to be deployed, using the **CONNECTION CHARACTERITICS** tab.

Following are the different parameters for**CONNECTION CHARACTERITICS** tab.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters

Parameter	Description
Protection	This parameter check box defines if the infrastructure connection or service is a protected or unprotected. Select the check box for Protected connection. For Unprotected connection, ensure the check box is unchecked.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Logical Link	This parameter check box 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. The **Enable NIM** is not applicable for a logical link during creation. You can enable or disable the NIM after logical link is created. For more information, see 2.8 "Determine the Infrastructure to be created" (p. 168). Select the check box if the infrastructure connection is a logical link. By default the check box is unchecked, with these exceptions: check box is checked by default for all SNC-I, SNC-N Protected infrastructure connections, Unprotected OCS Uplink ODUk infrastructure connections, or OPSA Alien Wavelength. The OMS-P Protected OMS templates do not display the **Logical Link** check box.
L-Band Frequency	This parameter check box when enabled, is used for creating a connection with L-Band frequency range. **Note:** For ODUk NNI service creation: • if **L-Band Frequency** check box is not selected, in the **ROUTE CONSTRAINTS**section available `C` and `C+L` band servers are displayed. • if **L-Band Frequency** check box is selected, in the **ROUTE CONSTRAINTS**section available `L` and `C+L` band servers are displayed.
Routing Mode	This parameter is a drop-down list. Supported values are **Automatic** (by default) or **Manual**. • If Routing mode is Automatic, specify partial constraints, that is, end-to-end connectivity is not needed. It is sufficient to include or exclude the preferences. 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 (at the physical level or at the logical level). **Note:** If routing mode is Automatic, specify the frequency constraint for Managed Plane without selecting any trails. The user has to specify atleast one trail and frequency constraint for ASON routed connections. • If Routing mode is Manual, 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 same node) are determined by the system.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Allow ASON Resources	This parameter is used for the connection creation of HO ODUk trail and ODUk service integrated provisioning of Managed Plane connections. Check this check box to create managed plane using ASON resources, by default this check box is not checked.
ASON	This parameter is a check box. • Select this check box if the connection is a Control Plane or Mixed Plane connection or an ASON MRN terminated or unterminated tunnel. If this check box is checked, in the **Parameters** section, the system activates the **Restoration** tab. If **ASON** check box is selected in the **Deploy Rules** section, 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. • Uncheck this check box, if the connection is a Managed Plane or Logical Drop Link connection. This field is not applicable for OTUk connection rates. For ASON routing constraints, see “Physical connections as a constraint for routing” (p. 733).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Auto Server Creation	This parameter check box determines if the user or NFM-T system creates the server layer for the infrastructure connection or service. The created infrastructure connection and the service, along with the server layer connection, becomes part of a group and is managed as a group. If the Auto Server Creation check box is checked, NFM-T automatically creates the server layer for the infrastructure connection or for the service, if the server layer is needed. For example: if the infrastructure connection or service connection is removed, the servers that were originally created for the particular connection are also removed. If the check box is unchecked, ensure to create each connection layer separately. **Provisioning Notes:** • If the Auto Server Creation check box is checked and the server of the connection that is being created already exists in the Allocated, Implemented, or Commissioned stage, the system rejects the provisioning request and outputs an error message. Cancel the server connection from the connection data table and re-submit the provisioning request. • Uncheck the check box during connection provisioning to create HO-ODUk infrastructure trail connections using pool ports for compound node uplink configurations that include multiple hops and/or protected ODUk infrastructure trails. 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, uncheck the **Auto Server Creation** check box. First create the OTU4 infrastructure trail, then the ODU4 infrastructure that terminates on the pool port, then the ODU2 protected connection, and finally the DSR service connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
	Auto Server Creation (continued) • Check the check box during connection provisioning to create HO-ODUk infrastructure trails using pool ports for compound node uplink configurations that include single hops and unprotected ODUk infrastructure trails. For example, for an OTU4 infrastructure connection between an 130SCUP and an SCUPB that has an ODU4 infrastructure connection between an ODU pool, check the **Auto Server Creation** box. 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** check box when creating the DSR. The system automatically creates the ODU4 connection on the pool ports, so you do not have to create the connection to the pool ports manually. **Note:** If you try to create the DSR service (with an ODU4 server layer) on an 1XANY100G circuit card, the ODU4 that terminates on the pool ports cannot be created because the ODU4 is the server for the DSR service; so, the ODU4 is simply terminated on the 1XANY100G card. • If **Manual** Routing mode is selected 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 is used as the routing constraints. For the second and/or consecutive DSR, the link connection(s) from the system created ODU4 connection that terminate on ODU pool ports is used as the routing constraints. The **Auto Server Creation** check 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, 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Provisionable Wave Key	This parameter is a drop-down list. Supported values are: **Keyed** (by default), **UnKeyed**, or **N/A**. This parameter is required for NEs, that allows 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, select the value **N/A**. • If the connection contains at least one NE that supports provisionable Wavelength Tracker, select **Keyed**. • If the connection contains at least one NE that supports provisionable Wavelength Tracker, select **UnKeyed** to disable Wavelength Tracker. The system displays the Wave Key parameter when you 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 card and **Auto Server Creation** is checked. • An ODUk infrastructure connection if one or more connection endpoints is an ODUk CTP on a 1UD200 card 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 card that supports a NNI client port rate that is equal to the line port rate (e.g. 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 card and the **Logical Link** field is checked and the **Auto Server Creation** field is checked.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
	The following conventions hold for the services that support Wave Key configuration: • For Transparent Alien Wavelength (OCH) services, the **Wave Key** field is set as **Keyed** by default. • For Transparent Alien Wavelength (unkeyed OCH) services, the **Wave Key** field is set as **UnKeyed** by default. • For Transparent OCHP Protected Alien Wavelength (OCH) services, the **Wave Key** field is set as **Keyed** by default. If you select **Keyed**, the system validates that end ports of the connection are on an unsupported NE or on a circuit card. 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 **Wave Key** field; that is, if you 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.
Customer Name	*Optional:* This parameter is a text box. Select the Customer Name for with the connection being created by clicking on the search icon. The customer names that are displayed in the list are names entered from the **ADMINISTER > Customers** navigation path on the WebUI. **Note:** • For auto-discovered connections and system auto-generated connections, there are no customer names. • Customer name is not saved and displayed, when a connection is discovered after a DB delete and Path Sync discovery. For more information, see *ADMINISTER - Customers* section in the *Administration Guide: Common Functions* guide.
Connection Alias	*Optional:* This parameter is a text box. Enter the connection alias to be associated with the connection being created. This alias is associated with the name that is entered in the Connection Name field. In addition, the Connection Alias field is controlled by installation parameters. **Note:** • The **Connection Alias** supports a maximum of 256 characters and special character `%` (percentage) is not supported. • Connection Alias is not saved and displayed, when a connection is discovered after a DB delete and Path Sync discovery. For more information, see 2.26 "Connection names and aliases" (p. 260).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Connection Name	*Optional:* This parameter is a text box. Enter a name to be associated with the connection being created. If a connection name is not entered, the system auto populates the name with the values from the **From Node** and **To Node** parameters and the name is displayed in the **SUMMARY** section. **Note:** Connection name supports a maximum of 39 Chinese or Japanese characters, or 178 ASCII characters. Special characters `,` (comma) and `%` (percentage) are not supported. This name 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. For more information, see 2.26 "Connection names and aliases" (p. 260) for details.
Target State	This parameter is a drop-down list. The supported values are: • **Defined**, when the termination points are defined. • **Allocated**, when the route is allocated. • **Implemented**, when the trail is implemented into the network element. • **Commissioned**, when the client and link connection are created.
ODUflex Bandwidth-(Gps)	This parameter is a text box. It is enabled only when *`Flexible Rate Client`* is selected for **`Service Rate`** parameter. The ODUflex (GFP) rate is a multiple of approximately 1.25 GHz, 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. Select the value from the spinner. 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, by selecting the Additional attributes. The number of time slots is obtained dividing the ODUflex Bandwidth (Gps) by 1.25 GHz. Refer to "ODUflex " (p. 256) for details on ODUflex connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Compute Latency	This parameter is a check box. By default, **Compute Latency** is checked. Latency measurement is used to compute the amount of time taken by a signal in traveling from the A-End to the Z-End for a service. This measurement is only available for created services with UNI rates (that is, 10 GbE, 100 GbE, 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 at which the **Compute Latency** operation was executed **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 (y-cable 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. • 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. • For a client-protected service with working and protection legs, the **Latency Timestamp** is the timestamp from the last measurement operation. • 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. • 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**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Roll Back On Failure	This parameter is a check box. Enable this check box for all types of services and infrastructure creation templates. When you check this option during the connection creation, on failure of connection, the creation is canceled.
Allow Uncommis-sioned Links	This parameter is a check box. Check this check box if you want the system to create the connection regardless of the commission status of the optical amplifiers and make the manual power adjustments from Wavelength Tracker for both egress and ingress ports on an uncommissioned link. Uncheck this check box, the connection fails if any optical amplifier in the connection is not commissioned. The NFM-T OTN allows you 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-2 CONNECTION CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Suggest Routes Before Deploy	This parameter is a check box. It displays possible routes that can be deployed for a connection. With a maximum of five possible routes from ROUTE 1 to ROUTE 5. The routes are also represented in a graph where you use the zoom option to zoom-in or zoom-out of the graph. To select a route, click on the **ROUTE <#>** button. • When the **Routing Mode** is set to `Automatic` and the **Suggest Routes Before Deploy** check box is checked, under **SUMMARY** section, **SUGGESTED ROUTES** pane is displayed. • When the **Routing Mode** is set to `Automatic` and the **Suggest Routes Before Deploy** check box is not checked, under **SUMMARY** section, **SUGGESTED ROUTES** pane is not displayed. • When the **Routing Mode** is set to `Manual` , the **Suggest Routes Before Deploy** check box is disabled. hence the **SUMMARY** section does not display the **SUGGESTED ROUTES** pane. • When the **Routing Mode** is set to `Automatic` and any Routing Constraint is selected in the **ROUTING CONSTRAINTS** section, then the **SUMMARY** section does not display the **SUGGESTED ROUTES** pane irrespective of the enabling or disabling of **Suggest Routes Before Deploy** check box. • When the **Routing Mode** is set to `Automatic` and the Frequency Constraint is selected in the **Frequency** tab of **ROUTING CONSTRAINTS** section, then the **SUMMARY** section does not display the **SUGGESTED ROUTES** pane irrespective of the enabling or disabling of **Suggest Routes Before Deploy** check box. • When the connection is modified (**OPERATE> Infrastructure Connection > More ⋮ > Modify Connection > Parameters**, the **Suggest Routes Before Deploy** check box is not displayed in the **DEPLOY RULES** section. **Note:** Few temporary connections may be created in the **Allocated** state as part of preview of the connection. Suggested Route feature does not work for Alien OCH service provisioning • When the user selects the **Suggest Routes Before Deploy** field for a topology with multiple routes, the system displays five possible routes during infrastructure connection provisioning. • When the user selects the **Suggest Routes Before Deploy** field for a topology with multiple routes, the system displays only one route during service provisioning. **Example:** Select the Alien OCH template *(/Best Practices/Service/Transparent/Unprotected/Alien Wavelength (unkeyed OCH)*. Deploy a service where there are multiple links between the NEs after selecting **Suggest Routes Before Deploy** check box. During deployment the **SUGGESTED ROUTES** pane displays only one route although there are multiple routes in the topology.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

OPTICAL LINE CHARACTERISTICS

OPTICAL LINE CHARACTERISTICS tab is enabled when **OTSig Tunnel** is set as the Rate. The OTSig Tunnel is enabled for cards that are equipped with ADD3 and ADD4 ASIC. The line port rate is OTSig regardless of the line capacity.

The client ports signal rates are:

- 100 GBE with ODU4 container
- 400 GbE with ODUflex as the container
- 100 GbE with ODUTC1 container for S6AD600H and SFM6 cards
- 400 GbE with ODUTC4 container for S6AD600H and SFM6 cards

ADD4 ASIC is supported for S6AD600H, S4X400H, DFC12/DFC12E, S5AD400H, DFM6/DFM6E, SFM6, and 2UX500 cards and ADD3 is supported for 8UC1T, 4UC1T cards.

Following are the different parameters for **OPTICAL LINE CHARACTERISTICS** tab.

Table 8-3 OPTICAL LINE CHARACTERISTICS Tab Parameters

Parameter	Description
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.
Profile Number	This parameter is a text box. Click the **Search** icon to select the **Profile Number**. Depending on the **Profile Number** selection, the values of the rest of the parameters change. To know the supported profile numbers, see Table 8-4, “Profile Number and supported Parameter values ” (p. 1236). To know the mapping between the profile and supported cards, see “Profile and Supported Cards” (p. 1267).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-3 OPTICAL LINE CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
OTU Type	Specifies the rate supported for the selected Profile Number. Select OTU4 for 100 GbE connections Select OTUC4 for 400 GbE connections For S6AD600H and SFM6 card, depending on the **Profile Number**, the applicable **OTU Type** is displayed: • For Profile Number 26 - the applicable OTU type is **6xOTUTC1** or **2xOTUTC1 and 1xOTUTC4**. **Note**: In NFM-T R21.12, 2xOTUTC1 and 1xOTUTC4 are not supported for Control Plane connections. • For Profile Number 27 - the applicable OTU type is **4xOTUTC1** or **1xOTUTC4** • For Profile Number 28 - the applicable OTU type is **3xOTU4** • For Profile Number 29 - the applicable OTU type is **4xOTU4** or **1xOTUC4** **Note:** In NFM-T R21.12, 1xOTUC4 is not supported on SFM6 card. • For Profile Number 32 - the applicable OTU type is **1xOTUC4 and 1xOTU4 or 5xOTU4** • For Profile Number 33 - the applicable OTU type is **3xOTUTC1** • For Profile Number 34 - the applicable OTU type is **1xOTUTC1 and 1xOTUTC4 or 5xOTUTC1** • For Profile Number 38 - the applicable OTU type is **5xOTU4** or **1xOTU4 and 1xOTUC4** **Note**: In NFM-T R22.6, profile number 38 supports only Managed Plane connections.
Payload Rate	This parameter defines the payload of the OTSiG in Gbaud per second.
Baud Rate	This parameter defines the baud rate of the OTSiG in Gbaud.
Encoding	This parameter indicates the modulation or line code which is applied on the selected port.
FEC Mode	FEC is Forward Error Correction, the FEC Mode field depends on the value set on the NE. Supported values are: **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**, **802.3bj**, **G.709**, **I.4**, and **I.7**.
Phase Encoding	This parameter specifies the phase encoding mode applied to the optical carrier of the line port.
Client OTU Type	This parameter defines the type of clients that can be transported by the OTSiG signal.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-3 OPTICAL LINE CHARACTERISTICS Tab Parameters (continued)

Parameter	Description
Transmit Shape	This parameter defines the type of transmitted waveshape, such as `Single Channel`, `Super Channel`, `Alien`, and `Use NE Value`.
Channel Width	This parameter is a drop-down list. 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 options available in the **Channel width** field depends on the option selected in the Profile Number. The values are 50 GHz, 62.5 GHz, 75 GHz, 87.5 GHz, 100.0 GHz, and 112.5 GHz displayed in a drop-down list, from where the desired value can be selected. **Channel Width** is not applicable for unamplified connections. Discovered unamplified tunnels will have the default **Channel Width** of 50 GHz. On an OTS Created with Line Driver (LD) pack that allows extra channels, if WTOCM-F card is configured then provisioning using the additional channels is allowed. Whether an LD pack supports extra channels is determined by the frequency range parameters supported by it.

Note: The parameters **Payload Rate, Baud Rate, Encoding, FEC Mode, Phase Encoding, OTU Type,** and **Transmit Shape** are read-only fields. The value of these parameters depend on the selected **Profile Number**.

Table 8-4 Profile Number and supported Parameter values

If	Then
the **Profile Number** is 1	• **Payload Rate**: 100 • **Baud Rate**: 56 • **Encoding**: QPSK • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 100 G via 56Gbaud QPSK with SDFEC-G2 for Flex Clients • **Channel Width**: 62.5, 75.0, 87.5 **Note:** 62.5 and 87.5 are not supported by GMRE/ASON.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 2	• **Payload Rate**: 200 • **Baud Rate**: 62 • **Encoding**: QPSK • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 200 G via 62Gbaud QPSK with SDFEC-G2 for Flex OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 87.5 is not supported by GMRE/ASON.
the **Profile Number** is 3	• **Payload Rate**: 300 • **Baud Rate**: 62 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 300 G via 62Gbaud 16SQAM with SDFEC-G2 for Flex OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 87.5 is not supported by GMRE/ASON.
the **Profile Number** is 4	• **Payload Rate**: 400 • **Baud Rate**: 62 • **Encoding**: 16QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 400 G via 62Gbaud 16QAM with SDFEC-G2 for Flex OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 87.5 is not supported by GMRE/ASON.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 5	• **Payload Rate**: 400 • **Baud Rate**: 67 • **Encoding**: 16QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 400 G via 67Gbaud 16QAM with SDFEC-G2 for Flex OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 75.0 is not supported by GMRE/ASON.
the **Profile Number** is 7	• **Payload Rate**: 100 • **Baud Rate**: 33 • **Encoding**: QPSK • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Differential • **OTU Type**: OTU4 • **Transmit Shape**: Single Channel • **Description**: 100 G via 33Gbaud QPSK with SDFEC-G2 for OTU4 Clients • **Channel Width**: 37.5, 50, 62.5, 75, 87.5 Currently, carrier profile 7 is supported for Managed Plane only.
the **Profile Number** is 8	• **Payload Rate**: 300 • **Baud Rate**: 67 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 300 G via 67Gbaud 16SQAM with SDFEC-G2 for Flex OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 75.0 is not supported by GMRE/ASON.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 9	• **Payload Rate**: 100 • **Baud Rate**: 33 • **Encoding**: QPSK • **FEC Mode**: SDFEC-ACC • **Phase Encoding**: Absolute • **OTU Type**: OTU4 • **Transmit Shape**: Single Channel • **Name**: Long haul 100 G interop ACC-FEC • **Details**: Long haul 100 G interop ACC-FEC • **Channel Width**: 37.5, 50, 62.5, 75, 87.5, and 100.0 **Note:** - 37.5, 62.5, 75, 87.5, and 100.0 are not supported by GMRE/ASON. - 50 GHz channel width is supported for Control Plane.
the **Profile Number** is 10	• **Payload Rate**: 200 • **Baud Rate**: 33 • **Encoding**: 16 QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Differential • **OTU Type**: OTU4 • **Transmit Shape**: Single Channel • **Description**: 200 G via 33Gbaud 16 QAM with SDFEC-G2 for OTU4 Clients • **Channel Width**: 37.5, 50, 62.5, 75, 87.5 Currently, carrier profile 10 is supported for Managed Plane only.
the **Profile Number** is 11	• **Payload Rate**: 200 • **Baud Rate**: 33 • **Encoding**: 16QAM • **FEC Mode**: SDFEC-ACC • **Phase Encoding**: Absolute • **OTU Type**: OTU4 • **Transmit Shape**: Single Channel • **Name**: Metro 200 G interop ACC-FEC • **Details**: Metro 200G interop ACC-FEC • **Channel Width**: 37.5, 50, 62.5, 75, 87.5, and 100.0 **Note:** - 50 GHz channel width is supported for Control Plane. - 37.5, 62.5, 75, 87.5, and 100.0 are not supported by GMRE/ASON.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 12	• **Payload Rate**: 200 • **Baud Rate**: 33 • **Encoding**: 16QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: OTU4 • **Transmit Shape**: Single Channel • **Name**: Metro 200 G interop ACC-FEC • **Details**: Metro 200G interop ACC-FEC • **Channel Width**: 37.5, 50.0, 62.5 **Note:** Channel width 37.5 and 62.5 do not support ASON.
the **Profile Number** is 15	• **Payload Rate**: 200 • **Baud Rate**: 67 • **Encoding**: QPSK • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 200 G via 67Gbaud QPSK with SDFEC-G2 for FLEX OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 75.0 is not supported by GMRE/ASON.
the **Profile Number** is 16	• **Payload Rate**: 500 • **Baud Rate**: 67 • **Encoding**: 32QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 500G via 67Gbaud 32QAM with SDFEC-G2 for FLEX OTU in OTSIG • **Channel Width**: 75.0, 87.5, 100.0

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 19	• **Payload Rate**: 100 • **Baud Rate**: 45 • **Encoding**: QPSK • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 100 G via 45Gbaud QPSK with SDFEC-G2 for FLEX OTU in OTSIG. • **Channel Width**: 50.0, 62.5, 75.0 **Note:** 50.0 and 75.0 are not supported by GMRE/ASON.
the **Profile Number** is 20	• **Payload Rate**: 200 • **Baud Rate**: 45 • **Encoding**: 8QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 200 G via 45Gbaud 8QAM with SDFEC-G2 for FLEX OTU in OTSIG. • **Channel Width**: 62.5, 75.0
the **Profile Number** is 21	• **Payload Rate**: 300 • **Baud Rate**: 62 • **Encoding**: 8QAM • **FEC Mode**: SDFEC-G2 • **Phase Encoding**: Absolute • **OTU Type**: FLEX • **Transmit Shape**: Super Channel • **Description**: 300 G via 62Gbaud 8QAM with SDFEC-G2 for FLEX OTU in OTSIG. • **Channel Width**: 75.0, 87.5 **Note:** 87.5 is not supported by GMRE/ASON.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 26	• **Payload Rate**: 600 • **Baud Rate**: 90.22 • **Encoding**: 16QAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: OTUTCn • **Transmit Shape**: Super Channel • **Description**: 600 G via 90.22Gbaud 16QAM with SDFEC-V for OTUTCn in OTSIG • **Channel Width**: 112.5, 100 Default value: 112.5
the **Profile Number** is 27	• **Payload Rate**: 400 • **Baud Rate**: 86.04 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: OTUTCn • **Transmit Shape**: Super Channel • **Description**: 400 G via 86.04Gbaud 16SQAM with SDFEC-V for OTUTCn in OTSIG. • **Channel Width**: 100, 112.5 Default value: 100
the **Profile Number** is 28	• **Payload Rate**: 300 • **Baud Rate**: 86.36 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: Flex • **Transmit Shape**: Super Channel • **Description**: 300G via 86.36Gbaud 16SQAM with SDFEC-V for FLEX OTU in OTSIG • **Channel Width**: 100, 112.5 Default value: 100

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 29	• **Payload Rate**: 400 • **Baud Rate**: 85.82 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: Flex • **Transmit Shape**: Super Channel • **Description**: 400 G via 85.82Gbaud 16SQAM with SDFEC-V for Flex OTU in OTSIG. • **Channel Width**: 100, 112.5 Default value: 100
the **Profile Number** is 32	• **Payload Rate**: 500 • **Baud Rate**: 87.36 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: Flex • **Transmit Shape**: Super Channel • **Description**: 500G via 87.36Gbaud 16SQAM with SDFEC-V for FLEX OTU in OTSIG • **Channel Width**: 100, 112.5 Default value: 100
the **Profile Number** is 33	• **Payload Rate**: 300 • **Baud Rate**: 84.23 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: OTUTCn • **Transmit Shape**: Super Channel • **Description**: 300G via 84.23Gbaud 16SQAM with SDFEC-V for OTUTCn in OTSIG • **Channel Width**: 100, 112.5 Default value: 100

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-4 Profile Number and supported Parameter values (continued)

If	Then
the **Profile Number** is 34	• **Payload Rate**: 500 • **Baud Rate**: 87.16 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: OTUTCn • **Transmit Shape**: Super Channel • **Description**: 500G via 87.16Gbaud 16SQAM with SDFEC-V for OTUTCn in OTSIG • **Channel Width**: 100, 112.5 Default value: 100
the **Profile Number** is 38	• **Payload Rate**: 500 • **Baud Rate**: 87.36 • **Encoding**: 16SQAM • **FEC Mode**: SDFEC-V • **Phase Encoding**: Absolute • **OTU Type**: Flex • **Transmit Shape**: Super Channel • **Description**: 500G via 87.36Gbaud 16SQAM with SDFEC-V for FLEX in OTSIG • **Channel Width**: 100, 112.5 Default value: 112.5

Note:

- 87.5 GHz channel width is not supported by GMRE/ASON for profile 1 and an error message `Status:GMRE does not support the selected channel width <Channel Width value> for the profile <ID>.` is displayed.
- In NFM-T R20.7, new profiles with XC width 75 GHz and 87.5 GHz are supported for flex grid networks only.
- When creating control plane connections using customized templates, re-verify the **Channel Width** field and update if required.
- When **Profile Number** is modified, ensure to select the applicable **Channel Width** as required.

Route Constraints

The ROUTE CONSTRAINTS section is divided into five tabs, which allows to specify the route to be taken for a connection. When an infrastructure or a service connection is created, you can provide a suggestion to the system on how to route the connection. The system takes into account the specified suggestions while it considers the hardware configuration, internal NE topology, and the available capacity to route a connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

If **Routing Mode** is `Manual`	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 same node) are determined by the system.
If **Routing Mode** is `Automatic`	Specify partial constraints, that is, end-to-end connectivity is not needed. It is sufficient to include or exclude the preferences. For Managed Plane, you 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. 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 preemptible 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). specify the frequency constraint for Managed Plane without selecting any trails. You need to specify at least one trail and frequency constraint for ASON routed connections.

Note:

- When you specify more links than are needed to establish a connection, the system discards the additional links and picks up any available frequency or time slot on the selected links.
- When you specify more trails, the system doesn't discard additional trails, instead it validates them and gives a failure message.

The ROUTE CONSTRAINTS sections is divided into five tabs: Infrastructure, Node, 3R, Physical Connection, and Frequency.

The following table depicts the types of Routing Constraints and the support on Managed Plane, Control, Plane, and Mixed Plane connections.

Table 8-5 Connection Creation Support

Constraint Type	Managed Plane	Control Plane	Mixed Plane
Infrastructure	√	√	√
3R	√	√	√
Node Constraint	x	√	√*
Physical Connection	x	√	√**
Frequency	√	√	√

Note:

* The scope of node is only within ASON domain. Trail constraints to be added as support for non ASON domain in the connection

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

** The scope of physical link is only within ASON domain. Trail constraints to be added as support for non ASON domain in the connection

If the **Routing Mode** is *Manual* and **ASON** check box is selected, the **Node** and **Physical Connection** tabs are disabled and not supported for ASON connection provisioning, that is in Manual routing mode the full end-to-end connectivity needs to be specified for all trail or Link connection.

The following table depicts the Connection modification support.

Table 8-6 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

The following options are displayed for a selected trail, infrastructure, 3R, physical Connections, and frequency constraints:

- INCREASE FREQUENCY: Increase the frequency of the link. Supported for Subsea frequency only.
- DECREASE FREQUENCY: Decrease the frequency of the link. Supported for Subsea frequency only.
- INCLUDE: Change constraint to be included, if it is added as excluded.
- EXCLUDE: Change constraint to be excluded, if it is added as included.
- SERVICE: Change the constraint to a service.
- PROTECTION: Change the constraint as protected.
- REMOVE: To remove the link.

Infrastructure tab

Infrastructure tab allows you to set up the intermediate cross-connects by specifying a full end-to-end connection or a partial connection and lets the system select the remaining settings.

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: Only one connection can be used for a logical link at a time. You can setup this template but it is only useful for one connection at a time. Read also "Creation of 3R object needs particular sequence to be stored in OTN DB" (p. 2436) for 3R more information.

From the *Infrastructure* tab, the **Near End Node** displays the A-end of the infrastructure trails that are displayed in the list then become the list of eligible trails ingress that node can support for a

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

connection. From the **Infrastructure Conenctions**, select the **Far End Node** which is the Z-end of the connection which is the egress trail. Select **INCLUDE** or **EXCLUDE** that node, the far-end is now the **Current Node**. The infrastructure trails that are then displayed are those egressing that node. In this manner, the you can navigate the network and go from the **From Node #1** towards the **To Node #1**.

Note: 10 GbE provisioning with an ODU2E container: In some cases during the selection of Link connections, 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 is carried, for example, 130SCX10. NFM-T displays the correct link connections that can support the ODU2e rate during provisioning.

Once the 10 GbE service has been set up, the server is marked with an ODU2E rate in the 360 degree server list panel of the connection.

Node tab

Select **INCLUDE** or **EXCLUDE** a node as constraint for routing traffic for L1 and L0 Managed, Control, or Mixed Plane connections when provisioning a new connection from the Routing Constraints section. When specifying the **INCLUDE** node constraint, the system attempts to route the connection by using any ingress/egress trail/link incident that is on that node. When specifying the **EXCLUDE** node constraint, the system ensures that no immediate server is incident on the excluded node.

INCLUDE and **EXCLUDE** behavior

- **INCLUDE**, 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 connection end points.
- **EXCLUDE** constraints has the highest priority. The system excludes the selected Node in the specified role (Service or Protection) completely. The node is excluded across all layers.

3R tab

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.

Select a 3R port when creating the photonic infrastructure. When selecting the 3R port, indicate the port should be in the working or in the protection part of the route by clicking on the **SERVICE** or **PROTECTION** button. To delete a routing 3R constraint from the data table select the constraint and click **REMOVE** button. The system deletes the routing constraint from the data table.

INCLUDE and **EXCLUDE** behavior

- **INCLUDE** specifes which 3R ports the system should select to regenerate the signal when they need to create a long span ODUk infrastructure that requires regeneration.
- **EXCLUDE** indicates which 3R ports system should avoid picking as a resource while routing.

Physical Connection tab

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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Specify the links to **INCLUDE** or **EXCLUDE** when 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. You can include or exclude physical connections as constraint for routing traffic for L1 and L0 Control, Managed, or Mixed Plane connections when provisioning a new connection from the Routing Constraints section.

From the list select a physical connection and click **INCLUDE** or **EXCLUDE**.

INCLUDE and **EXCLUDE** behavior

- **INCLUDE** 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 are weighted to be included.
- **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.

Frequency tab

Select the following parameters from this tab for a connection.

Table 8-7 Frequency tab Parameters

Parameter	Description
System Assigned Frequency	System assigns the frequency when this check box is selected. If this box is not selected, the system prompts to select the required frequency is DWDM or CWDM.
Enforce Physical Link Diversity	Check box for reusing the OTS link. By default, this field is enabled.
Subsea (1.25GHz)	Determines if the connection is a standard connection using 6.25 GHz grid step size or a subsea connection using 1.25 GHz grid step size. This parameter is displayed when **Routing Mode** is set to `Manual`.
CWDM	Course Wavelength-Division Multiplexers
DWDM	Dense Wavelength-Division Multiplexers
Frequency	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. The system only displays spare Link Connections that have a spare or an adjacent channel on both sides of the displayed Frequency. For more information, see 24.2 “Quick Help – The Create Connection Window” (p. 1970).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-7 Frequency tab Parameters (continued)

Parameter	Description
FREQUENCY MAP	This field is applicable only for Managed Plane connections. Click **FREQUENCY MAP** to view a graphical view (starting from the trail deploy wizard) the real status of the selected OMS frequencies, both allocated and available. Select one of the available frequency as constraint. for more information, see 24.5 "Quick Help – The OA&M Diagnostics Window " (p. 1990)

Note: Important Considerations.

- **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**.

- **HO-ODU4 Connections on 112SDX11 cards**

  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/OTL4.4connections, 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. End point change and frequency change are not supported for **Rearrange** of OTL4.4 connections.

- **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 **ROUTE CONSTRAINTS** to enforce or relax strict diversity rules for both unprotected and protected services.

  Disable the **Enforce Physical Link Diversity** parameter during creation of a protected connection if physical diversity is not required in the service and protection paths of the protected connection (that is, the OTS link can be reused in either path, or between the two paths). To create a connection, the routing engine finds suitable diverse paths in the network with the specified constraints. If it fails to find diverse paths, then both the service

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

and protected paths will allow reuse of the OTS link. However, the service and protection paths cannot reuse the infrastructure connection.

For SNCP connections, maximal diversity of paths will be attempted when strict diversity is not possible and OTS link reuse is allowed. For Y-cable and OPSB connections, maximal diversity of paths will not be attempted when strict diversity rules are relaxed by allowing for OTS link reuse.

The **Enforce Physical Link Diversity** parameter is available on **Service Definition** provisioning which includes Ethernet/Sonet/SDH/Data rate templates and transparent services.

Parameters

Parameters section is divided into tabs. These tabs depend on the type of service rate, signal type, and template used to create a connection.

The different tabs are: TRANSMISSION, ASSURANCE, WAVE KEY, PROTECTION, RESTORATION, OCHP, OTHERS.

TRANSMISSION tab

TRANSMISSION tab allows you to specify (in some cases to modify) parameters that control the transmission of the connection as it is being deployed. This tab is visible for all infrastructure, service, and multilayer connections.

Note: Transmission parameters are not supported on the OTSig trail with **OTU Type** as OTU4 and OTUC4. The **Transmission** parameters are displayed on the NE. Although, there is no support from NFM-T to either set this field during create or modify.

The following parameters are available in the TRANSMISSION tab.

Table 8-8 TRANSMISSION Tab Parameters.

Parameter	Description
Signal Type	**Signal Type** parameter is **Default** for an infrastructure connection, except for OMS-P Protected is **OMS** and OPSA-Protected is **OCH**. The **Signal Type** field varies for **SONET**, **Transparent**, **Data**, **Ethernet**, or **SDH** services.
Container	This parameter lists the supported container based on the **Signal Type** selected. For a service on an OTSiG tunnel using card S6AD600H, based on the model (standard or transcoding) the following possible containers are displayed: • For a 100 GbE service, containers ODU4 and ODUTC1 • For a 400 GbE service, containers ODUTC4 and ODUFlex

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-8 TRANSMISSION Tab Parameters. (continued)

Parameter	Description
Line Port Timeslot(s)	This parameter is required to assign the logical time slot of the Line Port for the 4DPA4 cards in FlexMux mode. The number of required selections in the Line Port Timeslot(s) field is based on the Signal Type of the Client Port. • For a Signal Type of OC-3, STM-1, or Fast Ethernet one selection in the Line Port Timeslot(s) field is required. • For a Signal Type of OC-12 or STM-4 four selections in the Line Port Timeslot(s) field are required. • For a Signal Type of OC-48 or STM-16 sixteen selections in the Line Port Timeslot(s) field are required. • For a Signal Type of 1GbE eight selections in the Line Port Timeslot(s) field are required. • For a Signal Type of FC100 seven selections in the Line Port Timeslot(s) field are required. • For a Signal Type of FC200 fourteen selections in the Line Port Timeslot(s) field are required. • For a Signal Type of HDSDI ten selections in the Line Port Timeslot(s) field are required. • For a Signal Type of SDSDI or DVBASI two selections in the Line Port Timeslot(s) field are required.
Port Administrative State	This parameter 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**. When AINS is selected, the Network Element will automatically transition a facility into the In-Service state after a signal is present on the facility without a failure condition for the length of time specified by the Automatic In Service Timer field.
AINS Timer	This parameter is used to set a timer at which the administrative state of the client port can be automatically set to *In Service*. If the port administrative state is set to **IS**, the **AINS Timer** field is set to **Default**. Enter the transition soak time out of AINS using the format Hours-Minutes where the minimum time is 00-01 and the maximum time is 168-00. This parameter specifies how long an input signal must be present on the facility without a failure condition before the system transitions the facility into the In-Service state. If not specified, the system AINS Timer is used.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-8 TRANSMISSION Tab Parameters. (continued)

Parameter	Description
Encoding	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. *Conditional, for D5X500 circuit cards only:* The **Phase Encoding** parameter is displayed if at least one connection end point is on a D5X500 card and if the connection rate is OTU4 or OTU4x2 or if the connection rate is ODU4, **Auto Server Creation** is selected, **ASON** is not selected. The **Phase Encoding** parameter is a drop-down list. Select **Absolute**, which is a compatibility mode with pilot, or **Differential**, which is the high performance mode without pilot, and **Use NE Value**. **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 card, 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 card. 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.
Transmit Shape	This parameter is a drop-down list, which is the type of transmitted waveshape. Supported values are: **Single Channel**, **Super Channel**, **Alien**, and **Use NE Value**.
Channel width	This parameter is a drop-down list. 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 50 GHz, 62.5 GHz, 75 GHz, displayed in a drop-down list, from where the desired value can be selected.
SSF Delay Timer(ms)	This parameter determines the delay before the client laser is switched off due to a server signal failure (SSF). For S13X100E, S13X100R and D5X500Q cards the valid values are in the range of 0-3100 ms. For all other cards the valid values are in the range of 0-2500 ms.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-8 TRANSMISSION Tab Parameters. (continued)

Parameter	Description
Link Span	For a Direct Link, determines if the route is amplified or unamplified. This parameter is displayed when **Rate** is set to `OTSig Tunnel`.
FEC	*Optional:* This parameter is a drop-down list. FEC is Forward Error Correction, the FEC Mode field is set to **Use NE Value** as default for infrastructure connections. When creating an ODUk integrated provisioning order that auto creates the OTUk, select the type of FEC for the particular connection. Supported values are: **RSFEC** (Reed-Solomon FEC, the default), **EFEC** (Enhanced FEC), **EFEC2** (Enhanced FEC2), **AFEC** (Adaptive FEC), **SDFEC** (Soft Decision FEC), **SDFEC-G2**, **SDFEC-ACC**, **NOFEC**, **802.3bj**, **G.709**, **I.4**, and **I.7**. The **FEC** parameter is not displayed when **ASON** connections are created. 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. Use the following guidelines for particular cards: • If any endpoint is a line port on a 112SDX11 or a port on a 4AN400 card, select the option RSFEC. • If any endpoint is a client port on D5X500 card the options are RSFEC, NOFEC, select the option 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, select the option 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, select the option SDFEC-G2. • If any endpoint is a line port on D5X500, select the option 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 card combinations the options are AFEC, SDFEC, and Use NE Values (the default).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-8 TRANSMISSION Tab Parameters. (continued)

Parameter	Description
Phase Encoding	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.
Polarization Tracking	This parameter allows you to provision the speed at which the coherent line receiver tracks state of polarization changes. This parameter is displayed when **Rate** is set to `OTSig Tunnel`. 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 can result 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 cards 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 cards. The supported values are **`Use NE Values`** (default value), **`Normal`**, and **`Fast`**.

ASSURANCE tab

Allows you to specify (in some cases to modify) parameters that control the transmission of the connection as it is being deployed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

The following parameters are available in the ASSURANCE tab.

Table 8-9 ASSURANCE tab parameters

Parameter	Description
Alarm Profile	This parameter is a drop-down list. **Use_NE_Value** (default value), **Enable alarm profile**, or **Disable all alarms**. Values are: • **Use_NE_Values** - This 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** - This sets the ASAP per port role and per layer rate, and alarm reporting is enabled. **Note:** Enabling alarm profile for the connection will extend the deployment to several minutes. • **Disable all alarms** - This 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 a service for an 1830 PSS NE, select **Disable all alarms**. **Provisioning Considerations** • When creating a 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 creating 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 creating 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 cards, when creating 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 card as part of the setting Alarm Profile for the ODU4 connection. • For the 2UC400 circuit card, when creating 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 card as part of the setting Alarm Profile for the ODU4 connection. • For the 11SDX11 circuit card, when creating 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-9 ASSURANCE tab parameters (continued)

Parameter	Description
Link Utilization Profile	This parameter sets the threshold profile for the link or infrastructure connection. This field defaults to **MEDIUM** and is not applicable for services.

WAVE KEY tab

A component of the Optical Power monitoring capability that is used to identify individual wavelengths through the network. A wave key is a number between 1 and 2048.

The following parameters are available in the WAVE KEY tab.

Table 8-10 WAVE KEY Tab Parameters

Parameter	Description
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, 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, select the Wave Key pairs (that is, be aware of the current Wave Key usage in the network to avoid Wave Key collisions. • For Transparent Alien Wavelength (unkeyed OCH) services, be default, the **Provisionable Wave Key** is set as **UnKeyed**, and **Wave Key Type** is set as **N/A**. **Note:** 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.
AZ Wave keying preference	The **AZ Wave Keying Preference** (to/from preference) is a drop-down list. Values are **None** (the default), **Duplicates Allowed**, or **No Duplicates Allowed**, which is only displayed if the Wave Key Type is **Automatic**. **None** represents that the 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*: all the wave keys must be unique within the domain. *Unlocked*: all the wave keys can be reused within the domain.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-10 WAVE KEY Tab Parameters (continued)

Parameter	Description
ZA Wave keying preference	The **ZA Wave Keying Preference** (from/to preference) is a drop-down list. Values are **None** (the default), **Duplicates Allowed**, or **No Duplicates Allowed**, which is only displayed if the Wave Key Type is **Automatic**. **None** represents that the 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*: all the wave keys must be unique within the domain. *Unlocked*: all the wave keys can be reused within the domain.
Wave Key Assignment(Legacy)	If the **Wave Key Type** is **Manual**, the **Wave Key Assignment (Legacy)** parameter field is activated. It 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, select the exact Wave Key pairs that are assigned to the connection. For **Automatic** routing, you must select the Lambda (frequency) before selecting the Wave Key pairs. For **Manual** routing, you must select at least one link connection before selecting the Wave Key pairs because valid Wave Key pairs are based on the frequency of 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. • If **System Assigned** is selected, NFM-T selects the Wave Key pairs that are assigned to the connection. NFM-T assigns values which are unique for all connections managed by NFM-T. If **User Selected** is selected, the user must select the exact Wave Key pairs that are assigned to the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-10 WAVE KEY Tab Parameters (continued)

Parameter	Description
AZ Wave Key Pair	The **AZ Wave Key Pair** (the from/to pair) is a text field. Click search icon and select value from 9170 to 9605 in increments of 5 (for example: 9170, 9175, 9180, 9185, ...9600, 9605). If the **Wave Key Assignment (Legacy)** is set to **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 the 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. **Note:** • The **AZ Wave Key Pair** and **ZA Wave Key Pair** fields are not displayed for OTU4 and OTL4.4 connections on 112SDX11 cards. • For manual wave key provisioning of connections with 112SDX11 endpoints, four pairs of wave keys are required. For the 112SDX11 card, 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 cards, 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.
ZA Wave Key Pair	The **ZA Wave Key Pair** (the to/from pair) is a text field. Click search icon and select value from 9170 to 9605 in increments of 5 (for example: 9170, 9175, 9180, 9185, ..9600, 9605). If the **Wave Key Assignment (Legacy)** is set to **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 the 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.

PROTECTION tab

A protection type for a service network connection or infrastructure network connection in which the traffic is protected from end to end (at the physical or logical level).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

The following parameters are available in the PROTECTION tab.

Table 8-11 PROTECTION Tab Parameters

Parameter	Description
Client Protection Type	If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 card, a 30AN300 card, a 4AN400 card, a 20P200, or a black box, and for connections in which 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 you select **None**, the remaining **Client Protection Type** parameters are not displayed.
Network Protection Type	*Optional:* If **ASON** is not selected, the **Network Protection Type** field is displayed. It is 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 cards and black boxes, **SNC-Nc** is displayed. For other protection types, the value is **None**. If you select **None**, the remaining **SNC Protection** parameters are not displayed.
Network Switch Mode	This parameter defines the network switching mode for SNC protection. The value is **Unidirectional** or **Bidirectional** for **SNC-N** protection, **Unidirectional** for **SNC-I** protection.
Network Hold Off Time(msec)	*Optional:* If **ASON** is not selected and the Network Protection type is not **SNC-Nc**, the **Network Hold Off Time (msec)** field is displayed. It is a drop-down list. Values are **0** (the default) to **100** in 20 msec increments and **100** to **10000** in 100 msec increments.
Network Protected Protection Method	*Optional:* If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 card, a 4AN400 card, 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** is not selected, the **Network Protected Protection Method** field is activated and displayed as a 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-11 PROTECTION Tab Parameters (continued)

Parameter	Description
Network Protecting Protection Method	*Optional:* If at least one connection endpoint is on an 1830 PSS OCS NE, a 30AN400 card, a 4AN400 card, 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** is not selected, the **Network Protecting Protection Method** field is activated and displayed as a 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).
ASON Sub-Network Protection Type	Controlled Plane parameter *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).
Open SNCP	Controlled Plane parameter *Optional:* If the **ASON Routed** field is selected and the **Connection Shape** is one of the supported **Bi** shapes, the **Open SNCP** check box is displayed. It is unchecked by default. Check this box if Open SNCP connection has to be created.
Soft Revertive SNCP Mode	Controlled Plane parameter *Optional:* If the **ASON** check box is selected and the **Connection Type** is one of the supported **Bi** directional 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).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

RESTORATION tab

Allows users to specify the connection behavior in the control plane domain.

The following parameters are available in the RESTORATION tab.

Table 8-12 RESTORATION Tab Parameters

Parameter	Description
ASON Tunnel	This parameter is a check box. Select the check box for the connection to be an ASON tunnel. If the box is unchecked, the connection becomes a Control/Mixed Plane connection.
L0-L1 Overlay	This parameter indicates the configuration is a L0-L1 overlay for ASON Routed connections.
Tunnel Type	This parameter indicates if the tunnel is terminated or unterminated for MRN connections.
ASON Restoration	*Optional:* This parameter is a drop-down list. • **No Restoration**: traffic is lost if a failure occurs. • **Source-based Restoration**: the Control Plane protects the traffic if a failure occurs by calculating a new route. • **Guaranteed Restoration**: the restoration path is pre-calculated.
TCM Level	This parameter 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	This parameter is a text field. You can enter the value that is needed.
Default priority	This parameter is a text field. The supported values are 1, 2, 3, 4, and 5. The default value is **4**
Default setup priority	This parameter is a text field. The supported values are 1, 2, 3, 4, and 5. The default value is **5**.
Reversion mode	This parameter is a drop-down list. Values are **Manual** (the default), **Auto** or **Soft Automatic**.
Wait for Server Restoration	This parameter is a drop-down list. Values are **Disable** (the default), **Enable**, or **Not Applicable**
Include Any Color Name	This parameter is a text box. Click the search icon to display the **Include Any Color Name** selection pane and select the appropriate color profile from the data table. The color specified must be the same color that is allocated to the link. Resource Coloring helps 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. Select different strategies to color-code their networks for ease of visibility.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-12 RESTORATION Tab Parameters (continued)

Parameter	Description
Exclude Any Color Name	This parameter is a text box. Click the search icon to display the **Exclude Any Color Name** selection pane and select the appropriate color profile from the data table to be excluded. The color must be same color that is allocated to the link. Resource Coloring helps you 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. Select different strategies to color-code their networks for ease of visibility.
Max Path Alarm Based Movements	This parameter is a text box. The default value is 0. The value range is 0-5. If value=0 the Path Alarm Based Movement by GMRE is Disabled. The field applies to L0 and MRN CP connections and not applicable to L1 CP connections. When the value is increased to > 0, **Movement Hold Off Time (in secs)** parameter is enabled. Parameter applies for a L0 CP or MRN SNC (not for a L1 CP and L2 UNI Services).
Movement Hold Off Time (in secs)	This parameter is a text box. Path Alarm Based Movements uses a configurable move-hold-off time (per LSP) during normal time . The default value is 300. The value range is between 30secs and 1h(3600secs). Default=5mins (300secs). This field is applicable only when the number of configured attempts is >0 and when fault was not present in the first 5 mins after setup and restoration. Parameter applies for a L0 CP or MRN SNC (not for a L1 CP and L2 UNI Services).

OCHP tab

The following parameters are available in the OCHP tab.

Table 8-13 OCHP Tab Parameters

Parameter	Description
OCHP Revertive Mode	*Optional:* This parameters enables the OCHP revertive mode, that is, the traffic is automatically switched back to the working circuit. Supported values are: **Enabled**, **Disabled** (default value).
Wait To Restore Time (min)	This parameter is displayed if the value of **OCHP Revertive Mode** is **Enabled**. Supported values are 1, 2, 3, .. 20. The default value is 5 minutes.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

OTHERS tab

The following parameters are available in the ROUTING tab.

Table 8-14 OTHERS Tab Parameters

Parameter	Description
Optical Impairment Routing (Experimental)	• None • Enforced • Best Effort
Rearrange	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**
Order Sensitive	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.

Summary

SUMMARY section is a collection of all the parameters available in the selected template (for example, ODUk or OTSiG Tunnel infrastructure template). This section lists all the default parameters and the set parameters. Verify all the parameters before deploying a connection.

SUGGESTED ROUTES

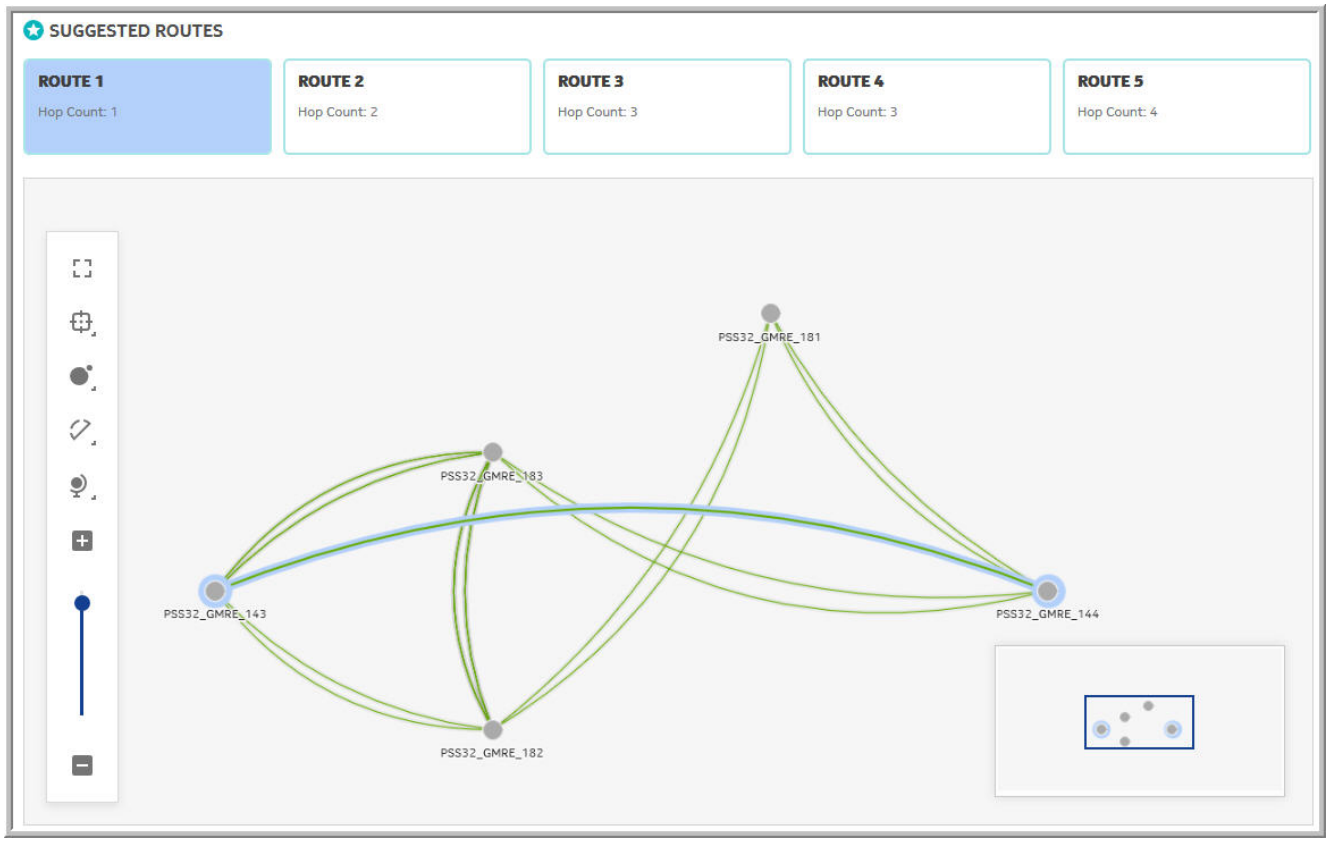
Selection of preview routes for unprotected connections

When **Routing Mode** is set to `Automatic`, the **SUGGESTED ROUTES** section displays possible routes that can be deployed for a connection (only if there are no routing constraints selected). With a minimum of one to maximum of five routes namely *ROUTE 1* to *ROUTE 5*. These routes are also displayed in a map.

Click on a tile *ROUTE #* to select a route.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-3 SUGGESTED ROUTES section for Unprotected Connections



Selection of preview routes for protected connections

For OPSA/OPSB, the number of routes can be a maximum of five pairs. `Working Route` and `Protected Route` are assigned their roles by default by NFM-T.

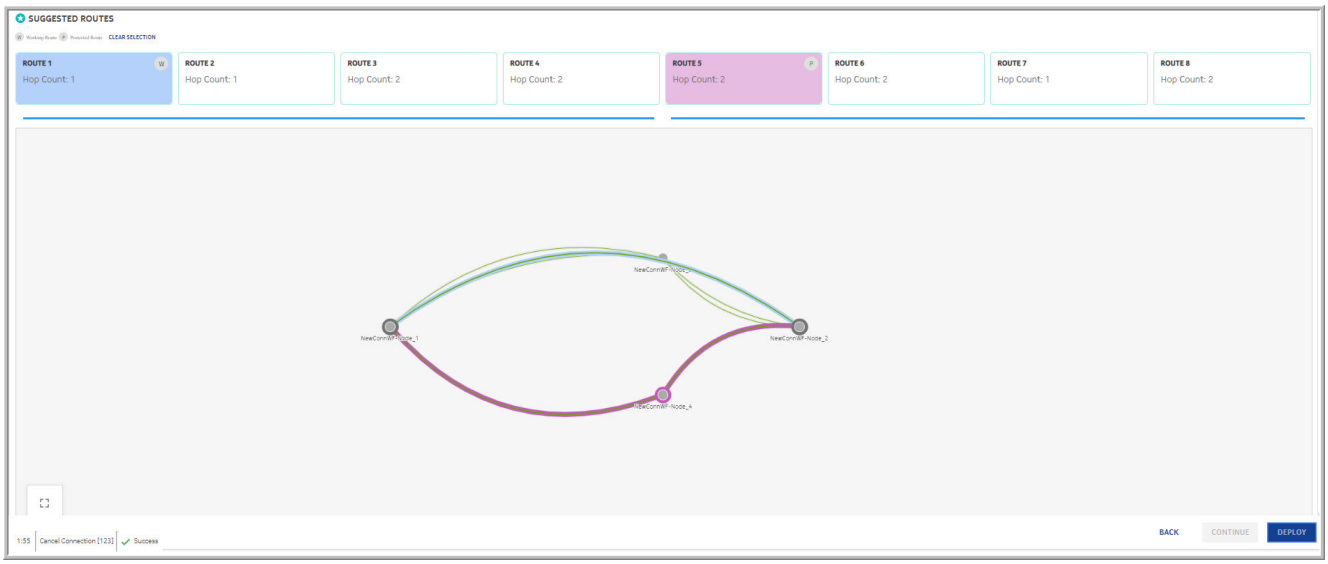
The `Working Route` tile is tagged with the letter **W** and has blue color fill, select the `Working Route` tile to view the route in the map, the route is highlighted in blue color.

The `Protected Route` tile is tagged with the letter **P** and has magenta color fill, select the `Protected Route` tile to view the route in the map, the route is highlighted in magenta color.

If more than one `Working Route` or `Protected Route` have been calculated, they are shown as separate tiles on the route preview screen.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-4 SUGGESTED ROUTES section for Protected Connections



To change the assignment of *Working Route* and *Protected Route*, the working and protection roles are assigned as follows:

1. *Working Route* is **ROUTE 1**, *Protected Route* is **ROUTE 2**. Click on any other route and it becomes the new *Protected Route*, replacing the default.
2. To replace both the *Working Route* and *Protected Route*, click on **CLEAR SELECTION**.
3. Automatically the first route clicked becomes *Working Route*, and the second route clicked becomes *Protected Route*.

For OPSA and OPSB, there are hardware constraints that limit the selection of *Working Route* and *Protected Route* pairs. In this case, routes are displayed in two groups. Each group of route tiles is underlined. One route from each group can be selected to make a valid working/protection pair.

The default route is the first route in the left group which is a *Working Route*. The default route is that the first route in the right group which is a *Protected Route*.

To change the protection route, click on any route tile in the right group. To change both the working and protection routes, click on **CLEAR SELECTION**.

The first route selected from any group becomes the *Working Route*. Then select from the other group to assign the *Protected Route*.

Note:

- Selecting a route on the map view, does not highlight the same route on the tile view, as the same span may be part of multiple routes.
- In some cases there may be only one *Working Route* or *Protected Route* found. Up to a maximum of five routes for working and protection are displayed. If no route is found,

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

the message *No Route Available. System could not find a route between <From Node #1> and <To Node #1>* is displayed in the **SUGGESTED ROUTES** pane.

Deploy

DEPLOY section displays the status of the provisioning task. The deployment status is represented in a progress bar which increases in percentage as the deployment moves states from **Defined** > **Allocated** > **Implemented** > **Commissioned**.

Different states of deployment:

- **Defined**: the termination points are defined.
- **Allocated**: the route is allocated.
- **Implemented**: the trail is implemented into the network element.
- **Commissioned**: the client and link connections are created.

A successful deployment, turns all the states in green color and a success message is displayed.

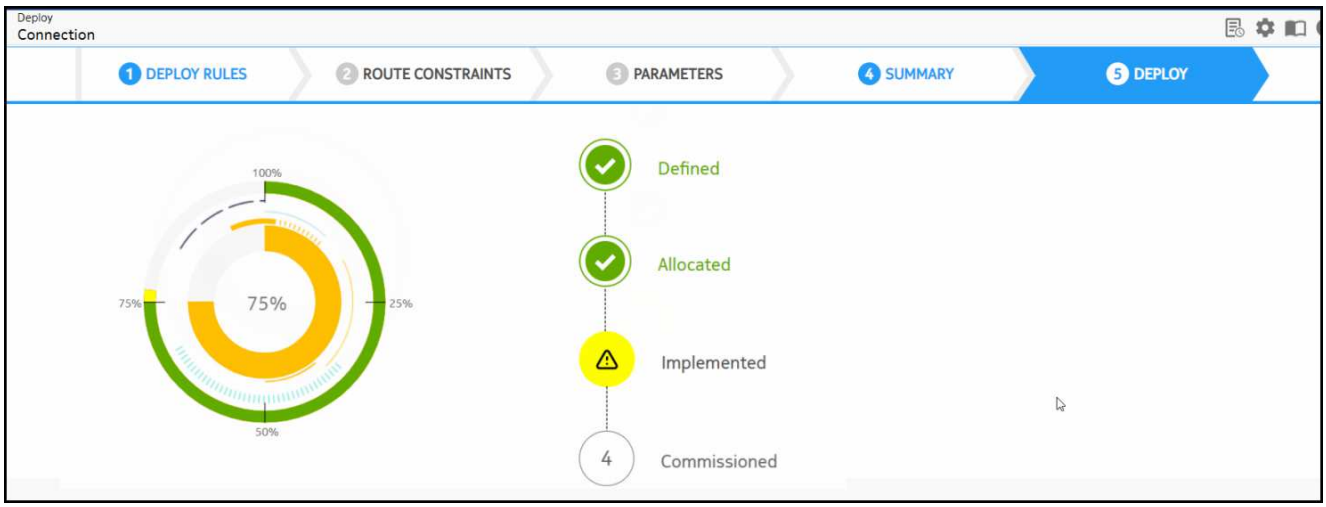
To view the new connection, click on **SHOW NEW CONNECTION(S)** or click **BIDIRECTIONAL OPTICAL POWER** to view the Optical Power page. You can also view the new connection from **OPERATE > Infrastructure Connections** page or **ADMINISTER > Jobs** page.

If there is a failure during deployment, the progress bar and the state at which the deployment failed turns red. An error message is displayed.

To view the error, click on **SHOW FAILED CONNECTION(S)**. You can also view the error from **ADMINISTER > All Records**. At this point you can also cancel the connection, click **CANCEL CONNECTION**.

When a timeout occurs, the service does not successfully move to commissioned state. A yellow warning symbol is displayed at the failed state as depicted in the Figure 8-5, “Deployment Timeout Warning” (p. 1266), and the corresponding error is displayed below it.

Figure 8-5 Deployment Timeout Warning



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Profile and Supported Cards

The following table provides the mapping between the profile and supported cards.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-15 Profile and Card Mapping

Profile Number	S2AD200	S4X400H	S4X400L	DFC12/ DFC12E	DFM6/ DFM6E	DD2M4	4UC1T	8UC1T	S5AD400H	SFM6/ S6AD600H	2UX500	2UX200	4UC400
1	NA	Yes	NA	Yes	NA	NA	NA	NA	NA	NA	NA	NA	NA
2	NA	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	NA	Yes	NA	NA
3	NA	Yes	Yes	Yes	NA	NA	NA	NA	NA	NA	NA	NA	NA
4	NA	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	NA	Yes	NA	NA
5	NA	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes	NA	Yes	NA	NA
7	Yes	NA	NA	NA	NA	NA	NA	Yes (MP)	NA	NA	NA	Yes	Yes
8	NA	Yes	Yes	Yes	NA	NA	NA	NA	NA	NA	NA	NA	NA
9	Yes	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA	Yes	NA
10	Yes	NA	NA	NA	NA	NA	NA	Yes (MP)	NA	NA	NA	Yes	NA
11	Yes	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA	Yes	NA
12	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA	Yes	NA	NA
15	NA	Yes	Yes	Yes	Yes	NA	NA	NA	NA	NA	NA	NA	NA
16	NA	NA	NA	Yes	NA	NA	NA	NA	NA	NA	NA	NA	NA
19	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
20	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA
21	NA	NA	NA	NA	NA	Yes	Yes	NA	Yes	NA	Yes	NA	NA
26	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA
27	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA
28	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA
29	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA
31	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA	NA	Yes
32	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA
33	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-15 Profile and Card Mapping (continued)

Profile Number	S2AD200	S4X400H	S4X400L	DFC12/ DFC12E	DFM6/ DFM6E	DD2M4	4UC1T	8UC1T	S5AD400H	SFM6/ S6AD600H	2UX500	2UX200	4UC400
34	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA
38	NA	NA	NA	NA	NA	NA	NA	NA	NA	Yes	NA	NA	NA

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note

1. Profile # 20 is supported only in the Managed plane for the 2UX500 card. Profile #20 is not supported by GMRE for the 2UX500 card.
2. Profile # 16 is supported only in the Managed plane for the DFC12E card. Profile #16 is not supported by GMRE for the DFC12E card.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.5 Deploy a Managed Plane Connection

Before you begin

Before you deploy a connection, ensure:

- From the Nodes page, the nodes or the network elements are `Supervised` and synchronized to `Normal` state.
- From the Equipment Manager page:
  - Configure the ports of the nodes with required signal rates.
  - Create internal links within the node and between the node as required.

Purpose

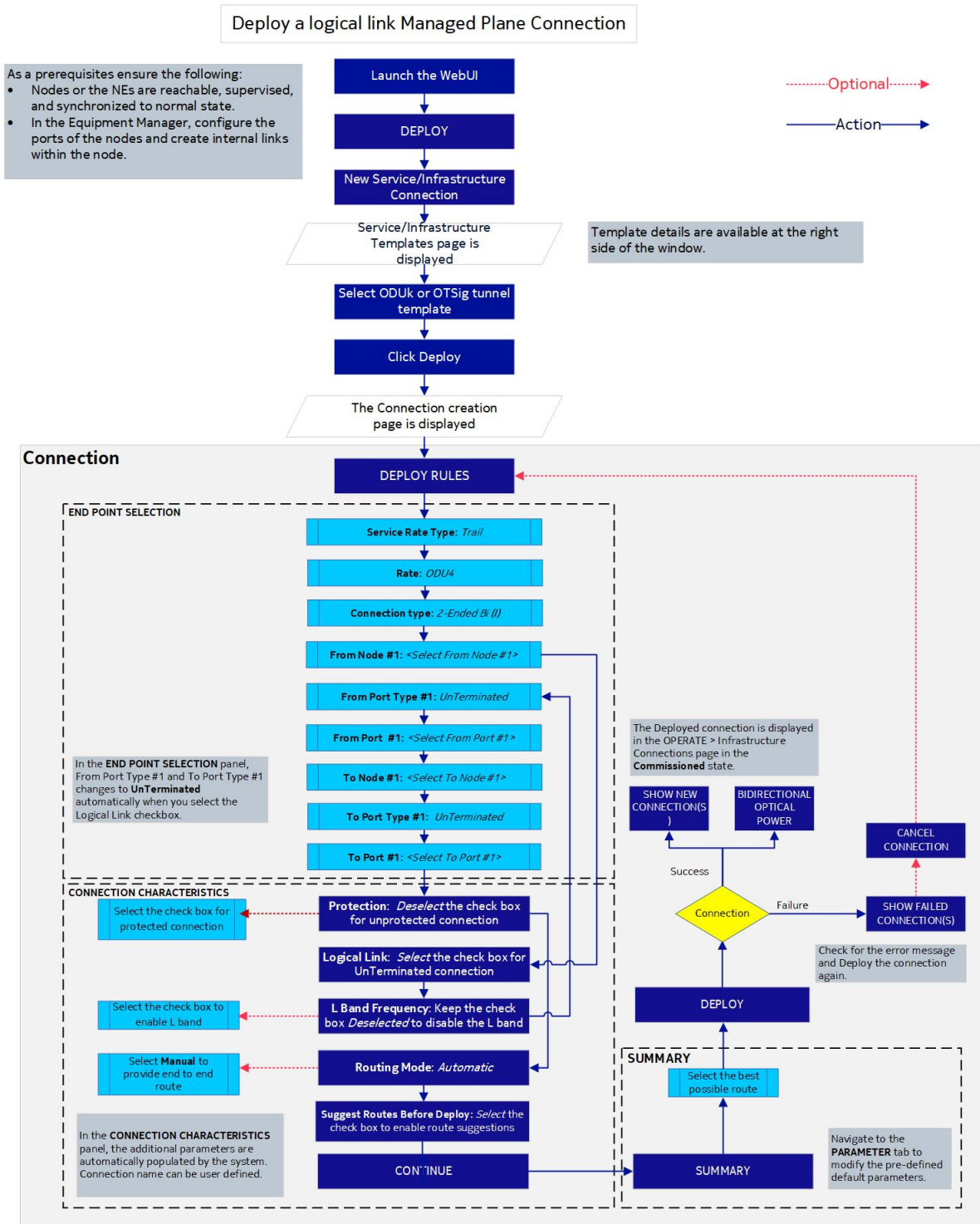
To deploy a Managed Plane logical link connection.

Workflow

This workflow covers the deployment scenario of a Managed Plane Logical Link Connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-6 Deployment of a Managed Plane Logical Link Connection



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task

1

From the WebUI, 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.

4

From the **END POINT SELECTION** panel:

1. The **Service Rate Type** parameter is automatically set to `Trail`.

   This depends on the type of template selected.
2. Select **Rate** as `ODU4`.

   Depending on the selected signal rate, configuration of other parameters may vary.
3. Select **Connection Type** as `2-Ended Bi (I)`

   Depending on the connection type selected, additional *From Node* and *To Node* fields are displayed.
4. Select **From Node #1** and **To Node #1**.

   Select the nodes and ports for deployment by clicking the search icon and selecting the node or port from the list displayed in the lower pane. Or type the node or port name in the text box if you know which node or port to be used.
5. Select **From Port Type #1** and **To Port Type #1** as `UnTerminated`.

   Note: For cards like D5X500, select the **Logical Link** parameter check box from **CONNECTIONS CHARACTERISTICS** pane and the system automatically sets the **From Port Type #1** and **To Port Type #1** to `UnTerminated` and then continue to the next step.
6. Select **From Port #1** which is the A-end of the connection and **To Port #1** which is the Z-end of the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

From the **CONNECTION CHARACTERISTICS** panel.

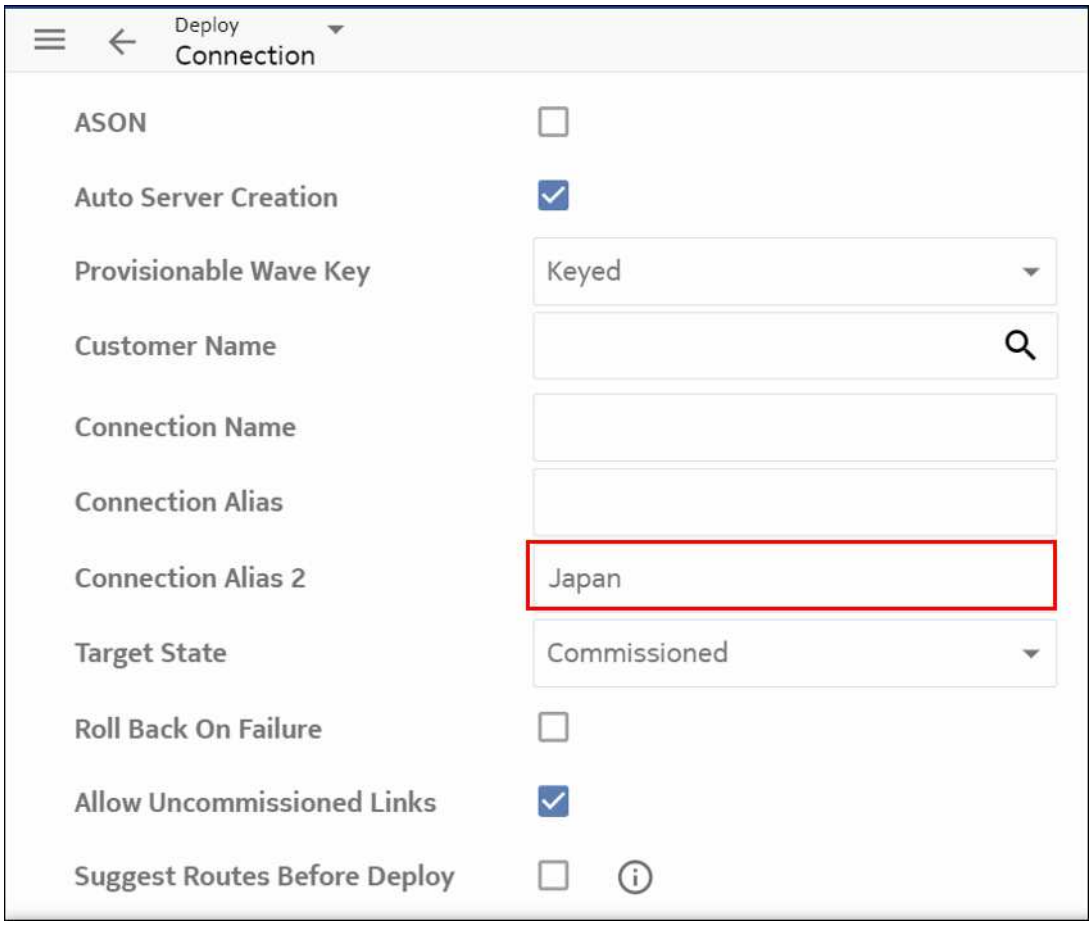
- Select **Logical Link** check box.
- Select **Suggest Routes Before Deploy** check box, for the system to display possible routes under **SUGGESTED ROUTES** pane of the **SUMMARY** section.

