Network Element Director

Fiber Service Platform 3000R7

Product Release: 22.2
Document Issue: A
Document Number: 80000073682

ADVA™
An Adtran Company

Adtran Holdings, Inc.
901 Explorer Blvd.
Huntsville, AL 35806
USA

Adtran Networks SE, formerly known as ADVA Optical Networking SE (an Adtran company)
Campus Martinsried
Fraunhoferstrasse 9a
82152 Martinsried/Munich
Germany

Terms of Use (“Terms”):

Acceptance of Terms

By using this content, including without limitation any services, portals, webpages, manuals, documentation and any other information provided herein (hereinafter referred to as “Content” and/or “Service”), you assent to the following terms of use. If you do not agree to these terms, please do not use this Content.

If you are using this Content on behalf of your employer/hirer/contractor, you represent and warrant that you are authorized to accept these Terms on your employer's/hirer’s/contractor’s behalf.

Use of the Content and Service

You agree not to access the Content by any means other than through the interface that is provided by Adtran Networks SE. Adtran Networks SE, formerly known as ADVA Optical Networking SE, includes its affiliates and successors (”Adtran”). You will not use the Service for any purpose that is unlawful or prohibited by these Terms. You may not use the Service in any manner that could damage, disable, overburden, impair, or otherwise result in unauthorized access to or interference with, the proper functioning of any Content, accounts, systems, networks of Adtran or its licensor(s).

If parts of the Content (including without limitation service) require you to open an account, to choose a password and/or a user name, you are entirely responsible for maintaining the confidentiality of your password and account, and for any and all activities that occur under your account. You will maintain and promptly update your account and any information you provide to Adtran to keep it accurate, current and complete.

You will notify Adtran immediately of any unauthorized use of your account or any other breach of security. Adtran will not be liable for any losses you incur as a result of someone else using your password or account, either with or without your knowledge. However, you could be held liable for losses incurred by Adtran due to someone else using your account at any time, without the permission of the account hold.

You may obtain direct access via the Content (including without limitation portal or system) to certain confidential information of Adtran and its suppliers and contractors, including without limitation technical, contractual, product, delivery, pricing, marketing and other valuable information that should reasonably be understood as confidential ("Confidential Information"). You must hold Confidential Information in strict confidence. Title to Confidential Information remains with Adtran or its respective suppliers and contractors.

No Warranties

ALL CONTENT IS PROVIDED ON AN ''AS IS AVAILABLE'' BASIS WITHOUT ANY WARRANTY OF ANY KIND EITHER EXPRESSED OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ADTRAN MAKES NO WARRANTY AS TO THE ACCURACY, COMPLETENESS, OR RELIABILITY OF ANY CONTENT AVAILABLE HEREIN. USE OF THE CONTENT IS AT YOUR SOLE RISK. YOU ARE RESPONSIBLE FOR VERIFYING ANY INFORMATION BEFORE RELYING ON IT AND FOR TAKING ALL NECESSARY PRECAUTIONS TO ENSURE THAT CONTENT IS FREE OF VIRUSES. The content of this document may include technical inaccuracies or typographical errors. Adtran may make changes at any time to the Content (including without limitation portals, systems, products or specifications) without notice and makes no commitment to update Content.

Adtran may provide economic projections and forward-looking statements on this Content (including without limitation on portals or systems) that relate to future facts. Such projections and forward-looking statements are subject to risks which cannot be foreseen and which are beyond the control of Adtran. Adtran is therefore not in a position to make any representation as to the accuracy of economic projections and forward-looking statements or their impact on the financial situation of Adtran or the market in the shares of Adtran.

Limitation of Liability

IN NO EVENT SHALL ADTRAN NETWORKS SE OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THE ACCESS OR USE OF THE CONTENT (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND BASED ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE), EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE SAME APPLIES FOR ANY HARDWARE OR SOFTWARE INCLUDED IN THE CONTENT, UNLESS A SIGNED AGREEMENT WITH ADTRAN NETWORKS SE OR ITS AFFILIATE(S) OR THE APPLICABLE PRODUCT LIABILITY LAW EXPRESSLY STATES OTHERWISE.

Trademarks and Copyright

Documents and information, including text, images, graphics, sound files, animation files, video files and their arrangement made available in the Content (including without limitation the portal or system) are subject to copyright and other intellectual property protection. They may not be copied for commercial use or distribution and may not be modified or reposted to other internet sites.

Unless otherwise indicated, all marks displayed on the Content (including without limitation portals) are subject to the trademark rights of Adtran Networks SE or the respective trademark owner. Adtran Networks SE and the Adtran Networks SE Logo are trademarks or registered trademarks of Adtran Networks SE in Germany and other countries.

Any software that is made available for download from the Content ("Software") is a copyrighted work of Adtran or the respective copyright owner.

The furnishing of this content does not give you any license or rights with respect any content, patents and/or trademarks herein, unless the Content (including without limitation software) is governed by the terms of your signed agreement with Adtran. Any reproduction or redistribution of the Content (including without limitation Software) not in accordance with the foregoing is expressly prohibited.

Third Party Content

Third-party content is the property of their respective owners and does not imply a partnership between Adtran and any other company. Any references to content that is not from Adtran are provided for convenience only and do not in any manner serve as an endorsement of that content.

Software generally known as "open source software" is licensed pursuant to the applicable license terms, accessible under the following link: https://advadocs.com/webhelp/4237/Default.htm. The copyright owners of such software disclaim all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose, and all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits.

Export Controls

The Content (including without limitation service, Software, or technology derived or obtained from the portals) may be subject to the export control laws and/or the import laws of various country ("Controlled Items"). This includes without limitation the export control laws and regulations of Germany, the European Union, and the United States. You agree to comply strictly with all such laws. In particular, you will not use, distribute, transfer or transmit the Controlled Items (even if incorporated into other products) except in compliance with such laws. You are also responsible for complying with all applicable legal regulations of the country where you are registered, and any foreign countries with respect to the use of the Controlled Items by you, your affiliates, subsidiaries, directors, employees, authorized users and permitted third parties, including end-users. Adtran will support you in obtaining any necessary export or import license for Controlled Items. You agree that none of the Controlled Items will be sold or otherwise transferred to, or made available for use by or for, any entity that is (a) named on the EU, U.S. or other government-issued Sanctioned Party Lists (Denied Party List, Restricted Party, etc.) or (b) engaged, directly or indirectly, in the design, development, production, stockpiling, or use of chemical or biological weapons, nuclear programs (including activities related to nuclear devices, nuclear reactors, and nuclear fuel-cycle activities), missiles and maritime nuclear propulsion projects, except as authorized under applicable laws and regulations.

You agree that, in the event you are notified by Adtran, a third party or a governmental agency about a license requirement for Controlled Items or particular transactions, you will not export or re-export the Controlled Items or pursue the transactions, directly or indirectly, until the required licenses are obtained, and work with Adtran, the third party or the governmental agency to procure the required licenses.

You agree to indemnify and hold harmless Adtran in the event of your non-compliance with any applicable German, EU, and U.S. export control laws and the export controls or import laws of other countries.

Governing Law and Place of Jurisdiction

The Content and any dispute arising out of or in connection with this Content is governed by German Law, without its choice of law provisions and the United Nations Convention on Contracts for the International Sale of Goods is hereby excluded. The District Court of Munich has exclusive jurisdiction for any dispute arising out of or in connection with this Content.

Privacy Statement

All terms related to our privacy information are available at: https://www.adva.com/en/about-us/legal/privacy-statement

All terms related to our privacy information for Customer Portal users are available at: https://advaoptical-communities.force.com/customerportal/CustomerPortalTCs

Contents

Preface

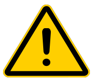
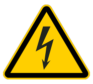
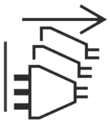
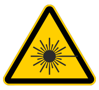
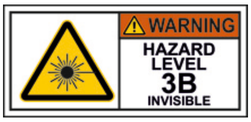
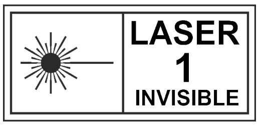
The pictures or graphics shown in this document are for reference only. They are based on the latest hardware revision available at the time of publication. The equipment you received might look different than pictures or graphics shown in this document.

Fiber Service Platform 3000R7 Documentation Suite

- Fiber Service Platform 3000R7 Hardware Description
- Fiber Service Platform 3000R7 High-Density Subshelf Hardware Guide
- Fiber Service Platform 3000R7 Installation and Commissioning Manual
- Fiber Service Platform 3000R7 Maintenance and Troubleshooting Manual
- Fiber Service Platform 3000R7 Management Data Guide
- Fiber Service Platform 3000R7 Module and System Specification
- Fiber Service Platform 3000R7 NETCONF User Guide
- Fiber Service Platform 3000R7 Network Element Director
- Fiber Service Platform 3000R7 Provisioning and Operations Manual
- Fiber Service Platform 3000R7 Safety Guide
- Fiber Service Platform 3000R7 FSP 3000 C Secure System Configuration Guide
- Fiber Service Platform 3000R7 TL1 Commands and Syntax Guide
- Fiber Service Platform 3000R7 TL1 Maintenance and Troubleshooting Manual
- Fiber Service Platform 3000R7 TL1 Module Parameters Guide

Safety Symbol and Message Conventions

You will see these symbols throughout the documentation. All personnel should correctly follow and not ignore any safety instructions.

Icon	Meaning	Description
	Warning	Means danger and alerts you to a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved and be familiar with standard practices for preventing accidents.
	Electric Voltage Warning	Means danger and alerts you to risks caused by electricity that could result in death or serious injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.
	Shock hazard warning. Disconnect all power plugs.	Indicates that all power sources must be disconnected before servicing to avoid shock hazard.
	Laser Radiation Warning	Warns you about the risk of possible laser radiation, which may result in a serious eye injury.
	Laser Radiation Warning – Hazard Level 3B	Warns you about the risk of possible laser radiation if the system is not used as designed or altered in any way.
	Laser Radiation Warning — Class 1 Laser	Warns you that the equipment contains Class 1 lasers, which are safe under all normal use conditions. It also alerts you to the risk of possible laser radiation if the system is not used as designed or altered in any way.

Icon	Meaning	Description
⚠ CAUTION LASER 1M invisible	Laser Radiation Warning – Class 1M Laser	Warns you that the equipment contains Class 1M lasers, which are safe for all conditions of use except when the beam is passed through magnifying optics. It also alerts you to the risk of possible laser radiation if the system is not used as designed or altered in any way.
⚠ CAUTION HAZARD LEVEL 1M INVISIBLE	Laser Radiation Warning – Hazard Level 1M	Warns you that the equipment contains Class 1M lasers, which are safe for all conditions of use except when the beam is passed through magnifying optics. It also alerts you to the risk of possible laser radiation if the system is not used as designed or altered in any way.
⚠	Caution	Alerts you to a potentially hazardous situation or condition that may result in minor or moderate injury.
⚠	Lifting Hazard Caution	Indicates a potentially hazardous situation or condition that may result in a personal injury or damage to equipment due to the weight of an object.
⚠	Skin Burn Caution	Indicates the risk of possible skin burns. When working with system components, be aware of proper handling procedures.
⚠	Electrostatic Caution	Indicates the possibility of equipment damage due to electrostatic discharge (ESD). If the ESD-prevention instructions are ignored or not followed correctly, damage can occur.
NOTICE	Notice	Indicates the risk of equipment damage, malfunction, process interruption, or negative impacts on surroundings.
📖	Documentation	Advises of the importance of carefully reading all instructions before proceeding or provides links to additional information to read. Failure to do so may result in personal injury or damage to equipment.

Icon	Meaning	Description
🗑	Waste Disposal Alert	Points out the importance of properly disposing of waste electrical or electronic equipment and its components. Disregard of the instruction can threaten the environment.
🗒	Note	Indicates supplemental information or helpful recommendations.

Documentation

Accessing Documentation

Documentation Portal	https://advadocs.com/

Documentation Feedback

We want our documentation to be as helpful as possible. Feedback is always welcome.

Email	admin@advadocs.com
Mail	Adtran Holdings, Inc. 901 Explorer Blvd. Huntsville, AL 35806 USA ADVA Campus Martinsried Fraunhoferstrasse 9a 82152 Martinsried/Munich Germany

Obtaining Technical Assistance

Product Maintenance Agreements and other customer assistance agreements are available for ADVA products through your ADVA distribution channel. Our service options include:

- 24 x 7 telephone support
- Web-based support tools
- On-site support
- Technical training, both on-site and at ADVA facilities in Germany and the USA
- Expedited repair service
- Extended hardware warranty service

Customer Portal

You can use the customer portal to:

- Access company information and resources at any time.
- Find information specific to your requirements, such as networking solutions, services, and programs.
- Resolve technical issues by using online support services.
- Download and test software packages.
- Order ADVA training materials.

Access	https://www.adva.com/en/customer-portal
Questions	customer-portal-admin@adva.com

Technical Services

Technical services are available to customers who need technical assistance with an ADVA product that is under warranty or covered by a maintenance contract.

Online	https://www.adva.com/en/about-us/contact
Email	support@adva.com

Call ADVA

Europe, Middle East and Africa
Martinsried/Munich, Germany
+49 (0)89 89 06 65 0

North America
Norcross, GA, USA
+1 678 728 8600

Network Element Director Quick Start Guide

The **Network Element Director** (NED) Quick Start Guide (QSG) contains information for experienced users of the **Craft** or **Web Console** to transition into using Network Element Director.

The NED Quick Start Guide contains these topics:

Logging in to NED

To use NED you need:

- A PC or laptop with a screen resolution of 1920 x 1080 or higher.
- A web browser — the latest versions or the latest Extended Support Release of Google Chrome, Microsoft Edge, or Mozilla Firefox.
- An IP connection to the node using one of these methods:
  - If the NCU has no database or is reset to factory defaults, do this: After you connect to the NCU C1, the NCU issues an IP address through DHCP. The NED login page opens.
  - A direct connection to NCU port C1 through a user-configured IP address or the default IP address of 192.168.1.1.
    If the option "HTTP Redirect to HTTPS" is disabled, you must enter "https://" before IP address.
  - A connection through an IP network with a minimum bandwidth of 256 kbps.

To log in:

1. Open a browser window.
2. In the address bar, type your node IP address.
3. Press Enter to open the login page.
4. Enter the user name.
5. Enter the password.
6. Click **Login**.

> If your user name includes a hyphen, the login fails.

If the login process includes two-factor authentication, you must enter an authentication username and password. The password includes a token code + a PIN. You might also encounter a challenge process, which requires you to answer a set of additional questions before you can log in. You can use both login methods only for remote authentication, either through RADIUS or TACACS+.

> At the prompt, after your first log in, change the default password.

Directly Accessing NED Applications

In addition to the NED login, on the login page you can directly log in to these applications:

- Equipment Install - If the modules are pre-provisioned, this application guides you to install the modules in the correct slots.
- Fiber Install - If you previously enter or download the physical connections, this application guides you to install fibers between the ports.
- Channels Overview - Provides a graphical overview of the optical channel power on ROADM and all associated equipment for channel monitoring.

You can use these applications to access NED or the other applications.

To log in:

1. Open a browser window.
2. In the address bar, type your node IP address.
3. Press Enter.
4. On the login page, select the appropriate application. The default is NED.
5. Enter the user name.

6. Enter the password.
7. Click **Login**.

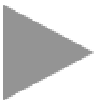
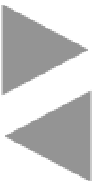
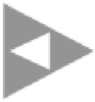
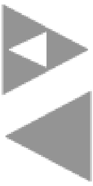
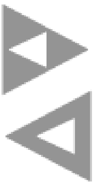
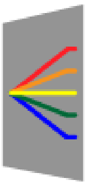
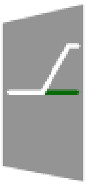
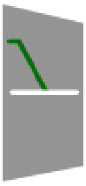
📝	If your user name includes a hyphen, the login fails.

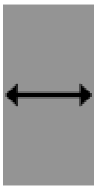
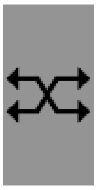
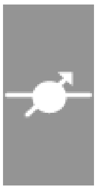
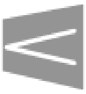
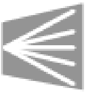
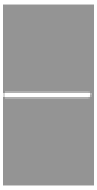
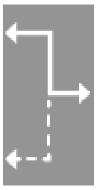
Icons and Symbols

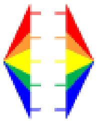
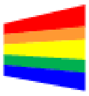
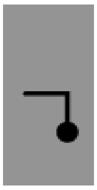
ⓘ	Information
⚠	Minor alarm
◆!	Major alarm
🛑!	Critical alarm
✇	Fan failure alarm
?	Help
⊗	Equipment mismatch

Module Symbols

These symbols represent equipment in the signal path.

Symbol	Description
	Amplifier module with an EDFA amplifier.
	Amplifier module with bidirectional EDFA amplifiers.
	Amplifier module with a RAMAN amplifier.
	Amplifier module with RAMAN and EDFA amplifiers.
	Amplifier module with bidirectional RAMAN amplifiers.
	Filter module with no upgrade port.
	Filter module with an upgrade port, N to C path.
	Filter module with an upgrade port, N to U path.

Symbol	Description
	Channel module that supports a signal path only between N to C port, such as transponder or muxponder modules.
	Channel module that supports signal paths between different ports, such as ADM or cross-connect modules.
	Optical power control module.
	Optical power splitter/combiner module.
	Optical power splitter/combiner module with multiple ports.
	Optical passthrough module.
	Optical switch module.

Symbol	Description
	ROADM module that provides bidirectional-channel power control but does not support channel routing.
	ROADM module that supports N port transmit channel power and directs channels to a specific C port.
	Module that terminates the signal path.

Accessibility and Shortcuts

NED is an Internet browser application that runs on your computer. You can change settings on your computer operating system or Internet browser to make it easier to see and use NED.

> Chrome, Firefox, and Edge browsers support accessibility functions.

This section contains these topics:

Using Browser Controls

Internet browsers provide accessibility options for those who have visual or physical disabilities. Accessibility features can also be helpful if you use a mobile device or table, or have a slow network connection. In your Internet browser you can change the appearance of items in NED:

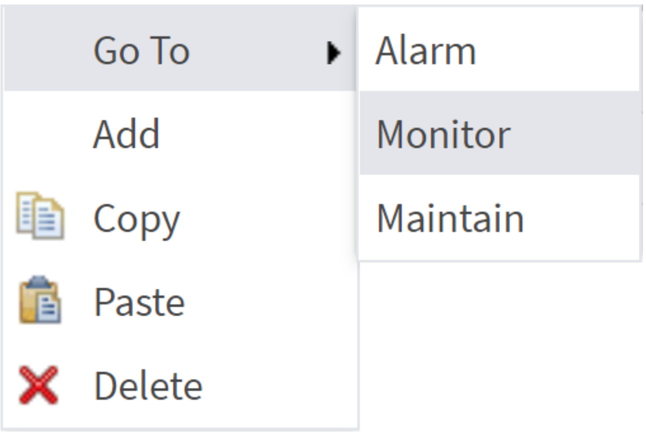
- Zoom in to enlarge the text: Press Ctrl + plus symbol (+).
- Zoom out to see more of the page: Press Ctrl + hyphen symbol (-).
- Return to the default size: Press Ctrl + zero (0).
- Change the font type and size.
- Change foreground and background colors.
- Increase the contrast: Press Left Shift + Left Alt + Function + Print Screen (or PrtScn)
- Specify the color for hyperlinks.

For more details, in your Internet browser Help or search engine, or on your PC, enter the search terms accessibility or ease of access.

See also **Shortcut Keys** for Network Element Director here.

Using Shortcut Menus

Right-click items in NED to open related shortcut menus. Use shortcut menus to change between applications while you maintain your current selection in the **Navigation Tree**. For example, after you configure a channel module, open the shortcut menu to change to the **Monitor** application on the same channel module.



Use shortcut menus to:

- Add items, such as optical lines or modules.
- Delete items.

- Copy and paste (clone) items and configuration information within a single node or to another node.
- Track Channels through a node by using **Node Channel Trace**.

Using Shortcut Keys

Shortcut	**Description**
F1	Open the FSP 3000R7 NED Help
Ctrl + Left Arrow Ctrl + Right Arrow	Navigate between equipment applications: Configure, Alarm, Monitor, and Maintain. Retains the navigation Tree selection.
QWERTY keyboards: Ctrl + \ QWERTZ and QWERTY keyboards: Ctrl + .	Navigate between all applications: Overview, Configure, Alarm, Monitor**,** Maintain, Node, Services, and Network. Does not retain the Navigation Tree selection.
Tab	Show shortcut buttons for navigation between applications.
F3	Select Overview.
F4	Select Configure.
F6	Select Alarm.
F7	Select Monitor.
F8	Select Maintain.
F9	Select Node.
F10	Select Services.
F11	Select Network.
Tab	Move forward through fields including buttons, links, areas, table headers, table rows, panels.
Shift + Tab	Move backward through fields including buttons, links, areas, table headers, table rows, panels.
Escape (Esc)	Exit selection without change or Cancel. Close overlay without change. Close NED Messenger window.
Enter	Select items such as buttons, rows, menus, and lists. Open or close windows.
Space Bar	Select items from a menu or list.Select or clear fields. Open or close windows.

Navigation Tree	Description
Down Arrow	Move down the tree.
Up Arrow	Move up the tree.
Right Arrow	Expand the tree item.
Left Arrow	Collapse the tree item.
Enter	Select the tree item.

Table Headers	Description
Left Arrow	Move left through columns; does not wrap.
Right Arrow	Move right through columns; does not wrap.
Enter	Sort a table column either in ascending or descending order.

Table Rows	Description
Up Arrow	Move up through rows; does not wrap.
Down Arrow	Move down through rows; does not wrap.
Left Arrow	Move left through columns; does not wrap.
Right Arrow	Move right through columns; does not wrap.

Tabs, Buttons, Fields, Lists	Description
Up Arrow	Move through options with wraparound; response is immediate.
Down Arrow	
Left Arrow	
Right Arrow	

Panels	Description
Up Arrow	Increase the Alarm panel size when you select size adjust, indicated by the blue line next to the relevant area.
Down Arrow	Decrease the Alarm panel size when you select size adjust, indicated by the blue line next to the relevant area.
Enter	Open or close the Navigation Tree when you select size adjust, indicated by the blue line next to the relevant area.

> If Windows requests confirmation of configuration changes, default to **Cancel**.

> If you press Tab or Shift + Tab, the software omits the **Edit** link. To change settings in the Configure and Monitor details windows, navigate to a row and then press Enter.

Navigation Path: Breadcrumbs

In the **Navigation Path**, click items to browse backward through the selected path. In web navigation this process is also known as following the breadcrumb trail.

Sorting Information

- To sort information, in the **Alarm Panel**, **Alarm** application and **Node** application (Logs), click the applicable column header.
- To sort identifiers, click the **Identifiers** column in tables where they appear. The software sorts the content based on shelf and slot numbers and ignores the type, for example: CH-.

Filtering

In some tables you can use Search or Search and Date Range. The table filters the text you enter in the search field or in the date range field. To filter the information, in the **Alarm** application, click a Module or shelf.

Copying and Pasting a Module Configuration

You can copy and paste the configuration of a provisioned module to an unprovisioned slot. When you paste a channel module configuration to a new slot, you can set the network-port channel number.

Complete these steps to copy and paste the module configuration to an unprovisioned slot.

1. Click **Configure**.
2. In the **Navigation Tree**, select the shelf where the module whose configuration you want to copy is located.
3. Complete one of these actions:

- Select the module, and in the **Main Window** click **Copy**.
- Right-click the module and select **Copy**.
- In the **Main Window** shelf graphic, right-click the module and select **Copy**.

4. To paste the copied module with its configuration, complete one of the actions in the table that follows.

To paste the module to a shelf in the same node:	1. In the **Navigation Tree**, select a shelf that has an unprovisioned slot where you can install the copied module configuration. 2. Complete one of these actions: • In the **Main Window**, click **Paste**. • Right-click the shelf and select **Paste**. • In the **Main Window** shelf graphic, right-click the unprovisioned slot where you want to install the copied module configuration. Select **Paste**. 3. In the dialog that opens, press Ctrl+V to paste the copied module configuration. 4. Click **Continue**. 5. In the **Paste Module** dialog, select **Target Shelf Number** and **Target Slot Number**. You can select only an unprovisioned slot to install the copied module configuration. 6. Click **Continue**. 7. If needed, specify the network-port channel number of the channel module. 8. Click **Continue**. 9. In the **Copy&Paste** dialog, click **Yes**.

To paste the module to a shelf in a different node:	1. Open a new browser tab or window. 2. Log in to the destination node. 3. Click **Configure**. 4. In the **Navigation Tree**, select a shelf that has an unprovisioned slot where you can install the copied module configuration. 5. Complete one of these actions: • In the **Main Window**, click **Paste**. • Right-click the shelf and select **Paste**. • In the **Main Window** shelf graphic, right-click the unprovisioned slot where you want to install the copied module configuration. Select **Paste**. 6. In the window that opens, press Ctrl+V to paste the copied module configuration. 7. Click **Continue**. 8. In the **Paste Module** window, select **Target Shelf Number** and **Target Slot Number**. You can select only an unprovisioned slot to install the copied module configuration. 9. Click **Continue**. 10. If needed, specify the network-port channel number of the channel module. 11. Click **Continue**. 12. In the **Copy&Paste** window, click **Yes**.

Graphical Indicators

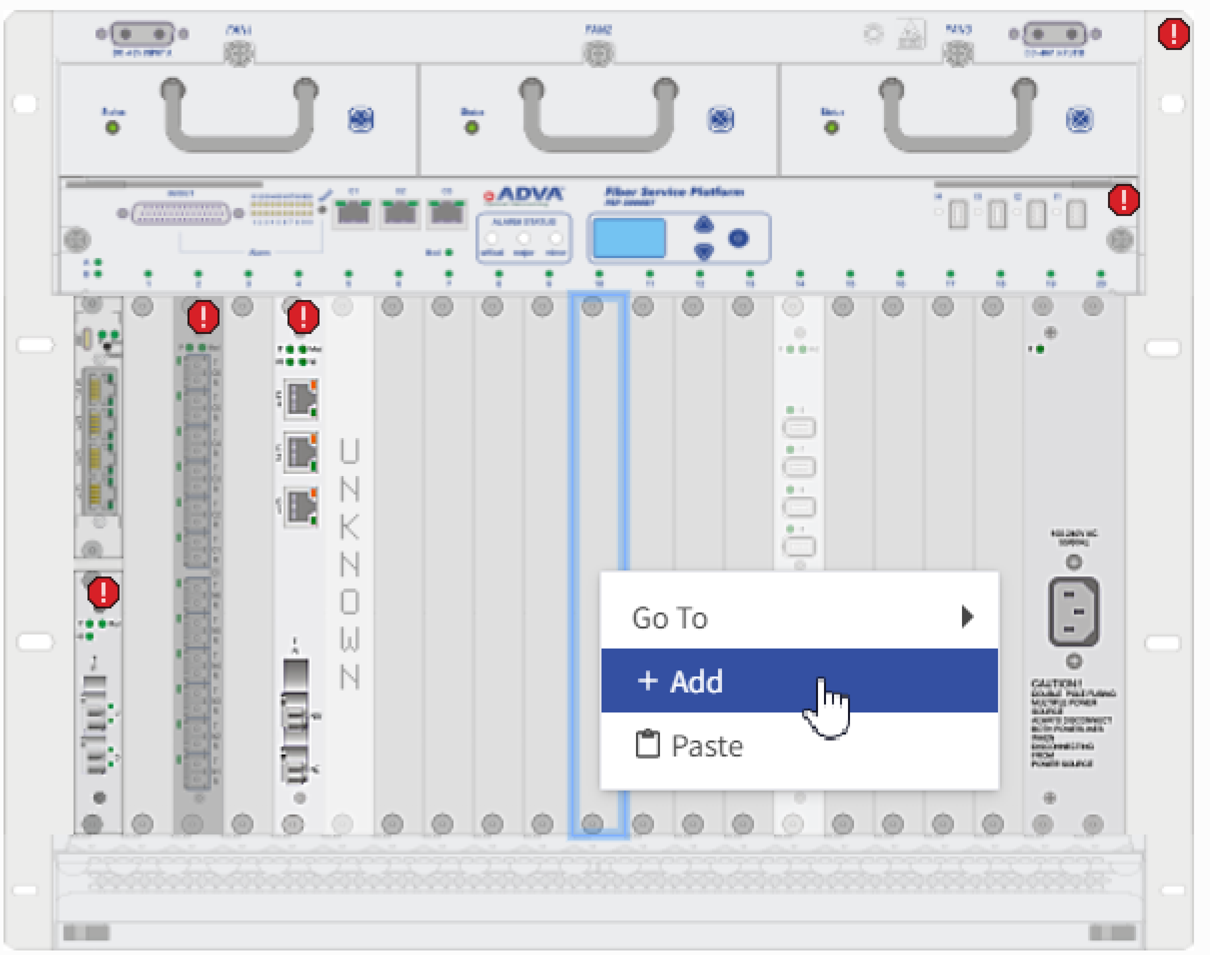
This section contains these topics:

Shelf Graphics

You can easily read an equipment installation or configuration status by color representation in the navigation tree:

Dark Gray	(Dark Gray) Equipment provisioned but not installed.
Gray	(Gray) Equipment installed and provisioned.
Light Gray	(Light Gray) Equipment installed but not provisioned.
Red	Equipment installed but does match not provisioned information (Mismatch).
Blue	Equipment installed and provisioned but in Standby.

You can also use a shelf graphic in the main pane.



Left-click:

- On the empty slot to add a module.
- On the equipment to open equipment level view.

Right-click on a shelf slot to open the context menu. In the context menu you can:

- Navigate to:
  - Alarm
  - Monitor

  - Maintain
- Add a module
- Copy or paste module provision settings
- Delete a module

Alarm icon over equipment shows the highest severity alarm reported by the equipment.

Module Graphics

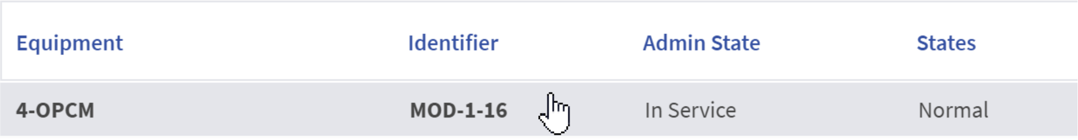
The main pane shows the front plate graphic of the selected module.

Navigation Tree

Normal text	Equipment provisioned but not installed.	Slot 7 4TCA-PCN-4GU+4G
Bold text	Equipment installed and provisioned.	Slot B **SCU**
Light text	(Light text) Equipment installed but not provisioned.	Slot 5 EDFA-DCGV (EDFA-DCGV)
Red text	Equipment installed but does not match provisioned information (Mismatch).	Slot 10 4ROADM-C96

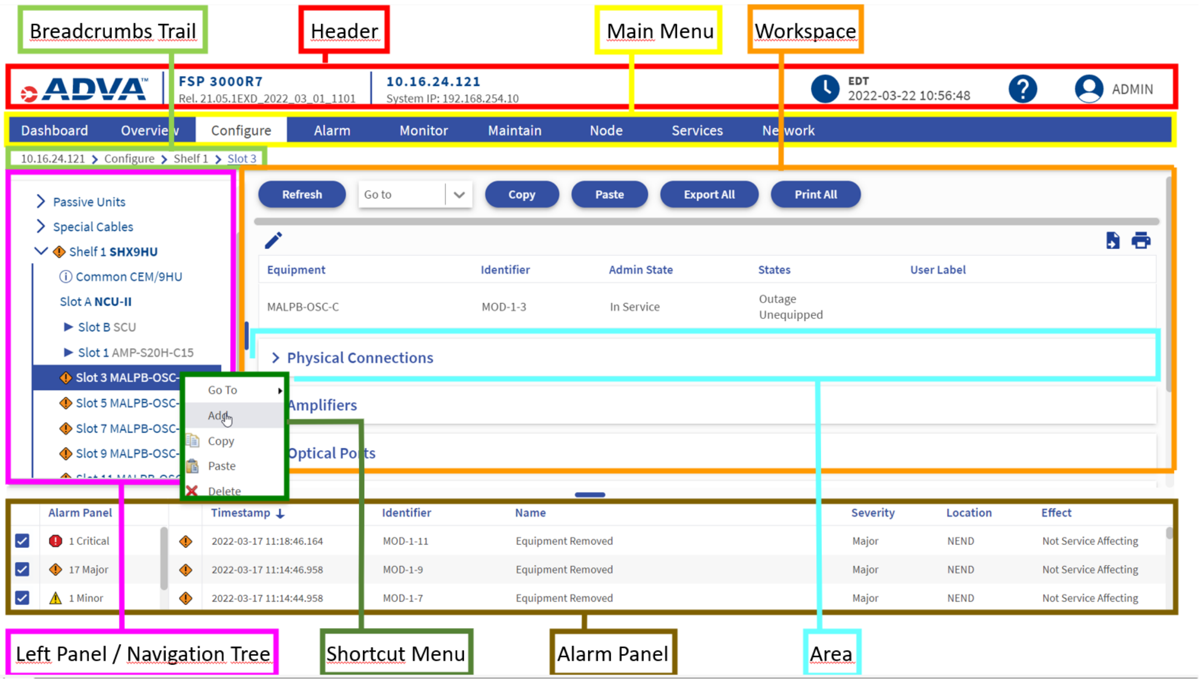
Highlighted Rows

Click a highlighted row to access all associated information.