Continue with the default values for the following parameters:

- **Protection**
- **L-Band Frequency**
- **Routing Mode**
- **Allow ASON Resources**
- **ASON**
- **Auto Server Creation**
- **Provisionable Wave Key**
- **Customer Name**
  Optional: Enter a Customer name or click the search icon to select a name from the *Customer Name* list.
- **Connection Name**
  Optional: Enter a connection name or the system auto populates the name of the connection using the values of **From Node #1** and **To Node #1**.
- **Connection Alias**
  Optional: Enter a connection alias as an identification to the connection, for example, the complete path taken by the connection until the To-Node.
- **Connection Alias 2**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Optional: Enter a connection alias 2 as an identification to the connection.



- **Target State**
- **Roll Back On Failure**
- **Allow Uncommissioned Links**

Note: Depending on the type of connection created and the **Rate** selected, additional tabs are displayed.
For more information on these parameters, see "Deploy Rules" (p. 1220) and "CONNECTION CHARACTERISTICS tab" (p. 1223).

6

Click **CONTINUE**.

Result: SUMMARY section is displayed.

Note: As the **Routing Mode** is set to `Automatic` the system directly goes to the **SUMMARY** tab.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

You can click **BACK** button to go back to the previous tab or click on any of the tabs to verify the settings on the other parameters.

7

Select a route from the **SUGGESTED ROUTES** pane of the **SUMMARY** section, to provision the connection.

For more information, see "Summary" (p. 1263).

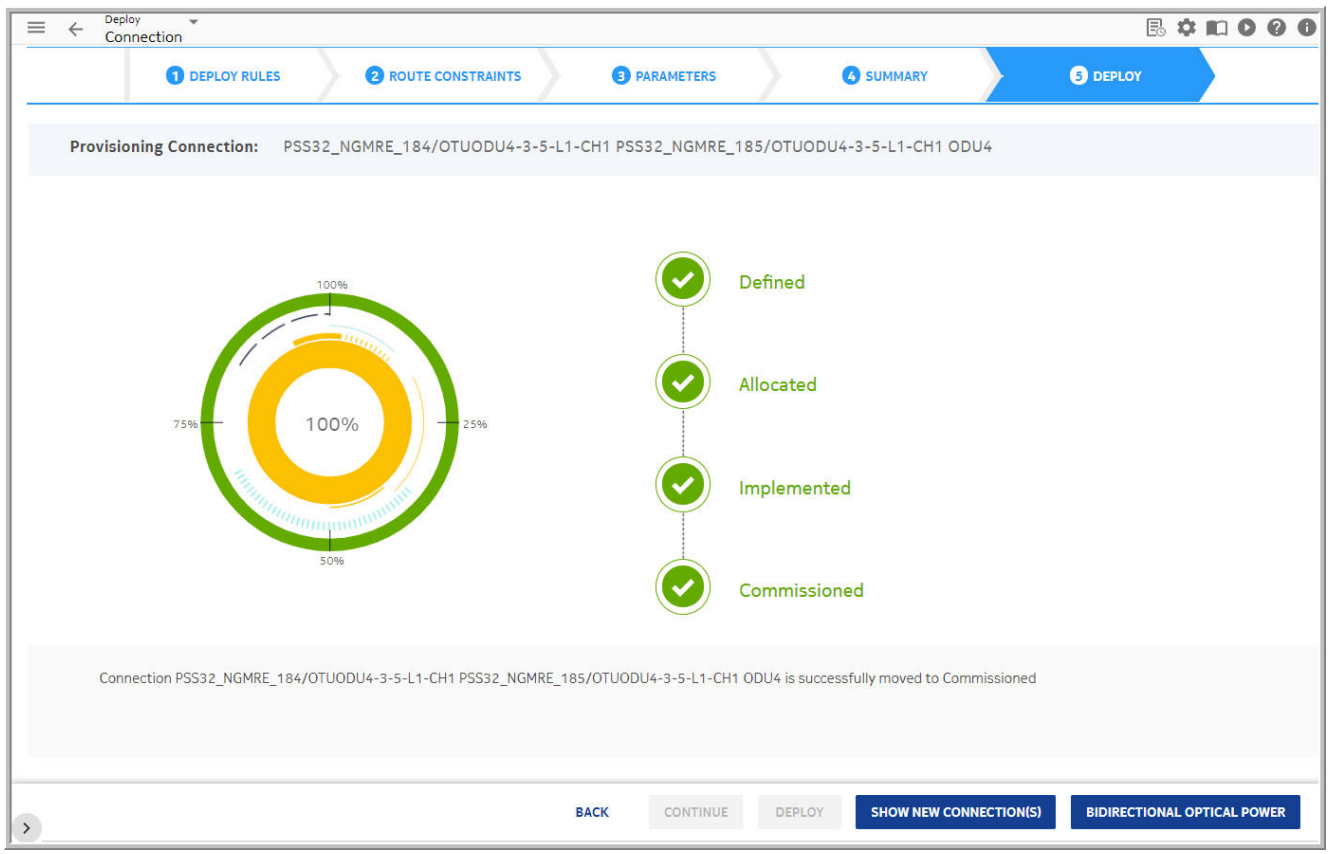
8

Click **DEPLOY**.

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.

Figure 8-7 Success Message for a Managed Plane Logical Link Connection



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9

Optional:

Click **SHOW NEW CONNECTION(S)** to view the new connection.

Note:

- When an ODUk connection is created, *SHOW NEW CONNECTION(S)* page displays the newly created ODUk and OTUk connections.
- When an OTSiG Tunnel is created, *SHOW NEW CONNECTION(S)* page displays only the newly created OTSiG Tunnel and not the OTSiG Trail.

Or

Click **BIDIRECTIONAL OPTICAL POWER** to view the Optical Power page.

10

Optional:

- Click **SHOW FAILED CONNECTION(S)** to view the deployed connection.
- You can also view the connection from **OPERATE > Infrastructure Connections** page.

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 an error message is displayed.

- Click **SHOW FAILED CONNECTION(S)** to view the failed connection.
- To view the log and status of the connection, navigate to **ADMINISTER > Jobs** or **ADMINISTER > All Records** page.
- To cancel the failed connection, click **CANCEL CONNECTION**. Rectify the error and try to deploy the connection again.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.6 Deploy an L0 Control Plane Connection

Before you begin

Before you deploy a connection, ensure:

- From the Nodes page, the nodes or the network elements are `Supervised` and synchronized to `Normal` state.
- From the Equipment Manager page:
  - Configure the ports of the nodes with required signal rates.
  - Create internal links within the node and between the node as required.
- Check if NEs are GMRE configured in L0 Control Plane domain.
- Check if Optical Multiplex Section (OMS) link is available.
  1. If OMS link is not available, create an OTS physical connection to generate an OMS link.
  2. Create NPA from the **OPERATE > NPAs** page.
  3. Add OMS Links to the NPA. Links are added in the `Locked` state.
  4. Unlock the links that are added to ASON. The ASON **Administrative State** of the link changes to `Unlocked`.

Purpose

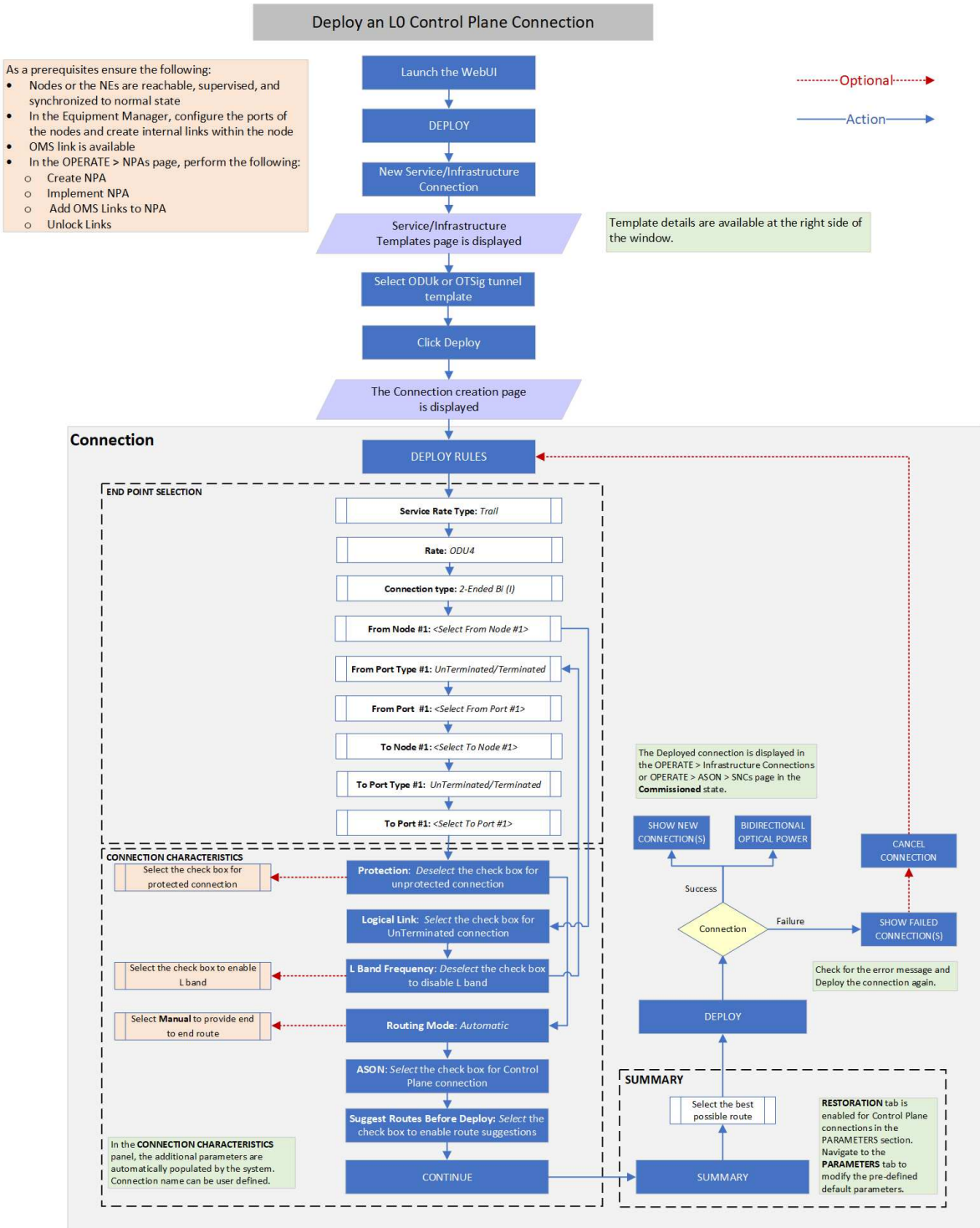
To deploy an L0 Control Plane connection.

Workflow

This workflow covers the deployment scenario of a Control Plane Connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-8 Deployment of an L0 Control Plane Connection



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task

1

From the WebUI, 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 for L0 Restoration* 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.

4

From the **END POINT SELECTION** panel:

1. The **Service Rate Type** parameter is automatically set to `Trail`.

   This depends on the type of template selected.
2. Select **Rate** as `ODU4`.

   Depending on the selected signal rate, configuration of other parameters may vary.
3. Select **Connection Type** as `2-Ended Bi (I)`

   Depending on the connection type selected, additional *From Node* and *To Port Type* fields are displayed.
4. Select **From Node #1** and **To Node #1** parameters.

   Select the nodes and ports for deployment by clicking the search icon and selecting the node or port from the list displayed in the lower pane. Or type the node or port name in the text box if you know which node or port to be used.
5. Select **From Port Type #1** and **To Port Type #1** as `UnTerminated` for logical link connections.

   Note: For cards like D5X500, select the **Logical Link** parameter check box from **CONNECTIONS CHARACTERISTICS** pane and the system automatically sets the **From Port Type #1** and **To Port Type #1** to `UnTerminated` and then continue to the next step.
6. Select **From Port #1** which is the A-end of the connection and **To Port #1** which is the Z-end of the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

From the **CONNECTION CHARACTERISTICS** panel.

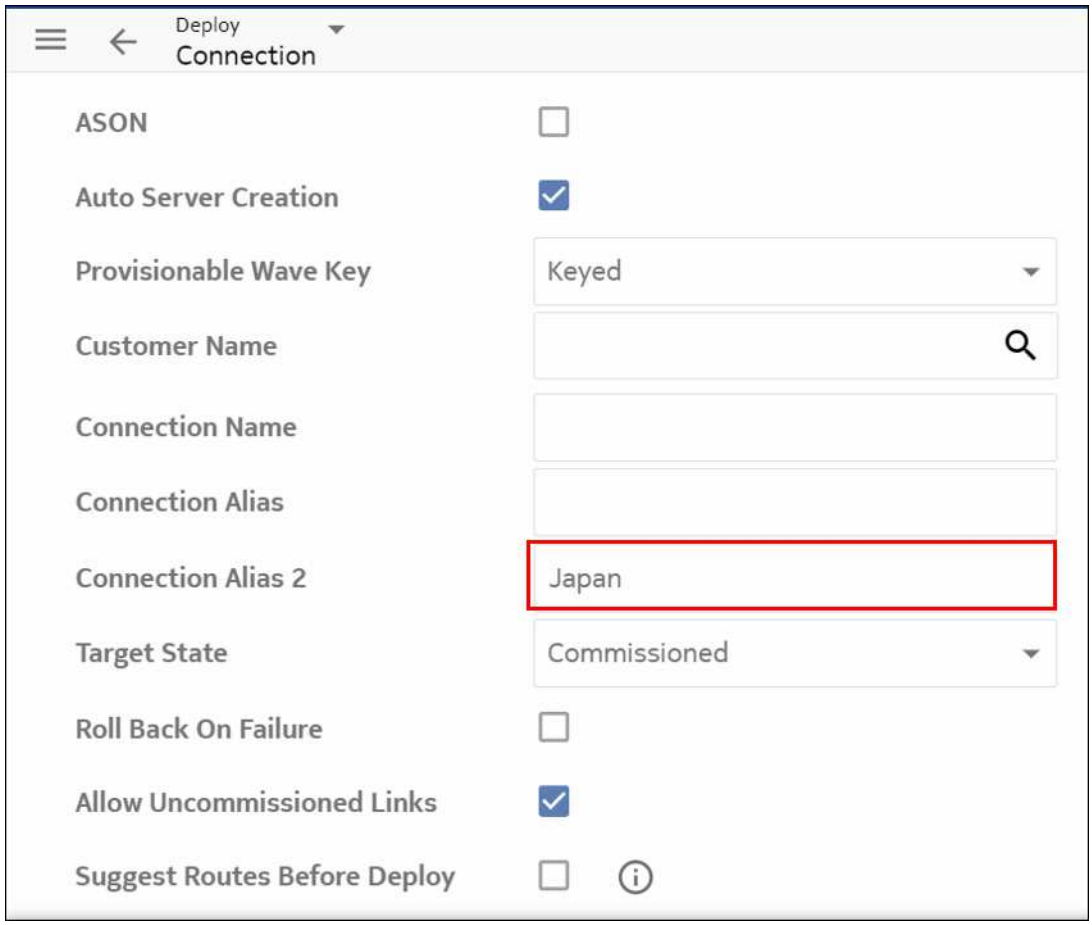
- Select **Logical Link** check box.
- Select **Suggest Routes Before Deploy** check box, for the system to display possible routes under **SUGGESTED ROUTES** pane of the **SUMMARY** section.

Continue with the default values for the following parameters:

- **Protection**
- **L-Band Frequency**
- **Routing Mode**
- **Allow ASON Resources**
- **ASON**
- **Auto Server Creation**
- **Provisionable Wave Key**
- **Customer Name**
  Optional: Enter a Customer name or click the search icon to select a name from the *Customer Name* list.
- **Connection Name**
  Optional: Enter a connection name or the system auto populates the name of the connection using the values of **From Node #1** and **To Node #1**.
- **Connection Alias**
  Optional: Enter a connection alias as an identification to the connection, for example, the complete path taken by the connection until the To-Node.
- **Connection Alias 2**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Optional: Enter a connection alias 2 as an identification to the connection.



- **Target State**
- **Roll Back On Failure**
- **Allow Uncommissioned Links**
- **Suggest Routes Before Deploy**

Note:

- Depending on the type of connection created and the **Rate** selected, additional tabs are displayed.
  For more information on these parameters, see "Deploy Rules" (p. 1220) and "CONNECTION CHARACTERISTICS tab" (p. 1223).
- For a Protected Control Plane connection, with **ASON** enabled, the parameter **OCHP Revertive Mode** is not applicable. Even though *OCHP Revertive Mode (PARAMETERS > OCHP > OCHP Revertive Mode)* is set to **Enable**, this option is not enabled on the NE.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- For a Protected Mixed Plane connection (Managed Plane + Control Plane), with **ASON** enabled, the parameter **OCHP Revertive Mode** can be set to *Enable*, as the Managed Plane supports OCHP.

6

Click **CONTINUE**.

Result: SUMMARY section is displayed.

Note: As the **Routing Mode** is set to `Automatic` the system directly goes to the **SUMMARY** tab.
You can click **BACK** button to go back to the previous tab or click on any of the tabs to verify the settings on the other parameters.

7

Select a route from the **SUGGESTED ROUTES** pane of the **SUMMARY** section, to provision the connection.

For more information, see "Summary" (p. 1263).

8

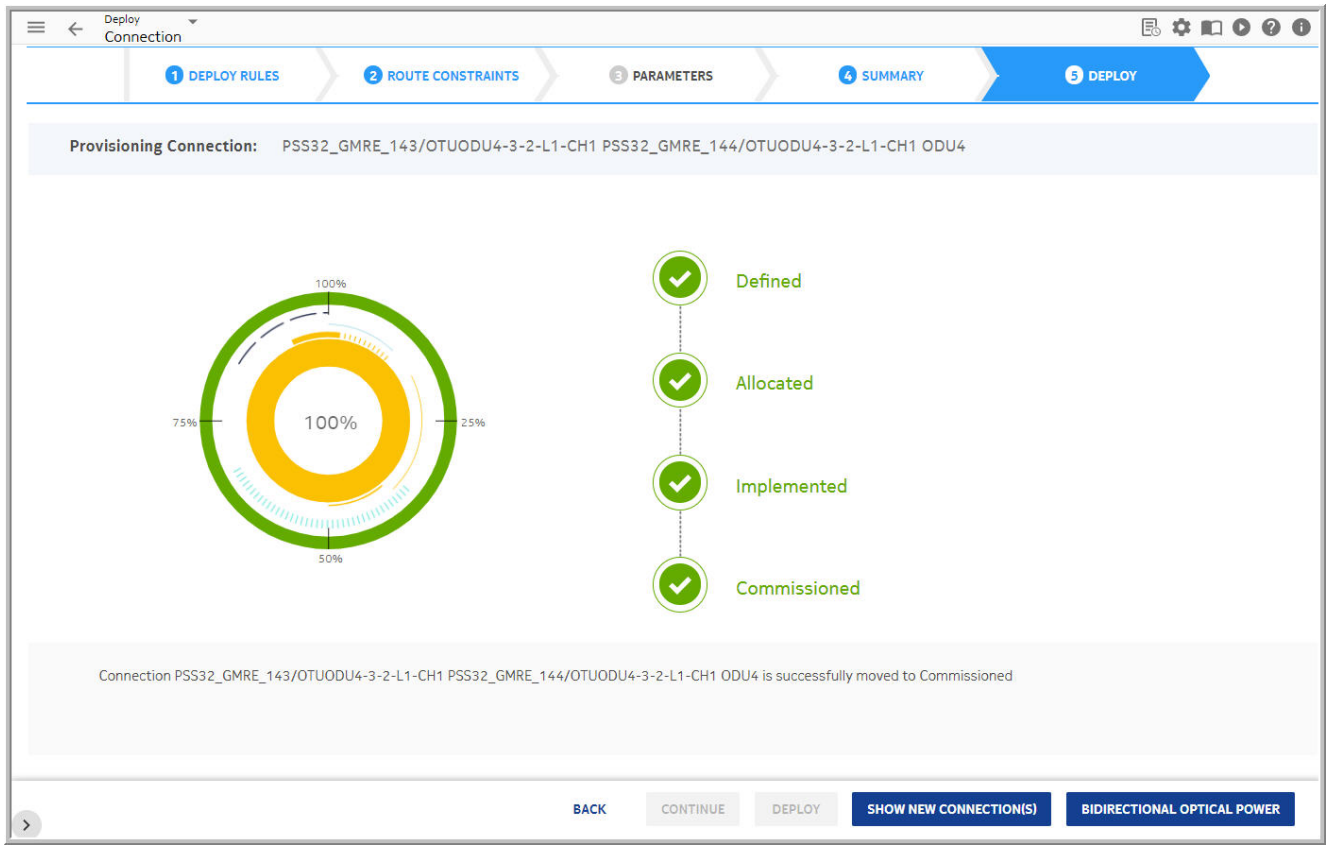
Click **DEPLOY**.

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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-9 Success Message for an L0 Control Plane Connection



9

Optional:

Click **SHOW NEW CONNECTION(S)** to view the new connection.

Note:

- When an ODUk connection is created, *SHOW NEW CONNECTION(S)* page displays the newly created ODUk and OTUk connections.
- When an OTSiG Tunnel is created, *SHOW NEW CONNECTION(S)* page displays only the newly created OTSiG Tunnel and not the OTSiG Trail.

Or

Click **BIDIRECTIONAL OPTICAL POWER** to view the Optical Power page.

10

Optional:

- Click **SHOW FAILED CONNECTION(S)** to view the deployed connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- You can also view the connection from **OPERATE > Infrastructure Connections** page.

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 an error message is displayed.

- Click **SHOW FAILED CONNECTION(S)** to view the failed connection.
- To view the log and status of the connection, navigate to **ADMINISTER > Jobs** or **ADMINISTER > All Records** page.
- To cancel the failed connection, click **CANCEL CONNECTION**. Rectify the error and try to deploy the connection again.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.7 Deploy a Connection with Routing Constraints

Before you begin

Before you deploy a connection, ensure:

- From the Nodes page, the nodes or the network elements are `Supervised` and synchronized to `Normal` state.
- From the Equipment Manager page:
  - Configure the ports of the nodes with required signal rates.
  - Create internal links within the node and between the node as required.
- Check if NEs are GMRE configured in L0 Control Plane domain.
- Check if Optical Multiplex Section (OMS) link is available.
  1. If OMS link is not available, create an OTS physical connection to generate an OMS link.
  2. Create NPA from the **OPERATE > NPAs** page.
  3. Add OMS Links to the NPA. Links are added in the `Locked` state.
  4. Unlock the links that are added to ASON. The ASON **Administrative State** of the link changes to `Unlocked`.

Purpose

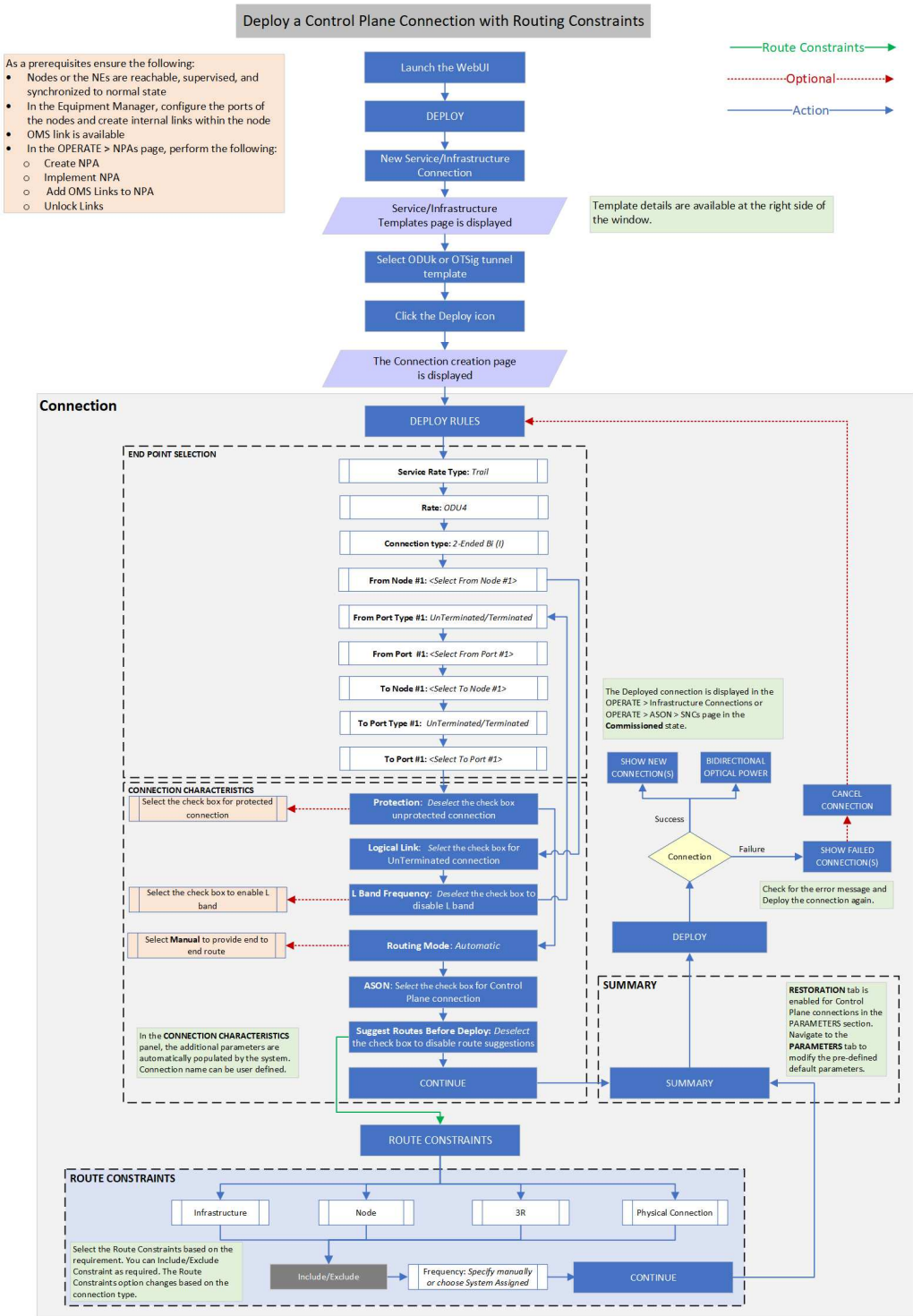
To deploy a connection with routing constraints.

Workflow

This workflow covers the deployment scenario of a connection with routing constraints.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-10 Deployment of a Connection with Routing Constraints



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task

1

From the WebUI, 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 for L0 Restoration* 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.

4

From the END POINT SELECTION panel:

1. The **Service Rate Type** parameter is automatically set to `Trail`.

   This depends on the type of template selected.
2. Select **Rate** as `ODU4`.

   Depending on the selected signal rate, configuration of other parameters may vary.
3. Select **Connection Type** as `2-Ended Bi (I)`

   Depending on the connection type selected, additional *From Node* and *To Port Type* fields are displayed.
4. Select **From Node #1** and **To Node #1**.

   Select the nodes and ports for deployment by clicking the search icon and selecting the node or port from the list displayed in the lower pane. Or type the node or port name in the text box if you know which node or port to be used.
5. Select **From Port Type #1** and **To Port Type #1** as `UnTerminated`.

   Note: For cards like D5X500, select the **Logical Link** parameter check box from **CONNECTIONS CHARACTERISTICS** pane and the system automatically sets the **From Port Type #1** and **To Port Type #1** to `UnTerminated` and then continue to the next step.
6. Select **From Port #1** which is the A-end of the connection and **To Port #1** which is the Z-end of the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

From the **CONNECTION CHARACTERISTICS** panel:

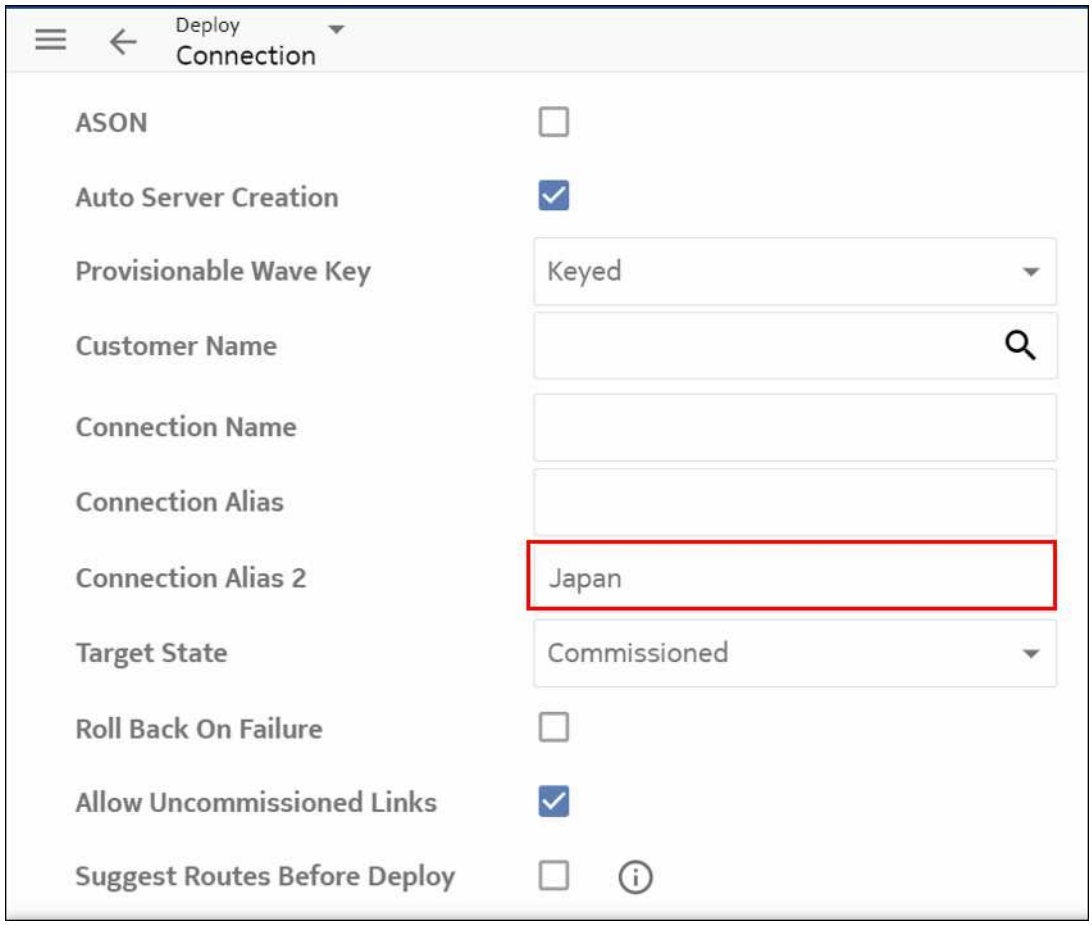
- Select **Logical Link** check box.
- Select **Routing Mode** as `Manual`, to specify all the constraints for an end-to-end connection.

Continue with the default values for the following parameters:

- **Protection**
- **L-Band Frequency**
- **Allow ASON Resources**
- **ASON**
- **Auto Server Creation**
- **Provisionable Wave Key**
- **Customer Name**
  Optional: Enter a Customer name or click the search icon to select a name from the *Customer Name* list.
- **Connection Name**
  Optional: Enter a connection name or the system auto populates the name of the connection using the values of **From Node #1** and **To Node #1**.
- **Connection Alias**
  Optional: Enter a connection alias as an identification to the connection, for example, the complete path taken by the connection until the To-Node.
- **Connection Alias 2**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Optional: Enter a connection alias 2 as an identification to the connection.



- **Target State**
- **Roll Back On Failure**
- **Allow Uncommissioned Links**
- **Suggest Routes Before Deploy**

Note: Depending on the type of connection created and the **Rate** selected, additional tabs are displayed. For more information on these parameters, see "Deploy Rules" (p. 1220) and "CONNECTION CHARACTERISTICS tab" (p. 1223).

6

Click **CONTINUE**.

Result: ROUTING CONSTRAINTS section is displayed. For more information, see "Route Constraints" (p. 1244).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7

From the Infrastructure tab:

1. Ensure the **Near End Node** value which is the A-end node of the connection is correct.
2. Select **Fully Specified** check box to automatically populate the near end node for selecting constraints.
3. Select a *Far End node* from the **Infrastructure Connections** section.

   Links associated with that node are listed in the **Link Connections** pane.
4. Select **INCLUDE** to specify the full end-to-end connection or partial connection and let the system select the remaining parts. The link is populated in the lower pane. You can include multiple links.

   Note: When **Routing Mode** is set to `Manual`, only **Include** option is available. **Exclude** option is not available.

8

Optional:

Select one of the following options:

- **PROTECTION**: Change the constraints as protected.
- **REMOVE**: To remove the routing constraints.

9

Click **CONTINUE**.

Result: SUMMARY section is displayed. For more information, see "Summary" (p. 1263)

10

Optional: Verify all the parameters set in the different sections.

11

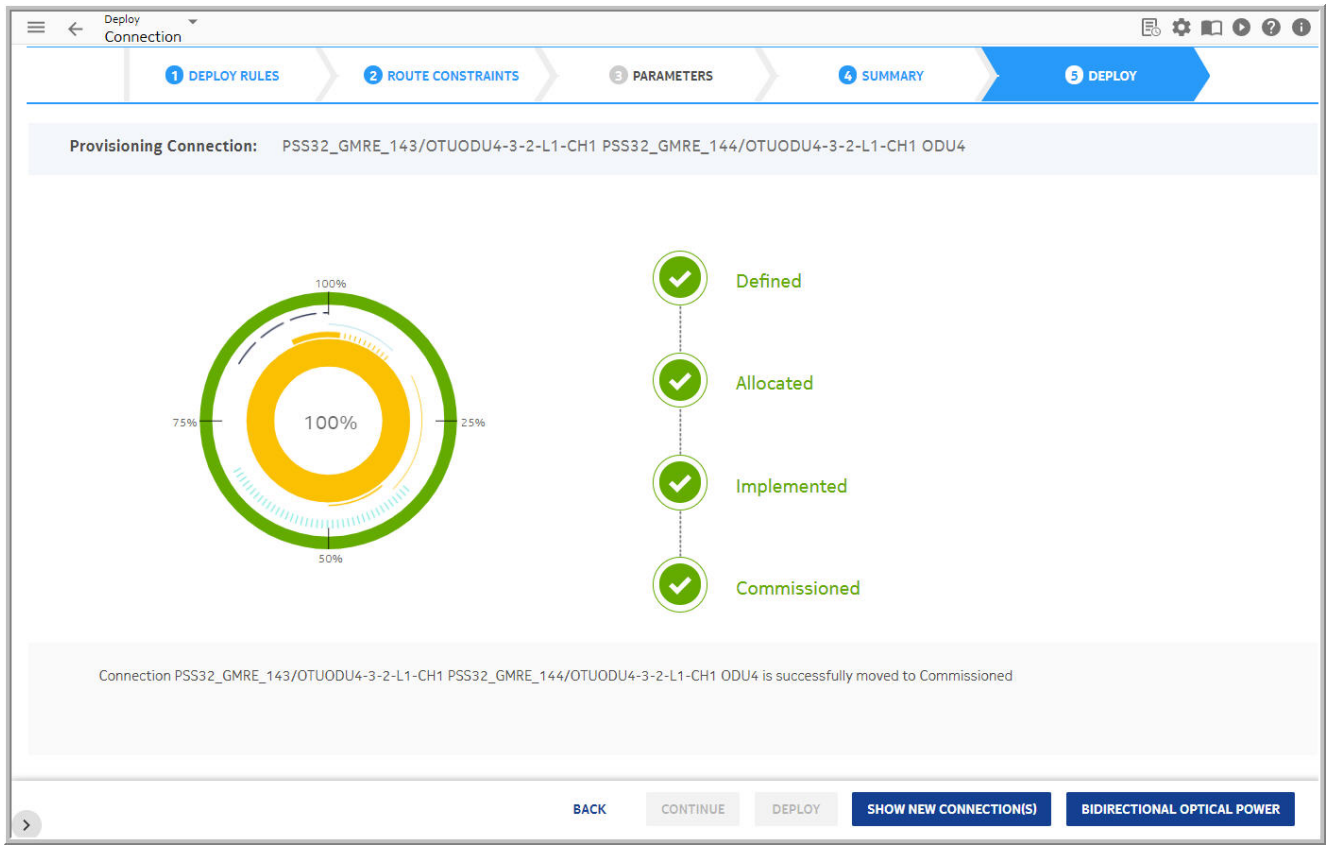
Click **DEPLOY**.

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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-11 Success Message for Connection with Routing Constraints



12

Optional:

Click **SHOW NEW CONNECTION(S)** to view the new connection.

Note:

- When an ODUk connection is created, *SHOW NEW CONNECTION(S)* page displays the newly created ODUk and OTUk connections.
- When an OTSiG Tunnel is created, *SHOW NEW CONNECTION(S)* page displays only the newly created OTSiG Tunnel and not the OTSiG Trail.

Or

Click **BIDIRECTIONAL OPTICAL POWER** to view the Optical Power page.

13

Optional:

- Click **SHOW FAILED CONNECTION(S)** to view the deployed connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- You can also view the connection from **OPERATE > Infrastructure Connections** page.

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 an error message is displayed.

- Click **SHOW FAILED CONNECTION(S)** to view the failed connection.
- To view the log and status of the connection, navigate to **ADMINISTER > Jobs** or **ADMINISTER > All Records** page.
- To cancel the failed connection, click **CANCEL CONNECTION**. Rectify the error and try to deploy the connection again.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.8 Deploy a Service

Before you begin

Before you deploy a service, ensure:

- From the Nodes page, the nodes or the network elements are `Supervised` and synchronized to `Normal` state.
- From the Equipment Manager page:
  - Configure the ports of the nodes with required signal rates.
  - Create internal links within the node and between the node as required.
- Ensure Infrastructure Connections are created.

  Note: 400 GbE service is supported only on an OTSiG tunnel created using DFM6, DFM6E, SFM6, S5AD400H, S6AD600H and DD2M4 cards.

  For DD2M4, ensure to create 100 GbE/OTU4 service for ODU4 connection. Similarly create 400 GbE service for ODUC4 connection.

  For DD2M4, the following restrictions apply for PSIM NE - 5.2 version:
  - 100 GbE/ODU4 Service on DD2M4

    C1, C2, C3 and C4 ports Service will be routed from L1 port
  - 400 GbE Service on DD2M4

    C2 port Service will be routed from L1 port and C4 port Service will be routed from L2 port

  For S5AD400H card, ensure the following
  - create 100 GbE service for ODU4 connection
  - create 400 GbE service for ODUC4 connection
  - create OTU4 NNI service for ODU4 connection

  For S6AD600H and SFM6 card, ensure the following :
  - Create 100 GbE service for ODUTC1, ODU4 connection.
  - Create 400 GbE service for ODUTC4 and ODUFlex connection.
  - Create OTU4 NNI Service for ODU4 connection.

Purpose

To deploy a service.

Task: Create an Ethernet service

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 an Ethernet service template as required. For example: *100G*.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

To create a 400G service, select a *400G* template.

Result: Default parameters of the 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.

4

From the **END POINT SELECTION** panel:

1. The **Service Rate Type** parameter is automatically is set based on the type of template selected. Example: `100G Ethernet`.
2. The **Rate** parameter is automatically set based on the type of template selected. Example: `100 GbE`.

   Depending on the selected signal rate, configuration of other parameters may vary.
3. Select **Connection Type** as `2-Ended Bi (I)`

   Depending on the connection type selected, additional node name and port name fields are displayed.
4. Select **From Node #1** and **To Node #1**.

   Select the nodes and ports for deployment by clicking the search icon and selecting the node or port from the list displayed in the lower pane. Or type the node or port name in the text box if you know which node or port to be used.
5. Select **From Port Type #1** and **To Port Type #1** as `Terminated`.
6. Select **From Port #1** which is the A-end of the connection and **To Port #1** which is the Z-end of the connection.

   Note:
   - In NFM-T R20.11, for a 400 GbE service, only C1 and C2 ports of the DFM6 or DFM6E are supported.
   - In NFM-T R21.4, for 400 GbE service, C5 ports of S5AD400H card must be used.
   - In R21.12, the DD2M4 card hosts four client ports (C1 to C4). C2 and C4 ports support all three rates (100 GbE, 400 GbE, and OTU4) whereas C1 and C3 ports support 100G/OTU4. If both C2 and C4 are equipped with 400 GbE, C1 and C3 ports cannot be used. If C1 is used for 100G/OTU4, then C2 (400G) cannot be used. If 100G/OTU4 is used on C1 and C2, then C4 (400G) cannot be used. If 100G/OTU4 is used on C3 and C4, then C2 (400G) cannot be used.
   - In R21.12, the S6AD600H and SFM6 card hosts six client ports and one line port (L1). The maximum capacity of S6AD600H and SFM6 card is 600 GbE.

     For a 400 GbE service, only the client port C6 must be used. When C6 port is used for 400 GbE, only ports C1 and C2 can be used for 100 GbE each, and not ports C3, C4, or C5.
   - In R21.12 the 2UX500 card hosts 2 line ports with shelf ID=1; slot ID=[1,2]. The maximum payload capacity of each line port is up to 400Gb/s. The capacity of the two-line ports

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

towards the backplane is up to 500 Gb/s in the single port group which supports ports 1 and 2. The 2UX500 card is applicable for 1830 PSS-8x and 1830 PSS-12x shelves.

5

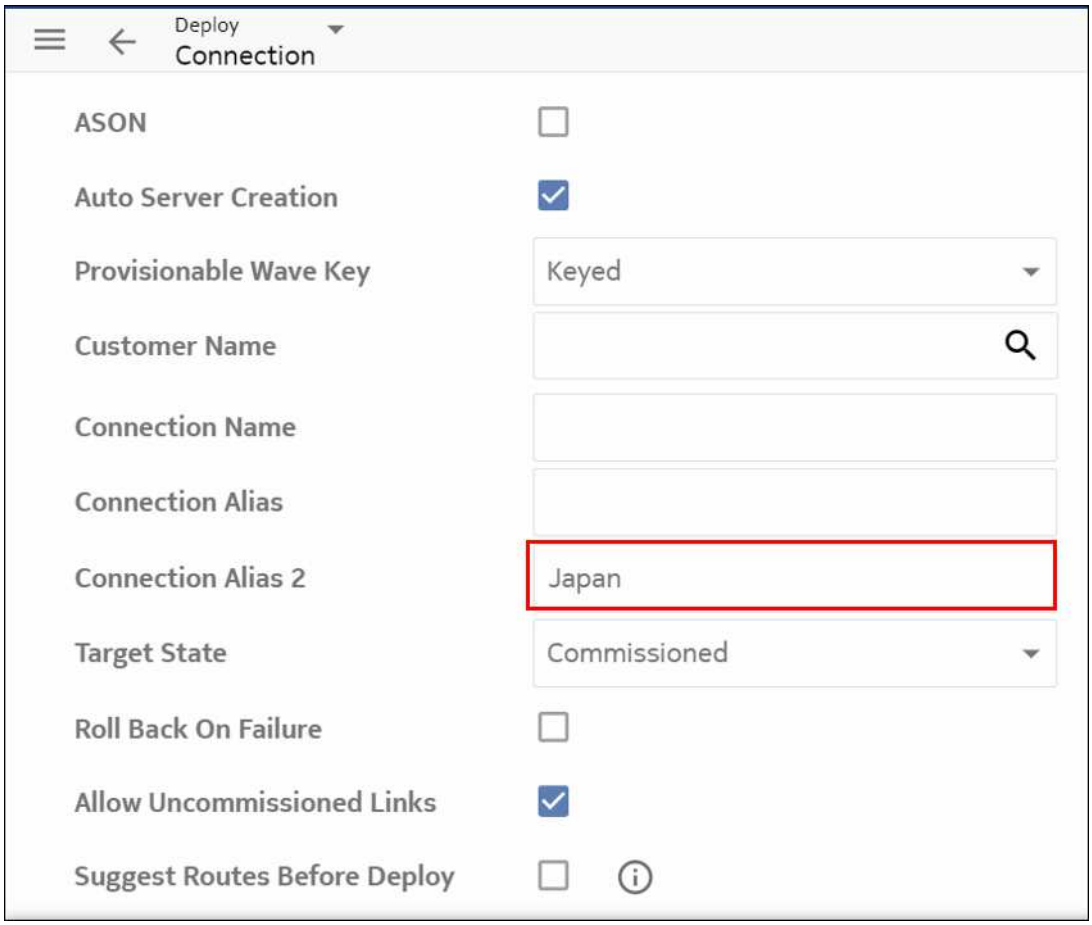
From the **CONNECTION CHARACTERISTICS** panel:

Continue with the default values for the following parameters:

- **Protection**
- **L-Band Frequency**
- **Routing Mode**
- **Allow ASON Resources**
- **ASON**
- **Auto Server Creation**
- **Provisionable Wave Key**
- **Customer Name**
  Optional: Enter a Customer name or click the search icon to select a name from the *Customer Name* list.
- **Connection Name**
  Optional: Enter a connection name or the system auto populates the name of the connection using the values of **From Node #1** and **To Node #1**.
- **Connection Alias**
  Optional: Enter a connection alias as an identification to the connection, for example, the complete path taken by the connection until the To-Node.
- **Connection Alias 2**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Optional: Enter a connection alias 2 as an identification to the connection.



- **Target State**
- **Roll Back On Failure**
- **ODUflex Bandwidth(Gps)**
- **Allow Uncommissioned Links**

Select **Suggest Routes Before Deploy** check box, for the system to display possible routes under **SUGGESTED ROUTES** pane of the **SUMMARY** section.

Note: Depending on the type of connection created and the **Rate** selected, additional tabs are displayed. For more information on these parameters, see "Deploy Rules" (p. 1220) and "CONNECTION CHARACTERISTICS tab" (p. 1223).

6

Click **CONTINUE**.

Result: SUMMARY section is displayed. For more information, see "Summary" (p. 1263)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

7

In the **PARAMETERS** section, verify the following in the **TRANSMISSION** tab:

- **Signal Type**: This is automatically set based on the **Service Rate Type** selected in **END POINT SELECTION** panel.
- **Container**: This is auto-populated based on the **Signal Type**.

  For a service on an OTSiG tunnel using card S6AD600H, based on the model (standard or transcoding) the following containers are displayed:
  - For a 100 GbE service, containers ODU4 and ODUTC1
  - For a 400 GbE service, containers ODUTC4 and ODUFlex

Select the applicable container as required.

8

Optional: Verify and modify the parameters in the different sections as required.

9

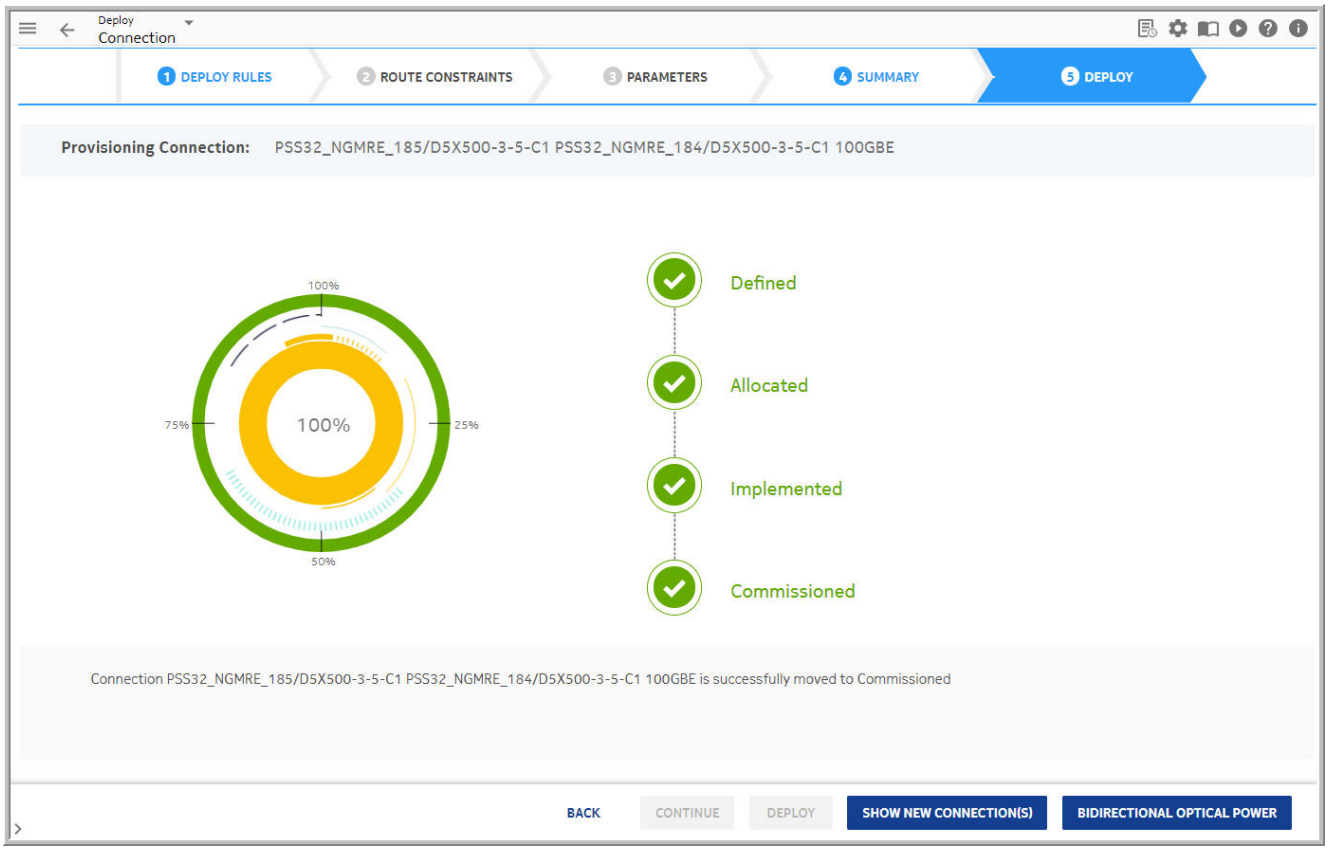
Click **DEPLOY**.

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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-12 Success Message for a Service



10

Optional:

Click **SHOW NEW CONNECTION(S)** to view the new connection.

Or

Click **BIDIRECTIONAL OPTICAL POWER** to view the Optical Power page.

11

Optional:

- Click **SHOW FAILED CONNECTION(S)** to view the failed deployment.
- You can also view the connection from **OPERATE > Infrastructure Connections** page.

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 an error message is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- To view the log and status of the connection, navigate to **ADMINISTER > Jobs** or **ADMINISTER > All Records** page.
- To cancel the failed connection, click **CANCEL CONNECTION**. Rectify the error and try to deploy the connection again.

12

In the WebUI, navigate to **OPERATE > Services**, to view the services that are created.

Result: The services that are created are displayed.

13

To view the Control Plane services, navigate to **OPERATE > SNCs**.

Note: In NFM-T R20.11, 400 GbE Control Plane services creation on a DFM6 and DFM6E card is not supported.

Result: The Control Plane services are displayed.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.9 Deploy 1:N Broadcast Connection

Before you begin

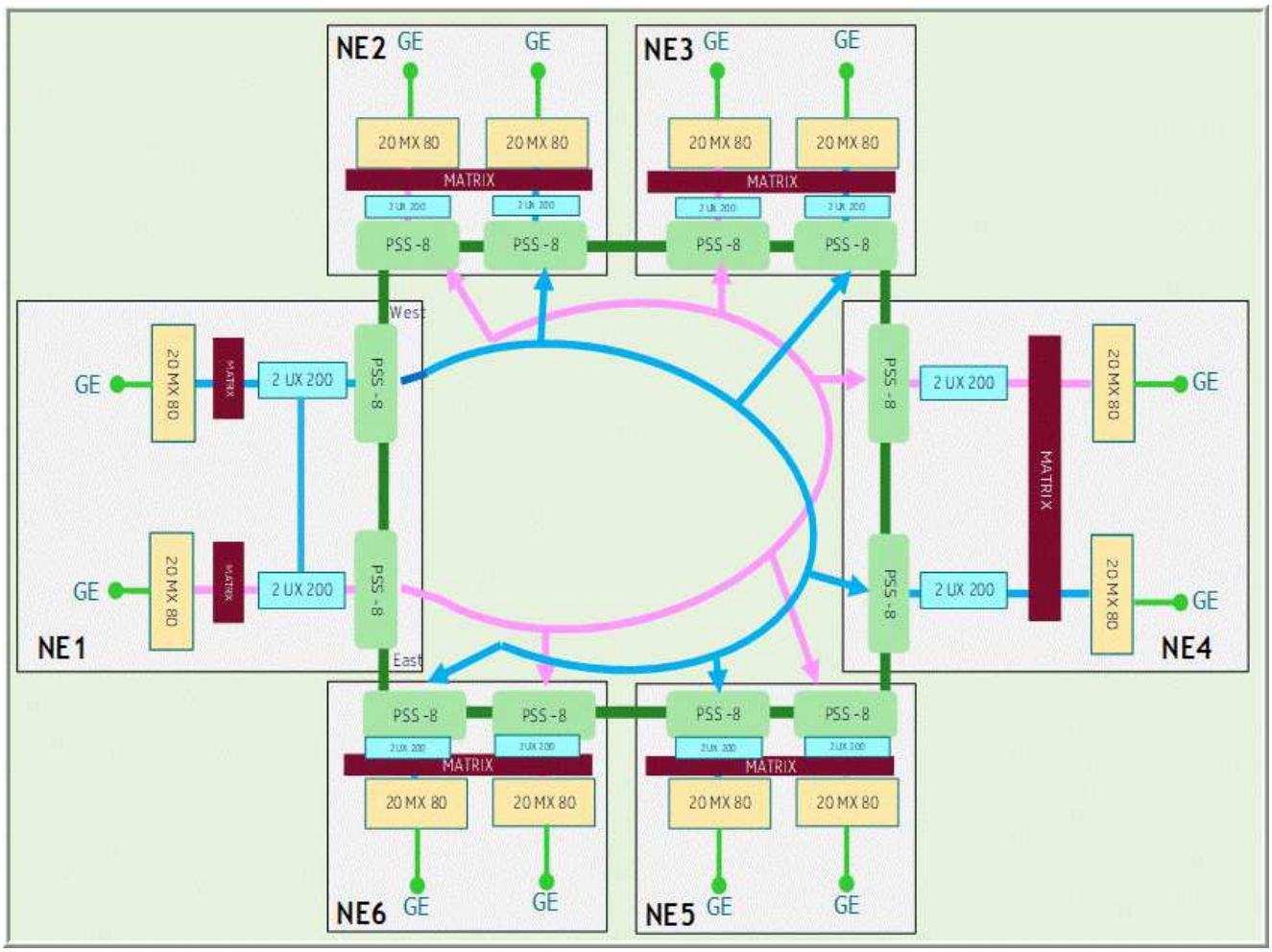
No Preconditions

Purpose

Follow the procedure to setup 1:N Broadcast connections.

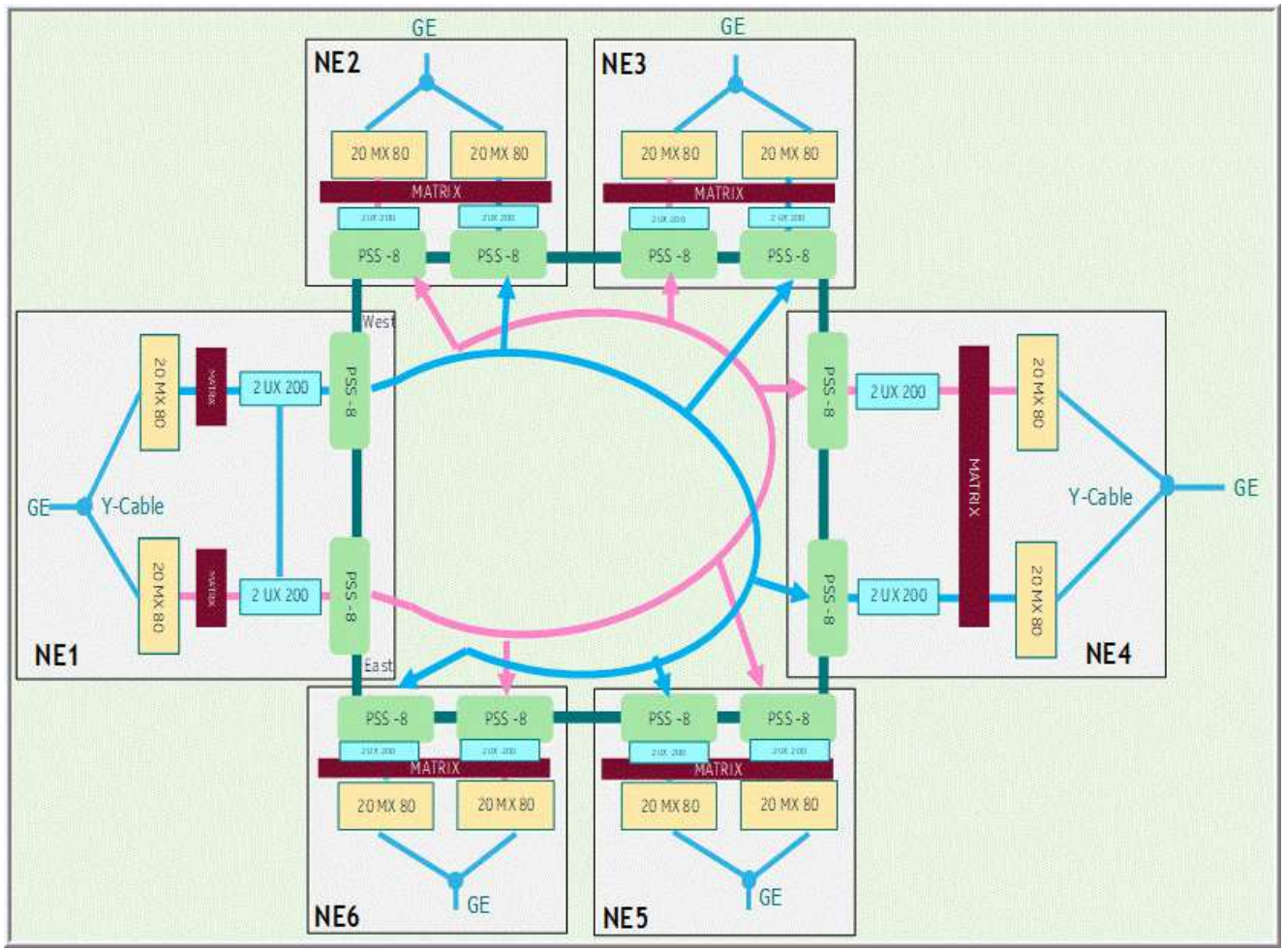
The broadcast configurations can be unprotected or with Y-cable Protection (Ring configuration).

Figure 8-13 Broadcast Connection - Point-to-Multi Points without Protection



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-14 Broadcast Connection - Point-to-Multi Points with Protection



Broadcast Connection with Y-Cable Protection

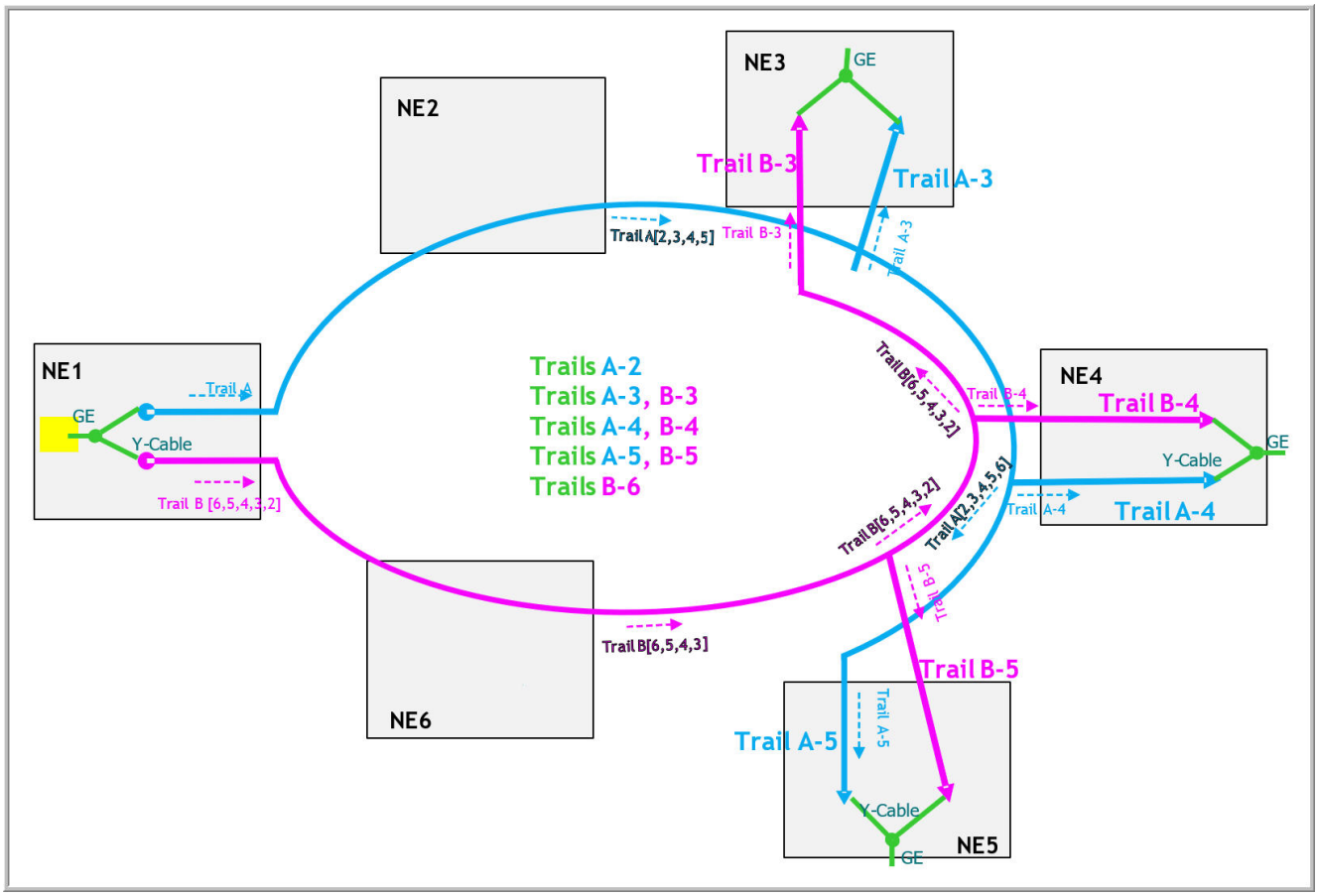
For a broadcast connection with Y-cable protection, the set of infrastructure must be double on the connection that needs to be setup. When provisioning the broadcast connection, you must deploy two sets of infrastructure connections ending on the nodes where the drop ports are located.

Two sets of connections are needed, one in working direction and one in protection direction. When Y-cable is inserted, then on both the farthest and nearest NE, at least one drop port is required.

The Figure 8-15, “Broadcast Connection - Example Schema” (p. 1303) is an example for a broadcast connection provisioning setup using Y-Cable protection, it aims to clarify the structures needed for the correct deploying of the broadcast connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-15 Broadcast Connection - Example Schema



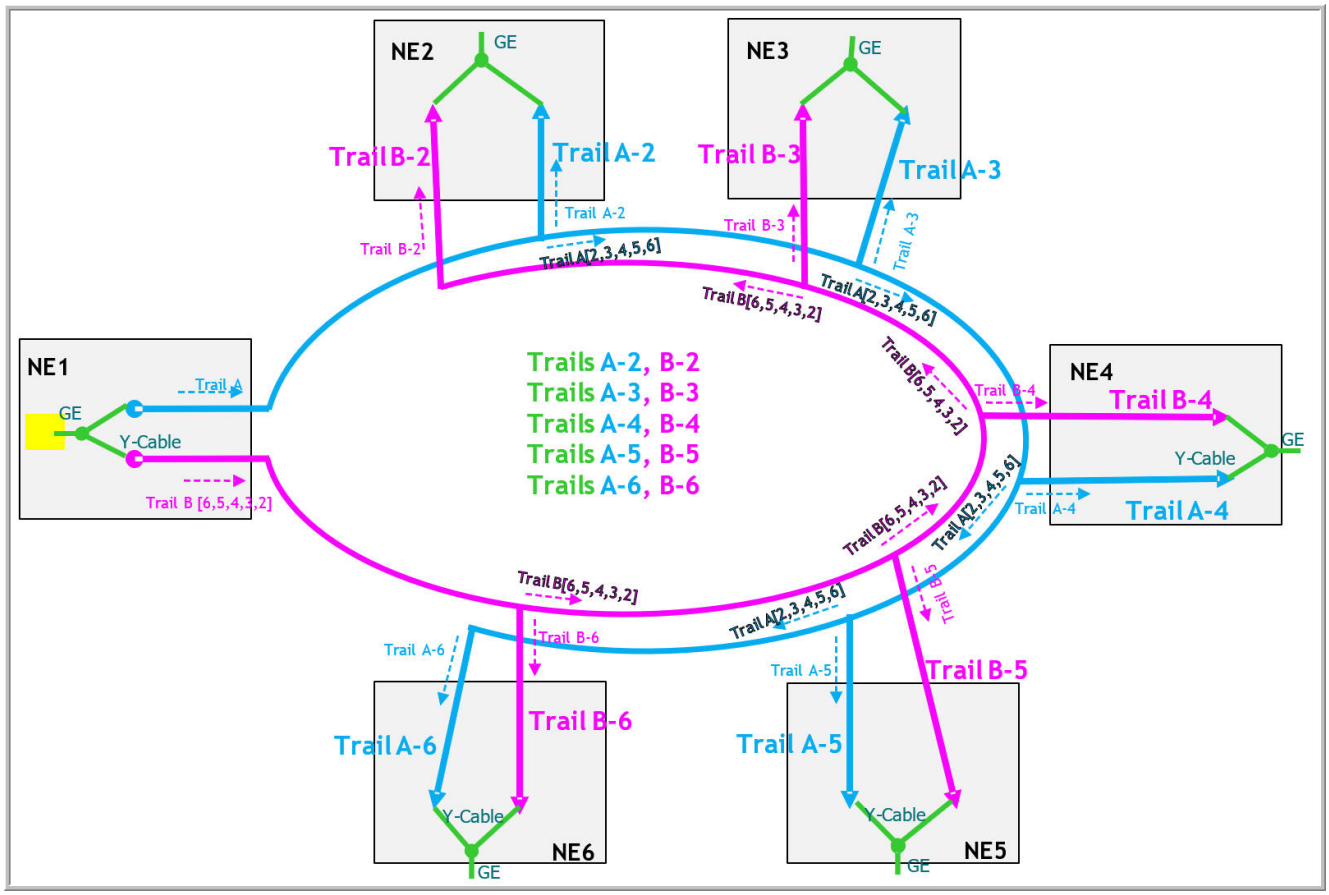
In this example, taking NE1 as the nearest and NE6 as farthest drop, infrastructures are created from NE1 to NE2, to NE3, to NE4, and to NE5 and on the other way, from NE1 to NE6, to NE5, to NE4, back to NE3.

Y-Cable is optional in the intermediate nodes. On the farthest drop, a drop port on the NE is needed to calculate the route correctly on the broadcast. To add drop ports on NEs always have a double infrastructure on the NEs you want to use. In this example, you will not be able to add drop ports on NE2 and NE6. If manual routing is used you have to specify the two end drops. Drops are on the nodes NE1, NE3, NE4 and NE5. This shows how the ring is provisioned if you want to drop on all the NEs, that is, additional infrastructure is also needed from node NE1 to NE6 and from NE2 to NE3.

The figure Figure 8-16, “Broadcast Connection - Example Schema with all nodes drop” (p. 1304), shows how the ring should be provisioned if the you want to add Drop on all the NEs, that means that additional infrastructure is needed also from node NE1 to NE6 and from NE2 to NE3.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-16 Broadcast Connection - Example Schema with all nodes drop



Provisioning Flow

1

From the WebUI, 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 *Gigabit Ethernet* 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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

4

From the **END POINT SELECTION** panel:

1. The **Service Rate Type** parameter is automatically is set based on the type of template selected. In this case: `Ethernet`.
2. The **Service Rate** parameter is automatically set based on the type of template selected. Example: `10 GbE`.

   Depending on the selected signal rate, configuration of other parameters may vary.
3. Select **Connection Type** as `1:N Broadcast Uni`
4. Select **From Node #1** and **To Node #1**.

   Select the nodes and ports for deployment by clicking the search icon and selecting the node or port from the list displayed in the lower pane. Or type the node or port name in the text box if you know which node or port to be used.
5. The fields **From Port Type #1** and **To Port Type #1** are automatically set as `Terminated`.
6. Select **From Port #1** which is the A-end of the connection and **To Port #1** which is the Z-end of the connection.

If the connection is Y-Cable protected, following data should be inserted:

- The From Port of the connection, the To Port of the connection, the Protection Drop Port, one working routing constraint and one protection routing constraint.
- The To Port must be the port furthest away from the From Port in the working path.
- The Protection Drop Port must be the port furthest away from the From Port in the protection path.
- The selected working routing constraint must have one endpoint on the From NE
- The selected protection routing constraint must have one endpoint on the From NE

Additional drop ports are optional, they can be added by modifying the connection.

5

From the **CONNECTION CHARACTERISTICS** panel:

Continue with the default values for the following parameters:

- **Protection**
- **L-Band Frequency**
- **Routing Mode**
- **Allow ASON Resources**
- **ASON**
- **Auto Server Creation**
- **Provisionable Wave Key**
- **Customer Name**
  Optional: Enter a Customer name or click the search icon to select a name from the *Customer Name* list.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- **Connection Name**

  Optional: Enter a connection name or the system auto populates the name of the connection using the values of **From Node #1** and **To Node #1**.
- **Connection Alias**

  Optional: Enter a connection alias as an identification to the connection, for example, the complete path taken by the connection until the To-Node.
- **Connection Alias 2**

  Optional: Enter a connection alias 2 as an identification to the connection.
- **Target State**
- **Roll Back On Failure**
- **ODUflex Bandwidth(Gps)**
- **Allow Uncommissioned Links**

Select **Suggest Routes Before Deploy** check box, for the system to display possible routes under **SUGGESTED ROUTES** pane of the **SUMMARY** section.

Note: Depending on the type of connection created and the **Rate** selected, additional tabs are displayed. For more information on these parameters, see "CONNECTION CHARACTERISTICS tab" (p. 1223) and "CONNECTION CHARACTERISTICS tab" (p. 1223).

6

Click **CONTINUE**.