Equipment	Identifier	Admin State	States
4-OPCM	**MOD-1-16**	In Service	Normal

Interface Description



Equipment	Identifier	Admin State	States	User Label
MALPB-OSC-C	MOD-1-3	In Service	Outage Unequipped	

Timestamp	Identifier	Name	Severity	Location	Effect
2022-03-17 11:18:46.164	MOD-1-11	Equipment Removed	Major	NEND	Not Service Affecting
2022-03-17 11:14:46.958	MOD-1-9	Equipment Removed	Major	NEND	Not Service Affecting
2022-03-17 11:14:44.958	MOD-1-7	Equipment Removed	Major	NEND	Not Service Affecting

Customizing the Dashboard

To customize the **Dashboard**, you can add, change, or remove tiles. Each tile provides an information overview related to a selected topic. To customize the **Dashboard** panel, click the settings icon to enter dashboard edit mode.

Table 1: Dashboard Edit Mode Actions

Action	Description
Change tile	On the top of the tile, from the tile type menu, select the tile type.
Move tile	Select the center of the tile and drag to place it in another position.
Resize tile	Select the bottom right corner of the tile and drag it to resize it.
Delete tile	On the top right of the tile, click the delete icon.
Add tile	On the top right of the **Dashboard** area, click the add tile icon, and then select the tile type.
Change layout	On the top right of the **Dashboard** area, click one of these: • 3 Column Layout icon. • 2 Column Layout icon.
Save layout	On the top right of the **Dashboard** area, click the save icon.
Cancel actions	On the top right of the **Dashboard** area, click the cancel icon.

Table 2: Tile Type

Tile Type	Data
Users	• Active Users • Active Sessions • Locked Users • Last Login • Last Failed Login

Table 2: Tile Type

Tile Type	Data
Equipment	• Mismatched • Removed • Faults • Disabled • Maintenance • Management • Installed • Unconnected Ports
Health Check	• NCU Uptime • Longest Working Amplifier in Node • Highest Temperature in Node • NCU Memory Usage
Power Consumption	• Node Power Consumption
Traffic Ports	• Loopback • Force Operation • Disabled • Maintenance • Management • Auto In Service • Unassigned
Temperature	• Highest Temperature in Node
Encryption	• FWP Encryption Update • Disabled • Bypass Allowed • Key Exchange Failures • Missing Session Key • Authentication Password Required/Missing
Software	• Active Software Release • Standby Software Release • Modules Not At Release

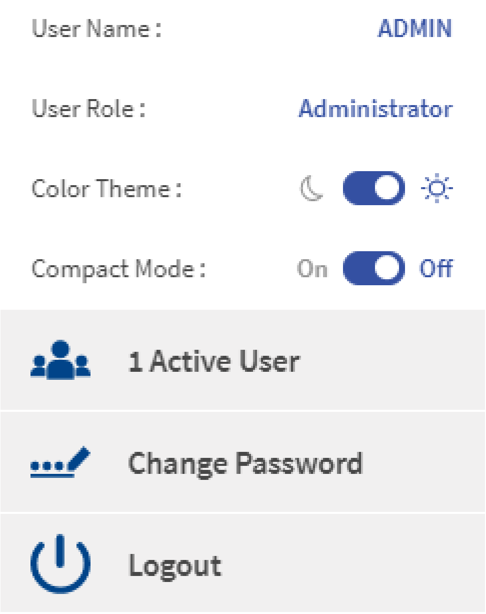
Table 2: Tile Type

Tile Type	Data
Amplifier Operation	• Identifier • Equipment • Admin State • Gain [dB] • Tilt [dB] • Operation [h]
Recent Alarms	• Name • Identifier • Timestamp

Using the User Menu

Use the **User Menu** to access color theme, compact mode and password change settings.

Click the user icon to access the menu.



User Name : ADMIN

User Role : Administrator

Color Theme : ☾ ● ☼

Compact Mode : On ● Off

Using NED Applications

This section contains these topics:

Overview

Use the **Overview** application to access shortcuts to important elements of the NED interface. When you use these shortcuts, you can configure equipment-related system settings. These settings are mainly service-related and extend beyond than a single shelf or module.

Select **Overview** to access these shortcuts.

Shortcut	Description
Inventory	View the installed equipment.
Physical Connections	View and enter connections, generally fibers, between equipment.
Span Equalization	Control amplifier gain for network fiber spans.
Channel Groups	View information about channels provisioned on configurable filters.
Equipment Protection	Display redundant controller information.
Management Network	View and configure IP networking functions.
Diagnositcs	Store and export optical reference data. View Resource Analyzer results for a selected path.

Select **Node** > **Controls** to enable the control plane and Ethernet CFM.

Configure

Select **Configure** to add and edit:

- Optical lines
- External channels
- Passive units
- Special cables
- Shelves
- Modules

Within each of these items you might find additional node elements that you can configure, such as ports and channels. Configuration areas display in the order you should use to complete them, from top to bottom.

The **Graphical View** displays the equipment state with different icons. Icons correspond with the three alarm types:

Icon	Alarm
⚠	Minor alarm
◆	Major alarm
🛑	Critical alarm

After you select a table row in the **Main Pane**, the **Configure Details** window for an equipment or entity item displays the related configuration details.

Alarm

Select **Alarm** to display active or previous alarms. Alarms display with this information:

- The item identifier.
- Time of occurrence.
- The severity.
- Its location.
- Its effect, either Service Affecting or Not Service Affecting.
- An icon that represents the severity. The severity icons are:

ⓘ	Information
⚠	Minor
🔶	Major
🛑	Critical

To filter and sort alarms: In the **Navigation Tree**, select the equipment or area.

- To view alarms that are not reported, select **Include Not Reported**.
- To filter information, in the **Search** field enter an applicable string. Use the pipe symbol (|) to filter for multiple strings.For example, to view all critical and major alarms, in the **Search** field enter: critical|major.
- In the calendar fields, select dates to filter the date range.
- Click a column header to sort the list.

To edit the severity of an alarm or event, in the **Main Pane**, right-click an entry in the list, and then select **Set <alarm name> on <equipment identifier>**.

To navigate to other applications, in the **Main Pane**, right-click an entry and select **Go To**.

To change the severity levels for future occurrences to an item, select **Configure Details** > **Configure**. Or, to change the severity levels for all items of a type, select **Node** > **Profiles** > **Alarm**.

Monitor

Use the **Monitor** application to view performance monitoring information and associated thresholds. Below the area, click **Edit** to change thresholds. To display performance monitoring data and manage thresholds, select **Monitor**.

In the **Navigation Tree**, click an item to select equipment.

Tab	Description
Current	Displays the most recent performance monitoring data.

Tab	Description
History	Displays historical performance monitoring data.
Chart	Displays historical performance monitoring data in a graphical view.
Reference	Shows snapshots of the physical performance monitoring data based on your requests.
Clear Counters	Resets the data-layer performance-monitoring error counters.

Invalid performance monitoring data displays in light gray. An asterisk * indicates a measurement interruption for all or part of the monitoring period. A loss of signal can cause measurement interruptions. A value of –99 indicates that the monitoring process recorded no valid values during the monitoring period.

Maintain

Use the **Maintain** application to view equipment maintenance operations.

Select **Maintain** to access functions such as loopbacks, protection switching, and equalization.

Node

Use the **Node** application to access system-level information.Select **Node** to access or specify this information:

Item	Description
General	Node information, functionality controls, default, date and time information, and SNMP access.
Database	View, backup and restore database.
Software	View, transfer and activate NCU and modules, and active and standby software.
File Storage	View and manage files for the Active NCU RAM, Active NCU permanent memory, and SCU.
Security	Control node access rights. Configure RADIUS or TACACS+.

Item	Description
Security Applications	Configure SSL/TLS, SSH, authentication settings, GNMI and QKD.
Users	Add, delete, change password, and specify other user settings. Access the NED Messenger, user chat interface.
Logs	View, export, and print logs. To store logs, click column headers.
Profiles	View, import, and export profiles.
Tools	Collecting data for technical support analysis, pinging an IP address, performing traceroute.

Some configuration details in the **Node** application affect the operation of modules within the node.

Services

Use the **Services** application to configure the node equipment path to carry data. In **Services**, you can create these bi-directional service segment types:

- **Passthrough Optical Channels**: Optical Line (OL) to Optical Line.
- **Add-Drop Optical Channels**: Channel module network port to an Optical Line.
- **Client Service**: Channel module client port to an Optical Line.

Network

You can access other nodes in the **Network** application, either directly or by gateway access. Select **Network** to access other nodes in the network.

- In the **Direct Access** column, click a link to access a node.
- In the **Gateway Access** column, click a link to access a node through a proxy server.

Using the Navigation Tree

The contents of the **Navigation Tree** depend on the application that you select. In most applications, the **Navigation Tree** is a nested view of shelves, modules, optical lines, and external channels that your node connects to. The **Overview** and **Node** applications display a list of items that you can view or configure.

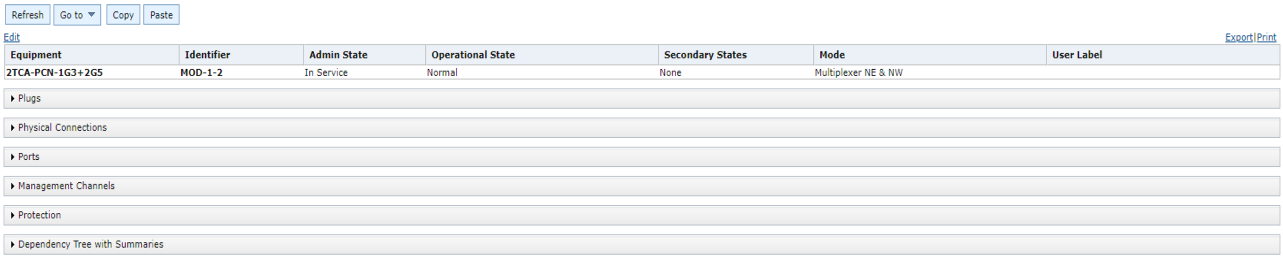
In the **Navigation Tree**, click an item to display its related information in the **Main Pane**.

The Main Pane

The **Main Window** displays information about items that you select in the **Navigation Tree**. In the **Main Window**, you can configure or view information about the selected item. Click highlighted lines to reveal more information. Right-click items to open shortcut menus.

Areas

In the **Main Pane**, you can view information about areas as a group. Complex views can contain many areas. Simplified views display information about only one area.

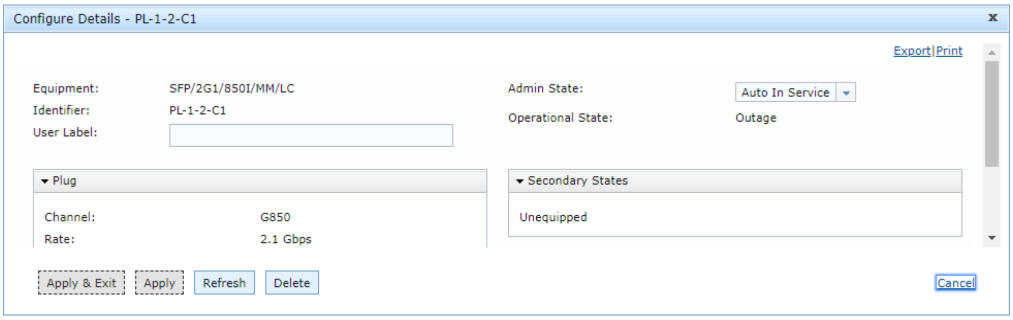


Equipment	Identifier	Admin State	Operational State	Secondary States	Mode	User Label
2TCA-PCN-1G3+2G5	MOD-1-2	In Service	Normal	None	Multiplexer NE & NW	

Click an area to display its rows of items. Click a highlighted row to access all of the information associated with the item.

The Configure Details Window

To open the **Configure Details** window, click a row that contains the summary information for an entity.


Configure Details - PL-1-2-C1

Equipment: SFP/2G1/850I/MM/LC
Identifier: PL-1-2-C1
User Label:
Admin State: Auto In Service
Operational State: Outage

Plug
Channel: G850
Rate: 2.1 Gbps

Secondary States
Unequipped

The **Configure**, **Node**, and **Overview** applications include **Configure Details** windows.

In the **Configure Details** window, you can export all displayed information. For example, you can export detailed configuration information about PKI, license management, or the management network.

The Alarm Panel

The **Alarm Panel** displays system alarms.

- To filter alarms, select or clear the alarm fields.
- To sort alarms, click the column headers.

Using the NED Buttons

Button	Click to
Apply	Save changes. If you do not click **Apply**, after you navigate away from the current window you will lose any changes you made.
Apply & Exit	Save changes and exit a window.
Cancel	Exit a window saving any configuration changes.
Delete	Delete the current equipment.
Refresh	Update the displayed information.
Export	Download the area contents in CSV format. The file uses tabs to separate the information.
Print	Print the area contents.
Alarm Cutoff	Deactivate the telemetry interface outputs. The outputs normally connect to equipment that alerts operators. Alarms raised on the node activate the telemetry interface outputs.

Identifiers

Identifiers represent the locations of items within a node and are unique to the node. Identifiers are the same as TL1 Access Identifiers (AIDs) for equipment or entities.

> In the examples that follow, you might not use the fields on the right. For example, in Item-Line-Channel, Optical Lines includes only Item and Line.

Item-Line-Channel	
OL-1	Optical Line
WCH-1-19600	Optical Channel

Item-Shelf-Slot -Port-Channel

SHELF-1	Shelf
MOD-20-4	Module
OM-15-17-N	Port
VCH-9-8-N-19600	Channel

Item-Shelf-Slot-Port-Passive Unit Port	
PSH-1-FCU-I1	Passive unit
ECH-1-FCU-I1-C2	External channel

Item-Shelf-Port	
OM-2-N	The ROADM-C40/40/OPM ports do not use the slot field.

Item-Shelf	
FCU-1	The item field identifies the common slot (FCU).

Item-Shelf-Slot-Port	
VCH-20-14-N1	The port field identities the port and channel for optical channels on some ROADM types.

Item-Shelf-Slot-Port	
GCC0-12-13-NE	The item field identifies the management channel.
ECH-4-3-C4	The item field identifies the external channel.

Workflow

To access additional information about each item, below the open areas click the highlighted rows. Follow these basic steps to work in NED:

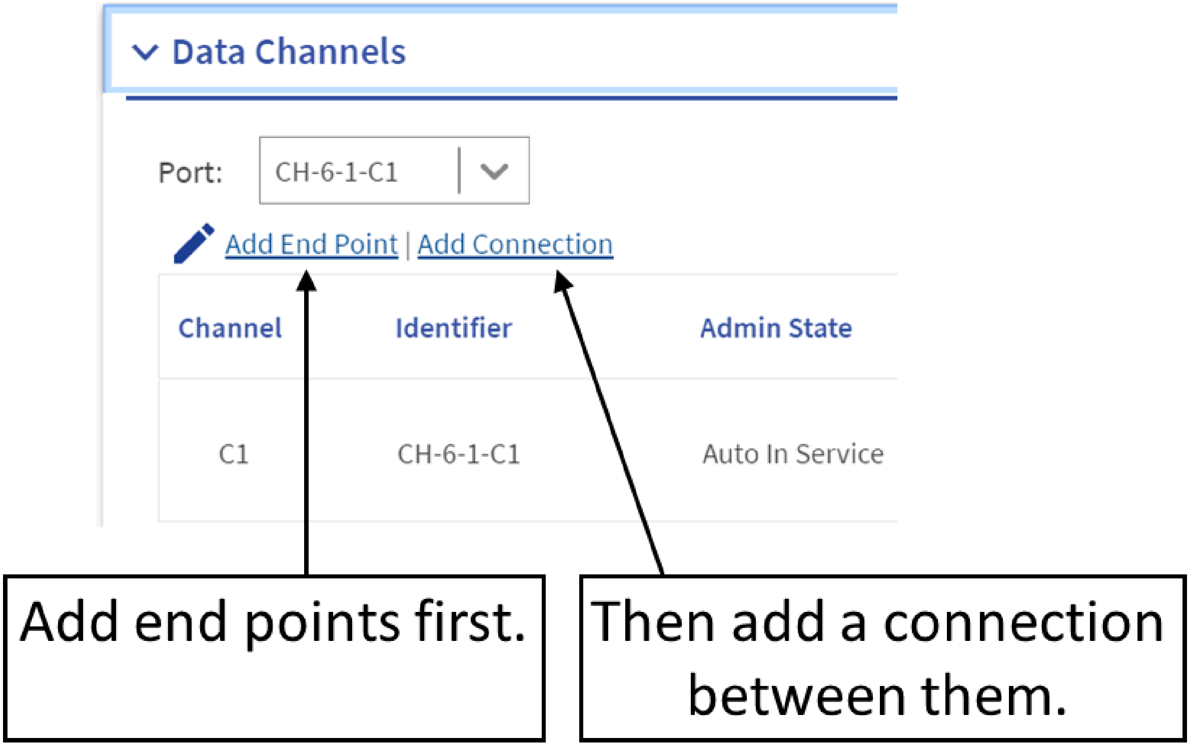
1. Select an application, and then in the **Navigation Tree** select an item.

2. In the **Details View**, click items to see more information.
   –or–
   Click **Edit** to configure items.
3. After you make any changes, click **Apply** to update these settings on the node.

> To browse to previous windows that you opened, only use the **Navigation Path**. Do not use the browser back or forward controls or the navigation history.

When you configure equipment in NED, select areas, and progress from top to bottom. Areas contain links to configuration tasks like to edit or add items.

If you need to perform more than one Add function on a area, work from left to right. For example, when you add data channels on a 5TCE-PCTN-10GU+AE module, first add two end points, and then add an interconnection.



Port: CH-6-1-C1

Channel	Identifier	Admin State
C1	CH-6-1-C1	Auto In Service

Add end points first.

Then add a connection between them.

Performing Basic NED Tasks

Task	Description
Add a shelf or unit.	1. Select **Configure**. 2. In the **Navigation Tree**, right-click **Node**, and then select **Add**. –or– In the **Main Pane** select **Add Shelf/Unit**. 3. Select options to configure the shelf, and then click **Add**.
Add an optical line.	1. Select **Configure**. 2. In the **Navigation Tree**, right-click **Optical Lines**, and then select **Add** –or– In the **Main Pane** select **Add Optical Line**. 3. Select options to configure the optical line, and then click **Add**.
Add external channels.	Adding External Channel for CSM and 4-OPCM: 1. Select **Configure** > **External Channels**. 2. In the **External Channels** area, click **Add**. 3. In the **Add External Channel** window, select options to configure the external channel, and then click **Add**. Adding External Channels in Optical Multiplex for CCM-C96/9 and 8PSM modules: 1. Select **Configure** > **External Channels**. 2. In the **External Channels in Optical Multiplex** area, click **Add**. 3. In the **Add External Channel** window, select options to configure the external channel, and then click **Add**.
Add passive units.	1. Select **Configure**. 2. In the **Navigation Tree**, right-click **Passive Units**. –or– In the **Main Pane**, click **Add Unit**. 3. Select options to configure the passive unit, and then click **Add**.

Task	Description
Add modules	1. Select **Configure**. 2. Right-click a shelf, and then select **Add**. 3. Configure options according to your network plan, and then click **Add**. When you search by name, you can type any portion of the equipment name into the **Equipment** field. The software can search based on that text.
Restart the NCU	1. Select **Overview**. 2. Select **Management Network**. 3. Click **NCU Restart**. 4. In the **Confirm NCU Restart** window, click **Restart**.

What's New

22.2

- Updated Provisioning Node Security section.
- Updated Configuring Certificate Authorities section.
- Updated Configuring a Pre-operational Self-Tests section.
- Updated Configuring an Audit Events section.
- Updated Setting the Node Parameters section.
- Updated Configuring TLS Mutual Authentication section.

22.1

- New Provisioning the Management Network - Background Information section.
- New Redundant Controllers section.
- New Management section.
- Deleted WCA-PCN-2G5U.
- Deleted 10WXC-PCN-10G.
- Updated Viewing Performance Monitoring Information section.
- Updated Securing the Node section.
- Updated Shelf Graphics section.
- New Retrieving Tributary Ports and Slots Information section.
- Updated Configuring the Transport Layer Security Protocol section.
- Updated Configuring the Secure Socket Shell Protocol section.
- New Configuring an NTP Server Authentication section.
- New Configuring a Pre-operational Self-Tests section.
- New Configuring an Audit Events section.
- Updated Using Licenses section.
- New Configuring TLS Mutual Authentication section.
- Updated Management Network Limitations section.
- Updated Configuring Cryptographic Keys section.

21.5

- New T-MP-M8DCT teraflex module.
- New Using NCU Management LAN and Links section.
- New Customizing the dashboard section.
- New ECDSA key type.
- New Securing a HD Management Connection section.
- New Manually Assigning Logical Interfaces to Optical Lines section.
- New Using Smartcards section.
- New Transferring FWPs of HD Modules section.
- New Automatic FWP Download to NCU Test feature.

21.2

- NED supports new accessibility and shortcut dashboard options.
- **Node** supports NCU Uptime.
- **Node** supports a warning message in case that a password change is required for SNMP Authentication Protocol.
- Revised the legal page for the PDF versions

21.1

- NED supports new dashboard.
- **Node** supports Security and Security Applications.
- **Monitor** supports input power for nodes and shelves.
- **Overview** supports local and remote Inventory.

20.3

- **Overview** supports new columns in Port Summary.

20.2

20.1

- NED supports interface update for alignment to other products.
- **Overview** supports IS-IS for Management Network.
- **Overview** supports cross connect summary for ROADMs.
- **Configure** supports OPPM support of revertive switching.
- **Configure** supports password change for HD shelves.
- **Configure** supports exporting of all module parameters and settings at once.
- **Node** supports port User Label for SysLog.

19.3

- **Configure** supports improved track channel visualization (Node Channel Trace), allowing to show derived power levels on a path through a node.
- **Node** supports node management approved IP addresses for IPv6.
- **Node** supports gRPC Network Management Interface.
- **Node** supports automatic download of FWP during software update.
- **Node** supports software signature validation for packages sent to the **Standby Software Release** area.

19.2

- NED supports a visual indicator of a fan fail alarm.
- Guided Fiber Installation supports F8 Module Port LEDs.
- **Overview** supports DHCPv6 client support for Zero Touch Provisioning including DHCP relay agent.
- **Configure** supports user label for each PTP connection.
- **Node** supports Module Authentication.
- **Node** supports Network Intelligence instead of Control Plane on NCU-III.

19.1

- NED supports direct access to Guided Equipment Installation, Guided Fiber Installation and the Channels Overview from the login view.
- NED supports an improved shelf adding process.
- NED supports HTTP Strict Transport Security (HSTS).
- Maximum password length was increased to 128 characters.
- **Overview** supports access to Guided Equipment Installation via the Equipment Install button.
- **Configure** supports adding passive shelves and modules.
- **Configure** displays all user labels; the Operational State and Secondary States columns were combined into one column called States.
- **Node** supports an improved download process for modules.
- **Node** supports Quantum Key Distribution.
- New plug support: QSFP28-10X10G-1310S-SM-MPO. This plug supports aggregation of ten Ethernet 10G services into a 100G service.

Overview

This section contains these topics:

Physical Connections

A number of features, including control plane, require information about the fiber and cable connections between modules.You need to enter these connections first to match your installation before you can use all the supported Node features.

> **Physical Connection** areas are associated with equipment in **Configure** that are limited to **Navigation Tree** selection. You can use these areas to display, enter, or delete physical connections for the associated equipment.

1. Select **Overview**.
2. Select **Physical Connections**.
3. Click the row for source port to enter or delete the physical connection from the port.

> You can use the **Search by all columns** field to filter the table by the text that you enter. For a more precise search, use the search syntax (Regular Expressions).

Install Guide

You can use the online **Install Guide** for assistance as you install the physical connections, or fibers. This guide graphically presents the shelf or shelves and highlights the ports that you need to connect. The Install Guide also initiates the equipment LEDsto blink green so you can identify the module or ports that you need to connect.

- Select **Next** to move to the next connection, which sets **Guided Install** to **Done** for the connection. After the software sets the Guided Install to Done, the Install Guide will not display the connection again.
  –or–
- Select **Skip** to move to the next connection without setting **Guided Install** to **Done**. You can see the connection in the **Install Guide**.

> **Install Guide** is dimmed or unavailable until the software loads all connections.

You can also select **Overview > Physical Connections** to select a single connection from the list and open the **Physical Connection - Details** window. Click **Install Guide** to open the Guided Installation window and mark the connection as done or undone, which sets this connection to **Available** in the **Install Guide**.

Installing Equipment

The Guided Module Installation (GMI) assists you to insert equipment in its proper location. Use GMI on one piece of equipment at a time. The installation requires you to first provision the equipment and install and connect the shelves to the master shelf. If you request this information, GMI will graphically in Network Element Directorindicate the equipment you need to install and shows you its location with a blinking LED where possible. GMI .

GMI access is not active when all equipment is correctly installed.

You can go to **Overview > Inventory** and click **Equipment Install** to identify the missing equipment and send a blink LED command to CEM for the first identified missing equipment.

Selecting **Refresh** identifies all the the missing equipment again and sends a blink LED command to CEM for the first identified missing equipment.

Selecting **Next Shelf** identifies the next shelf with missing equipment, updates the view to that shelf and sends blink command to the selected equipment.

Selecting **Close** sends stop blink command and closes the view.

Using Span Equalization

Span equalization automates the gain provisioning of variable gain amplifiers used as pre-amplifiers, boosters, and line-amplifiers between network elements.

This section contains these topics:

Span Equalization Requirements

Span equalization requires these conditions to operate in a network:

- You must enable an optical supervisory channel (OSC) on all spans between the nodes.
- You must enter all fiber connections to the amplifier modules and ROADM devices in **Physical Connections**. For more information about entering physical connections, see Adding Physical Connections.
- You must associate a booster amplifier with every transmit network interface.

Span Equalization Options

The **Span Equalization** operation options are:

- **Disable**: You must manually provision gain settings for all amplifier modules in the network.

> If you set **Span Operation** to **Disable**, all related amplifier modules Power Per Channel (PPC) and setpoint values reset to their default values.

- **Evaluate**: The first step to enable span equalization is for the NCU to verify the **Physical Connections** to determine which amplifier modules qualify for span equalization. The software makes no changes to the gain settings in this mode.
- **Existing Gain**: **Span Equalization** adopts the current gain settings for all qualified amplifier modules, calculates the values of the control parameters based on the gain settings of the qualified amplifier modules, and stores those values. While operating in **Existing Gain** mode, **Span Equalization** recalculates only the gain of pre-amplifier or line-amplifier modules after the software detects an LOS clear transition, or after you send an explicit request sent by clicking the **Start** button. You can use **Existing Gain** primarily in existing, or *brownfield*, networks.

If **Span Operation** is **Existing Gain**, you can trigger a gain calculation at any time:

- In the **Configuration** area, select an **Optical Line**.
- In the **Optical Line** row, click **Start**.

- **Auto Gain**: **Span Equalization** calculates and sets the initial gain for the qualified amplifier modules after an LOS clears. **Span Equalization** calculates only the gain for pre-amplifier or line-amplifier modules when the LOS clears, or after you send an explicit request by clicking the **Start** button. You can use **Auto Gain** primarily in new, or *greenfield*, networks.
- **Dynamic Gain Adjust**: This option applies when the **Span Operation** is either **Auto Gain** or **Existing Gain**. After you enable **Dynamic Gain Adjust**, the NCU computes a new gain value for pre-amplifier and line-amplifier modules every two seconds to compensate for span loss changes. When needed, the process makes the gain adjustments slowly, in small increments. Therefore, fast transitions in span loss require multiple seconds to complete compensation.
- **Amplifier Auto Shutdown:** You can setBooster Amplifier Automatic Power Shutdown (APS) to operationally disable the amplifiers in both directions when the system detects a fiber break between the two nodes.

Span Equalization Limitations

These are the limitations:

- Span Equalization is enabled at the node level meaning all amps at that node are enabled for Span Equalization to operate.
- Span Equalization requires a booster amp out each degree of a node.
- Span Equalization requires that all nodes in the network have Span Equalization enabled to work at all. In other words, it is a system wide feature.
- Dynamic Span Equalization only adjusts the gain of EDFAs configured as an in-line amplifier or pre-amplifier because they terminate a span.
- Dynamic Span Equalization does not adjust any Ramans or any EDFAs configured as booster amplifiers.
- Dynamic Span Equalization will attempt to increase the gain of an in-line amplifier or pre-amplifier if the span loss increases over time.
    - If the gain of the in-line amplifier or pre-amplifier is maxed out, there is no additional gain available and an alarm will be raised (Gain out of Range).

  - Network designs expecting Dynamic Span Equalization to work must allow some gain range for Dynamic Span Equalization to use to compensate for additional span loss.

Changing the IP addressing scheme of an active network is service-affecting.

- Span equalization does not operate when the optical supervisory channel (OSC) messaging between nodes is disrupted.
- Therefore, any change in the IP addressing scheme of an active network requires topology detection to be rerun successfully before span equalization can resume normal functioning.

Using automatic span equalization to set the average power-per-channel (APPC) at the output of amplifiers in a multi-span network may be subject to errors. These potential errors should be accommodated in the network design.

In general, the accuracy of the APPC setting at each amplifier depends on potential errors in the APPC setting of the upstream amplifier, potential errors in span loss measurement, and the gain setting at the current amplifier.

- Small errors in the measurement of DWDM transmit and receive power levels at each amplifier (<0.3 dB).
- Small errors in the gain setting (<0.3 dB) accumulate as the number of line-amplifier nodes between consecutive ROADM nodes increases.
- An APPC error is typically highest for systems commissioned with a single DWDM channel due to the higher errors in the gain setting and power measurement at the lower total power level represented by a single channel.
- The errors decrease as the number of channels increases due to automatic span equalization automatically recalculating the span loss and resetting the amplifier gain levels.
- With three or more channels, typical errors in APPC on networks with up to five spans between consecutive ROADM nodes could reach 1.5 dB, typically trending towards a lower power setting.
- The errors are reset at each ROADM node to within 1 dB of the desired power-per-channel (PPC) value.
- By contrast, manually setting the APPC (which requires on-site presence and an optical spectrum analyzer) can also be affected by errors which cannot be quantified.