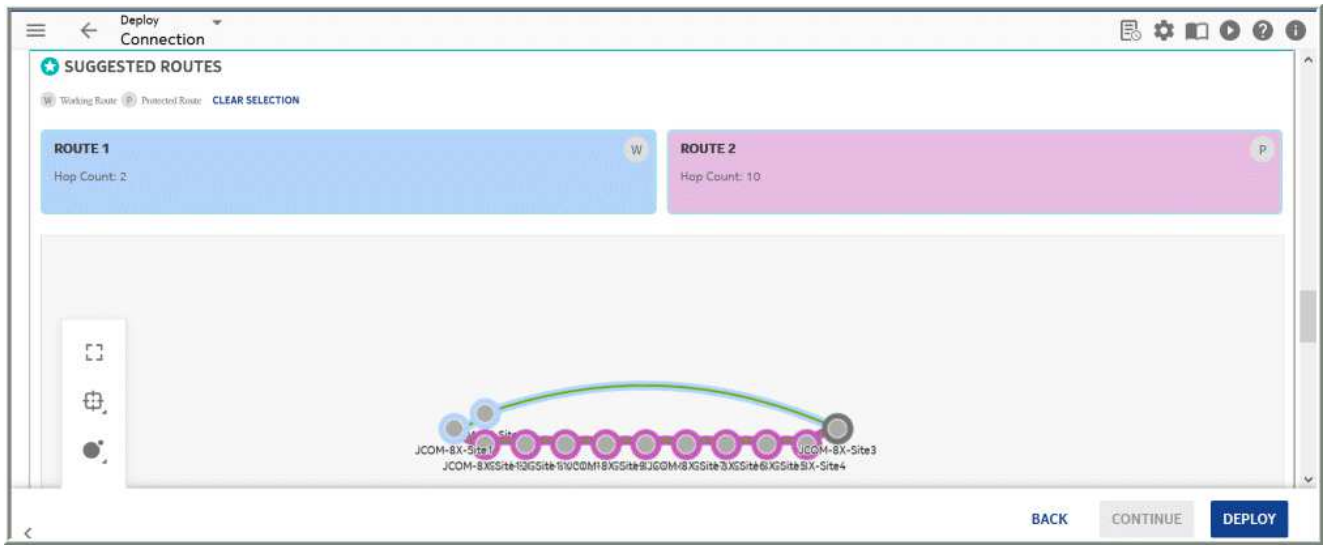
Result: SUMMARY section is displayed. For more information, see "Summary" (p. 1263)

7

The SUGGESTED ROUTES panel is displayed. The *Working Route* and the *Protected Route* are displayed in different colors.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-17 Deploy Broadcast Connection - Suggested Routes Panel

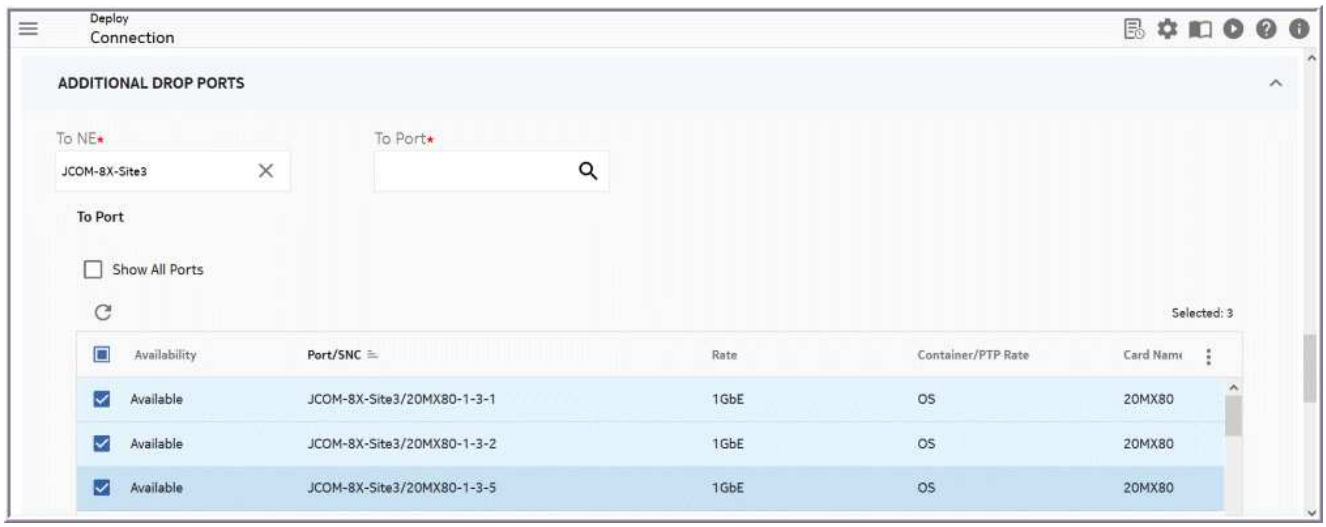


Use the button CLEAR SELECTION to clear the proposed selection.

8

At this point you can add additional drop ports.

Figure 8-18 Deploy Broadcast Connection - Additional Drop Ports



Select the **To NE** clicking on the magnifying glass to display the NE list.

Select the **To Port** clicking on the magnifying glass to display the Ports list.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

One or several ports can be selected. Click the **SELECT** button to confirm the selection.

You can use the **REMOVE** button to remove selected ports from the selection.

Click the **ADD** button on the upper right corner to add the drop port selected.

Result: The list of Additional Drop Ports is displayed.

9

Optional:

In the **PARAMETERS** section, verify the following in the **TRANSMISSION** tab:

- **Signal Type**: This is automatically set based on the **Service Rate Type** selected in **END POINT SELECTION** panel
- **Container**: This is auto-populated based on the **Signal Type**.

10

Optional: Verify and modify the parameters in the different sections as required.

11

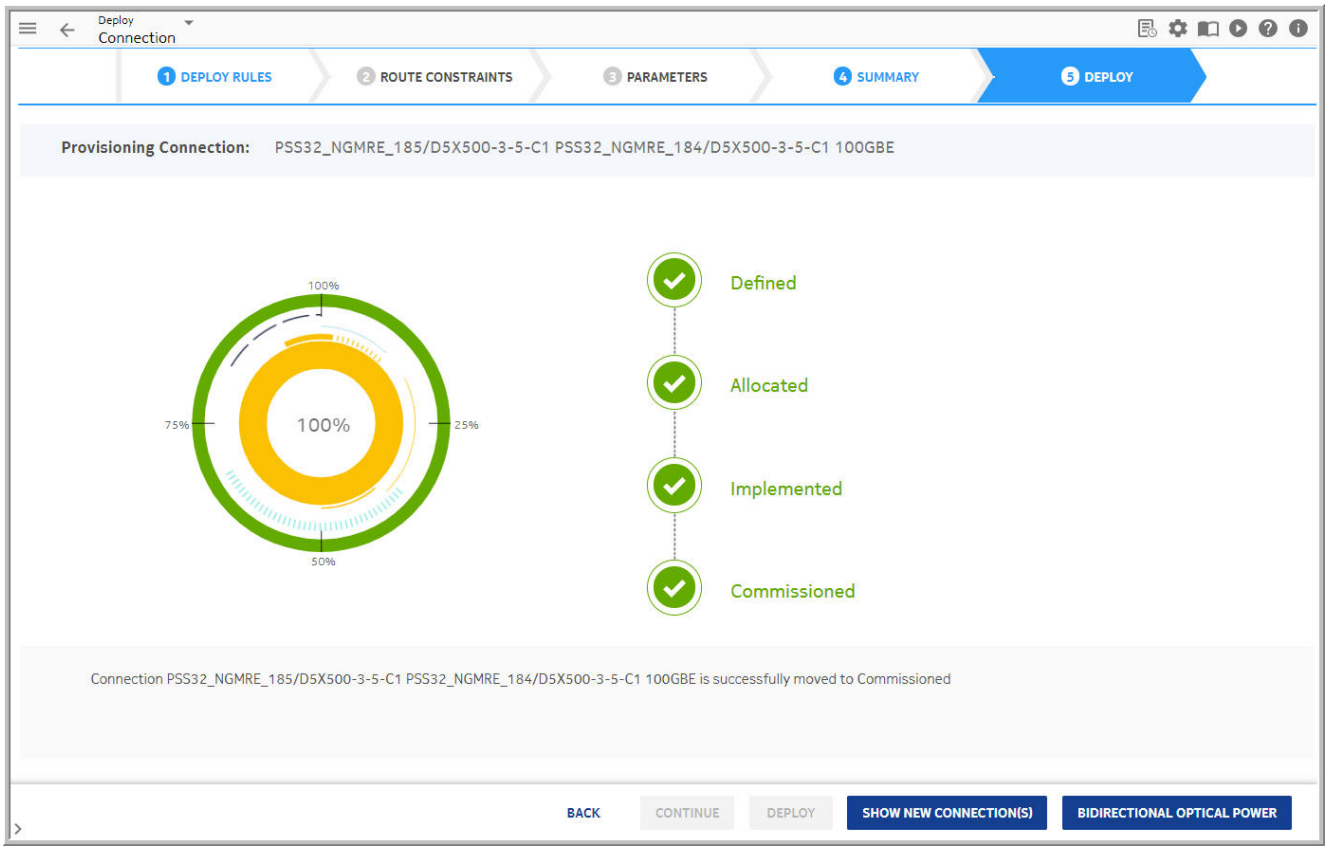
Click **DEPLOY**.

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.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-19 Success Message for a Service



END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.10 Create an end to end ODUFlex service

Before you begin

No Preconditions

Purpose

To create an end-to-end ODUFlex service for Managed and L1 Control plane network.

In Control Plane, only ODUFlex with GFP mapping is supported. CBR is not supported.

Related information

See "ODUflex " (p. 256).

Task: Create an ODUFlex connection For Managed Plane

1

Create a Managed Plane Logical Link connection between the uplink cards of 1830 PSS-24x NEs.

To view the NEs and cards supported, see "ODUflex " (p. 256)

To create a Managed Plane logical link connection, see 8.5 "Deploy a Managed Plane Connection" (p. 1271).

2

Select **`/Best Practices/Service/Ethernet/Unprotected/Full Rate`** template and create a service with the **Service Rate** as **Flexible Rate Client** with the IO cards or uplink cards of the supported NEs.

If the user selects the **Service Rate** as **Flexible Rate Client**, the **ODUflex Bandwidth(Gps)** field is enabled in the **CONNECTION CHARACTERISTICS** pane. The **Container** field in the **PARAMETERS** tab is set to **ODUflex** by default.

The **ODUflex Bandwidth(Gps)** rate is a multiple of approximately 1.25 GHz, to correspond to the capacity of an integer number of higher order ODU time slots, and the packet flow is adapted to that rate.

Select the value from the spinner.

The number of ODU0 time slots used is fixed, depending on the bandwidth selected. The number of the time slots is displayed in the Infrastructure connection list.

The number of time slots is obtained dividing the ODUflex Bandwidth (Gps) by 1.25 GHz.

3

From the WebUI, navigate to **OPERATE > Services**, to view the services that are created.

Result: The ODUFlex services that are created are displayed.

1. If the **Service Rate** selected is **Flexible Rate Client** during provisioning, the **Rate** column displays the rate as well as the **ODUflex Bandwidth(Gps)** selected during provisioning.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2. Select a service and click the **More** icon. All the related operations can be performed.

END OF STEPS

Task: Create an ODUFlex connection for L1 Control Plane connections

1

Create a Managed Plane Logical Link connection with the between the uplink cards of 1830 PSS-24x NEs.

To view the NEs and cards supported, see "ODUflex " (p. 256)

To create a Managed Plane logical link connection, see 8.5 "Deploy a Managed Plane Connection" (p. 1271).

2

To create an L1 control plane connection, assign the logical link to NPA.

To assign the Logical link to NPA, perform **Add Links to ASON** from ASON NPA page.

Ensure to Unlock the link added to NPA.

Result: The Logical link is added to NPA successfully.

3

Create a service with the **Service Rate** as **Flexible Rate Client** with the IO cards or uplink cards of the supported NEs.

If the user selects the **Service Rate** as **Flexible Rate Client**, the **ODUflex Bandwidth(Gps)** field is enabled in the **CONNECTION CHARACTERISTICS** pane. The **Container** field in the **PARAMETERS** tab is set to **ODUflex** by default.

The **ODUflex Bandwidth(Gps)** rate is a multiple of approximately 1.25 GHz, to correspond to the capacity of an integer number of higher order ODU time slots, and the packet flow is adapted to that rate.

Select the value from the spinner.

The number of ODU0 time slots used is fixed, depending on the bandwidth selected. The number of the time slots is displayed in the Infrastructure connection list.

The number of time slots is obtained dividing the ODUflex Bandwidth(Gps) by 1.25 GHz.

4

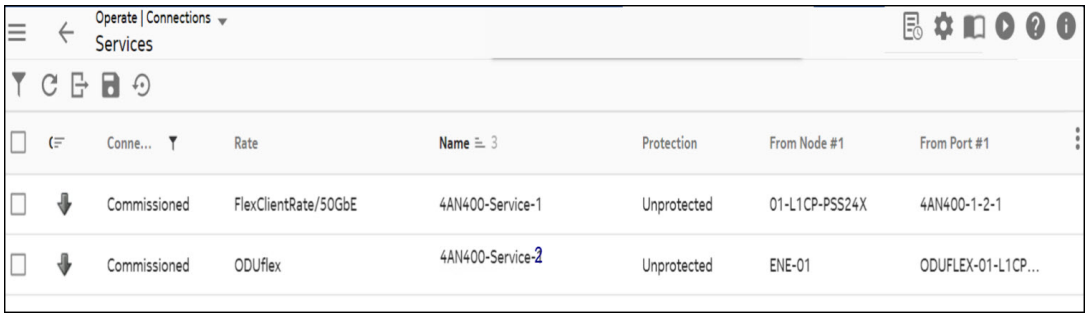
From the WebUI, navigate to **OPERATE > Services** to view the services that are created.

Result: The ODUFlex services that are created are displayed.

1. The **Rate** column displays the rate as well as the selected **ODUflex Bandwidth(Gps)**

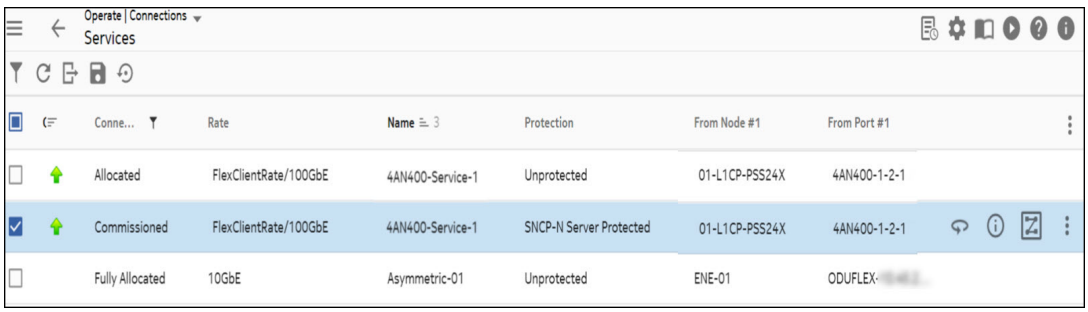
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

during provisioning.



2. Select a service and click the **More** icon. All the related operations can be performed.
3. *[Optional]* To add protection for an uprotected service, select a service and click the **More** icon. Select the **Modify Connection > Add Protection** or **Modify Connection > Add ASON Protection - System Routed**.

   To add protection, the system navigates to the Provisioning window. To add system assigned protection, select **Add ASON Protection - System Routed**. The protection is assigned internally in GMRE and the **Services** page is automatically updated with the Server protection details. The **Route** from the **ASON SNCs** page displays both the **Main** and **Spare** paths. See Step 5.



   The Routing Display displays the working and the protection path.

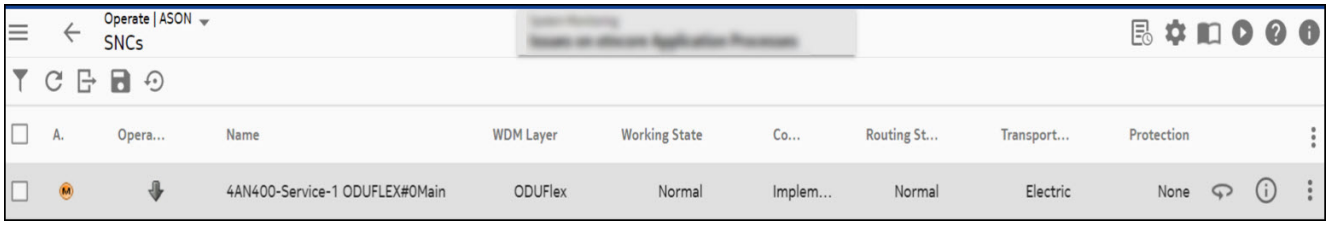
   Alternately, you can also modify the parameters, connection name and so on, from the list of options.
4. **ODUflex Bandwidth(Gps)** cannot be modified during the modification of the parameters.

5

To view the Control Plane services, navigate to **OPERATE > SNCs**.

If the **Rate** selected is **Flexible Client Rate**, the **Rate** column displays the **Rate** as well as the **ODUflex Bandwidth(Gps)** selected during provisioning. The **WDM Layer** column displays the **ODUFlex** as the container.

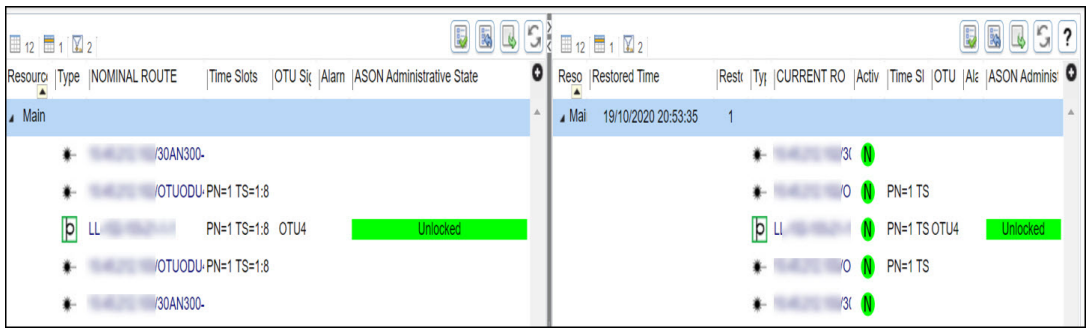
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

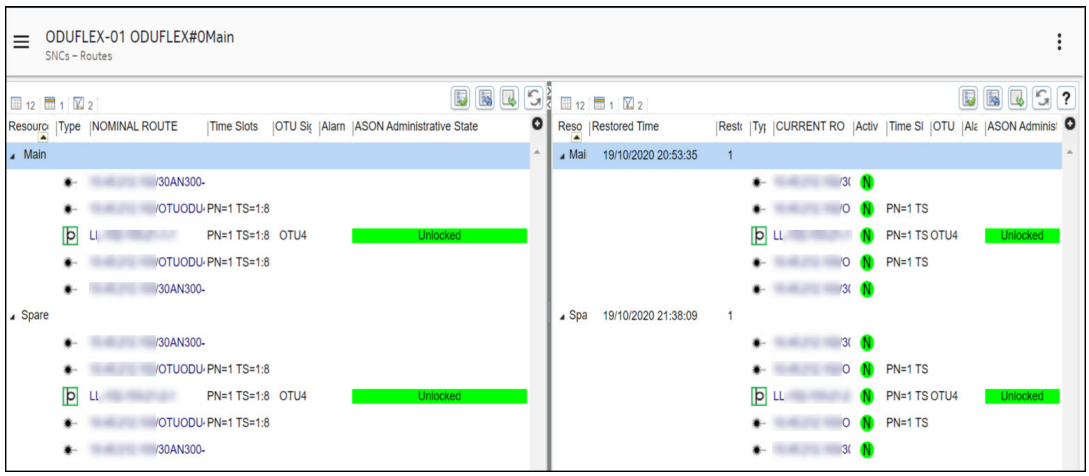


Result: The Control Plane services are displayed.

1. To view the route of the connection, select the **More** icon and click **Routes** .

   The current and nominal route is displayed. The time slots that are set are also displayed.





2. To reroute the connection, select the **More** icon and perform **Convert Current to Nominal**

   The connection is rerouted.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.11 Manage an OTSig Tunnel

Overview

Create an OTSig Tunnel for ADD3 such as 4UC1T, 8UC1T and ADD4 ASIC cards such as DFC12, DFC12E, DFM6, DFM6E, DD2M4, SFM6, 2UX500, S4X400H, S6AD600H, and uplink cards 4UC400, 2UC400, and OT card D5X500Q.

Create an Unprotected MRN Terminated OTSig tunnel. To create a Managed Plane connection with OTSig Tunnel, set the **Rate** as **`OTSig Tunnel`** without checking the **ASON** check box.

For OTSig tunnel the connection naming conventions are as per Table 8-16, “OTSig tunnel and trail – Naming Convention” (p. 1314).

Table 8-16 OTSig tunnel and trail – Naming Convention

Connection Type	Unprotected
Without 3R	• OTSig tunnel: *`NE1/Port1 NE2/Port2 OTSIGTunnel`* • OTSig trail: *`NE1/Port1 NE2/Port2 OTSIG#1`*

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-16 OTSig tunnel and trail – Naming Convention (continued)

Connection Type	Unprotected
With 3R	User-defined connection naming: • OTSig tunnel: *<User-defined name>*. For example, *Kp-S4X-Internal_OS-T1*. • OTSig trails: - *<User-defined name> NE1/Port1 NE2/Port2 OTSIG#1* . For example, *Kp-S4X-Internal_OS-T1 06-CDCF-IRD20-MCS816/OTSIG-8-8-1 12-CDCF-IRD20MCS1615/OTSIG-8-8-1 OTSIG#1*. - *<User-defined name> NE2/Port2 NE3/Port3 OTSIG#2*. For example, *Kp-S4X-Internal_OS-T1 12-CDCF-IRD20MCS1615/OTSIG-8-8-1 10-CDC-F-WR20-TFM/OTSIG-3-8-1 OTSIG#2*.
	System generated connection names: • OTSig tunnel: *NE1/Port1 NE3/Port3 OTSIGTunnel*. For example, *06-CDCF-IRD20-MCS816/OTSIG-8-7-1 10-CDC-F-WR20-TFM/OTSIG-3-7-1 OTSIGTunnel*. • OTSig trails: - *NE1/Port1 NE2/Port2 OTSIG#1*. For example, *06-CDCF-IRD20-MCS816/OTSIG-8-7-1 24-CDC-F-1.0/OTSIG-11-3-1 OTSIG#1*. - *NE2/Port2 NE3/Port3 OTSIG#2*. For example, *24-CDC-F-1.0/OTSIG-11-3-1 10-CDC-F-WR20-TFM/OTSIG-3-7-1 OTSIG#2*.

Related information

See the following topic in this document:

- 2.31 “Provisioning connections for ADD4 cards” (p. 286)
- “Best Practices templates” (p. 669)
- “Optical line characteristics” (p. 706)
- “OTSiG tunnel” (p. 258)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Before you begin

Ensure to design and publish an OTSig template from **DESIGN > Service/Infrastructure Template**. The templates includes trails with optical trail service type *OTSIG Tunnel*.

Ensure that the OPS Physical Connection is created with the cards 4UC1T, 8UC1T, DFC12, DFC12E, DFM6, DFM6E, SFM6, S13X100, D5X500Q, 1UX100, 2UX200, 2UX500, 2UC400, 4UC400, DD2M4, S4X400H, S2AD200, S6AD600H and S5AD400H with Signal Type OTSig. See Step 5.

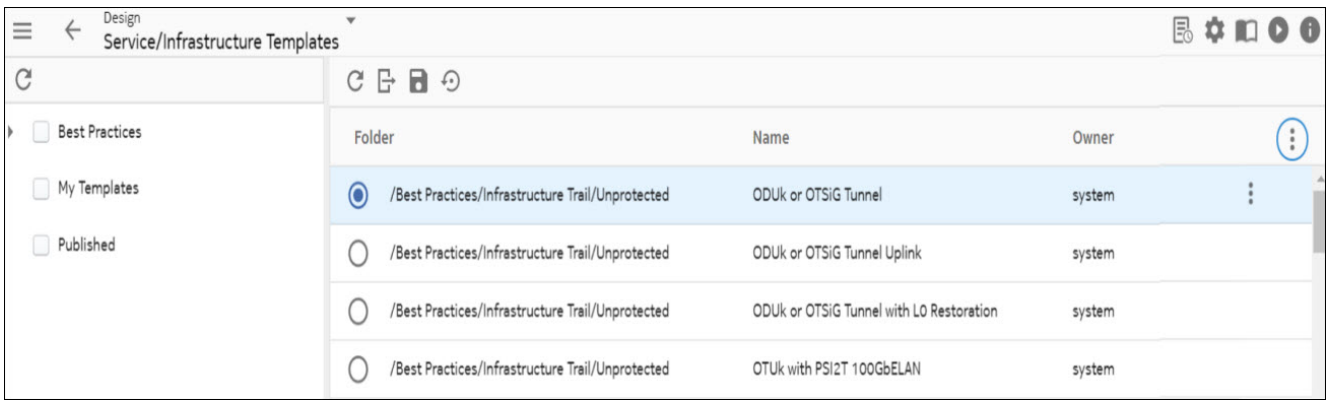
Task: To create an OTSig Tunnel

Complete the following steps to create an OTSig Tunnel.

1

[Optional]: Create and publish the connection template, if necessary.

Figure 8-20 OTSig Tunnel Best Practice Template



Complete the steps of the procedure7.12 "Deploy a template to make a connection" (p. 754).

Note: The optical trail service type includes OTSIG Tunnel template.

2

From the NFM-T GUI, follow the path:

DEPLOY > New Service/Infrastructure Connection

3

Select **/Best Practices/Infrastructure Trail/Unprotected** with **ODUk or OTSiG Tunnel** and click **Deploy** ( ) button.

Result: The system displays the **Connection** window with the **DEPLOY RULES** section selected.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

4

In the **Rate** field, select **OTSig Tunnel**.

The **Connection Type** field is automatically set to **2 Ended Bi (I)**.

Result: The **OPTICAL LINE CHARACTERISTICS** pane is enabled.

5

In the **From Node #1**, **To Node #1**, **From Port #1**, and **To Port #1** fields, click on the search icon to display the list of available NEs and Ports.

Ensure that the NEs releases are R13.0 onwards for 1830 PSS PHN and R4.0 onwards for 1830 PSI-M.

Select line ports for unamplified connections, see Step 26 for details.

6

Ensure the **Protection** checkbox is not selected.

7

Optional: Check the **L Band Frequency** checkbox to deploy a connection with the frequency in the L Band.

8

Select the required **Routing Mode** (Automatic or Manual) from the drop-down.

Note: For Control Plane connections, only Manual **Routing Mode** is supported.

9

Optional: Check the **Allow ASON Resources** checkbox for creating OTSig Tunnel as a Foreign Connection.

Note: The selection integrates Managed Plane connection on ASON network.

10

Check the **ASON** checkbox for Control Plane connections.

Note:

- In NFM-T R20.11, Control Plane connections on a **DFM6** and **DFM6E** card is not supported.

11

Ensure the **Auto Server Creation** checkbox is selected.

Auto Server Creation checkbox is selected by default to automatically provision the server layer OCH, OTUk, and ODUk when a client is provisioned.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

12

For S5AD400H card, select **Unkeyed** in the **Provisionable Wave Key** field.

13

Optional: In the **Customer Name** field select a name from the list clicking on the magnifying lens to display the customer name list.

14

Optional: If you want to insert a **Connection Name**, type the name of the connection, otherwise it will be assigned automatically by the system.

15

Optional: In the **Alias** field insert an alias for the connection. Field is filled with the old alias. Field supports blank Alias.

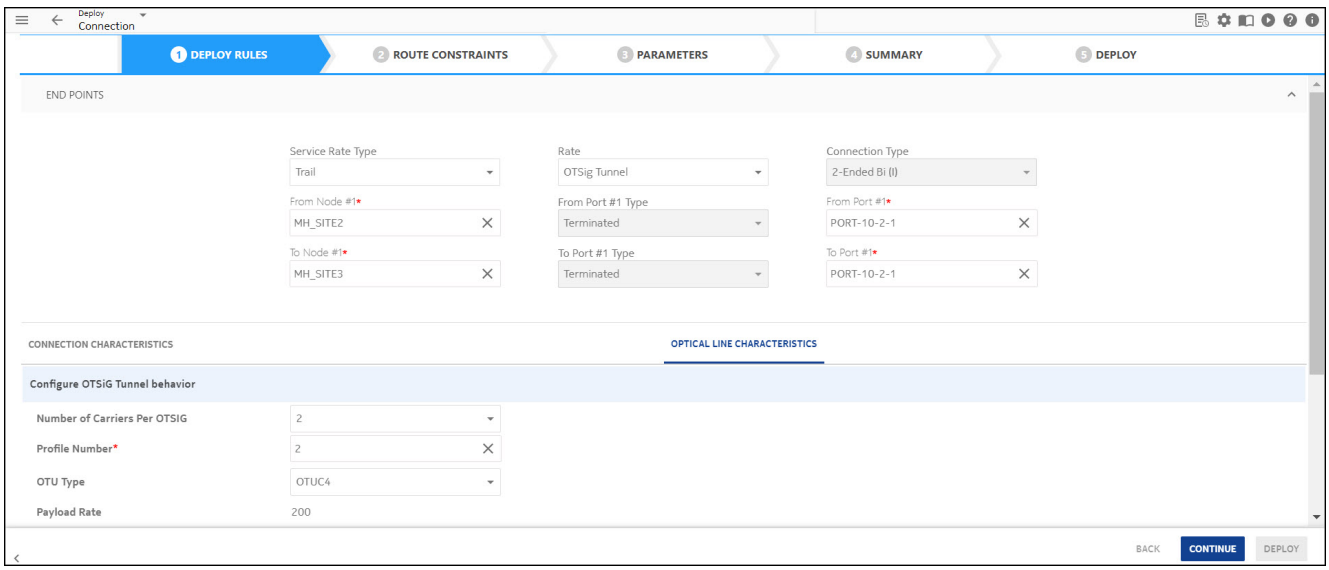
16

Optional: In the **Alias 2** field, enter a connection alias 2 as an identification to the connection.

17

In the **OPTICAL LINE CHARACTERISTICS** pane as shown in the following figure, the **Profile Number** field is set to the value, **2**.

Figure 8-21 Optical Line Characteristics pane - 4UC1T for Dual Carrier



Click the **Search** icon on the **Profile Number** field to display the **Line Mode Profile** window as shown in the following figure to select the required profile based on the selected card and the

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

supported profile. For more information on the profiles supported per card, see Table 8-15, “Profile and Card Mapping” (p. 1267).

Based on the card and Profile Number, the options in the **Profile Number** window changes.

Figure 8-22 Profile window

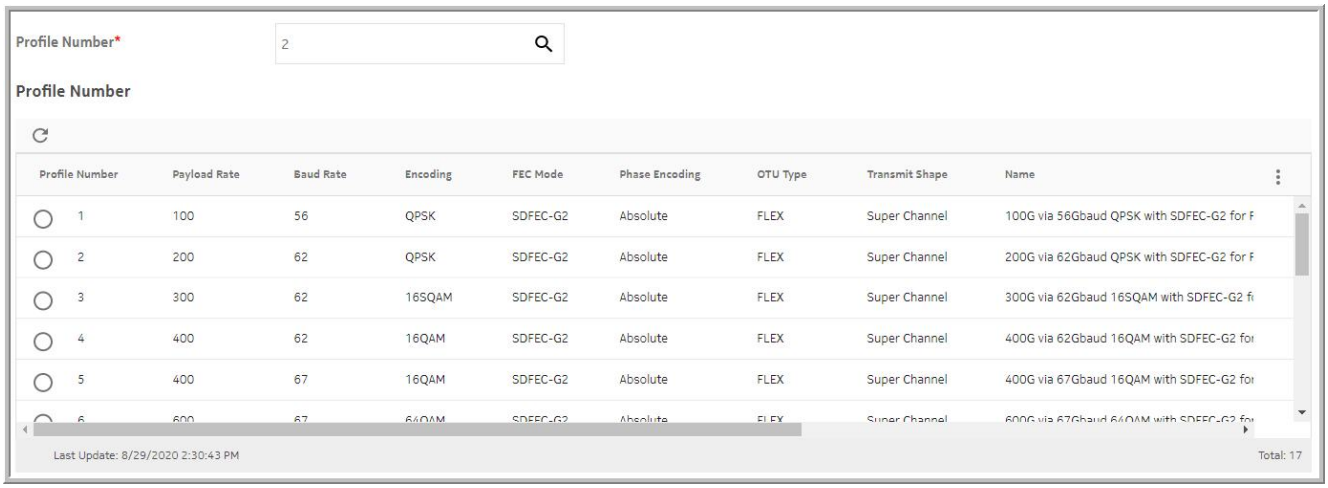
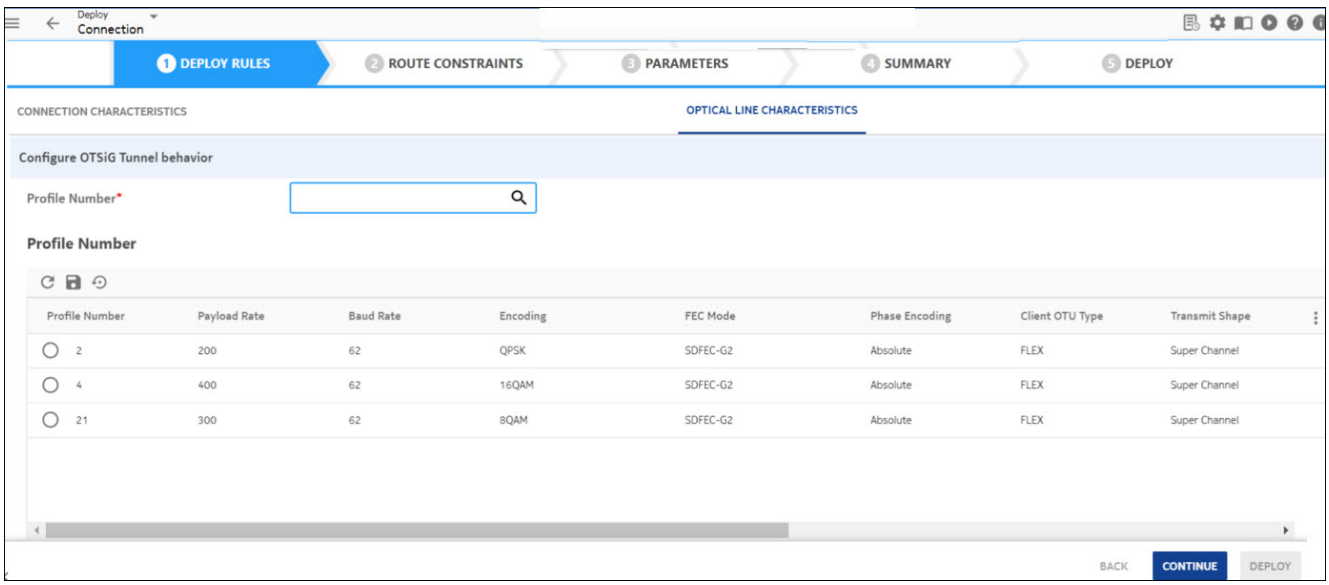
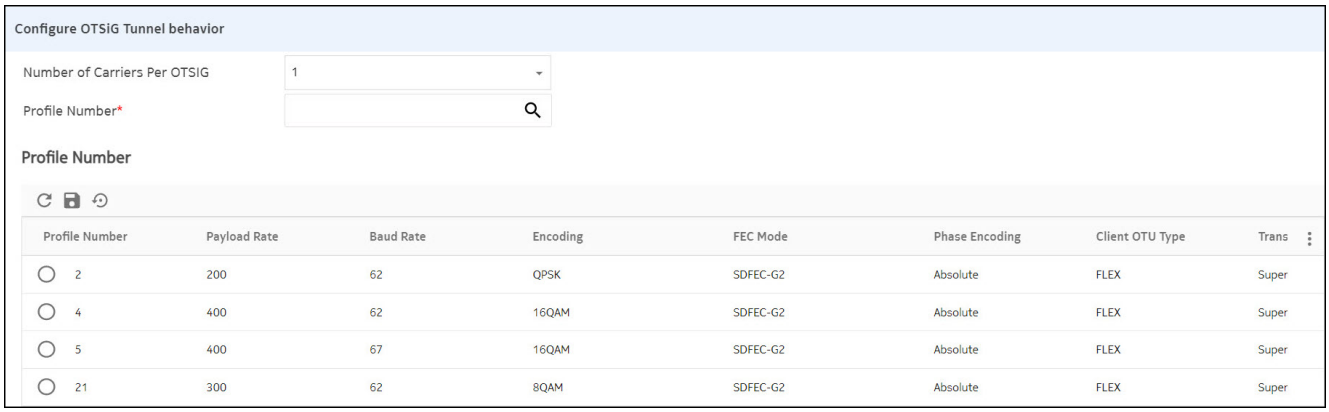


Figure 8-23 Profile window for S5AD400H



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-24 Profile window for DD2M4



Profile Number	Payload Rate	Baud Rate	Encoding	FEC Mode	Phase Encoding	Client OTU Type	Trans
2	200	62	QPSK	SDFEC-G2	Absolute	FLEX	Super
4	400	62	16QAM	SDFEC-G2	Absolute	FLEX	Super
5	400	67	16QAM	SDFEC-G2	Absolute	FLEX	Super
21	300	62	8QAM	SDFEC-G2	Absolute	FLEX	Super

Result: The values of the remaining parameters are filled accordingly to the **Profile Number** selected.

Note: To enable **Polarization Tracking** view see "Enable the Polarization Tracking view in the Profile window" (p. 1327).

Based on the card selected, the value in the **OTU Type** changes:

- S4X400H and S4X400L cards display OTU4 option.
- DFM6 and DFM6E cards display OTUC4 option.
- 2UX500 displays:
  - Line OTU Type: OTU4 (2x, 3x or 4x based on the profile)
- S5AD400H card displays OTU4 and OTUC4 options.
- DD2M4 cards display OTU4 and OTUC4 options, Payload Type 21 displays 100G and OTU4 Payload Type 22 displays 400G

  For 400 GbE connections, ensure to select Profile Number 4 with OTU Type as OTUC4.
- 4UC1T card for 400G, dual carrier tunnel, ensure to select **Profile Number** 2, **Number of Carriers Per OTSIG** 2, and **OTU Type** as OTUC4.
- For **S6AD600H** and **SFM6** cards, it displays OTU4, OTUC4, OTUTC1, or OTUTC4 as per the profile selected.

18

Optional:

For an OTSig Tunnel on the line ports of DFM6 and DFM6E cards, an additional field **Number of Carriers Per OTSIG** is displayed. Specify the number of carriers required to meet the client signal rate. Select 1 for single carrier or 2 for dual carrier from the drop-down as required.

The **Profile Number** support is based on the **Number of Carriers Per OTSIG** specified:

- If **Number of Carriers Per OTSIG** selected is *1*, the profile numbers supported are *4* and *5*.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- If **Number of Carriers Per OTSIG** selected is *2*, the profile numbers supported are `2` and `15`.

19

[Optional]: For an OTSig Tunnel on the line ports of S5AD400H card, select **OTU4** or **OTUC4** from the drop-down list in the **OTU Type**.

Based on the Profile Type selected on S5AD400H card, the options in the **OTU Type** field changes.

- Profile ID 2 supports OTU4 mode.
- Profile ID 4 supports either OTU4 and OTUC4 mode for 100 GbE and 400 GbE connections
- Profile ID 21 supports OTU4 mode.

20

Optional:

For OTSig Tunnel on the line ports of DD2M4, select **OTU4** or **OTUC4** from the drop-down list in the **OTU Type**.

Note: For DD2M4, L1 is not equal to L2. You can create two different profiles on 2 line ports.

21

[Optional] For an OTSig Tunnel on the line port of **S6AD600H** and **SFM6** card, select the required **OTU type** for the following profiles as required:

- If the **Profile Number** selected is 26, maximum of **6xOTUTC1** or **2xOTUTC1 and 1xOTUTC4** are supported.

  Note: In NFM-T R21.12, 2xOTUTC1 and 1xOTUTC4 are not supported for Control Plane connections.
- If the **Profile Number** selected is 27, maximum of **4xOTUTC1** or **1xOTUTC4** are supported.
- If the **Profile Number** selected is 28, maximum of **3xOTU4** are supported.
- If the **Profile Number** selected is 29, maximum of **4xOTU4** or **1xOTUC4** are supported.

  Note: In NFM-T R21.12, 1xOTUC4 is not supported on SFM6 card.
- If the **Profile Number** selected is 32, maximum of **1xOTUC4 and 1xOTU4 or 5xOTU4** is supported.
- If the **Profile Number** selected is 33, maximum of **3xOTUTC1** are supported.
- If the **Profile Number** selected is 34, maximum of **1xOTUTC1 and 1xOTUTC4 or 5xOTUTC1** is supported.
- If the **Profile Number** selected is 38, maximum of **5xOTU4** or **1xOTU4 and 1xOTUC4** are supported.

  Note: In NFM-T R22.6, profile number 38 supports only Managed Plane connections.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

22

[Optional] OTSig is introduced between the Port/OTSi and OTU's to enable flexible and dynamic networking and to support baud rate of 100G. This facility is not present on legacy cards (like D5X500Q) and is masked within the port facilities. Therefore the legacy cards are added with an hidden static mapping explicitly to mimic OTSig model.

For an OTSig Tunnel on the line port of **D5X500Q** and **4UC1T** card, select the required **OTU type** for Managed Plane connection:

- For **Profile Number** 20, set **Pluggable Module Type** to **`Auto`**, and **Transmit Shape** to **`Single`**.

For more information on Profiles, see Table 8-4, “Profile Number and supported Parameter values ” (p. 1236)

Note: For OTSig tunnel creation on D5X500Q, the default OTUStruct allocation for L1 is *OTU4#1&OTU4#2* and L2 is *OTU4#4&OTU4#5*. As the quad constraint of D5X500Q card, the C1/C2/C3 ports can only be cross connected to channels of OTSiG Tunnel using L1 and C4/C5 ports cross connected to OTSiG Tunnel using L2.

23

[Optional] For an OTSig Tunnel on line port of **4UC400** and **8UC1T** and **2UC400** and **4UC1T/2UX500**

- For **Profile Number** 7, set **Transmit Shape** to **`Single`**
- For **Profile Number** 20, set **Pluggable Module Type** to **`Auto`**, and **Transmit Shape** to **`Single`**

For more information on Profiles, see Table 8-4, “Profile Number and supported Parameter values ” (p. 1236)

24

From **PARAMETERS > RESTORATION** tab.

Note: To move from one tab to another, perform one of the following steps:

- From the **DEPLOY RULES** section, if the **Routing Mode** is set to *`Manual`*, clicking **CONTINUE** button moves from **DEPLOY RULES** > **ROUTING CONSTRAINTS** > **PARAMETERS** > **SUMMARY** sections. To move to the previous section, click **BACK** button.

  From the **DEPLOY RULES** section, if the **Routing Mode** is set to *`Automatic`*, clicking on the **CONTINUE** button takes you to the **SUMMARY** tab.
- Click on a tab to set the parameters.

25

The **ASON Tunnel** check box is selected and **Tunnel Type** is set to **MRN Terminated** automatically. These settings cannot be edited.

Set the **ASON Restoration** field to **No Restoration**, **Source-Based Restoration**, or **Guaranteed Restoration**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

26

Optional: To create unamplified connections using Link Span, ensure to follow the prerequisites for OT to OT and FOADM configurations:

- The **From Port #1** and **To Port #1** must be line port.
- For OT to OT configuration, set **Provisionable Wave Key** as **UnKeyed** under **DEPLOY RULES > CONNECTION CHARACTERISTICS** pane and **Wave Key type** as **Automatic** under **PARAMETERS > WAVE KEY** tab.
- For FOADM configuration, set **Provisionable Wave Key** to **UnKeyed** under **DEPLOY RULES > CONNECTION CHARACTERISTICS** pane and **Wave Key type** to **Manual** under **PARAMETERS > WAVE KEY** tab.

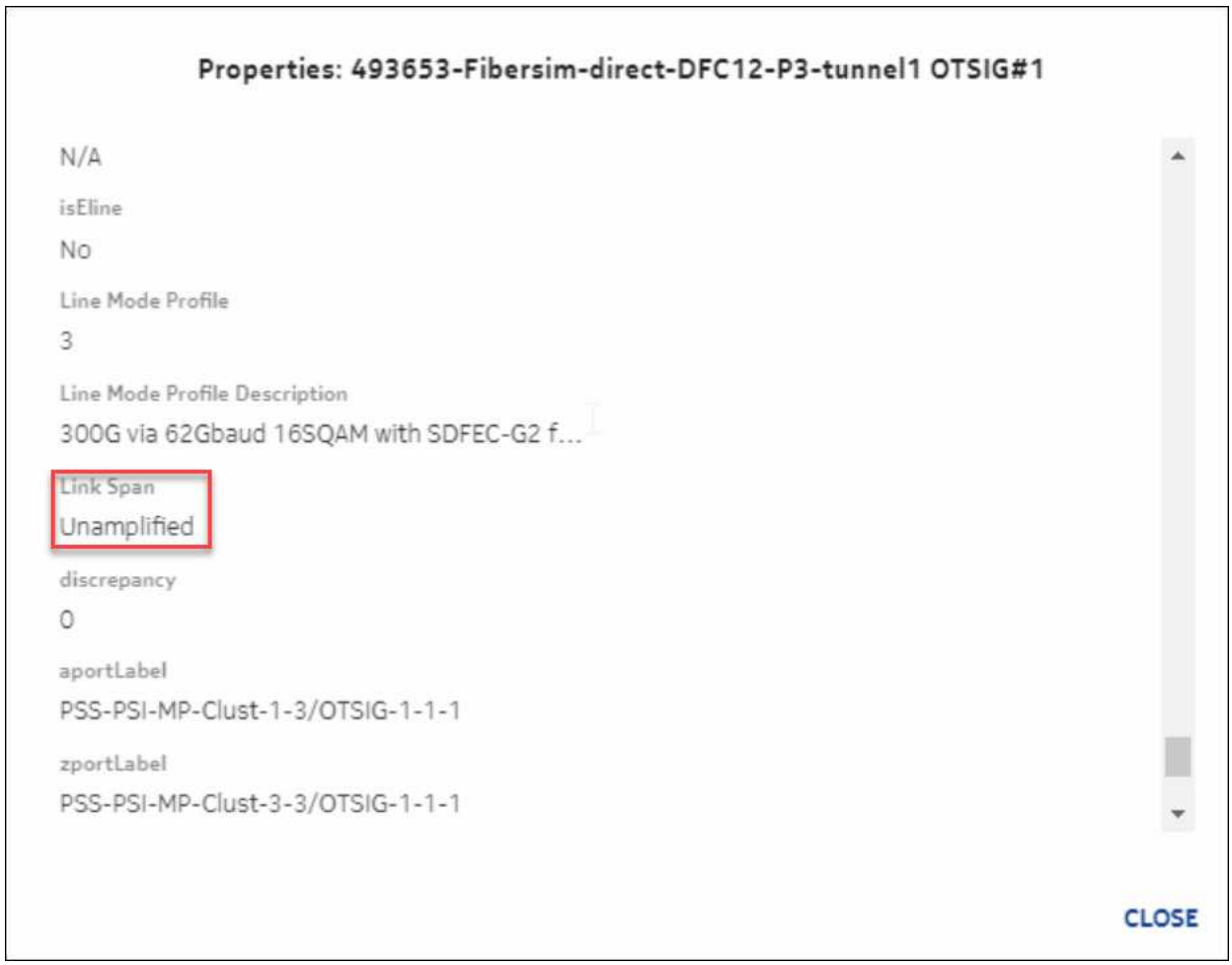
By default, the **Link Span** parameter is set to **Amplified** under **DEPLOY RULES > OPTICAL LINE CHARACTERISTICS** tab. **Link Span** values are **Amplified** and **Unamplified** . Set the **Link Span** value to **Unamplified**.

Note: Modifying transmission parameter to **Use NE Values** is not a valid test scenario.

The following figure shows an example of the OTSig connection with Link Span parameter.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-25 Example Infrastructure Connection – OTSig Tunnel – Link Span



The Link Span parameter can be viewed from Equipment Manager **Port Details** and **Configure** tab as shown in the following figures.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-26 Equipment Manager – Port Details tab

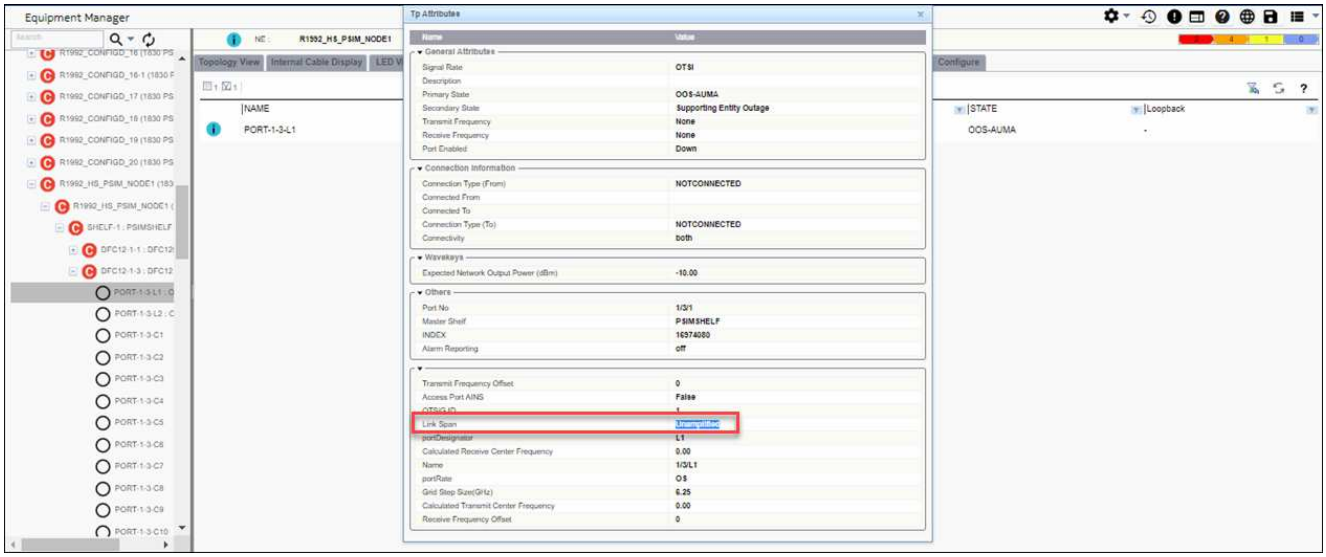
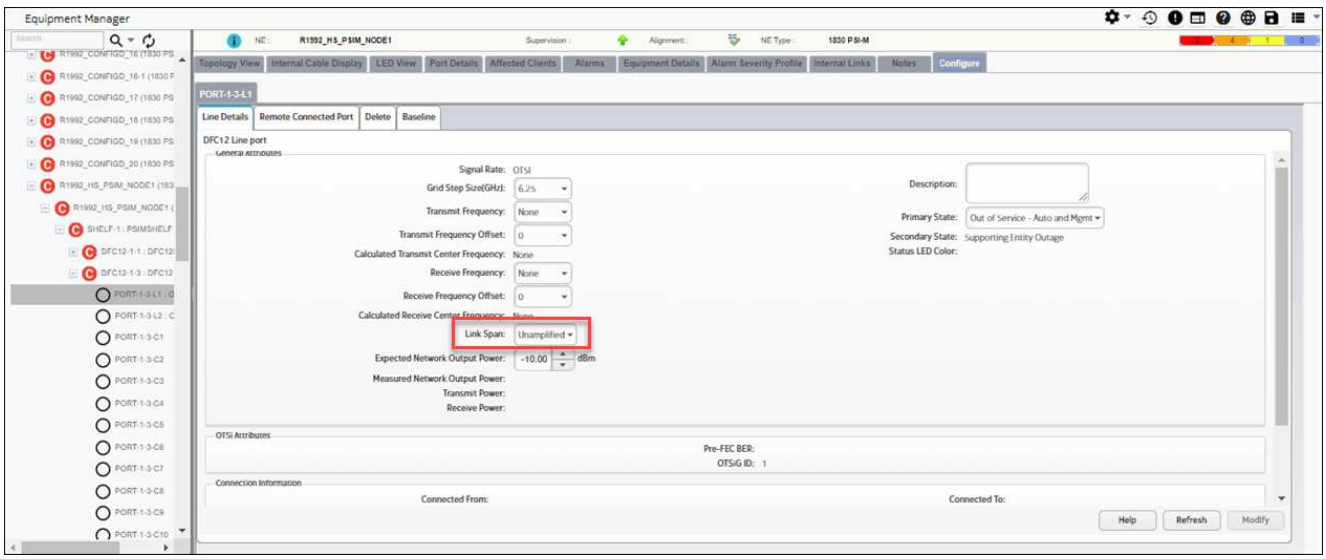


Figure 8-27 Equipment Manager – Configure tab



Note: Link Span modification is allowed only on OTSig trail for the supported configurations.

Result: The Link Span parameter is set to *Unamplified*.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

27

Click on **PARAMETERS > ASSURANCE** tab.

In the **Alarm Profile** field, select **Enable alarm profile** to set the ASAP per port role and per layer rate. The alarm reporting is enabled.

The **Disable all alarms** sets the alarm severities to NR (Not Reported) on each port that is involved in the connection.

The **Use_NE_Values** does not allow the use of the ASAP feature; but, it does enable alarm reporting.

28

Click **CONTINUE**.

29

Optional: You can verify all your settings in the **SUMMARY** tab before deployment.

30

Click **DEPLOY**.

Result: The **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.

31

Optional:

Click **SHOW NEW CONNECTION(S)** to view the new connection.

Note: When an OTSiG Tunnel is created, *SHOW NEW CONNECTION(S)* page displays only the newly created OTSiG Tunnel and not the OTSiG Trail.

Or

Click **BIDIRECTIONAL OPTICAL POWER** to view the Optical Power.

Result: The **SHOW NEW CONNECTION(S)** page displays the OTSig Tunnel created.

When an OTSig tunnel is created using the DFM6, DFM6E, SFM6, DD2M4 or S5AD400H card, the corresponding ODUC virtual server is also discovered as part of the Managed plane tunnel creation. It is not visible to the end user immediately upon tunnel creation. The ODUC virtual server can be seen after the first service is created using the particular tunnel. In case of Control plane ODUC is not displayed in the NFM-T user interface. Since ODUC becomes terminated to unterminated and is similar to ODU4 VS, ODUC4 will have Delete and DB delete options.

To view the ODUC Trail:

- Include the **Created By** column to the display, using the **Manage Columns** option.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Click the filter option corresponding to the **Created By** column, and select **System** check box.

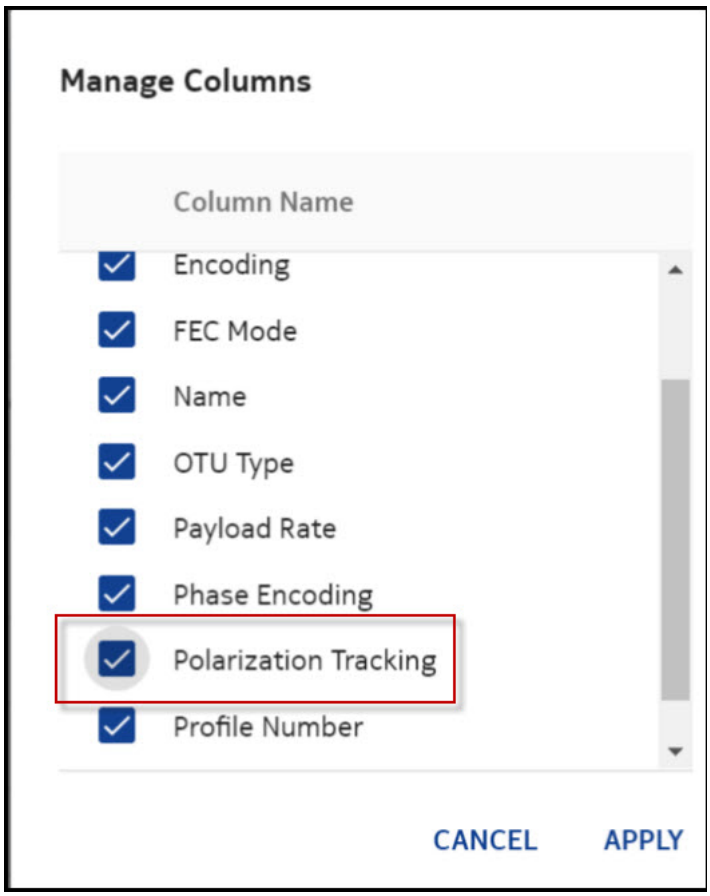
END OF STEPS

Enable the Polarization Tracking view in the Profile window

By default, the **Polarization Tracking** value is hidden in the in the **Profile Number** window. The user must perform the following procedure to enable the **Polarization Tracking** view in the **Line Mode Profile** window.

Complete the following steps to view the **Polarization Tracking** in the **Profile Number** window.

1. In the **Optical Line Characteristics** tab, click the **More** icon at the right end of the table header, click **Manage Columns**.
2. Enable the **Polarization Tracking** check box and click **APPLY**.



The **Polarization Tracking** column is added to the **Line Mode Profile** window with the possible values listed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task: To create a protected ASON OTSig trail

Perform the following steps to create a protected ASON OTSig trail.

1

From the WebUI, navigate to **DEPLOY > New Service/Infrastructure Connection**.

2

Select **/Best Practices/Infrastructure Trail/Unprotected** with **ODUk or OTSiG Tunnel** and click **Deploy** ( ) button.

Result: The system displays the **Connection** creation page with the **DEPLOY RULES** section selected.

3

In the **Rate** field, select **OTSig Tunnel**.

The **Connection Type** field is automatically set to **2 Ended Bi (I)**.

Result: The **OPTICAL LINE CHARACTERISTICS** pane is enabled.

4

In the **From Node #1**, **To Node #1**, **From Port #1**, and **To Port #1** fields, click the search icon to display the list of available Nodes and Ports. Select the required nodes and ports.

5

In the **CONNECTION CHARACTERISTICS** panel, ensure the following:

- Select the **Protection** check box for OCHP protected connection.
- Select the **ASON** check box.
- Set the **Provisionable Wave Key** to **Keyed**.

6

Click **CONTINUE**.

Result: The **SUMMARY** tab is displayed.

7

Click **DEPLOY**.

Result: An OCHP protected OTSig trail is created.

8

Click **SHOW NEW CONNECTIONS** to view the connection. Click the **Routing Display** icon to view the end-to-end routing display for the connection.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: OTSig 3R configuration is not supported for OCH Protected OTSig tunnel over L0 CP network.

Reference:

- See 8.11.12 " Task: To Modify the route of OTSig Tunnel" (p. 1337) and 7.63 "Modify Route (Reroute) of a connection" (p. 987) for **Reroute**.
- See 10.44 "Switch SNC routes" (p. 1560) for **Switch SNC Routes**.
- See 7.90 "Perform protection switching" (p. 1106) for **Protection Switching**.

END OF STEPS

Task: To delete a protected ASON OTSig trail

Perform the following steps to delete a protected ASON OTSig trail.

1

From the WebUI, navigate to **OPERATE > NPAs**.

2

Select the NPA, click the corresponding **360^0 View** icon and select **LINKS** tab.

Result: The system displays the **LINKS** associated to the OTSig trail.

3

Select the link associated to the OTSig trail from the list and click the corresponding **More** icon.

4

Click **Administrative State** and then select **set to Locked**.

Result: A warning message is displayed.

5

Click **YES** to continue the lock operation. Alternatively, click **NO** to terminate the operation.

Result: The selected link is set to locked.

6

To delete the associated OTSig trail, from the WebUI, navigate to **OPERATE > Infrastruture Connections**.

7

Select the required OTSig trail from the list.

8

Click the corresponding **More** icon.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: A confirmation message is displayed.

9

Click **YES** to continue. Alternatively, click **NO** to terminate the operation.

Result: The selected OTSig trail is removed from the system.

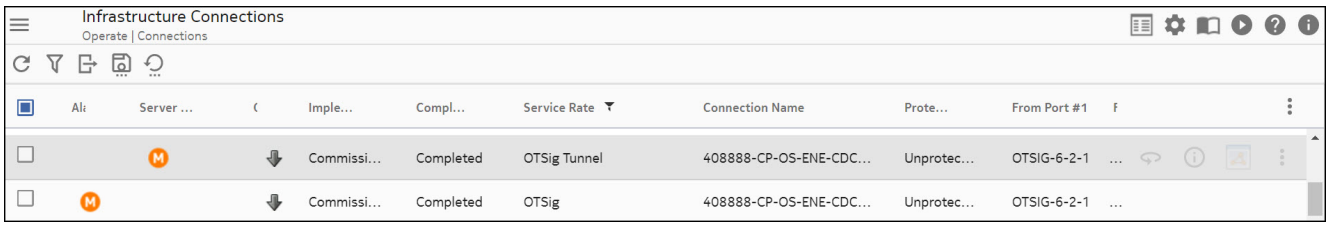
END OF STEPS

Task: To view OTSig Tunnel, Rate, Servers, SNCs

1

Navigate to **OPERATE > Infrastructure Connections** window.

Figure 8-28 OTSig Tunnel Control Plane Connection



Result: The connection with OTSig Tunnel along with OTSig Trail is displayed.

For 400 GbE connections, ODUC4 trail is discovered along with OTSig Tunnel and OTSig trail in Managed Plane connections.

Note: For Control Plane connections, filter the infrastructure connection with **OTSig Tunnel** as the **Service Rate** and **Category** as **ASON MRN Tunnel**. The infrastructure connection with **OTSig** as the **Signal Rate** and **Category** as **ASON Implicit Server** is automatically created.

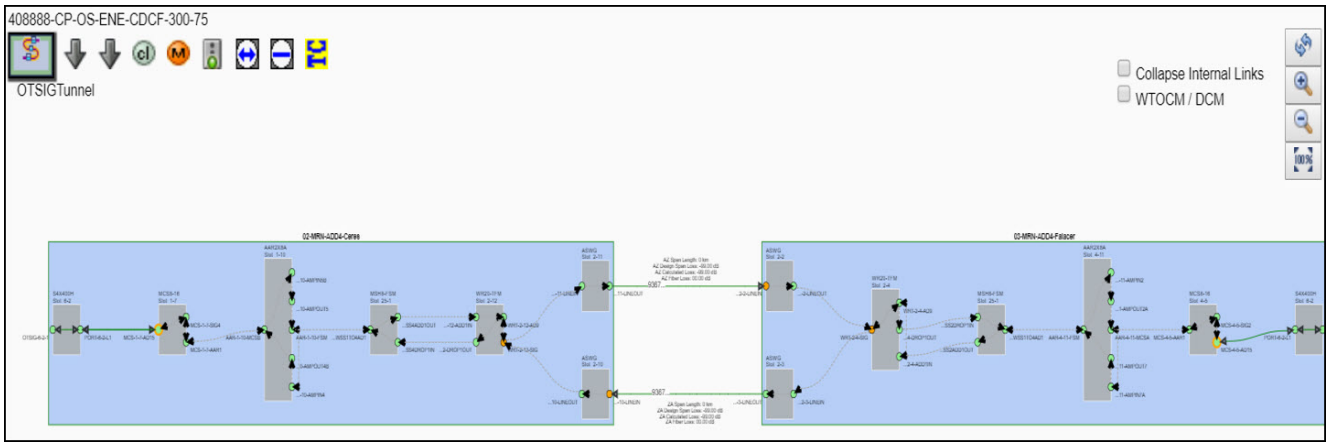
2

Select the OTSig tunnel connection and click the **Routing Display** icon.

Result: The **Routing Display** is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-29 OTSig Tunnel Routing Display



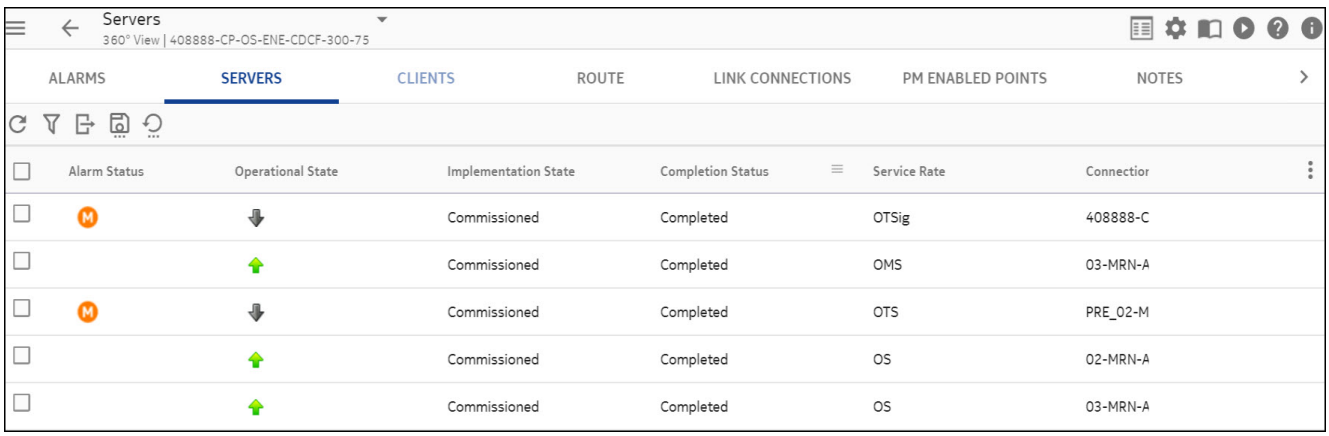
3

Select the OTSig tunnel connection and click the **360° View** icon

Result: The **360° View** tabs are displayed.

Select the **Servers** tab to view the associated servers with Service Rates.

Figure 8-30 Servers tab of OTSig Tunnel



4

Select the **LINK CONNECTIONS** tab to view the channels with the **Effective Rate**. Based on the variable Profile Number selected during tunnel creation, the underlying channels are displayed accordingly.

For example, if the Profile Number selected was 2, there are two ODU4 channels with 100G capacity.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: For MRN Tunnel, OPS link as iNNI and OTSIG tunnels are automatically assigned to NPA.

Result: The number of Link Connections for that particular connection is displayed.

For Control Plane connections, the **State** columns displays **Reserved for ASON**.

For example, if the Profile Number selected was 2, there are two ODU4 channels with 100G capacity.

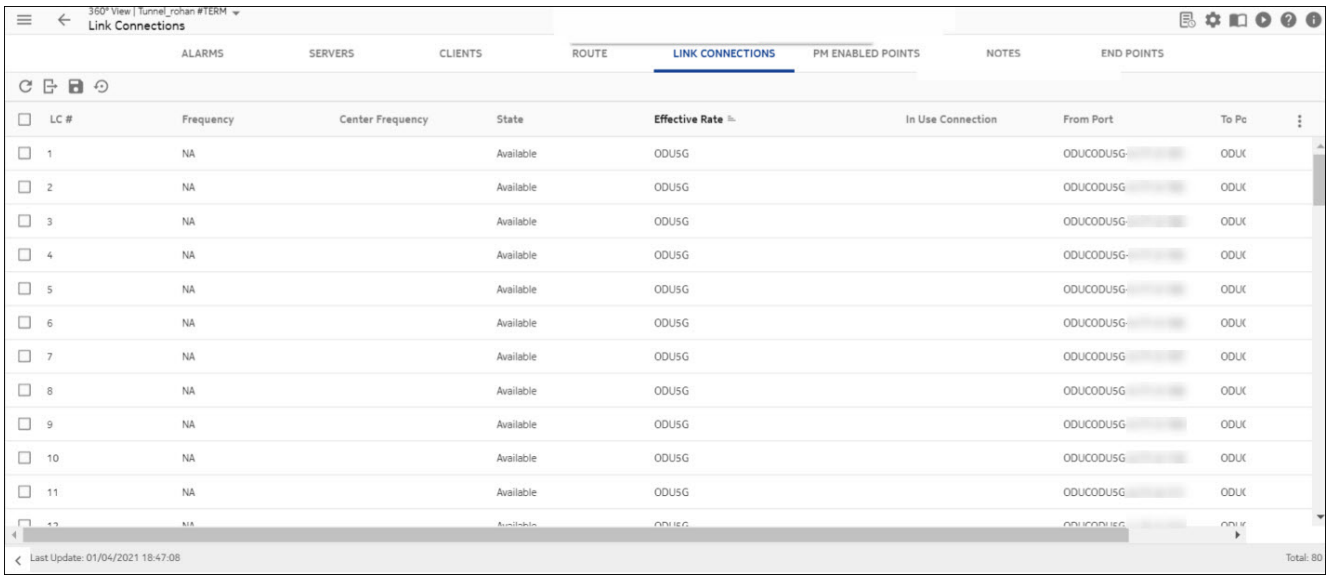
Based on the Profile Type selected on S5AD400H card, the options in the **OTU Type** field changes.

- Profile Number 2 supports OTU4 mode. The **LINK CONNECTIONS** tab displays two 100 GbE ODU4 connections after the tunnel is deployed.
- Profile Number 4 supports either OTU4 and OTUC4 mode. The **LINK CONNECTIONS** tab displays two ODU4 connections after the tunnel is deployed.

  If the Profile Number selected is 4 and OTU Type selected is OTU4, the **LINK CONNECTIONS** tab displays four 100 GbE ODU4 connections after the tunnel is deployed.

  If the Profile Number selected is 4 and OTU Type selected is OTUC4, The **LINK CONNECTIONS** tab displays one 400 GbE ODUC4 and 80 ODU5G connections after the tunnel is deployed.
- Profile Number 20 supports OTU4 mode. The **LINK CONNECTIONS** tab displays two ODU4 connections after the tunnel is deployed.
- Profile Number 21 supports OTU4 mode. The **LINK CONNECTIONS** tab displays three ODU4 connections after the tunnel is deployed.
- Profile Number 26 and Profile Number 27 supports ODUTC1 for 100 GbE, and ODUTC4 for 400 GbE connections.
- Profile Number 29 supports ODU4 for 100 GbE and ODU4 NNI connections.

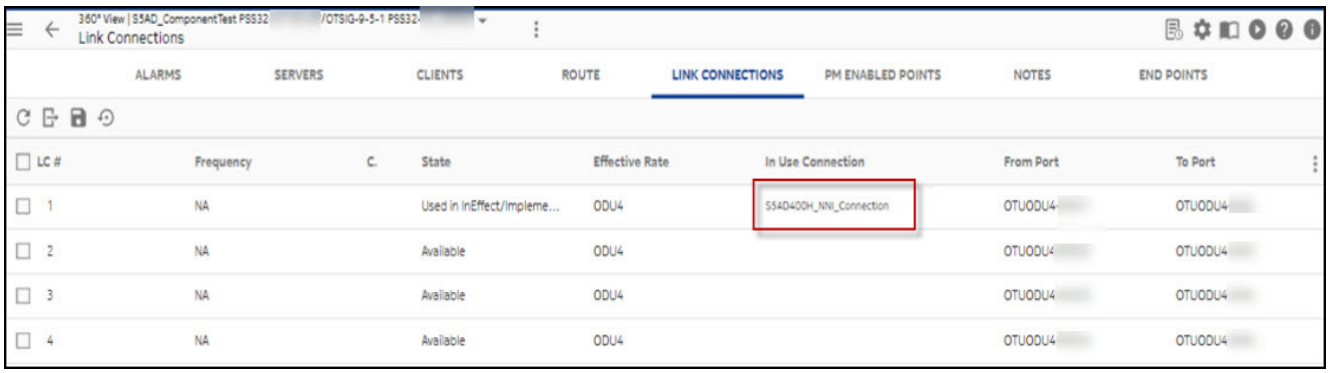
Figure 8-31 Link Connections tab for ODUC4 mode



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

For S5AD400H card, the **In Use Connection** displays the associated OTU4 NNI service.