These amplifiers support span equalization:

- EDFA-C-S20-GCB-DM (this is a fixed gain booster but is supported)
- EDFA-C-D20-VGC-DM
- EDFA-C-D20-VLGC-DM
- EDFA-C-S26-VGC-DM (1510 Osc)

- EDFA-C-S26-VGCB-DM (1528 Osc)
- Raman-C10 (followed by EDFA)
- AMP-S20H-C15
- AMP-S20L-C15
- EDFA-S20H
- EDFA-S20L
- 2EDFA-S20L-S10L
- Embedded 9ROADM EDFA
- MAP-OSC-C96
- MAPB-OSC-C96
- MALPB-OSC-C
- MTP-OSC-C
- MTPB-OSC-C

Span Equalization does not support:

- Spans protected with VSM or RSM modules
- Spans using EDFA-DGC modules

You must ensure the setpoint for all booster amplifiers matches the measured channel power at the input to each booster amplifier on fixed optical add-drop multiplexer (OADM) nodes.

Span Equalization may raise an alarm against the next amplifier when Raman amplifiers are used and the desired PPC cannot be achieved. The next amplifier may be in a ROADM module or the next node.

Span Equalization does not include Raman amplifiers in Dynamic Span Equalization. Dynamic span equalization only adjusts the gain of the amplifier following the Raman amplifier to compensate for span loss changes.

Span Equalization requires communication between nodes using OSC. Changing the IP information on a node can prevent this communication. **Topology Detection** on the optical supervisory channel module (OSCM) must be performed to re-establish the communication between the nodes. This enables span equalization to resume operation.

The average power-per-channel (APPC) accuracy is limited by the amplifier gain and span loss measurement accuracy.The accuracy of APPC at each amplifier includes any measurement errors in the upstream APPC. The measurement errors accumulate as the number of amplifiers between ROADM nodes increase. ROADM modules reset the APPC accuracy to within 1 dB. An APPC error is typically highest for systems commissioned with a single channel, the APPC becomes more accurate as the number of channels increases. The network design should accommodate these measurement errors.

> When **Far End Status > Gain Control** is **Disable**, the node on the other end of the span has **Span Operation** set to either **Evaluate** or **Disable**, so span equalization messages are not sent.

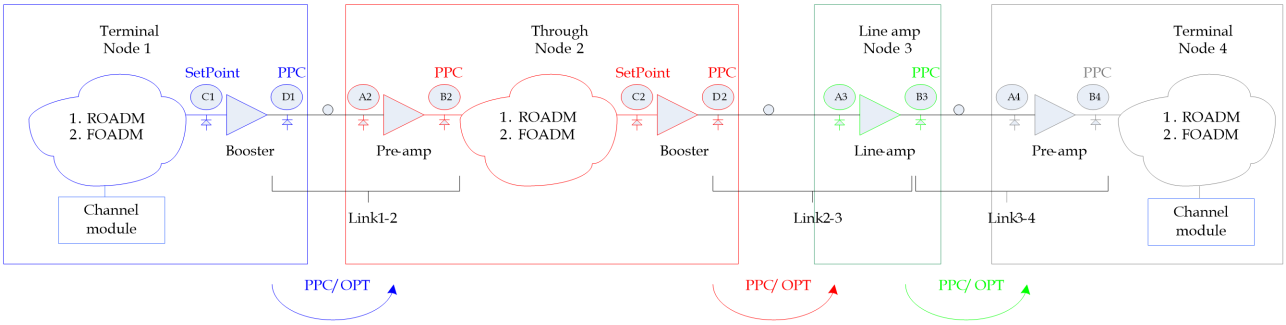
Example Configurations

The next two sections describe the provisioning steps required to operate span equalization on two sample linear networks.

New Network

This example demonstrates a greenfield, four-node linear network.

Figure 1: Span Equalization Linear Network Example: New Network



This example assumes these conditions:

- The network is a new, or greenfield, equipment installation, and the installation process is completed, including all fibers and cables.
- All equipment has been added and is operational (**Admin States** set to **In-service**, **Automatic In-Service**, **Management** or **Maintenance**).
- All fiber connections have been added in **Physical Connections**.
- Nodes are connected using an optical supervisory channel (OSC) which is operational, without alarms.
- All amplifier ports have been added and are operational.
- A channel module N port has been added and is operational.
- If applicable, the channel module **Auto Laser Shutdown** must be set to disabled, and **Error Forwarding Mode** must not be set to **Laser Off**.

- If applicable, all ROADM ports to be used have been added and are operational. A connection (cross-connection) for the channel has been added through the ROADM module(s).

For this example, the goal is to establish a service from Node 1 to Node 4.

1. Trigger the amplifier qualification process on all nodes. On Node 1:
2. Select **Overview**.
3. Select **Span Equalization**.
4. Set **Span Operation** to **Evaluate**.
5. Click **Apply**.

   Repeat these steps for Nodes 2 through 4.

   The NCU determines the amplifier modules that qualify for adoption by span equalization, and the list of qualified amplifier modules appears in the **Configuration** area under **Span Equalization** for each node.

> Span equalization requires that you set **Span Operation** to **Evaluate** before additional span operation options become accessible.

6. Verify at each node that all booster amplifiers, line amplifiers, and pre-amplifiers qualify for span equalization and appear in the **Configuration** area under **Span Equalization**.

   If an amplifier module that should qualify for span equalization does not appear in the list, the most likely reason is a missing or incorrect connection in the **Physical Connections**. SeeAdding Physical Connections for more information about entering physical connections.
7. If required by your network plan, select the Node 1 booster amplifier in **Span Equalization Configuration** area and change the default setpoint and PPC in the **Configure Details** window. Repeat for each amplifier module on each node, as required.
8. To enable span equalization on all nodes, perform these actions:
   a. For Node 1, click **Span Equalization > Span Operation > Auto Gain**.
   b. Click **Apply** to enter your selections.

      Repeat this step for Nodes 2 through 4.

      The network is now ready for first channel provisioning and span equalization amplifier module gain setting.

> When **Span Equalization> Amplifier Auto Shutdown** is set to **Enable**, booster amplifiers connected to the span are operationally disabled when a fiber break is detected between the two nodes.

> The next step applies to each qualified amplifier module in the network but is not repeated in this procedure.

9. Perform this step when using span equalization with the control plane. To perform span equalization without the control plane, skip to the next step.

   Create a bi-directional tunnel between the channel module network ports in Nodes 1 and 4.

   a. The control plane performs these actions:
      - establishes the necessary cross-connections in the Node 1 ROADM
      - equalizes the channel power level to the setpoint value
      - **Span Equalization** sets the booster amplifier gain
      - valid span equalization messages are sent to Node 2 pre-amplifier

   b. After 6 to 8 seconds, **Span Equalization** sets the gain of the Node 2 pre-amplifier module.

   c. The control plane establishes the necessary cross-connections in the Node 2 ROADM module and equalizes the channel power to the setpoint value. **Span Equalization** sets the booster amplifier gain and sends valid messages to the Node 3 line-amplifier module.

   d. After 6 to 8 seconds, **Span Equalization** sets the gain of the Node 3 line amplifier and sends valid messages to the Node 4 pre-amplifier module.

   e. After 6 to 8 seconds, **Span Equalization** sets the gain of the Node 4 pre-amplifier.

> The 6-8 second delay for **Span Equalization** to set the gain of pre-amplifiers and line-amplifiers only occurs during the provisioning of the first channel across a span. These delays do not occur when adding additional tunnels.
>
> This procedure references the configuration process for Node 1 to Node 4, however the process then proceeds in the reverse direction.

> Perform the next steps when provisioning span equalization without using the control plane. If you are not using the control plane, you must manually establish cross-connections at each ROADM module at each node—in the particular order described.

10. Establish the necessary cross-connections in the Node 1 ROADM modules, the channel power is automatically adjusted to the setpoint value.

    Span Equalization sets the booster amplifier gain and sends valid PPC messages to the Node 2 pre-amplifier module.

    After 6 to 8 seconds, **Span Equalization** sets the gain of the Node 2 pre-amplifier.
11. Establish the necessary cross-connections in the Node 2 ROADM modules, the channel power is automatically adjusted to the setpoint value.

    Span Equalization sets the booster amplifier module gain and sends valid messages to the Node 3 line-amplifier.

    After 6 to 8 seconds, **Span Equalization** sets the gain of the Node 3 line amplifier and sends valid messages to the Node 4 pre-amplifier.

    After 6 to 8 seconds, **Span Equalization** sets the gain of the Node 4 pre-amplifier.
12. Establish the appropriate cross-connections in the Node 4 ROADM module.

    The Node 4 channel module receives the appropriate receive power level for proper operation.
13. Repeat steps 6 through 8 in the reverse order.

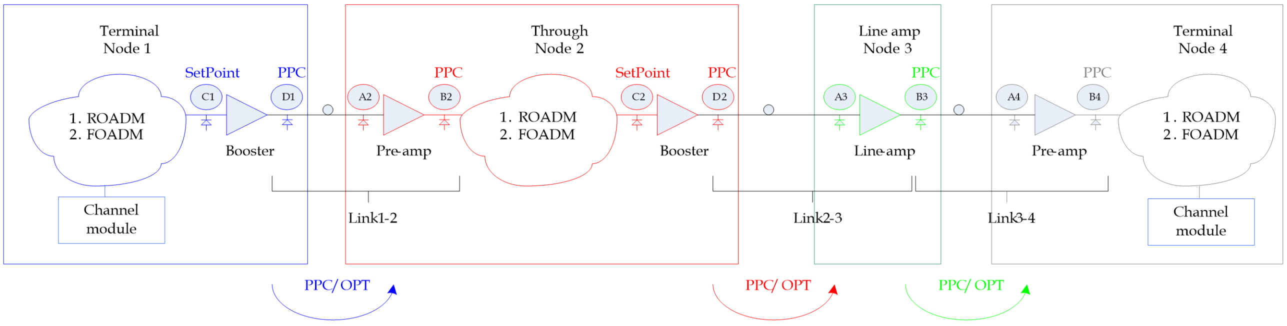
> After an amplifier module is placed in service, no further changes to the setpoint and PPC values are allowed while **Span Equalization** is enabled. To change the gain the amplifier, perform these actions:
>
> 1. Set **Admin State** to **Maintenance**
> 2. Change **Gain Offset**
> 3. Request **Span Equalization** to calculate the new gain.
>
> Changes should be performed at this point, if required. However, a change to **Gain Offset** could cause a disruption in the service.

Existing Network

This example demonstrates an existing, or brownfield, four-node linear network.

NOTICE	Performing this procedure could cause service interruptions in your network. This procedure should only be performed during a maintenance window.

Figure 2: Span Equalization Linear Network Example: Existing Network



This example assumes these conditions:

- The network is an existing, or brownfield, equipment with cable and fiber installation completed.
- All fiber connections have been added in **Physical Connections**.
- All qualified amplifier modules are in service and do not have a LOS.
- All ROADM are established and operational.
- Nodes are connected using an optical supervisory channel (OSC) which is operational, without alarms.

For this example, the goal is to enable **Span Equalization** for all nodes in the existing network.

	An amplifier module can be in service and not have a LOS due to excessive amplified spontaneous emission (ASE) noise at the network input with no channels present. Before selecting the **Existing Gain** option, take precautions to ensure all in-service amplifier module gain settings have been provisioned properly.

1. Trigger the amplifier qualification process on all nodes. On Node 1:
2. Select **Overview**.
3. Select **Span Equalization**.

4. Set **Span Operation** to **Evaluate**.
5. Click **Apply**.

   Repeat this action for Nodes 2 through 4.

   Each NCU determines the amplifier modules that qualify for span equalization. The qualified amplifier modules appear in the **Configuration** under **Span Equalization**.

> Span equalization requires setting **Span Operation** to **Evaluate** before additional span operation options are accessible.

6. For a ROADM node, perform this step. For a Fixed OADM or line-amplifier nodes, skip to the next step.

   After amplifier qualification process completes, perform these actions:
   a. Change the **Span Operation** to **Existing Gain**.
   b. Click **Apply** on each node to use the existing gain settings for qualified amplifier modules.

> When **Span Equalization** > **Amplifier Auto Shutdown** is set to **Enable**, Booster amplifiers connected to the span are operationally disabled in both directions when a fiber break is detected between the two nodes.

7. For a Fixed OADM or line-amplifier node, perform this step.

   Select each booster amplifier in the **Span Equalization** > **Configuration** area and enter the appropriate setpoint and PPC values in the **Configure Details** window.
   a. For all qualified booster amplifiers, connect an optical spectrum analyzer (OSA) to the amplifier output monitor port to determine the average channel power.
      For more information about using OSAs to measure optical power levels, refer to the “Measuring and Leveling of the Network Line” section of the *Installation and Commissioning Manual.*
   b. Select each qualified booster amplifier module in the **Span Equalization** > **Configuration** area. In the **Configure Details** window, enter the measured average channel power into **Power Per Channel**. The NCU then computes the required setpoint.
   c. Select each pre-amplifier or line-amplifier and enter the appropriate PPC value.

d. For all qualified pre-amplifier and line-amplifier, connect an OSA to the amplifier output monitor port to determine the average channel power.

e. Select each qualified pre-amplifier or line-amplifier module in the **Span Equalization > Configuration** area. In the **Configure Details** window, enter the measured average channel power into **Power Per Channel**.

f. In the **Span Equalization** area, set **Span Operation** to **Existing Gain**.

g. Click **Apply** on each node.

Provisioning the Management Network

This section contains these topics:

Background Information

The FSP 3000R7 Data Communications Network (DCN) carries management information, signaling, and other communication within and between network elements (NEs) and management systems in the network.

You can use the DCN for:

- Communication:
  - SNMP - Traps and Get/Set messages.
  - TL1 via telnet using port (2024).
  - Telnet/SSH.
  - HTTPS.
- File transfer:
  - Software update.
  - Database backup and restore.
  - Support data retrieval.
- Time and date synchronization using NTP.
- Inter NE communication:
  - OSPF to provide dynamic IP routing.
  - OSPF-TE and RSVP-TE to support control plane operation.

You can implement the DCN with:

- External equipment.
- Optical supervisory channels (OSC).
- Embedded communication channels (ECC).

For the DCN, you must specify:

- IP addresses.
- Default routes.
- Static routes.
- Possibly a routing protocol (OSPF).

The system supports dual IPv4/IPv6 operation.

You must configure DCN according to the plan using a local connection to each node.

> OSC connects to the NCU with management LANs. ECC conntects to NCU with management links. The node supports up to 20 management LANs and 300 management links.

This section contains these topics:

Management Network Equipment

The following module types are or may be part of the management network:

- NCU
  - Ethernet ports (C ports with RJ-45 connectors)
  - Management LANs
  - Management Links
- SCU
- OSCM
  - OSC ports (N ports)
  - Ethernet ports (C ports with RJ-45 connectors)
- OSFM
  - N port (supports OSC)
  - C port (connects to OSCM N port)
- Amplifiers
  - N port (supports OSC)
  - C port (connects to OSCM N port)

- CEM
  - Ethernet ports (C ports with RJ-45 connectors)
- UTM
  - Ethernet ports (C ports with RJ-45 connectors)
- Channel Modules
  - N ports (supporting GCC, DCC or EOC)
  - C ports (supporting GCC, DCC or EOC)

> Only a single Management Channel can be configured on a channel module port (i.e. if GCC0 is configured, then GCC1 or GCC2 on the port cannot be used.)

Ethernet ports with RJ-45 connectors support:

- 10 Mbps, 100 Mbps, or auto-negotiation
- Full or Half duplex operation
- Auto MDI/MDI-X

Management Links support:

- IPv4 over PPP technology according to IETF RFC 1332

Management LANs support:

- IP connections

Management Network Limitations

- RSTP suppots networks with up to 31 NEs.
- Ring ground switching supports networks with up to 6 NEs.
- If available bandwidth is not sufficient, you cannot provision more management LANs and links.
- To prevent any delays during unusual management network activity, change the OSPF parameters. Unusual management network activity may cause additional consumption of NCU CPU and memory.
- You cannot route high-density module GCC management traffic to other destinations.

Table 3: Management LANs and Links

NCU Family	NCU-II / NCU-II-P / NCU-S	NCU-3
Total Bandwidth Available	20000 Kbps	620000 Kbps

Table 3: **Management LANs and Links**

NCU Family	NCU-II / NCU-II-P / NCU-S	NCU-3
Total Links Available	50	300
Routes Supported	600	• 600 • 1200 (as of release 20.1.1)
Area Border Router (ABR)	3	3
Max number of NEs per OSPF area	100	100
Bandwidth used by Link	See Max Tx Rate for associated Management Channel	
Total LANs Available	4	20
Link State Advertisement (LSA)		4800
Routes read time		up to 3 minutes
Supported SCU Types	SCU, SCU-S, SCU-II	SCU-II
Backplane maximum Tx rate	20000 Kbps	80000 Kbps
Bandwidth used by LAN per Module		
• CEM9HU • OSCM-PN • UTM • MAP, MALP, MAPB, MALPB • MTP, MTPB	512 to 20000 Kbps (default 1024 Kbps)	512 to 80000 Kbps (default 1024 Kbps)
• HDSCM-PN	512 to 20000 Kbps (default 8192 Kbps)	512 to 80000 Kbps (default 40960 Kbps)

IP Addresses

IP addresses must be assigned to support management network communication including the one for the default gateway. The IP address numbering plan should take into consideration possible growth in the network especially when networks are connected without routers. Allocate dedicated IP sub-networks to each section of the management network. Other restrictions on specifying IP addresses are covered in Management Network Topologies.

The following guidelines are applicable to typical networks and allow for OSPF optimization by summarizing routes:

- All numbered IP interfaces must have unique IP addresses.
- The NE uses the IPv4 link-local address space as specified in RFC 3927 (prefix 169.254/16) internally so this address range MUST NOT be used to configure IP interfaces.
- System IP addresses
    - All System IP addresses in the network should be in their own unique subnet
    - System IP addresses may be grouped into different subnets
    - Ensure all other IP addresses are not in the System IP subnet(s)
- Management LANs
    - Configure each Management LAN in a unique subnet
    - All Ethernet ports connected to a Management LAN are in the Management LAN subnet
    - Management LANs may be configured as unnumbered IP interfaces
- Management Links
    - Configure Management Links in the network should be in their own unique subnet
    - All Management Links may be in the same subnet
    - Management Links may be grouped into different subnets
    - Management Links may be configured as unnumbered IP interfaces
- Logical Interfaces (LIF/LIF-CP)
    - Logical interfaces cannot be in the same subnet as any other IP interface of the network element
- IP Host
    - IP Hosts must be in the same subnet as the LAN (Management LAN, Management Link, System IP or Ethernet port) to which it is connected
    - IP Hosts PPP IP address should be in a different subnet than the LAN to which it is connected
    - IP Hosts loopback IP address should be in a different subnet than the LAN to which it is connected

OSPF Areas

A management network may be structured, or subdivided, into routing areas to simplify administration and optimize traffic and resource utilization. Each area maintains a separate Link State DataBase (LSDB) whose information may be summarized towards the rest of the network by the connecting router. OSPF supports network subdivision into areas. The topology of an OSPF area is not known outside of the area to reduce the traffic routing. An NE which has IP interfaces in multiple OSPF areas is known as an Area Border Router (ABR) and must always have at least 1 OSPF interface enabled .

OSPF Area types :

- Backbone - core of a network (i.e. OSPFAREA-0.0.0.0)
  - All other OSPF areas must connect to the backbone area.
  - Inter-area routing is performed by routers connected to the backbone area and associated areas.
- Normal - distributes routing information using LSAs.
- Stub - does not advertise routing information.
  - A routing metric must be configured for a stub area.
  - LSAs have a single default route used to reduce the size of LSDBs and routing tables.
  - All external destinations must be reachable through ABRs.

All routers in the same area must agree on the area type, stub or normal.

> An OSPF area should not contain more than 100 IP routers.
>
> Routers with areas configured to different types will not form an adjacency and will not exchange routing information.

ABRs use the stub routing metric to advertise a single default route into the stub area. Different routes in a stub area may be different routing metric values. ABRs can be prioritized as the primary, secondary, etc. path out of the stub area.

Stub areas have the limitations due to the restricted LSAs:

- Routers cannot redistribute static routes.
- TID is not available to routers.
- Control Plane Path Computation information is not available to routers.

Dynamic Routing - OSPF

Dynamic routing using the OSPF protocol can be enabled on a IP interface basis. OSPF is enabled on Management Links and disabled on Ethernet ports by default.

When OSPF is enabled on an IP interface:

- OSPF Areas may be configured (OSPFAREA-0.0.0.0 is configured by default)
- OSPF Areas have a configurable Routing Metric (cost) (default: 100)
- Hello packets are sent every 10 seconds
- Routers in the same OSPF Area form adjacencies by sharing Link State Advertisements (LSAs)
- LSAs use the System IP address as the Router ID

- LSAs are exchanged with the adjacent routers:
  - Ethernet ports send a broadcast network LSA with the netmask equal to the Ethernet port netmask (network route).
  - Management Links sends a stub network LSA with netmask equal to 255.255.255.255 (host route)
  - Loopback IP interface sends a router LSA (host route)

Optimal routes are calculated and entered in the routing table using the LSAs from all OSPF-enabled IP interfaces.

Static Routing

Static routes can be added, including a default gateway route. The static routes are added to the routing table. To ensure the default gateway is reachable, the default gateway route should be added especially if OSPF is disabled or an alternate route is needed.

- Static routes are added to the routing table when the IP interface becomes operational (i.e. at boot time or runtime when the cable is connected and the interface is enabled).
- The default gateway IP interface cannot be deleted until the associated static route has been deleted.

Each static route has a configurable routing metric. The value of the routing metrics determines the priority for the route. A route with low routing metric value has priority over a route with a higher routing metric value. By default, static routes have a routing metric of 1, giving them the highest priority after direct connection routes. Static routes take effect immediately after being added and do not require an NCU restart. Static routes are restored to the routing table when the IP interface recovers from an outage (e.g. Ethernet cable is unplugged, or a port is disabled).

Understanding the Routing Table

Before sending an IP packet, the system examines the routing table to determine which interface is used to route the IP packet to the destination. The IP packet is routed to route with the lowest metric value.

The routing table as 3 types of routes:

Direct - Automatically added by the system from interfaces which have an assigned IP address.

- Routing metric of 0.
- Broadcast IP interfaces can directly reach all hosts in the same IP subnet as the IP interface.
- Point-to-Point IP interfaces can directly reach the far-end host. The far-end IP address is only known when the connection is established.

Dynamic - Automatically added by the system as they are learned using OSPF.

- Routing metric calculated from the user entered routing metrics for all IP interfaces in the path to the destination.
- OSPF must be active to exchange routing information between the neighboring routers.

Static - Added by the user (i.e. default gateway route).

- Routing metric entered by the user.

The routes are automatically removed from the routing table when the IP interface of the route becomes inactive (e.g. an Ethernet cable is disconnected, an channel module with an assigned ECC is removed). The routes are automatically restored when the IP interface becomes active again. Destinations reached by dynamic routes, may be routed using a different IP interface when OSPF is used.

The NCU family support up to 600 routes in the routing table.

Examples:

Adding SC-1-A-C1 with IP Address: [192.168. 36.242] and IP Mask: [255.255.255. 0] adds the following route to the routing table:

```
Destination   Gateway        Mask              Type     Device       Metric
192.168.36.0  0.0.0.0        255.255.255.0     Local    SC-1-A-C1    0
```

Adding LINK-1-A-1 with Near End IP Address: 11.12.13.14 and Far End IP Address: 11.12.13.15 adds the following route to the routing table:

```
Destination   Gateway        Mask              Type     Device       Metric
11.12.13.15   0.0.0.0        255.255.255.255   Local    LINK-1-A-1   0
```

Enabling Gateway Proxy ARP

Gateway Proxy ARP allows the NCU to respond to ARP requests for IP addresses outside the bridged IP sub-net without setting up static routes or OSPF. Gateway Proxy ARP is supported by all NCU types.

> OSPF and Proxy ARP on all Management links must be disabled.

In the Network Element Director:

1. Select the **Overview** Application.
2. Click **Management Network** in the **Navigation Tree**.
3. Click the **Management Ports** blade in the main pane to display the Management Ports.
4. Click the management port row to open Configure Details window.

5. Set **Gateway Proxy ARP** to **Enable** in the **ARP Configuration** blade.
6. Click **Apply & Exit**.

IP Tunnels

The NEs support IP tunnels as per IETF standards RFC 2003 and RFC 2784. There are two variants of IP tunnels: IP-IP and IP-GRE. Both these standards allow encapsulation of IP packets within another IP packet. Adtran Networks SE supports both these variants of IP tunnels.

An IP tunnel can be used for control plane connectivity as well as DCN connectivity. In both cases the functionality and configuration parameters remain the same.

An IP tunnel is modeled as a logical interface (LIF or LIF-CP entity). OSPF is supported on these tunnel IP interfaces. The user may configure the protocol parameters if needed.

An IP tunnel may be used in the following cases:

- An NE which is not directly connected to an OSPF backbone needs to be part of the OSPF backbone.
- In a network topology where multiple OSPF areas are configured, the Path Computation Server (Control Plane from Adtran Networks SE) must have OSPF adjacencies to each of the non-backbone areas. To accomplish this for each non-backbone area at least one of its ABRs must have an IP tunnel configured to the Path Computation Server which is configured to be part of the OSPF backbone.
- Tunnels may be configured to connect to Network Elements that are not from Adtran Networks SE to get a direct point-to-point IP connection.
- Tunnels may be used to get connectivity over different administrative domains (address spaces) in the network.

Management Network Topologies

The following sections establish a reference model for the Management Network topologies. For each topology, the main characteristics are listed. Connection scenarios other than those described are not supported.

Connecting the Management Network

The NCU is required to support the management network on the NE. Most management packets are routed by the NCU to other interfaces. All equipment management in an NE is performed by the NCU. SCUs are required for communication between the NCU and other modules. When an NE has more than 1 shelf, the shelves must be connected via the SCU D and U ports.

Management LAN must be added to connect the UTM or CEM Ethernet (C) ports to the NCU.

OSCMs can be connected to the NCU by connecting an NCU C port to an OSCM C port with an Ethernet cable or by adding a Management LAN. Internally, all OSCM ports are interconnected with an internal Ethernet switch, so the OSCM ports are in the same Ethernet broadcast domain. Connecting the OSCM and NCU with an Ethernet cable provides the best performance. However, security may mandate the use of the Management LAN. Ethernet ports on the NCU, OSCM, UTM or CEM can be connected to the management system to provide remote access or can be used for local access.

Management Channels on channel modules must be connected to the NCU using Management Links.

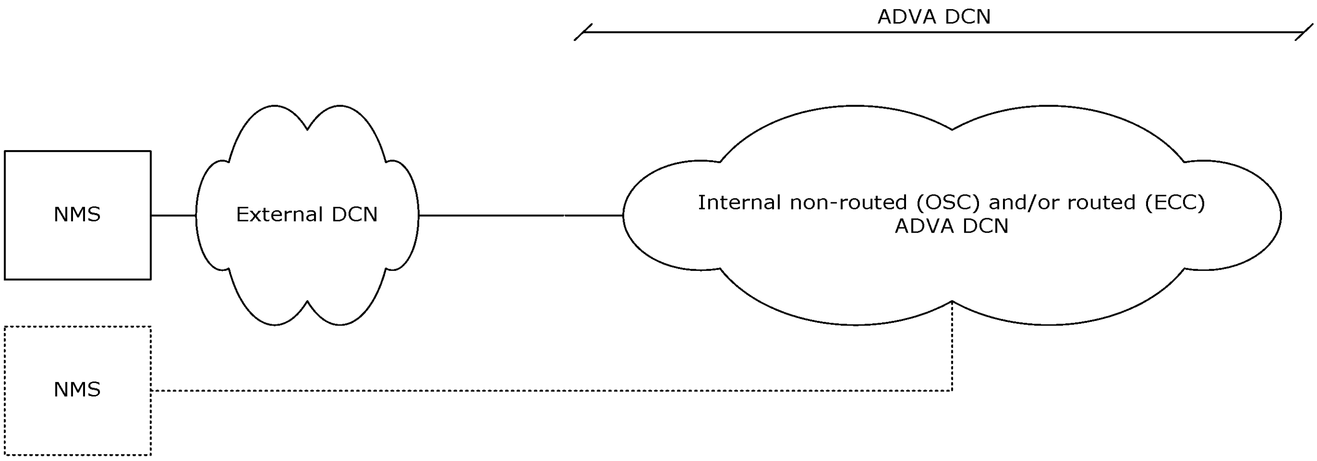
The Admin State on the Ethernet ports, Management LANs and Management Links must be in-service and the interface must be operational to support connection to the management network.

📄	Using a Management LAN to connect the NCU other modules limits the maximum throughput to 512 Kbps, even when the Ethernet ports are configured for 100 Mbps.

A Reference Model

The management network consists of management channels and transport devices interconnecting the NEs. The management network may include 3rd party routers and switches recommended by ADVA as needed for some topologies.

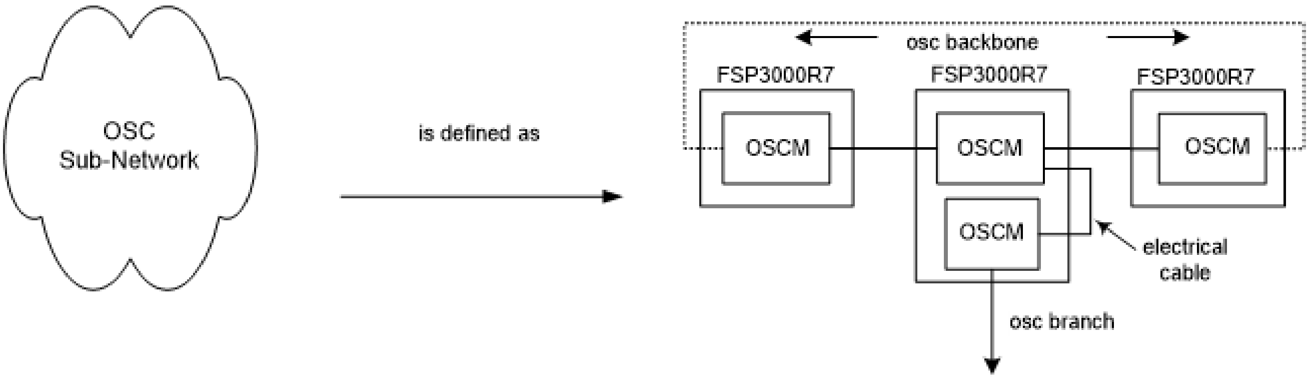
Figure 3: Reference Model



The figure shows the NMS may be connected directly to a FSP 3000R7 Ethernet port, or indirectly through an external DCN. When the NMS is not directly connected to the an external DCN is necessary and must be implemented by the customer.

A “non-routed” network refers to a Layer-2 Ethernet switch network. A “routed” network refers to a Layer-3 IP routed network.