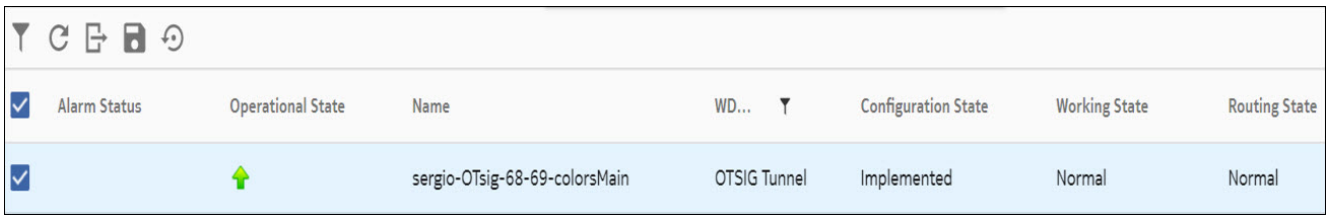
Figure 8-32 Link Connections tab for S5AD400H with OTU4 NNI service



5

For Control Plane Connections, select the **More** icon and select **ASON SNC** which is enabled.

Figure 8-33 OTSig Tunnel ASON SNC



Result: The list of SNCs are displayed.

6

Select the SNC and click the **More** icon and select **Routes**.

Result: The Nominal and Current Route are displayed.

END OF STEPS

Task: To create a Service on top of the OTSig

1

Navigate to **DEPLOY > New Service/Infrastructure Connection**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Select a **100G Ethernet** or **400G Ethernet** from the list of templates and click the **Deploy** icon.

For S5AD400H, select the template */Best Practices/Service/Transparent/Unprotected* to create a OTU4 NNI service. Click **Deploy**.

Result: The Connection window is displayed.

3

Select the client ports on both the ends.

The user has the option to create the following types of services:

- DSR client connection for the 100 GbE client (ODU4 container)
- ODU4 client connection for the OTU4 client

  For Control Plane connections, the ODU4 client connection for OTU4 client is supported with ENE.

  The OPS link from ENE to client must be assigned as Drop link in NPA before service provisioning.

  For S5AD400H card, the client ports displays C1, C2, C3, and C4 in the port selection list for an OTU4 NNI service.

  For ASON routed NNI service, ENE is mandatory and OPS between the client port and the ENE must be added to NPA as a drop link. The **Administrative State** must be set to **Unlocked** state.

  Note: ENE is not required for ASON routed UNI service.

  For OPSB protected service, all the OPSB related internal links must be added to NPA as Drop link. The **ASON Administrative State** must be set to **Unlocked** state.
- DSR client connection for the 400 GbE client (ODUC4 container)

4

Click **Deploy**.

5

Navigate to **OPERATE > Services** page to view the services riding on top of OTSig Tunnel.

Result: The list of 100 GbE or 400 GbE services are displayed.

Ensure to perform the following prior to deleting Tunnels or services

.

- MRN tunnel is locked by the user
- OPS between ENE and Client needs to be locked and removed from NPA.
- OPSB internal TLs also needs to be locked and removed from NPA.
- Port AID to create NNI service is "ODU4-PORT-shelf-slot-Client-1.

6

Navigate to **OPERATE > Infrastructure Connections** page.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: An ODUj connection with **Rate** as **ODUfex** is created.

The **5G Tributary Size** column indicates that the ODUflex is of 5G time slot. The supported values are N/A and True. If the ODUflex is not of 5G timeslot, the **5G Tributary Size** column remains empty or N/A.

Note: The **5G Tributary Size** is also displayed in **Clients** and **Server** tab of **Infrastructure Connections** page along with the **Show New Connections** page.

END OF STEPS

Task: To view the Parameter Mismatches for Link Span

Optional: Complete the following steps to view the Parameter Mismatches for Link Span.

1

Navigate to **Infrastructure Connections > 360^0 View > Servers**

2

Select the connection with Service Rate as **OTSig** trail and click the **More** icon.

3

Select **Modify Connections > Parameters**. The Modify Parameters widow is displayed.

4

On the **Transmission Parameters** pane, click **More Parameters > Mismatches** to view the Parameter Mismatches for Link Span.

Note: Any discrepancies between the **Link Span** values (**Current Value**, **From Port Discrepancy**, or **To Port Discrepancy**) of NE and NFM-T is displayed in the **Modify Transmission Parameters** window. For more details, see 7.112 "Parameter Mismatches" (p. 1161).

Note: Any discrepancy in the Transmission Parameters for the Dual carrier OTSIG Tunnel, specifically, the OTSIG tunnel with otustruct = L1 and L2, is shown for L1 port only. No discrepancy in Transmission Parameters is shown for port L2.

If the user performs a discrepancy of the Transmission Parameters on port L2 from NE ZIC, the OTSIG Trail connection is displayed in the **Parameter Mismatches** tab in the **Network Inconsistencies** screen, except the **Transmission Parameters Mismatch** tab in the **Modify Parameters** screen does not show any discrepancy between the parameters as the system shows Transmission Parameters discrepancy for port L1 only.

Task: To delete OTSig Tunnel and OTSigTrail from NFM-T database

Optional: Perform the following steps to DB Delete **OTSig Tunnel** and **OTSigTrail**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

1

From the WebUI follow the path **OPERATE > Infrastructure Connections**.

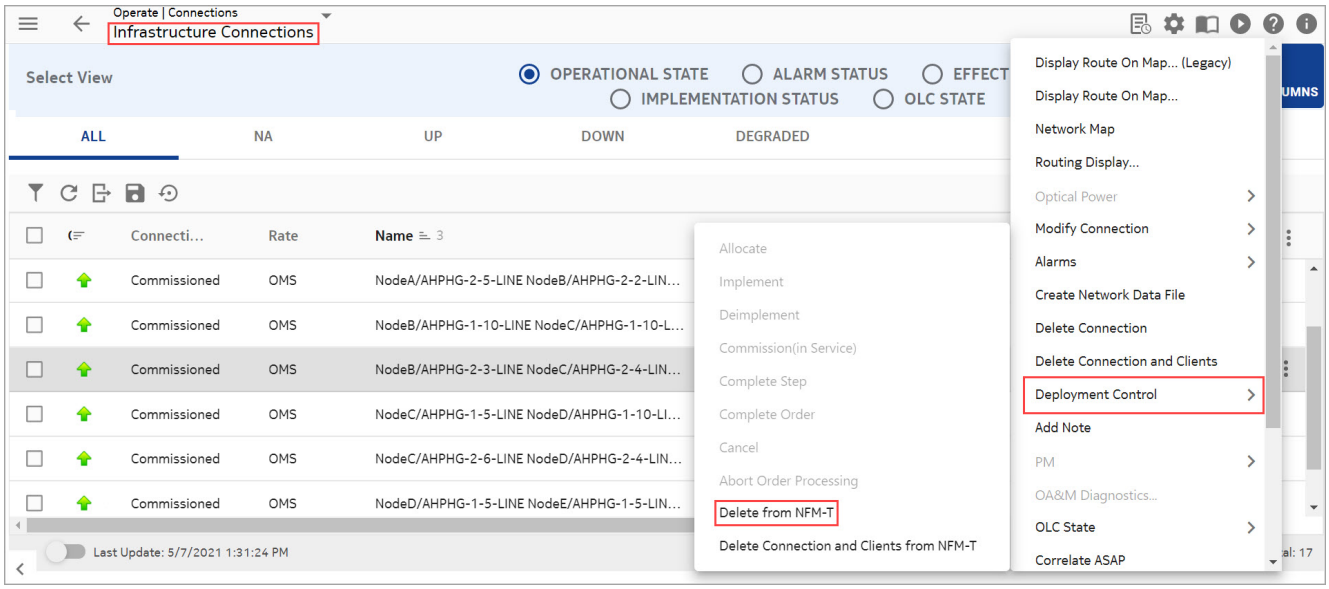
2

Select the tunnel with Service Rate as **OTSigTunnel** and **OTSig Trail** that needs to be deleted from NFM-T and click the corresponding **More** icon .

3

Select **Deployment Control > Delete from NFM-T** as shown in the following figure.

A confirmation message is displayed.



4

Click **OK** to delete the connection from NFM-T. Alternatively, click **CANCEL** to abort the operation.

Note: The DB Delete must be performed for **OTSig Tunnel** to delete both **OTSig Tunnel** and **OTSig Trail**. Removal of only the **OTSig Trail** is not allowed.

The **OTSig Tunnel** and **OTSig Trail** are deleted from the NFM-T database.

To discover the Managed Plane connections see 8.11.11 "Task: To discover the Managed Plane connection that is deleted from NFM-T database" (p. 1337).

To discover the Control Plane connections, see "ASON synchronization" (p. 1568).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task: To discover the Managed Plane connection that is deleted from NFM-T database

To discover the Managed Plane connection that is deleted from NFM-T database follow the steps:

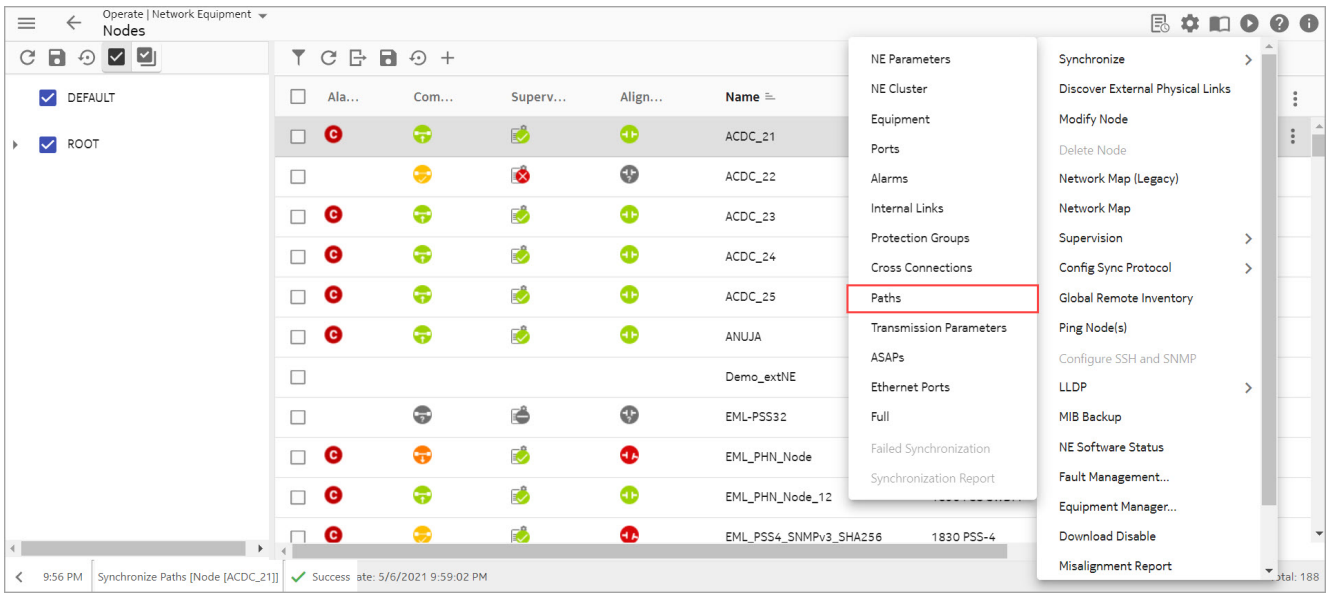
1

From the WebUI, follow the path **OPERATE > Nodes**.

2

Select a node and click the **More** icon and select **Synchronize > Paths** to perform the path synchronization as shown in the following figure.

Figure 8-34 Node Path Synchronization



3

Navigate to **OPERATE > Infrastructure Connections** to view the discovered **OTSig Tunnel** and **OTSig Trail** that are DB Deleted.

The connections that are deleted from NFM-T are discovered during path synchronization.

Task: To Modify the route of OTSig Tunnel

Perform the following procedure to modify the route of the OTSig tunnel for Managed Plane and Control Plane connections. See 7.63 “Modify Route (Reroute) of a connection” (p. 987) for more details.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

1

From the WebUI, navigate to **OPERATE > Infrastructure Connections**.

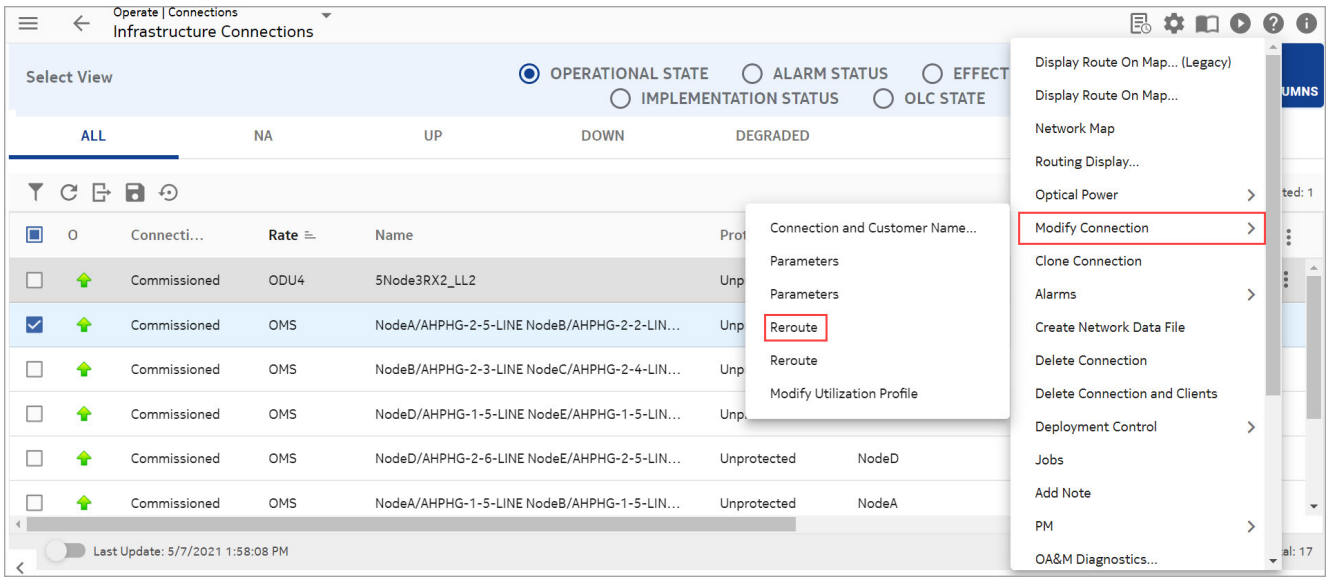
2

Select the connection with **Service Rate** as **OTSig Tunnel** and click the corresponding **More** ⋮ icon.

3

Click **Modify Connection > Reroute...**.

Figure 8-35 Modify Route



4

Optional: In the **DEPLOY RULES > CONNECTION CHARACTERISTICS** panel, select **ASON** checkbox for Control Plane connections.

5

In the **CONNECTION CHARACTERISTICS** panel, select the required **Routing Mode** (Automatic or Manual) from the drop-down.

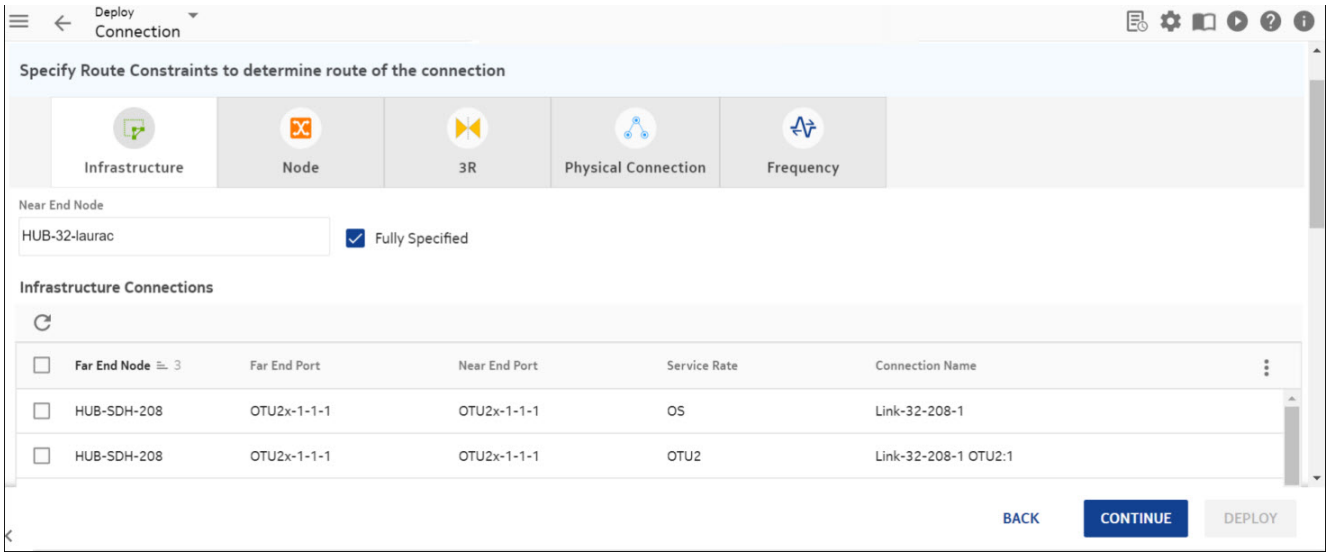
Note: For Control Plane connections, only Manual **Routing Mode** is supported.

6

Navigate to **ROUTE CONSTRAINTS** tab and choose the required routing constraints to perform the reroute operation. For more information, see "Routing Constraints" (p. 723) and 7.6 "Routing Constraints" (p. 731).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-36 Routing Constraints



The following tables provide the supported Routing Constraints and the respective parameters for OTSig tunnel for Managed Plane and Control Plane connections.

Table 8-17 Routing Constraints Supported for Managed Plane

Constraint	Manual Routing for OTSig Tunnel	Automatic Routing for OTSig Tunnel
Trail/Link Constraint	Yes	Yes
3R Constraint	Yes	Yes
Node Constraint	No	Yes
Physical Link Constraint	No	Yes

Table 8-18 Parameter Constraints Supported for Managed Plane

Parameter	Manual Routing for OTSig Tunnel	Automatic Routing for OTSig Tunnel
System Assigned Frequency	Yes	Yes
User defined frequency	Yes	Yes
Rearrange (Hard)	Yes	Yes
Rearrange (Soft)	No	No

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 8-19 Connectivity Constraints Supported for Managed Plane

Connectivity Constraint	Manual Routing for OTSig Tunnel	Automatic Routing for OTSig Tunnel
Full constraints	Yes	Yes
Partial constraints	Yes	Yes
Mixed constraints	Yes	Yes

Table 8-20 Routing Constraints Supported for Control Plane

Constraint	Manual Routing for OTSig Tunnel	Automatic Routing for OTSig Tunnel
Trail/Link Constraint	Yes	Yes
3R Constraint	Yes	Yes
Node Constraint	Yes	Yes
Physical Link Constraint	Yes	Yes

Table 8-21 Parameter Constraints Supported for Control Plane

Constraint	Manual Routing for OTSig Tunnel	Automatic Routing for OTSig Tunnel
System Assigned Frequency	Yes	Yes
User defined frequency	Yes	Yes
Rearrange (Hard)	Yes	Yes

Table 8-22 Connectivity Constraints Supported for Control Plane

Connectivity Constraint	Manual Routing for OTSig Tunnel	Automatic Routing for OTSig Tunnel
Full constraints	Yes	Yes
Partial constraints	Yes	Yes
Mixed constraints	Yes	Yes

See 8.11.13 “Task: To select frequency for 3R recoloring manually” (p. 1341) to manually select frequency for 3R recoloring.

7

Click **Deploy**. A warning message is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: When the reroute is stopped in the state other than **Commissioned**, the operation such as move forward, complete must be performed on the rearranged order with order number starting with R.

8

Click **OK** to continue the reroute operation. Alternatively, click **Cancel** to abort the reroute operation.

Note: After reroute operation is performed on the OTSig tunnel, default PM is enabled for the OTSig tunnel. Default PM includes selection such as 15-Min and 24-Hour PM with TP Monitoring Selection as All-points irrespective of the PM state prior to the reroute operation.

9

Optional: See 10.44 "Switch SNC routes" (p. 1560) to Convert **OTSig Tunnel** from **Current** to **Nominal** route.

Note:

- Conversion of **Current Route** to **Nominal Route** can be performed only on the rerouted Control Plane connections.
- The option **Modify Connections > Reroute...** is available for **OTSig Tunnel** only and not for the OTSig trail.
- When the OTSig tunnel is rerouted with 3R Regen changes, the user must **Enable NIM** or **Disable NIM** and **Modify PM** Disable and Enable All points as required for all the client connections that are riding on the rerouted OTSig tunnel.
- For Control Plane connections when Nominal Route and Current Route has two different frequencies, link connections associated to OPS physical connection displays the current route frequency and the OMS links display the Nominal Route frequency.

  The Nominal Route Routing Display indicates the current route frequency on the OPS or OS link connections and nominal route frequency on the OMS link connections. However, the OTSiG trail represents both the nominal and current route frequencies in the **Frequency** column of the **SERVERS** tab.

Task: To select frequency for 3R recoloring manually

By default, the frequency of the OTSig Tunnel is system assigned. You must select the frequency for 3R recoloring manually using **Map** or **Routing Constraints** tab of the OTSig Tunnel towards the left pane of the window. Perform the following steps to select the frequency for 3R recoloring using **Routing Constraints** tab.

1

From the WebUI, navigate to **OPERATE > Infrastructure Connections**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

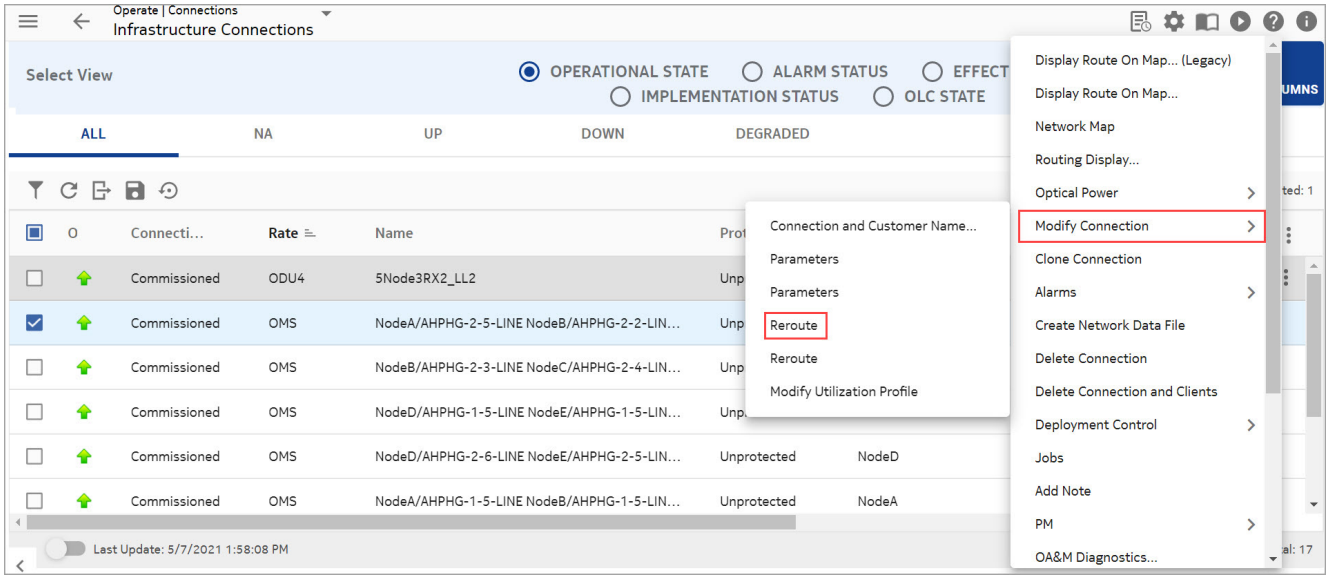
2

Select the connection with **Service Rate** as **OTSig Tunnel** and click the corresponding **More** icon.

3

Click **Modify Connection > Reroute...**.

Figure 8-37 Modify Route



4

In the **ROUTE CONSTRAINTS** tab of the OTSig Tunnel, select **Frequency** sub-tab. Uncheck the **System Assigned Frequency** option.

5

Select the required **Trail** or **Link**.

6

Click **Frequency Map**. The **Frequency Map** window is displayed.

Perform one of the following options to add individual frequency.

- Select one or more links from Route Constraint table and select **Frequency Map** to choose frequency. The selected frequency is displayed in the Routing Constraints table and Frequency column. If all the links are not selected, then the system determines the remainder based on the existing entry.
- In the Routing Constraints table, under frequency column, enter the frequency.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Select the Link or Links in Routing Constraints table and enter the frequency in **Frequency** field below **Frequency Map**.

7

Click **Deploy**.

8

Click **OK** to continue the reroute operation with the selected 3R recoloring frequency. Alternatively, click **Cancel** to abort the reroute operation.

For more information on **Modify Route** procedure, see 8.11.12 " Task: To Modify the route of OTSig Tunnel" (p. 1337).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.12 Deploy a Disjoint Service

Purpose

This feature explains the deployment of a disjoint service and the support of SRG Diversity in Managed Plane connection for of 4-Ended Double Simple (II) connection shape. The 4-ended service end points can be either on 1830 PSS, 1830 PSD, or 1830 ONE NEs. The 4 Ended Double Simple Bi (II) connection shape is supported for all UNI and NNI protected services.

This features supports the following scenarios:

- A 4-ended service shape where the 2 independent legs are set with a single Service Deploy action
- Disjointness between the two legs is based on a combination of SRG diversity, node diversity, and physical link diversity

The 4-Ended service is created as two disjoint links, but is inventoried/displayed in the NFM-T protected services list as a single disjoint connection. The end points are on two different NEs.

The Diversity Rule parameters provides the following three options:

- Enforce SRG And Node Diversity
- Enforce SRG Diversity
- Link diversity

Note: If the user modifies the SRGs of the existing physical connection which has clients riding over it after service deployment, then the modification impacts the Diversity Rule. Such services are listed under Impacted Client connections.

Related information

See

- 8.3 “Service or infrastructure connection template” (p. 1217)
- 7.19 “Create an OTN physical connection” (p. 784)
- 6.4 “Create a SRG” (p. 605)

Before you begin

Ensure that at least two OPS Physical Connections are available.

Creation of SRG

To create and manage an SRG, see 6.4 “Create a SRG” (p. 605).

Creation of Physical Connection

To create an OPS or OTS physical connection, see 7.19 “Create an OTN physical connection” (p. 784).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Correlate an SRG with a Physical Connection

To correlate an SRG with a Physical Connection6.6 "Correlate a SRG with a Physical Connection" (p. 610)

Deploy a 4-Ended Double Bi (ii) service

Complete the following steps to deploy a 4-Ended Double Bi (ii) service.

1

From the WebUI, 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 following template: */Best Practices/Services/Ethernet/Unprotected/Full Rate*.

3

Click **Deploy** ( ) button on the selected template.

Result: The **Connection** window is displayed with **DEPLOY RULES** section selected by default.

4

From the **END POINT SELECTION** panel:

1. The **Service Rate Type** parameter is automatically is set based on the type of template selected. Example: `100G Ethernet`.
2. The **Rate** parameter is automatically set based on the type of template selected. Example: `10 GbE`.

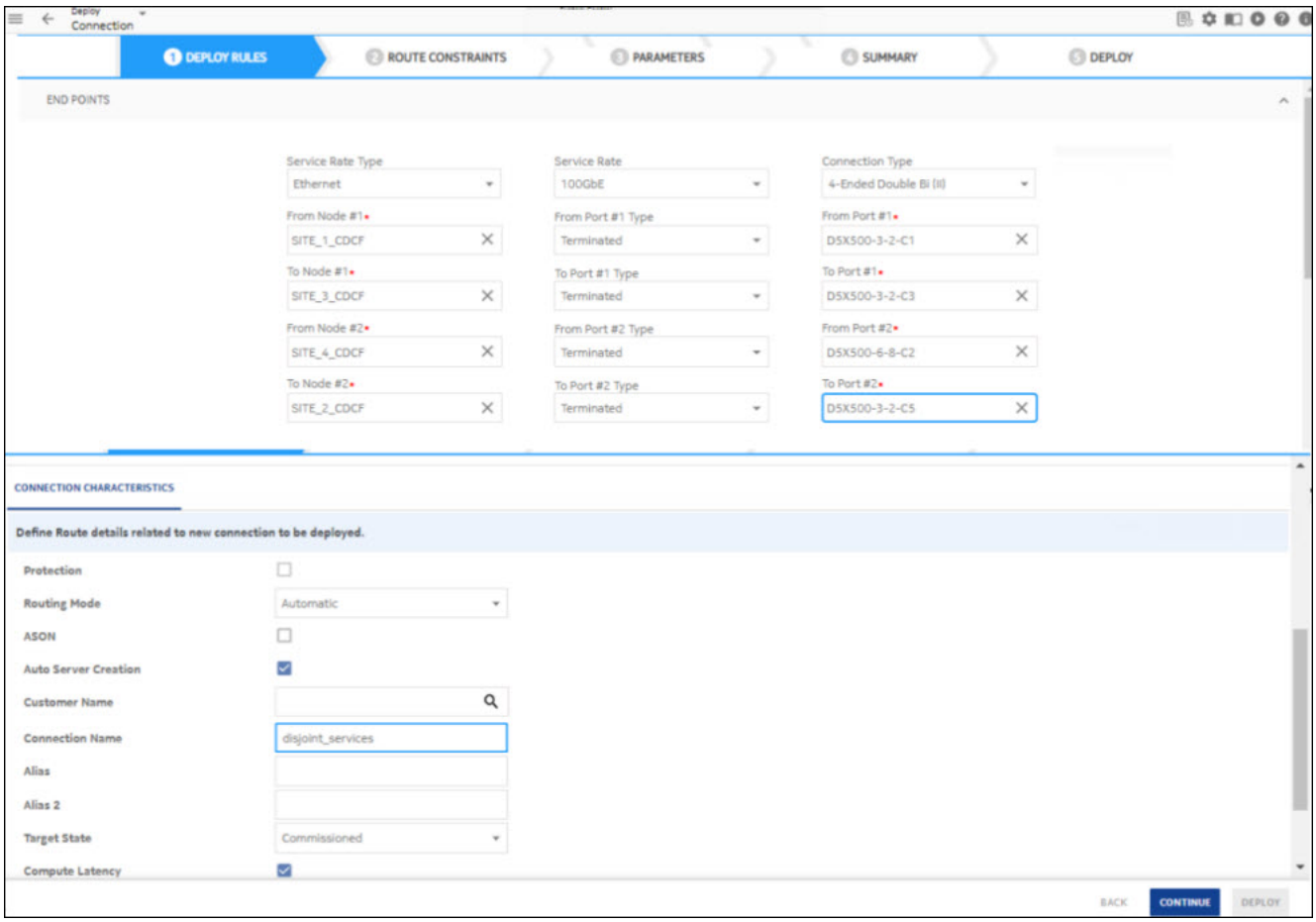
   Depending on the selected signal rate, configuration of other parameters may vary.
3. Select **Connection Type** as `4-Ended Double Bi (ii)`

   Depending on the connection type selected, additional node name and port name fields are displayed.
4. Select **From Node #1**, **From Node #2**, **From Node #3**, and **From Node #4**. Select **To Node #1**, **To Node #2**, **To Node #3**, **To Node #4**.

   Select the nodes and ports for deployment by clicking the search icon and selecting the node or port from the list displayed in the lower pane. Or type the node or port name in the text box if you know which node or port to be used.
5. Select **From Port Type #1**, **From Port Type #2**, **From Port Type #3**, **From Port Type #4**. Select **To Port Type #1**, **To Port Type #2**, **To Port Type #3**, **To Port Type #4** as `Terminated`.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-38 Disjoint services port selection



5

In the **CONNECTION CHARACTERISTICS** panel, configure the parameters.

The **Protection** check box is grayed out by default.

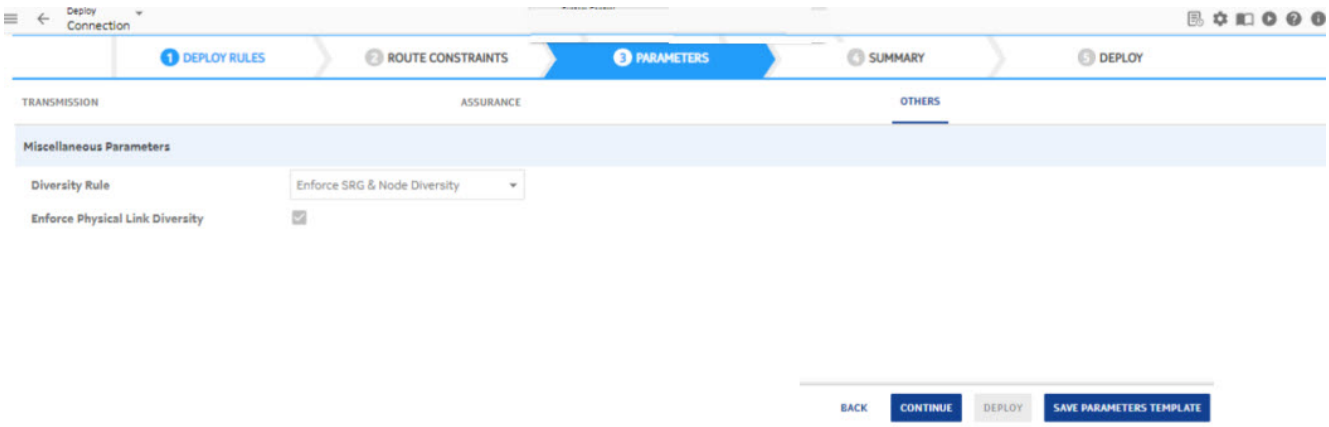
AutoServer Creation check box is selected by default.

6

In the **PARAMETERS** section, click the **OTHERS** tab.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-39 Disjoint Services parameters



Result: The **Diversity Rule** menus are displayed.

In the **Diversity Rule** field, select one of the following

- **Enforce SRG and Node Diversity**: Uses SRGs and Node if they are diverse to the provided diversity
- **Enforce SRG Diversity**: Uses SRGs only if they are diverse to the provided diversity constraints. node can be used for both legs (violate node diversity)
- **Link Diversity**: Uses SRGs only if they are diverse to the provided diversity constraints and allows SRG violations in the new route. A SRG violation alarm is raised in that case. SRG diversity can be violated and also node diversity.

When the user selects **Enforce SRG and Node Diversity** or **Enforce SRG Diversity**, the **Enforce Physical Link Diversity** is grayed out. If the user selects **Link Diversity**, the **Enforce Physical Link Diversity** is enabled.

- The **Enforce Physical Link Diversity** supports a way to relax link diversity for protected services. If selected, it indicates diverse working and protected paths for protected connections.
- if **Enforce Physical Link Diversity** check box is not selected, it indicates that it is used to override physical link diversity between working and protect paths as a method of last resort for protected connections

Click **SAVE PARAMETERS TEMPLATE** to save the template.

7

Click **CONTINUE**.

Result: The **SUMMARY** section is displayed

8

Click **DEPLOY**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Once the deployment is successful a success message is displayed at the bottom of the section.

Result: The **DEPLOY** section is displayed. As the deployment progresses, the progress bar increases in percentage and the states move from *Defined* > *Allocated* > *Implemented* > *Commissioned*.

9

Click **SHOW CONNECTIONS** to view the connections

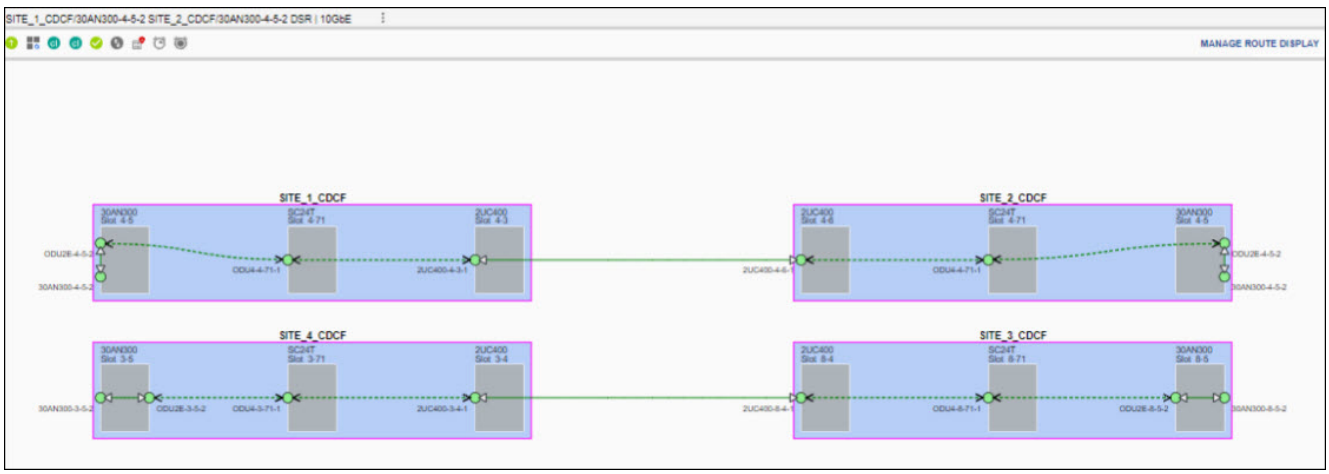
Result: The newly created connections are displayed.

10

Select the **Routing Display** icon to view the end to end routing display.

Result: Two independent routes are displayed.

Figure 8-40 Disjoint Services: Routing Display



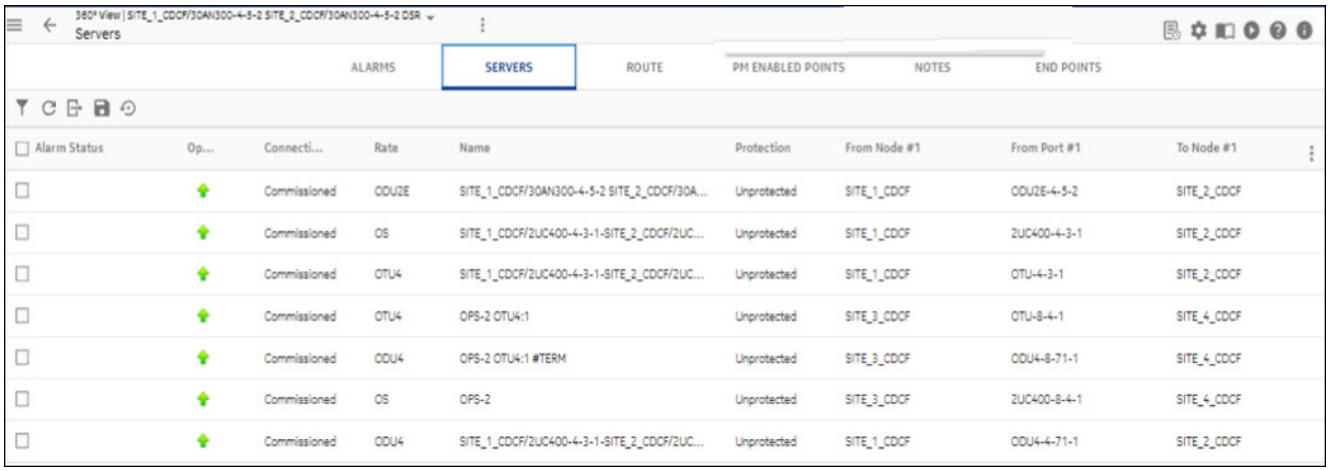
11

Select the connection and click the **360° View** icon. Select the **SERVERS** tab.

Result: The OPS physical connections involved in the route is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-41 Disjoint Services: Servers tab



Alarm Status	Op...	Connecti...	Rate	Name	Protection	From Node #1	From Port #1	To Node #1
		Commissioned	ODU2E	SITE_1_CDCF/30AN300-4-5-2 SITE_2_CDCF/30A...	Unprotected	SITE_1_CDCF	ODU2E-4-5-2	SITE_2_CDCF
		Commissioned	OS	SITE_1_CDCF/2UC400-4-3-1-SITE_2_CDCF/2UC...	Unprotected	SITE_1_CDCF	2UC400-4-3-1	SITE_2_CDCF
		Commissioned	OTU4	SITE_1_CDCF/2UC400-4-3-1-SITE_2_CDCF/2UC...	Unprotected	SITE_1_CDCF	OTU-4-3-1	SITE_2_CDCF
		Commissioned	OTU4	OPS-2 OTU4:1	Unprotected	SITE_3_CDCF	OTU-8-4-1	SITE_4_CDCF
		Commissioned	ODU4	OPS-2 OTU4:1 #TERM	Unprotected	SITE_3_CDCF	ODU4-8-71-1	SITE_4_CDCF
		Commissioned	OS	OPS-2	Unprotected	SITE_3_CDCF	2UC400-8-4-1	SITE_4_CDCF
		Commissioned	ODU4	SITE_1_CDCF/2UC400-4-3-1-SITE_2_CDCF/2UC...	Unprotected	SITE_1_CDCF	ODU4-4-71-1	SITE_2_CDCF

12

When the user performs **Compute Latency**, the first set of route is specified as working latency and the second set of leg is specified as protected latency. This is because there are two separate parallel routes for a single service.

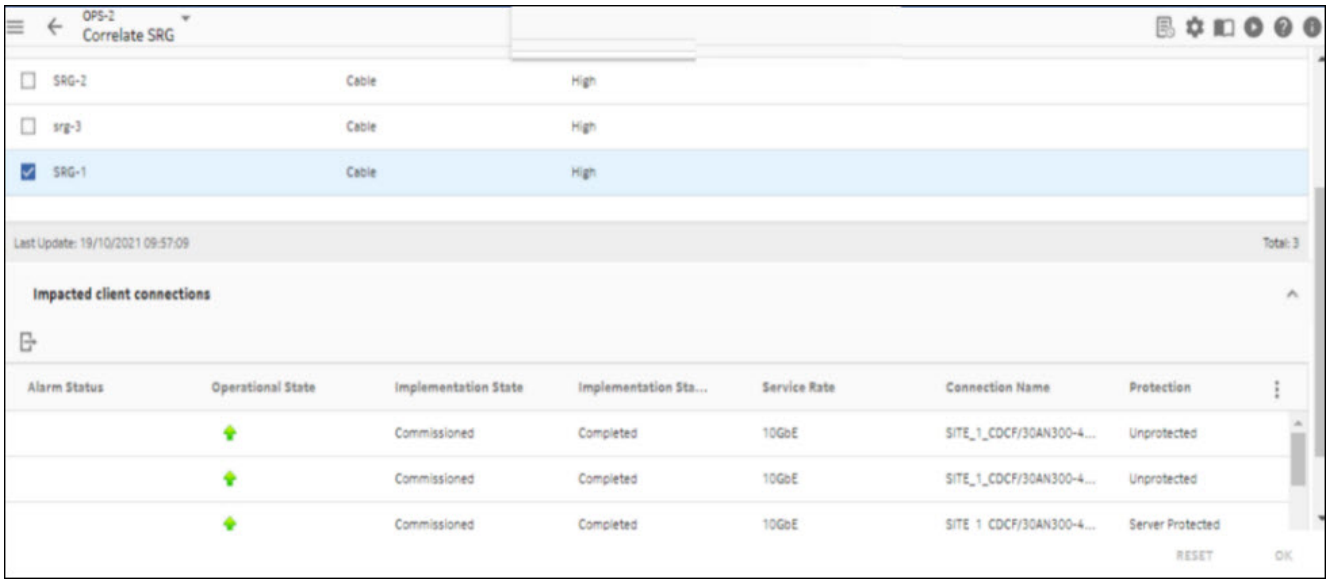
13

[Optional] If the user modifies the SRGs of the existing physical connection which has clients riding over it after service deployment, then the modification impacts the **Diversity Rule**. Such services are listed under **Impacted Client connections** panel of the **Correlate SRG** window. If the user tries to deploy the service with the same **Diversity Rule** after the SRG modification, the system displays the following error during deployment.

Route not found: likely due to the non-availability of SRG diverse path or Node diverse path.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-42 Impacted client connections



END OF STEPS

Multiple Diverse Paths

When there are multiple diverse paths available, the path with shortest route will be picked. When there are two or more paths with the same number of hops, the path that is returned by the system first will be picked. If no alternate diverse path is available for protection, creation will fail saying that system cannot find the route that is fully diverse from working leg.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.13 Create ASON hairpin service

Overview

ASON hairpin service is a connection which has the ason termination points on same node (single node in GMRE domain).

The two termination points in the GMRE node located on:

- the same card
- two different cards of the same shelf

Purpose

Use this task to create a hairpin service.

Steps

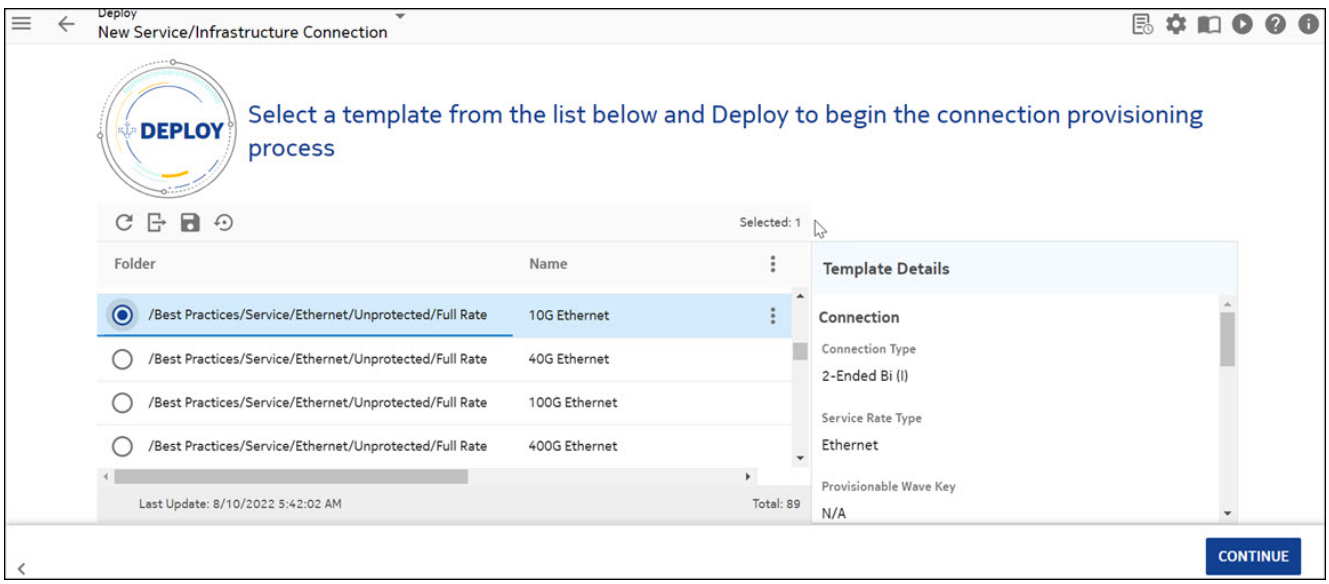
Perform the following steps to create a hairpin service:

1

From the NFM-T GUI, navigate to **DEPLOY > New Service/infrastructure Connection**.

Select **/Best Practices/Service/Ethernet/Unprotected/Full Rate**, **Gigabit Ethernet**, and click **CONTINUE**.

Figure 8-43 Connection provisioning



Result: The system navigates to the **Connection** page.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

In the **DEPLOY RULES** section, select:

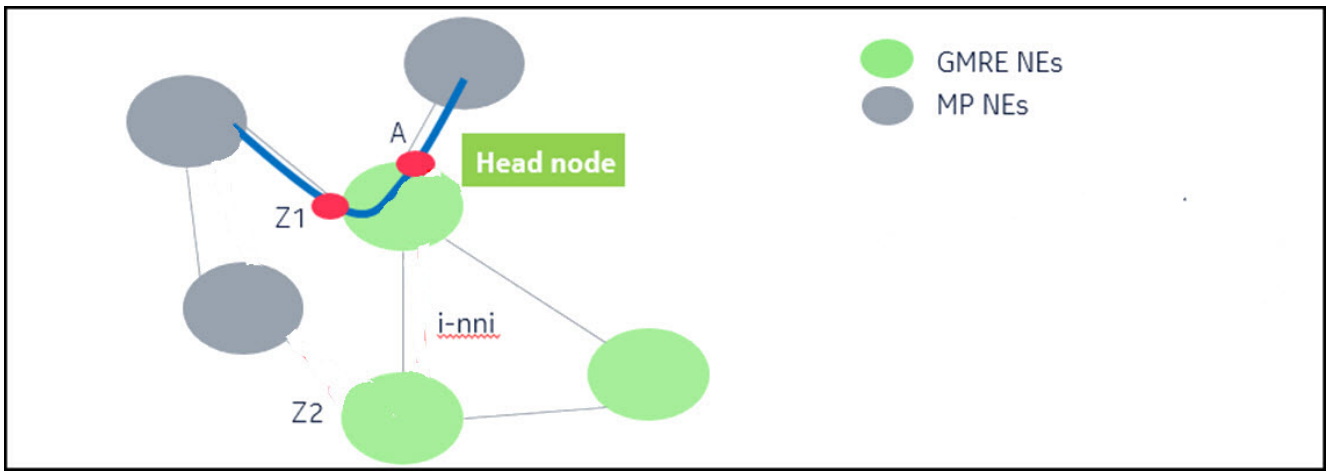
- **Service Rate Type**: Ethernet or Transparent
- **Service Rate**: Select a rate
- **Connection Type**: 2-Ended Bi (I) (default value)
- Select the two nodes at the ends of the connection, using the fields **From Node #1** and **To Node #1**.
- In the **From Port #1** and **To Port #1** fields, click the magnifier icon to display the list of the available ports. Select the ports.

Note: This procedure is for creating a GBE service. For other types of clients, proper values for **Service Rate Type**, **Service Rate** must be selected.

Notes: The termination points (ports) can be:

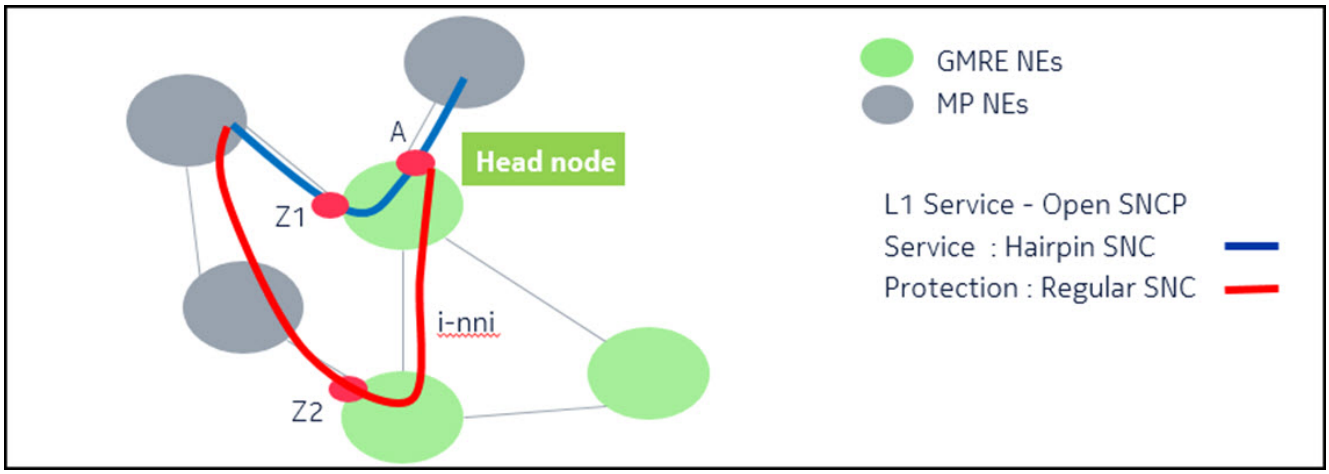
- two ports of the same card on a shelf.
- two ports of two different cards on a shelf

Figure 8-44 Unprotected hairpin



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-45 Protected regular SNC (Protected hairpin)



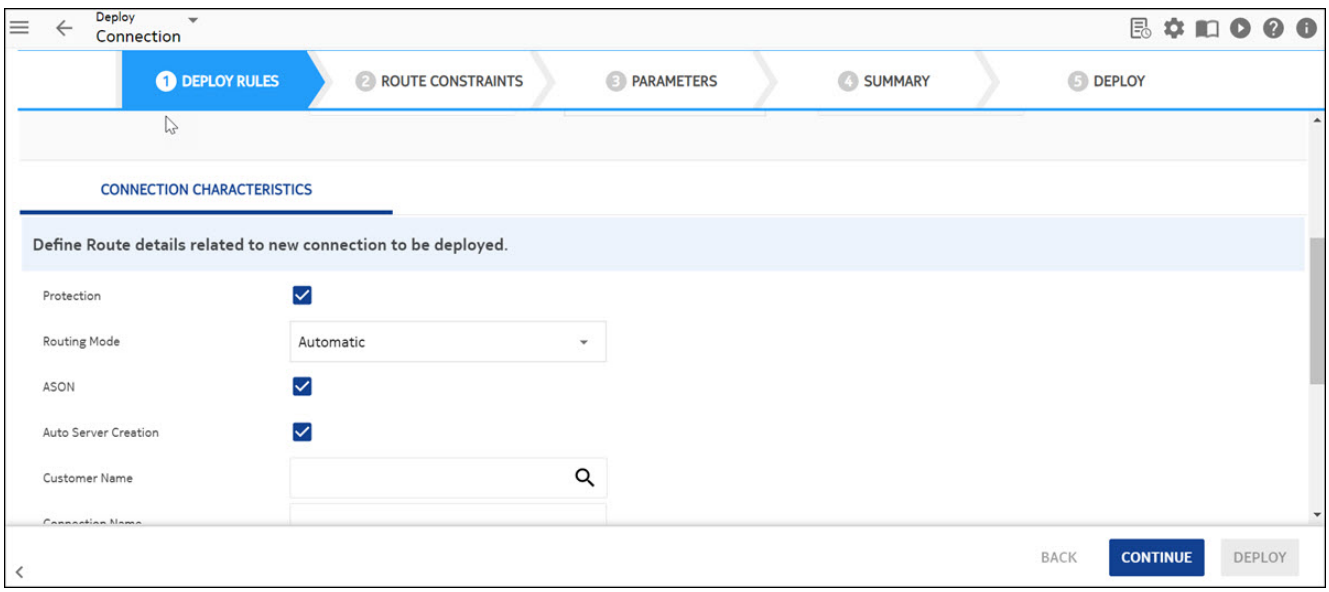
3

(Optional) In the **CONNECTION CHARACTERISTICS** section, you can add a custom name to the connection in the **Connection Name** field. If the field is kept blank, the connection name is assigned by the system.

4

Select **Protection** check box for a protected connection.

and select the **ASON** check box for a control plane connection.



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

Click the **SUMMARY** section to view all the details of the connection.

6

Click **DEPLOY** to deploy the connection.

Result: The **DEPLOY** section is displayed, showing the progress in the deployment of the connection.

7

Click **ROUTING DISPLAY** to view the routing display of the newly created connection.

Result: The system opens a new tab and displays the routing display for the selected connection.

Note: The service can also be discovered from the **OPERATE** > **Nodes** page. From the selected node, click the **More** icon, and then navigate to **Synchronize** > **Paths**.

8

Navigate to **OPERATE** > **ASON SNCs**. For unprotected hairpin ASON SNCs, the restoration mode will always be *No Restoration*. If the user tries with a restoration mode other than *No Restoration*, the SNC will still be created with "No Restoration" only.

Notes: Protected hairpin connection:

- Open SNCP rules are applicable for a protected connection.
- For the unprotected hairpin, reroute is supported only on the Managed plane segment.
- Protected hairpin is managed with open SNCP. The Protected hairpin can only be open SNCP connection. The user must select open SNCP check box to create protected hairpin connection.
- Double hairpin connection is not supported in Control plane.
- Open SNCP rules are applicable for the modify connection of the protected hairpin.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8.14 Interworking configuration in OTN for ADD4 cards

Before you begin

Ensure the required cards are provisioned and the NEs and ports are configured.

The following are supported.

- ADD4 cards: S4X400H, DFC12, DFC12E
- I/O cards: 10AN1T, 4AN400, 4MX200, 4MX400
- NE types: 1830 PSS-32, 1830 PSS-24X, 1830 PSS-12X, 1830 PSS-8
- Keyed and Unkeyed services
- Cluster or Dangling OT configurations, Symmetric and Asymmetric
- Client Service: 1 G, 10 G, OTU2, 100 G, OTU4, STM-64 (all service protections are supported on 1830 PSS-NX cards)
- Protection types Supported/covered: ODU SNCP, Y-Cable, and OPSB

Purpose

To configure and support OTU4 interconnect between 10AN1T/4AN400 and S4X400H/DFC12/DFC12E cards on MRN, L1 GMPLS, and Managed Plane Logical Link configurations.

References

For more information on connections, see the following topics:

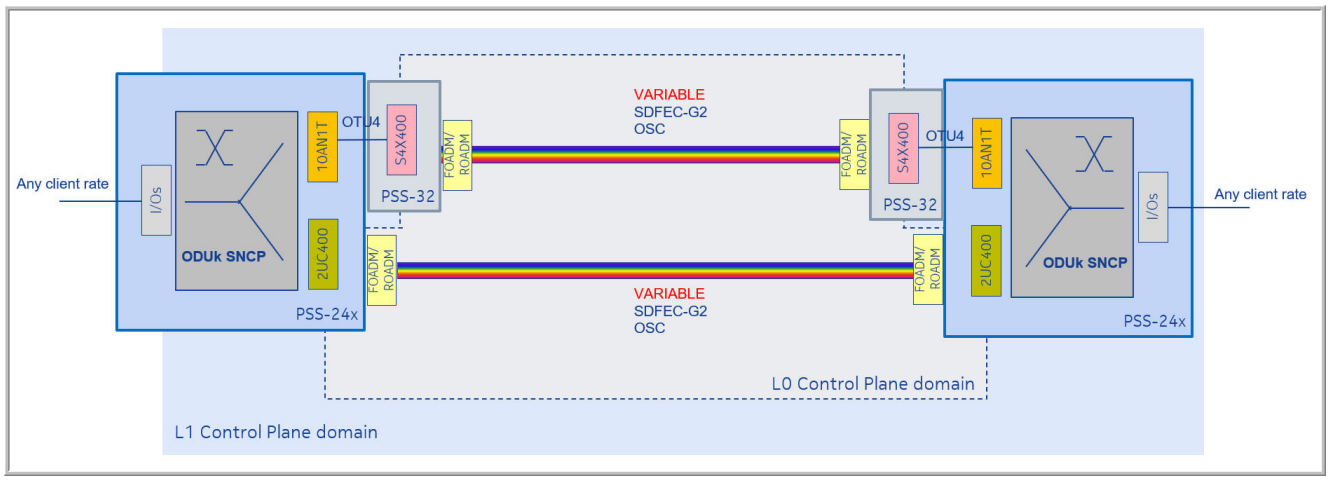
- 7.19 “Create an OTN physical connection” (p. 784)
- 8.11 “Manage an OTSig Tunnel ” (p. 1314)
- 10.15 “Add links and remove links from ASON” (p. 1462)
- 8.5 “Deploy a Managed Plane Connection” (p. 1271)
- 8.6 “Deploy an L0 Control Plane Connection” (p. 1278)
- 8.8 “Deploy a Service” (p. 1294)

1830 PSS-24X Logical Link and Services Setup

The following figure is an example that depicts the interworking configuration between 10AN1T and S4X400 cards.

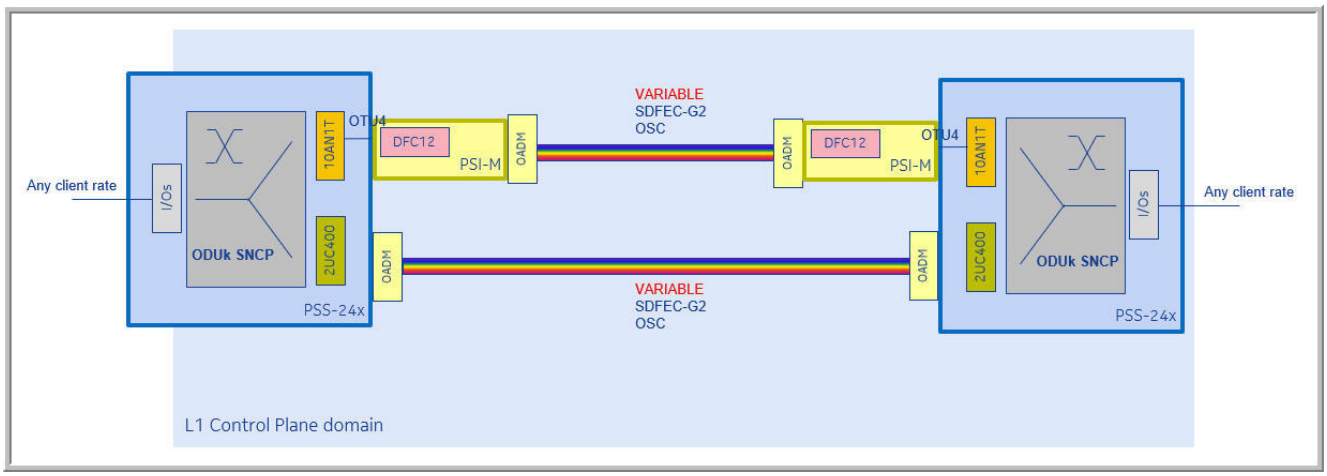
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-46 Interworking configuration between 10AN1T and S4X400 cards



The following figure depicts the interworking configuration between 10AN1T and DFC12 cards.

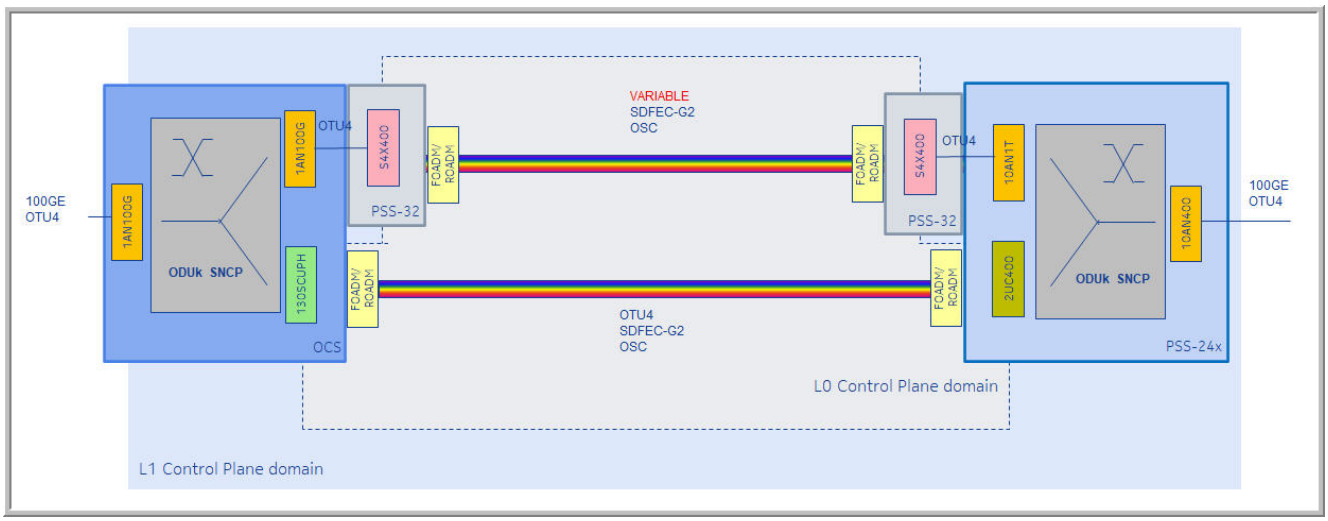
Figure 8-47 Interworking configuration between 10AN1T and DFC12 cards



The following figure depicts the interworking configuration between 10AN1T and S4X400 cards on different shelves.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-48 Interworking configuration between 10AN1T and S4X400 cards on different shelves



Example configuration for 10AN1T and S4X400 cards OTU4 interconnect on MRN GMPLS configuration

1

Create a physical connection (OPS) topology between 1830 PSS-32 S4X400 cards and filter cards on the A-end and Z-end.

Refer the image Figure 8-46, “Interworking configuration between 10AN1T and S4X400 cards” (p. 1356) for the connection setup.

Result: Physical connection (OPS) between the 1830 PSS-32 S4X400 cards are created successfully.

For more information, see 7.19 “Create an OTN physical connection” (p. 784).

2

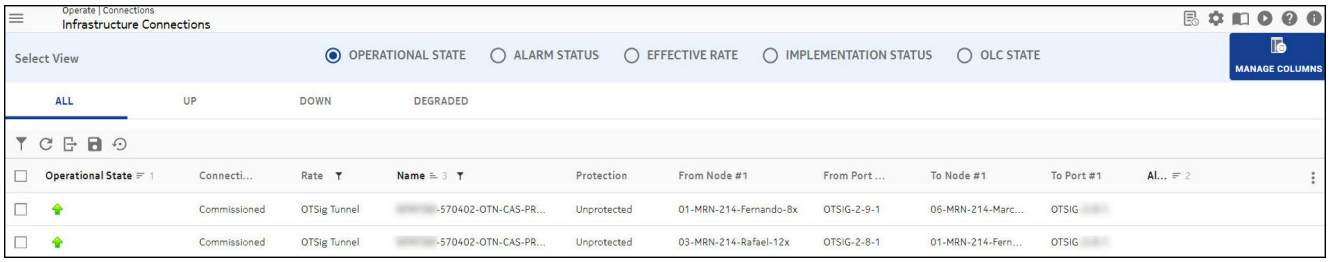
Create a MRN terminated OTSig Tunnel between the 1830 PSS-32 S4X400 cards on the A-end and the Z-end.

Select a **Profile Number** under **OPTICAL LINE CHARACTERISTICS** pane of the *Deploy* template.

Result: OTSig Tunnel is created successfully.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-49 OTSig Tunnel between the 1830 PSS-32 S4X400 Cards



For more information, see 8.11 “Manage an OTSig Tunnel ” (p. 1314).

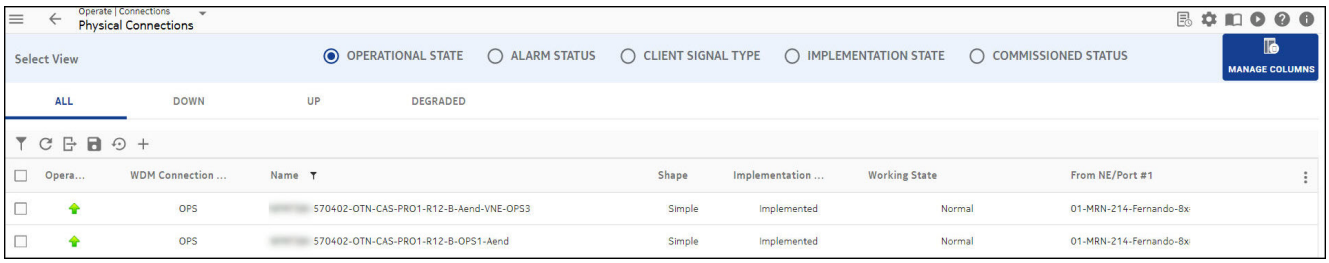
3

Create a physical connection (OPS) Drop link between the 10AN1T and 1830 PSS-32 S4X400 cards’ Client ports on A-end and the Z-end.

Note: If 10AN1T and S4X400 cards are added on the same node across different shelves, then create an internal OS between the same ports on A-end and Z-end.

Result: Physical connection (OPS) Drop link between the 10AN1T and the 1830 PSS-32 S4X400 client ports are created successfully.

Figure 8-50 Physical Connection (OPS) between the 10AN1T and the 1830 PSS-32 S4X400 Client Ports.



For more information, see 7.19 “Create an OTN physical connection” (p. 784).

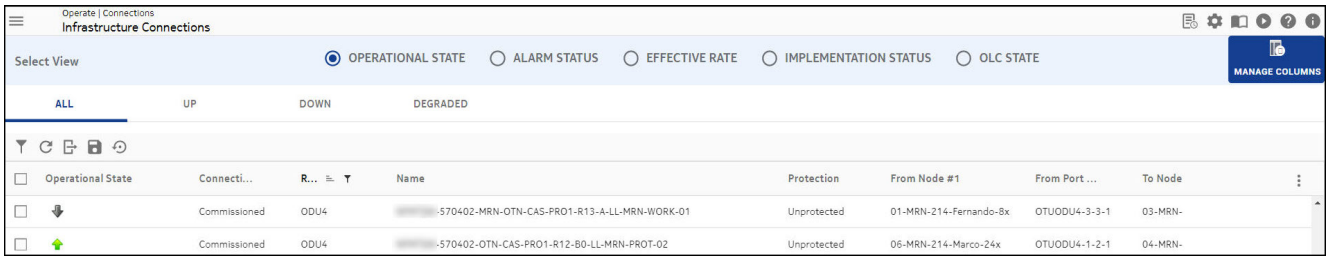
4

Create an ASON ODU4 Long Logical Link connection between the ports of 10AN1T cards on A-end and Z-end on the working path.

Result: ASON ODU4 Long Logical Link connection between the ports of 10AN1T cards are created successfully.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-51 ASON ODU4 Logical Link connection between the ports of 10AN1T cards



For more information, see 8.5 “Deploy a Managed Plane Connection” (p. 1271).

5

Assign the Drop link OPS/Internal OS to NPA.

To assign the Logical link to NPA and add I-NNI links, perform *Add Links to ASON* from *ASON NPA* page.

Ensure to *Unlock* the link added to NPA.

Result: The Logical link is added to NPA successfully.

For more information, see 10.15 “Add links and remove links from ASON” (p. 1462).

6

Create a ASON MRN Terminated Logical Link connection between the ports of 2UC400 cards with signal type as OTU4 on A-end and Z-end.

Note: For 2UC400 card with signal type as OTU4x2, creation of ODU4 MRN Terminated Logical Link between 2UC400 and 2UC400 is not supported unless there is OTSIG involved.