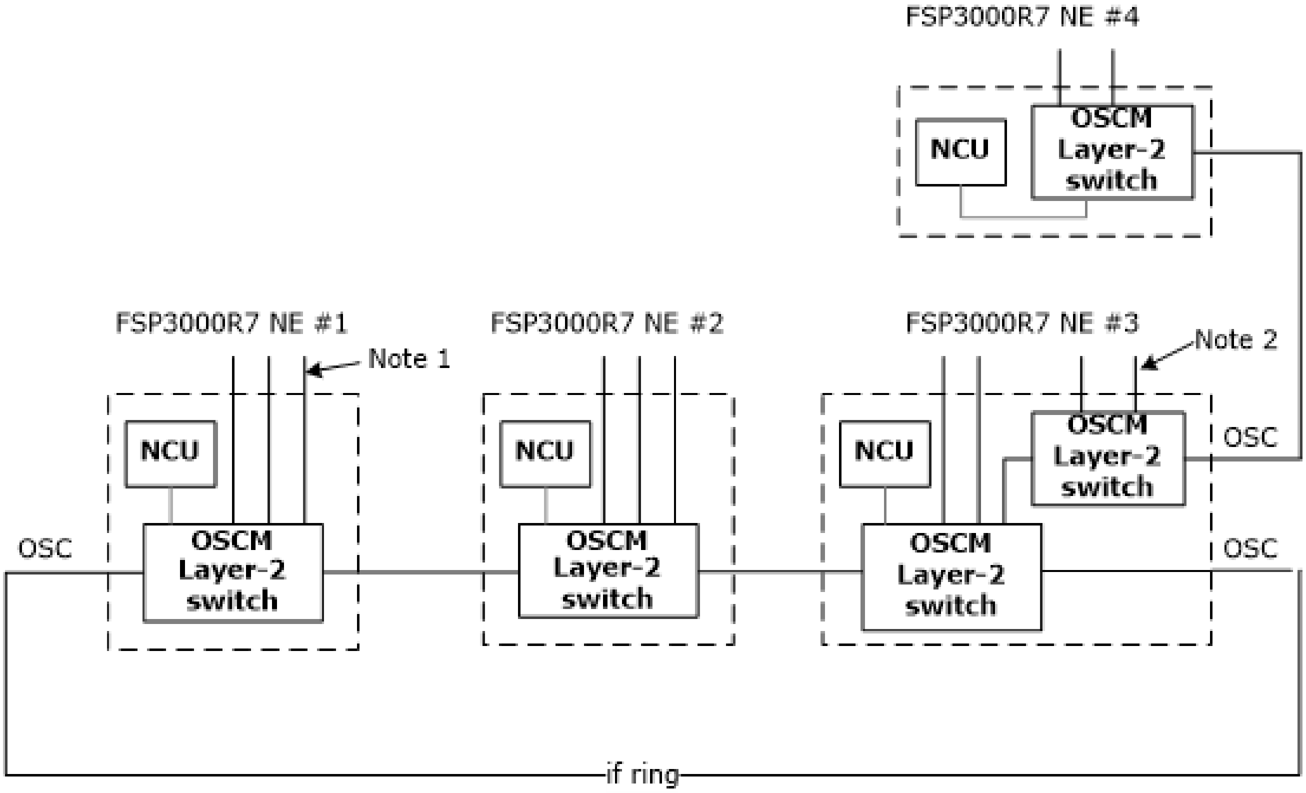
Figure 4: OSC Network: Backbone with a Branch



Optical Supervisory Channel (OSC) sub-networks are composed of NEs connected by OSC in point-to-point, linear add/drop, ring, or mesh topologies.

Optical Supervisory Channel (OSC) networks are OSC sub-networks connected with Ethernet cables or switches.

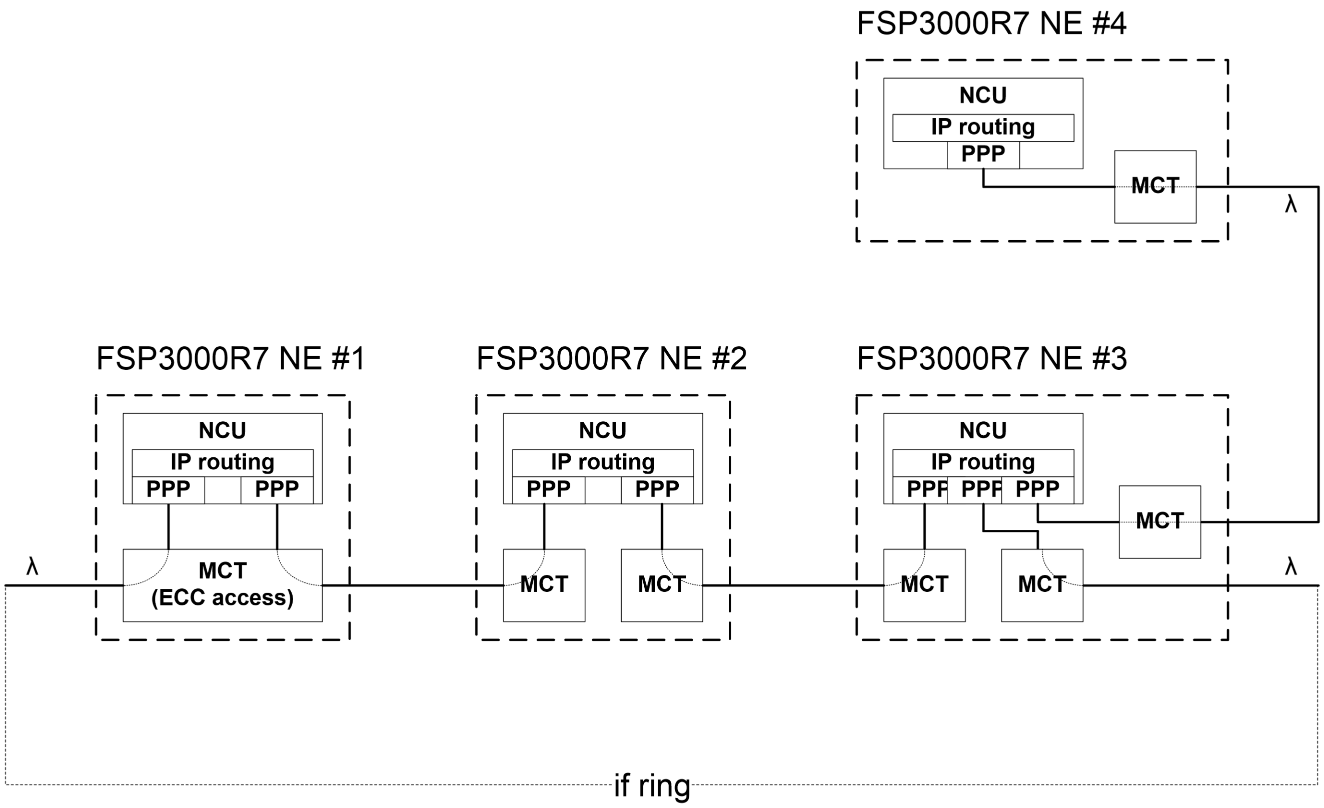
OSC Diagram



Note 1: Three RJ45 connectors are available for attaching other equipment to the OSC (assuming the front cable connection is used)

Note 2: Four RJ45 connectors are available for attaching other equipment to the OSC (assuming the front cable connection is used)

Figure 5: ECC Network with a Feeder



Example Scenarios

In the following example scenarios, figures support the text. If a figure specifies two Ethernet IP interfaces for an Fiber Service Platform 3000R7 NE, then this scenario is only possible when using an NCU2E (with two RJ45 connectors).

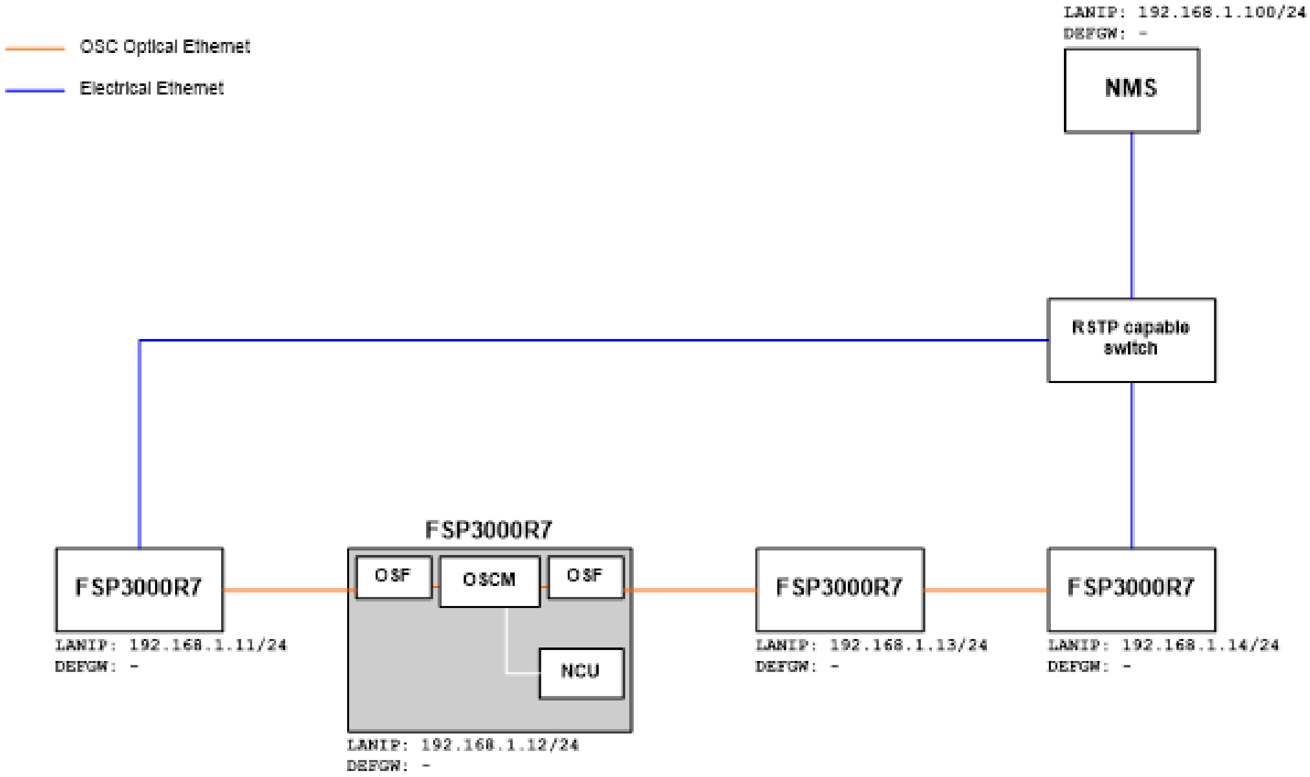
The following examples are provided:

Linear Add-Drop with OSC

To support protection in a linear add-drop network with an OSC, the NEs at both ends of the linear add-drop network should each have a connection to the NMS.

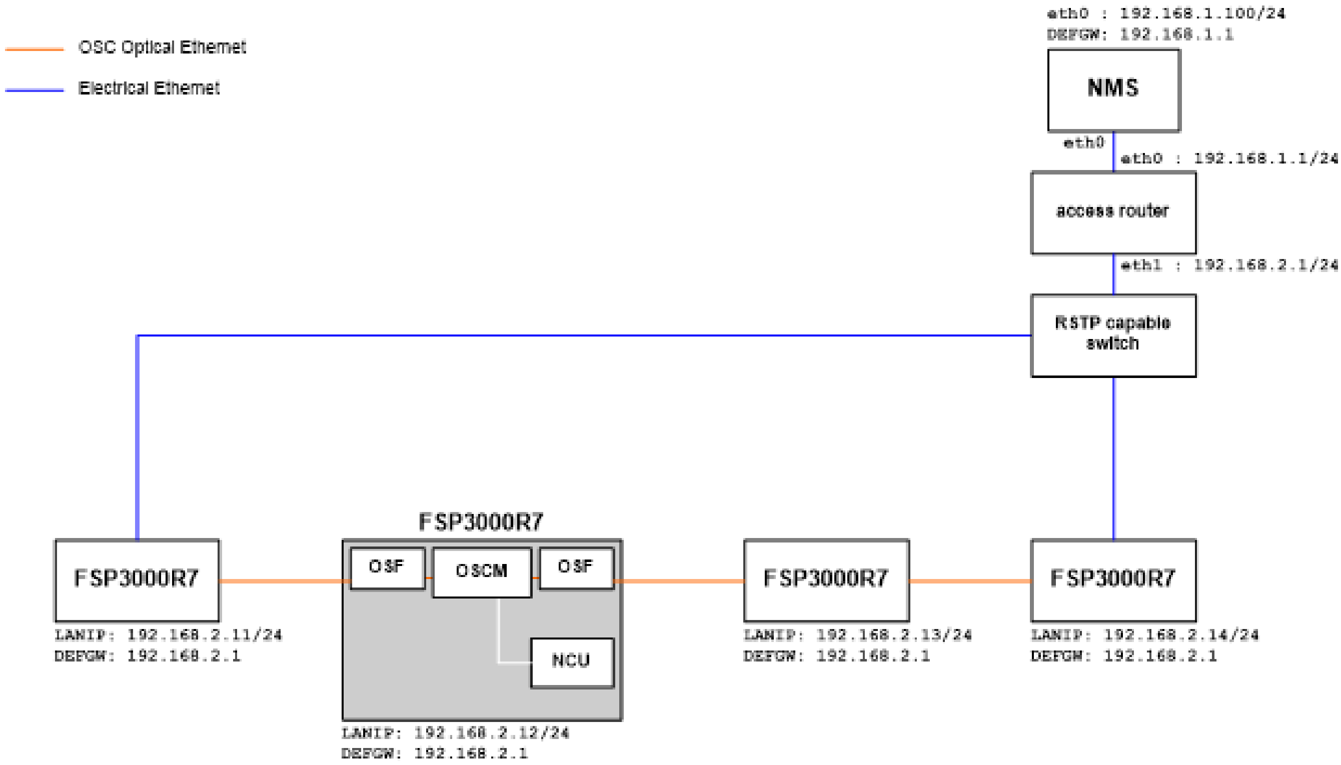
The NMS can be connected directly to the OSC modules in both NEs using a 3rd party switch. As mentioned (see Layer 2: OSC Loop-Free Protection) this switch must then be (R)STP capable. The NMS and all NEs are in the same IP subnet, and protection is done at Layer 2 (TDP and RSTP).

Figure 6: Example Scenario of Linear Add-Drop with OSC - RSTP Capable



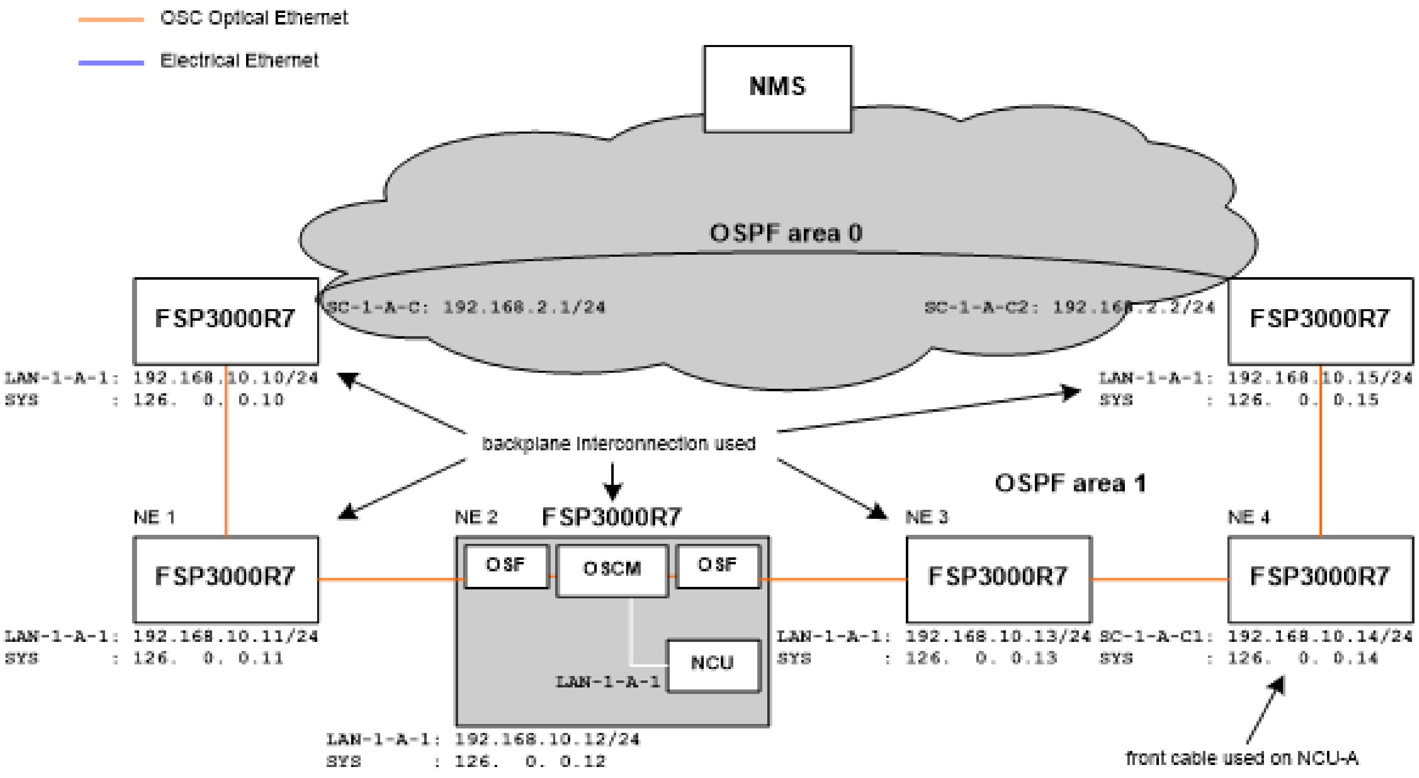
Default gateway entries in the NE routing tables are not necessary in this (hypothetical) scenario. In the real world however the NMS is likely to be connected to the RSTP switch over a router, and the NMS will be in a different subnet; the NE default gateway entries (or alternatively a static route to the NMS IP subnet) then point to this access router.

Figure 7: Example Scenario of Linear Add-Drop with OSC - RSTP Switch Over a Router



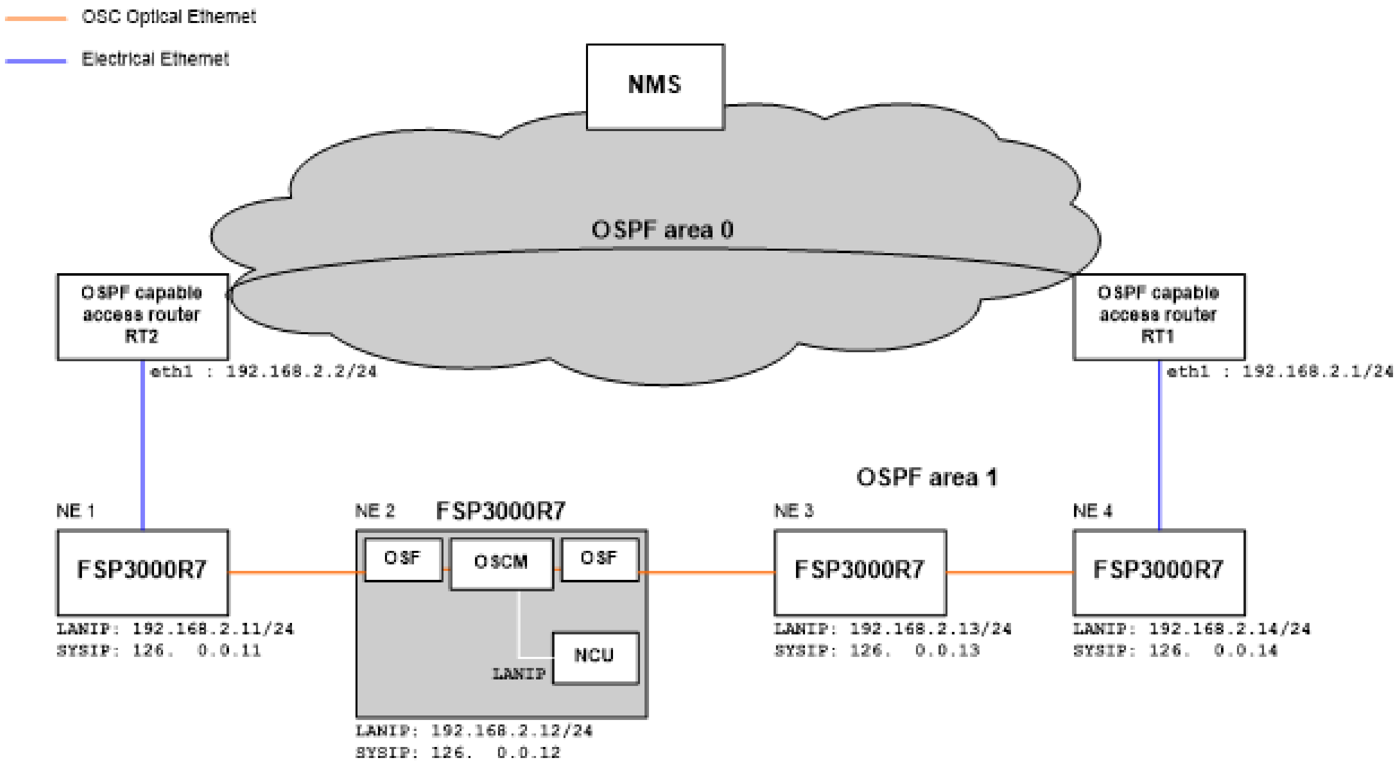
This would actually be sufficient as a fast protection scheme, but due to the physical distance between the NEs at the ends of the linear add-drop network connecting to the NMS it will be more likely that these NEs are connected with the NMS over one or more routers each. These access routers must then be OSPF capable.

Figure 8: Example Scenario of Linear Add-Drop with OSC - NEs as Access Routers



For demanding DCNs, ADVA recommends using devices that are designed specifically for IP routing as access routers (see Figure 9).

Figure 9: Example Scenario of Linear Add-Drop with OSC - Separate Access Routers



Since the FSP 3000R7 NEs support routing between their IP interfaces, it is possible to use the edge NEs as access routers (see Figure 23 on p. 107). To do this, use the NCU front connectors.

The access routers will distribute routes for external destinations (among these is the route to the NMS) into OSPF area 1[1]. To support a protection scenario these access routers have to communicate with each other over a second interface located either in the same area or in the backbone area[2].

The protection scenario goes as follows: After a cut in the OSC linear network, area 1 is now partitioned so that two separated area 1's exist, as well as two Ethernet LANs having the same IP subnet. This is a situation that obviously should be rectified as quickly as possible. As long as the OSC Ethernet is partitioned, the Ethernet IP addresses cannot be reliably used to reach the NEs. Only the ones reachable by the access router with the "shortest" path to the OSC Ethernet LAN will be reachable, the other partition will not.

Nevertheless, loss of connectivity to the NEs in the meantime can be avoided by configuring the NEs with a System IP address different from the Ethernet IP address (i.e. do not use the “unnumbered” option for the Ethernet IP interface) in such a way that OSPF will distribute host[3] routes to these System IP addresses (either in the same area or in the backbone area). It is therefore advisable to always address the NEs with their System IP address (in the NMS and in other applications) and avoid using the “unnumbered” configuration for the Ethernet IP interfaces in such a topology.

Linear Add-Drop with ECC

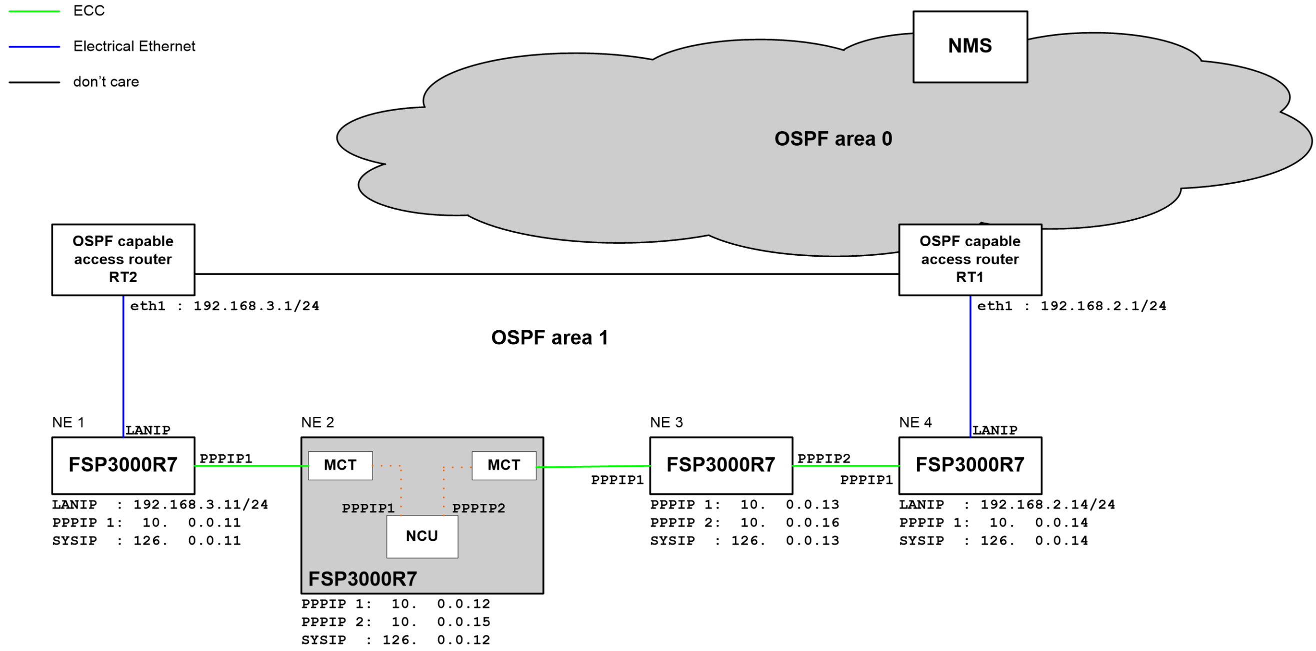
Protection in a linear add-drop network with ECCs is similar to protection in a linear add-drop network with OSC; the only difference is that packets are routed hop-by-hop rather than switched into the OSC LAN.

[1] The most economic solution would be to configure area 1 as a stub area. However, this is currently not supported by the FSP 3000R7.

[2] The advantage of having the access router secondary interfaces in the same area as the interfaces to the NE is that the System IP host routes may be aggregated towards the backbone area; the advantage of having the secondary interfaces in the backbone area is that the NMS can be connected redundantly to both routers in the backbone.

[3] One drawback of this protection scenario is that host routes for each NE in the LAN are sent into the backbone area. This is however unavoidable if full protection for a linear LAN is to be provided.

Figure 10: Example Scenario of Linear Add-Drop with ECC



The access routers will distribute routes for external destinations (among these is the route to the NMS) into OSPF area 1. To support a protection scenario, these access routers have to communicate with each other over a second interface located either in the same area or in the backbone area.

The protection scenario goes as follows: After a cut in the ECC linear network, area 1 is now partitioned so that two separated area 1's exist. This is a situation that obviously should be rectified as quickly as possible.

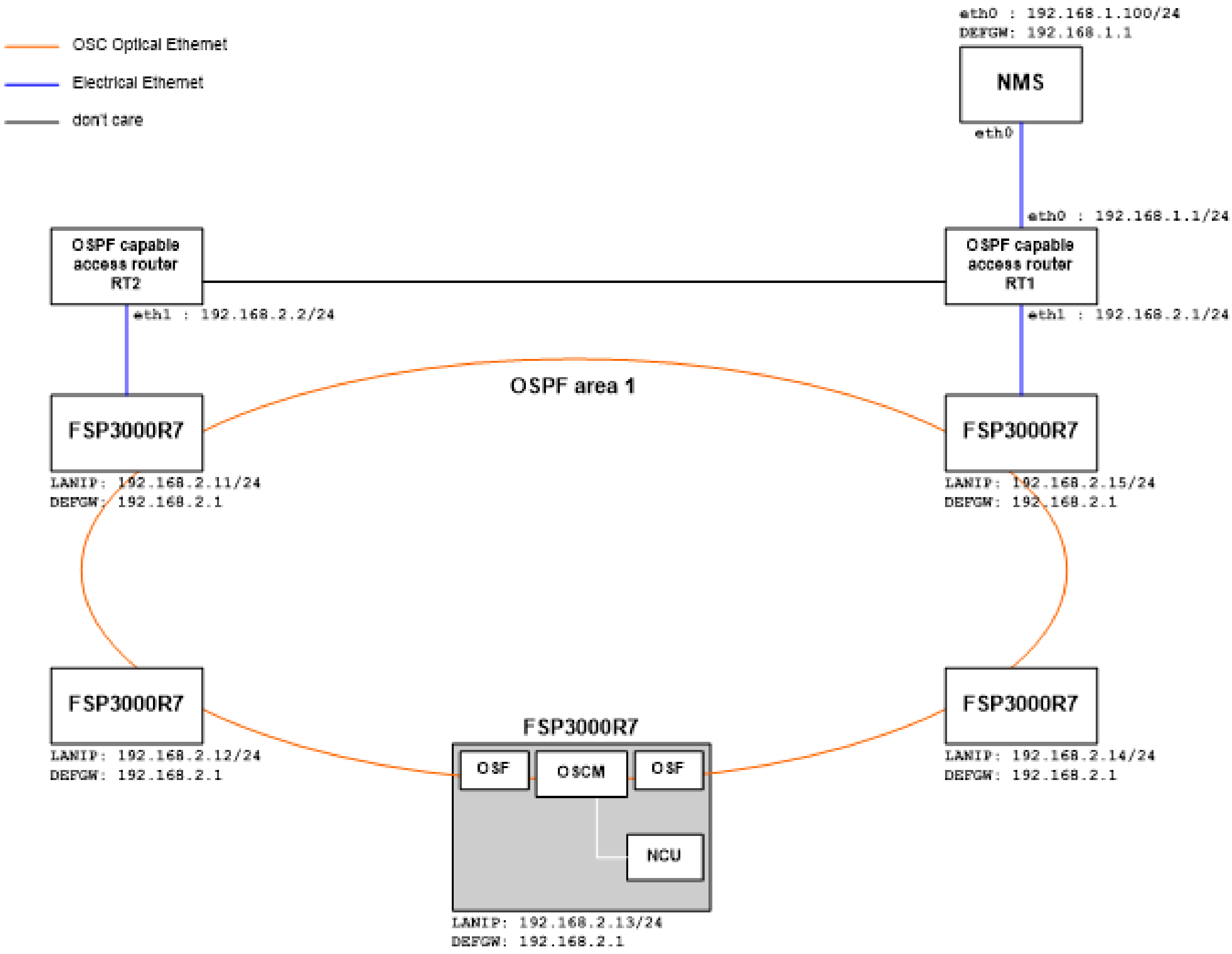
Nevertheless. connectivity to the NEs is not lost in the meantime, as OSPF will update the routes to the PPPIP addresses to avoid the failure. The routes to the System IP addresses will also be updated. It is advisable to always address the NEs with their System IP address (in the NMS and in other applications).

Ring with OSC

To support protection in a network with an OSC, two NEs in the ring should each have a connection to the NMS.

The same remarks as with a linear add-drop network apply, leading to the topology with two access routers communicating over a second interface either in the backbone area or in the same area.