Result: ASON MRN Terminated Logical Link connection between the ports of 2UC400 cards are created successfully.

For more information, see 8.5 “Deploy a Managed Plane Connection” (p. 1271).

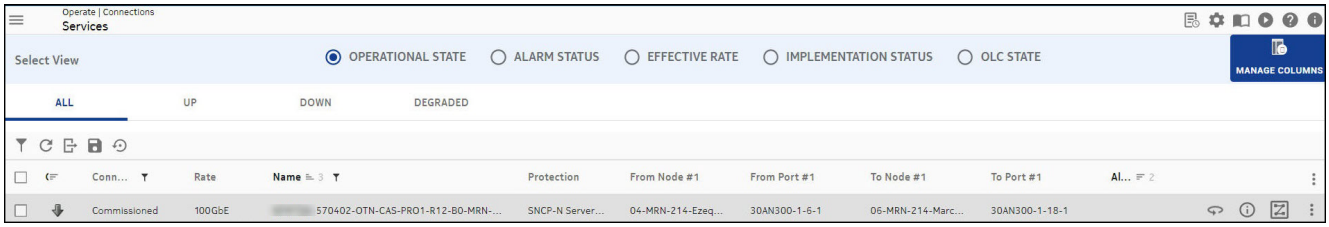
7

Create a 100 GbE ASON Routed service between I/O cards on the A-end and Z-end.

Result: 1000 GbE ASON Routed service between I/O cards are created successfully.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-52 100 GbE ASON Routed Service between I/O Cards



Note:

1. The following services can be created on top of a Long Logical Link connection:
   - OPSB service (UNI, NNI)
   - Protected service (UNI, NNI)
   - Unprotected service (UNI, NNI)
2. For NNI services, OPS should be created between VNE and I/O packs and same OPS needs to be added in NPA as drop link and should be unlocked.

For more information, see 8.8 “Deploy a Service” (p. 1294)

END OF STEPS

Example configuration for 10AN1T and DFC12 cards OTU4 interconnect on L1 GMPLS configuration

1

Create a physical connection (OPS) topology between 1830 PSI-M DFC12 (DFC12E card is also supported) cards and filter cards on the A-end and Z-end.

Refer the image Figure 8-47, “Interworking configuration between 10AN1T and DFC12 cards” (p. 1356) for the connection setup.

Result: Physical connection (OPS) between the 1830 PSI-M DFC12 cards are created successfully.

For more information, see 7.19 “Create an OTN physical connection” (p. 784).

2

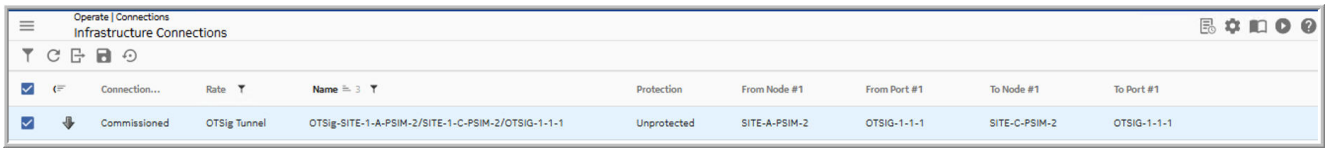
Create an OTSig Tunnel between the 1830 PSI-M DFC12 cards on the A-end and the Z-end.

Select a **Profile Number** under **OPTICAL LINE CHARACTERISTICS** pane of the *Deploy* template.

Result: OTSig Tunnel is created successfully.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-53 OTSig Tunnel between the 1830 PSI-M DFC12 Cards



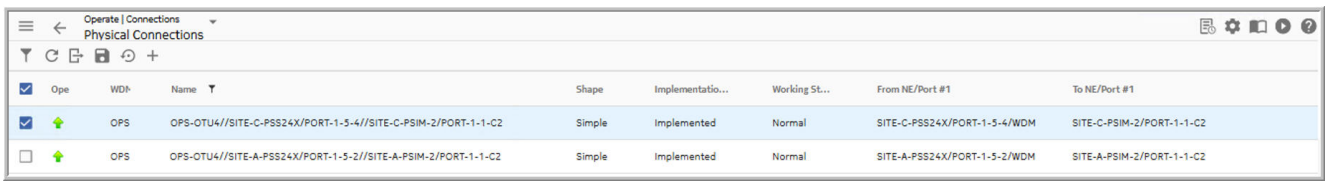
For more information, see 8.11 “Manage an OTSig Tunnel ” (p. 1314).

3

Create a physical connection (OPS) between the 10AN1T and 1830 PSI-M DFC12 cards’ Client ports on A-end and the Z-end.

Result: Physical connection (OPS) between the 10AN1T and the 1830 PSI-M DFC12 client ports are created successfully.

Figure 8-54 Physical Connection (OPS) between the 10AN1T and the 1830 PSI-M DFC12 Client Ports.



For more information, see 7.19 “Create an OTN physical connection” (p. 784).

4

Create a Managed Plane Non-Integrated Long Logical Link connection between the ports of 10AN1T cards on A-end and Z-end.

Note: Ensure the **Auto Server Creation** option is not selected under **CONNECTION CHARACTERISTICS** pane of the *Deploy* template.

Result: Managed Plane Non-Integrated Long Logical Link connection between the ports of 10AN1T cards are created successfully.

Figure 8-55 Managed Plane Non-Integrated Logical Link connection between the ports of 10AN1T cards

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

For more information, see 8.5 “Deploy a Managed Plane Connection” (p. 1271).

5

Assign the Logical Link to L1 Control Plane NPA.

To assign the Logical link to NPA, perform *Add Links to ASON* from *ASON NPA* page.

Ensure to *Unlock* the link added to NPA.

Result: The Logical Link is added to NPA successfully.

Note: In case of bundling of the TE Link, the Long Logical Link needs to be assigned in SRG while adding the link to NPA.

For more information, see 10.15 “Add links and remove links from ASON” (p. 1462).

6

Create an ODU4 Logical Link between 2UC400 and 2UC400 cards, and assign the Logical Link to NPA.

To assign the Logical Link to NPA, perform *Add Links to ASON* from *ASON NPA* page.

Ensure to *Unlock* the link added to NPA.

Result: ODU4 Logical Link is created between 2UC400 and 2UC400 cards and the Logical Link is added to NPA successfully.

For more information, see 10.15 “Add links and remove links from ASON” (p. 1462).

7

Create a 1000 GbE ASON Routed service between I/O cards on the A-end and on the Z-end.

Result: 1000 GbE ASON Routed service between I/O cards are created successfully.

Figure 8-56 1000 GbE ASON Routed Service between I/O cards

Note:

1. The following services can be created on top of a Long Logical Link connection:

- OPSB service (UNI, NNI)
- Protected service (UNI, NNI)
- Unprotected service (UNI, NNI)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2. For NNI services, OPS should be created between VNE and I/O packs and same OPS needs to be added in NPA as drop link and should be unlocked.

For more information, see 8.8 "Deploy a Service" (p. 1294)

END OF STEPS

Example configuration for I/O card and DFC12 card OTU4 interconnect on Managed Plane configuration

1

Create a cluster physical connection (OPS) topology between 1830 PSI-M DFC12 (DFC12E card is also supported) cards and filter cards on the A-end and Z-end.

Refer the image Figure 8-47, "Interworking configuration between 10AN1T and DFC12 cards" (p. 1356) for the connection setup.

Result: Cluster physical connection (OPS) between the 1830 PSI-M DFC12 cards are created successfully.

For more information, see 7.19 "Create an OTN physical connection" (p. 784).

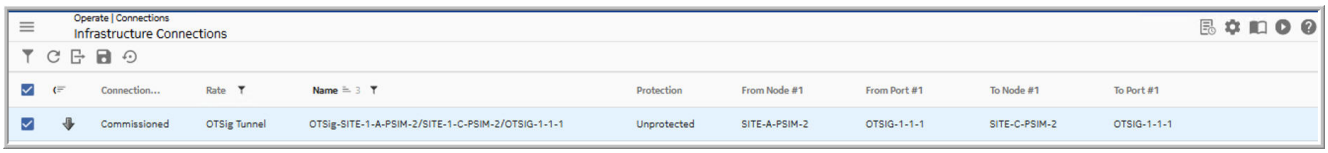
2

Create an OTSig Tunnel between the 1830 PSI-M DFC12 cards on the A-end and the Z-end.

Select a **Profile Number** under **OPTICAL LINE CHARACTERISTICS** pane of the *Deploy* template.

Result: OTSig Tunnel is created successfully.

Figure 8-57 OTSig Tunnel between the 1830 PSI-M DFC12 Cards



For more information, see 8.11 "Manage an OTSig Tunnel " (p. 1314).

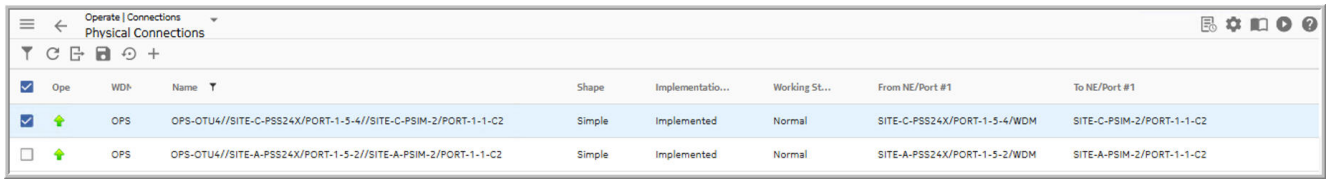
3

Create a physical connection (OPS) between the I/O and 1830 PSI-M DFC12 cards' Client ports on A-end and the Z-end.

Result: Physical connection (OPS) between the I/O and the 1830 PSI-M DFC12 client ports are created successfully.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-58 Physical Connection (OPS) between the I/O and the 1830 PSI-M DFC12 Client Ports.



For more information, see 7.19 “Create an OTN physical connection” (p. 784).

4

Create a Managed Plane Non-Integrated Long Logical Link connection between the ports of I/O cards on A-end and Z-end.

Note: Ensure the **Auto Server Creation** option is not selected under **CONNECTION CHARACTERISTICS** pane of the *Deploy* template.

Result: Managed Plane Non-Integrated Long Logical Link connection between the ports of I/O cards are created successfully.

Figure 8-59 Managed Plane Non-Integrated Logical Link connection between the ports of I/O cards

For more information, see 8.5 “Deploy a Managed Plane Connection” (p. 1271).

5

Create an ODU4 Logical Link between 2UC400 and 2UC400 cards.

Result: ODU4 Logical Link between 2UC400 and 2UC400 cards is created successfully.

For more information, see 8.5 “Deploy a Managed Plane Connection” (p. 1271).

6

Create a 100 GbE service between I/O cards on the A-end and on the Z-end.

Result: 100 GbE service between I/O cards are created successfully.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 8-60 100 GbE Service between I/O Cards

Note:

1. The following services can be created on top of a Long Logical Link connection:
   - OPSB service (UNI, NNI)
   - Protected service (UNI, NNI)
   - Unprotected service (UNI, NNI)
2. For NNI services, OPS should be created between VNE and I/O packs and same OPS needs to be added in NPA as drop link and should be unlocked.

For more information, see 8.8 “Deploy a Service” (p. 1294)

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Part III: ASON

Overview

Purpose

An Automatically Switched Optical Network (ASON) is an intelligent optical network that can automatically manage the signaling and routing through the network. This part of the document provides an overview about ASON and NPA management with special focus on 1830 PSS and 16x6 Network Elements.

Contents

Chapter 9, ASON Features	1369
Chapter 10, Working in ASON	1421

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9 ASON Features

9.1 Overview

Purpose

This chapter provides features that apply to the ASON environment.

Contents

9.1 Overview	1369
Soft Revertive SNCP	1371
9.2 Overview	1371
9.3 Soft-Revertive ASON SNC management	1372
9.4 Actions on NFM-T	1374
Overlay in GMPLS Domain	1379
9.5 Overlay Configuration in GMPLS Domain	1379
Optical Feasible Routing	1382
9.6 Optical Feasible Routing	1382
9.7 Supported Network Configurations	1384
Schedule ASON Revertive Switching	1385
9.8 Description	1385
9.9 Schedule the Revertive Switching for ASON Routed Connection	1386
9.10 Actions on a scheduled Job	1390
Multi-Region Networks	1391
9.11 MRN and Intra Node Link	1391
9.12 Unterminated FA Tunnel Support	1395
9.13 Terminated FA Tunnel Support	1399
9.14 20P200+S4X400H Mating Management in Control Plane Configuration	1405
Longspan Support in NFM-T	1411
9.15 High Level Steps Sequence	1411
Foreign Connections	1413
9.16 Foreign Connection management	1413

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

GMRE Naming Rules	1417
9.17 Naming Rules for Long Span Support	1417
9.18 GMPLS Support Preconditions	1419

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Soft Revertive SNCP

9.2 Overview

General

This function allows to configure the reversion mode for protected ASON SNC (E-SNCP, O-SNCP, PRC), the full GMRE soft reversion feature, for L0 and L1.

The Soft SNCP reversion supported by GMRE is not the standard revertive SNCP using the APS protocol with provisionable WTR. The standard revertive SNCP switchs the traffic back to the main as soon as the Main SNCP leg is available again, that is in state back from failure, after the configured time (WTR).

If the SNCP reversion implemented by GMRE is enabled, it applies the switch of a protected SNC as soon as triggered by automatic or manual reversion. The SNC is SNCP protected. The switch of the SNC is done either to the nominal main or to the main/spare. It depends on the user provisioned mode and after the user provisioned time.

For this reason this is referred as Soft Revertive SNCP. The *Soft* reversion implemented by GMRE overrides so the standard APS by NE.

The Soft Revertive SNCP attribute defines the Wait-Time-to-Restore (WTR) for a SNC to move back from Current to Nominal route, after the failure affecting the latter is repaired. It applies only to GMRE connections *ready to revert* and *protected*: SNCP protected and PRC.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.3 Soft-Revertive ASON SNC management

Description

On the NFM-T the user can configure the reversion mode for the ASON SNC types in L0 and L1 GMPLS: O-SNCP (not restored in GMRE, SNCP protected) and O-PRC for L0 and E-SNCP (not restored in GMRE, SNCP protected) and E-PRC for L1. For a restored SNC, the values can be changed.

The soft revertive feature applies, for optical configurations, to OTN shelf, PSS-24X, PSS-8X, PSS-36, PSS-64, and to uni-directional and bi-directional protection schemes per LSP (ASON SNC) configurable from Deploy template. It applies, for digital configurations, to PHN models (PSS-32, PSS-16, PSS-16II, PSS-8, PSS-8x/24x) and OCS models for the uplink cards.

For an unprotected ASON SNC the soft revertive SNCP mode is **Not Applicable** as default and cannot be changed.

Interactions/step sequence of timers in ASON

The following timers now apply in SNC ASON:

- link WTR – this timer is configured by NFM-T to declare a link as good when it was stable long enough
- nominal WTR – not configured by NFM-T while internal to GMRE to declare a nominal route as available when GMRE detects, it is used for auto nominal reversion.
- soft-revertive SNCP timer - to switch the SNCP selector to the nominal leg

Timer execution example

For a better understanding of the association between the *link WTR*, the *reversion to nominal* and the *revertive SNCP Timer*, see the following example highlighting GMRE step sequence flow.

Suppose the *revertive SNCP mode* selected by the user for the protected SNCP is **anyNominal**:

1. Both protected SNC legs are on backup: SNC state in GMRE is backupMain, backupSpare. GMRE runs periodic verification of the SNCP state

   ⇒ no action as both legs are on backup
2. The Link on nominal spare is repaired

   ⇒ link WTR applies - when expires the link is declared as working
3. Nominal route verification applies using nominal reversion WTR, GMRE internal WTR for automatic nominal reversion, not provisionable by NFM-T

   ⇒ GMRE detects nominal spare is available and raise **Ready to revert** alarm
4. If automatic nominal reversion or manual triggers Revert to nominal, GMRE reroutes the Spare leg

   ⇒ new LSP state: backupMain – nominalSpare
5. GMRE periodic verification of SNCP state detects (backupMain, nominalSpare)
6. Configured Soft-revertive SNC Timer applies

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

⇒ when it expires, being soft-revertive mode anyNominal and nominal spare is available, GMRE switches SNCP to nominal spare on head node and is also found through signaling on the tail node.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.4 Actions on NFM-T

Create the Connection

On the NFM-T system, to create a soft revertive SNC follow the actions:

1

Follow the path **DEPLOY > New Service/Infrastructure Connection**.

Select template **/Best Practices/Infrastructure Trail/OCHP Protected** with **ODUk**.

The OCHP protected template is displayed.

2

For details on deploying the connection see the procedure 8.5 "Deploy a Managed Plane Connection" (p. 1271)

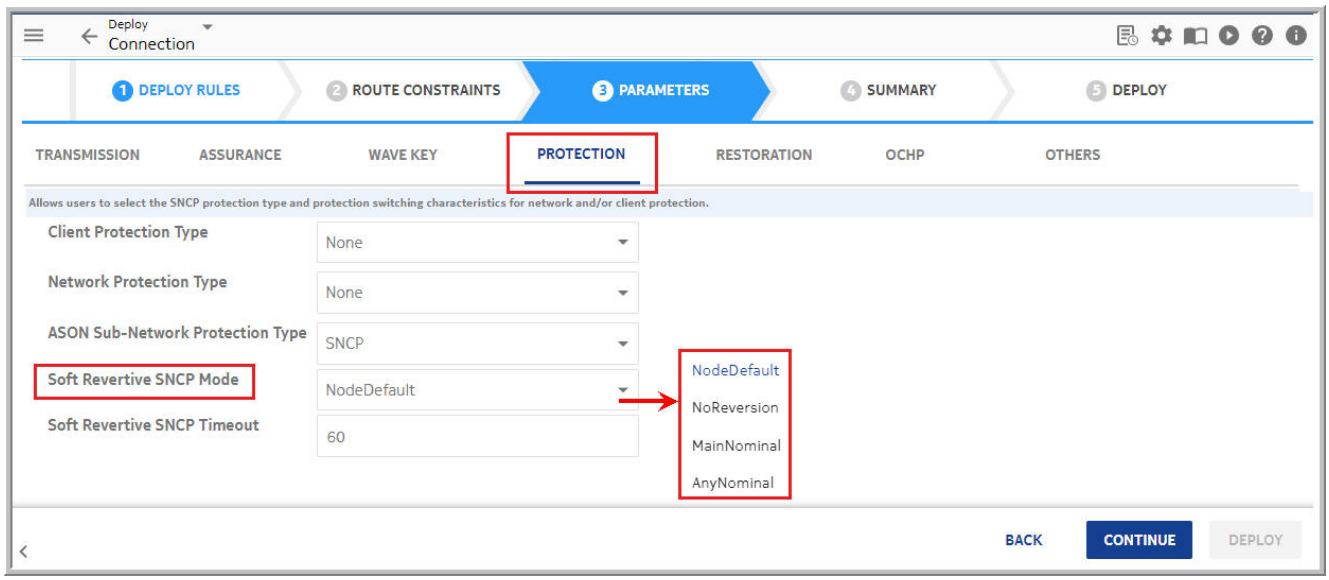
Check the **ASON** check box and ensure the **Protection** check box is checked (it is checked by default) in the **DEPLOY RULES** tab.

3

To manage the soft revertive GMRE feature use the parameters in the **PARAMETERS > PROTECTION** tab.

Set **ASON Sub-Network Protection Type** to **SNCP**.

Figure 9-1 Create Connection - Soft Revertive SNCP Mode



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Soft Revertive SNCP Mode 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.

  The default value for this parameter when the deploy page is displayed is *NoReversion*.

  Note:
  - The default value at SNC creation is *NodeDefault*, the values for the created SNC are the values defined for the Node.
  - If the mode selected is *MainNominal* or *AnyNominal* the field **Soft revertive SNCP Timeout** is displayed to insert the timer value.

Soft Revertive SNCP Timeout: time in seconds (range 60-600), less than 60 seconds is not allowed.

Note: Soft Revertive SNCP Timeout parameter is not applicable for *NoReversion* and *NodeDefault* options. On creation the value is set to 0. The default value for *MainNominal* and *AnyNominal* is 60.

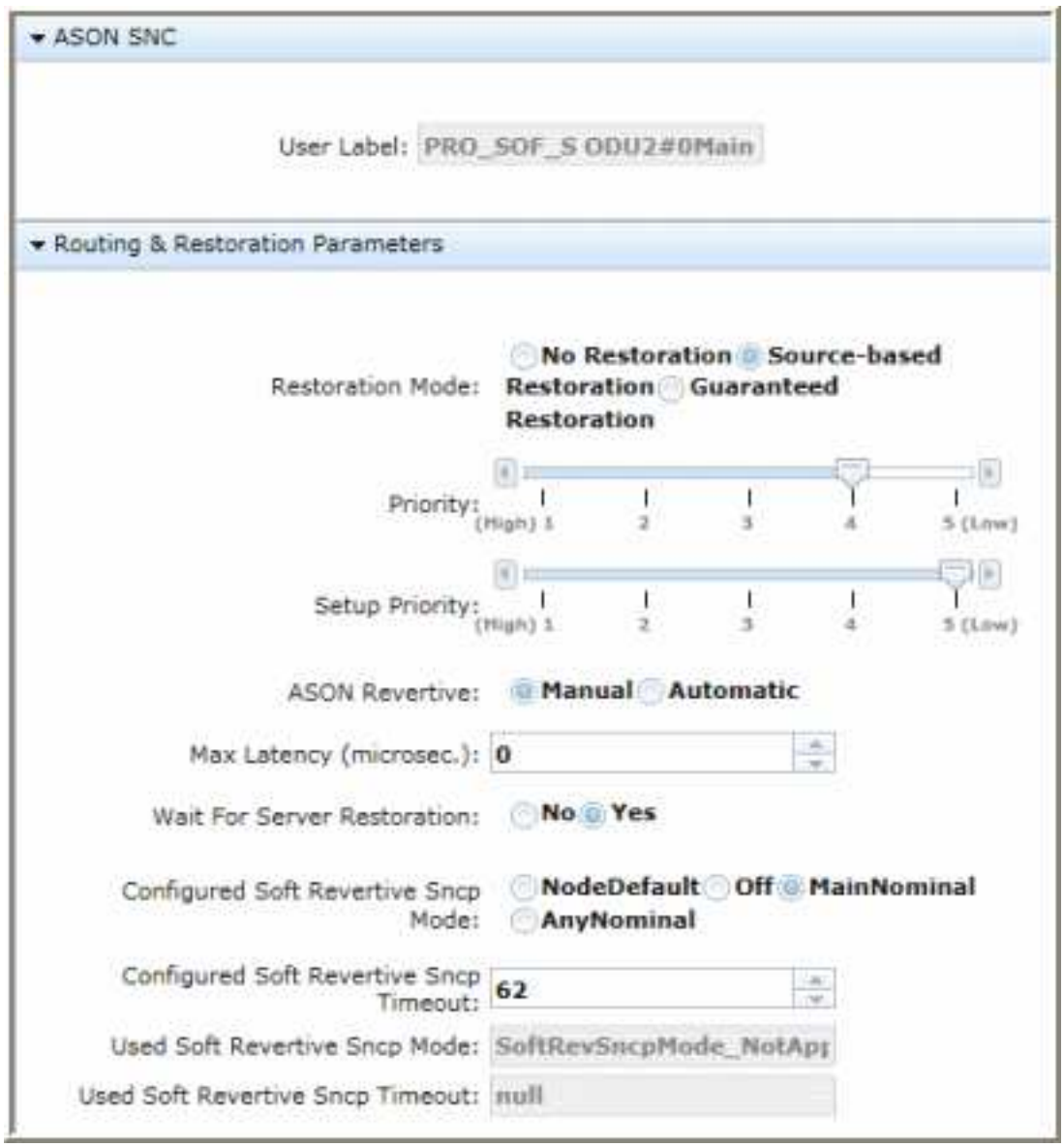
Modify ASON SNC parameter

The soft revertive parameters can be modified on the Modify Trail Parameters window.

From the WebUI main menu follow the path **OPERATE > ASON > SNC**, the list of SNCs is displayed, select the SNC to modify the parameter, then right click and select **Modify Attributes** from the popup menu.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-2 Modify Trail Parameters



The **Configured Soft Revertive Sncp Mode** and the **Configured Soft Revertive Sncp Timeout** parameters can be modified.

If the **Configured Soft Revertive Sncp Mode** is set to the value `NodeDefault` or `Off`, the timer is automatically set to zero.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

NodeDefault Behavior

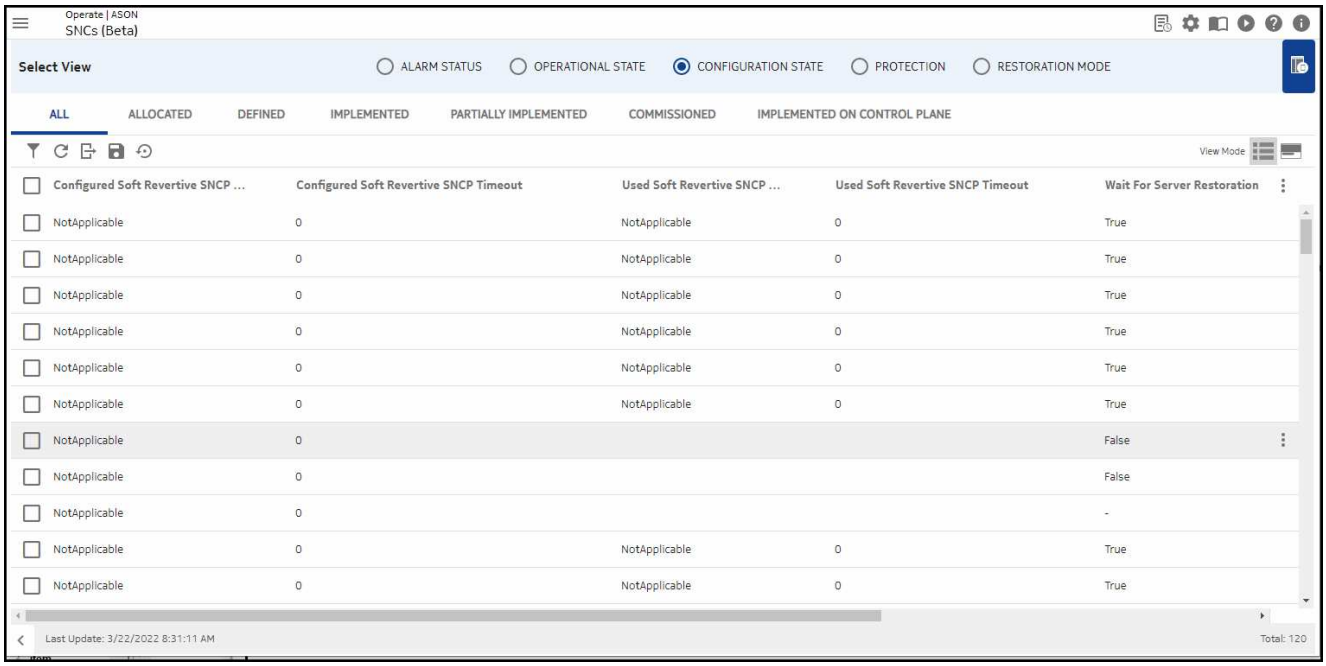
If the mode is NodeDefault the values for SNC configured parameters are updated by the GMRE applications. If a value is changed on the node, it will be updated on the connection with the node as Head Node.

SNCs List

In the ASON SNCs list, the following values are displayed:

- Configured Soft Revertive SNCP Mode, the value is set at creation or modification by the user.
- Configured Soft Revertive SNCP Timeout, this value is set at creation or modification by the user if the Soft Revertive SNCP Mode is MainNominal or AnyNominal.
- Used Soft Revertive SNCP Mode, this value is the last synchronized value from the GMRE application.
- Used Soft Revertive SNCP Timeout, this value is the last synchronized value from the GMRE application.

Figure 9-3 Soft Revertive - SNC List Attributes



In the ASON SNCs is uprotected the following values are displayed

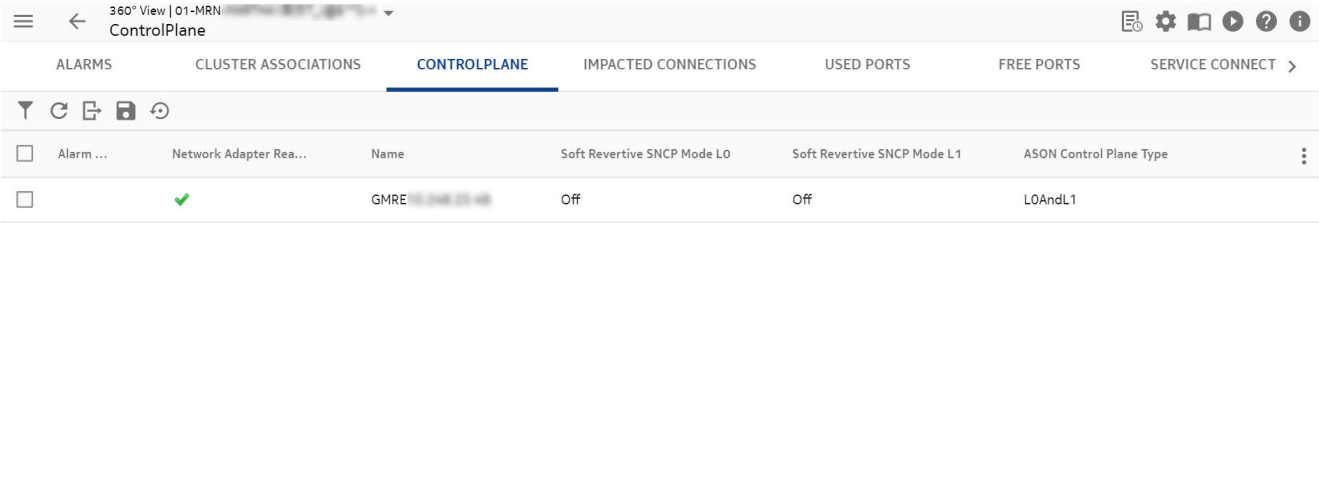
- Configured Soft Revertive SNCP Mode, Not Applicable.
- Configured Soft Revertive SNCP Timeout, 0.
- Used Soft Revertive SNCP Mode, Not Applicable.
- Used Soft Revertive SNCP Timeout, 0.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Control Plane List

The fields for the soft revertive configuration are listed in the Control Plane tab that is displayed and kept up-to-date with GMRE Control Plane, Node values within the Nodes and NPAs lists. See 25.15 “CONTROL PLANES tab” (p. 2089) for more details.

Figure 9-4 Soft Revertive - Control Plane Fields



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Overlay in GMPLS Domain

9.5 Overlay Configuration in GMPLS Domain

Description

The overlay configuration is intended as a configuration in which two control planes, either L0 and also L1, are active in compound nodes, such as L0 GMPLS on PSS SWDM and L1 GMPLS on PSS-36/64/24x. In this kind of configuration, the user can create a connection HO-ODUk restored in L0 GMPLS and then a service restored in L1 GMPLS. There is no coordination between the two GMPLS control planes because this is not an MRN configuration.

Three basic NE/node configurations are considered:

- single SWDM NE (1830 PSS-PHN and 1830 PSS-24X) with L0 & L1 GMPLS active
- Compound node with:
  1. 1830 PSS-PHN and 1830 PSS-OCS
  2. single SWDM NE (1830 PSS-PHN and 1830 PSS-24X) and 1830 PSS-OCS

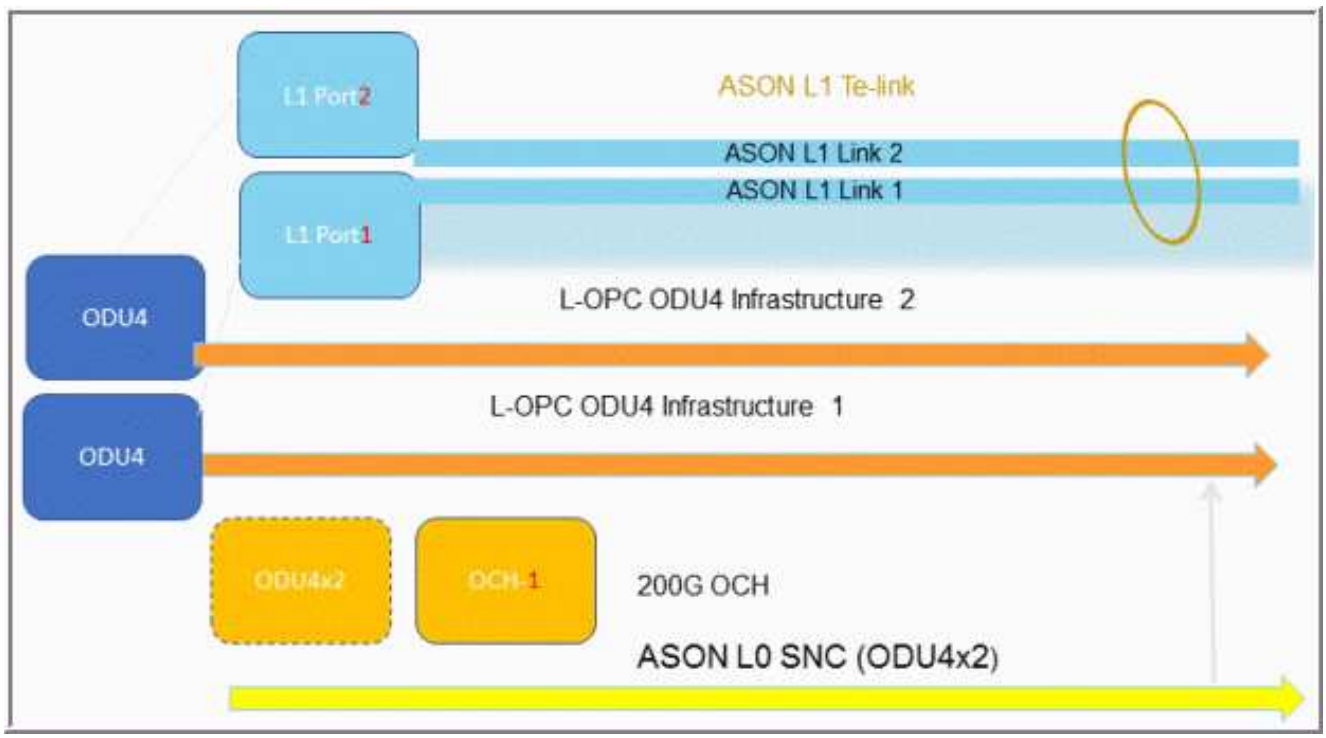
The networks can use one or all these configurations. The overlay configuration is a step of the network evolution toward MRN, The first step to move to MRN is the L0 GMPLS activation. Once L0 GMPLS is activated, the network will be in overlay configurations. The reason is that L0 GMPLS activation transforms the OTUk channels in L0 GMPLS SNCs, not into tunnels.

High level provisioning flow

The figure is used to explain the provisioning of the overlay configuration in GMRE domain.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-5 OTN/ASON target view for L1 and L0 CP in Overlay



The first step sets up the ODU4 Infrastructure from OTN, OTN provisions L0 ASON SNC ODU4x2 to ASON, see 10.2 "Deploy connection- ASON specific parameters" (p. 1424) and 10.3 "Connection creation - ASON specific" (p. 1429).

When the L-OPC ODU4 Infrastructure is created, by OTN, ASON creates L1 Logical link 1 involving Port 1, see Figure 9-5, "OTN/ASON target view for L1 and L0 CP in Overlay " (p. 1380)

ASON SNC ODU4x2 is linked to L-OPC ODU4 Infrastructure 1

The second step sets up the ODU4 Infrastructure 2 from OTN, OTN does not provision ASON SNC ODU4x2 to ASON

At L-OPC ODU4 Infrastructure 2 creation and notified by OTN, ASON creates L1 Logical link 2 involving Port 2

At L-OPC ODU4 Infrastructure 2 creation notification by OTN, ASON creates L1 Logical link 2 involving Port 2

User adds L1 Logical links 1 and 2 to ASON, see 10.15 "Add links and remove links from ASON" (p. 1462)

As soon as both Logical link, 1 and 2, are added to ASON, they are bundled in the same TE-Link based on same Costs and SRGs

User sets up L1 ODU Infrastructure and, if the infrastructure is ASON routed involving the board, ASON SNCs is created on top of L1 Logical Links.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Setup in the Create Connection window

The overlay configuration setup uses the create connection window, see 10.2 “Deploy connection-ASON specific parameters” (p. 1424) and 10.3 “Connection creation - ASON specific” (p. 1429). The selection in the Service definition panel is: **ASON Routed** (check the box), **ASON Tunnel** (check the box) and **Tunnel Type = L0-L1 Overlay**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Optical Feasible Routing

9.6 Optical Feasible Routing

General Flow

The function for optical feasible routing applies to find a route for OTN in the given topology keeping the impairment parameters managed by the GMRE application. The module that accomplishes this function is called General Path Computation (GPC) engine.

GPC Process

The status of the GPC process can be seen in the System Monitor window. See the *Administration Guide* for detailed information.

Network Configuration

The Network is configured using the Planning Tool and the configuration is downloaded to the Network using the CPB application. If a new Segment is added to the network, a new Upload may be necessary based on the type of changes made. For example if new NEs are added and OtLine ports are configured along with and then later the TELinks are added, the TELinks are managed by the GPC process, and the OT Lines are not, since the new added NE can have no control plane enabled and the GPC process rejects the OtLine port that is attempted to be added.

The Network Upload operations can be monitored using the CLOG application following the path **ADMINISTER > User Activity Log > All Records**, that displays the log of all the activities. The operations can be triggered also following the path **Operate > Upload topology**.

Save a Template

Follow the path **DESIGN > Service/Infrastructure Template** to display the window. The template is stored in the **Best Practice** directory of the Service/Infrastructure Templates window. See "Design and deploy a new service/infrastructure connection with templates" (p. 669)

The template is located under the folder */Best Practices/Infrastructure Trail/Unprotected* and select the template **Optical Feasibility**.

To create the template select the template **Optical Feasibility** in the list on the left tree side of the window and follow the path **Save As ...** from the popup menu.

The **Create Template** window is displayed. This template has the field **Optical Impairment Routin**g that can assume the values Enforce or None. Save and publish the template to use it for creating new services.

Deploy the Connection

When the template is chosen for deployment, this is enabled only when ASON-Routed is selected. If the **Enforce** option is chosen, GPC computed route is requested and if the route is not found, the connection request is terminated with an error message.

If the **Best Effort** option is chosen, then GPC computed route is computed. If the route is not found, an OTN based routing is attempted.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

If **None** option is selected, GPC routing is bypassed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.7 Supported Network Configurations

Description

Supported Network Configurations for Optical Feasible Routing are:

- L0 Control Plane Connection starting and ending on OT Line ports (Transponders, Muxponders, Switchponders) on PSS-32 Shelf on either end.
  - OPSA protected connections
  - Unprotected connections
  - On a CDC-F Node
  - On a Config-D, D’ Node
  - On a WR ROADM nodes
  - On a combination of these NE types around the network.
  - Passing through a PSS-16, PSS-16II ILAs and DGEs.
  - With a set of 3Rs along the route in working and protection route.
- L0 Control Plane connection shall support connections across both FlexGrid capable and FixedGrid constrained network elements.
- 1830 PSS-24X/8X IO/Uplink Cards

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Schedule ASON Revertive Switching

9.8 Description

Schedule ASON Revertive Switching

This function allows the user to select one or more Service or Infrastructure Connections ASON Routed from the list to schedule the reversion to nominal by provisioning the scheduled date (month/day/year) and time (hour:minutes AM/PM). The connection Category is not *Managed Plane.*

At the scheduled date and time expiration, NFM-T system checks the ASON SNCs belonging to the ODU Infrastructure Connections under scheduled reversion. The switch to nominal is performed for the connections that are in *Manual* Reversion mode and *Ready to revert*.

If the ASON SNCs are not *Ready to revert*, the system does not perform the action and the user must reschedule the reversion date and time.

Scheduled Job Column

In the Service or Infrastructure Connection data table a column **Scheduled Job** is displayed.

The column **Scheduled Job** in the Service or Infrastructure Connection data table is set to **Y** when the Service or Infrastructure Connection is selected in a scheduled job, the field is blank otherwise.

Once the scheduled job on the Service or Infrastructure Connection is completed, timed out or expired, the field is updated to blank.

Scheduled Job Warning and Error

When the Service or Infrastructure Connection is selected for a job, the connection cannot be selected for another job. The Schedule Job command displays an error when the job is already scheduled for another job. In case of multiple Services/Infrastructure Connections selection, some connections can have the *ASON Revert to Nominal* already scheduled, in this case the system implements a best effort approach displaying a warning message to user for the connection that cannot do the reversion switch because already scheduled in another job.

In case the user deletes or modifies a Service or Infrastructure Connection parameters when a job is scheduled, the system automatically removes the job from the job list with a warning message.

If the user performs a delete or delete a Connection and Clients operation on a connection, which is part of the Scheduled Job then the confirmation message alerts the user that it is also part of a scheduled job.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.9 Schedule the Revertive Switching for ASON Routed Connection

Purpose

This procedure defines how to schedule the revertive switching for ASON routed connections. The function applies for connections that have implementation state complete and the service rate starts with ODU.

There is no limit to the number of Services or Infrastructure Connections selected in the list, to create the ASON Reversion job. The only limitation is the maximum number of rows supported in the data table interface.

Task: Schedule the Revertive Switching for ASON Routed Connection

Complete the following steps to schedule the revertive switching for ASON routed connections.

1

Follow one of the navigation paths from the WebUI:

OPERATE > Infrastructure Connections

OPERATE > Services

OPERATE > Services > Servers

Result: Depending on your selection, the system displays a data table that lists all of the requested connections.

2

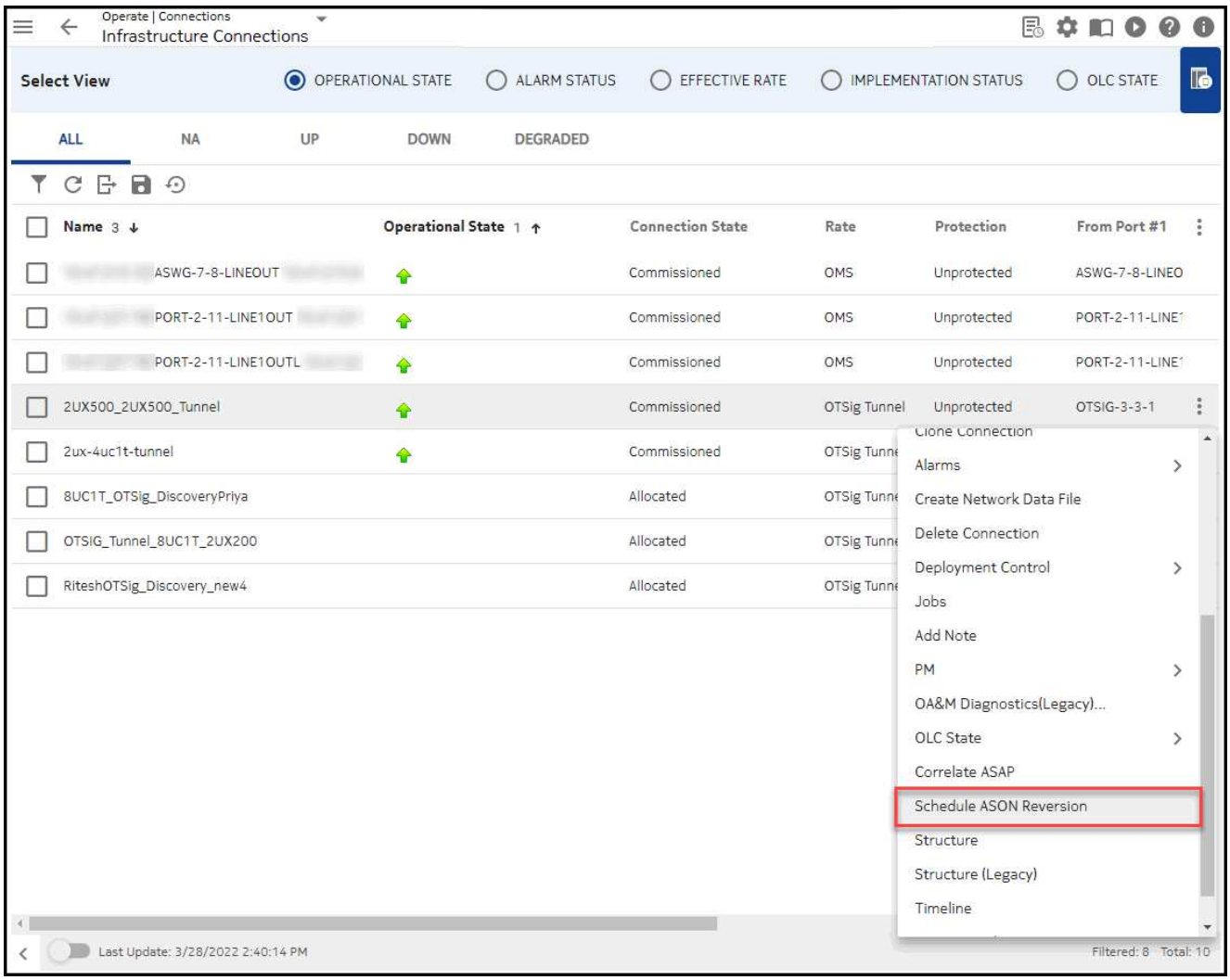
Select, clicking on the Select icon, one or more connections on which you want to schedule the revertive switch and do one of the following:

If...	Then
you select a single connection	select the **More** ⋮ icon at the right end of the row to display the popup menu
you select more connections	select the **More** ⋮ icon at the left upper part of the window to display the popup menu

Result: The popup menu is displayed with further actions. Figure 9-6, “Schedule Ason Reversion - Popup Menu” (p. 1387) shows the popup menu on the Infrastructure Connections page.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-6 Schedule Ason Reversion - Popup Menu



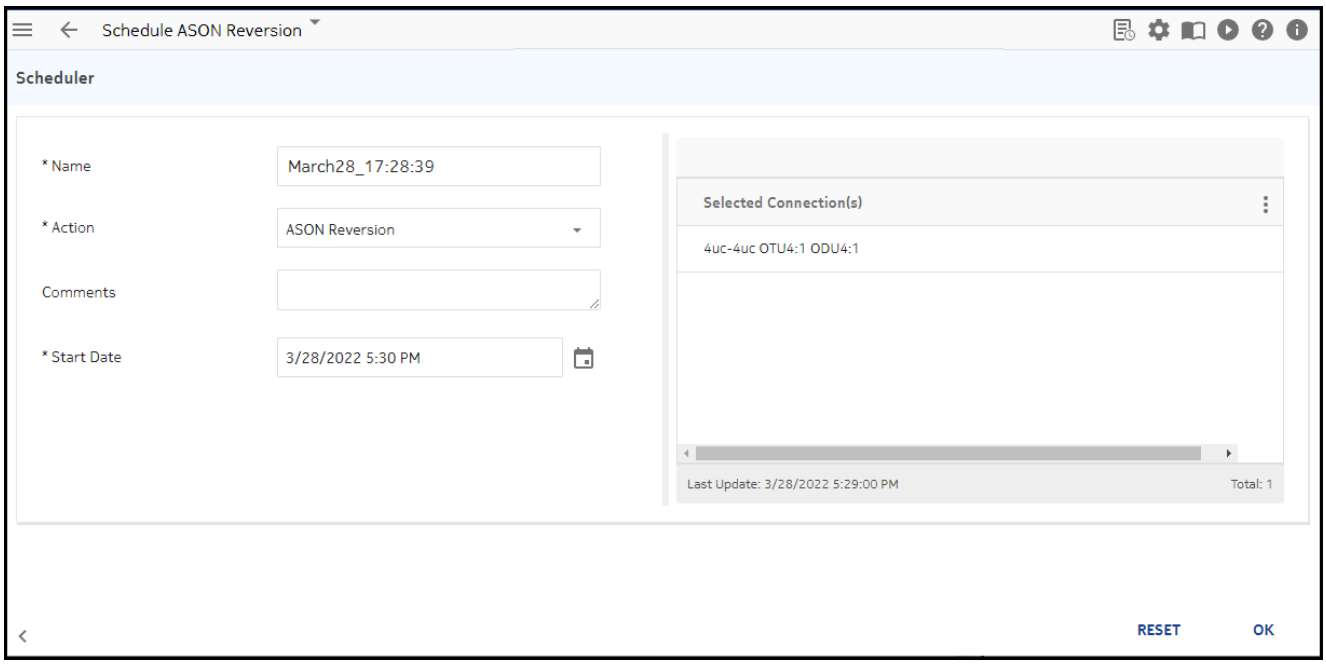
3

Follow the path **Schedule ASON Reversion** from the popup menu.

Result: The Schedule ASON Reversion page is displayed. See Figure 9-7, “Schedule ASON Reversion page” (p. 1388)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-7 Schedule ASON Reversion page



4

In the **Name** field, a default name is displayed, the name is composed using the month and day, underscore character and the current time. You can retain it or assign a different name to the job.

5

In the **Action** field, retain the default **ASON Reversion**.

6

Optional: In the field **Comments** write a description that can be useful for the scheduled job.

7

In the field **Start Date**, enter the scheduled start date and time in the mm/dd/yyyy hh:mm AM/PM format.

OR

Click the Calendar icon and select the date and time from the calendar that is displayed.

8

In the **Selected Connections** list, you can see the connections that you have selected.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Note: The list displayed depends on the list of connections you started the scheduled job. If you started from Services, the list displayed is the Service list, if you started from the Infrastructure Connections, the list displayed is the Infrastructure Connections list.

9

Click **OK** to confirm and schedule the ASON reversion job.

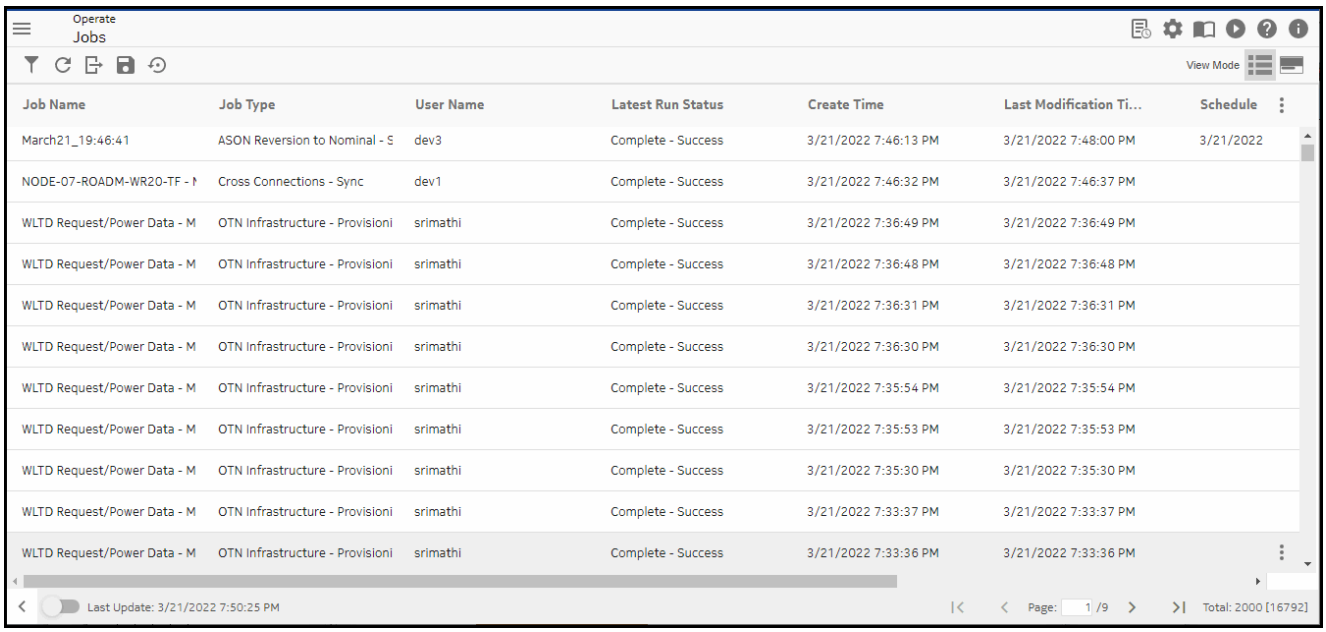
Result: On successful job submission, a Confirmation dialog box appears.

10

Click **Yes** to go to the **Jobs** page.

Result: The Jobs page is displayed and you can view the job details. See Figure 9-8, “Ason Revertive Schedule - Jobs List” (p. 1388)

Figure 9-8 Ason Revertive Schedule - Jobs List



Click **No** in the Confirmation dialog box to stay on the same page.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.10 Actions on a scheduled Job

Overview

From the **Jobs** window you can perform following actions on the scheduled job:

- Run History: displays the history window for the selected job. Here you can see errors if occurred, and descriptions of the same.
- Abort: only enabled if the job is running.
- Reschedule: displays the Schedule Job window, you can modify the start date and time for the job, the description of the job, or add or delete connections from the scheduled job.
- Delete: you can delete the job.
- Selected Service/Infrastructure Connections: displays a box with the selected connections for the scheduled job.

Note: If the ODU4 connection is a cross to connection, the jobs scheduled for the revertive switch is done also on the other connection on the ODU4.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Multi-Region Networks

9.11 MRN and Intra Node Link

Multi-Region Networks (MRN)

Multi-Region/Multi-layer Networks (MRN) supported by GMRE R10.1 adds the combination of WDM and 1830 PSS-24x with GMRE features.

The MRN configuration is implemented with UL-WDM link in the same Node. The UL-WDM in compound, for example OCS-PHN, was in previous configurations a link between two Nodes provisioned to GMRE as I-NNI. For the link inside the same Node, a new link type, *transitional*, is introduced by GMRE application for 1830 PSS-24x nodes. See 9.12 “Unterminated FA Tunnel Support” (p. 1395) .

MRN and L1 Control Plane support for L2 cards

From NFM-T Release 19.9, the following 1830 PSS-24x L2 and OCS cards support protected and unprotected L1 Control Plane connections and MRN tunnels.

- 1830 PSS-24x
  - 30SE300
  - 6SE300
- 1830 PSS-64 and 1830 PSS-36 OCS
  - 103SCEC
  - 11OCEC

The client Ethernet cards are located in an ODU switch shelf with external Ethernet facing client ports and the ODUPTF connected to the ODU switch matrix acting as a transition to the ODU layer. The ODU switching is performed in the 1830 PSS-24x or 1830 PSS-64 / 1830 PSS-32 shelves.

ODUPTFs are logical ports with variable signal rates.

Note: The 6SE300 and the 30SE300 cards must be configured as a packet switch before the ODUPTF is assigned. The WAN side allows up to 400 Gbps capacity.

GMRE provides the connectivity between the ODUPTFs supporting clients with L2 switch and to the supported Ethernet layer. During ODUk Infrastructure Connection provisioning, ODUPTF is created in the NE by sending XoS requests and assigned to GMRE as L1 drop and as ODUk SNC end points. After the provisioning of the connection, the logical WANIF ports are displayed in the EQM window. During service creation, only the WANIF ports are displayed in the port selection fields (To Port and From Port) of the **Create Connection** window.

For L1 Control Plane connections, create a service with WANIF ports on an L1 logical link that is assigned to NPA.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-9 Relation of WANIF-ODUPTF for 1830 PSS OCS

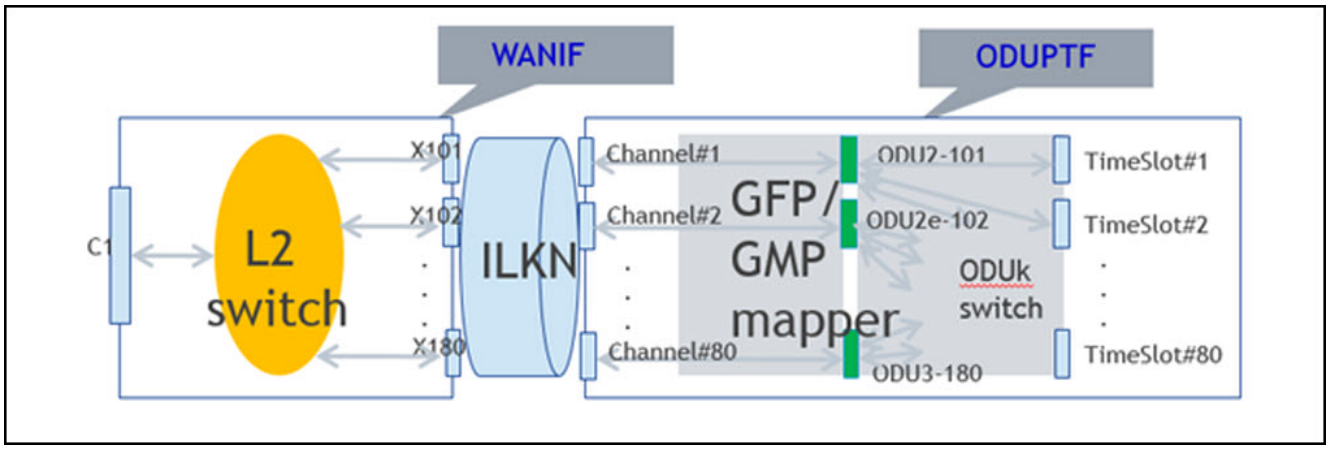
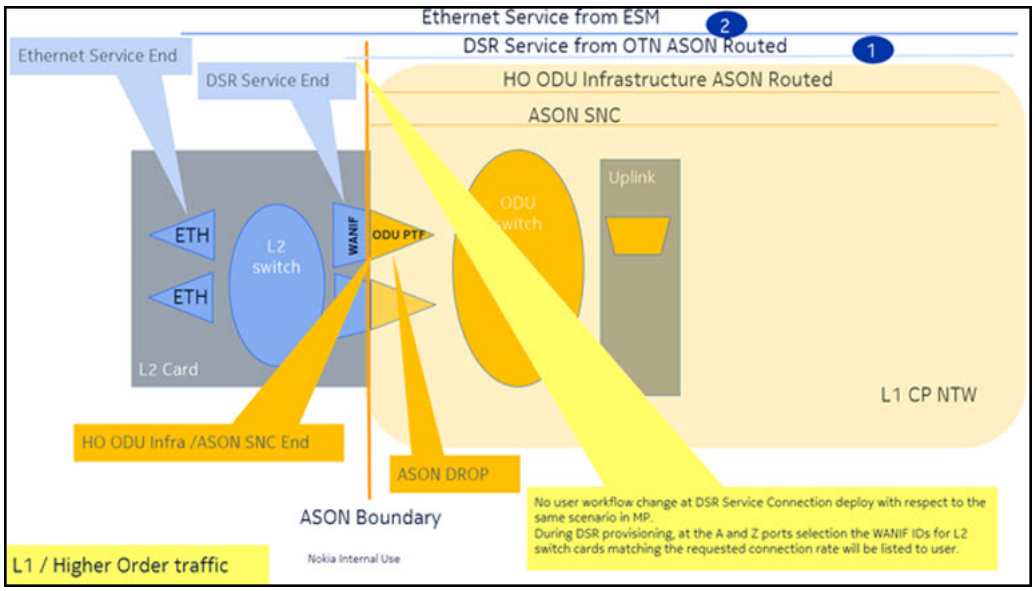


Figure 9-10 ODUPTF Scenarios



For MRN tunnel, create a service with WANIF ports on an unterminated MRN tunnel that is assigned to NPA.

For the particular WANIF logical port selected during service creation, the OTN creates TPs in the NE and sends the request to ASON.

The following table provides the information of the ODUPTFs used as SPC end points in L1 GMRE and MRN scenarios for L2 cards and OCS cards.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 9-1 1.6 L2 cards with ODUPTF in L1 GMRE and MRN scenarios

Supported L2 and OCS cards	Layer 1 GMRE and MRN Support	iNNI Rates Supported
6SE300/30SE300	ODUPTF configured as SPC endpoint • ODU4 • ODU2e	• OTU2e • OTU4 • OTU4x2
103SCEC/11OCEC	ODUPTF configured as SPC endpoint • ODU4 • ODU3 • ODU2 • ODU2e	• OTU2 • OTU2e • OTU3 • OTU4

Intra Node Provisioning Flow

In the unassigned link condition, at card plug-in and cable configuration, NFM-T autodiscovers the link and automatically assign it to the ASON NPA. The intra node provisioning is supported in 1830 PSS-PHN and OCS NEs along with 1830 PSS-8x and 1830 PSS-24x.

1

The internal link between shelves of the same NE, is visible in NFM-T

2

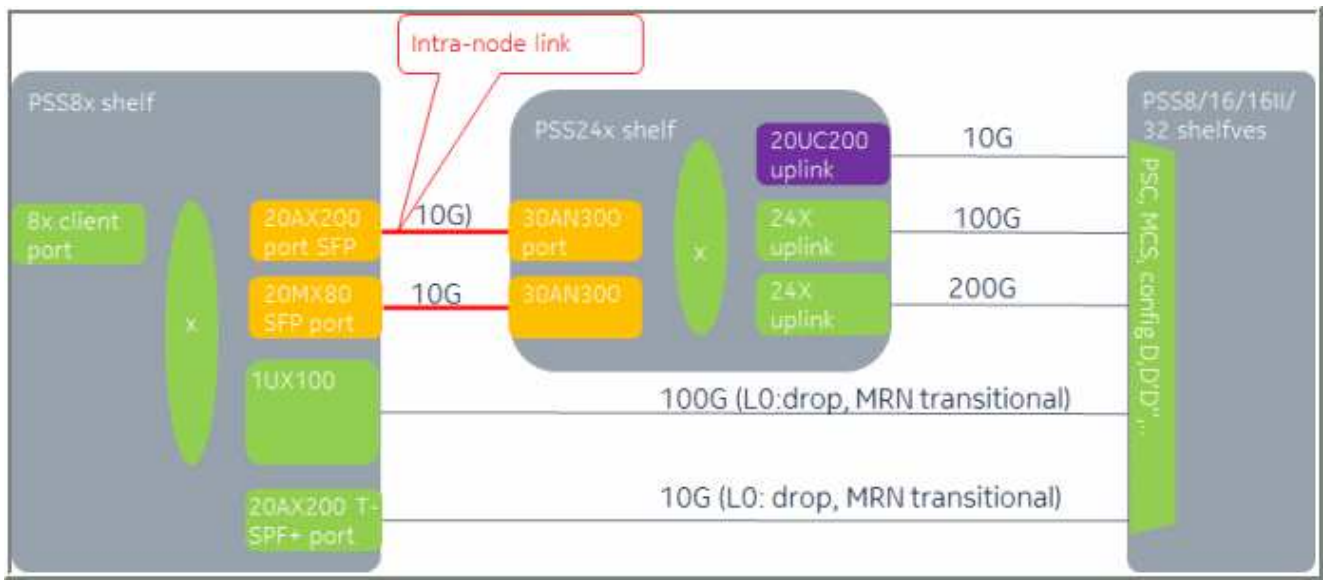
Based on inter-shelves link provisioning, the two ports at the ends point to each other at XoS; an internal physical link is created, that automatically triggers the add link to NPA with provisioning to GMRE

3

The link is displayed as I-NNI ASON link in ASON NPA and can be managed as normal I-NNI link. When the link is assigned to the NPA, the inter-shelves link cannot be removed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-11 Intra Node Link - Cascaded Configuration - Single Hybrid Node



4

When the links are displayed in the ASON NPA, they can be removed from it. In this case the ports on the NE are assigned to the managed plane.

5

The inter-shelves link can be removed but the ports remain MP assigned. The links can be removed from the NE user interface or from the EQM application.

6

The inter-shelves link can be re-provisioned from the NE user interface or command language interface or from the EQM application. From the assigned port MP the GMRE does not start the auto-discovery, the internal physical link is automatically added to NPA with provisioning to the GMRE application.

For more information on ASON NPAs, see the following:

10.6 “ASON NPA” (p. 1438).

10.10 “ASON NPA table columns” (p. 1450).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.12 Unterminated FA Tunnel Support

Overview

The FA Tunnel is supported in 1830 PSS-PHN and OCS NEs along with 1830 PSS-8x and 1830 PSS-24x.

The unprotected FA Tunnel can be created between 1830 PSS-8X with L1 GMPLS, 1830 PSS-24x, and OCS with MRN.

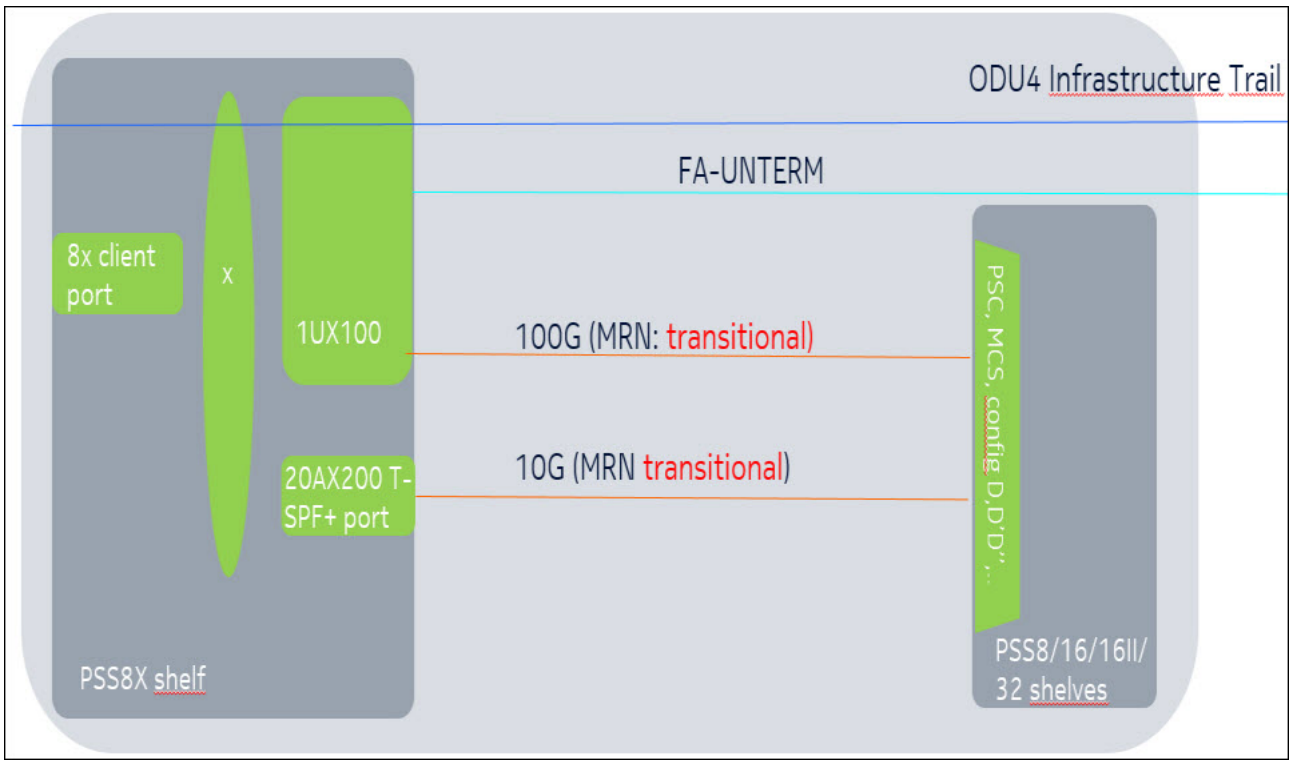
The 1830 PSS-8x interconnects with 1830 PSS-24x uplink cards. The unprotected FA Tunnel can also be created between two PSS-8x.

During the creation of unprotected FA tunnel, transitional links are managed by GMRE implicitly for MRN.

Note: In 1830 PSS-24x, each shelf represents a logical Layer T Data plane node and up to 8 PSS-24x shelves are supported per node.
In 1830 PSS-8x, each shelf represents a logical Layer 1 Data plane node and up to 8 PSS-8x shelves are supported per node.

This feature is supported for 100 G Uplink cards for 1UX100.

Figure 9-12 MRN with UL-WDM link in the same Node: Hybrid Node



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Task: To setup the FA tunnel in the Create Connection window

Complete the following steps to setup the FA tunnel in the **Create Connection** window.

1

From the WebUI, follow the navigation path:

DEPLOY > New Service/Infrastructure Connection

Result: The system displays the list of services or infrastructure connection templates.

2

Select a connection template from the list, for example, **ODUK with L0 Restoration** and click **Deploy** button.

Result: The system displays the **Connection** window with the **DEPLOY RULES** section selected by default.

3

In the **Rate** field, select one of the options from the drop-down list.

4

Ensure the **Protection** check box is not selected.

5

Select the **Logical Link** check box.

Selecting this check box, the **From Port Type #1** and **To Port Type #1** fields are set to **UnTerminated**.

6

Configure the following: **From Node #1**, **From Port #1**, **To Node #1**, **To Port #1**, **Customer Name**, **Connection Name**, and **Connection Alias**. Check the **Allow ASON Resources** and **ASON** check boxes.

7

From the **PARAMETERS > RESTORATION** tab, select the **ASON Tunnel** check box. System enables the **Tunnel Type** field.

Note: To move from one tab to another, perform one of the following steps:

- From the **DEPLOY RULES** section, if the **Routing Mode** is set to `Manual`, clicking **CONTINUE** button moves from **DEPLOY RULES** > **ROUTING CONSTRAINTS** > **PARAMETERS** > **SUMMARY** sections. To move to the previous section, click **BACK** button.

  From the **DEPLOY RULES** section, if the **Routing Mode** is set to `Automatic`, clicking on **CONTINUE** button takes you to **SUMMARY** tab.
- Click on the tab you want to set the parameters.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

8

Select **Tunnel Type** as **MRN UnTerminated**.

9

In the **ASON Restoration** field, select **Source-based Restoration**, **No Restoration**, or **Guaranteed Restoration**.

If one end is on 1830 PSS-8X, select **No Restoration**, otherwise the connection creation fails during deployment.

10

Click **CONTINUE** to go to the **SUMMARY** tab.

11

Optional: You can verify all your settings in the **Summary** tab before deployment.

12

Click **DEPLOY**.

For more information, see 10.2 “Deploy connection- ASON specific parameters” (p. 1424) and 10.3 “Connection creation - ASON specific” (p. 1429).

Result: The connection is created.

END OF STEPS

Task: To view and manage FA Tunnels

Complete the following steps to view and manage FA tunnels.

1

From the WebUI, follow the navigation path:

OPERATE > NPA.

For more information on ASON NPAs and ASON SNCs, see the following:

10.6 “ASON NPA” (p. 1438).

10.10 “ASON NPA table columns” (p. 1450).

10.34 “ASON SNC table columns” (p. 1527).

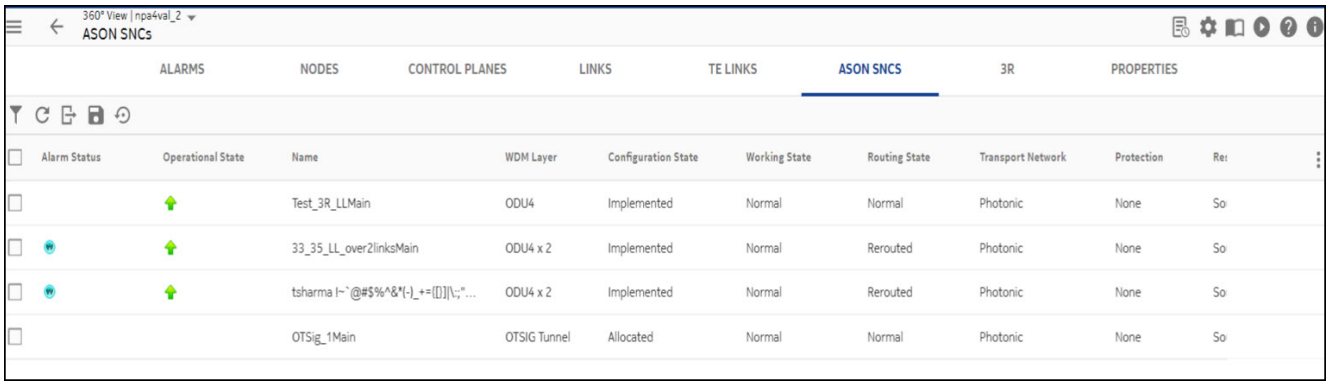
2

In the lower panel, click the **ASON SNCs** tab and select the unprotected FA tunnel

OR Navigate to **OPERATE > ASON SNCs**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-13 Operate - ASON SNCs



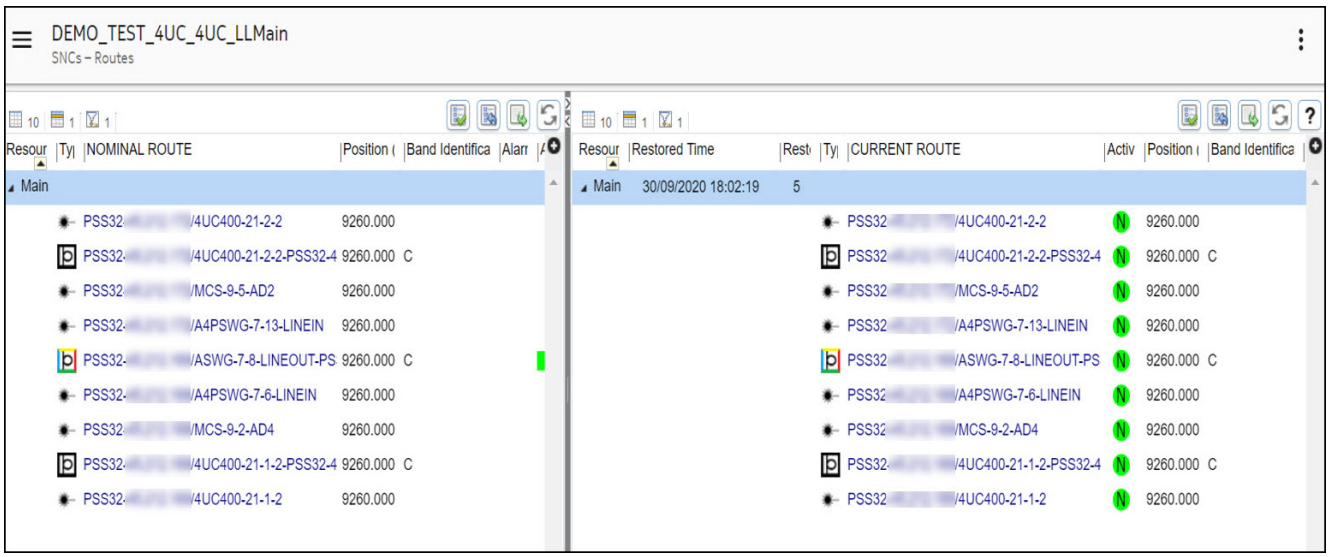
3

Click the unprotected FA Tunnel and the system navigates to details of unprotected FA tunnel.

4

Select a SNC, click the **More** icon. and select **Routes**. The **Nominal Route** and the **Current Route** is displayed.

Figure 9-14 FA Tunnel: Current Route and Nominal Route



For more information, see 25.42 “Routes Tab” (p. 2145).

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.13 Terminated FA Tunnel Support

Overview

Terminated FA Tunnel support can be any of below combinations

- Uplink card of OCS and Optical Transponder (OT) cards (130SNX10/130SCX10) of PSS-32
- Optical Transponder (OT) cards (130SNX10/130SCX10) of PSS-32 on both sides
- Uplink card (4UC400) of 1830 PSS-24x and Optical Transponder (OT) cards (130SNX10) of 1830 PSS-32

Note: Terminated FA Tunnel is supported between the uplink card (4UC400) of 1830 PSS-24x and Optical Transponder (OT) cards (130SNX10), of 1830 PSS-32. Terminated FA Tunnel for 1830 PSS-24x is supported from 1830 PSS NE Release 12.0, GMRE Release 12.0.

NFM-T supports the FA-TERM tunnel with 100G in ASON network with 1830 PSS-24x MRN configuration and photonic NE with L0 Control Plane in the same ASON domain (Single NPA).

In this configuration, MRN tunnel is at Layer L0 GMPLS, whereas services riding over the MRN tunnel is in the Layer L1 GMPLS.

Note: Ensure to assign the rate to the respective ports in the Equipment Manager window.

If the **Encapsulation Mode** is GPF-P, the **Container** is set to ODU2.

If the **Encapsulation Mode** is CBRLAN11.096, the **Container** is set to ODU2e.

Task: To create MRN Terminated Tunnel

Complete the following steps to create an MRN tunnel as a Logical Link:

1

From the WebUI, follow the navigation path:

DEPLOY > New Service/Infrastructure Connection

Result: The system displays the list of services or infrastructure connections.

2

Select an **ODUk** infrastructure template and click **Deploy** button.

Result: The system displays the **Connection** window with the **DEPLOY RULES** tab selected.

3

Select **Rate** as `ODU4` and **Connection Type** as `2-Ended Bi(I)`.

4

In the fields **From Node #1**, **From Port Type #1**, **To Node #1**, **To Port Type #1**, select the 1830 PSS-24X uplink card (4UC400, 2UC400) on one end and the client port 1830 PSS-32 Muxponder card (130SNX10, 130SCX10) on the other end.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

Ensure the **Protection** check box is not selected.

6

Select the **Logical Link** check box.

7

Check the **ASON** check box.

8

Optional: In the **Customer Name** field select a name from the list clicking on the magnifying lens to display the customer name list.

9

Optional: If you want to insert a **Connection Name**, type the name of the connection, otherwise it will be assigned automatically by the system.

10

Optional: In the **Connection Alias** field insert an alias for the connection. Field is filled with the old alias. Field supports blank Alias.

11

Select **PARAMETERS > RESTORATION** tab.

Note: To move from one tab to another, perform one of the following steps:

- From the **DEPLOY RULES** section, if the **Routing Mode** is set to `Manual`, clicking **CONTINUE** button moves from **DEPLOY RULES** > **ROUTING CONSTRAINTS** > **PARAMETERS** > **SUMMARY** sections. To move to the previous section, click **BACK** button.

  From the **DEPLOY RULES** section, if the **Routing Mode** is set to `Automatic`, clicking on **CONTINUE** button takes you to **SUMMARY** tab.
- Click on the tab where you want to set the parameters.

12

Select the **ASON Tunnel** check box, to enables the **Tunnel Type** field.

13

Set the **Tunnel Type** to **`MRN Terminated`**. Click **CONTINUE**.

14

Optional: You can verify all your settings in the **SUMMARY** tab before deployment.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

15

Click **DEPLOY**.

Result: The connection is created.

Note: Ensure that the GMRE version is R12.0 or higher before creating an MRN tunnel, otherwise the FA-TERM creation for 1830 PSS-24x uplink to muxponder card fails during implementation.

16

To view the deployed tunnel, navigate to **OPERATE > Infrastructure Connections** or **OPERATE > ASON > SNCs** page.

Note: The FA Term tunnel created between 1830 PSS-24x uplink cards and OT cards is marked as Infrastructure Connection and not Logical Link in the Infrastructure Connections list.

17

From the WebUI, follow any of the following navigation paths:

OPERATE > ASON> SNCs.

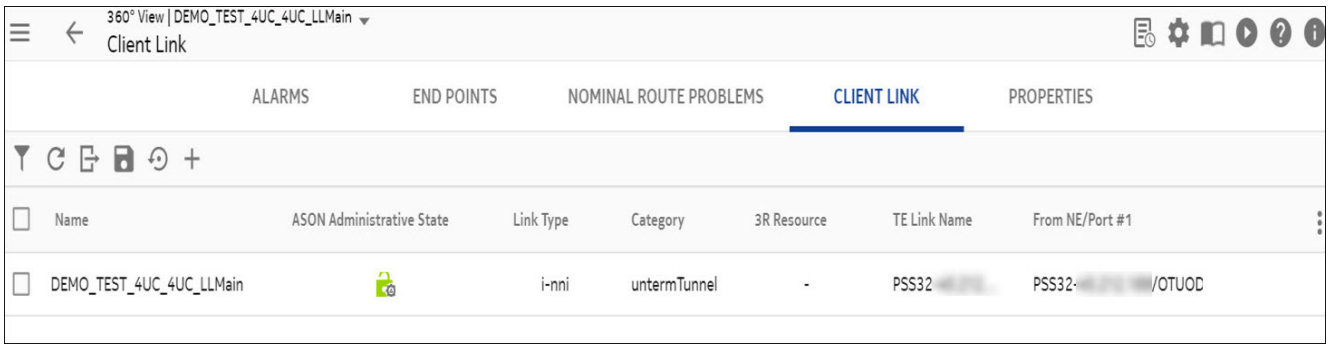
OPERATE > ASON > NPAs and select the **ASON SNCs** tab.

Result: The list of control plane connections are displayed.

18

To view the MRN connection, navigate to **OPERATE > ASON > SNCs > 360° View** and select the **Client Link** tab.

Figure 9-15 Client Link Tab



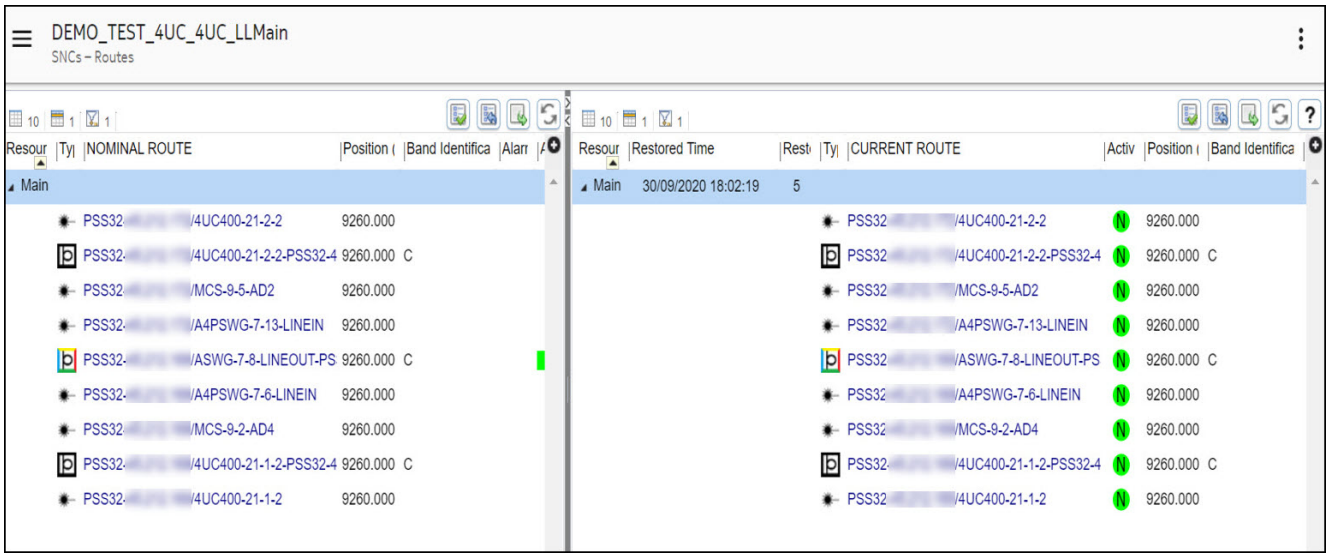
Note: The port naming is `ODU4 <ShelfID>-71-<FTPRangeIndex.>`, for example, ODU4-21-71-4107. These ports are displayed as the end points of 1830 PSS-24x uplink for the Tunnel.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Before deleting the Tunnel, ensure to lock the link that is implicitly added to NPA during tunnel creation. Deletion of the MRN tunnel is not allowed unless the tunnel link from NPA is in **Locked** state.

19

Select the connection, click the **More** icon and select **Routes** .



Result: The **Nominal Route** and the **Current Route** is displayed.

END OF STEPS

Task: To create services over MRN tunnel

The user can create services over MRN tunnel, the service creation is supported with rate 10 GbE (ODU2), 10 GbE (ODU2e), STM-64, and OC-192:

1

From the WebUI, follow the path

DEPLOY > New Service/Infrastructure Connection

Result: The system displays the list of services or infrastructure connections.

2

Select **/Best Practices/Service/Ethernet/Unprotected/Full Rate** with **10 G Ethernet** and click **Deploy** button.

Result: The system displays the **Connection** window with the **DEPLOY RULES** tab selected.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

By default, the **Service Rate** is set to 10 GbE.

4

Set **Connection Type** as **`2-Ended Bi(I)`**.

5

In the fields **From Node #1**, **From Port Type #1**, **To Node #1**, and **To Port #1**, select the 1830 PSS-24x IO card (30AN300/20AN80) on one end and client port of 1830 PSS 32 Muxponder card (130SNX10/130SCX10) on the other end .

6

Ensure the **Protection** check box is not selected.

7

Select the **ASON** check box.

8

Optional: In the **Customer Name** field select a name from the list clicking on the magnifying lens to display the customer name list.

9

Optional: If you want to insert a **Connection Name**, type the name of the connection, otherwise it will be assigned automatically by the system.

10

Optional: In the **Connection Alias** field insert an alias for the connection. Field is filled with the old alias. Field supports blank Alias.

11

From **PARAMETERS > RESTORATION** tab, select the **ASON Tunnel** check box.

Note: To move from one tab to another, perform one of the following steps:

- From the **DEPLOY RULES** section, if the **Routing Mode** is set to *`Manual`*, clicking **CONTINUE** button moves from **DEPLOY RULES** > **ROUTING CONSTRAINTS** > **PARAMETERS** > **SUMMARY** sections. To move to the previous section, click **BACK** button.

  From the **DEPLOY RULES** section, if the **Routing Mode** is set to *`Automatic`*, clicking on **CONTINUE** button takes you to **SUMMARY** tab.
- Click on the tab you want to set the parameters.

12

Set **Container** as *`ODU4`*, click **CONTINUE**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

13

Optional: You can verify all your settings in the **SUMMARY** tab before deployment.

14

Note: For creating a 10GbE-ODU2 rate, pass GFP-F as encapsulation mode in Transmission parameters panel of additional settings

Click **DEPLOY**.

Result: The service is created.

15

To view the deployed service, navigate to **Operate > Services** or **Operate > ASON > SNCs** page.

16

From the WebUI, follow any of the following navigation paths:

OPERATE > ASON> SNCs.

OPERATE > ASON > NPAs > 360° View > ASON SNCs tab

Result: The list of connections are displayed.

17

Select the SNC, click the **More** ⋮ icon and select **Routes** .

Result: The **Nominal Route** and the **Current Route** is displayed.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.14 20P200+S4X400H Mating Management in Control Plane Configuration

Description

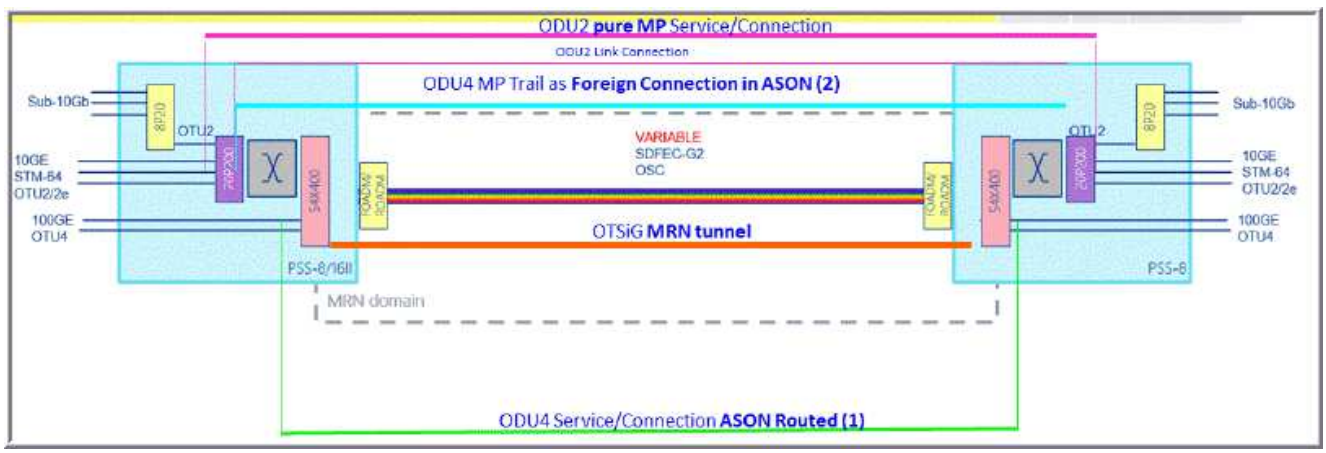
The management of 20P200+S4X400H mating configuration for Control Plane configuration is described.

The full capacity of 20P200+S4X400H configuration is 600 G at 67 Gbaud, but it can work with other line modes like 400 G, 500 G. The requirement for GMPLS is not to support the full mating, but for mating it is required that GMPLS Control Plane tolerates connections created by NFM-T.

This configuration requires foreign connection management Managed Plane for supporting 20P200 L1 in GMRE. NFM-T generates the virtual servers on top over the existing MRN Tunnel between S4X400 packs when mated with 20P200 packs. The server behaves as foreign connection, to ensure a ODU4 infrastructure can get created as higher order to support lower order services of 10G (via 20P200) or sub-10G (via 8P20).

20P200 + S4X400 service pack in mate configuration has no restriction on the profile management side, that means that S4X400 pack supported profiles applicable for this mate feature as well.

Figure 9-16 20P200+S4X400H Mating Configuration CP Example



Provisioning Flow

A description of the connection and services to be created in Managed Plane and Control Plane are detailed in this provisioning flow.

1

Setup of GMRE core network involving L0 and L1 (or at least L0) enabled NEs with 13.0.4 version.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

2

Create the OTS and OMS required physical connections and assign OMS to NPA as I-NNI (Unlocked).

3

In general, S4X400 has two backplane ports. Mating is permitted even if one set of backplane ports (A and Z ports) are respectively assigned.

Provision 20P200, S4X400 packs in PSS-8 / PSS-16II shelf by following below mating N/N+1 rules table and assign their backplane ports respectively with signal type OTL4.10 for mating.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-17 Mating Rules Table

PSS8 slot	2	3	4	5
PSS16II slot	3	4	5	6
PSS16II slot	7	8	9	10
1	S4X400	20P200	x	x
2	x	x	20P200	S4X400
3	20P200	S4X400	x	x
4	x		S4X400	20P200

4

Create MRN Tunnel between S4X400 packs.

See "Deploy a new service or infrastructure connection with template" (p. 1216) for detailed description of the create infrastructure and service procedure.

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

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Select the template **ODUk/OTSig Tunnel - Unprotected** and click on **Deploy...**

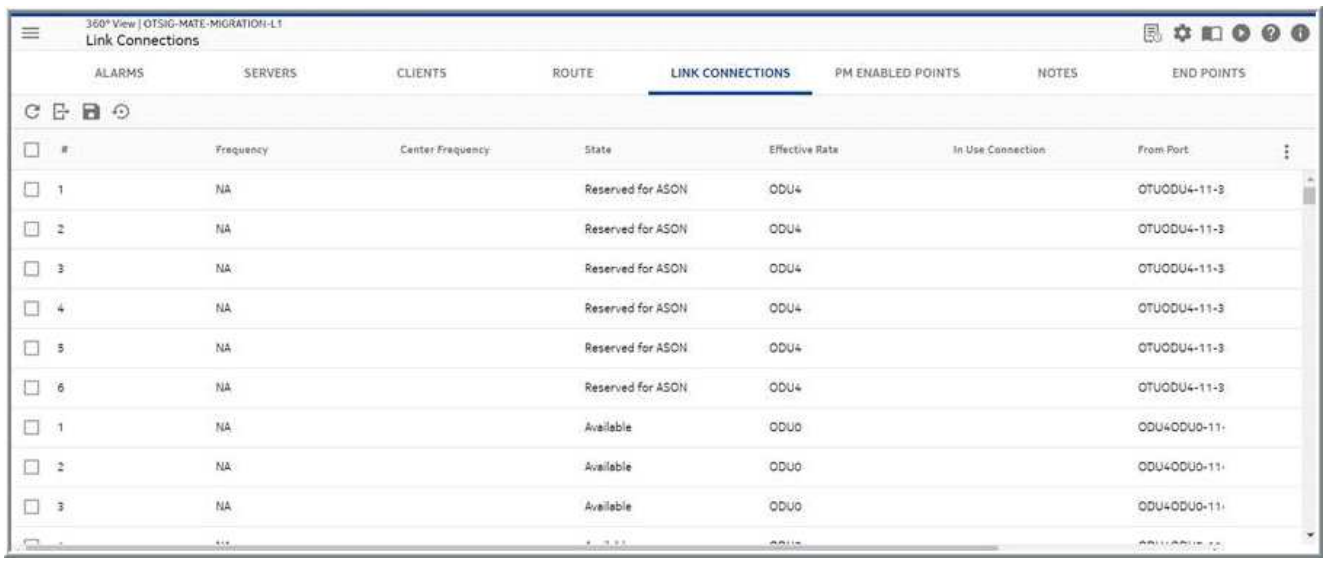
  In the **Deploy Rules** panel select
  - Service Rate Type: Trail
  - Rate: OTSig Tunnel

    The **Connection Type** field is automatically set to **2 Ended Bi (I)**.
  - Select the From and To Node and the ports that are the S4X400 NE ports
  - In the Connection characteristic panel, check the **ASON** field.
  - Insert the Connection Name.
  - In the Optical Line Characteristic panel select the Profile Number.

Click **DEPLOY** to create the tunnel.

In the **LINK CONNECTION** panel of the 360° View of the created tunnel, you can list the ASON reserved channels.

Figure 9-18 ASON reserved channels



5

Create 10 G managed plane service from 20P200 to 20P200

See "Deploy a new service or infrastructure connection with template" (p. 1216) for detailed description of the create infrastructure and service procedure.

- From the WebUI follow the path **DEPLOY > New Service/Infrastructure**
- Select the template **ODUk/OTSig Tunnel - Unprotected** and click on **Deploy...**

  In the **Deploy Rules** panel select
  - Service Rate Type: Ethernet
  - Rate: 10 GbE

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Select the From and To Node and the ports that are the 20P200 NE ports
- Insert the Connection Name.

Click **DEPLOY** to create the connection.

In the **LINK CONNECTION** panel of the 360° View of the created tunnel, you can list the used connections for the created service.

Figure 9-19 Service Created - Used Connections

6

Create 1G managed plane service from 8P20 to 8P20 packs.

In case of cascading to 8P20 from 20P200. Assign ILKN to one of the unused backplane port of the 20P200

For example: if BP1 of 20P is set to ILKN then ports from 1 to 10 of 20P can be used to create OS with 8P20 Line side.

If BP2 of 20P is set to ILKN then ports from 11 to 20 of 20P can be used to create OS with 8P20 Line side.

Create the Sub 10G MP service from 8P20 to 8P20.

7

Create a 100GBE/ODU4 NNI PATH ASON routed service connection between S4X400H client ports.

Note: 100 G MP service between S4X-S4X is not allowed over MRN Tunnel.

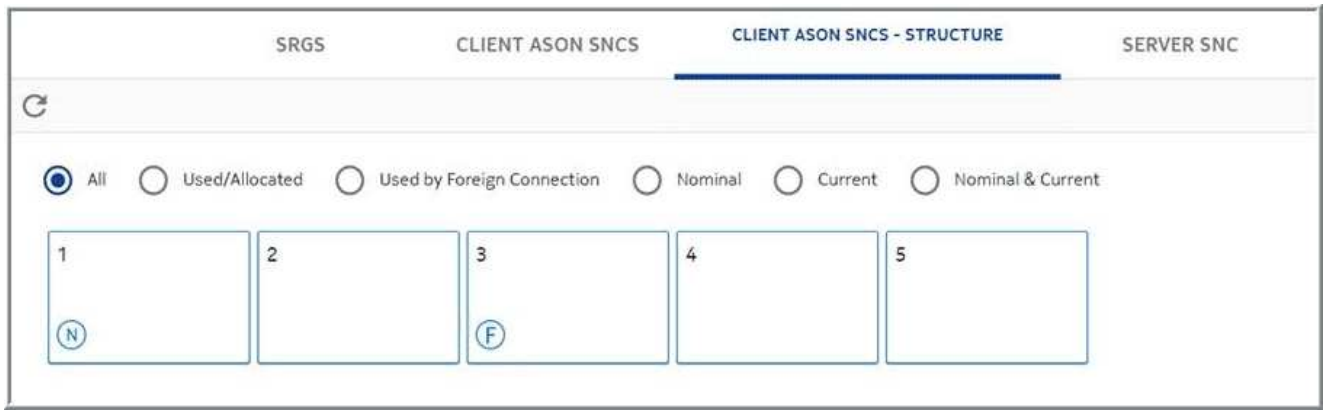
If user tries to create Managed Plane service when no Virtual Server is created on top of OTSig MRN tunnel the MP service creation fails with following error message:

System could not find route as no VS is generated, please check BP ports assignment rule and mating rule first then proceed further.

• OTSig MRN Tunnel PAYMAP structure tab is shown/updated with **F** entry for MP service which is being created on top of MRN tunnel. If the Managed Plane service is deleted, the entry returns to available state, the **F** is erased.

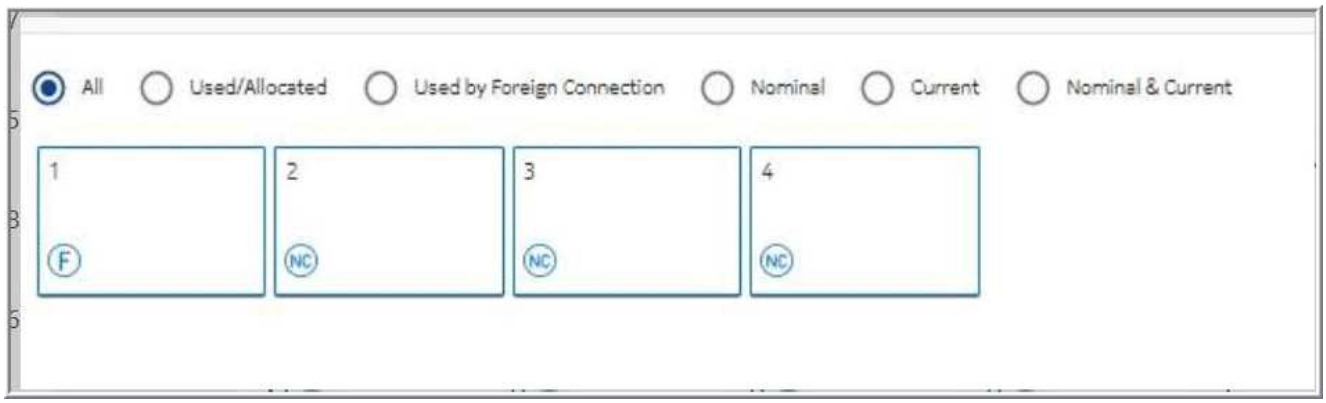
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-20 Client ASON SNC Structure - 1



• OTSig MRN Tunnel PAYMAP structure tab is shown/updated with **N** or **C** or **NC** entry for ASON Control Plane service which is being created on top of MRN tunnel.

Figure 9-21 Client ASON SNC Structure - 2



End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

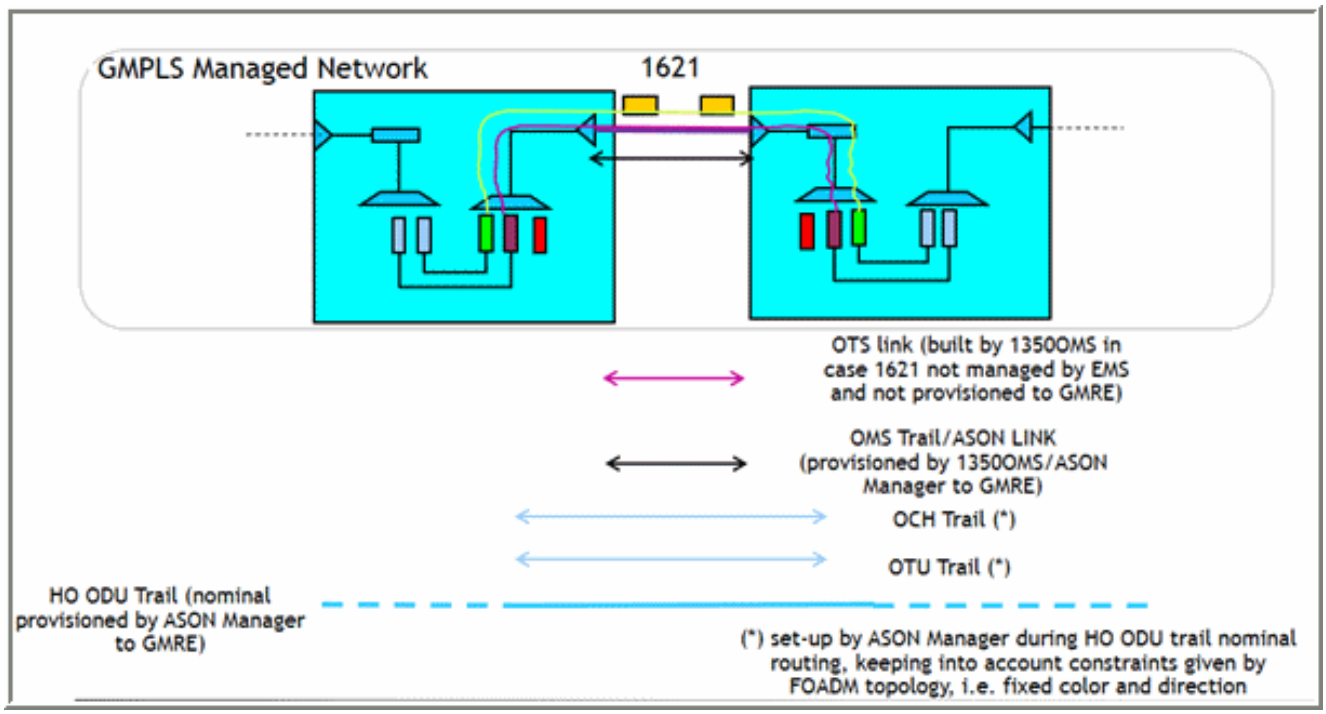
Longspan Support in NFM-T

9.15 High Level Steps Sequence

Overview

The figure shows the characterization of an OTS span between two 1830 PSS-PHN stations with 1621 SLE submarine in-between as *Ultra Long Span*.

Figure 9-22 Support for Longspan



Steps Sequence

1

The NFM-T uploads managed NEs and related ports. The GMRE presence is detected on uploaded NEs

2

If 1621 SLE Network Elements are managed by EMS/XoS, the NFM-T user creates the OTS Link between 1621 NEs and OTS ports. If the NEs are not managed by EMS/XoS, the user creates OTS links between 1830 PSS Network Elements. See 2.22 “Link connections” (p. 244) and 2.24 “Auto Discovery” (p. 248)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

Implement the OTS link, the OMS trail is automatically built between OMS terminations on top of the OTS links and also on top of ASON link (1:1 with OMS Trail) in case of GMRE presence on the two 1830 PSS at the edge. If the longspan info is available on the NE's OTS port, then the info is propagated to the OMS/ASON link, otherwise the user has to manually provision it.

4

Discover the internal cables inside 1830 PSS NE, see Auto DiscoveryThe information about the equipment configuration (D, D', FOADM, and so on) are recognized and stored in NFM-T. The information are color/colorless, direction/directionless, and the OCH matrix connectivity restrictions.

5

Any alarms on OTS ports is correlated to the related OTS link, any alarm on OMS is correlated to both OMS trail and ASON link.

6

Create the NPA describing the ASON domain, see 10.8 “Create and remove an NPA” (p. 1443), then add the ASON links internal to ASON domain as I-NNI type, and the links at the boundary of the ASON domain as Drop links. See 10.15 “Add links and remove links from ASON” (p. 1462)

7

Implement the NPA. All the commands are sent to the GMRE to describe the ASON domain topology in terms of data bears and TE-Links with related SRGs and costs.

8

Allocate an HO ODU trail, two layer routing (HO-ODU/OCH so to optimize routing also in case of 3R). The OCH matrix restriction (Stage 4)

9

Implement the HO ODU trail. The HO ODU LSP full nominal route is calculated and provisione to GMRE.

10

The setup of cross-connections on the NE is done manually on the NE.

11

The user can display the HO ODU LSP nominal route and each server OCH trail, including the trail on the Long Span.

12

The current route for a given LSP can be retrieved from GMRE.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Foreign Connections

9.16 Foreign Connection management

Foreign Connection management in L0 Control Plane (CP)

A **Foreign Connection** can be generically defined as a connection that crosses different domains. This is an end-to-end *Managed Plane* connection that uses *ASON* resources but is not restored.

L0 CP admits the creation of the Foreign Connection by the Managed Plane in L0 CP managed network/domain.

Foreign Connection can be created by the management system in the need to support both optical pass through in Metro-Core and/or Core networks, controlled by the L0 CP.

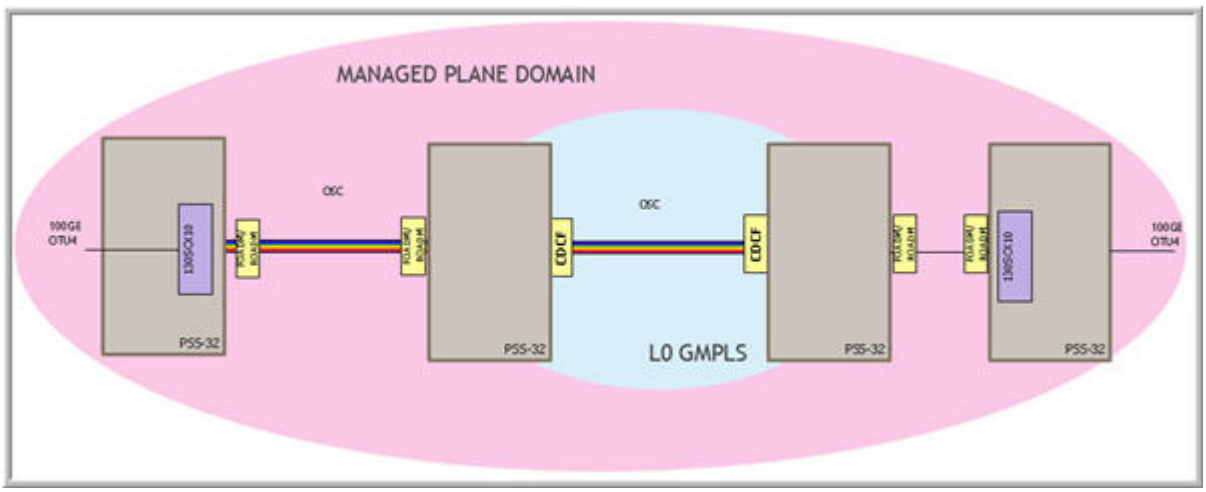
In all cases, L0 CP does not consider the Foreign Connection, simply tolerates the coexistence with connections initiated in L0 CP.

All the resources in L0 CP domain that are used by Foreign Connections are identified by the system as *"unavailable"*, so they are not used by ASON for restoration purposes.

Then, in this context, the concept of **"foreign"** apply only to **ASON** domain. Within OTN, it is just a regular managed plane connection that is routed through ASON domain. End to end routing is managed by OTN itself, ASON is not involved.

The following scenario illustrate an example of Foreign Connections crossing an L0 Control Plain domain.

Figure 9-23 Foreign Connection – Example of scenario



L0 NEs enabled with GMRE can be partially or not at all involved in the restoration network, similar to L1 NEs

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

ASON impact

Foreign connections may have impact also on ASON networks:

- **ASON L0 NPA definition changes.**
  The user may need to perform L0 resource partitioning on OTS links. Not all OTS links are added in L0 restoration network. Links and ports intended to be used for Foreign Connections are moved out of the restoration network.
- **ASON does not manage** the portion of the connection going through ASON domain. It only ensures that resources assigned to these connections are blocked and not available for Control Plane routing and restoration purposes. Resources are released and available by CP when OTN deletes the connection.
- **ASON does not provide** restoration of Foreign Connections, within Control Plane domain.

Note: The OTS links connecting to Managed Plane nodes, that are not GMRE-enabled, cannot be included in the NPA domain.

Foreign Connection for OTSig Tunnel

OTSig Tunnel as a Foreign Connection is supported in ASON domain. The OTSig connection is routed across ASON domain without involving GMRE restoration.

Foreign Connection for OTSig Tunnel in Control Plane is supported for the following cards:

- S4X400H, S5AD400H, S6AD600H
- SFM6, DFC12, DFM6
  For DFM6, both single carrier and dual carrier foreign connections are supported.
- 4UC1T, 8UC1T
- 2UX200

To deploy OTSig Tunnel as a Foreign Connection, select **Allow ASON Resources** checkbox in the **CONNECTION CHARACTERISTICS** panel under **DEPLOY RULES** section.

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

Note:

- In NFM-T R22.6, a Foreign Connection using 3R is supported for Managed Plane resources and Control Plane resources with nodes not assigned to ASON NPA.
  When 3R constraint is added in a Foreign Connection, the OTSig trail parameter values are as follows:

Allow ASON Resources	hasASONReources	Indicates
`Yes`	`Yes`	OTSig trail towards Control Plane
`Yes`	`No`	OTSig trail towards Managed Plane

- For Foreign Connection, the timeslot under the **CLIENT ASON SNCS - STRUCTURE** tab is displayed with Ⓕ icon, see 25.13 “Client ASON SNCS Structure Tab” (p. 2085)

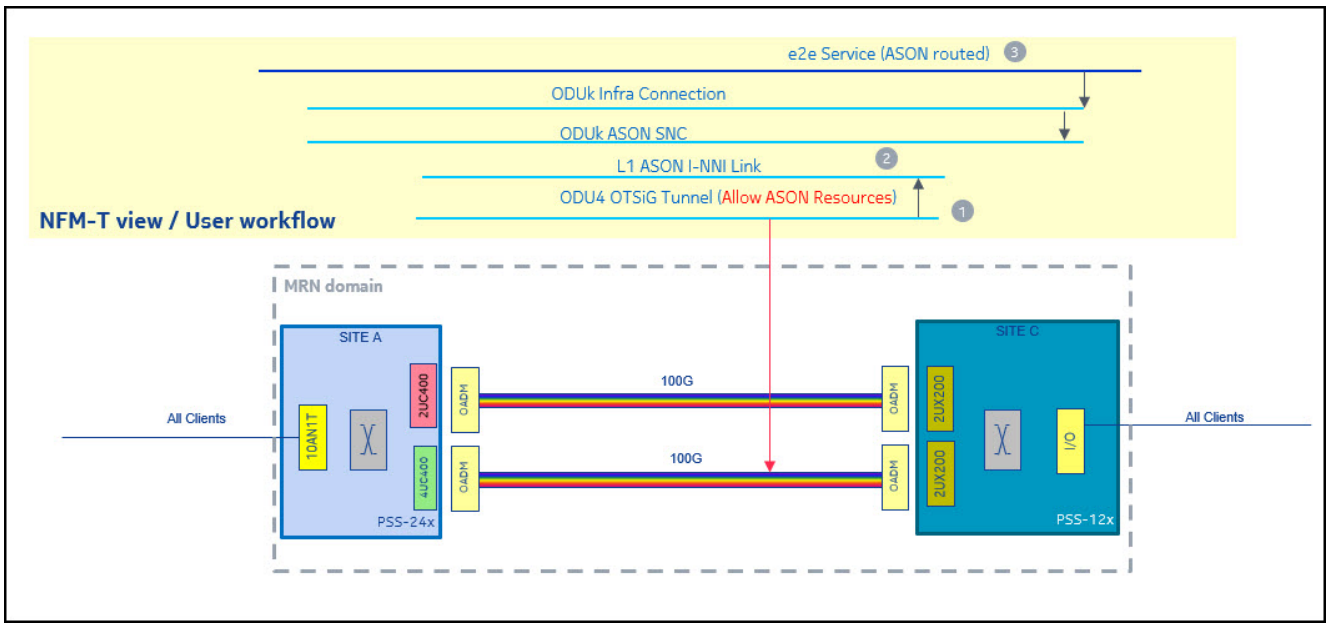
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Scenarios

The following illustrates the scenarios for OTSig Tunnel as Foreign Connection for 2UX200 and 10AN1T cards:

The user adds an OTSig Tunnel as Foreign Connection to ASON NPA, and then creates ASON routed client service on top of the OTSig Tunnel, see Figure 9-24, “Foreign Connection- ASON routed client service” (p. 1414)

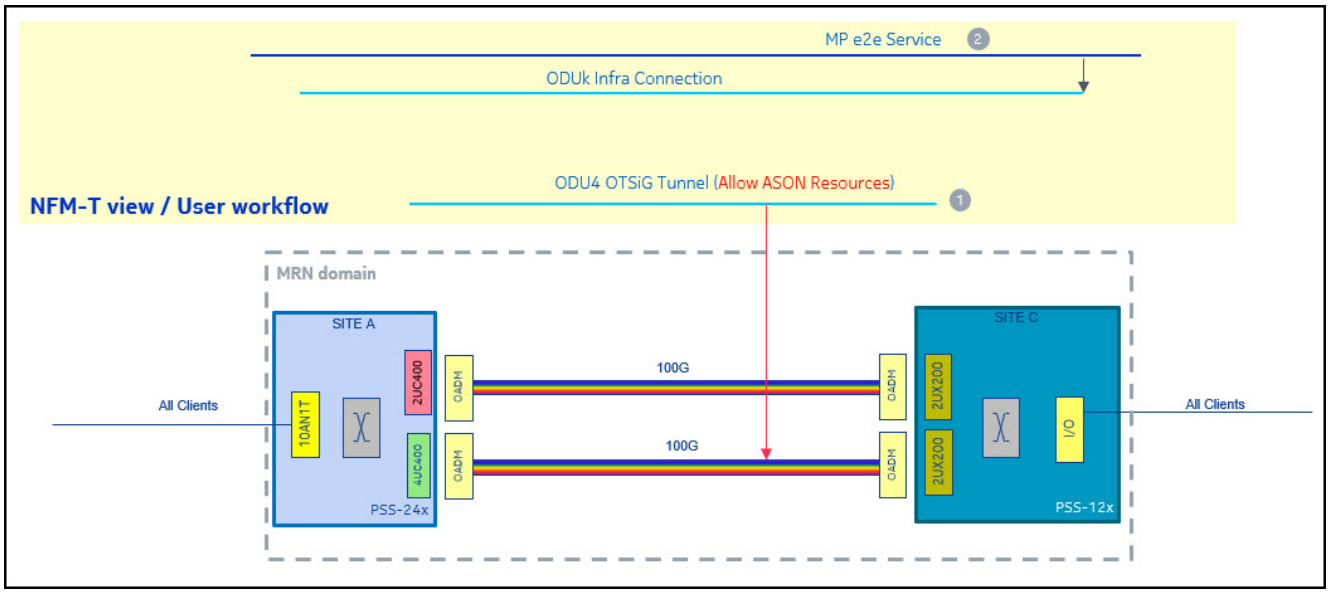
Figure 9-24 Foreign Connection- ASON routed client service



The user does not add the Foreign Connection to ASON NPA, and then creates a Managed Plane (MP) service on top of the OTSig Tunnel, see Figure 9-25, “Foreign Connection- MP service” (p. 1416)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 9-25 Foreign Connection- MP service



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

GMRE Naming Rules

9.17 Naming Rules for Long Span Support

GMRE Rules for correct naming of the cross-connections supporting Long Span

The user creates manually cross-connections for the setup of the Ultra Long Span OTS between two 1830 PSS-PHN stations with 1621 SLE submarine, and these connections have to follow the correct naming rules.

OCH Trail name syntax

The OCH trail name is defined as a string by the NE.

The GMRE uses the following syntax for:

- Source Transmit side of the OT: **`GMPLS: AtoZ: <dpNodeId>:<OtLinePort>`**
- Source Receive side of the OT: **`GMPLS: ZtoA: <dpNodeId>:<OtLinePort>`**

The *dpNodeId* is the assigned GMPLS node id for WDM node that generates the traffic. Therefore, the *dpNodeId* is dependent on the direction. The *dpNodeId* is a unsiged32 bit integer.

The *OtLinePort* is the index of the OT line port in receive direction, the composition is listed in the table:

Table 9-2 OtLinePort composition

OtLinePort digit	Value
d7d8	02 - L0 addressing transparent port, 04 - L0 addressing OTU client port, (15 for MRN or 17 for UNI) (i)
d5d6	OT line port index (p)
d3d4	OT board (b)
d2	shelf id the OT is plugged in (s)
d1	rack id - usually rack 1 (r)
`rssbbppii` in decimal	

An example of port ID is:

```
12030402 with rack = 1, shelf = 2, board = 3, port = 4, index 02
```

An example of a GMPLS OCH trail is:

`GMPLS: AtoZ: 4711:102030402`, with data plane node id **`4711`** and the port as described in the Table 9-2, “OtLinePort composition” (p. 1417).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

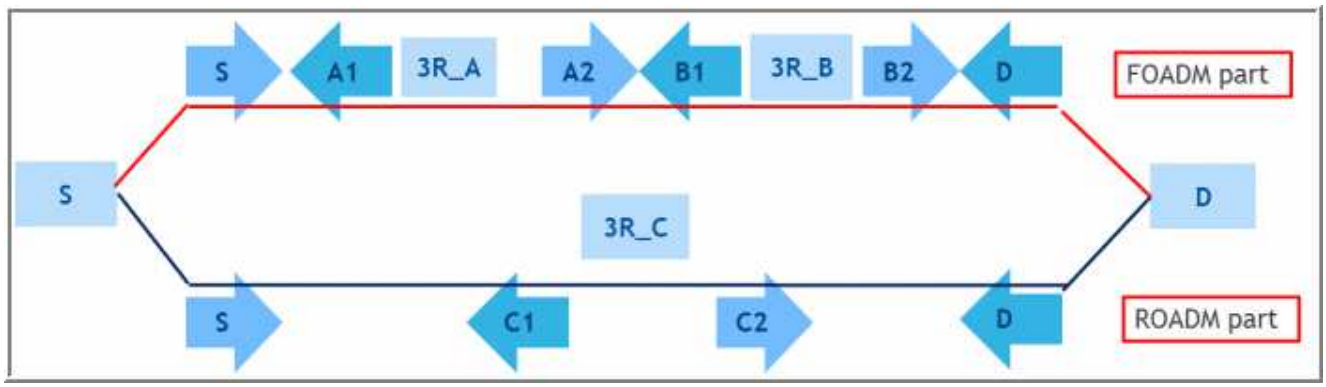
The OCH trail name usage with OPSA and unidirectional 3R are shown in the figure Figure 9-26, “OCH Trail Name Usage” (p. 1417) with 3R points on the FOADM and ROADM legs. A 3R point stitches together two independent OCH trails, one for each direction.

S: generates the **`S trail name`** in transmit direction and receives **`A1`** from FOADM main and **`C1`** from ROADM spare side: the *dpNodeId* for **`S`** is the *dpNodeId* of S trail, for **`A1`** it is the *dpNodeId* for **`3R_A`** and for **`C1`** it is the *dpNodeId* for **`3R_C`**.

D: generates the **`D trail name`** in transmit direction and receives **`B2`** from FOADM and **`C2`** from ROADM side: the *dpNodeId* for **`D`** is the *dpNodeId* of **`D`**, for **`B2`** it is the *dpNodeId* for **`3R_B`** and for **`C2`** it is the *dpNodeId* for **`3R_C`**

3R_A: generates **`A1`** toward the source and **`A2`** towards the next 3R and receives **`S`** from source and **`B1`** from **`3R_B`**: the *dpNodeId* for **`A1`** and **`A2`** is the *dpNodeId* for **`3R_A`**, for S it is the *dpNodeId* form S, and for **`B1`** it is the *dpNodeId* for **`3RB`**.

Figure 9-26 OCH Trail Name Usage



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

9.18 GMPLS Support Preconditions

Overview

The following items are preconditions for GMPLS support:

1. FOADM leg must be assigned to main in the OPSA commissioning.
2. FOADM OPSA XCs must be present when OT is assigned to GMRE. For OPSA in GMPLS they must be unidirectional to allow 3R points.
3. FOADM OPSA XC OCHTrail names must be in GMPLS syntax in both directions and they must be consistently with the peer end configuration.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10 Working in ASON

10.1 Overview

Purpose

This chapter provides the end-to-end working of ASON in the NFM-T GUI.

Contents

10.1 Overview	1421
Deploy phase	1424
10.2 Deploy connection- ASON specific parameters	1424
10.3 Connection creation - ASON specific	1429
10.4 ASON protected trail on 11QPA4 card	1432
10.5 Path alarm based restoration movements	1433
Operate ASON NPAs	1438
10.6 ASON NPA	1438
10.7 Cluster configuration for Control Plane	1440
10.8 Create and remove an NPA	1443
10.9 View the list of NPAs	1447
10.10 ASON NPA table columns	1450
10.11 More operations on ASON NPA	1452
10.12 ASON NPA state transition diagram	1453
10.13 ASON link state transition diagram	1457
10.14 Access and view the misalignment report for a link	1461
10.15 Add links and remove links from ASON	1462
10.16 Modify TCM defect raising time	1470
10.17 Assign an ASON I-NNI link to a TE Link and SRG	1473
10.18 Change ASON WTR	1475
10.19 Correlate an ASAP with an NPA	1477
10.20 Enable or disable auto restoration of links	1480
10.21 Implement/deimplement an NPA	1482

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.22 Manage 3Rs	1485
10.23 Manage jobs in ASON	1493
10.24 Modify TE Links	1495
10.25 Perform link maintenance	1497
10.26 Perform switched connection sync in Control Planes tab	1502
10.27 Set the ASON administrative state of links	1504
10.28 UNI management support for EPL service	1508
10.29 Upgrade CTP naming for Flexgrid support	1513
10.30 Activate GMRE for Control Plane NE	1514
10.31 View NE cluster configurations in ASON SNC and ASON NPA pages	1517
Operate ASON SNC	1521
10.32 ASON SNC	1521
10.33 View the ASON SNCs	1522
10.34 ASON SNC table columns	1527
10.35 More operations on ASON SNC	1532
10.36 ASON SNC state transition diagrams	1534
10.37 View the inherited priorities of an SNC	1542
10.38 View a misalignment report for an SNC	1544
10.39 Correlate an ASAP with SNC	1546
10.40 Enable/Disable the test mode for an SNC	1550
10.41 Manage SNCP in ASON SNC	1553
10.42 Manage SNC constraints	1554
10.43 Modify the attributes of an SNC	1557
10.44 Switch SNC routes	1560
10.45 Set a preconfigured Backup Route in ASON SNC	1563
ASON synchronization	1568
10.46 Overview	1568
10.47 Introduction	1569
10.48 Perform ASON NPA synchronization	1570
10.49 Perform an ASON SNC synchronization	1574
Manage Reversion Control Group	1577

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.50 Overview	1577
10.51 Reversion Control Group	1578
10.52 Create Reversion Control Group	1579
10.53 View and remove the Reversion Control Group	1584
10.54 Reversion Control Group table columns	1587
10.55 Manage and schedule the jobs for Reversion Control Group	1588

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Deploy phase

10.2 Deploy connection- ASON specific parameters

Overview

The NFM-T follows the G.709 standard layer rates for connection provisioning, but with minimal entry from the part of the user. The only fields that are to be populated when provisioning infrastructure connections or services are those fields that specify the from and to nodes and ports. The user has the option to populate other fields from the selected template or the user can select the default value. The system automatically discovers the required physical connections.

Deploy connection

The **Connection** window has multiple tabs to assist in the deployment of the connection.

- DEPLOY RULES
- ROUTE CONSTRAINTS
- PARAMETERS
- SUMMARY
- DEPLOY

Note: *Transmission Parameters settings are not supported for Mixed Plane and Control Plane connections.*

For the description of all the parameters of the Deploy Connection window, see "Deploy a new service or infrastructure connection with template" (p. 1216).

Connection characteristics

The following fields are displayed in the **CONNECTION CHARACTERISTICS** tab for ASON:

Table 10-1 Connection Characteristics

Parameter	Description
Allow Ason Resources	This parameter is used for the connection creation of HO ODUk trail and ODUk service integrated provisioning of Managed Plane connections. Check this check box to create managed plane using ASON resources. If the check box is not checked while provisioning, connection fails with an error message indicating that OMS link is CP. The LC state of the OMS Link Connections is shown as **Available** which means OMS links are capable of carrying both MP and CP connections. When the resource is used, the state changes to **Used in InEffect/Implemented**. See Figure 10-1, "Link Connection Tab" (p. 1426)
ASON	The **ASON Routed** field is a check box. It displays a check mark if the connection is to be a Control Plane or 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.

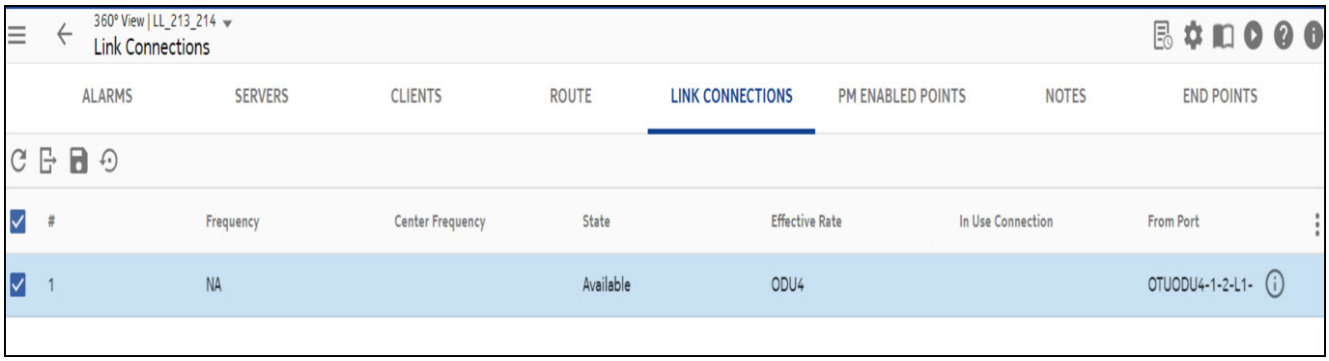
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 10-1 Connection Characteristics (continued)

Parameter	Description
ASON Tunnel	*Optional*: If the **ASON Routed** field is checked, the **ASON Tunnel** field is displayed for infrastructure connections with these exceptions: The ASON Tunnel field is not displayed for OPSA Alien Wavelength (OCH) and OMS-P Protected OMS connections. If the **ASON Routed** field is checked for an infrastructure trail, the **ASON Tunnel** field is a check box that is displayed. Check it to select the type of ASON tunnel.
Provisionable Wave Key	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** From R21.4, the user can provision Unkeyed service in ASON domain.
Tunnel Type	The Tunnel Type field is a drop-down list to select the type of ASON tunnel. The possible values are : **MRN Terminated**, **MRN UnTerminated** or **L0-L1 Overlay**. See 9.5 "Overlay Configuration in GMPLS Domain" (p. 1379)
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** • With **No Restoration**, traffic is lost if a failure occurs • With **Source-based Restoration**, the Control Plane protects the traffic if a failure occurs by calculating a new route • With **Guaranteed Restoration**, the restoration path is pre-calculated and it improves the restoration time respect to SBR type. The **Guaranteed Restoration** option is supported for L0 Control Plane. All 10G and 100G OTs support MRN naming. However this naming is not supported for the following: • Cards: - D5X500 - D5X500L - D5X500Q - 12P120 - S13X100R - S13X100E • ASON Restoration Type - Guaranteed Restoration If ASON SNC is provisioned with **Source-based Restoration** restoration type, and user wants to modify the restoration type to **Guaranteed Restoration**, it fails with error - "Guaranteed Restoration is not supported for MRN ports". To overcome this issue, it is suggested to create ASON SNC with restoration type as **Guaranteed Restoration**, and hence the user is allowed to change the type from **Guaranteed Restoration** > **Source-based Restoration** > **Source-based Restoration**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-1 Link Connection Tab



Routing Constraints tab

See "Route Constraints" (p. 1244).

The control plane connections supports partially qualified routing for manual connections. If the user selects Manual Routing, and provides *partial* routes, ASON Routing finds the complete route or the remaining route honoring the partial route passed.

Restoration tab

In the **RESTORATION** subtab in the **PARAMETERS** tab, the following fields are displayed for ASON:

Table 10-2 RESTORATION sub tab

Parameters	Description
ASON Tunnel	The Tunnel Type field is a drop-down list to select the type of ASON tunnel. The possible values are : **MRN Terminated**, **MRN UnTerminated** or **L0-L1 Overlay**.
L0-L1 Overlay	Specifies the Overlay

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 10-2 RESTORATION sub tab (continued)

Parameters	Description
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** • With **No Restoration**, traffic is lost if a failure occurs • With **Source-based Restoration**, the Control Plane protects the traffic if a failure occurs by calculating a new route • With **Guaranteed Restoration**, the restoration path is pre-calculated and it improves the restoration time respect to SBR type. The **Guaranteed Restoration** option is supported for L0 Control Plane. All 10G and 100G OTs support MRN naming. However this naming is not supported for the following: • Cards: - D5X500 - D5X500L - D5X500Q - 12P120 - S13X100R - S13X100E • ASON Restoration Type - Guaranteed Restoration If ASON SNC is provisioned with **Source-based Restoration** restoration type, and user wants to modify the restoration type to **Guaranteed Restoration**, it fails with error - "Guaranteed Restoration is not supported for MRN ports". To overcome this issue, it is suggested to create ASON SNC with restoration type as **Guaranteed Restoration**, and hence the user is allowed to change the type from **Guaranteed Restoration** > **Source-based Restoration** > **Source-based Restoration**.
TCM Level	The **TCM Level** field is a drop-down list that determines the Tandem Connection Monitoring level. The values are no TCM (the default), Level 1, Level 2, Level 3, Level 4, Level 5, or Level 6. See 2.28 "TCM connections" (p. 268) Level 6 is a private level and the user cannot use it.
Max Latency	The users can enter the value that is needed.
Default Priority	The value 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	Values are Manual (the default), Auto, or Soft Automatic.
Wait For Server Restoration	Values are Disable (the default), Enable, or Not Applicable. This field is applicable only for MRN infrastructure.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Table 10-2 RESTORATION sub tab (continued)

Parameters	Description
Include Any Color Name	The **Include Any Color Name** field is an icon-activated field. Click the **Search** 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 of same color that is allocated to the link. Resource Coloring helps 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. Click the **Search** 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 of 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
Max Path Alarm Based Movements	The **Max Path Alarm Based Movements**field is a text box. The default value is 0. The value range is 0-5. If value=0 the Path Alarm Based Movement by GMRE is Disabled. The field applies to L0 and MRN CP connections and not applicable to L1 CP connections. When the value is increased to > 0, **Movement Hold Off Time (in secs)** parameter is enabled. Parameter applies for a L0 CP or MRN SNC (not for a L1 CP and L2 UNI Services).
Movement Hold Off Time (in secs)	The **Movement Hold Off Time (in secs)** field is a text box. Path Alarm Based Movements uses a configurable move-hold-off time (per LSP) during normal time . The default value is 300. The value range is between 30secs and 1h(3600secs). Default=5 mins (300secs). This field is applicable only when the number of configured attempts is >0 and when fault was not present in the first 5 mins after setup and restoration. Parameter applies for a L0 CP or MRN SNC (not for a L1 CP and L2 UNI Services).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.3 Connection creation - ASON specific

Connection creation and OTS links as constraint

Creating an ASON connection in L1 (OCS), physical links of type OTS cannot be provided as constraints, because in the SNC L1 allocation phase the creation cannot be done correctly. Routing of L1 connection does not take into account OTS links unless this is a tunnel.

In case of allocation L1 SNC terminated on two L1 termination points, the relation between physical OTS link and logical ASON link is not known.

If the OTS physical links termination points belongs to an MRN tunnel, then they can be used as constraint for the ASON L1 connection.

ASON implicit server and Alarm Profile

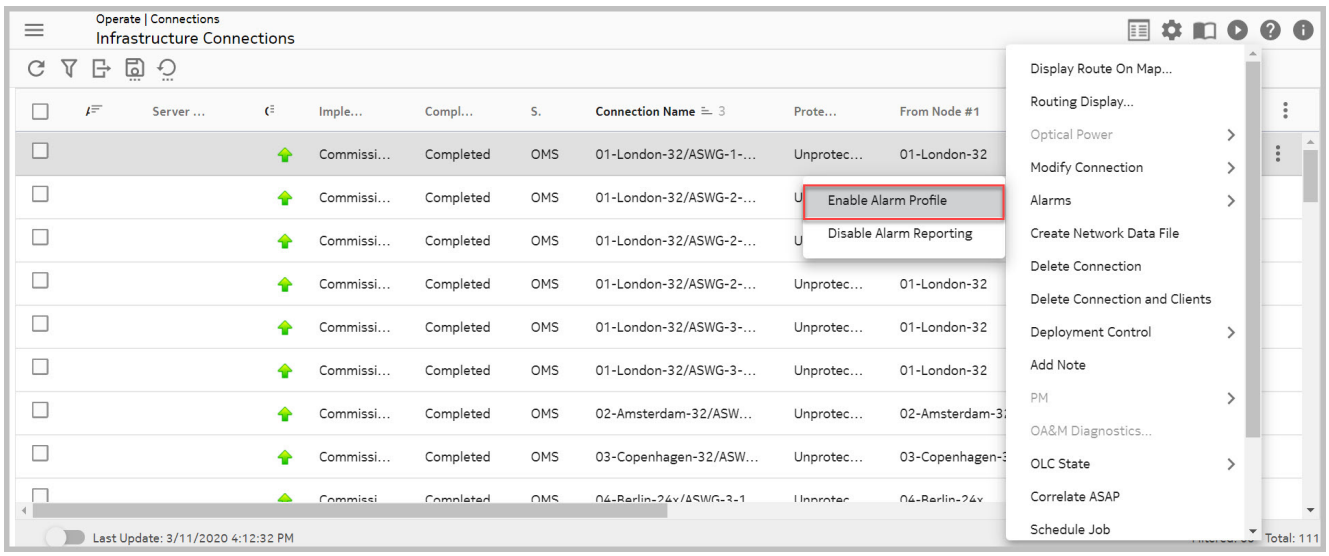
ASAP profile is not set on the ASON implicit server connection during the Connection Creation using the Assurance tab on the Connection Creation window. This is the behavior because no commands are sent by OTN application for the implicit server connection category during Connection Creation.

The user can enable or disable ASAP profile on this connection category, once the connection is created and available in 360° overview page.

To modify the alarm profile setting, navigate as **OPERATE > Infrastructure Connections**, then select the connection in the list, click the **More** icon and select **Alarms > Enable Alarm Profile** from the popup menu.

See "The Category of a connection" (p. 225) for further details.

Figure 10-2 Connections List - Select Enable ASAP



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

L1 Control Plane support

The L1 Control Plane configuration is supported also on 1830 PSS-8x Network Elements, the supported cards are:

- IUX200 as uplink card;
- 20MX80 and 20AX200 are the I/O cards.

1830 PSS-8x NE interworks with OCS and 1830 PSS-24x cards:

- **OCS cards**: 130SCUPC and 130SCUPH
- **1830 PSS-24x cards**: 1UC and 4UC

See 9.11 “MRN and Intra Node Link” (p. 1391) and 9.12 “Unterminated FA Tunnel Support” (p. 1395) for further details.

Route computation with 3R in ASON

When a 3R is present in the setup of a connection, ASON algorithm chooses the frequencies of each OCH span separated by 3R independently and according to the loading plan.

In case same frequency is needed the user specifies the routing constraints.

The figure displays an example for a provisioned ODU4-8QAM trail from D5x500L-100GBE-prop with a 3R constraint given. The WLT shows two different frequencies at the span before the 3R and after the 3R.

Figure 10-3 3R in ASON example

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.4 ASON protected trail on 11QPA4 card

Description

To manage the configuration of 11QPA4 with E-SNCP correctly, it is necessary to configure it in advance and do a port synchronization only when all ports are configured.

This is a prerequisite because ports must be considered together for the provisioning, in order to upload the correct ASON configuration. The single event of internal cabling or signal type configuration on an individual port is not enough to upload the correct configuration. The protection schema can be taken into account only after the port synchronization operation.

The correct provisioning flow is:

- Port Configuration, see *Equipment Management* section of the NFM-T NE Management Guide.
- Port synchronization. To perform the port synchronization for the NE. Select **OPERATE > Nodes** from the menu option. Right click on the involved NEs land select **Synchronize > Ports**.
- Provision the ODUk / DSR path.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.5 Path alarm based restoration movements

Overview

NFM-T manages the path alarm based restoration movements by GMRE. This allows full end-to-end diverse route of LSP current upon intermediate OTU transmission alarms or intermediate equipment failures. Two new parameters are managed by NFM-T for Connections ASON Routed in L0 CP or MRN domain and with Restoration Mode SBR/GR to trigger the path alarm based GMRE restoration. OPS protected services is also supported, that is, SNCP/PRC, in L0 and MRN configurations. Path alarm based restoration movements are not applicable for OCH service with Alien restoration.

Purpose

The Path alarm based restoration movement feature allows moving a service away from its current route when it has failed, and no restoration is triggered. Therefore, failure is due to undetected root cause.

Restoration triggers are defined as root cause along a service and restoration is diverse to the point of failure which might be a span failure, an equipment failure, or a connectivity failure.

The path alarm based restoration movement is triggered, when service is failed, no restoration trigger with point of failure is raised, and performs full end to end diverse. It is a movement, like a soft-reroute, and performs only when there is an alternative path and is performed like a maintenance action using the lowest setup priority and no preemption using the setup=holding priority.

Undetected root cause problems happen when (intermediate) nodes are not available, or specific NE hardware errors are not handled by GMRE.

The main criteria of path alarm based restoration movement is the monitoring of end points. For example, It could be a TCM-TTP being present on the uplink cards that monitors the health of the TCM segment end to end. However, TCM is not available on most of the OTs. Therefore, the GMRE takes into account the OTU TTP layer alarms on the end points. As Layer 0 services can pass across 3R, and 3Rs terminate the OTU layer and looping back the OTUODU signal, an end to end correlation on the OTU end points is required. Ensure that the path alarm based restoration movement must not be performed on Service End point equipment failure. 3R points are not end points and movement can be performed through a different 3R.

Path alarm based restoration movement must also be supported on OPS protected services when a protection leg fails, based on the ops-port loss state.

Path alarm based restoration movement guidelines

Following are the guidelines for a management of path alarm based restoration movement:

- The Path alarm based restoration movement can be disabled and enabled per service. Default is disabled.
- The Path alarm based restoration movement uses a configurable move-hold-off time (per LSP) during normal time . Default is 5 mins. The range is from 30 seconds to 1h = 3600sec.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- If the Path alarm based restoration movements at a given time is not possible (for example, when there is no route), then the node shall retry periodically every 5 mins as reattempt time.
- The Path alarm based restoration movement are applicable for the following conditions:
  -
    - path alarms are raised, and
    - the move-hold-off-timer expired, and
    - no restoration trigger happened, and
    - no end point failures are reported.
  - If movements are not possible (no route), then the node must periodically retry to move to the maximum number of movements.
  - If end point failures are cleared while path alarms are present and a movement shall be triggered with the next reattempt.
- The Path alarm based restoration movement are not applicable for the following:
  - When restoration is triggered
  - When maintenance movements are attempted (nominal reversion, soft reroute)
  - When one or both of the two end points have end point failures
- Path alarm based restoration movements are applicable for Layer 0 and MRN tunnel services, but not for Layer 1 ODU or Ethernet UNI services.
- Path alarm based restoration movements are not applicable for alien services due to missing of OTU monitoring capabilities.

Supported configurations and scenarios

Layer 0 services

Alarms are detected on the OT line ports (end points and 3R) and forwarded through RSVP signaling to the source node for alarm correlation.

The use cases when the Path alarm based restoration movements are triggered are as follows:

- When the path alarm is present
- When no end point alarm is present
- When move-hold-off are expired
- When reattempt timer has expired
- When maximum attempts are not reached

A diverse path is requested when the following conditions are met/matched:

- If a new route is found, then move traffic
- If no new route is found, then retry periodically every 5 mins to get a new route.

When the conditions change or are not matched, the events that happen are as follows:

- When EP point failure disappears, then allow movement
- When maximum reattempts are changed to lower than the counter, then do not move until maximum attempts are reached higher than the counter
- When maximum reattempts are changed to higher value, then allow movement

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

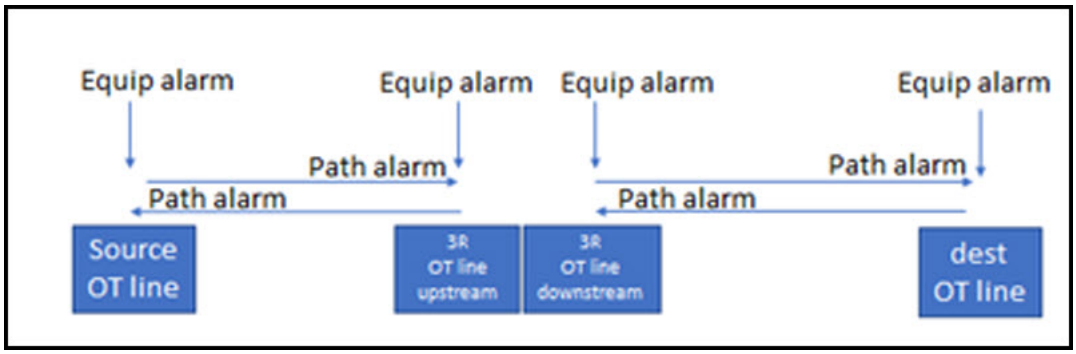
- If path alarm is cleared, then cancel reattempt and do not allow movement
- When restoration alarms are triggered (trigger restoration or maintenance action), then clear the move-hold-off-timers and clear reattempt counter

Note: While path alarms are present, and move-hold-off timer are expired, a reattempt timer is triggered each 5 mins.