Figure 11: Example Scenario of Ring with OSC - Using NCU-A/NCU-B, No Backplane Interconnection



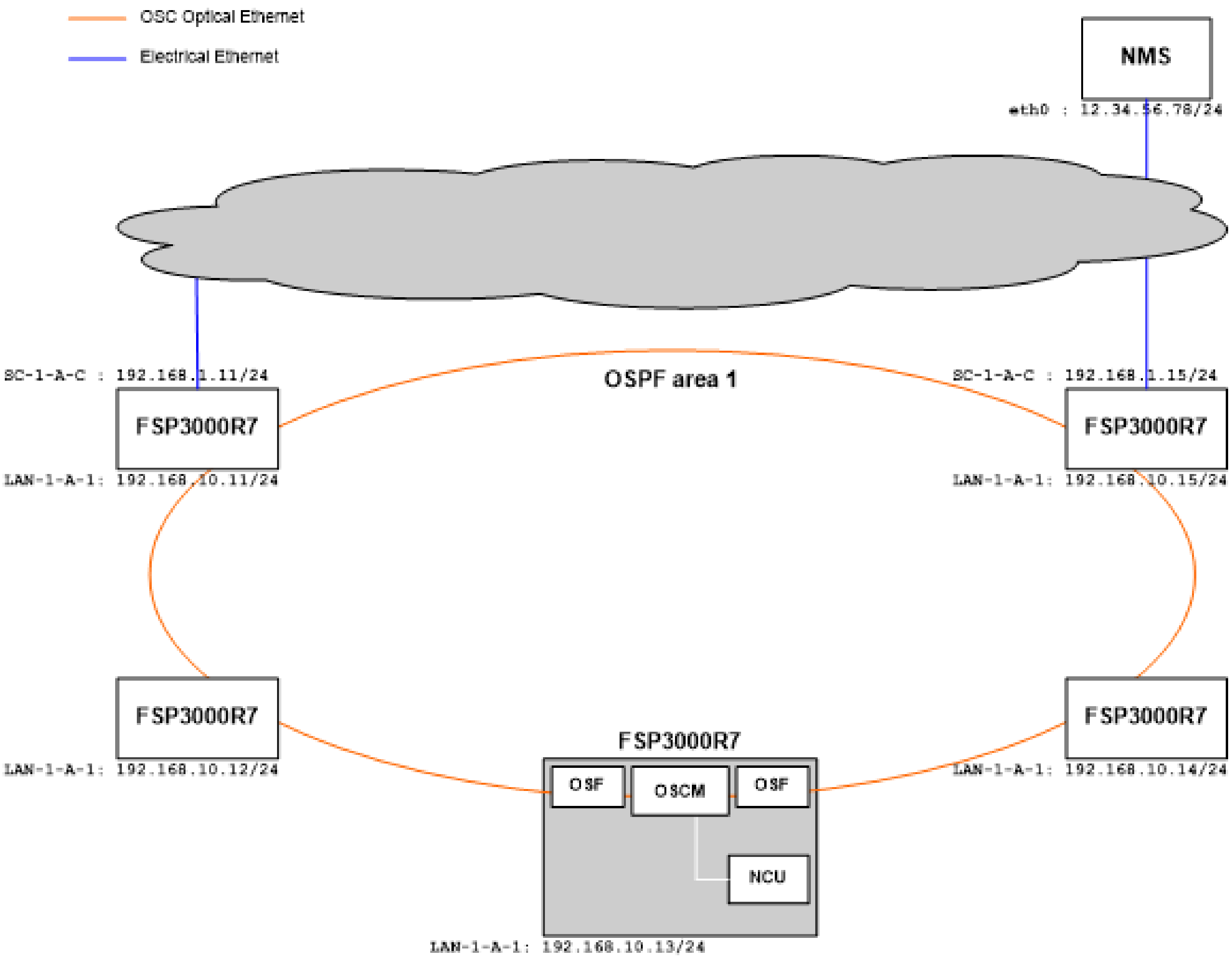
There are 2 kinds of failures possible here:

1. A single break in the ring; this will be handled by TDP, and will be invisible at Layer 3.
2. A failure of one of the gateway NEs or access routers or of the link between a GNE and an access router; this will be handled by OSPF.

Note that the access routers, the communication between them and the use of host routes to the System IP addresses are still useful in case both failures occur at the same time.

The access router function may be taken over by the GNEs in the ring. The main thing is that instead of attaching the external DCN and the OSC to 2 OSC module Ethernet ports (Layer 2) between which switching is performed, they are attached to 2 NCU Ethernet IP interfaces (Layer 3) between which routing is performed.

Figure 12: Example Scenario of Ring with OSC - Using Backplane Interconnection


OSC Optical Ethernet
Electrical Ethernet
NMS
eth0 : 12.34.56.78/24
SC-1-A-C : 192.168.1.11/24
OSPF area 1
SC-1-A-C : 192.168.1.15/24
FSP3000R7
FSP3000R7
LAN-1-A-1: 192.168.10.11/24
LAN-1-A-1: 192.168.10.15/24
FSP3000R7
FSP3000R7
FSP3000R7
LAN-1-A-1: 192.168.10.12/24
OSF
OSCM
OSF
LAN-1-A-1: 192.168.10.14/24
NCU
LAN-1-A-1: 192.168.10.13/24

Single Ring Topologies

In a ring of NEs, the following management connectivity scenarios are possible:

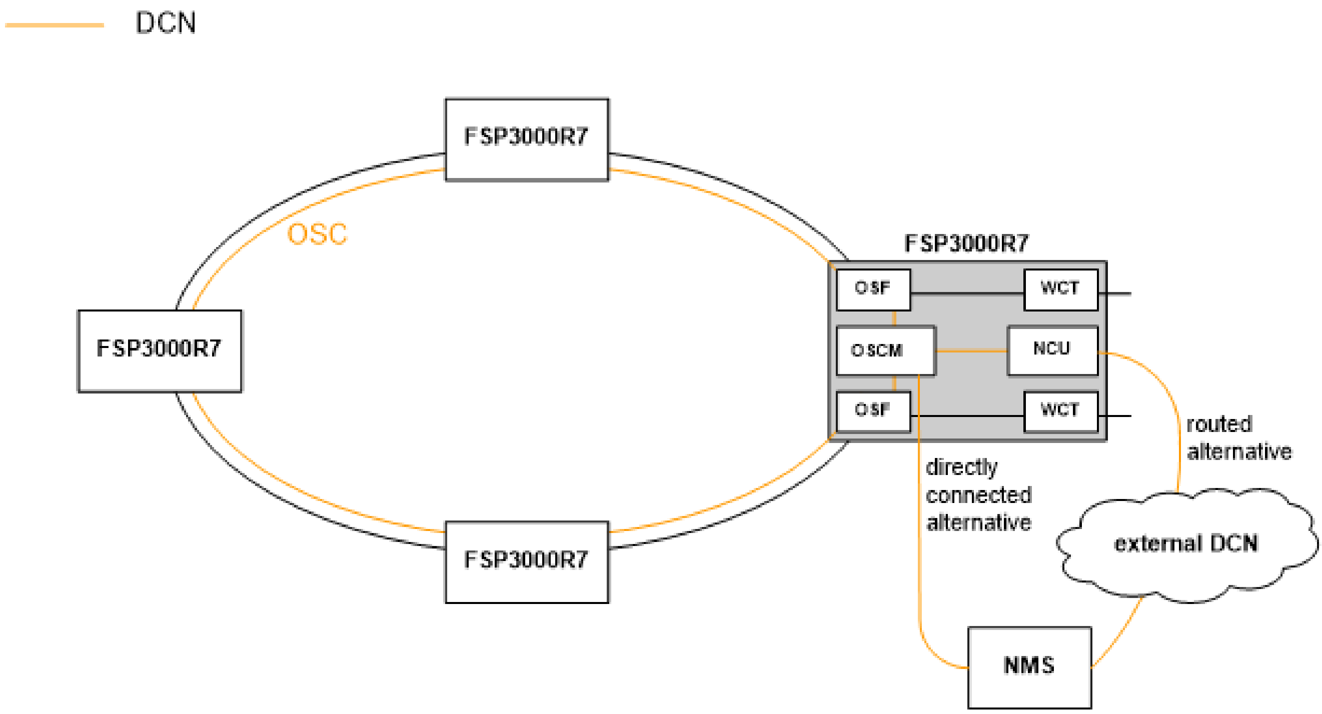
Management Over OSC in a Single Ring

Characteristics of management over OSC:

- Each NE in the ring must be equipped with an OSC supporting module.
- Each NCU must be attached to the DCN via a front cable Ethernet connection or via a backplane interconnection to (one of) the OSC module(s) in the local NE.
- The NMS must be attached to the DCN via an electrical Ethernet cable connection to an NCU or an OSC module of a GNE in the ring.
- Any co-located equipment must be attached to the DCN via an electrical Ethernet cable connection to the OSC module of the local NE. If the number of free Ethernet ports of the OSC module is exhausted, an external 3rd party switch must be used.

- The ADVA DCN forms a single switched Ethernet.
- Protection is based on TDP (Layer 2) in the optical Ethernet ring.

Figure 13: Management Over OSC in a Single Ring



Attaching the NMS to an OSC module places the NMS in the same broadcast domain as the whole ring NEs; therefore in such a topology the NMS should be configured with an IP address in the same IP subnet as the OSC IP addresses of the ring NEs (i.e. for each NE the IP address as configured on its NCU Ethernet IP interface attached to the OSC).

Attaching the NMS to an NCU places the NMS in a broadcast domain different from the one of the ring NEs (because the NCU performs Layer-3 routing between its Ethernet IP interfaces). Therefore, in such a topology the NMS should be configured with an IP address in an IP subnet different from the one of the OSC IP addresses of the ring NEs. The GNE NCU will then route packets between the NMS and the other NEs in the ADVA DCN. An external DCN may be in between the NMS and the GNE. This is a common way to separate the customer DCN from the ADVA DCN.

Please note that both the direct and the routed connection alternatives are available for all the following scenarios, even if this is not explicitly shown in the figures.

Management Over ECCs in a Single Ring

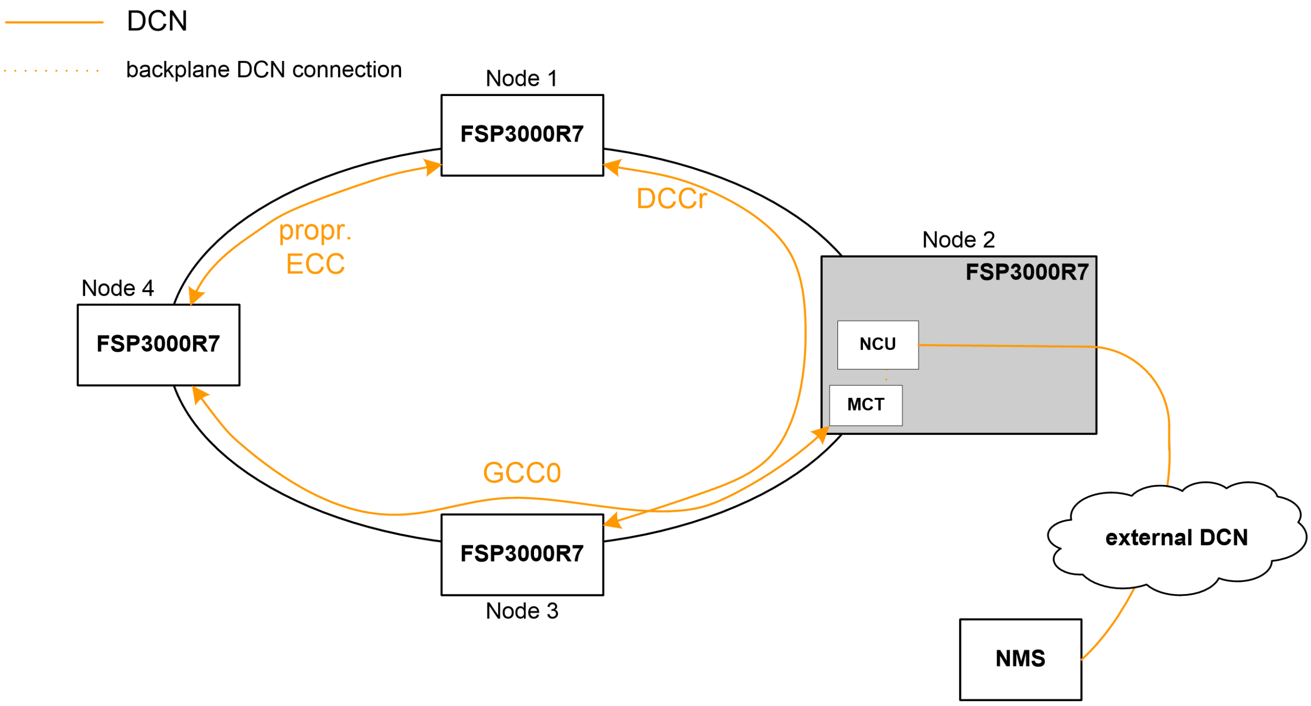
Characteristics of management over ECCs:

- Each NE in the ring must be equipped with one or more ECC capable channel modules (MCTs)[1]; the ECC links need to form at least a spanning tree

[1] The MCTs at either side of a wavelength span, must both be capable of and configured to extract the same ECC (e.g. both DCCr or both GCC0, etc.).

- There is no need for OSC modules (cost reduction + gain of optical budget)
- Each NCU must be attached to the DCN via one or more PPP connection(s) over the ECC(s) (routed)
- The NMS must be attached to the DCN via an electrical Ethernet cable connection to an NCU in the ring (GNE)
- Protection is based on OSPF (Layer 3) in the NCUs; for some ECCs MSP protection (Layer 2) is available

Figure 14: Management Over ECCs in a Single Ring



In Figure 14, connectivity between all nodes (though non-redundant, thus unprotected) is provided: e.g. Node 3 can reach Node 2 in 3 hops over Node 1 and Node 4.

Management Over External DCN in a Single Ring

Characteristics of management over external DCN:

- Management connectivity between the NMS and the NEs must be provided over a dedicated WDM wavelength or via another customer-owned network
- There is no need for OSC modules (cost reduction + gain of optical budget) nor ECC capable channel modules (MCTs)
- Each NCU must be attached to the external DCN via its front Ethernet connection
- The NMS must be attached to the external DCN
- Protection is based on dedicated WDM wavelength protection or customer-specified protection in external DCN

This scenario is mentioned for the sake of completeness only.

Interconnected Rings

In a number of interconnected rings of Fiber Service Platform 3000R7 NEs the following management connectivity scenarios are possible:

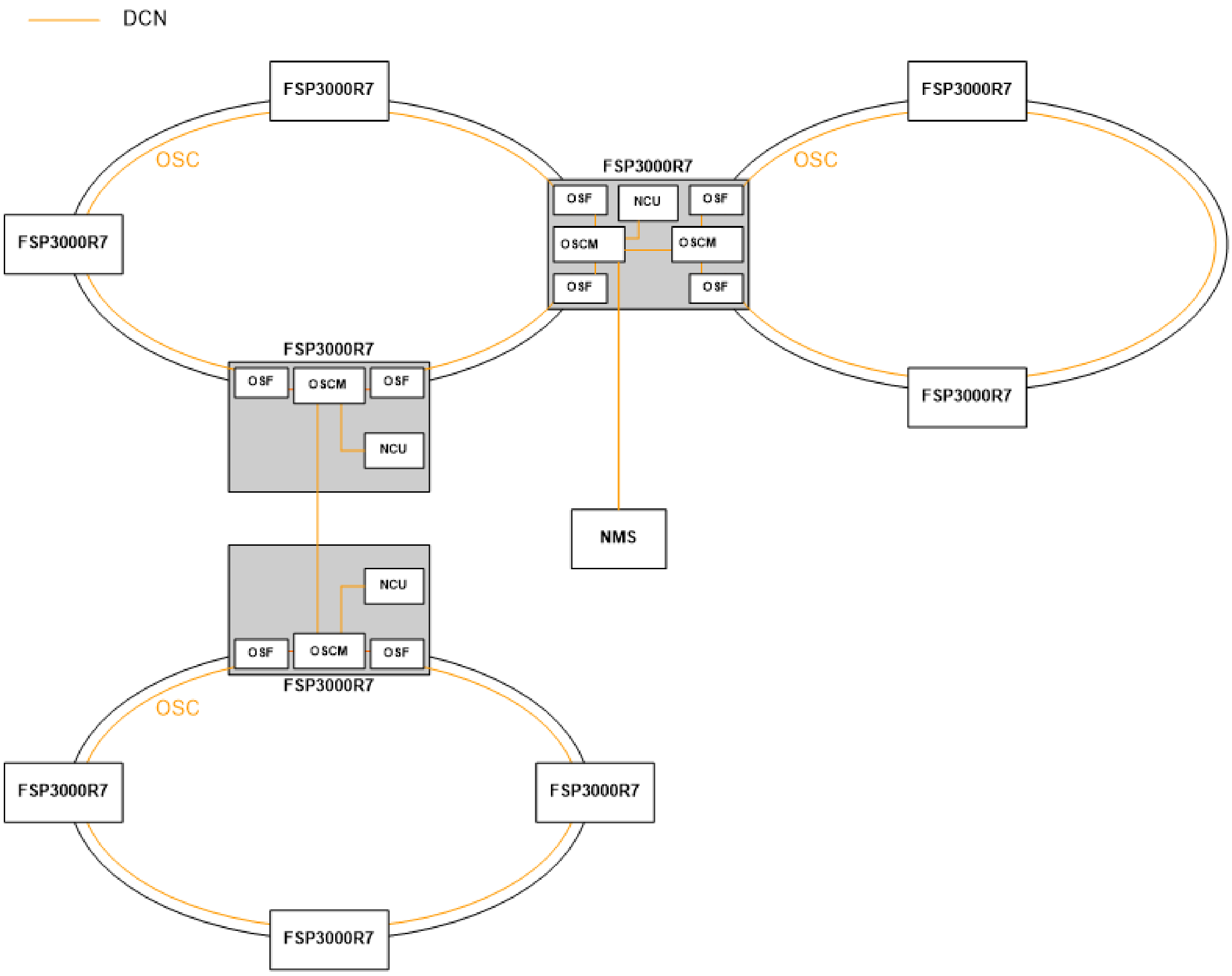
Management Over OSC in Interconnected Rings

For each ring, the characteristics as described in "Management Over OSC in a Single Ring" apply.

Additional characteristics of management over OSC in interconnected rings:

- NE which interconnect two optical rings should use a separate OSCM-PM for each optical ring.
- These two OSCMs exchange management traffic:
  - Through the backplane interconnection. In this case traffic is switched from one ring to another. Note that this is only possible if both OSCMs reside in the same NE.
  - Through a direct front cable between their front Ethernet ports. In this case traffic is switched from one ring to another
  - Through a router between their front Ethernet ports. In this case traffic is routed from one ring to another. The router interconnection must be a 100Mbit/s full duplex link, and the router must be capable of handling the traffic without traffic loss.
- All rings connected by direct cables or by backplane interconnections form one Ethernet broadcast domain. This is only advisable for small OSC networks in which the number of hosts in the broadcast domain remains within limits, and for which it is important to save the cost of an extra router.

Figure 15: Management Over OSCs in Interconnected Rings



Management Over ECCs in Interconnected Rings

For each ring, the characteristics as described in Management Over ECCs in a Single Ring apply.

Additional characteristics of management over ECCs in interconnected rings:

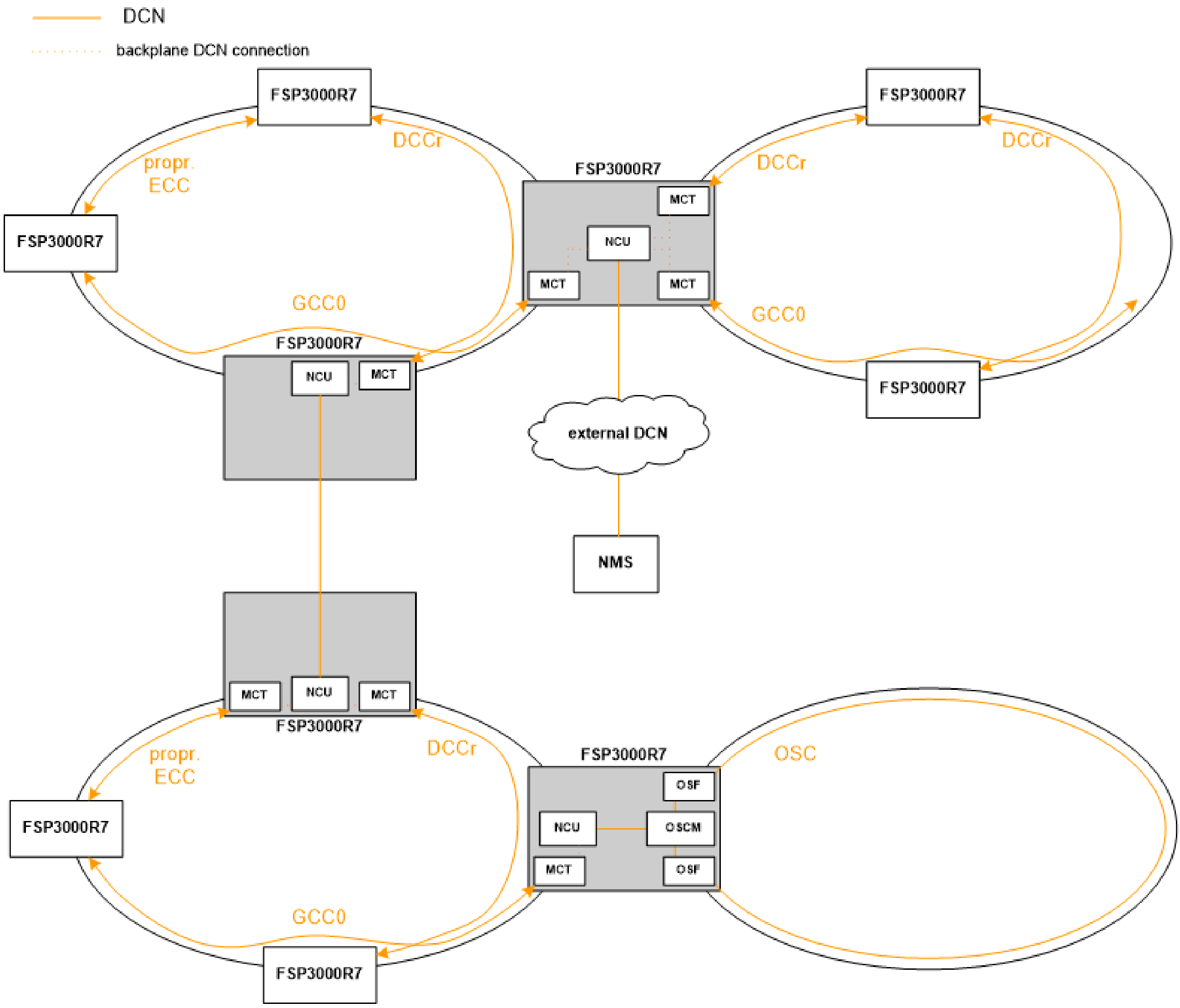
- Each pair of optical rings of FSP 3000R7s is interconnected by means of either a single FSP 3000R7 NE, which is part of both rings
  - Each ring must have at least one ECC termination in the shared FSP 3000R7 NE
  - The NCU in the shared FSP 3000R7 NE will exchange management traffic between these ECCs. Traffic is routed from one ring to another.

or by two FSP 3000R7 NEs, each of which is part of a single ring

- Each ring must have at least one ECC termination in its own FSP 3000R7 NE
- The NCUs in the two FSP 3000R7 NEs exchange management traffic through their front Ethernet IP interfaces. Traffic is routed from one ring to another.

- One or more OSC modules may be used to interconnect a ring with OSC and a ring without OSC

Figure 16: Management Over ECCs in Interconnected Rings



Feeders

Each NE in an optical ring or linear add-drop topology may provide backbone access to a number of feeders. Such a feeder may be an Fiber Service Platform 3000R7 NE, FSP 3000, FSP 2000, FSP1500, FSP150, or a 3rd party NE. It may be connected directly or through a 3rd party SDH/SONET network. These management connectivity scenarios are possible:

- Fiber Service Platform 3000R7 feeders may be managed over the OSC (if an OSC module is present), over an ECC or via an external DCN
- FSP 3000/FSP 2000 feeders can only be managed through an external DCN. This is because:

  - Neither the FSP 3000 nor the FSP 2000 offer access via an ECC
  - Neither the FSP 3000 nor the FSP 2000 offer access via the OSC (not supported for reasons of incompatibility with the Fiber Service Platform 3000R7 OSC (wavelength and/or topology protocol)) FSP 3000/FSP 2000 feeders can thus only be managed through an external DCN.
- The FSP1500 can only be managed via an ECC or via an external DCN

In all these cases, it is assumed that:

- The NMS is attached to the DCN via an electrical Ethernet cable connection to one OSC module in the ring

Management of an FSP 3000R7 Feeder Over the OSC

For a ring, the characteristics as described in Management Over OSC in a Single Ring or in Management Over ECCs in a Single Ring apply.

Additional characteristics for the FSP 3000R7 Feeder over OSC:

- Backbone NE should have an OSC for each degree. Feeder NE can be connected with OSC or GCC management channels.

Each additional OSC module will support:

- A single unprotected feeder (in which the optical port serves 1 feeder NE)

Each additional OSCM-PN will support either:

- Up to 2 unprotected feeders (in which each optical port serves 1 feeder NE), or
- Up to 2 dual-homed feeders (any combination of bullet 1 and 2 is possible) (in which each optical port serves one dual-homed feeder NE), or
- A single point-to-point protected feeder (in which both optical ports serve the same feeder NE).

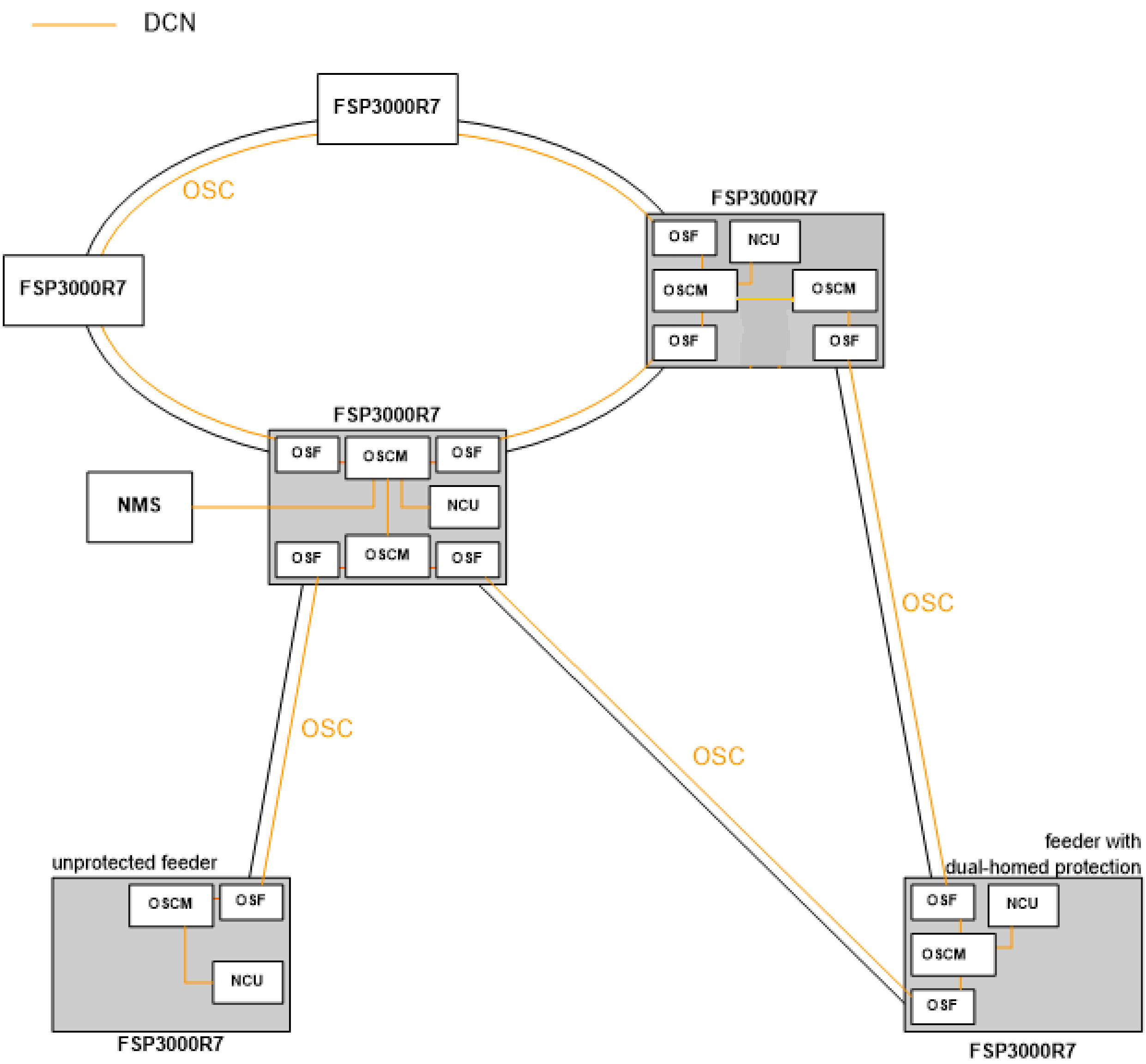
Each feeder NE must be equipped with at least one OSC module. Each additional OSC module will support an unprotected OSC connection to the backbone (in which the optical port is served by a backbone NE)

- Each OSCM-PN will support either:
  - An unprotected OSC connection to the backbone (in which only 1 optical port is used and served by a backbone NE), or
  - A point-to-point protected OSC connection to the backbone (in which both optical ports are served by the same backbone NE), or
  - A dual-homed protected OSC connection to the backbone (in which each optical port is served by a different backbone NE)
- The feeder NCU must be attached to the DCN via a front cable Ethernet connection or via a backplane interconnection to the OSC module in the feeder NE

- The feeder belongs to the single switched Ethernet formed by all NEs that are interconnected with OSC modules
- Protection for a point-to-point protected feeder is based on TDP (Layer 2)
- Be sure to enable the (R)STP on the electrical Ethernet OSCM ports prior to interconnecting them. See Layer 2: OSC Loop-Free Protection".

For more information about protection, see DCN Resiliency and Protection.

Figure 17: Unprotected and Dual-Homed Protected Feeder Connection Over OSC



Management of an FSP 3000R7 Feeder Over ECCs

For a ring, the characteristics as described in Management Over OSC in a Single Ring and Management Over ECCs in a Single Ring apply.

Additional characteristics for the FSP 3000R7 Feeder over ECCs:

- Each backbone NE that has a feeder attached, must be equipped with at least one ECC capable channel module (MCT)[1] leading to the feeder.

Each ECC will support:

- a single unprotected feeder (in which the ECC serves 1 feeder NE)

Each pair of ECCs will support either:

- Up to 2 unprotected feeders (in which each ECC serves 1 feeder NE), or
- Up to 2 dual-homed feeders (any combination of bullet 1 and 2 is possible) (where each ECC serves 1 dual-homed feeder NE), or
- A single point-to-point protected ECC branch (in which both ECCs serve the same feeder NE).

Each feeder NE must be equipped with at least one MCT[2] leading to the backbone.

Each ECC will support:

- An unprotected ECC connection to the backbone. See Management of an FSP 1500 Feeder Over ECCs (in which the ECC is served by a backbone NE).

Each pair of ECCs will support either:

- A point-to-point protected ECC connection to the backbone (in which both ECCs are served by the same backbone NE), or
- A dual-homed protected ECC connection to the backbone (in which each ECC is served by a different backbone NE)

The feeder NCU must be attached to the DCN via one or more connections over the ECCs (routed)

Protection is based on OSPF (Layer 3) in the NCUs; for some ECCs MSP protection (Layer 2) is available

[1] The MCTs at either side of a wavelength span, must both be capable of and configured to extract the same ECC (e.g. both DCCr or both GCC0, etc.).

[2] The MCTs at either side of a wavelength span, must both be capable of and configured to extract the same ECC (e.g. both DCCr or both GCC0, etc.).