L0 alarm processing

L0 path based alarm restoration movement requires handling on each transmission OCH segments. The movements are from source to 3R, from 3R to 3R, from 3R to destination.

Figure 10-4 L0 path based alarm movements



Each OCH segment is generated and terminated and allows bidirecitonal fault handling as well.

MRN tunnels

The TEP alarm triggers client restoration independently from the L0 LSP movement. The movement may appear at any time independent of the client layers.

Protected services

NFM-T reacts with path movements on OPS switch events when active legs are failed and not triggered for restoration.

In case of movement, the new route is diverse to the redundant leg and the current route(s) of the failed leg.

For example, If an OPS protected service has only one working leg, when it falls back to SBR, then the normal path alarm based restoration behavior for single legged services is applicable.

Path alarm based restoration movement configurations/reporting

LSP configuration

Maximum number of movements: 0 = disabled, maximum number - 5, default 0

Path-alarm hold-off timer: 30secs to 1hour, default 5 mins

LSP alarms

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

ReversionBlocked-due-to-movement or **Reversion Blocked – Path Alarm Movement (at NFM-T user)** - indicates that automatic reversion is blocked for movements due to unknown reasons. Alarm is cleared on restoration or reversion.

The **Reversion Blocked- Path Alarm Movement** alarm is raised by GMRE when the OTU Path alarm is present and GMRE has successfully performed the first movement.

MovementBlocked or **Path Alarm Movement Blocked – Max Reached (at NFM-T user)** - indicates that no more movements are performed as maximum number of movements has been reached. Alarm is cleared on restoration or reversion. Alarm is not raised when maximum is 0. The alarm will be raised for main and spare legs separately.

Path Alarm Main Movement Blocked – Max Reached and **Path Alarm Spare Movement Blocked – Max Reached** are raised by GMRE respectively for main or spare leg when the following conditions are met for that particular leg:

- Move attempts by GMRE is equal to the provisioned maximum number of attempts and **Reversion Blocked – Path Alarm Movement** is raised when the OTU Path alarm is still present.
- Next move is tried by GMRE

Path alarm movement attempts and diversity

A path-alarm-based movement is full diverse to the current route (first attempt). All subsequent movements are diverse to the sum of current routes (from second, third, and so on). The full diverse excludes required diversity for cluster links and C-F links (so single links from OT to mesh).

A restoration trigger or maintenance (including reversion) command clears the diversity list and the attempt counter.

An LSP in LSP-maintenance mode does not have movement. As each movement causes a change on the current route. In case of no-route-found and movement has not reached the maximum attempts, then the movement is triggered periodically every 5 mins.

Path alarm based restoration movement provisioning

The two parameters that are applicable for a L0 CP or MRN SNC (not for a L1 CP and L2 UNI) in the ASON Routed Connection, Restoration tab are as follows:

- **Path Alarm Based Movements Attempts** (value range 0-5, default=0)
  If value=0, then the Path Alarm Based Movement by GMRE is disabled.
- **Path Alarm Based Hold-off-time** (value range 30secs-1h, default=5 mins)
  Applicable only in case, the number of configured attempts is >0 during the normal time. Applicable when the fault was not present in the first 5 mins after setup and restoration.

Note: Path Alarm Based Hold-off-time field is hidden in case **Path Alarm Based Movements Attempts** field is set to 0 (disabled).

Manual reversion to nominal

On detection of the new **Reversion Blocked- Path Alarm Movement** alarm on ASON SNC, GMRE blocks the automatic reversion. The movement by GMRE is based on the OTU end point alarm

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

detection and not on alarm root cause. As a consequence **Switch to Nominal** is enabled based on above **Reversion Blocked- Path Alarm Movement** alarm. The user needs to attempt **Switch to Nominal** only after clearing the path alarm on the nominal route else the manual reversion may not be successful and existing alarms on the ASON SNC shall continue to persist.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Operate ASON NPAs

10.6 ASON NPA

Description

The Network Protection Architecture (NPA), is a set of NEs, protection blocks, and physical links that work together to create a dedicated protection mechanism or are grouped together to establish service layer protection.

The NFM-T uses NPA to associate resources that are part of the same protecting structure. By creating and implementing the NPA, users can specify the role of a physical link and they can assign a reduction cost factor and a usage cost factor to the physical link.

When an ASON NPA is built, the related TE-Links are automatically created in the NFM-T and in the involved GMREs.

To see the list of NPAs use 10.9 "View the list of NPAs" (p. 1447)

Note: From R21.4, NFM-T supports a single ASON NPA with 1500 GMRE enabled nodes. Only GMPLS L0 nodes are supported in the ASON NPA.

NPA uses

The NFM-T uses NPA to associate resources that are part of the same protecting structure. By creating and implementing NPA, users can specify the role of a physical link and they can assign a reduction cost factor and a usage cost factor to the physical link.

NPAs, TE Links, and 3Rs

Associated with NPAs are the following related objects, which users can access from the NPA data table:

- A *Traffic Engineered link*, or a *TE Link*, is a unique application entity that is configured through grouping component links. The groupings can be based on different attributes such as SRGs, link metrics, or latency parameters.
- A *3R* is a user-selected optical regeneration group that consists of a node and two NNI transponder line ports that *reshape*, *retime*, and *retransmit* a signal.
- Higher order (HO) ODU 3R regeneration - client-client regeneration:
  - Configures two OTs cabled through client
  - Transponder regeneration: 11STAR1, 11STAR1A, 43STA1P
  - Add/Drop ports are listed on the cards for ODU3R regeneration
  - Add/Drop ports are listed for all the cards

NPA and L1/L0 terminated ASON SNC discovery

The ASON management of L1/L0 Terminated of ASON SNC discovery is:

- Complete NPA discovery

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Terminated L0/L1 E2E discovery of protected (SNCP/OPSA) connection and unprotected connection

The management of PSS24x NEs is at L1 and L0 level.

The operations on discovered connections and NPA can be managed from NFM-T GUI.

Related information

For information that is related to ASON, NPAs, SRGs, TE Links, 3Rs, and Color Profiles, refer to the following:

- "Connection setup using the nominal, optimal, and current routes" (p. 391)
- 3.8 "ASON protection and restoration" (p. 394)
- "ASON in NFM-T" (p. 379)
- 6.14 "Resource Coloring" (p. 627)
- 6.15 "Resource Coloring strategies and allocation example" (p. 629)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.7 Cluster configuration for Control Plane

Overview

A cluster configuration consists in managing a set of separately managed network elements together as a **Compound** node. The network elements are interconnected by optical lines where one or more network elements are treated as a **Main node** and one or more network elements are treated as a **Tributary node**. The terms **Main** and **Tributary** relates to the direction that a main node controls a subset of functions on ports on the tributary node using a management interface.

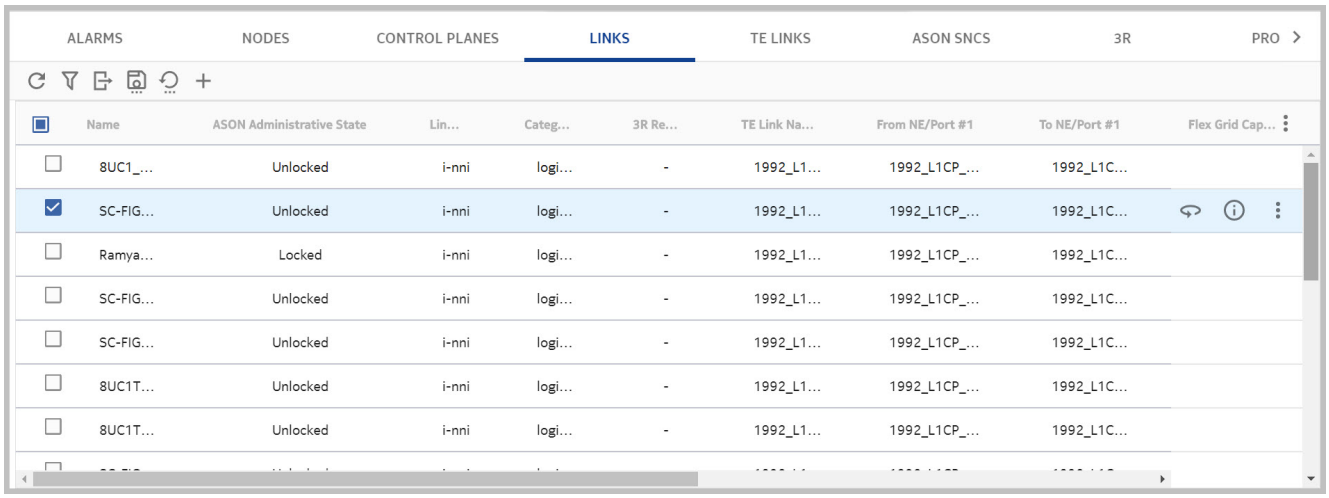
Note: Tributary nodes should be GMRE capable.

Cluster configurations are used in networks for scalability reasons. From 1830 PSS NEs R11.0 onwards, the node is scaled to support more than 24 shelves.

1830 PSS NE support release specifications	1830 PSS NEs supporting Cluster configurations on L0 GMPLS	1830 PSS NEs supporting Cluster configurations on MRN	1830 PSS NEs supporting Cluster configurations on L1 GMPLS
1830 PSS NEs R11.0 onwards	1830 PSS-8, 1830 PSS-16, 1830 PSS-16 II, and 1830 PSS-32	-	-
1830 PSS NEs R11.1 onwards	1830 PSS-8x, 1830 PSS-12x, 1830 PSS-24x	1830 PSS-24x, MRN unterminated	1830 PSS-24x
1830 PSS NEs R12.0 onwards	-	1830 PSS-24x MRN terminated or FA-TERM	-

OPS Links between the NEs in a cluster are supported and managed automatically by NFM-T/GMRE routing. The corresponding ports must be configured from EQM/NE. OPS links must be created from **OPERATE > Physical Connections** page. The drop links and the uplinks cannot be added manually for this OPS in NPA, but gets implicitly added as part of connection provisioning in L0. This drop link is the GMRE boundary. The administrative change in NPA is applicable only for L1 Cluster drop links. For L0 Cluster drop links, if user tries to change the ASON administrative state, then an error message is displayed.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.



For MRN, add the cluster link manually as i-NNI link to NPA.

Cluster configurations are supported in the combination of WDM mesh (1830 PSS-8/ 1830 PSS-16/ 1830 PSS-16II/ 1830 PSS-32) with a single OCS extension.

Following are the additional cluster configurations supported from R19.2 onwards:

- Cluster combination MxN SWDM NEs (only photonic 1830 PSS and transponders/ muxponders/ switchponders). 1830 PSS-32, 1830 PSS-16, 1830 PSS-16II, 1830 PSS-8 Extension/Tributary shelves with OTs in cluster configurations, called Drop OT, is supported in L0 GMPLS and MRN, and not supported in L1 GMPLS.

  1830 PSS-24x and 1830 PSS-8x Extension/Tributary shelves in cluster configurations is supported in L1 GMPLS, L0 GMPLS, and MRN.

  1830 PSI shelves, as a sub-group of drop OTs is supported in L0 GMPLS and MRN, and not supported in L1 GMPLS.

  Note:A set of OTs, 1830 PSI-2T, 1830 PSI-M is supported in tributary node.

  Examples: M x 1830 PSS-32/1830 PSS-16/1830 PSS-24x/1830 PSS-8x SWDM NE and N x SWDM NE. M corresponds to number of PHN NE and N corresponds to number of OCS NE.
- Cluster supporting off-grid tuning (FlexGrid) of the central frequency of 1830 PSS SWDM OTs and uplinks.
- Cluster configurations with OCS is not supported on 1830 PSS R11.0 and 1830 PSS R11.1 NEs.

Following are the limitations in cluster configurations:

- OPSA/OPSflex protection is not supported for cluster configuration. This is applicable only if the OPSA/OPSflex is located in the main NE of cluster (with filters/WSS), and not if it is together with an OT pack. OPSA/OPSflex protections for uplinks is not supported by GMRE.
- Default OPSA protected configuration is supported when both the OPSA and OT packs are on the main shelf.
- 3R is not supported if the 3R is hosted on a secondary NE of the clustered NE. 3R is supported only if the 3R is hosted in the main NE (the NE with WSS/LD).

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- The NEs in a cluster configuration should be defined in advance before the L0 GMPLS provisioning on the Create Node window.

Cluster configuration is also supported on 1830 PSI-2T and 1830 PSI-M NEs interworking with 1830 PSS-32, 1830 PSS-16II, 1830 PSS-8.

Table 10-3 Supported Cluster scenarios

Extension Type	L0 GMPLS support	L1 GMPLS support	MRN support
OT without OPS	Yes 1830 PSS R11.1 NE onwards	NA	H-LSP
OT with OPS	Yes 1830 PSS R11.1 NE onwards	NA	-
Transponder/ muxponder OT without OPS	Yes 1830 PSS R11.1 NE onwards	NA	FA-TERM, FA-TERM2c
Transponder/ muxponder OT with OPS	Yes 1830 PSS R11.1 NE onwards	NA	-
1830 PSI-2T/ 1830 PSI-M without OPS	Yes 1830 PSS R11.1 NE onwards	NA	-
1830 PSI-2T/ 1830 PSI-M with OPS	Yes 1830 PSS R11.1 NE onwards	NA	-
1830 PSS-24x/ 1830 PSS-8x uplink without OPS	Yes 1830 PSS R11.1 NE onwards	Yes 1830 PSS R11.0 NE onwards	H-LSP, FA-TERM, FA-UNTERM, FA-TERM2c
1830 PSS-24x/ 1830 PSS-8x uplink with OPS	No	No	-
FA-TERM 1830 PSS-24x, FA-Unterm 1830 PSS-24x and 1830 PSS-8x	Yes	-	Yes

For more information on cluster NEs, cluster NE management, and cluster association, see "Compound node scenarios" (p. 181), "Multi-NE Clusters" (p. 183), and .

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.8 Create and remove an NPA

When to use

Use this task to create or remove a Network Protection Architecture (NPA).

Related information

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

An internal link (an I-NNI) is a link that is inside an ASON domain (for OMS in GMRE L0 and for OTU in GMRE L1).

This task provides the main navigation method in which you can create the NPA for ASON. However, if the ASON NPA tabbed topic is displayed from another navigation path, perform this task by selecting the ASON NPA tabbed topic and clicking the **More** icon on an ASON SNC and then clicking on the appropriate icon.

See following related topics:

- 10.21 “Implement/deimplement an NPA” (p. 1482)

Before you begin

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

To remove the NPA, ensure that the NPAs are in **Defined** state.

Task: Create an NPA

Complete the following steps to create an NPA for ASON.

1

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

OPERATE > ASON > NPAs.

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

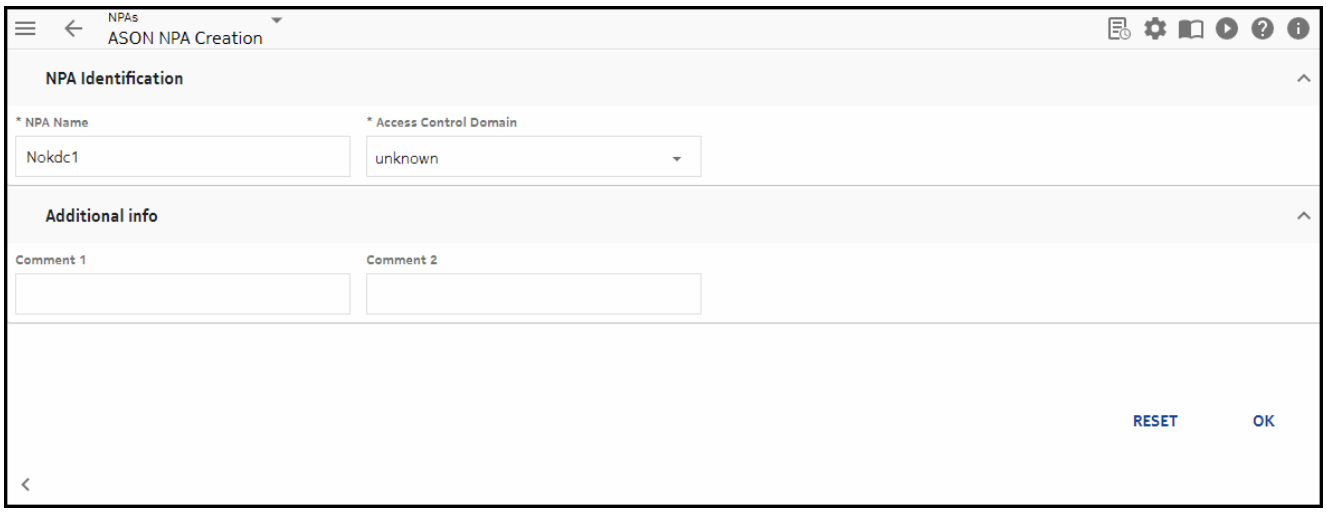
2

Click **Create NPA** icon from the top left.

Result: The system displays the **ASON NPA Creation** window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-5 ASON NPA Creation window



Note: ASON NPA is contained within a single domain. No further partitioning of the ASON NPA is supported from the current release. To facilitate migration, an option is provided to modify the NPA and associate a domain to it. For newly created NPAs, the system enforces to associate a domain to the NPA. If domains do not exist, the system associates the NPA to the Global domain. See the chapter *Domain partitioning* in *Administration Guide*.
If the user changes the domain of NPA that is in **Implemented** state, the system displays an error message mentioning that there are links added to the NPA which are in a different domain. To rectify this, go to **Add Node** window of the **OPERATE > Nodes** page and change the domain in the ACD field.
The user can create and associate a domain to the user.

3

In the **Name** field, enter a name to identify the NPA.

4

In the **Access Control Domain** field, select the domain from the drop-down list. If the user wants to create the NPA in a global domain, select **Unknown**.

Note: The users are assigned to one domain ONLY. When you add links to the NPA, the system displays only the links that are part of that particular domain.
The user belonging to a partitioned domain can only view NPAs which belong within the domain. The user can perform an operation if both the nodes are in the same domain.

5

Optional: In the **Comment 1** field, enter any relevant comment.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

6

Optional: In the **Note 2** field, enter any additional relevant comments.

7

Click **OK**.

Result: The system creates the NPA and displays a success message.

The configuration state is set to **Defined**.

END OF STEPS

Task: Remove an NPA

Complete the following steps to remove an NPA that has been created and is listed on the NPA data table.

1

From the NFM-T GUI, follow this navigation path

OPERATE > ASON > NPAs.

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

2

Do the following:

- Click the **More** ⋮ icon on the NPA to be deleted and select: **Remove**

  Result: The system displays a confirmation message.

3

Click **OK**.

Result: The system removes the selected NPA from the NPA data table.

If the NPA to be removed is currently in the **Implemented** state, it must first be moved to **Deimplemented**.

END OF STEPS

Modify the ACD for an NPA

To modify the ACD value for an NPA, do the following:

- Select the NPA in the list.
- From the NFM-T GUI, follow this navigation path
  OPERATE > ASON > NPAs > 360° View > Properties
- The **Properties** data table appears under the Properties tab.
- In the **Security** section modify the **ACD** value in the corresponding field.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- Click on **OK** to save the modification.
- Click on **Refresh** after saving the new ACD value.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.9 View the list of NPAs

Purpose

Use this task to view the list of NPAs.

Task

Complete the following steps to view the list of NPAs.

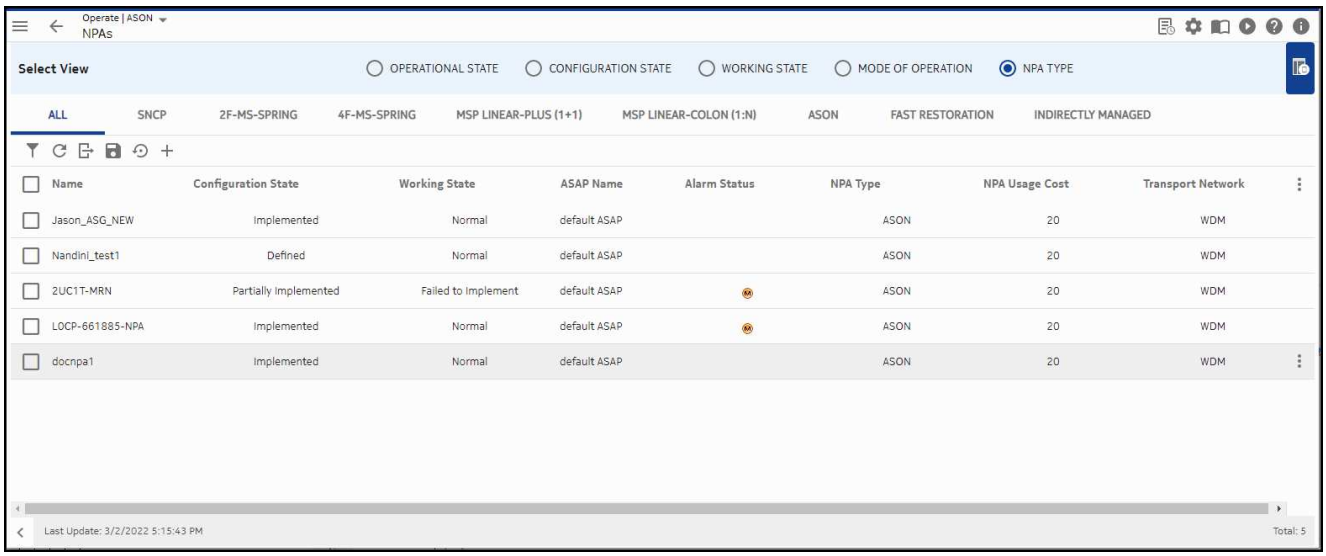
1

From the NFM-T GUI, follow this navigation path

OPERATE > ASON > NPAs

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

Figure 10-6 List of ASON NPAs



2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click Apply to close the window and return to the main page.

See 26.7 “Manage data columns” (p. 2213) for a detailed description and usage of the Manage Columns window.

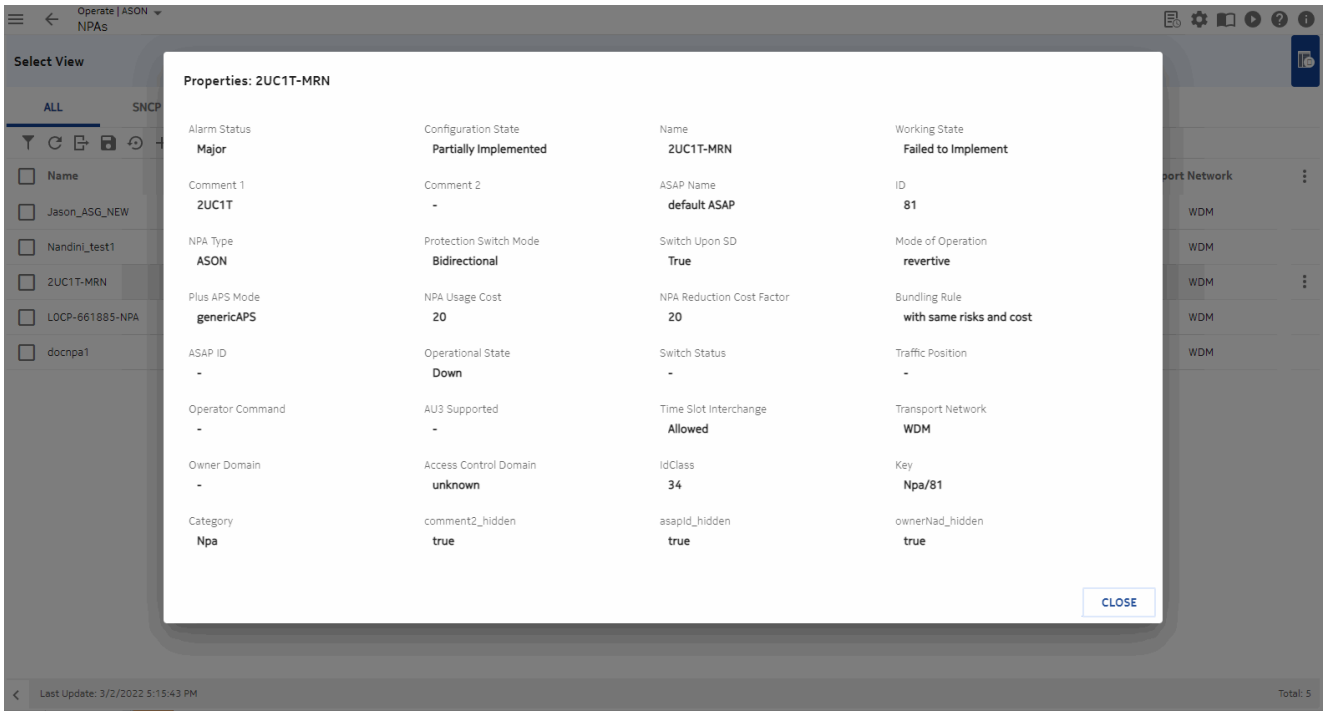
3

On the main page, select an NPA, click the **More** icon at the end of the selected row and click the **Properties** icon

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The system displays the additional attributes of the selected NPA.

Figure 10-7 Additional attributes of ASON NPAs



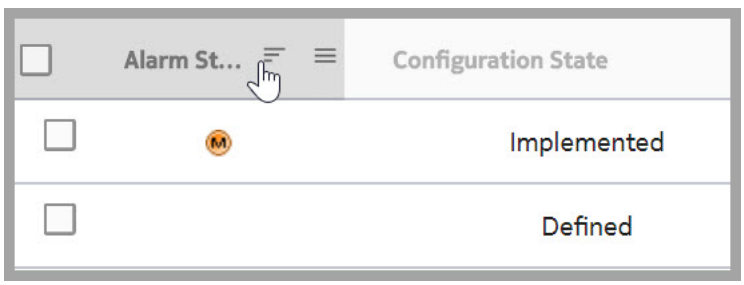
4

For information on the operations of the icons, see "Screens icons" (p. 2241).

5

Select the **Sorting** icon to sort the data in the column in ascending or descending order.

Figure 10-8 Data table sorting



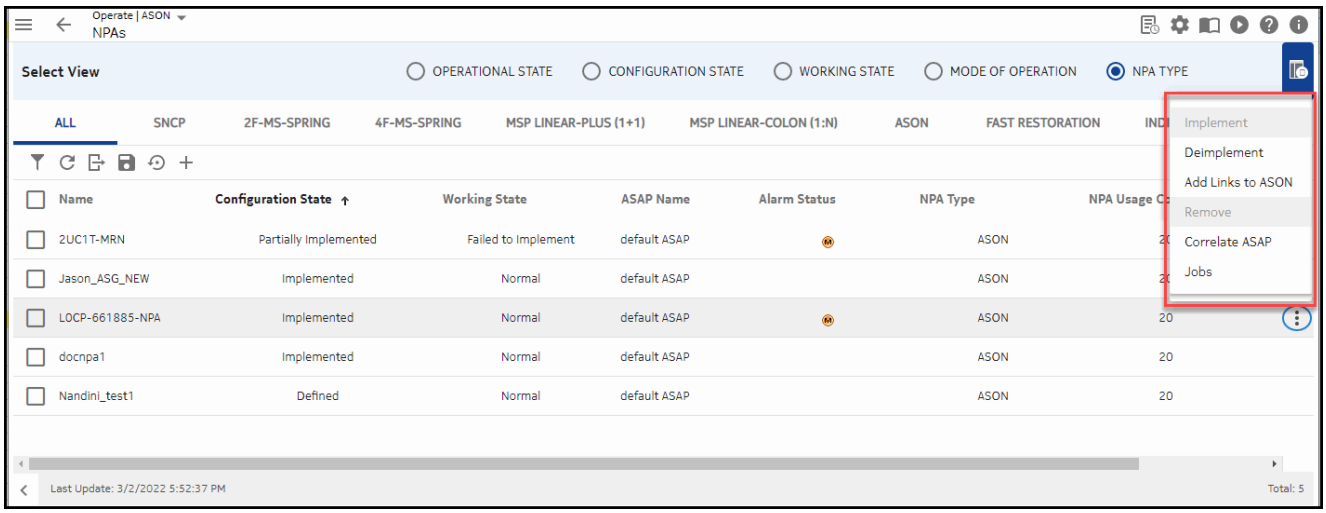
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

6

Select an NPA and click the **More** icon for the selected object.

Result: The system displays a list of operations that can be performed on the selected NPA.

Figure 10-9 NPA main list operations



7

To implement or deimplement an NPA, see 10.21 “Implement/deimplement an NPA” (p. 1482).

8

To add links to ASON or remove links from ASON, see 10.15 “Add links and remove links from ASON” (p. 1462).

9

To correlate ASAP, see 10.19 “Correlate an ASAP with an NPA” (p. 1477).

10

To manage jobs, see 10.23 “Manage jobs in ASON” (p. 1493).

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.10 ASON NPA table columns

Table column description

ASON NPA columns are described in the table, the description *Not applicable for ASON NPA* indicates that this field has no significance for the NPA of type ASON.

Column	Description
Access Control Domain	The **Access Control Domain** column displays the specific domain where the node must be assigned to. By default it is set to unknown.
Alarm Status	The **Alarm Status** displays the status of alarm that has occurred 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**.
ASAP ID	The **ASAP ID** column displays the identification number of the Alarm Severity Assignment Profile.
ASAP Name	The **ASAP Name** column displays the name of the Alarm Severity Assignment Profile to be **default ASAP** or the actual name of the ASAP.
AU3 Supported	Not applicable for ASON NPA
Bundling Rule	The **Bundling Rule** column displays the bundling rule that is associated with the TE Link and connection to be **all together**, **one to one**, or **with same risks and costs**.
Comment 1 **Comment 2**	Display user comments about the object being created or modified.
Configuration State	The **Configuration State** column displays the current state of the ASON NPA Minor modification
ID	The **ID** column displays the Network Protection Architecture identifier for the selected object.
Mode of Operation	Not applicable for ASON NPA
Name	The **Name** column displays the name that is identified with the ASON network.
NPA Reduction Cost Factor	The **NPA Reduction Cost Factor** column displays the value of the reduction cost factor assigned for the NPA, the default value is 20. By creating and implementing NPA, users can specify the role of a physical link and they can assign a reduction cost factor and a usage cost factor to the physical link.
NPA Type	Specifies the type of NPA (**ASON**)
NPA Usage Cost	Not applicable for ASON NPA
Operational State	Not applicable for ASON NPA
Operator Command	Not applicable for ASON NPA
Owner Domain	The **Owner Domain** column displays the domain of the user who has created the object, in this case the NPA.
Plus APS Mode	Not applicable for ASON NPA
Protection Switch Mode	Not applicable for ASON NPA
Switch status	Not applicable for ASON NPA
Switch Upon SD	Not applicable for ASON NPA
Time Slot Interchange	Not applicable for ASON NPA

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Column	Description
Traffic position	Not applicable for ASON NPA
Transport Network	Displays the type of transport network, whether **Electric** or **Photonic**. The photonic layer of OTN is provided through Wavelength Division Multiplexing (WDM) NEs. The electrical layer of OTN is provided through both WDM and Optical Cross-connect System (OCS) NEs or only through a network of OCS NEs that carry either the same data rate level as the photonic layer or a lower data rate level that is multiplexed and transported through the photonic layer.
Working State	The **Working State** column displays whether the working state of the selected ASON NPA is **Normal**, **Failed to Implement**, **Failed to Deimplement**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.11 More operations on ASON NPA

More option description

Users can select an item in a data table, click the **More** icon for the selected object, and view a list of additional operations for that item.

The selection of the following menus depend on the type of the selected object, based on the selected type of object, some of the items in the table may be disabled. From a physical connection selected from **Physical Connections**, the user can access different actions that are possible.

Table 10-4 More Operations on ASON NPA

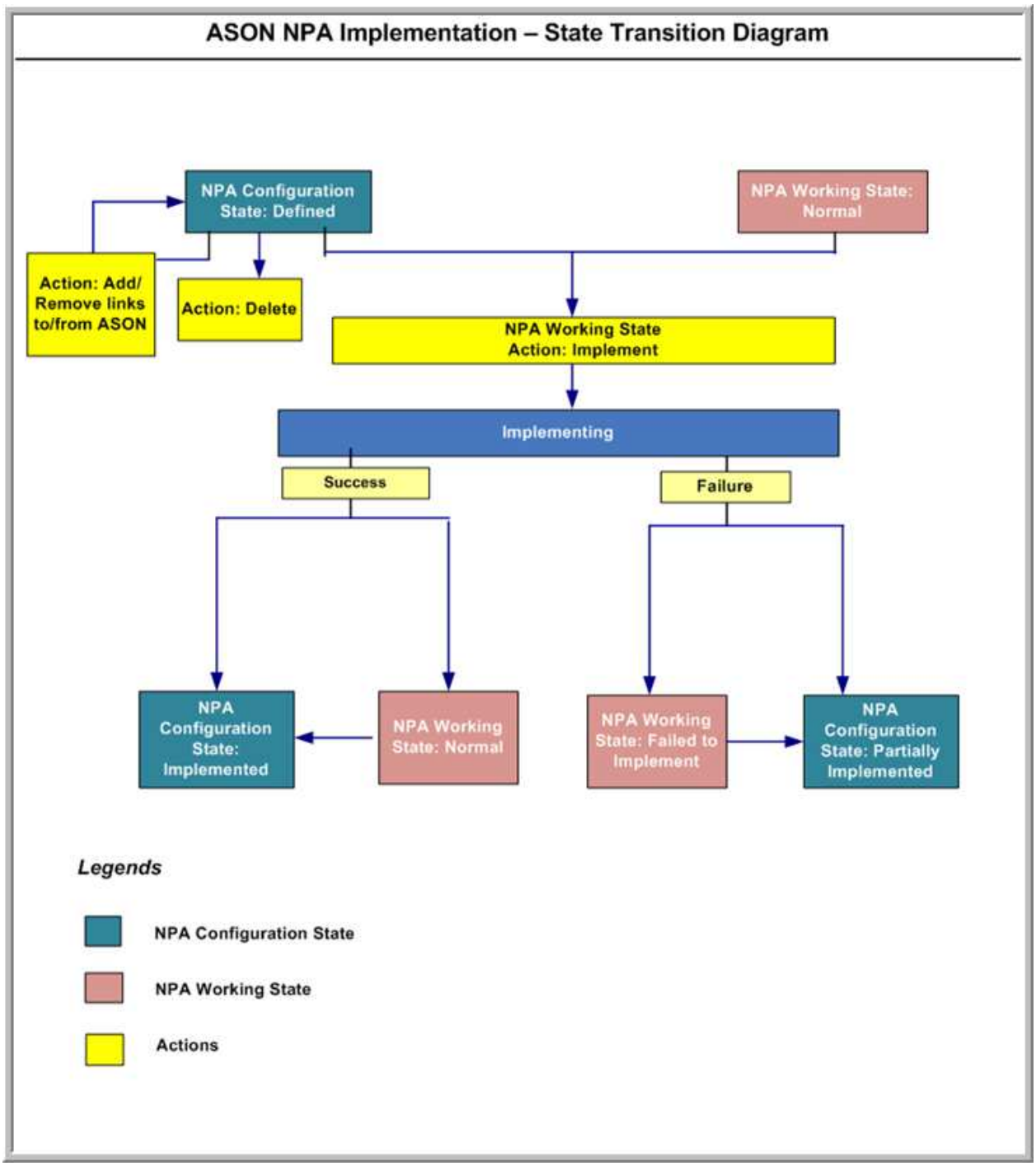
Menu Item	Description
Implement	Specifies that the object has been implemented, but it is not yet available for end-customer use. See 10.21 “Implement/deimplement an NPA” (p. 1482).
Deimplement	Specifies that an object that is currently in the Implement state must be deimplemented. See 10.21 “Implement/deimplement an NPA” (p. 1482).
Add Links to ASON	Provides an option to Add Links to ASON NPA. See 10.15 “Add links and remove links from ASON” (p. 1462)
Remove	Removes the links from ASON. See 10.15 “Add links and remove links from ASON” (p. 1462)
Correlate ASAP	Correlates an Alarm Severity Assignment Profile (ASAP) with an NPA. See 10.19 “Correlate an ASAP with an NPA” (p. 1477)
Jobs	Manage jobs for an NPA. See 10.23 “Manage jobs in ASON” (p. 1493)

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.12 ASON NPA state transition diagram

ASON NPA Implementation - state transition diagram

Figure 10-10 ASON NPA Implementation - State Transition Diagram

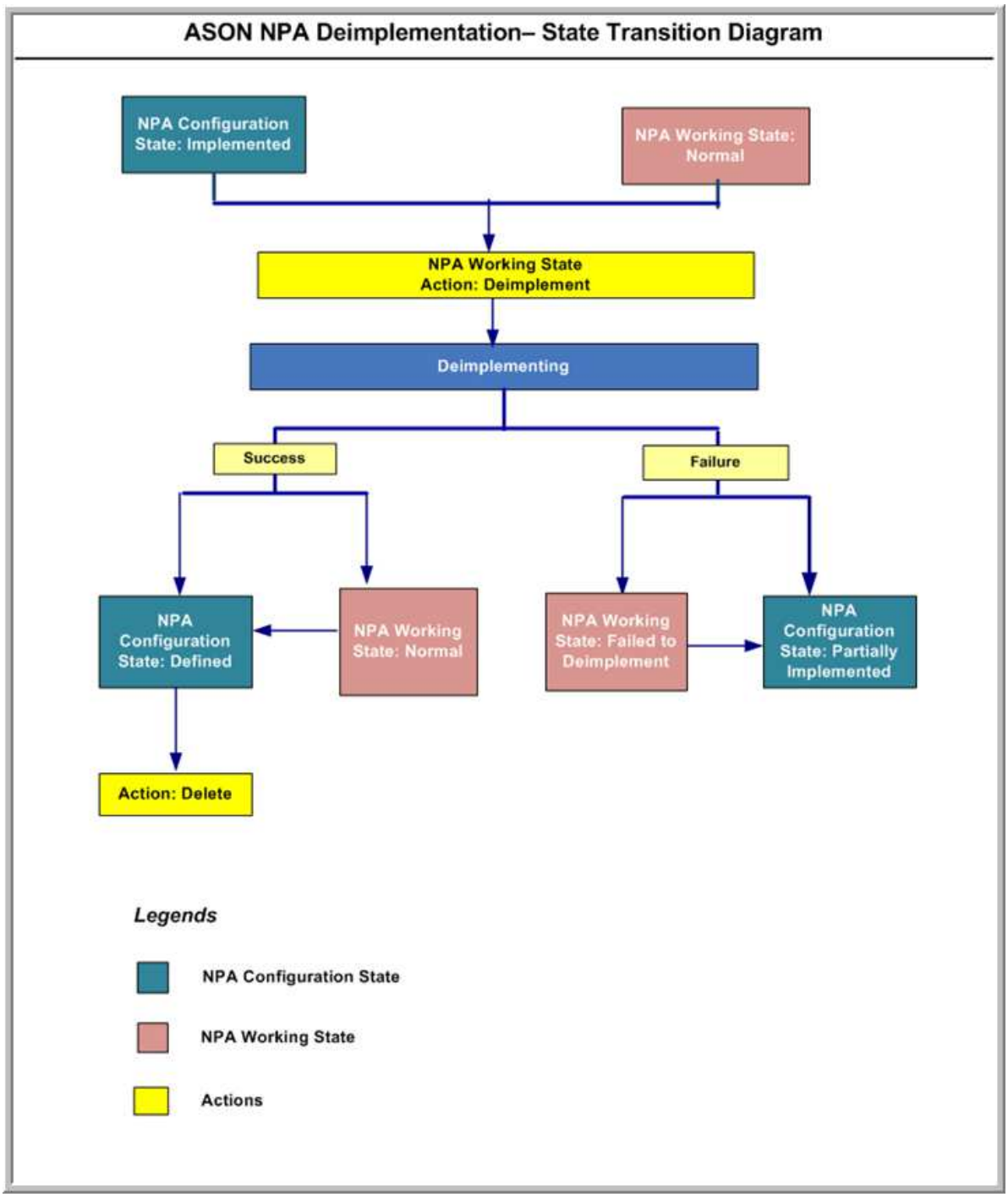


© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

ASON NPA Deimplementation - state transition diagram

Figure 10-11 ASON NPA Deimplementation - State Transition Diagram

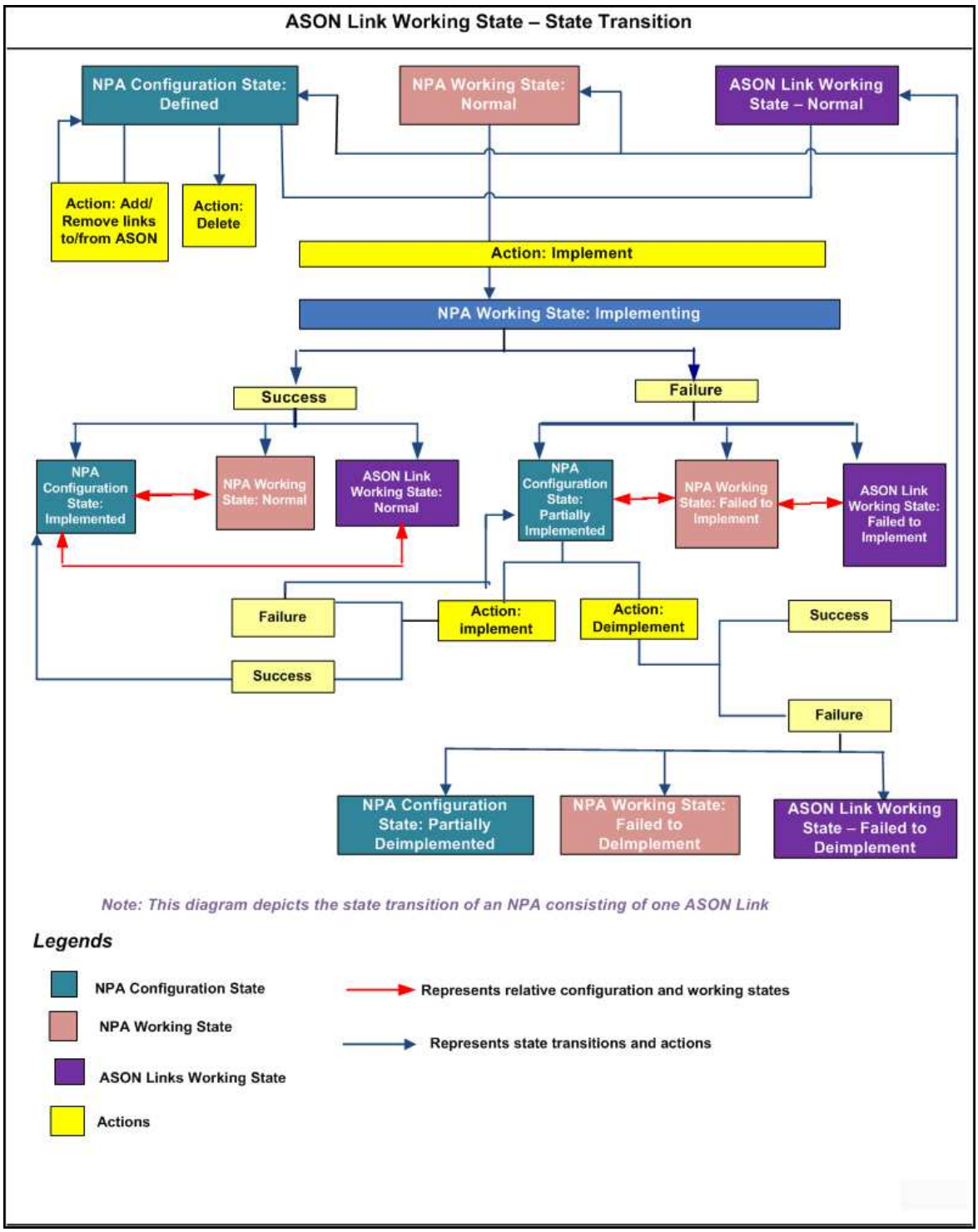


© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.13 ASON link state transition diagram

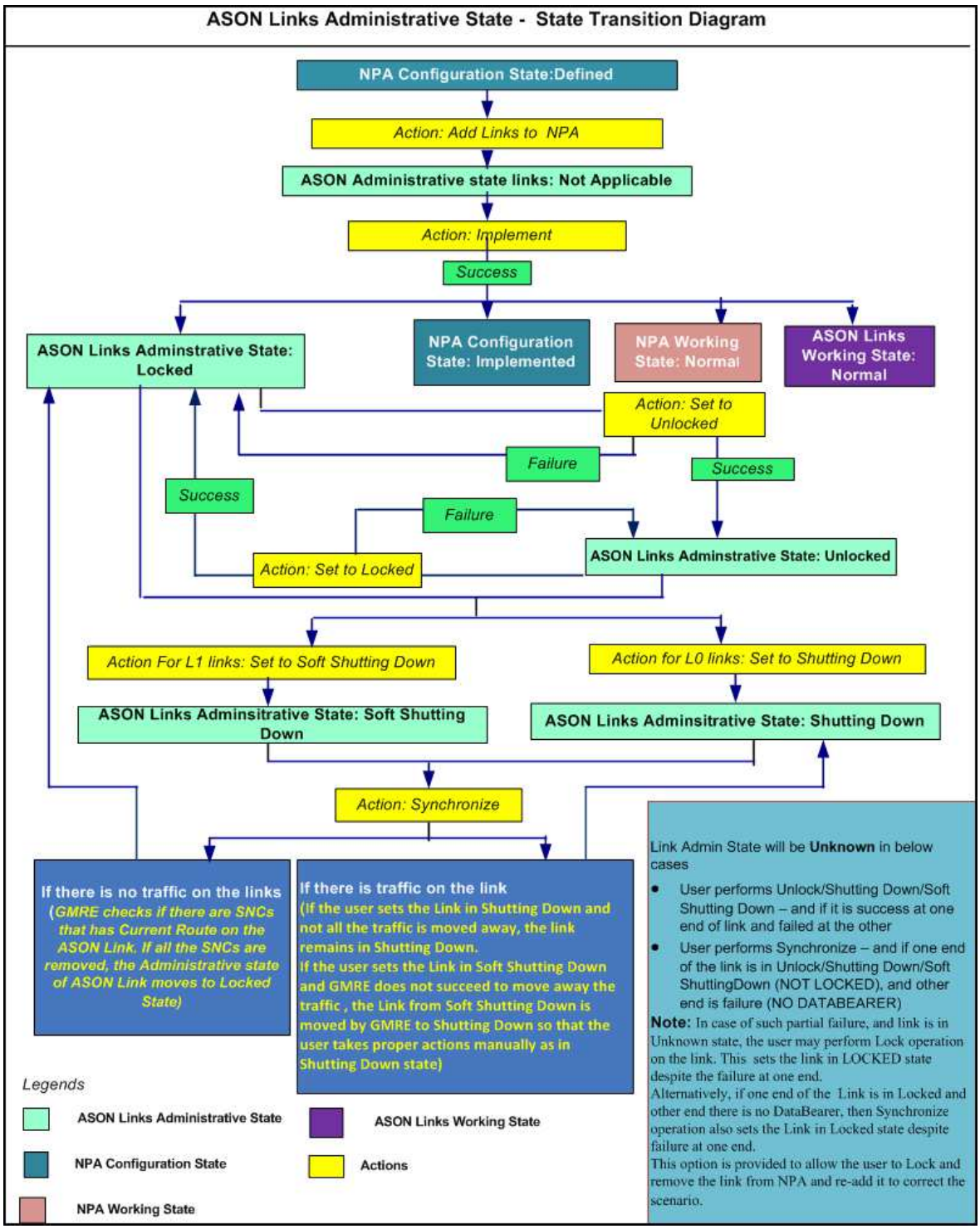
ASON link Working state - state transition diagram



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

ASON link Implementation state - state transition diagram



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.14 Access and view the misalignment report for a link

When to use

Use this task to access and view the Misalignment Report for a link for an ASON or a TE Link.

Ensure that the links are created.

Task

Complete the following steps to access and view the Misalignment Report for an ASON or a TE Link.

1

From the NFM-T GUI, follow one of the navigation paths

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

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

2

Click the **More** icon for the selected object.

3

Click **Misalignment Report** from the popup menu.

Result: The system displays the Misalignment Report for the selected link.

Note: The Misalignment Report displays data only for objects involving ASON SNC links for Control Plane connections.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.15 Add links and remove links from ASON

Purpose

Use this task to add and remove links in ASON.

The NPA must already be created.

The NPA must be listed in the NPA data table in the **Implemented** or **Partially Implemented** configuration state.

A drop link is an external OS connection that is assigned to an NPA in ASON. A drop link connection is the link between the Managed Plane domain and the Control Plane domain.

An internal link (an I-NNI) is a link that is inside an ASON domain (for OMS in GMRE L0 and for OTU in GMRE L1).

This task provides the main navigation method in which you can add links to or remove links from ASON. However, if the ASON NPA tab is displayed from another navigation path, you can perform this task by selecting the ASON NPA tab and clicking on the appropriate icon on an ASON SNC.

This task enables you to add links to and remove links from ASON from different starting locations on the NFM-T GUI.

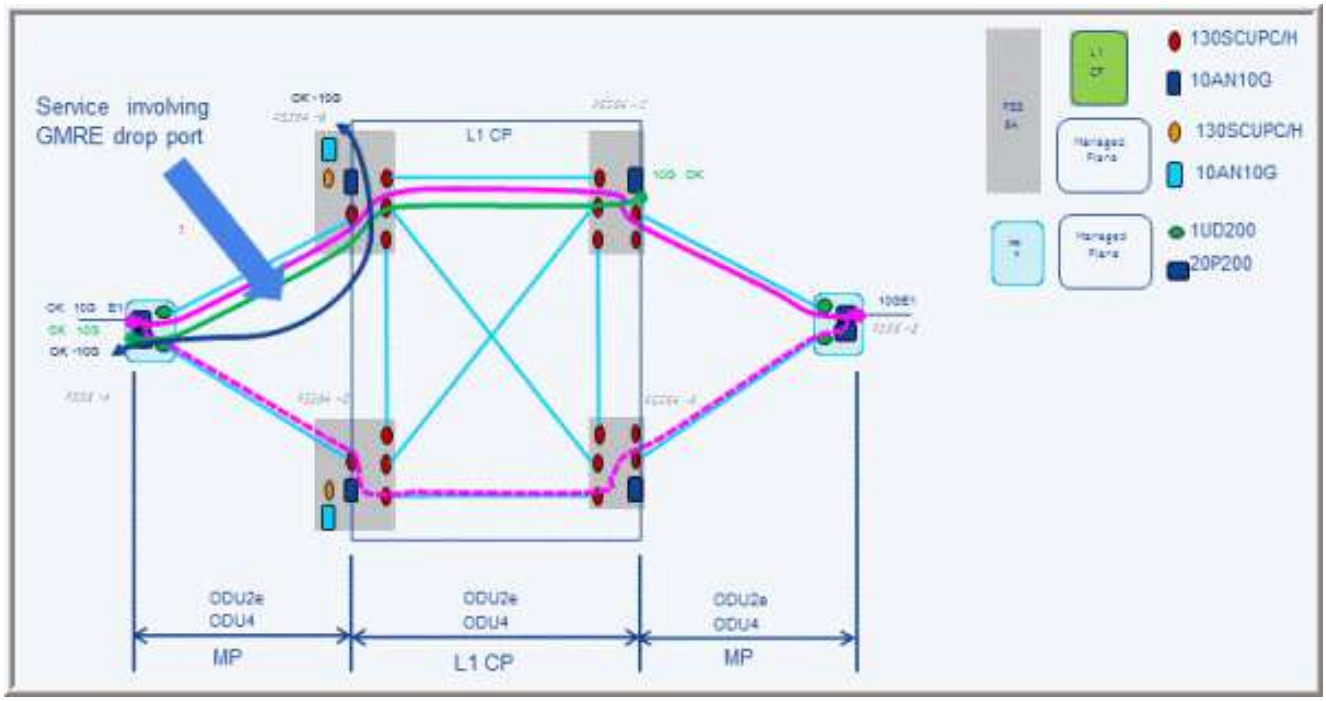
This task provides the main navigation method in which you can add links to or remove links from ASON and from different starting locations on the NFM-T GUI.

Note: To support the GMRE restrictions in supporting Guaranteed Restoration, at add Link to ASON, no assignment is provisioned to GMRE while adding the link to ASON. The user can assign the link to GMRE in the ASON SNC consistently on both ends.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Drop port shared between ASON and Managed Plane

Figure 10-12 Add Links - Shared Ports



In the figure you can see an example of a connection ODUj pure managed plane involving one GMRE drop port, the aim is to share drop ports between ASON and managed plane. The connection provisioning for mixed plane configures where Management Plane services terminated on the Layer 1 Control Plane border nodes, as shown in the figure.

The drop link can be used as shared, it can be used for managed-plane ODUk/service allocation as well. The drop link can be set as shared by the user, see "Task: Enable/disable shared link" (p. 1467)

On existing Mixed plane services you can enable shared port on drop link thereby start using unused bandwidth for managed plane if required.

Task: Add links to ASON

Complete the following steps to add or remove links from ASON.

1

From the NFM-T GUI, follow the navigation path

OPERATE > ASON > NPAs > More icon > Add Links to ASON

OPERATE > ASON > NPAs > 360° View > LINKS > Create icon

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

OPERATE > Network Profiles > Shared Risk Groups > 360° View > ASON Links tab

OPERATE > Network Profiles > Color Profiles > More icon > Used In > ASON Links tab **> Add Links to ASON icon**

OPERATE > Network Profiles > Color Profiles >More icon > Matched By > ASON Links tab **> Add Links to ASON icon**

Result: The system displays the lists of NPAs in a data table.

2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click Apply to close the window and return to the main page.

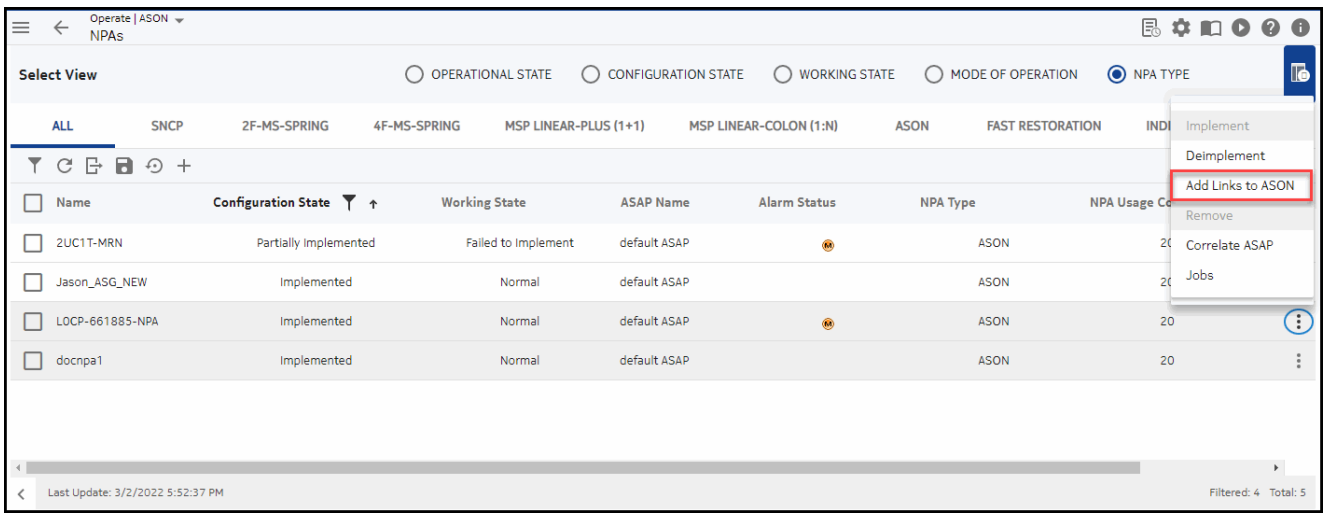
See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the Manage Columns window.

3

Click on the NPA or link to which you want to add links and perform the following:

Click the **More** icon and select **Add Links to ASON** from the popup menu that appears.

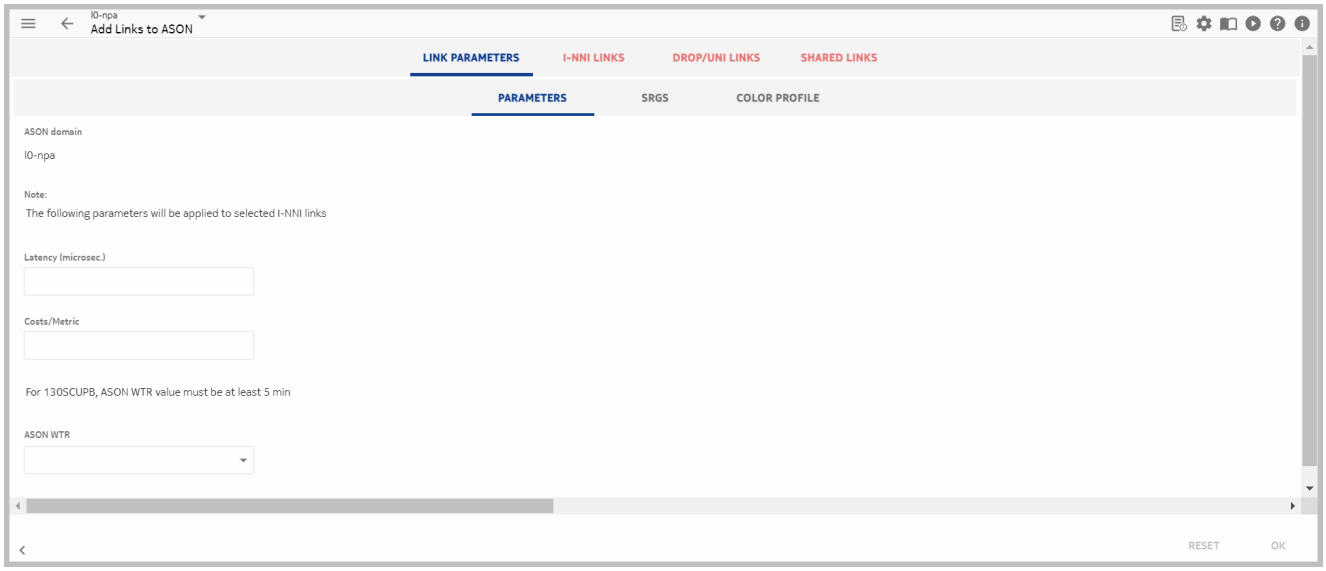
Figure 10-13 Add Links to ASON option



Result: The system displays the **Add Links to ASON** window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-14 Add Links to ASON window



4

In the **LINK PARAMETERS** tab configure the following:

- Under **PARAMETERS** sub-tab, enter appropriate values for **Latency (microsec)** and **Cost/Metric** fields. 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 1 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 **ASON WTR** field, select the value from the drop-down list.
- In the **SRGS** sub-tab, select one or more SRG from the available options.

  Note: SRGs can be added only if no links has already an associated risk.
- In the **COLOR PROFILE** sub-tab, select one of the profiles from the available options.

5

Select one or more links from one of the following tabs:

- **I-NNI LINKS**
- **DROP/UNI LINKS**
- **SHARED LINKS**

Note: If the NPA added is part of a particular domain, the I-NNI and drop links display links that are associated to the domain.
If the NPA is not associated to any ASON Links, associate the domain to NPA. If the NPA is associated to any ASON Links, then validate if all links belong to same domain.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: The selected links are displayed in the lower panel of respective tab

6

Click **OK**.

Result: The system adds the parameter specifications to the NPA and displays a success message at the bottom of the window.

END OF STEPS

Task: Remove links from ASON

Complete the following steps to remove links from ASON.

1

From the NFM-T GUI, follow one of these navigation paths:

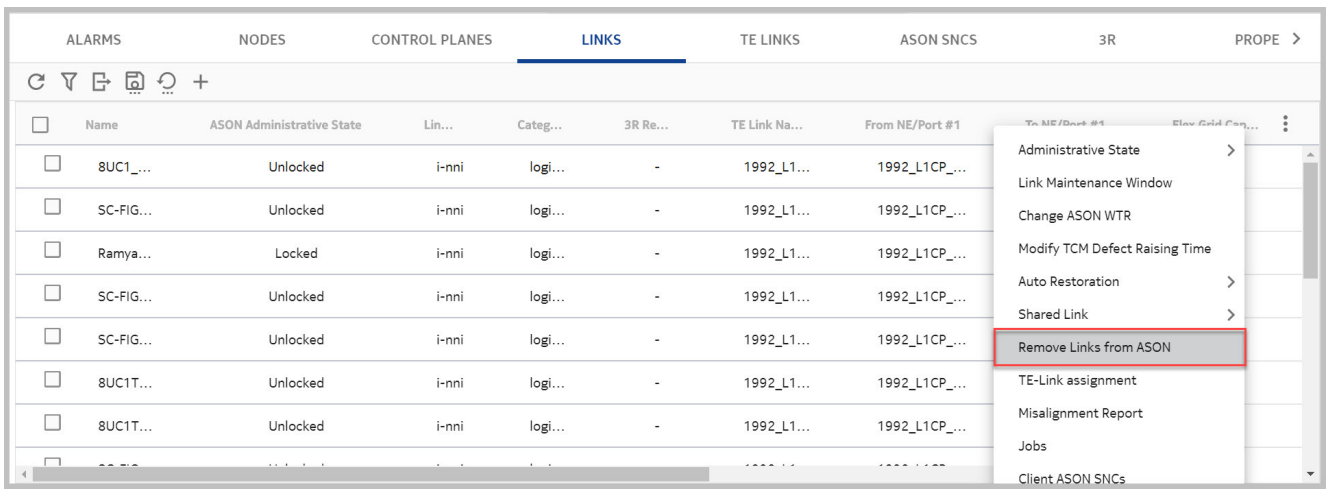
OPERATE > ASON > NPAs > 360° View > LINKS tab

2

In the **LINKS** data table, locate the link to be removed

- Click the **More** icon and select **Remove Links from ASON** from the popup menu.

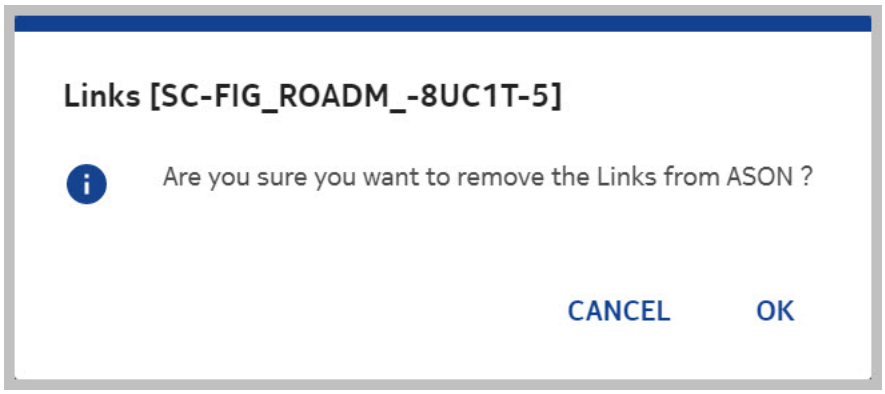
Figure 10-15 Remove Links from ASON



Result: The system displays a confirmation message.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-16 Confirmation message



3

Click **OK**.

Result: The system removes the selected link from ASON.

END OF STEPS

Task: Enable/disable shared link

Important! This operation is available only on drop links.

Complete the following steps to enable or disable links added to an ASON NPA.

1

From the NFM-T GUI, the navigation path:

OPERATE > ASON > NPAs > 360° View > LINKS tab > More ⋮ icon > Shared Link

2

Click **Enable/Disable**.

3

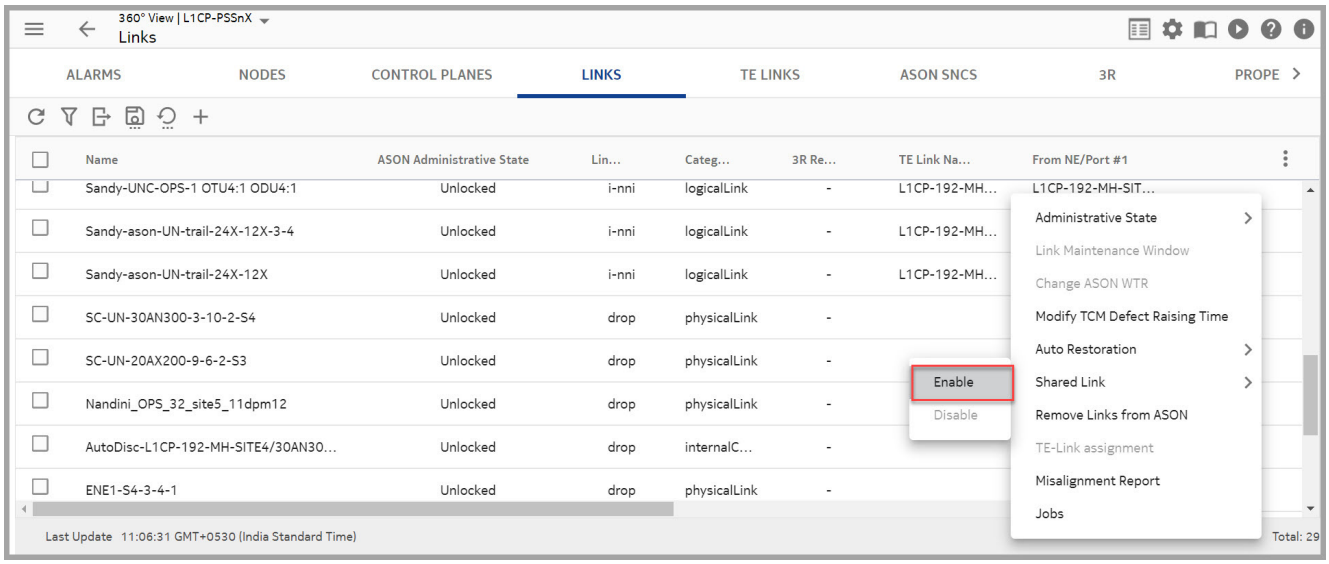
In the **LINKS** data table, locate the link to be shared or unshared and do one of the following:

- Click the **More** ⋮ icon and from the popup menu, follow this path: **Shared Link > Enable**
- Click the **More** ⋮ icon and from the popup menu, follow this path: **Shared Link > Disable**

Note: The two operations are mutually exclusive, if the link is already shared, the option **Disable** is enabled. If the link is not shared, the option **Enable** is enabled.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-17 Enable/Disable Links added to NPA



Result: The system displays a confirmation message.

Figure 10-18 Enable/Disable Shared Link - Confirmation Message

4

The system enables or disables the selected link on the ASON NPA.

END OF STEPS

Validation for shared links add, remove, enable, and disable

Error messages can be received if the assign, remove, enable or disable sharing cannot be performed :

- If a Managed plane connection is already riding on an OS drop link then you cannot add the link as drop and shared link to NPA.

  An error message is received: *Selected link(s) cannot be assigned as there is infrastructure/ service(s) riding over it.*
- If a connection is already riding over a shared OS drop link then you cannot remove the shared drop link from NPA.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

An error message is received: *Selected link(s) cannot be unassigned as there is infrastructure/service(s) riding over it.*

- If a connection is already riding over a shared OS drop link then you cannot disable the sharing on the drop link.

  An error message is received: *Selected link(s) cannot be unshared as there is infrastructure/service(s) riding over it.*

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.16 Modify TCM defect raising time

Purpose

Use this task to modify the TCM defect raising time on a link in ASON NPA.

The NPA must already be created.

The NPA must be listed in the NPA data table in the **Implemented** or **Partially Implemented** configuration state.

A standard hold-off time of 20 ms is used by default by GMRE. As OLP protection may take up to 50 ms to switch, a longer hold-off timer can be used to suppress restoration actions when the OLP protection has not yet switched. For that purpose, the hold-off is configurable by the user. The new configurable time must be specified when at least on OTS span of the MS trail is OLP protected, or at least one segment of the trail is OPSA protected.

Hold-off timer applies to TCM monitored links, such as L1 Overlay and FA-UNTERM, when the TCM alarm is detected, GMRE will wait for that configured timer before triggering restoration of client traffic.

GMRE default value is 20 ms for a TCM monitored link, independently from the server protection (OPSA, OPSFlex, OLP), even unprotected NFM-T connection relies on GMRE default value (20 ms) at provisioning of the link to GMRE.

This task provides the steps to manually change the GMRE default value. This can be necessary in case no more server protection on the Link or in case of reroute or in case the value has to be increased, for example, for OLP.

The command **Modify TCM Defect Raising Time** is available in the right-click menu on L1 Logical links and FA-Unterm tunnels.

Task

Complete the following steps to modify the TCM defect raising time on a link in ASON NPA.

1

From the NFM-T GUI, follow the navigation path

OPERATE > ASON > NPAs > 360° View > LINKS tab > More ⋮ icon > Modify TCM Defect Raising Time

OPERATE > Network Profiles > Shared Risk Groups > 360° View > ASON Links tab > **More** ⋮ icon **> Modify TCM Defect Raising Time**

OPERATE > Network Profiles > Color Profiles (tab) > More ⋮ icon > Used In (tab) > ASON Links (tab)

OPERATE > Network Profiles > Color Profiles (tab) > More ⋮ icon > Matched By (tab) > ASON Links (tab)

Result: The system displays the lists of NPAs in a data table.

2

Select the NPA where you need to modify the TCM defect raising time on a link.