Figure 18: Unprotected and Protected Feeder Connection Over ECC

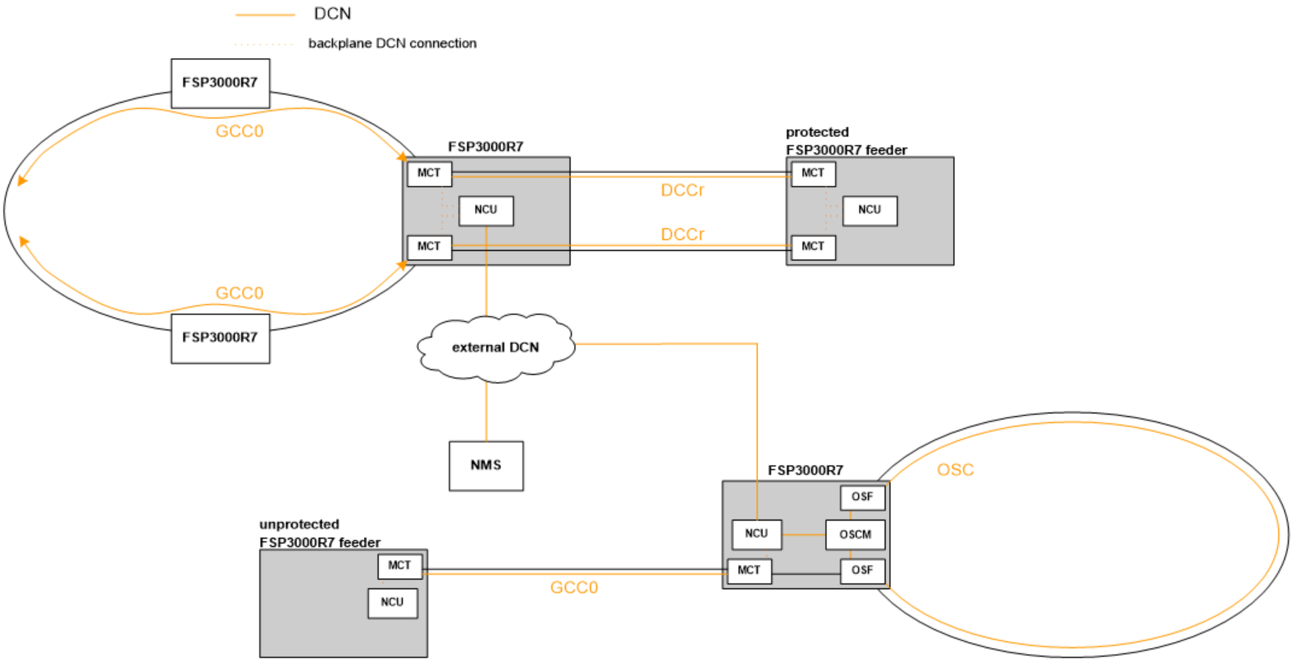
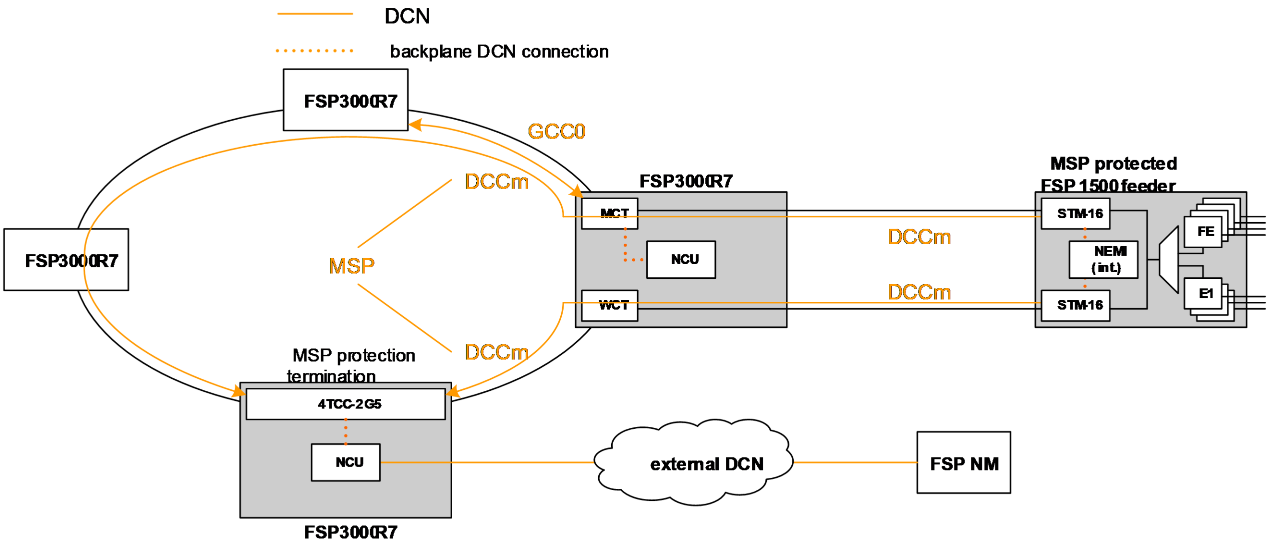


Figure 19: MSP Protection Termination and MSP Protected Feeder Connection Over ECC



Management of an FSP 1500 Feeder Over ECCs

For a ring, the characteristics as described in Management Over OSC in a Single Ring and Management Over ECCs in a Single Ring apply.

Additional characteristics for the FSP 1500 Feeder over ECCs:

- Each backbone NE that has an FSP 1500 feeder attached, must be equipped with at least one ECC capable channel module (MCT)[1] leading to the feeder FSP 1500

[1] The MCTs at either side of a wavelength span, must both be capable of and configured to extract the same ECC (e.g. both DCCr or both GCC0, etc.).

- Each feeder must be equipped with at least one MCT[1] leading to the backbone
- The feeder FSP 1500 must be attached to the DCN via one or more connection(s) over the ECC(s) (routed)
- Protection is based on OSPF (layer 3) in the NCU and in the FSP 1500; for DCCm MSP protection (layer 2) is available

Figure 20: Unprotected and Protected Feeder Connection Over ECC

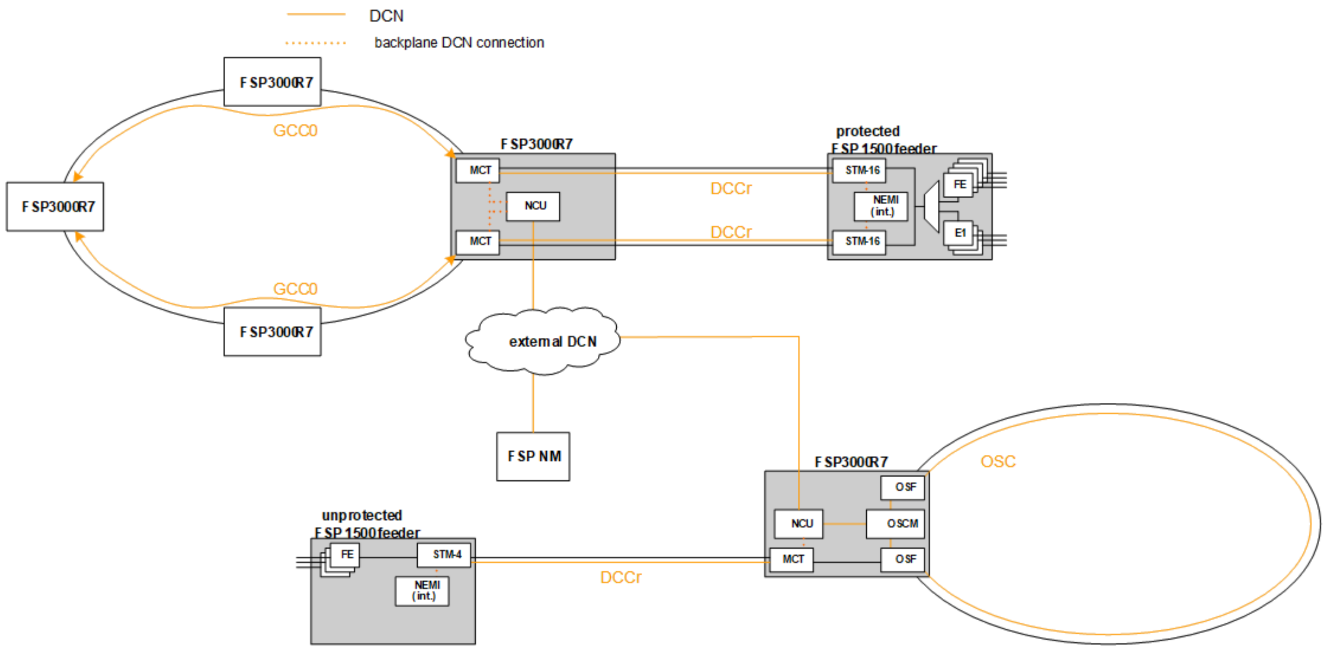
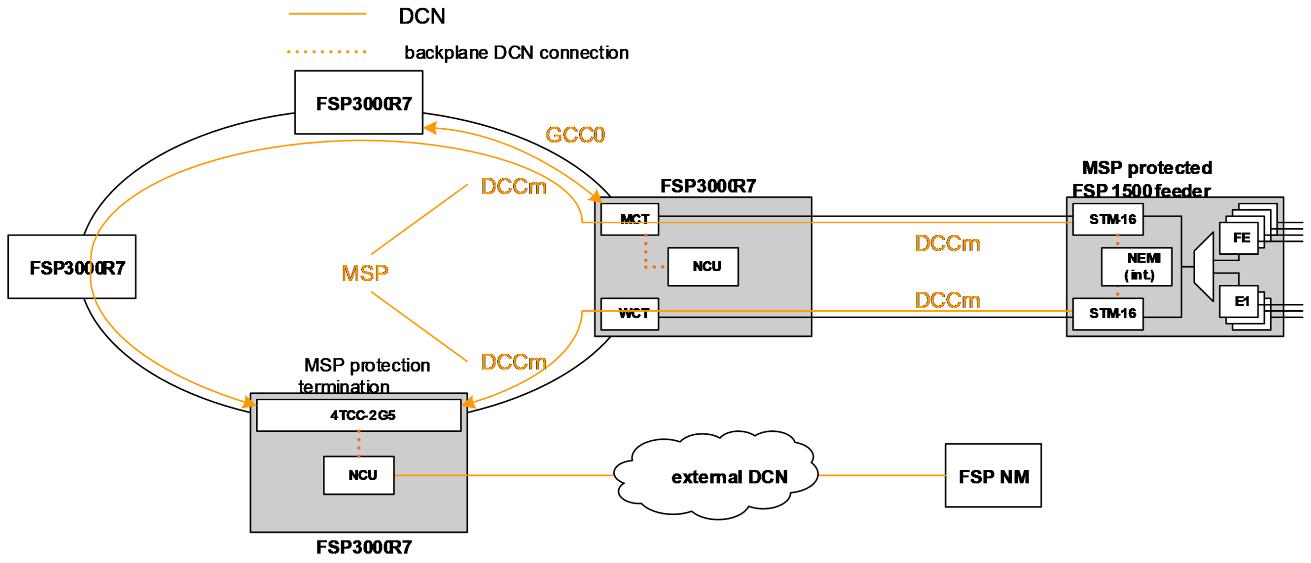


Figure 21: MSP Protection Termination and MSP Protected Feeder Connection Over ECC



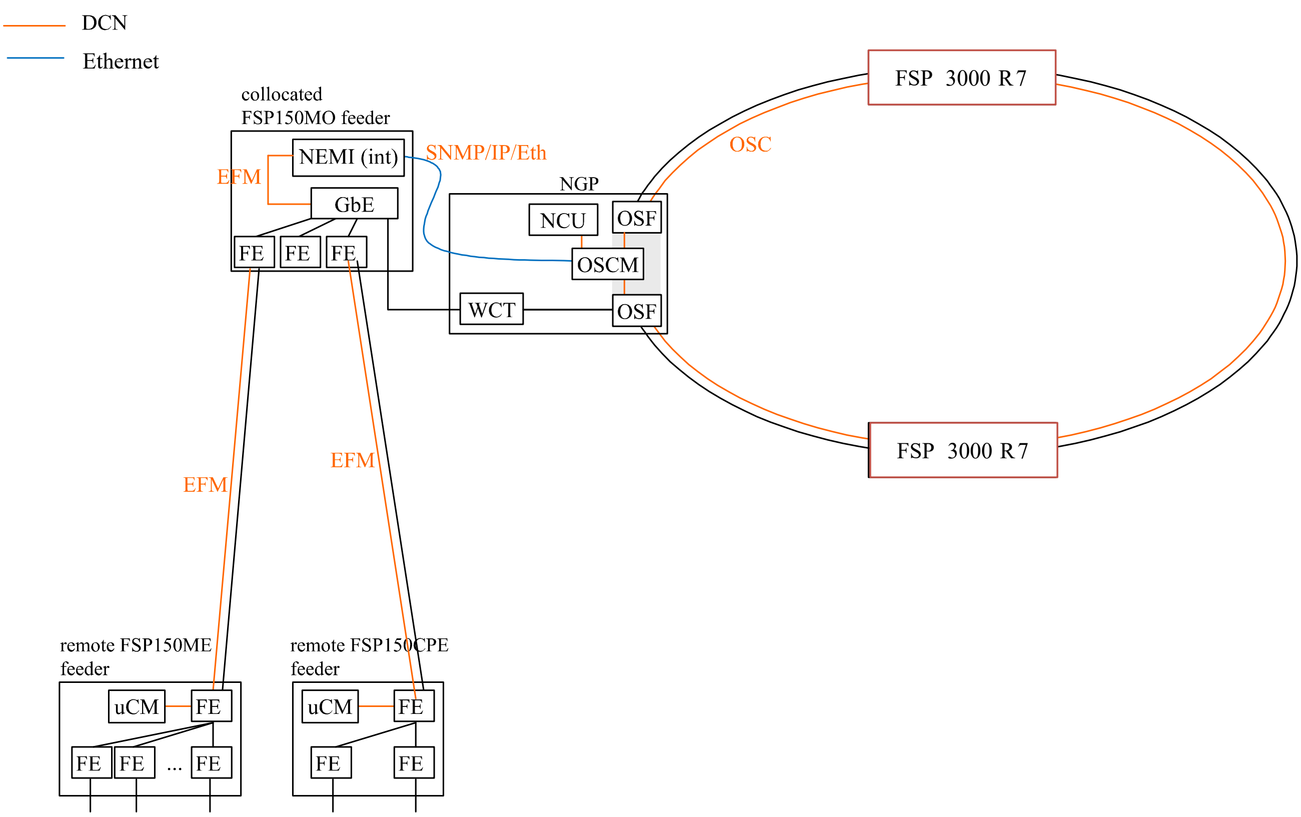
Management of an FSP 150 Feeder Cascade over Local Ethernet

Characteristics:

[1] The MCTs at either side of a wavelength span, must both be capable of and configured to extract the same ECC (e.g. both DCCr or both GCC0, etc.)

- The feeder FSP 150 management port (100BaseTX) must be attached to one of the front electrical Ethernet ports on the Fiber Service Platform 3000R7 NE (on the NCU or an OSC module). Therefore, the aggregating feeder FSP150 must either be co-located with the backbone Fiber Service Platform 3000R7 NE, or a dedicated long-haul Ethernet transport (i.e. external DCN) must be provided
- The FSP 150 must be attached to the DCN via its front Ethernet connection
- At least the first FSP 150 in the feeder cascade has to contain a NEMI to provide an SNMP/IP management interface. No management capabilities over EFM are supported in the Fiber Service Platform 3000R7

Figure 22: Feeder Cascade Over Local Ethernet

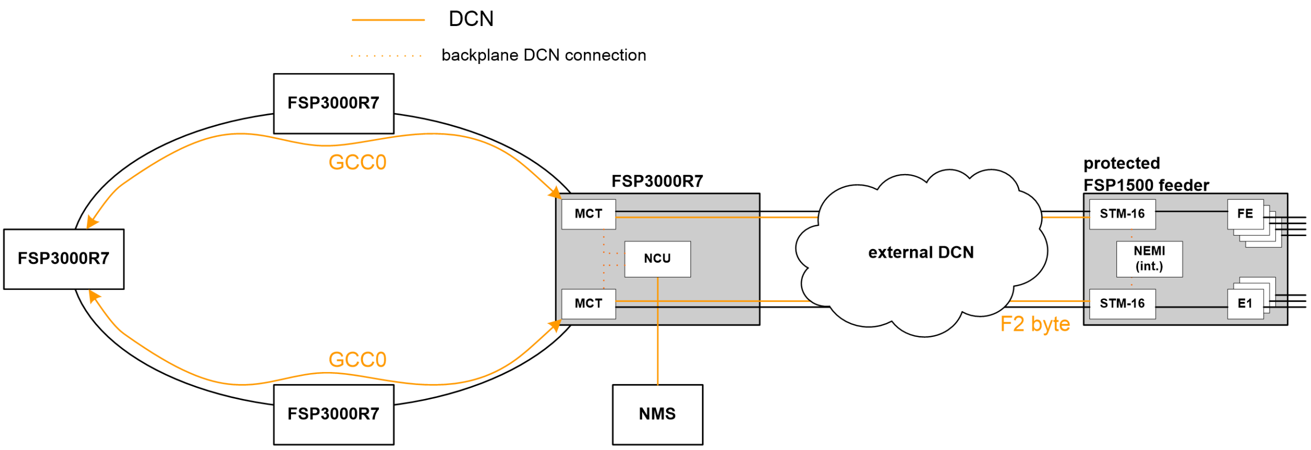


Management Across a 3rd Party SDH/SONET Network

Characteristics:

- DCCr can be used for a Siemens MSI SDH cloud.
- For other SDH clouds, the only possibility is to use the F2 byte in the path overhead (not supported).

Figure 23: Connection Over 3rd Party SDH/SONET Network



NMS Attachment Points

Every Fiber Service Platform 3000R7 equipped with an OSC module is able to function as a GNE (Layer-2 switching) towards the OSC.

Every Fiber Service Platform 3000R7 is able to also function as a GNE (Layer-3 routing) towards the DCN in general.

The NMS should be positioned near the center of the complete DCN topology and with the maximum bandwidth possible. Thus, it should preferably be connected to an Fiber Service Platform 3000R7 NE that is part of an Fiber Service Platform 3000R7 self-healing ring OSC backbone (see Layer 2: OSC Loop-Free Protection), or has DCN resiliency support otherwise.

In a large or branching DCN (e.g. one with several interconnected OSC backbones) the NMS should be attached to the backbone closest to the most central DCN location (taking the topology into consideration). This most central location is found to be the location making the number of links and/or time to reach every NE as low as possible.

Choosing this location will normally result in the lowest DCN traffic load possible, and as a consequence, the problems with latency or DCN outage caused by DCN equipment failure will be as low as possible.

DCN Resiliency and Protection

The NEs offer some DCN resiliency and protection features to cope with line breaks and equipment malfunctioning. These are discussed in the following paragraphs.

The main goal is to provide resilient connectivity between each NE and its NMS. A prerequisite for all these protection scenarios is the existence of redundant paths.

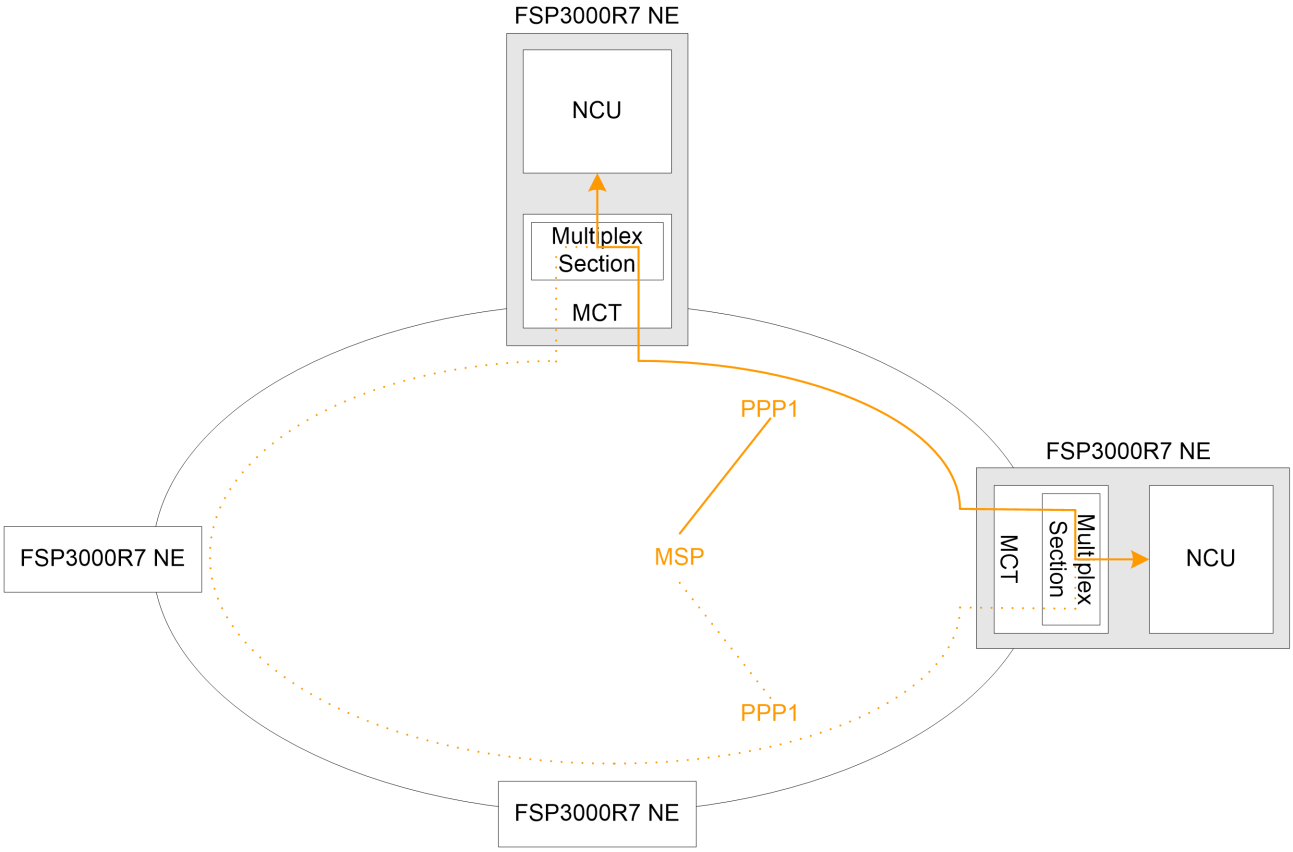
Layer 1: Line Protection/MSP

The following protection scenario is only available for a pair of Fiber Service Platform 3000R7 NEs connected by an LDCC/DCCm ECC in hot-standby mode (this pair of NEs can be anywhere in the network).

For a pair of NEs connected by an LDCC/DCCm ECC in hot-standby mode, DCN resiliency at Layer 1 is offered by means of the Line Protection (SONET) a.k.a. Multiplex Section Protection (SDH) protocol. With Line Protection/Multiplex Section Protection (MSP) the LDCC/DCCm ECC bytes are duplicated and sent both on the active and standby network port. On the receiving side, they are taken from the active port only. The bytes from the standby port are ignored. As such there is in fact only 1 ECC and this ECC is protected at Layer 1. A single PPP session is run over this ECC, resulting in a single PPP IP interface.

In case of a line break between the active ports, the standby ports at the NEs on either end switch to become active, and the ECC bytes are taken from these newly active ports. The PPP session at Layer 2 does not notice this switch-over at all, since it is extremely fast (below 50ms). Likewise, Layer-3 connectivity remains totally unaffected.

Figure 24: Layer 1 - Line Protection/MSP



Layer 2: OSC Loop-Free Protection

The following protection scenario is only available in a ring of Fiber Service Platform 3000R7 NEs managed over the OSC.

In a ring of NEs managed over the OSC, DCN resiliency at Layer 2 is offered by means of a proprietary spanning tree protocol further referred to as the "OSC Loop-Free" protocol[1].

This OSC Loop-Free protocol is based on the standard RSTP protocol, yet it does not conflict with it if:

- The (multicast) MAC addresses used for the OSC Loop-Free protocol PDUs are within the MAC address space allocated to Adtran Networks SE
- OSC Loop-Free protocol PDUs are transported on the optical ports of the OSC modules only
- OSC Loop-Free protocol PDUs are transported transparently by any standard (R)STP bridge/switch
- Standard (R)STP PDUs are transported transparently over the optical ports

Similarly to (R)STP, the OSC Loop-Free protocol:

- Sets logical breaks in Fiber Service Platform 3000R7 OSC rings to prevent loops[2]
- Removes logical breaks in Fiber Service Platform 3000R7 OSC rings to maintain connectivity between all NEs in the case of a physical break
- May function as a relatively fast (less than 1 sec.) protection protocol that implements a self-healing OSC ring when detecting loop breaks.

In addition to the OSC Loop-Free protocol running on optical ports, an instance of standard RSTP protocol runs on electrical Ethernet ports of the OSC modules. These protocols detect and break loops in the optical and electrical domain. Extreme care needs to be taken to prevent such loops as they may cause broadcast storms, bringing the entire OSC DCN down. If such loops cannot be avoided, the RSTP functionality has to be enabled from the user interface on the OSC modules. The figures below show some typical examples of such possible loops.

[1] The OSC Loop-Free protocol is not to be confused with the Topology Detection Protocol (TDP). TDP is used by and only needed for the Versatile (Group) Protection Switching functionality, distributing the number of FSP 3000R7 nodes in a (linear or ring) OSC network, their System IP addresses, and their place in the OSC network.

[2] The location of the logical break cannot be retrieved via any user interface.

Figure 25: OSC Loop-Free Protection - set logical breaks

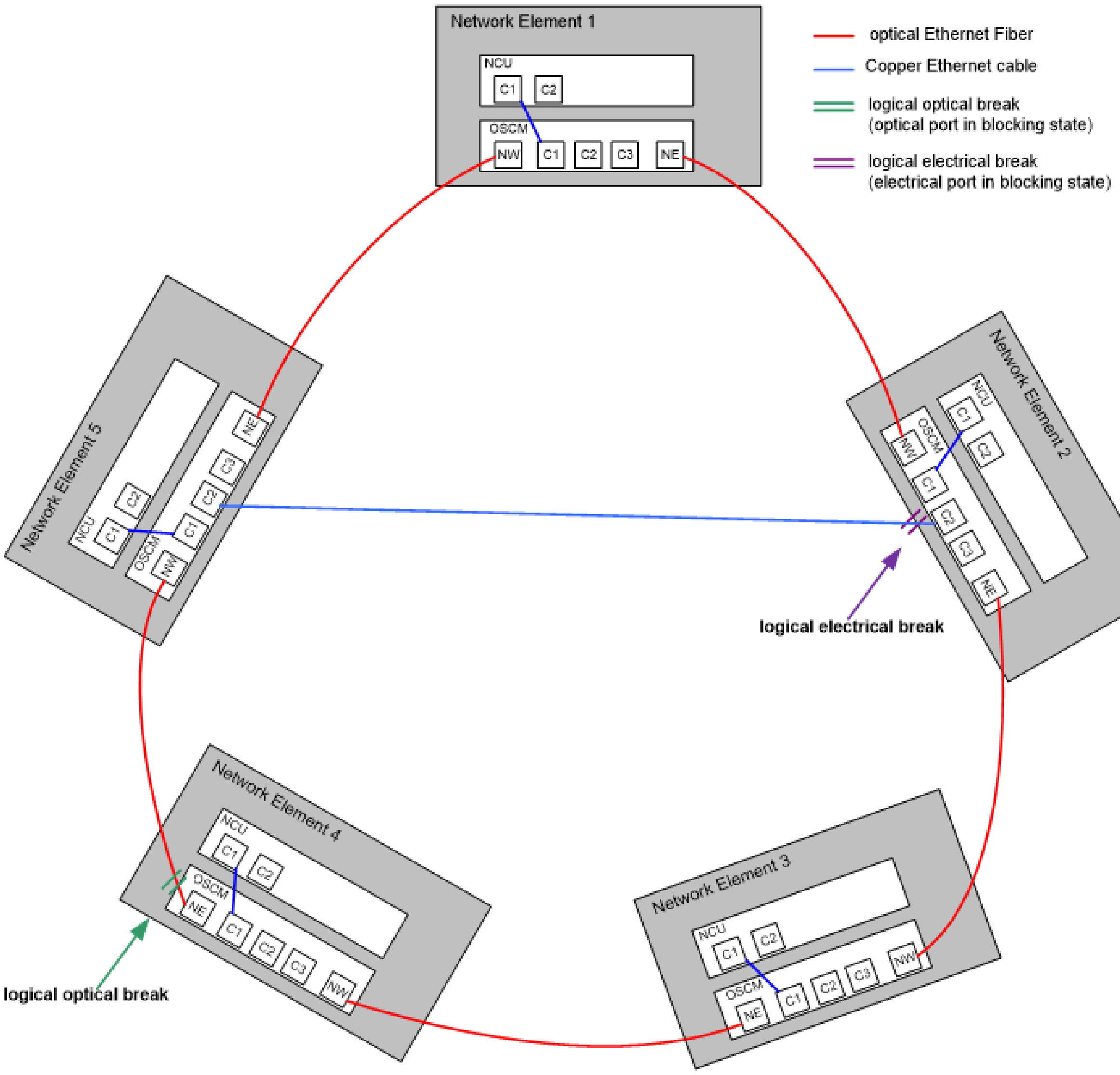


Figure 26: OSC Loop-Free Protection - logical break removed to maintain connectivity

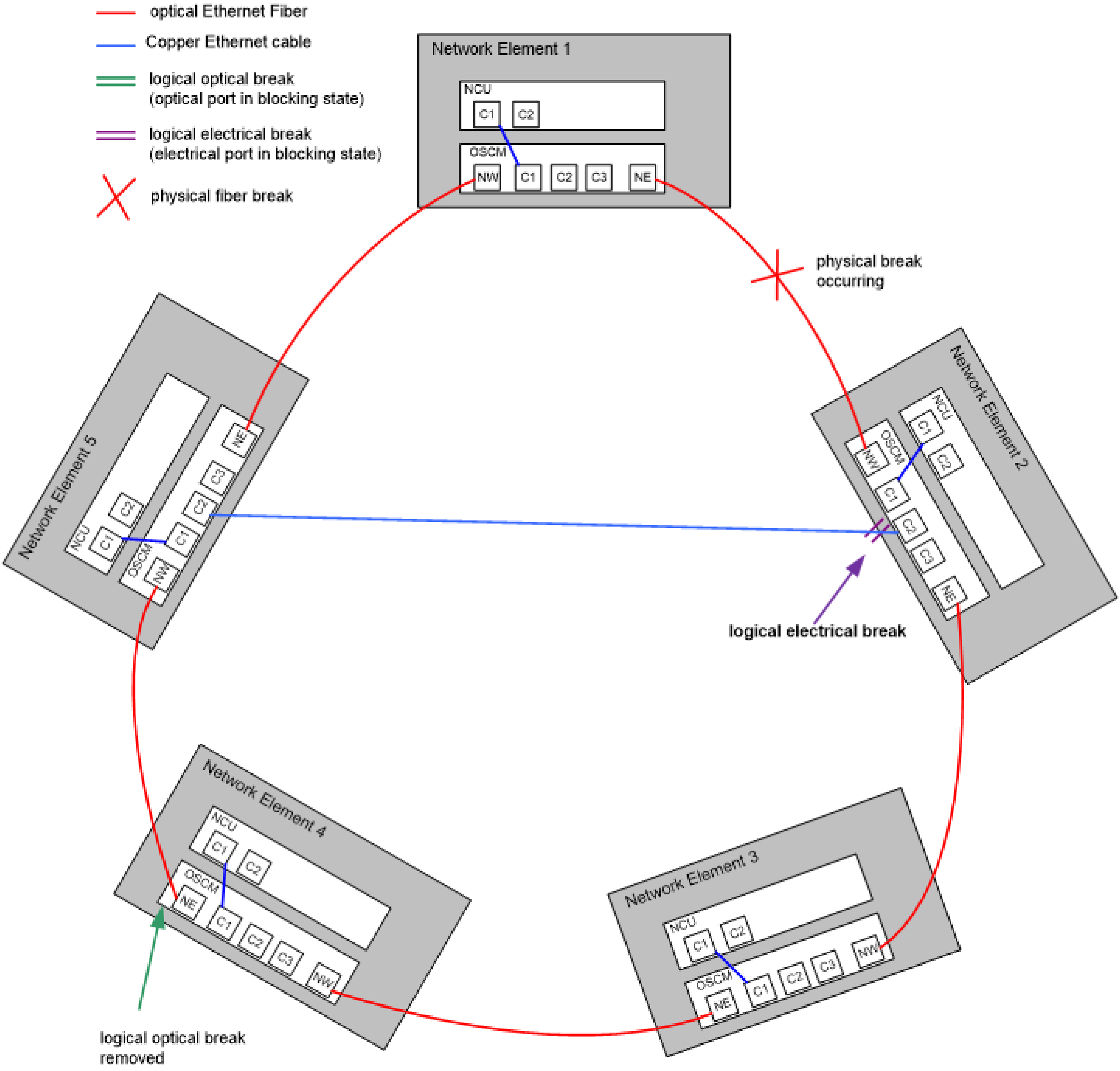
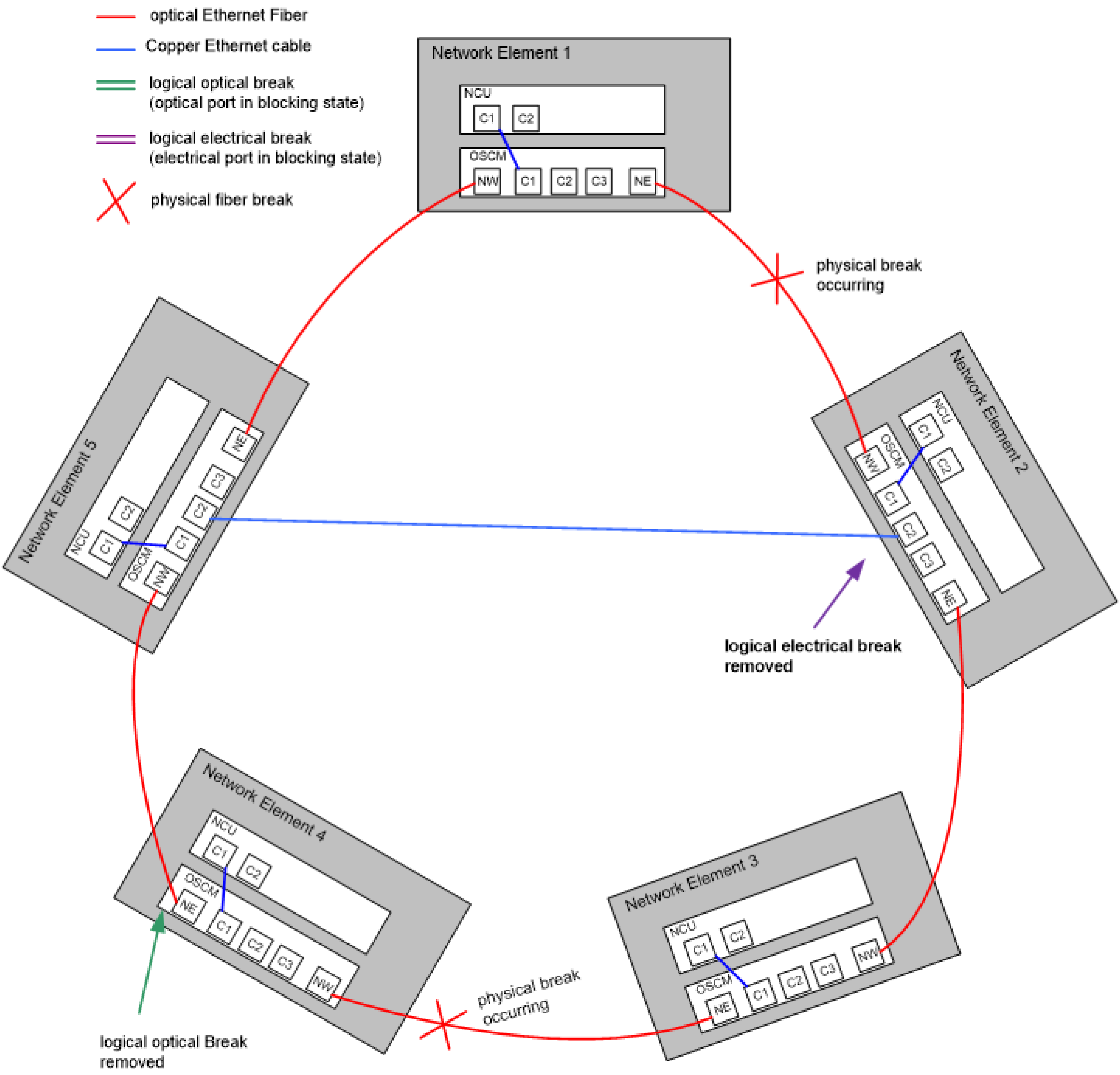


Figure 27: OSC Loop-Free Protection - multiple fiber breaks, more logical breaks removed



Notice that with regard to loop prevention, the backplane connection is equivalent to a front cable. Hence, the remark about Ethernet loops, RSTP, and broadcast storms also applies to a backplane connection. More specifically, when attaching multiple OSC modules to the same LAN-1-A-X, care must be taken to not create an Ethernet loop. It is recommended to use an OSCM with two optical interfaces instead of attaching multiple OSC modules to the same LAN-1-A-X.

Topology Detection (TDP) is only needed when Versatile Protection is used. For TDP to work it is required that the pairs of OSC modules in the ring are inter-connected by network east and network west ports. That is, the NE port of one OSC module is interconnected to the NW port of the opposite OSC module.

Layer 3: OSPFv2

The following protection scenario is generally available for all Fiber Service Platform 3000R7 NEs. At Layer 3, DCN resiliency is offered in Fiber Service Platform 3000R7 NEs by means of the standard OSPFv2 protocol.

OSPFv2 is a dynamic routing protocol for IPv4 routing capable devices such as the Fiber Service Platform 3000R7. Each router will exchange information with the other routers in the area about which neighboring routers and networks can be reached through it, and at which cost. The totality of this information can then be used by each router to calculate the optimal route (the "shortest path") to each destination, and this route is programmed into the routing table.

If at some point an IP route to a destination becomes invalid (because of a line break, etc.) then updates will be sent and each router will calculate a new IP route around the failure to the destination. This way OSPF may function as a (relatively slow) protection protocol, provided that redundant paths are present in the network. The general characteristics of OSPF in Fiber Service Platform 3000R7 have already been discussed in Dynamic Routing - OSPF.

In the following paragraphs, some topologies are described in-depth with regard to Layer-3 connectivity protection.

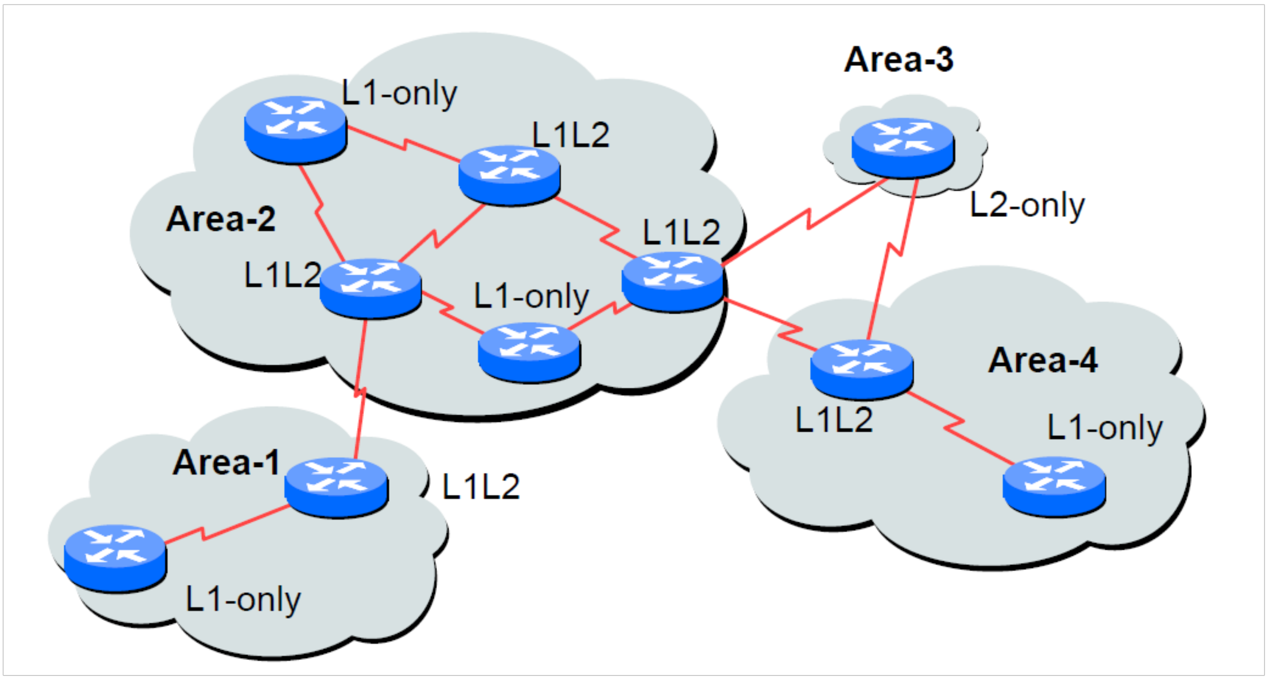
Intermediate System-to-Intermediate System (IS-IS)

Intermediate System-to-Intermediate System (IS-IS) is an Interior Gateway Protocol (IGP) that runs within an Autonomous System (AS). It uses link-state information, utilizing the shortest path first (SPF) algorithm to calculate routes. IS-IS is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. Each IS-IS router distributes information about its local state (usable interfaces and reachable neighbors, and the cost of using each interface) to other routers using the Link State PDU (LSP) messages. This information is used to build up a database containing the topology of the AS using a variant of the Dijkstra algorithm. The router is using this database as an input to populate its routing table. The topology database gets recalculated every time an AS topology change is detected. IS-IS provides a two-level hierarchy utilizing the concept of "area routing", for example, the information about the topology within a defined area of the AS is not propagated to the routers not being a part of this area.

Operation

IS-IS routing protocol has a two-level hierarchy. Level 1 routers exchange routing information with other Level-1 Routers in the same area. Routers that operate at Level 2 exchange routing information with other Level-2 devices regardless of whether they are in the same area. Contiguous Level 2-capable routers are forming the AS backbone. Routers can also operate as both (L1/L2). These routers are the gateways for their Level 1 area, used for the inter-area routing. The default configuration is both Level 1 and Level 2 at the same time which allows an IS-IS network to run with a minimal configuration in a plug-and-play fashion.

Figure 28: IS-IS Router Areas



Designated IS (DIS)

On an IS-IS broadcast network, a router must be elected as the DIS at each hierarchy level.

The main responsibilities of the DIS are:

- Creating and updating a central Link State Database (LSDB) used for reporting links to all systems on its broadcast network.
- Advertising the current state of the LSPs, as stored in the LSDB (through the Complete Sequence Number PDUs (CSNPs)).

The IS-IS routers are using the interface's configurable IS-IS DIS Priority to elect the DIS. If multiple routers in the broadcast network have the same highest DIS priority, the router with the highest Subnetwork Point of Attachment (SNPA) address becomes the DIS. SNPA addresses on a broadcast network are MAC addresses associated with the router’s interface. The DIS election is preemptive i.e. at a specific point in time, there can only be one DIS, and every new IS-IS router with a higher IS-IS DIS Priority will take over this role.

Using NCU Management LAN and Links

The NCU supports management LAN and links to other modules in HD shelves that connect to the Network Manager, such as ENC, other NEs, or the ECM. All of these connections share the complete LAN and link capacity:

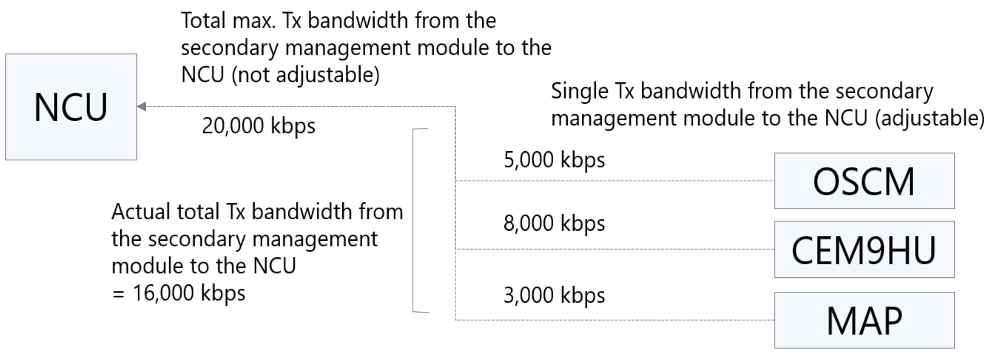
- For the NCU-II and NCU-II-P module, the total management LAN and link capacity is 20,000 kbps.
- For the NCU-3 module, the total management LAN and link capacity is 80,000 kbps.

You can view the used and maximum LAN and link bandwidth in the **System** panel: **Overview** > **Management Network** > **System**.

For more details, see Management Network Limitations.

The NCU supports an unlimited data rate to other modules. The SCU supports unlimited bandwidth in either direction, transmit and receive. For other modules that support these connections, you can adjust the Tx bandwidth.

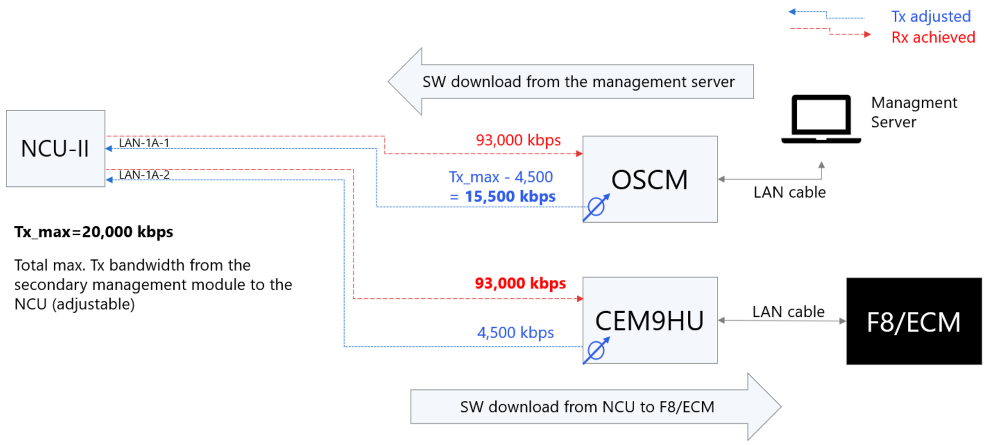
Figure 29: Bandwidth Sharing Example


Total max. Tx bandwidth from the secondary management module to the NCU (not adjustable)
NCU
20,000 kbps
Single Tx bandwidth from the secondary management module to the NCU (adjustable)
5,000 kbps
OSCM
8,000 kbps
CEM9HU
3,000 kbps
MAP
Actual total Tx bandwidth from the secondary management module to the NCU = 16,000 kbps

Recommendation:

- Save the bandwidth on modules that carry heavy management traffic in the Rx direction. For example, use the CEM9HU, which has a physical connection, to an ECM for file transfer from the NCU to the ECM.
- Use the remaining bandwidth for other modules that carry heavy management traffic in Tx direction. For example, use the OSCM, which has a physical connection to the file server, for file downloads from the external file server to the NCU.

Figure 30: Recommended Use Example



To adjust the backplane transmission rate, complete these steps:

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf and module.
3. In the main pane, select the applicable module to open the **Configure Details** window.
4. In the **Configure Details** window, **Basic** area, **Max Tx Rate [kbps]** field, enter the value.
5. Click **Apply & Exit**.

Provisioning the Management Network

Complete these steps on each node in the network and set parameters according to your network plan.

If you are using the Message-Digest algorithm 5 (MD5) for Open Shortest Path First (OSPF) authentication, you must disable OSPF extensions (i.e. Cisco Link Level Signaling (LLS)). Only 1 authentication key is supported, KEYID 1.

1. Select **Overview** > **Management Network** > **System**.
2. In the **System** area, enter values in these fields:
   a. **IP Operation**
   b. **IP Address**
   c. **IP Mask**
   d. **Default Gateway**
   e. **IPv6 Default Gateway**

> **LAN/Link Bandwidth Used [kbps]** and **LAN/Link Bandwidth Max [kbps]** provide information about the NCU bandwidth for supporting management LAN and links that might affect their provisioning.

3. Click **Apply**.
4. In the **Routes** area, click **Add** to enter any explicit routes required by your planning guide.
5. In the **Routes for IPv6** area, click **Add** to enter any IPv6 routes required by your planning guide.
6. Select **Management Network** > **Interfaces**.
7. In the **Management Ports** area, click **Add** or modify NCU, OSCM, UTM or CEM/9HU ports, as required by your planning guide.
8. In the **Management Channels** area, embedded communication channels (ECC) may be provisioned after the modules and ports (services) are provisioned under **Configure**.

9. In the **Management LANs** area, click **Add** to provision backplane LANs and connect to modules or ports as required by your planning guide. OSCM, CEM/9HU, and UTM modules can be connected with these LAN connections to the NCU. OSCM modules may also be connected to the NCU with Ethernet cables.
10. In the **Management Links to Module Management Channels** area, ECC may be linked to the NCU to establish the communication path from the ECC to the Management Network.
11. Select **Management Network** > **OSPF**.
12. In the **OSPF Areas** area, click **Add** to enter any OSPF areas required by your planning guide.
13. Select **Management Network** > **IS-IS**.
14. In the **IS-IS** area, configure the IS-IS Routing as required by your planning guide.

Provisioning IP Operation

This section contains these topics:

Background

To manage communication outside of the network, you can provision the node to support IPv4 addresses, the default, for both IPv4 and IPv6 addresses. Intra-network communication supports only IPv4.

IPv4 is a connectionless protocol for packet-switched networks and uses 32-bit addresses. IPv6 uses 128-bit addresses. These two protocols differ and can communicate only indirectly. However, service providers must continue to support both protocols transparently to their customers.

Network node equipment can support both protocols by using a dual-stack solution. This method uses network interfaces that can originate and understand both IPv4 and IPv6 packets. ADVA node equipment supports dual-stack operation.

The next section describes how to provision IPv6 addresses.

Provisioning IP Operation

Complete these steps to set the node to support IPv6. The default is IPv4.

You must have a user account with admin rights to complete this procedure.

1. Select **Overview > Management Network** > **System**.
2. In the **System** area, **IP Operation** field, select **IPv4 and IPv6**.
3. In the **IPv6 Default Gateway** field, enter the appropriate IP address.

4. Click **Apply**.
5. Restart the node.

Provisioning the Domain Name System

Complete these steps to provision a Domain Name System (DNS). You can use domain names instead of IP addresses when you configure the Public Key Infrastructure (PKI).

1. Select **Overview** > **Management Network** > **System**.
2. In the **Domain Name System (DNS)** area, complete these fields:
   - **DNS Operation**: select this field.
   - **DNS server**: select the applicable servers.
   - Click **Apply**.

> Only PKI servers support DNS.

Resolving ECM Database Mismatch

To resolve an ECM database mismatch:

1. Select **Overview**.
2. Select **Management Network** > **Interfaces**.
3. In the **Management of HD Shelves** area, select the proper row and click **Resolve**.
4. In the **Resolve Database Mismatch** window:
   - Select **Restore From File** to restore the database from a valid file provided by the user.
   - Select **Accept Current** to accept the current ECM database and reboot. This option is service affecting and will interrupt the traffic.
   - Select **Reset To Factory** to perform a restore to factory database and reboot. This option is service affecting and will interrupt the traffic.
5. Click **Resolve**.

Configuring OSC Modules

1. Select **Overview** > **Management Network** > **Interfaces**.
2. In the **Management LANs** area:
   a. Click **Add**.
   b. In the **Identifier** area, select an identifier.

   c. In the **Add Facility** window, complete the fields as specified in your network plan.
   d. Click **Add**.

3. Add management LAN members according to your network plan:
   a. Select **Configure**.
   b. In the navigation tree, click the top area to access module details for an OSCM module in Shelf 1.
   a. In the **Management LAN** field, select an option.
   c. Repeat this process for all modules in Shelf 1.
4. Restart the node as described in Restarting the NCU

Redundant Controllers

This section contains information about FSP 3000R7 redundant controllers for the node and shelf control units (NCU-II-P and SCU-II), which support the high availability feature. Redundant controllers protect the FSP 3000R7 equipment against failures of the NCU-II-P and SCU-II hardware or software components.

Redundancy for the NCU allows the user to access and manage the node by using the SNMP, Network Element Director, Craft, or TL1 management interfaces. In the event of a controller failure, availability is maintained when the standby controller becomes the active controller.

This section includes the following topics:

High Availability Features and Capabilities

These NCU-II-P features support the high availability:

- Front panel LEDs indicate whether the controller is active or standby.
- Support NCU-II-P switch-over:
  - Front panel button.
  - User command.
- Support fail-over when the active controller has a failure.
- Generate an alarm (partner not available) to indicate when a controller is not protected.
- Support switch-over inhibit via the user for NCU-II-P interfaces .
- Automatically synchronize database changes between NCU-II-Ps.

The NCU-II-P module supports management control within the node. These controllers operate as either the active or standby controller. The active controller allows the user to manage the node, collect monitoring information, and report alarms. The standby controller is powered up and waits in standby mode. The module is ready to become active in the event of a failure or on request by the user. The NCU-II-P supports cold standby and requires minutes for the switch-over to complete restoring management control. The switch-over time depends on the size and configuration of the NE. The switch-over interval does not affect or lose traffic.

Controller Placement

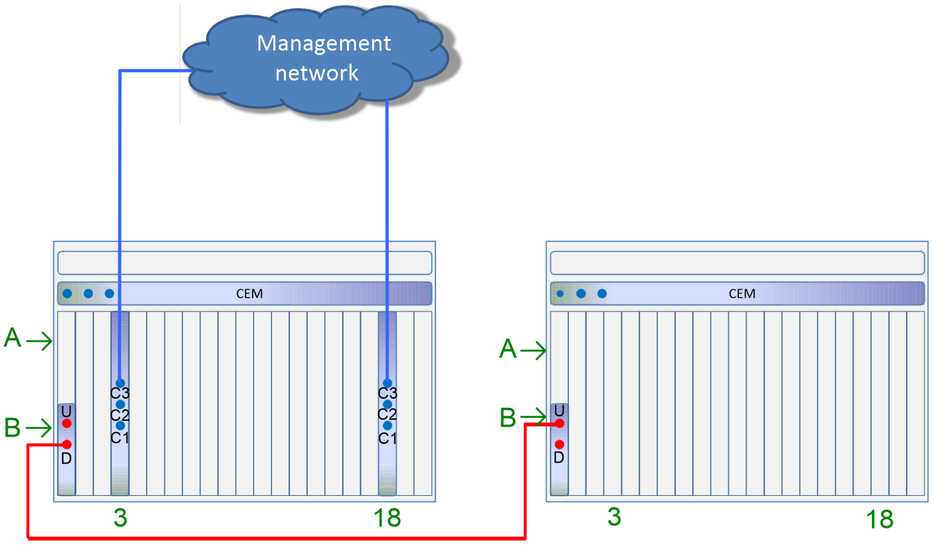
The master shelf in a multi-shelf high availability configuration must contain redundant NCU-II-Ps, regardless of whether one or two SCU-IIs are used per sub-shelf.

> Nodes with redundant SCU-IIs in all shelves are limited to 20 shelves maximum.

Up to release 11.2.2, you must place SCU-IIs in slot B in both the master shelf and sub-shelves, regardless of whether you are incorporating high availability redundant node controllers (NCU-II-P) or not. From Release 11.2.2 onward, if high availability is being incorporated, you must place SCU-IIs in both slots A and B, and node controllers (NCU-II-P) in slots 3 and 18 of the master shelf, in order to achieve full redundancy.

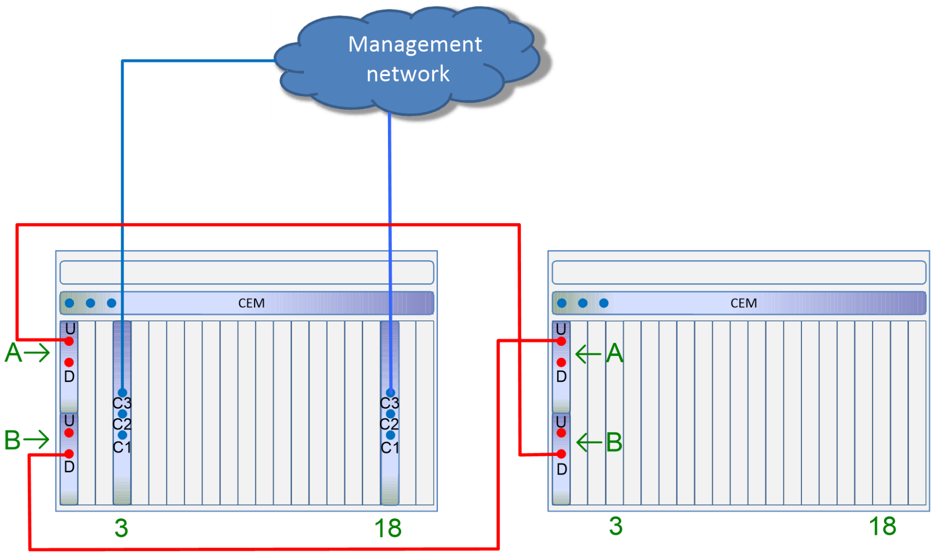
The next figure illustrates the system configuration before Release 11.2.2. Redundant node controllers are connected to the management network from their Ethernet client (C) ports. Shelf controllers are connected from their (U) and (D) ports between SCU-IIs in slot B from the master shelf to a sub-shelf.

Figure 31: High Availability Redundant NCU-II-Ps and Single SCU-IIs



The next figure illustrates the system configuration after Release 11.2.2. After this release, you must place SCU-IIs in slots A and B and redundant NCU-II-Ps in the master shelf, slots 3 and 18 to achieve the highest level of redundancy. This configuration removes any single point of failure of the node and shelf control units.

Figure 32: High Availability Redundant NCU-II-Ps and SCU-IIs



You can make connections to the management network from both NCU-II-Ps, either to a single router, or to increase availability, to separate routers. It is recommended that you use a fully redundant management network that does not have any single points of failure. See DCN Redundancy.

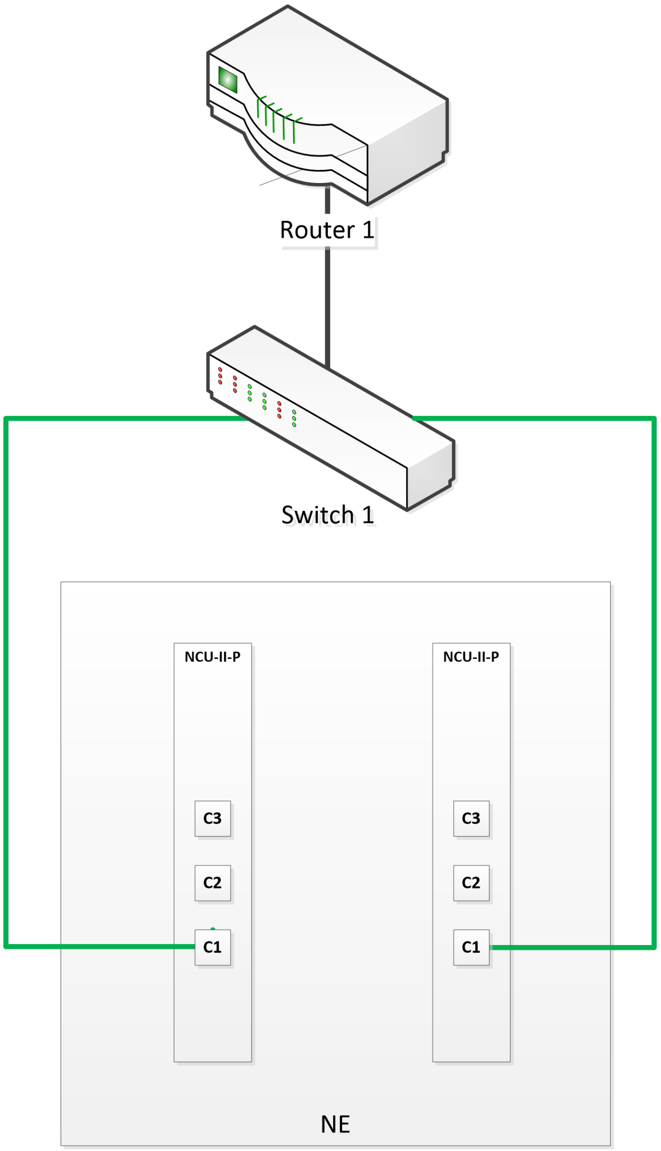
DCN Redundancy

NCU-II-Ps are designed with redundancy in mind but external DCN failures resulting from routing equipment, cabling, and network failures can decrease the high availability functionality. To resolve this issue, we offer redundant DCN configurations in the following sections that you can install in your network.

Basic Configuration Without DCN Redundancy

ADVA does not recommend the most basic configuration, which does not provide any DCN redundancy. It is an example to illustrate the single points of failure in the following sections.

Figure 33: Basic Configuration Without DCN Redundancy



This configuration only protects the Network Element (NE) from an NCU-II-P hardware or software failure.

Reliability

This configuration does not protect the NE from single points of failure. The disadvantages are:

- NCU-II-P cabling failure (single cable).
- Switch failure (single switch).
- Router failure (single router).
- General network failure (single network).

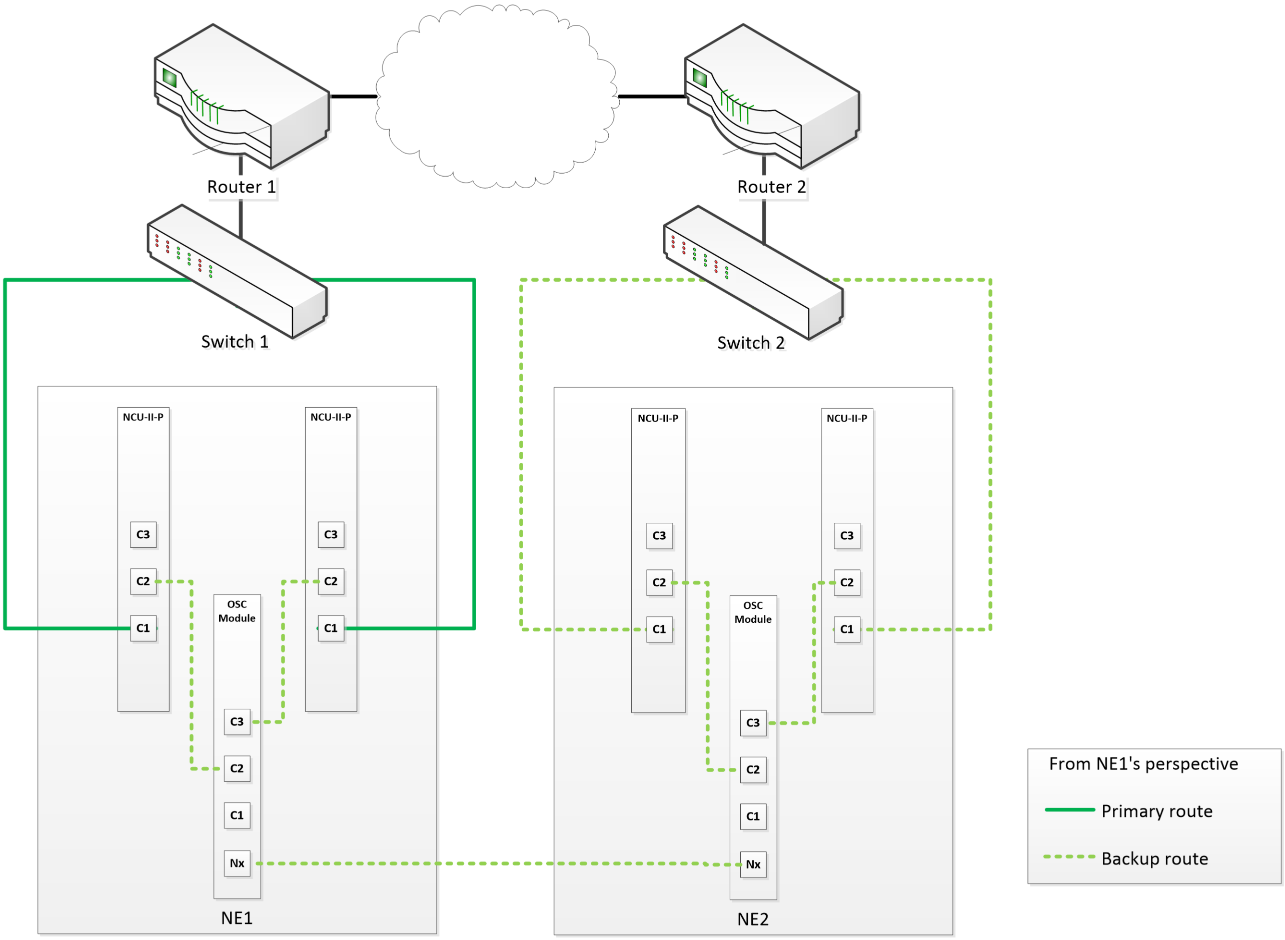
Variants

- Use two routers to work in a redundant configuration to protect from router failure.
- Use two switches to work in a redundant configuration to protect from switch failure.
  - Only if the switch is connected to the standby NCU-II-P.
  - If the switch is connected to an active NCU-II-P, you would still lose connectivity.