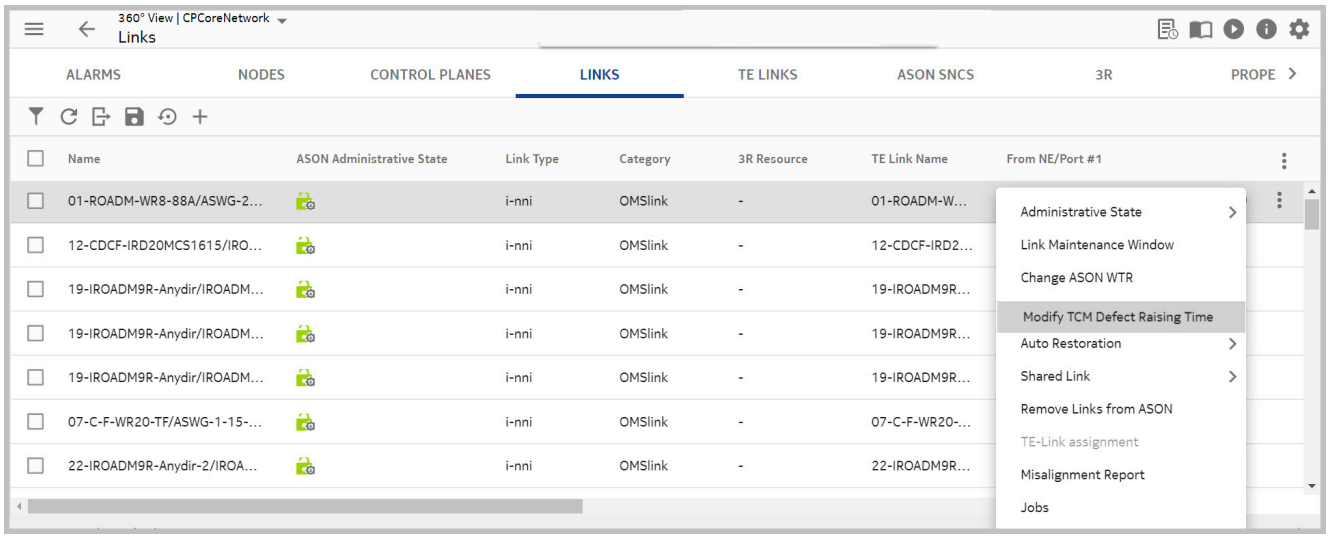
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

Click on **360° View** > **LINKS** tab :

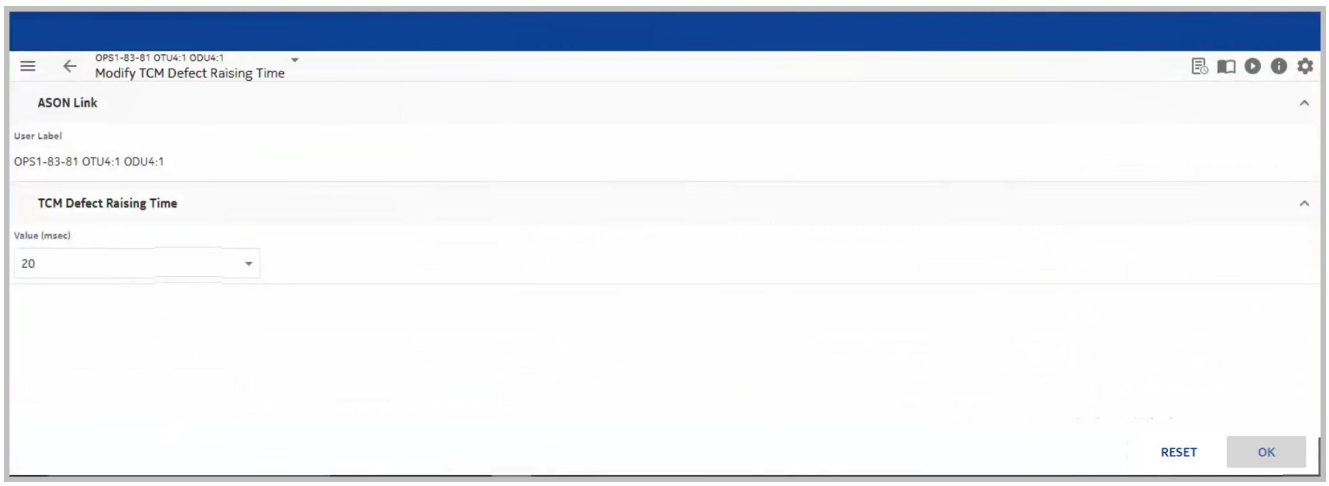
- From the LINKS data table, click the **More** icon on the selected link and select **Modify TCM Defect Raising Time** from the popup menu.

Figure 10-19 Modify TCM Defect Raising Time option



Result: The system displays the **Modify TCM Defect Raising Time** window.

Figure 10-20 Modify TCM Defect Raising Time window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

4

Select the time in milliseconds from the drop-down list in the field Value.

5

Click **OK** , to confirm the modification.

Result: The Defect Raising Time is modified with the selected value.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.17 Assign an ASON I-NNI link to a TE Link and SRG

Purpose

Use this task to assign an ASON I-NNI link that is associated with a selected ASON NPA to a TE Link and SRG.

Ensure that the NPAs that are created is in **Implemented** state.

Task

Complete the following steps to assign an ASON I-NNI link that is associated with a selected ASON NPA to a TE Link and SRG.

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > ASON > NPAs > 360° View > LINKS

Result: The system displays the 360° view of NPAs.

2

Select **LINKS** tab.

Result: The system displays the list of links available.

3

Select an I-NNI link, click the **More** ⋮ icon and select **TE-Link Assignment** option.

Result: The system displays the **TE-Link Assignment** window.

The ASON Link area of the window is pre-populated with the name of the ASON link that you selected and the Current TE Link. The remaining fields are pre-populated with the original or default value assigned.

Figure 10-21 TE-Link Assignment window

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

The ASON Link area of the window is pre-populated with the name of the ASON link that you selected and the Current TE Link. The remaining fields are pre-populated with the original or default value assigned. The **Name** and the **Current TELink** fields are auto populated.

Select **Existing** or **New** in the **Final TELink** field.

If the user has selected **New**, see 4.

If the user has selected **Existing**, see 5.

4

If you have selected **New** in the **Final TELink** field, the system displays the following fields:

- In the **TE-Link parameters** pane, configure the following parameters:
  - **Costs/Metric**: Select a value from the list. 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 1 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 value is 20.
  - **Latency (microsec)**: displays the time in microseconds for the selected TE Link

    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 0.
  - Select the **Color Profile** from the **Color Profile Available Objects** window.
- In the **SRGs** panel, select an SRG and the same is populated in the **SRG** panel.

5

If you have selected **Existing** in the **Final TELink** options, click the **Search** icon to add the **Final TElink Name** in the **TE-Link parameters** pane. You can add the Assigned TE Links from the **Assignable TE-Link list** window.

6

Click **OK**.

Result: The ASON link is updated.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.18 Change ASON WTR

When to use

Use this task to change Wait Time to Restore (WTR) of a physical connection and/or a logical link.

Related information

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 *Spare*, to guarantee the traffic. Once the *Main* path is restored, the traffic is switched from the Spare back to the Main.

The Color Profile data table has tabs for **Used In** and **Matched By**. These tabs have a subtab for **ASON Links**. The **ASON Links** subtab and **Links** tab, which is displayed under ASON NPAs 360° tabs, provide the same actions and functions for links. Step 1 of this task provides you with all possible navigation paths from **OPERATE >** .

See the following topics in this document:

- 10.6 “ASON NPA” (p. 1438)

Before you begin

Ensure that the physical connections and the logical links belong to ASON.

Task

Complete the following steps to change the WTR of a physical connection or a link

1

From the NFM-T GUI, follow one of these navigation paths:

OPERATE > ASON > NPAs > 360° View > LINKS (tab) > More ⋮ icon **> Change ASON WTR**

OPERATE > Network Profiles > Shared Risk Groups > 360° View > ASON Links (tab) > More ⋮ icon **> Change ASON WTR**

OPERATE > Network Profiles > Color Profiles > More ⋮ **icon > Used In > ASON Links (tab)**. Right Click and select **Change ASON WTR**

OPERATE > Network Profiles > Color Profiles > More ⋮ **icon > Matched By > ASON Links (tab)**. Right Click and select **Change ASON WTR**

Result: The Change ASON WTR screen is displayed.

2

The following actions are used for modification in **Change ASON WTR**

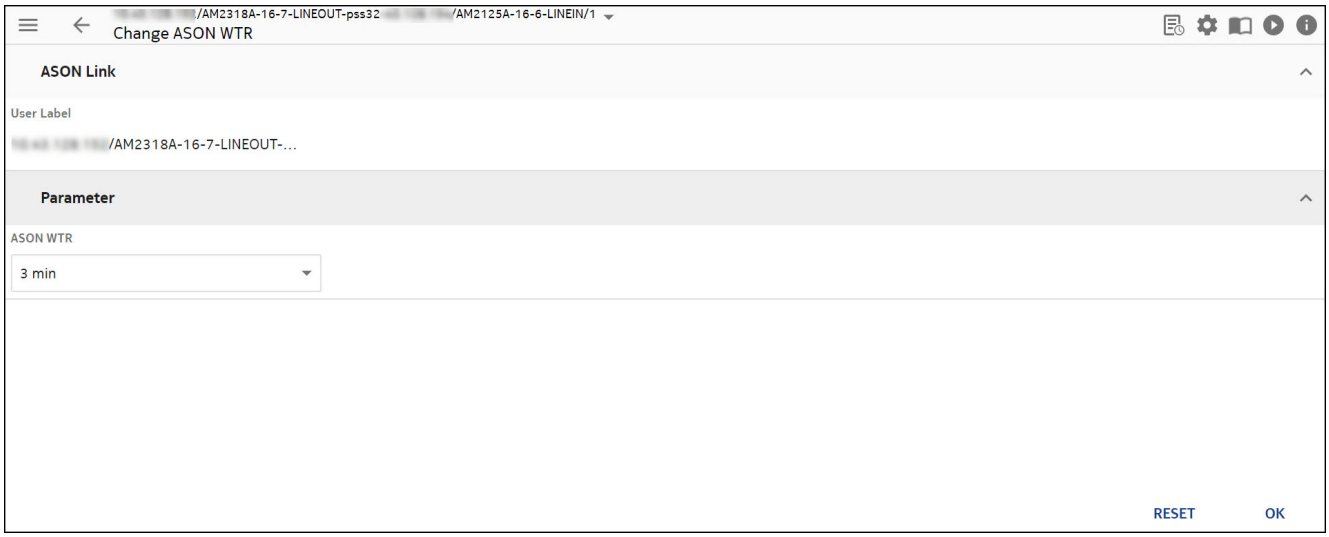
- For the data table displayed under ASON Links tab from Color Profiles, right click on the selected link, and click **Change ASON WTR**

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

- For the data table displayed under LINKS tab under NPA 360° View, on the selected link, click the **More** icon and select **Change ASON WTR** from the pop up menu.

  Result: The **Change ASON WTR** window is displayed.

Figure 10-22 ASON – NPAs – Change ASON WTR window



3

The **Name** field is auto populated by default.

In the **ASON WTR** field, change the value. Options are displayed in various minutes.

4

Click **OK**.

Result: The system is updated with the new value.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.19 Correlate an ASAP with an NPA

When to use

Use this task to correlate an Alarm Severity Assignment Profile (ASAP) with an NPA.

Ensure that the NPAs are created.

Task

Complete the following steps to correlate an ASAP with an NPA.

1

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

OPERATE > ASON > NPAs.

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

2

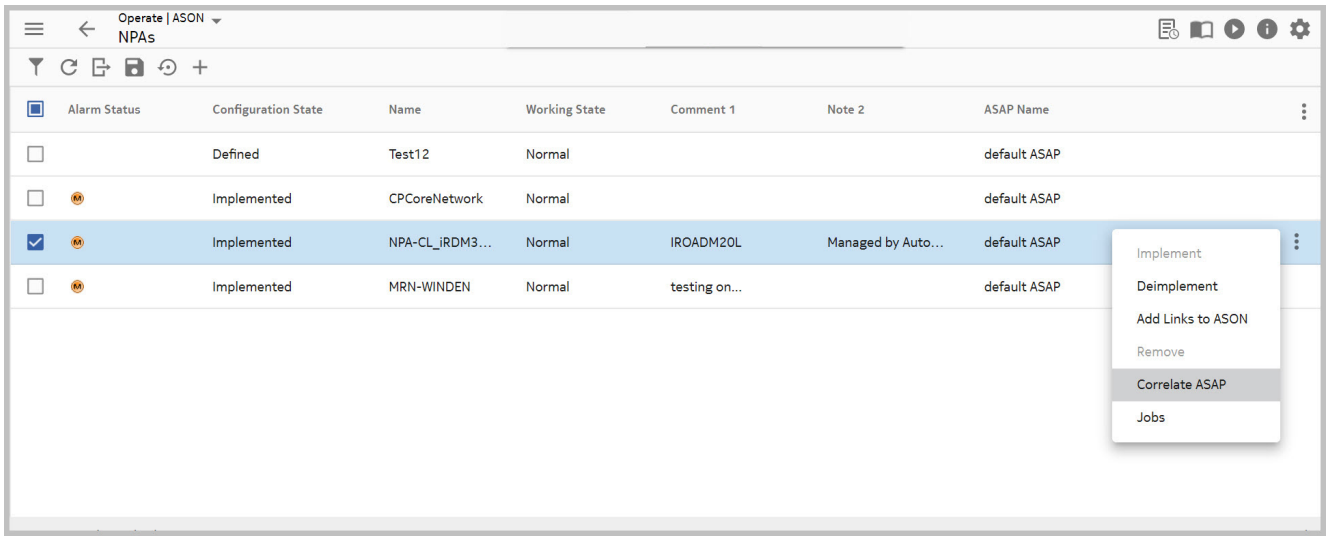
Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click Apply to close the window and return to the main page.

See 26.7 “Manage data columns” (p. 2213) for a detailed description and usage of the Manage Columns window.

3

Select an NPA that you want to correlate, click the **More** icon and select **Correlate ASAP**.

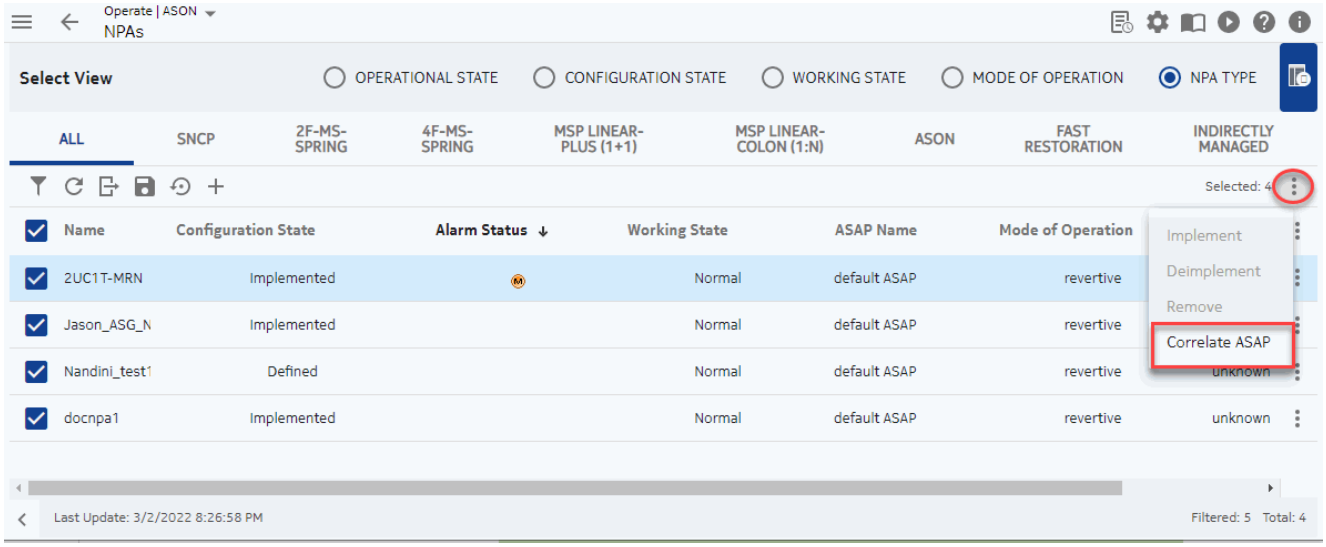
Figure 10-23 Correlate ASAP option



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

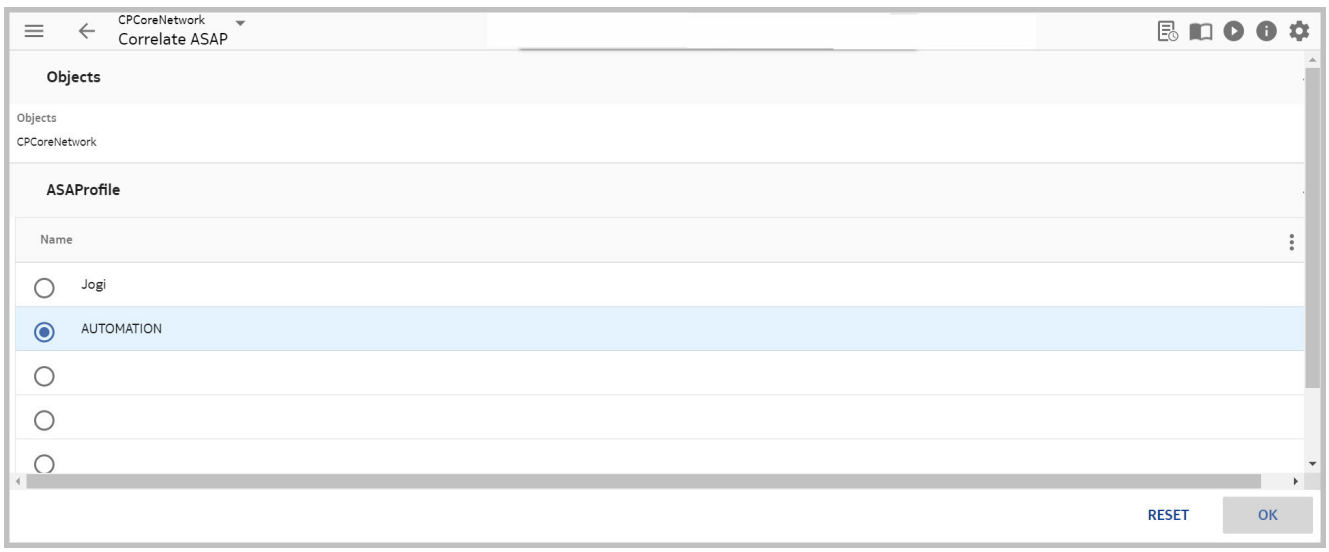
Select multiple NPAs to be correlated, click the **More** icon and select **Correlate ASAP**.

Figure 10-24 Correlate ASAP option Multiple NPAs



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

Figure 10-25 Correlate ASAP window



4

Select the **ASAProfile**.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

5

Click **OK**.

Result: The system correlates the NPA to the ASAP selected and the system displays success message.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.20 Enable or disable auto restoration of links

Purpose

Use this task to enable or disable the auto restoration of the links.

Ensure that the NEs are reachable and the NPAs are in **Implemented** state.

Task

Complete the following steps to enable or disable the automatic restoration of links

1

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

OPERATE > ASON > NPAs >360° View > LINKS

2

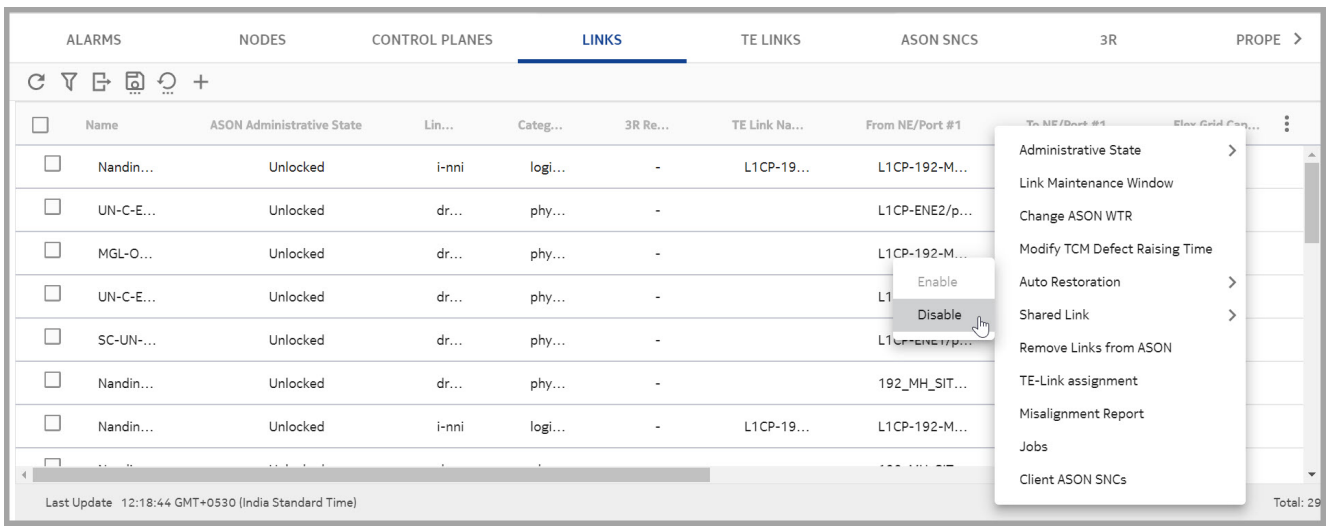
Select the **LINKS** tab.

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

3

Click the **More** icon on the selected Link and click **Auto Restoration > Enable** or **Auto Restoration > Disable**. The selection depends on the current restoration state of the link.

Figure 10-26 Auto Restoration > Enable/Disable



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Result: Depending on the configuration state of the link and the selection, the system displays a success message.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.21 Implement/deimplement an NPA

Purpose

Use this task to implemented or deimplement a selected NPA.

Ensure that the NPAs are created.

The NPA must be listed in the NPA data table in the **Defined** or **Partially Implemented** Configuration State. The NPA is **Partially Implemented**, if a process has failed while attempting to implement the NPA.

This task provides the main navigation method where the user can implement or deimplement the NPA for ASON.

Task: Implement an NPA

Complete the following procedure to implement an NPA.

1

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

OPERATE > ASON > NPAs

Result: The list of NPAs are listed in the data table.

2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click Apply to close the window and return to the main page.

See 26.7 “Manage data columns” (p. 2213) for a detailed description and usage of the Manage Columns window.

3

To implement an NPA, do the following steps

- Select the NPA where you want to perform the operation, click the **More** icon and select **Implement** from the popup menu.

  Result: The system displays a confirmation message whether or not the user wants to implement the particular NPA.

4

Click **OK**.

Result: The system displays a Success message at the bottom of the window

The **Configuration State** changes to **Implemented** on the NPA data table and the system displays a message at the bottom left of the window:

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

```
Implement <NPA Name> ✓ Success
```

The system automatically creates the TE Link using the following physical connection bundling rules:

- For L0, the TE-Link is 1:1. with OMS.
- For L1, the bundling rules are the following:
  - same A-Z nodes
  - same cost and latency
  - same SRG

END OF STEPS

Task: Deimplement an NPA

Complete the following steps to deimplement an NPA.

1

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

OPERATE > ASON > NPAs

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

Ensure all the links from NPA are removed prior to deimplementing an NPA.

2

Click the **Manage Columns** ( ) icon in the **Select View** area to add or remove columns or views from the page. Click Apply to close the window and return to the main page.

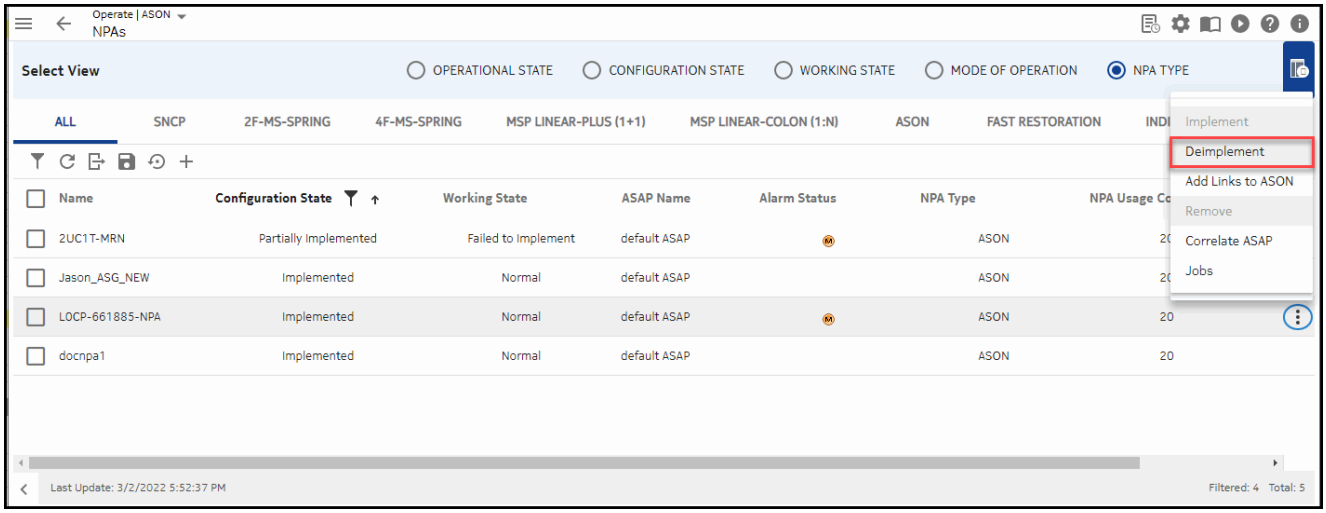
See 26.7 "Manage data columns" (p. 2213) for a detailed description and usage of the Manage Columns window.

3

To deimplement an NPA, do the following steps

- Select the NPA where you want to perform the operation, click the **More** icon and select **Deimplement** from the popup menu. .

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.



Result: The system displays a confirmation message.

4

Click **OK**

Result: The **Configuration State** changes to **Deimplemented** on the NPA data table and the system displays the following message at the bottom left of the window:

`Deimplement <NPA name> ✓ Success`.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.22 Manage 3Rs

Purpose

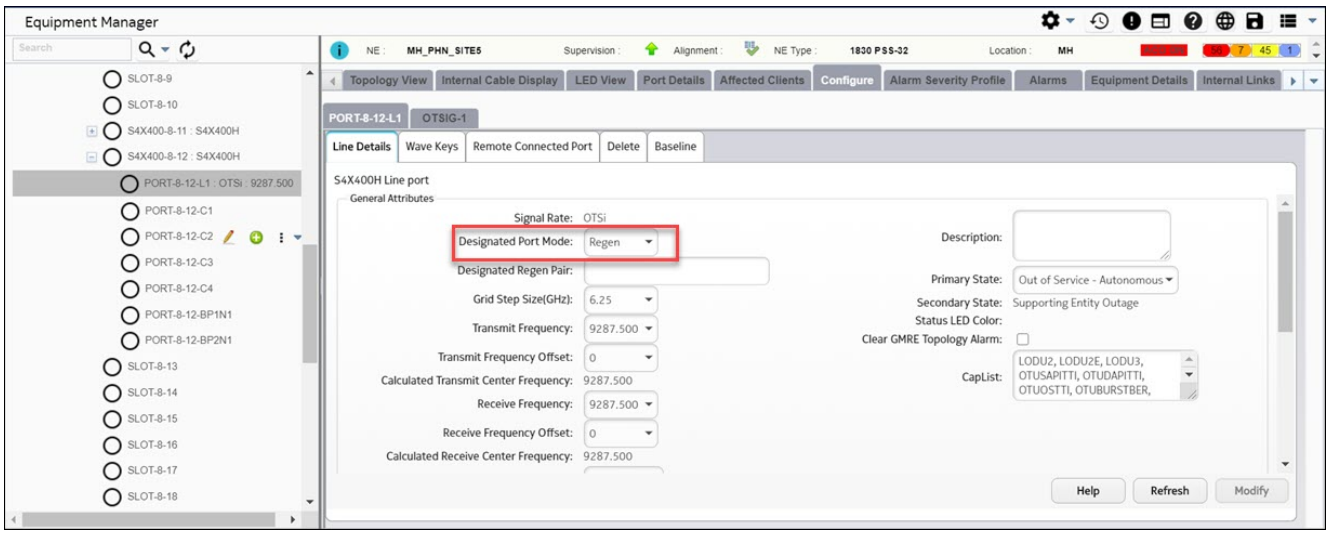
A 3R is a user-selected optical regeneration group that consists of a node and two NNI transponder line ports that reshape, retime, and retransmit a signal. Managing 3Rs for an NPA includes the creation of the 3R, the addition of the 3R to an existing NPA, the implementation of an existing 3R, and the removal of a 3R from an existing NPA.

3R is 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 10-27 OTSi – Designated Port Mode – Regen



Use these tasks to manage 3Rs for an existing NPA, ensure that the NPA is created.

When you add a 3R to an NPA or remove a 3R, the NPA is listed in the NPA data table in the **Implemented** or **Partially Implemented** configuration state.

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.

FOADM links

For FOADM links, the GMRE database of the transponder is built only after the cross connection is created manually from the NE. To create ASON 3R on FOADM links, manually create the cross

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

connection on the NE to retrieve the resource available in the GMRE database and then create 3R and unlock the links. See 10.27 “Set the ASON administrative state of links” (p. 1504) for details to unlock the links.

Task: Create a 3R

3R can be created from the Nodes or from the NPA page. If the node is already added to NPA, then the 3R is automatically added to the NPA. For S4X400H, S5AD400H, and S6AD600H, if the 3R is not a part of the NPA, then it is in allocated state. Complete the following steps to create a 3R from the NPA page.

1

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

OPERATE > ASON > NPAs > 360° View > 3R tab

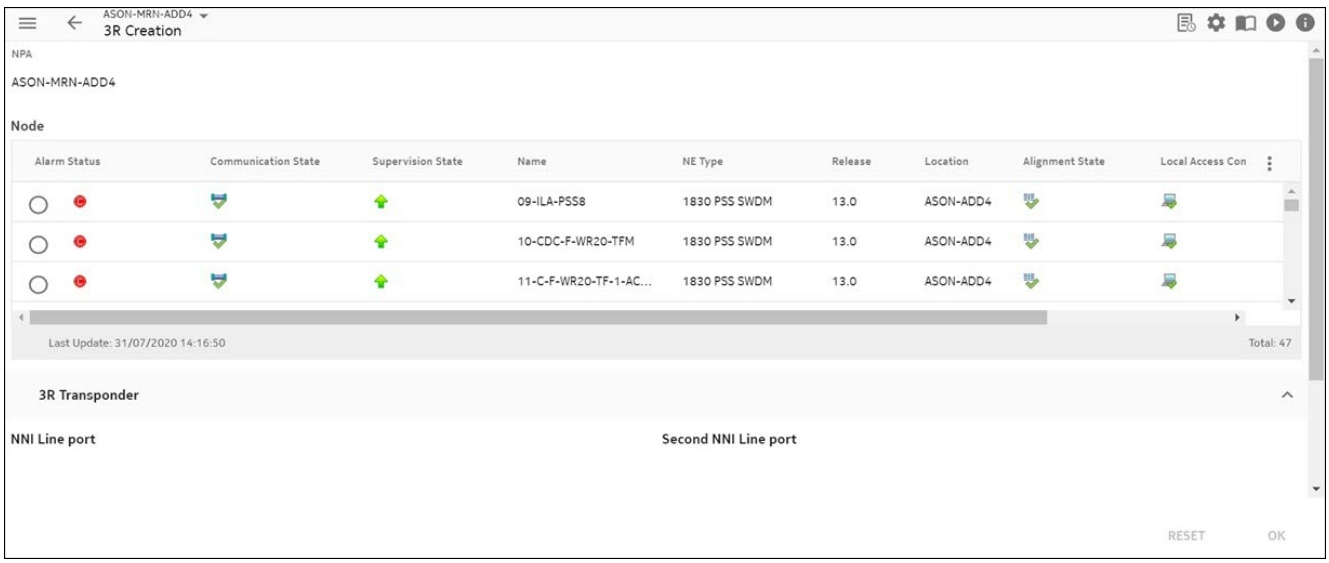
Result: The system displays the list of 3R in the data table.

2

Click the **Create** icon on the top left of the window.

Result: The system displays the **3R Creation** window.

Figure 10-28 3R Creation window



3

Select a node to be added to the 3R from the **Node** panel.

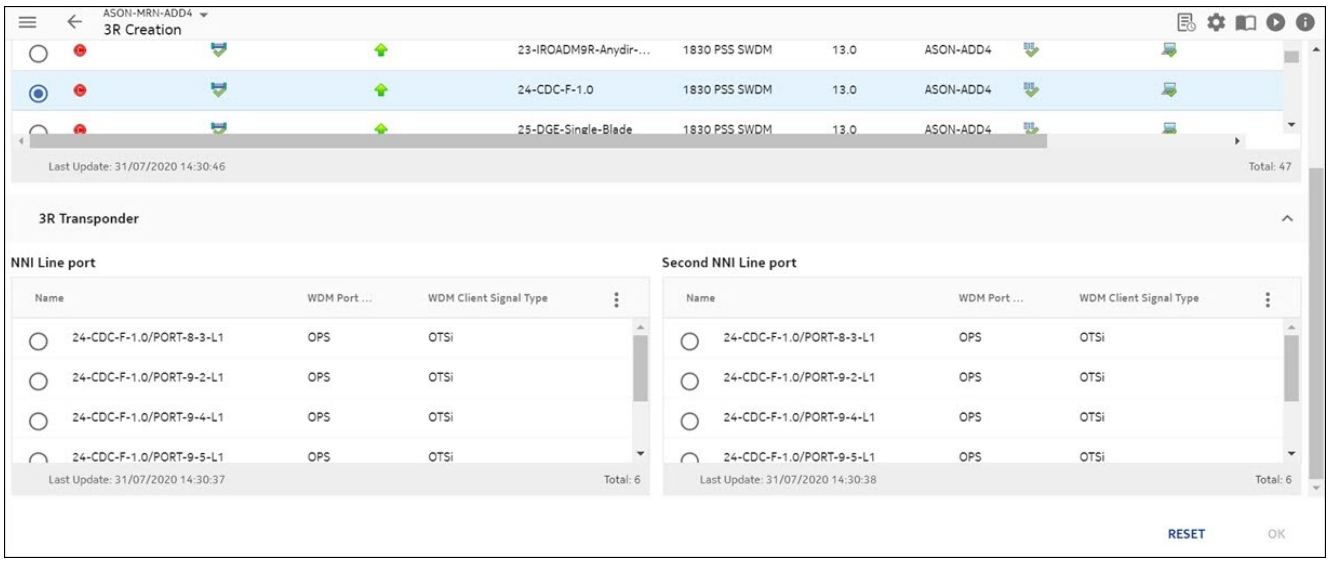
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

4

In the **3R Transponder** panel, configure the following fields:

- In the **NNI Line port** field, select a port to be added to the 3R Transponder panel.
- In the **Second NNI Line port** field, select a port to be added to the 3R Transponder panel.

Figure 10-29 3R Creation window: Add NNI Line ports



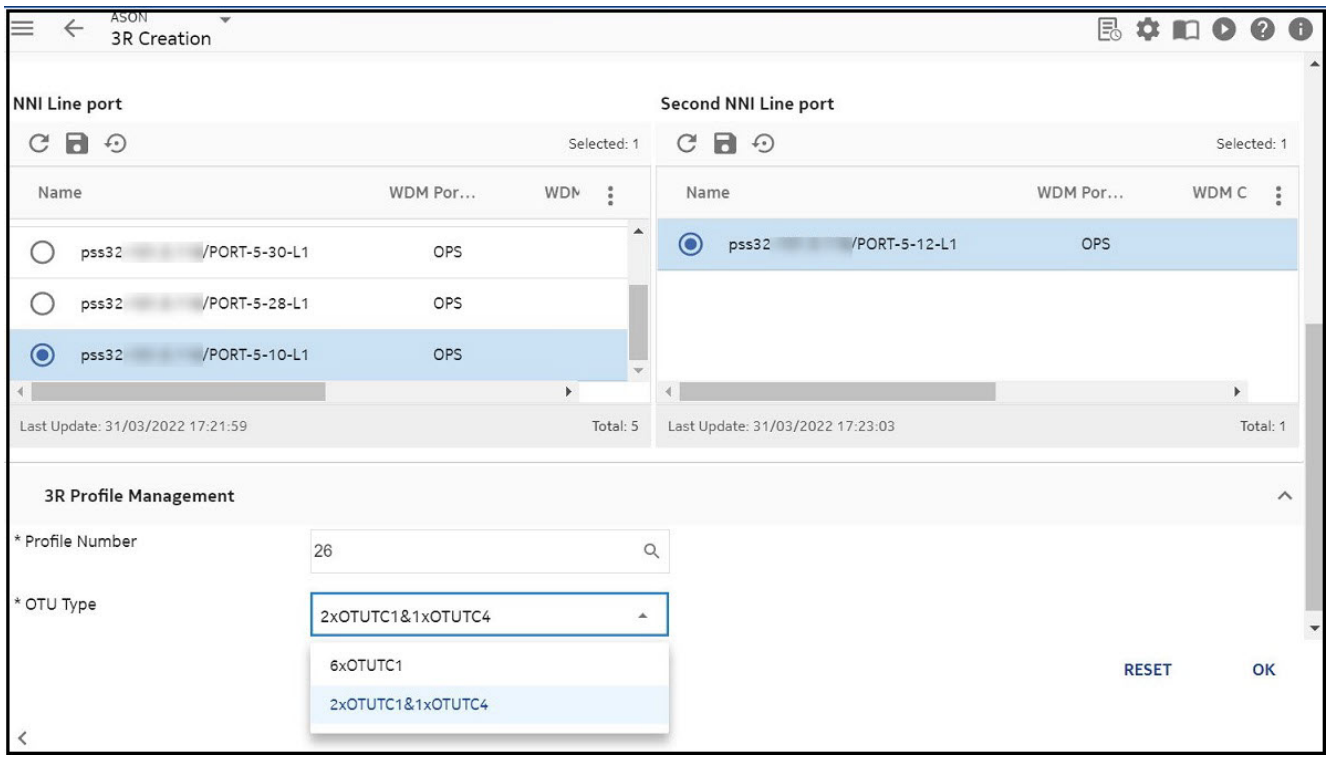
5

For S4X400H, S5AD400H, and S6AD600H, from the **3R Profile Management** panel, select the **Profile Number** and **OTU Type** as required.

Note: Both sides of the Regen is configured with the same profile ID as the profile ID is set on the Regen pair during 3R creation.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-30 3R Profile Management



6

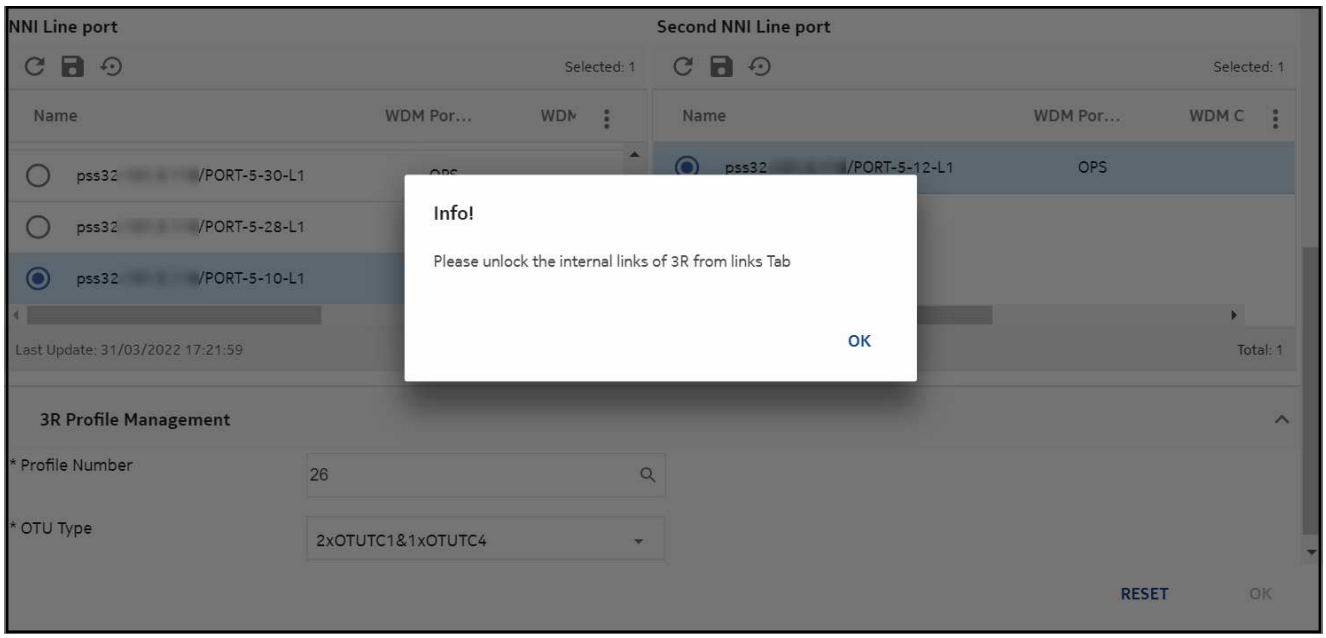
Click **OK**.

Result: The system adds the selected node and transponder ports as a 3R. The **3R** tab displays the created 3R with the profile ID and OTU structure details.

A pop-window is displayed informing that the internal links of 3R must be unlocked from the Links tab.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-31 Unlock 3R links



END OF STEPS

Task: Add a 3R to an existing NPA

Complete the following steps to add a 3R to an existing NPA.

1

From the NFM-T GUI, follow one of the navigation path:

OPERATE >Nodes > 360° View > 3R tab

OPERATE > ASON > NPAs > 360° View > 3R tab

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-32 Nodes – 3R

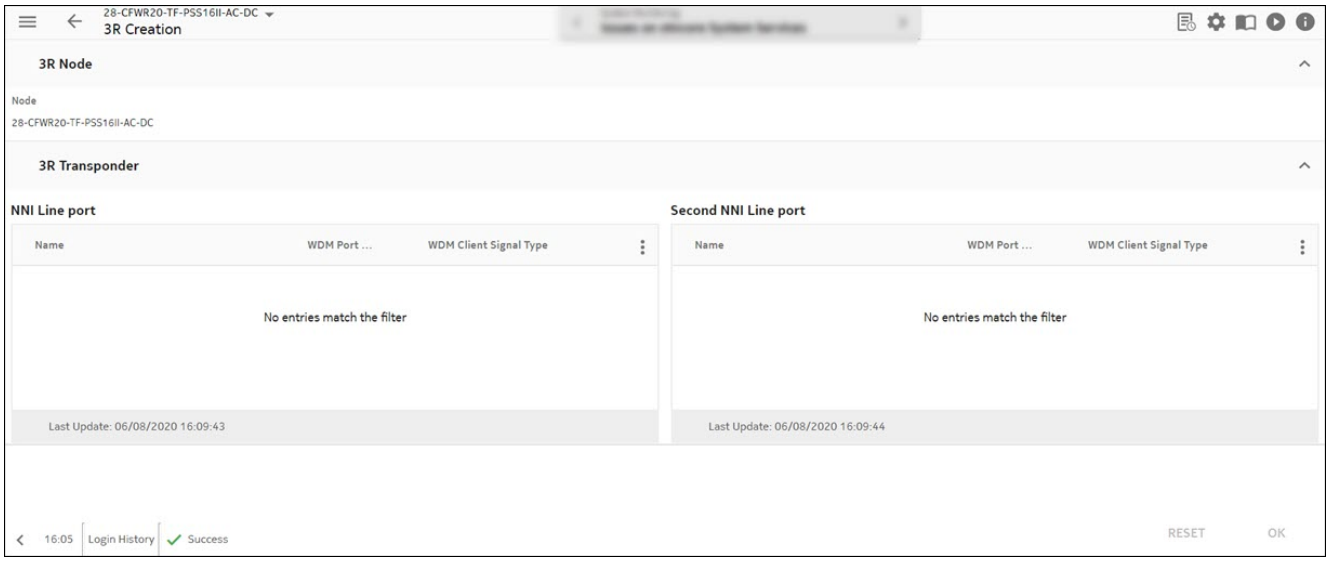
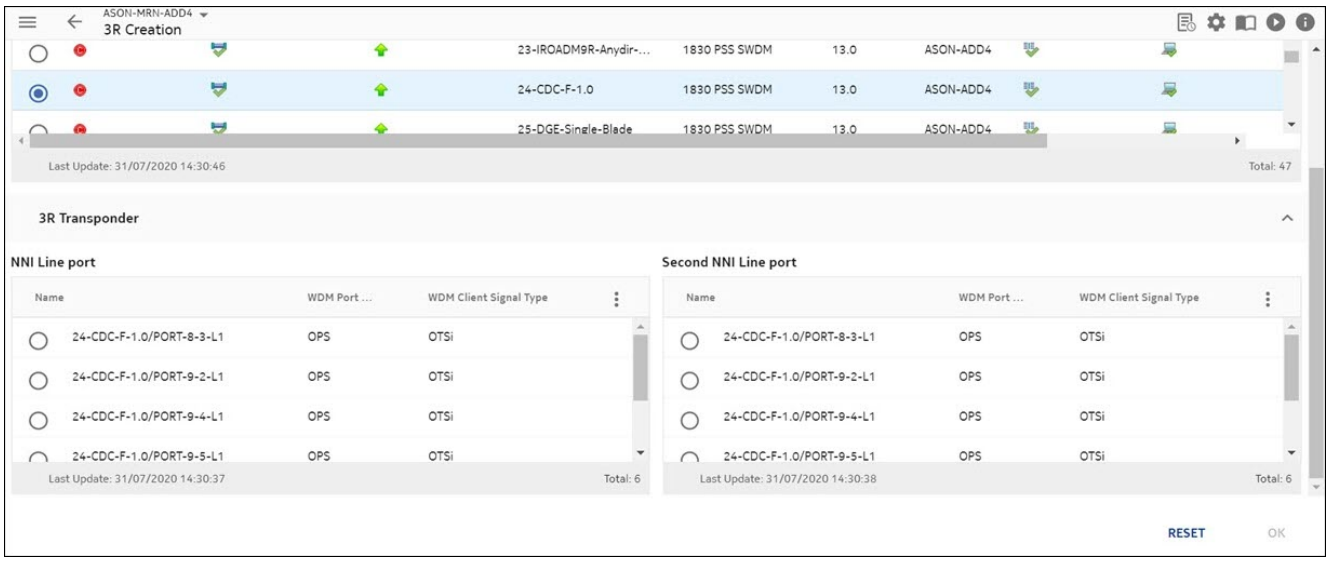


Figure 10-33 ASON – NPAs – 3R



Result: The 3R tab is displayed.

2

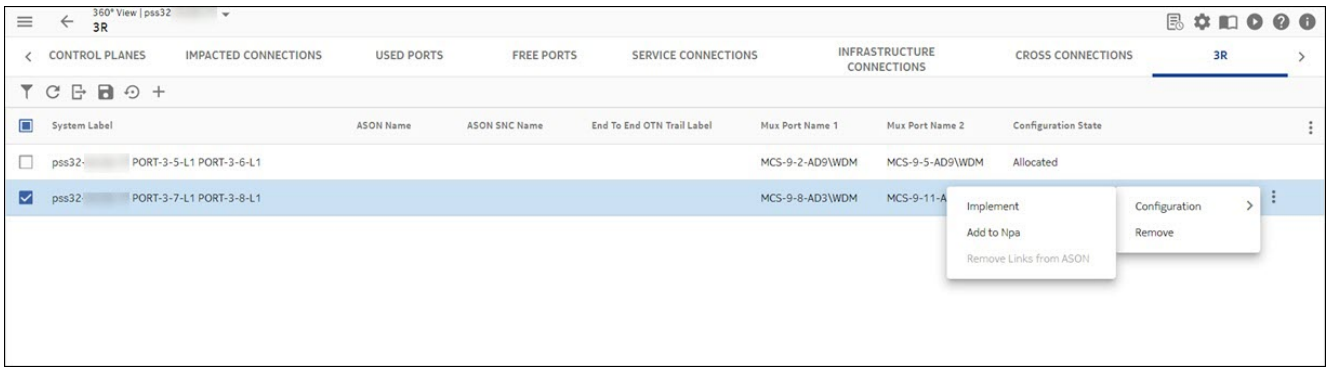
Select the 3R and then click the corresponding **More** icon.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

Click **Configuration > Add to Npa**.

Figure 10-34 3R functions



Result: The 3R is added to the selected NPA.

END OF STEPS

Task: Remove links from ASON

Complete the following steps to remove the links from ASON.

1

From the NFM-T GUI, follow this navigation path:
OPERATE > ASON > NPAs > 360° View > 3R tab.

2

Select the 3R and then click the corresponding **More** icon.

3

Click **Configuration > Remove Links from ASON**.

Result: The links are removed from the ASON.

See Figure 10-34, “3R functions” (p. 1491)

END OF STEPS

Task: Implement an existing 3R

Complete the following steps to implement an existing 3R.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

1

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

OPERATE > ASON > NPAs > 360° View > 3R tab

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

2

Select the 3R and then click the corresponding **More** icon.

3

Click **Configuration > Implement** to implement a 3R.

Result: The Configuration State changes to **Implemented** state in the 3Rs data table based on the selection.

See Figure 10-34, “3R functions” (p. 1491).

END OF STEPS

Task: Remove a 3R from an existing NPA

Complete the following steps to remove a 3R from an existing NPA.

1

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

OPERATE > ASON > NPAs > 360° View > 3R tab

Result: The system displays a list of NPAs in a data table.

2

Select the 3R and then click the corresponding **More** icon.

3

Click **Remove**.

Result: The 3R is removed from the existing NPA and deleted OTSig Structs created on the NEs.

See Figure 10-34, “3R functions” (p. 1491).

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.23 Manage jobs in ASON

Purpose

Use this task to manage jobs for an NPA.

Task

Complete the following steps to view the jobs for an NPA.

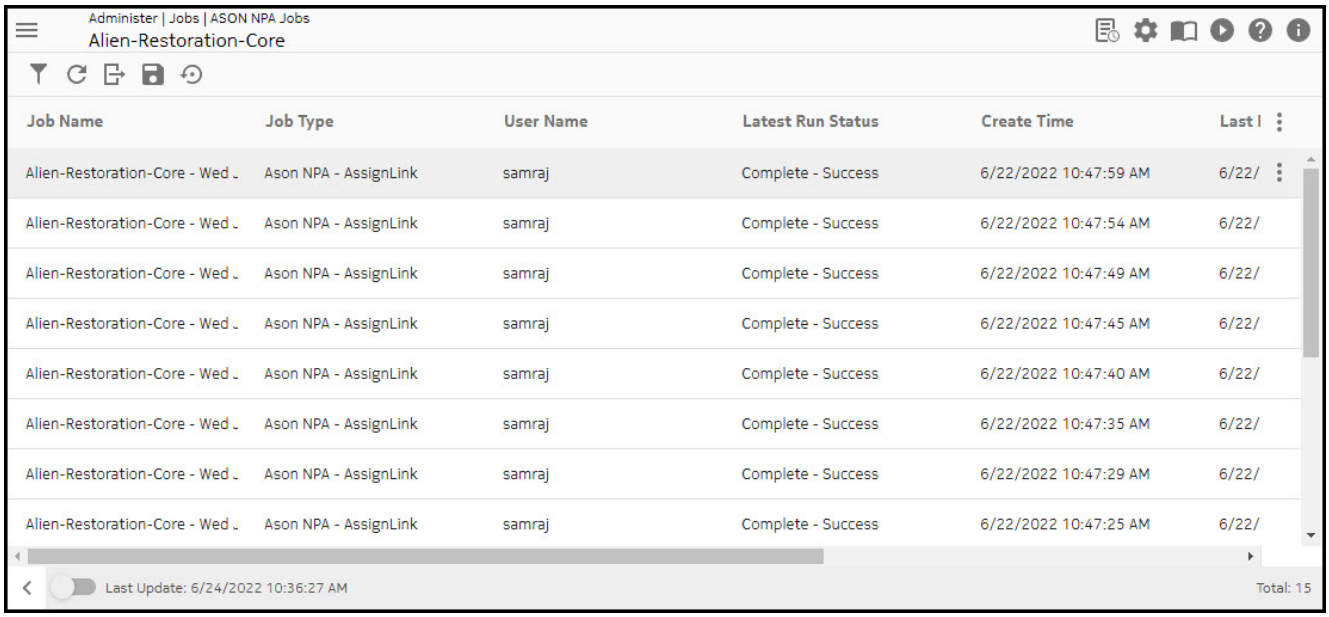
1

From the NFM-T GUI, follow this navigation path

OPERATE > ASON > NPAs > More icon > Jobs.

Result: A page displays the list of Jobs in the data table.

Figure 10-35 NPA Job window



2

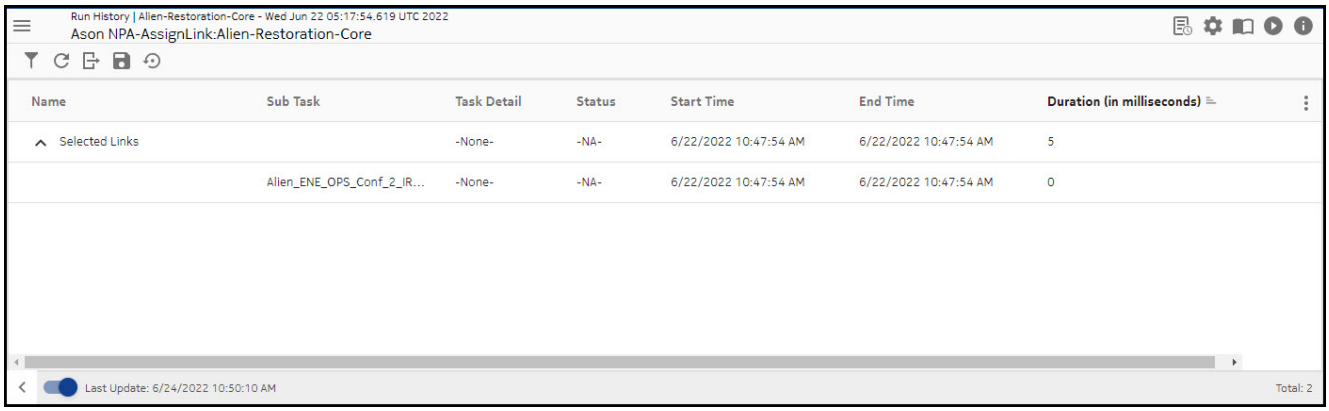
To reschedule a job right click and select **Reschedule Job** option.

3

To view the Job run details, right click and select **Run History** option.

Result: The system displays the **Results Details** window.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

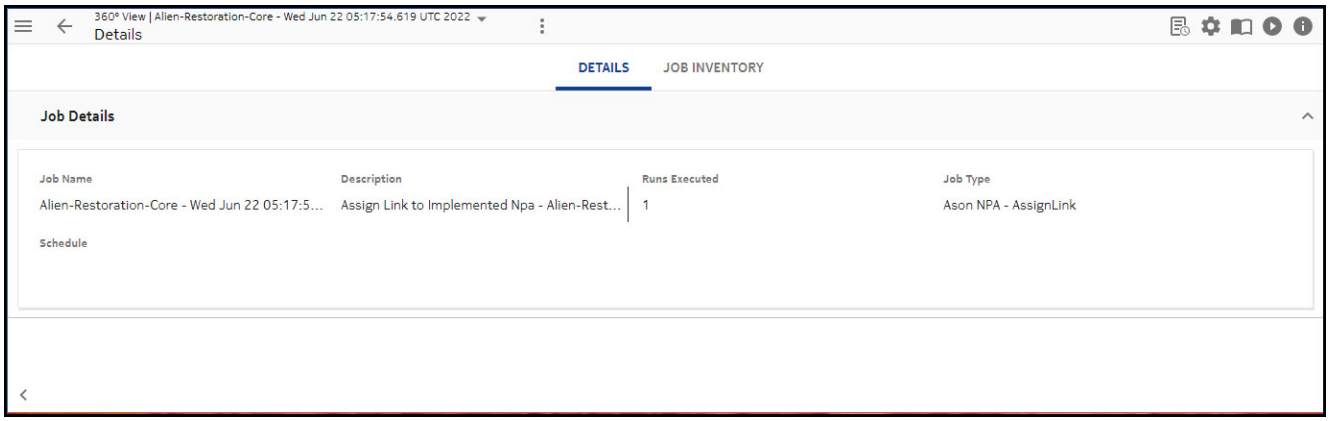


4

To delete a job, right click and select **Delete** option.

5

To view the details, click the **Details** tab in the lower panel.



6

To view the job inventory, click the **Job Inventory** tab in the lower panel.

End of steps

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.24 Modify TE Links

Purpose

Use this task to modify a Traffic Engineering (TE) link that is assigned to an NPA, color profile, or SRG.

Ensure that the NPAs are in **Implemented** state.

Task

Complete the following steps to modify a TE Link that is assigned to an NPA, color profile, or SRG.

1

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

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

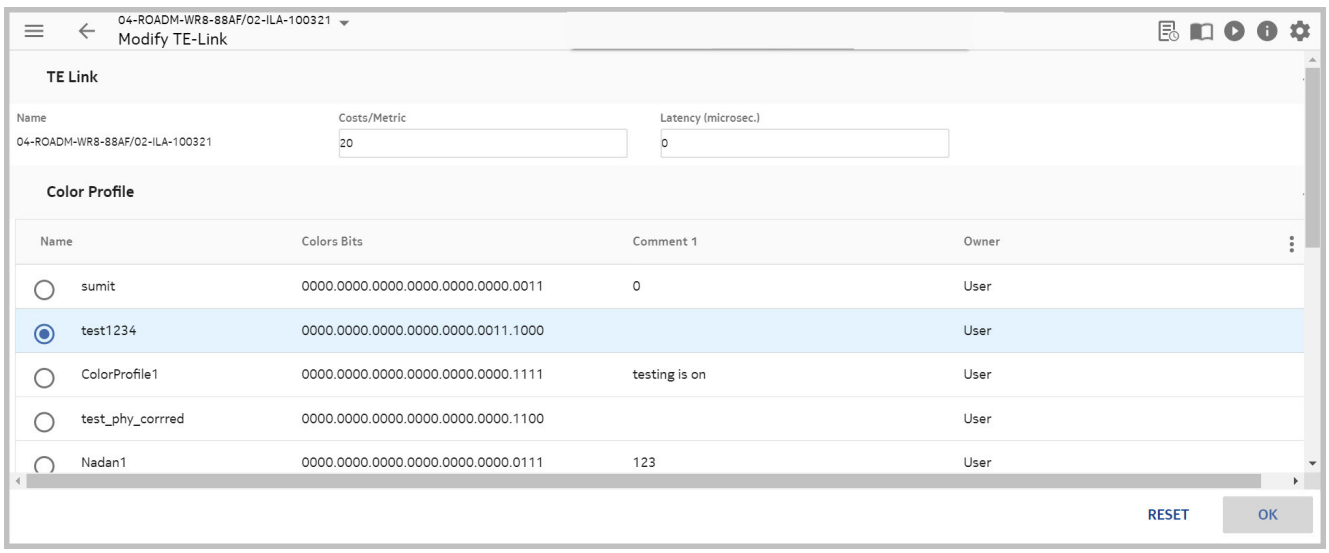
Result: The system displays the list of TE Links in the data table.

2

Select a TE Link, click the **More** icon, and click **Modify TE-Link**.

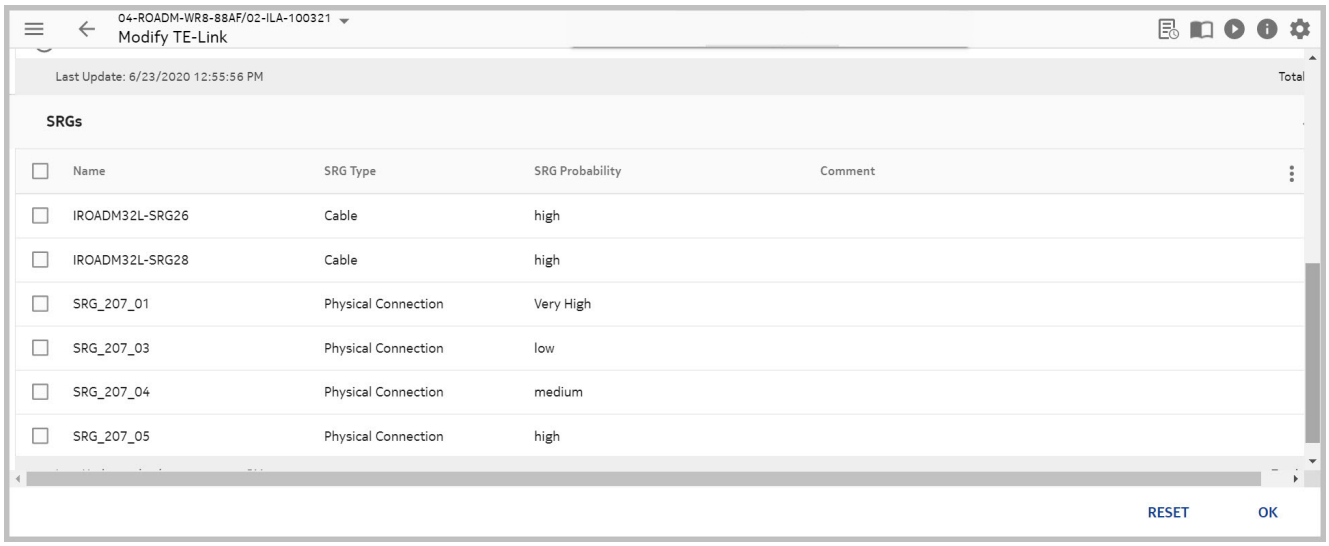
Result: The system displays the **Modify TE-Link** window.

Figure 10-36 Modify TE-Link window



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-37 Modify TE-Link window - SRG



3

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

- The **Name** field is auto populated.
- In the **Cost/Metric** field, use the up and down arrow to select the 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. Also, 0 is accepted only for FA-TERM and FA-UNTERM tunnels. The default is **20**.
- In the **Latency (microsec)** field, use the up and down arrow to specify a valid time for latency.
- In the **Color Profile** field, select the Color Profile.

4

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

5

Click **OK**.

Result: The system modifies the TE Link.

END OF STEPS

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

10.25 Perform link maintenance

Purpose

Use this task to access and perform the link maintenance.

Ensure that the NPAs are available and are in **Implemented** state.

Task

Complete the following steps to access the **Link Maintenance Window**:

1

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

OPERATE > ASON > NPAs > 360° View > LINKS (tab)

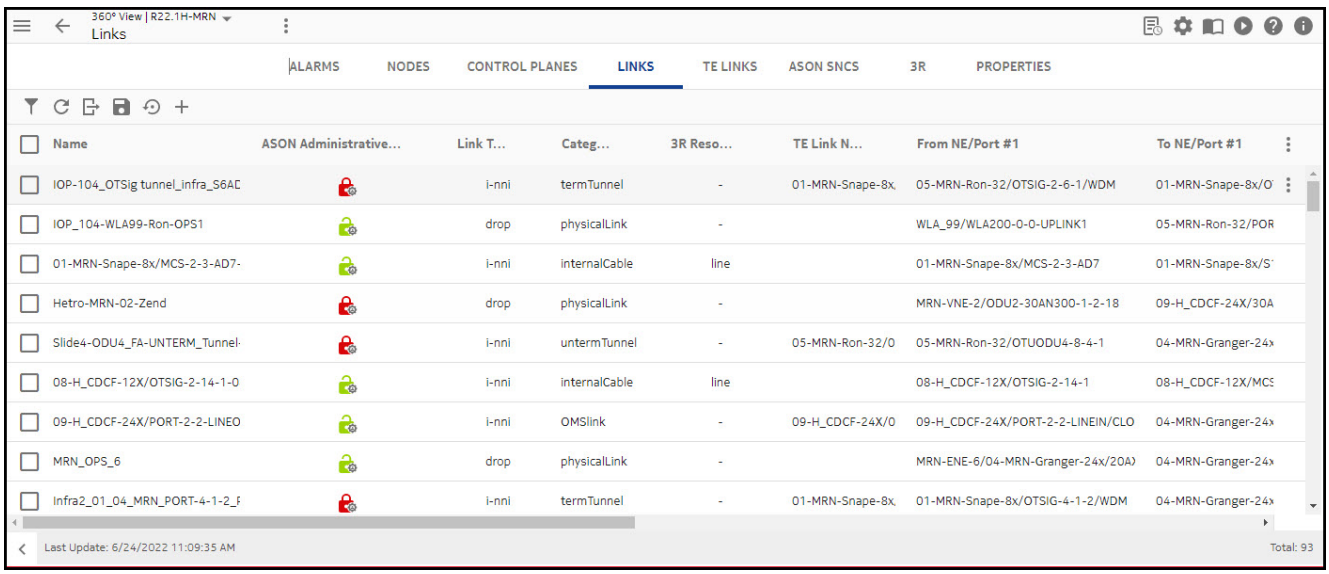
Result: The system displays the Links in the data table.

2

Select a link, click the **More** icon and select **Link Maintenance Window**.

Result: The system displays the **Link Maintenance Window** page, containing the Link Maintenance data table and its tabbed topics.

Figure 10-38 Link Maintenance window



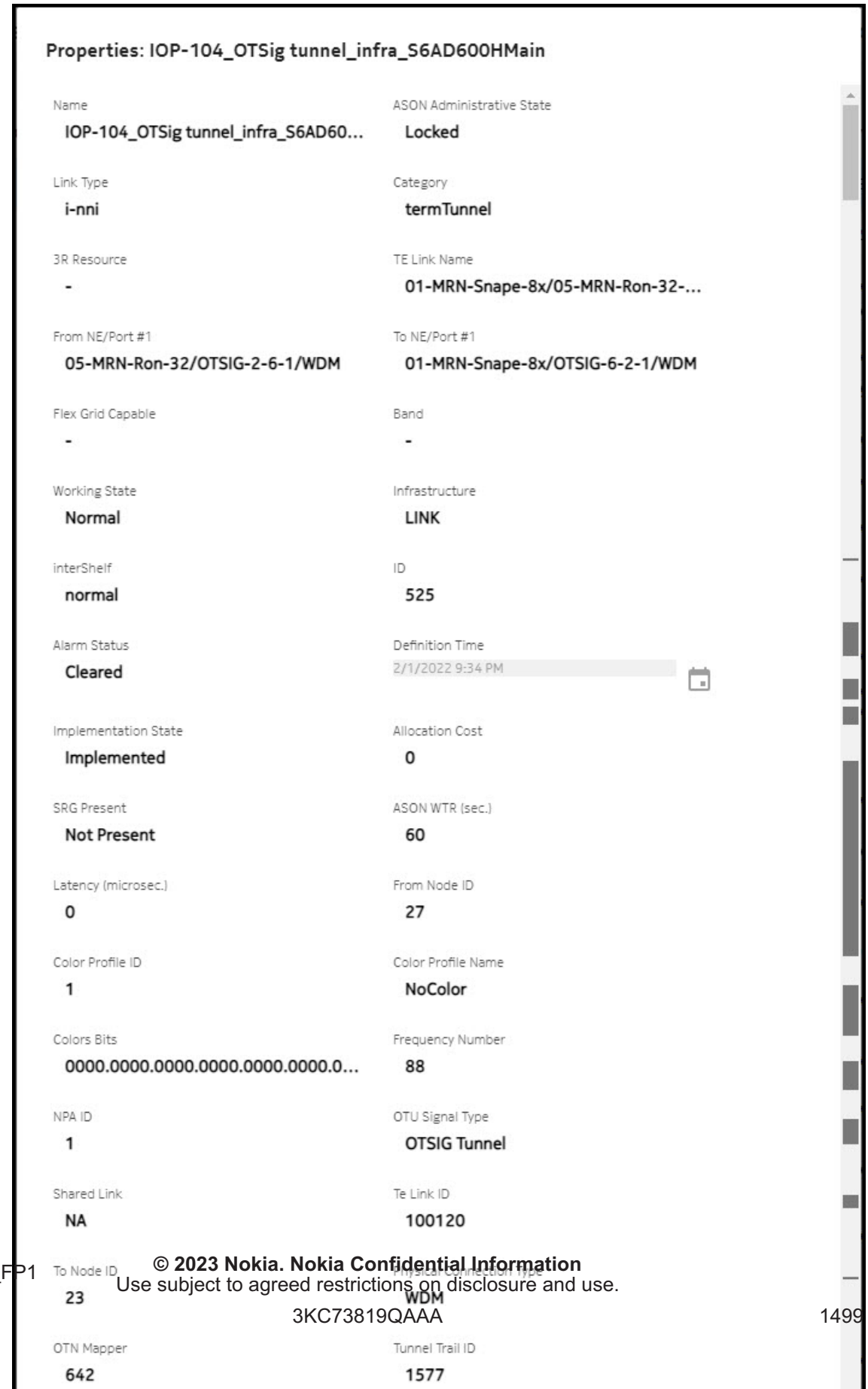
© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

3

To view the additional attributes of the selected link, click the **More** icon and select the attribute icon.

© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

Figure 10-39 Link Maintenance window - Attribute icon



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.

4

Perform the following operations from the **Link Maintenance** Window:

- Set the Administrative State. See 10.27 “Set the ASON administrative state of links” (p. 1504).
- Access Link Management Window.
- Change ASON WTR. See 10.18 “Change ASON WTR” (p. 1475).
- Add and Remove Links from ASON. See 10.15 “Add links and remove links from ASON” (p. 1462).
- Enable or Disable Auto Restoration of Links. See 10.20 “Enable or disable auto restoration of links” (p. 1480).
- Enable or Disable Shared Links. See “Task: Enable/disable shared link” (p. 1467).
- Assign TE Links. See 10.17 “Assign an ASON I-NNI link to a TE Link and SRG” (p. 1473).
- View the Misalignment report for a link. See 10.14 “Access and view the misalignment report for a link” (p. 1461).
- Access Jobs page.

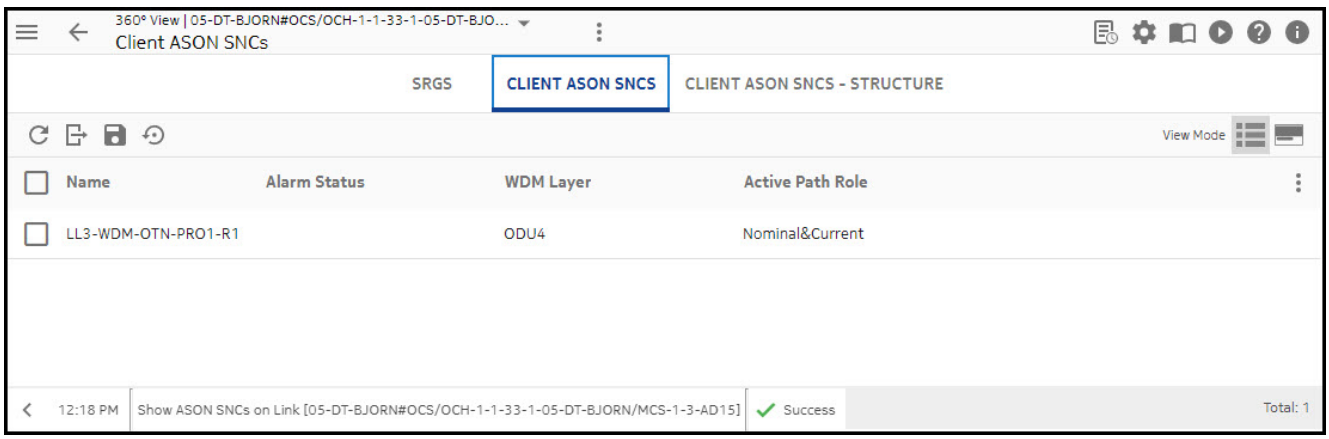
5

To view the tabbed topics for a particular link in the same browser window, select a link in any column except for the Name column, scroll down to the bottom of the window, and click on one of the following tabs: **SRGs**, **Client ASON SNCs**, **Client ASON SNCs - STRUCTURE**, or **Server Physical Connections**.

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

For example, the following figure depicts the **Client ASON SNCs**.

Figure 10-40 Client ASON SNCs tab



© 2023 Nokia. Nokia Confidential Information
Use subject to agreed restrictions on disclosure and use.