Using OSC Modules

This configuration requires at least two NEs that interconnect using OSC modules.

Figure 34: NEs With Interconnected OSC Modules



In this example, the OSPF configuration is for a single area. The NCU-II-Ps can manage only 600 routes in the routing table. For that reason, you must protect the NCU-II-P from the OSPF route distribution. Review these guidelines.

- On routers 1 and 2, OSPF is enabled on the ports that associate with the NCU-II-Ps.
- If STP/RSTP is enabled on switches 1 and 2, you must configure the switch ports that connect to the NCU-II-Ps as STP/RSTP EDGE ports. For example, configure the ports using a Cisco PortFast setting. This setting is necessary because FSP 3000R7 systems do not generate topology changes. You must use them as end devices or stations.
- On the NE 1 and 2 configurations, the NCU-II-P C1 port is numbered and has OSPF enabled. The C2 port is unnumbered with OSPF enabled.
- Configure the router without a default gateway.
    - The static route to 0.0.0.0 through the gateway must use the NCU-II-P C1 port. The port must have a metric that is greater than the default gateway metric that the router distributes.
    - If the router distributes the default gateway, the default gateway must be the same on all of the interconnected NEs.
    - The routing metric on the NCU-II-P C2 port must be greater than 0.

VLAN Support

All management modules with an Optical Supervisory Channel (OSC) support a VLAN subnetwork. Amplifiers with OSC also support VLAN.

The OSC channel receives a VLAN tag from the external device with a value of 1 to 4095, and then transmits this value to the other modules. The card on the other end of the channel receives each VLAN tag with a value of 1 to 4095. The OSCM-PN electrical ports ignore the tags and pass all frames between their own optical and backplane ports. Because of port limitations, to transmit frames from the OSC channel to the Ethernet port, you must set the transmission rate to 100 Mbps. You must set the parameter MTU [Byte] to 1400 on the NCU configuration settings.

Reliability

This configuration protects the NE from:

- NCU-II-P failure SW/HW: The NCU-II-P high availability functionality protects the NE from this failure.
- NCU-II-P cabling failure (single cable).
    - A second means of communication protects the NE by setting the OSC module to OSPF enabled.
    - Without OSPF, this node is reachable only by hop to hop.
- Switch failure (single switch).
    - A second means of communication protects the NE by setting the OSC module to OSPF enabled.
    - Without OSPF, this node is reachable only by hop to hop.
- Router failure (single router): Using OSPF on the routers and NEs protects this NE.

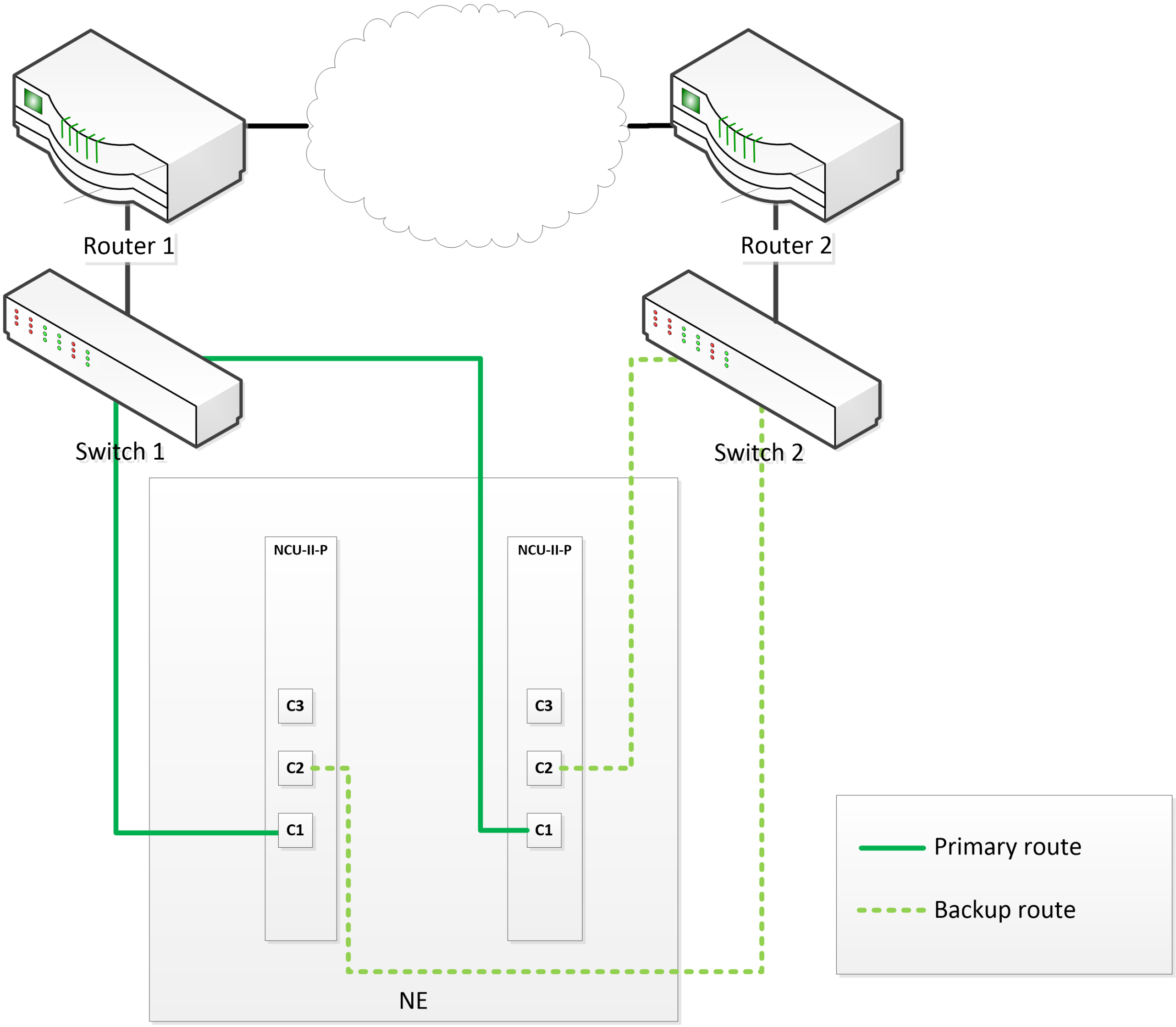
Variants

- No OSPF on the router and NCU-II-P.
  - The advantage is that no router configuration change is required.
  - The disadvantage is that a single point of failure introduced on the NE-to-router connection has no protection against cabling and switch failures.
- Disabling the static route redistribution.
  - The disadvantage is the introduction of a single point of failure on the NE-to-router connection, which does not protect against cabling failures.
  - The disadvantage is that if more than two NEs connect to the OSC ring, you must provision each static route to point to the OSC ring.
- Using a single router.
  - The advantage is that of using only one router instead of two.
  - The disadvantage is the introduction of a single point of failure on the router.
- Using a single switch.
  - The advantage is using one switch instead of two.
  - The disadvantage is the introduction of a single point of failure on the switch.

Using Redundant NCU Front Panel Connection

This configuration uses only the NCU-II-P front ports for management connectivity. Only one NE is required.

Figure 35:   NCU-II-P Front Panel Connection



In this scenario, you configure OSPF for a single area. You need to protect the NCU-II-Ps from receiving route distribution from OSPF since they can only handle 600 routes in the routing table. Make sure:

- For Routers 1 and 2 you enable OSPF on the ports that are associated with the NCU-II-Ps.
- In case Switches 1 and 2 have STP/RSTP enabled, you configure the switch ports that are connected to the NCU-II-Ps as STP/RSTP EDGE ports (i.e.Cisco PortFast setting), because FSP 3000R7 systems do not generate topology changes and should be treated as end devices/stations.

NE is configured like this:

- NCU-II-P C1 port numbered, OSPF enabled and OSPF Area X.
- NCU-II-P C2 port numbered, OSPF enabled and OSPF Area X.

You must set routing for no default gateway.

- Static route to 0.0.0.0 through gateway must use the NCU-II-P C1 port with a metric higher than the default gateway’s metrics distributed from the routers.
  - You will have two static routes if the routers distribute the default gateway. It must be the same on all of the interconnected NEs.
- Static route to 0.0.0.0 through gateway must use the NCU-II-P C2 port with a metric higher than the default gateway’s metric set for the NCU-II-P C1 static route.

Reliability

This configuration protects the NE from:

- NCU-II-P failure SW/HW.
  - Protected by the NCU-II-P’s high availability functionality.
- NCU-II-P cabling failure (single cable).
  - Protected by using a second NCU-II-P port with OSPF enabled.
  - Without OSPF, the node can only be reached via the NCU-II-P C2 port's IP address because the System IP is not reachable.
- Switch failure (single switch).
  - Protected by using a second NCU-II-P port with OSPF enabled.
  - Without OSPF the node can only be reached via the NCU-II-P C2 port's IP address because System IP is not reachable.
- Router failure (single router).
  - Protected by using OSPF on the routers and NE.

Variants

- No OSPF on the router and NCU-II-P.
  - The advantage is that no router configuration change is required.
  - The disadvantage is a single point of failure introduced on the NE-to-router connection (not protecting against cabling and switch failures).
- Using single router.
  - The advantage is only using one router instead of two.
  - The disadvantage is the introduction of a single point of failure to the router.
- Using single switch.
  - The advantage is using one switch instead of two.
  - The disadvantage is introducing a single point of failure to the switch.

Summary

The redundant NCU-II-P front panel connection method has several advantages over using the OSC module connection method:

- Fewer modules, connections, switch ports, fiber connections, IP addresses.
- No OSPF static routes are required.

The differences in the two configurations are listed below.

OSC module connection method:

- DCN Modules in node required.
- Connection to a different node required.
- Two switch ports are required per node.
- Two fibers are required per node (both transmit and receive).
- Four patch cords are required per node (two front plane and back plane OSC connections).
- Static routing configuration is required on the NCU.
- Two IP addresses are required per node (C1 and the system IP address).
- One OSPF area used.
- OSPF static routes redistribution recommended.

NCU-II-P front panel connection method:

- No DCN modules are required in the node.
- No connection is required to a different node.
- Four switch ports are required per node.
- Zero fibers are required.
- Four patch cords are required per node.
- Static routing configuration is required on the NCU.
- Three IP addresses are required per node (C1, C2, and the system IP address).
- One OSPF area is used.
- OSPF static route redistribution is not required.

For information about how to provision these DCN redundancy configurations, refer to the *Provisioning and Operations Manual.*

State Summary

State Summary displays the **Admin**, **Operational**, and **Equipment States** for all module entities in a shelf. Use this view to determine the status of modules and root cause of issues. The **State Summary** also provides the entity hierarchy, which can help you understand entity relationships.

> Place the cursor over shelves, modules, or plugs to display the equipment type. Place the cursor over other entities to display facility type.

1. Select **Overview**.
2. Select **State Summary**.
3. Select the shelf number from the **Shelf** list.

> Click **Refresh** to update the parameters in **State Summary**.

Port Summary

Port Summary displays on overview of configured ports on the node. Information including **Admin State**, **Operational State**, **User Label**, **Termination Level**, **Auto Laser Shutdown** and **Error Forwarding Mode** is displayed. **Port Summary** can be useful to find which port(s) support a customer when the user labels are entered.

You can find **Port Summary** under **Overview > Port Summary**.

Search

You can use the **Search by all columns** field to filter the table to the text entered in the field.

For more precise search you can use Regular Expressions.

^	string starts with
$	string ends with
.	any character
*****	0 or more characters

+	1 or more characters
|	or

For example:

- Network ports: -N.*$
- Client ports: -C.*\d$
- Network channels: ^(CH|ETH).+-N.*$
- Client channels: ^(CH|ETH).+-C.*\d$

Using Resource Analyzer

Use **Resource Analyzer** on the node where the control plane path computation fails. Usually, path computation failures are caused by missing or incorrect physical connections. The path display stops where a physical connection is missing. An incorrect fiber entry causes the path to be routed to the incorrect equipment. Path computation can also fail when a required resource is already in use. For example, if a channel or cross-connect is already assigned, control plane will reject the request and send out a channel blocking error code.

Resource Analyzer can also be used to ensure the path in the node is available and the physical connections are entered before executing the control plane.

Complete these steps to use **Resource Analyzer**:

1. Select **Overview**.
2. Select **Diagnostics > Resource Analyzer**.
3. Select the **End Point Types**.
4. Select the **End Points**.
5. Select a **Channel**.
6. The path is displayed to the extent possible from each end point in the lower portion of the **Main Pane**.
7. If the path computation fails because a required resource is in use, **Blocking Resources** will be accessible.
8. Click **Blocking Resources** to see which required resource is in use.

Analyzing Physical Connections (Fiber Map)

The **Fiber Map** diagnostics tool analyzes **Physical Connections** to identify missing or improper connections.

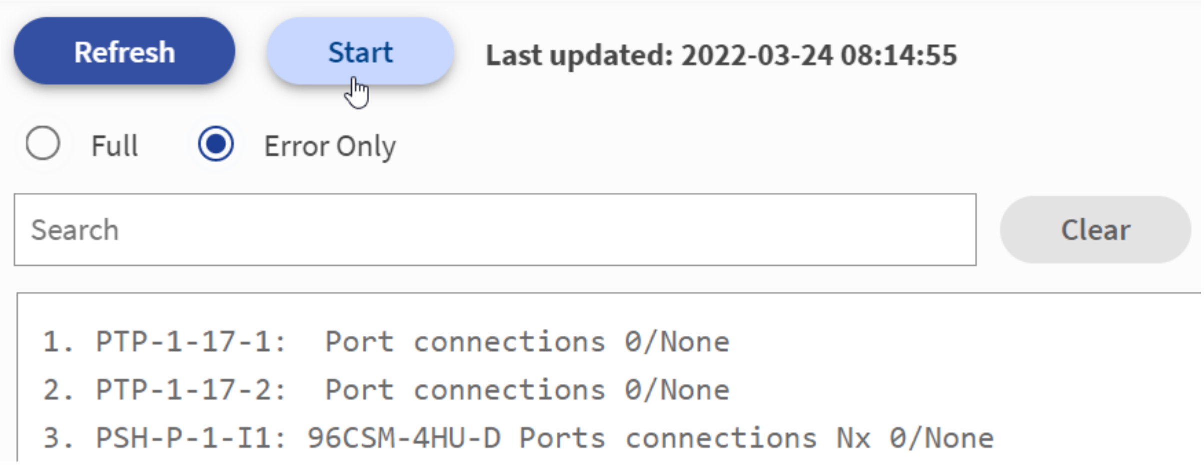
	When Physical Connections have been entered correctly, you should see no messages in this window. This tool limits the number of messages to 101. If you receive 101 error messages, then troubleshoot the cause and run the diagnostic again.

To use the tool, complete these steps:

1. Select **Overview**.
2. Select **Diagnostics > Fiber Map**.
3. Click **Start**.

   To see a list of all physical connections, select **Full**. To only view errors, select **Error Only**.

To filter the results, enter a search term as shown below:



Last updated: 2022-03-24 08:14:55

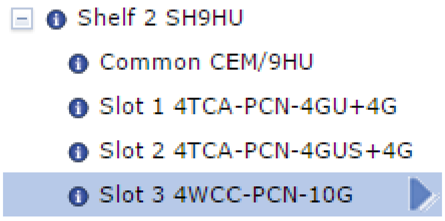
```
1. PTP-1-17-1:  Port connections 0/None
2. PTP-1-17-2:  Port connections 0/None
3. PSH-P-1-I1: 96CSM-4HU-D Ports connections Nx 0/None
```

	The filter is case-sensitive; it will match connections, but not Connections.

Fixing Errors

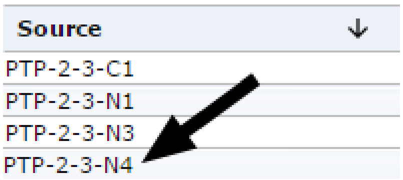
Assuming the PTP-2-3-N4 identifier shown in the example above, fix the error by completing these steps:

1. Select **Configure**.
2. Navigate to the affected item in the **Equipment View** under **Shelf 2 > Slot 3**.



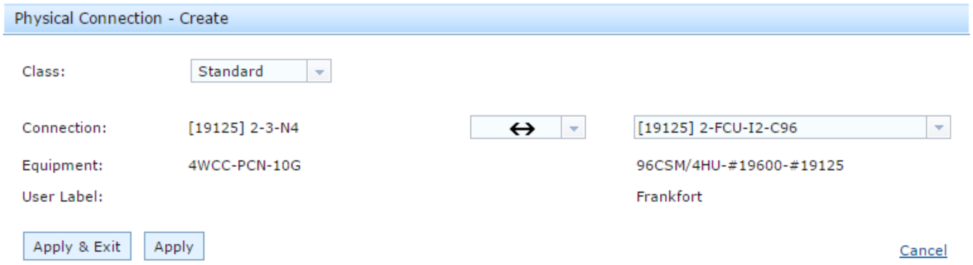
Shelf 2 SH9HU
Common CEM/9HU
Slot 1 4TCA-PCN-4GU+4G
Slot 2 4TCA-PCN-4GUS+4G
Slot 3 4WCC-PCN-10G

3. Inside the **Physical Connection** area, click the row containing PTP-2-3-N4.



Source
PTP-2-3-C1
PTP-2-3-N1
PTP-2-3-N3
PTP-2-3-N4

4. Connect the N port to another port in the **Connection** field, according to your network plan.



Physical Connection - Create

Class:	Standard		
Connection:	[19125] 2-3-N4	↔	[19125] 2-FCU-I2-C96
Equipment:	4WCC-PCN-10G		96CSM/4HU-#19600-#19125
User Label:			Frankfort

5. Click **Apply & Exit**.

ROADM Connections

ROADM Connections displays an overview of configured ROADM connections on the node. Information including **Channel**, **Identifier**, **Admin State**, **State**, **Local Port**, **Connection**, **Linked Port**, **Bandwidth / Facility** and **User Label** is displayed. **ROADM Connections** can be useful to find where the ROADM connections go to. To see details about a ROADM connection, click the row of your interest to expand it.

You can find **ROADM Connections** under **Overview > ROADM Connections**.

Searching

You can use the **Search** field to filter the table to the text entered in the field. You can click **Clear** to clear the search field.

Refreshing

You can click the **Refresh** button, to refresh the list of ROADM connections.

Sorting

The information is sorted by the **Channel** column by the default. To sort the view differently, click the desired column. To change the order from ascending to descending, click the same column again.

Editing

1. Click **Edit**.
2. Change the available fields in accordance with your network plan.

> Editable fields are available when the connection is expanded and Edit selected.

3. Click **Apply**
   - or -
   Apply & Exit
   - or -
   Cancel.

Exporting

You can export the ROADM connections to a CSV file. To do that, click **Export**. The file will be saved in your browsers default download directory.

Printing

You can print the ROADM connections. To do that, click **Print**.

Manually Assigning Logical Interfaces to Optical Lines

An optical line is the data plane representation of a physical network fiber connected to an NE. The control plane needs optical lines to represent the connections in an the IP network. The control plan uses the IP network for:

- Topology and resource auto discovery.
- Path computation.
- Signaling.
- Resource management.

An optical line represents a network fiber for WDM transport.

A pair of optical line entities (OLs) represents an optical line transporting WDM traffic.

To enable control plane, you need to create the logical interface entities at each end of an optical line. The exception is when you use the VSM/RSM module. In this case, there is only one LIF-CP needed for both ends of an optical line.

Each logical interface entity holds the required IP information of:

- The optical line endpoints (OL entities).
- The management network (DCN) interface through which information about the corresponding optical line will be discovered.

> If you configure Control Plane using TID node name syntax, a System ID change for any NE using Control Plane with TID is not supported. Changing the system ID causes LIF CPs / TNLs WDM / TNLs OTN / PATHs WDM / PATHs OTN to have old TIDs that no longer exist in the network. This change may also affect services discovery by the ENC.
>
> Before a System ID change, you have to delete all Control Plane entities (TNL_WDM, TNL_OTN, PATH_OTN, PATH_WDM, and LIF_CP) whether you use the abandon procedure or not and recreate them.

Complete the following procedure to manually create Logical Interface Entities.

1. Select **Node** > **General** > **Controls**.
2. In the **Network Control** area, **Control Plane** field select **Enable**.
3. Select **Overview** > **Control Plane** > **Logical Interfaces CP**.
4. In the **Logical Interfaces** area, click **Add**.
5. In the **Create: LIF-CP** area, select the logical interface entity access identifier from the list.

> It is recommended to select the logical interface entity access identifier that matches the OL entity access identifier that it shall be associated with.

6. Click **Next**.
7. Select **Facility Type** from the list.

> It is recommended to use unnumbered logical interfaces. Numbered logical interfaces should only be used if a DCN plan requiring numbered interfaces has been developed and is in place.

If you use numbered logical interfaces for a DCN plan, see Using Numbered IP Configuration for DCN Plan.

If you use unnumbered logical interface, continue with these steps:

1. Click **Next**.
2. Select the **Management Interface** from the list. You can select one of these interfaces:
   - An external DCN channel, selectable as an SC-<shelf>-<slot>-{C|C1|C2} entity on the NCU.
   - An OSC channel, selectable as an SC-<shelf>-<slot>-{NW|NW} entity on the OSCM-PN module.
     It is required that a reference on the module is provisioned to a LAN-1-A-# entity on the NCU or to the SC-1-A-{C|C1|C2} copper Ethernet ports on the NCU (front cable option).
   - An external DCN channel, selectable as an SC-<shelf>-<slot>-{C1|C2|C3} entity on the UTM or CEM/9HU module.
     It is required that a reference is provisioned on the module to a LAN-1-A# entity on the NCU module.
   - An ECC (EOC-x-y-z) based LIF-CP.
3. Select the **TE Switch Level** from the list.
4. Enter the **Far End Target ID** or **Far End Node IP**.

> If someone changes the network element System IP address, the relationship to the TID you have specified for logical interface entities (LIF-CPs) on other network elements may be severed. Any affected LIF-CPs designating their FEND entities via TIDs must be removed and re-added after a change to the System IP address of a neighboring element.

> It is recommended to leave the rest of the parameters on this page to their default values. It is only necessary to edit them in special cases.

5. Click **Next**.
6. Enter the **Trans. Layer Term. Point**. The type of access identifier you enter depends on if the optical line entity is WDM or Ethernet based:
   - OL-4, which represents a WDM based optical line entity.
   - ETH-1-2-NW, which represents one endpoint of a Ethernet based optical line entity.
7. Enter **Far End TLTP (Trans Layer Term Point)**.
8. Enter **Far End Target ID** or **Far End Node IP**.

Using Numbered IP Configuration for DCN Plan

If you selected to use a numbered IP configuration, in the **Create: LIF-CP** area, continue with these steps:

1. Enter the **IP Address**.
2. Enter the **IP Mask**.

> You must have a DCN plan in place, and enter IP information according to this in order to have a functional control plane when using numbered IP interfaces.

3. Select **Management Interface** from the list.
4. Select **TE Switch Level** from the list.
5. Leave the rest of the parameters on this page to their default values. It is only necessary to edit them in special cases.
6. Click **Next**.
7. Enter the **Trans. Layer Term. Point**.
8. Set the **Admin State** to **Auto In Service**.
9. Click **Apply** then **OK**.

Configure

This section contains these topics:

Adding Shelves

Node configurations might be limited based on their equipment and shelf controllers, either NCUs or SCUs. Review this list.

Node Equipment	**Supports**
NCU-S	2 shelves, SH1HU.
NCU or NCU2E	Up to 20 shelves, SH1HU or SH7HU.
NCU-II or NCU-II-P	Up to 26 shelves.
NCU-3	Up to 40 shelves.
A redundant SCU-II in all shelves	Up to 20 shelves.
An SCU only	Shelf IDs 1 to 50.
All SCU-IIs	Shelf IDs 1 to 99.
A ROADM	Up to 20 shelves with shelf IDs 1 to 20.

1. Select **Configure**.
2. In the main pane, click **Add Shelf/Unit**.
3. See your network plan to enter all the options required for the shelf. Options vary according to the selected shelf type.

   Some configuration options populate automatically if the node recognizes the equipment.

   You cannot edit the **Shelf Height [HU]**.

4. Click **Add** to add the new shelf.
5. If multiple SCU/SCU-IIs connect in a ring, and your configuration uses an NCU-II/NCU-II-P, select **Configure > Node** > **Discover Shelf**.

You can add an **Unknown Shelf** from the **Equipment** list in the **Add/Shelf Unit** window to serve as a third-party shelf or unit. These shelves are part of the maximum shelf limit of 26 shelves that you can provision.

Adding, Changing, or Deleting High Density Shelves

Requirements

To install or connect cables to a high-density (HD) shelf, see the *FSP 3000R7 High-Density Subshelf Guide*.

Adding HD Shelves

1. Establish communication to the HD shelf, as described in Preparing to Add HD Shelves.
2. To provision the HD shelf before you install it, see Adding Shelves.
3. Assign a shelf number to the HD shelf, as described in Assigning the HD Shelf Number.

Changing HD Shelves

1. Replace the HD shelf.
2. Disassociate the HD shelf number for the shelf you plan to change. See Deassigning the HD Shelf Number.
3. Assign the shelf number to the new HD shelf, as described in Assigning the HD Shelf Number.

> If you change the HD connection password, the password also changes on each connected ECM. The software saves the changes on the NCU. If you remove the ECM from the system and place it in the spare pool, remember to reset the password to the default or set the ECM to RTF.

Deleting HD Shelves

1. Delete the HD shelf.
2. Remove the cable connection to the HD shelf.
3. To disassociate the HD shelf number with the shelf you plan to delete, proceed to Deassigning the HD Shelf Number.

> If you change the HD connection password, the password also changes on each connected ECM. The software saves the changes on the NCU. If you remove the ECM from the system and place it in the spare pool, remember to reset the password to the default or set the ECM to RTF.

Preparing to Add HD Shelves

Requirements

- The node must have an NCU-II, NCU-II-P, or later, NCU type.

Preparing Connections in Nodes With an HDSCM

> ADVA recommends that you use a cable to connect the HDSCM to the NCU between the Cx ports.

1. Connect the NCU Cx port to the HDSCM Cx port.
2. Connect the HDSCM D1 port to the ECM S1port.
3. Connect the HDSCM U1 port to the ECM S2 port.

To connect the NCU to HDSCM using an NCU LAN, complete these steps:

1. Navigate to **Management LAN**, **Overview** > **Management** > **Network**, and add the NCU LAN.
2. In the **Equipment Details** view, **Configure** > **HDSCM** area, select the management LAN that you added in the previous step.
3. Connect the HDSCM D1 port to the ECM S1 port.
4. Connect the HDSCM U1 port to the ECM S2 port.

Preparing Connections in Nodes Without an HDSCM

1. Connect the first HD shelf CEM M1 port to the NCU C2 or C3 port, or to the OSCM Cx port.
2. To add additional HD shelves, connect the CEM M2 port to the CEM M1 port of the next HD shelf.
3. Configure the NCU port or LAN that connects to the first HD shelf to serve as a DHCP server. After you specify the connections for the HD shelves, the NCU software makes the required changes.
4. Configure the CEM M1/M2/M3 ports of the HD shelves to serve as a DHCP clients. These ports are set as DHCP clients by default. If these ports are not set as DHCP clients, correct the DHCP settings. To correct the settings, connect the ports directly to the Fiber Service Platform 3000 C management interface.
   For more details, see the Fiber Service Platform 3000 C user documentation suite.
5. Set a valid time and date on the NCU. See Manually Setting the Time, Date, and Time Zone.

🗒	See the HD Subshelf Configuration chapter in the FSP 3000R7High-Density Subshelf Hardware Guide for instructions to connect the shelves.

Adding HD Shelves to the Node

1. Select **Configure**.
2. In the navigation tree, select **Node**.
3. In the main pane, select **HD Shelves**.
4. In the **HD Shelves** area, complete these fields:
    a. **Management Interface**:
        - If you connect the first HD shelf to the NCU or OSCM, select SC-1-A-C2 or SC-NCU-Cx. Use the NCU identifier, which corresponds to the NCU port that connects to the OSCM or HD shelf CEM.
        - If the first HD shelf connects to equipment using a LAN to the NCU, select LAN-1-A-x or LAN-NCU-x. Use the NCU LAN identifier that connects the NCU to the equipment.

    b. **Admin State**: select **In Service**.
    c. **HD Connection Mode**: select the applicable mode.
    d. (Optional) **Change HD Password** and **Confirm HD Password**.

5. Click **Apply**.

🗒	In the main pane, the system displays each installed and connected to the specified management interface HD shelf with its corresponding shelf serial number.

🗒	If the system does not show the HD shelf : • Refresh your screen. The system needs up to 60 seconds to display newly connected HD shelves. • Recover the ECM from database maintenance mode. See the Installing the ECM or SCM chapter in theFSP 3000R7 High-Density Subshelf Hardware Guide.

Assigning the HD Shelf Number

Each HD shelf uses the shelf serial number to associate with the shelf.

1. Select **Configure**.
2. In the **Navigation Tree**, select **Node**.

3. In the main pane, click an HD shelf graphic. The shelf serial number identifies each shelf.
4. Select a shelf number.
5. In the **Admin State** field, select **In Service**.
6. Click **Apply**.

Deassigning the HD Shelf Number

Each HD shelf number is associated with the shelf serial number. Complete these steps to delete this association.

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. Select the **Management of HD Shelves** area.
4. Select the shelf entry from the list.
5. In the **Admin State** field, select **Management**.
6. Click **Apply**.
7. Click **Delete** and acknowledge the warning.

Adding Modules

Before you can add a module to a node, you must first create the shelf entity that will contain the module. You can create a module that you inserted but that you did not yet enter in the database. Or, you can create the module in an unequipped slot by pre-provisioning the module.

1. Select **Configure**.
2. In the navigation tree, select the relevant shelf.
3. In the main pane of the shelf, click **Add Module**.
4. In the **Add Module** window:
   a. Select the relevant **Slot** and **Equipment**.
      You can type any portion of the equipment name in the **Equipment** field to search by name.
   b. Complete relevant fields according to your network plan.

      The **Navigation Tree** will then list the new module.

> If any FWP-Mismatch NSA or FWP-Mismatch SA conditions are raised for this module, see the Maintenance and Troubleshooting Manual to resolve these conditions before you continue to the next step. Wait until the FWP-Mismatch alarms are resolved before you make any provisioning changes to this module.

5. In the navigation tree, navigate to the new module, and then click the module to display the **Details View**.
6. To edit the default options, complete the relevant fields.
7. To change the admin state of the module, change the admin states of the provisioned entities such as plugs, ports, and so forth.
8. Click **Apply & Exit**.

Adding Plugs

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to configure.
4. In the main pane, click the **Plugs** area.
5. Click **Add** to open the **Add Plug** dialog box.
6. From the **Plug** list, select the correct plug.
7. In the **Equipment** list, select the correct equipment type.
8. See your network plan to enter the **Channel**, **Rate**, and **Reach** settings.
   Admin State should be **Auto In Service**.
9. Click **Add**.

   The new plug is listed in the **Plugs** area **Details** window.

> The plug list might contain plugs that the module does not support. If you select an unsupported plug and click **Add**, an error message displays. Always select a supported plug described in Module and Pluggable Interface Compatibility.

Adding Physical Connections

First provision the shelf, module, or plug before you can add the physical connections. Create the physical connections between the physical termination points (PTPs). When you add associated equipment, the system auto-creates PTPs.

1. Select **Configure**.
2. Navigate to the appropriate module.
3. Select **Physical Connections**.
   a. The in-progress icon indicates that the software is retrieving information from the equipment. Wait for the process to complete.
4. Scroll to the applicable **PTP**. Click it to open the **Physical Connection - Create** window. In the **Physical Connection - Create** window, the equipment user label displays to help you make the correct physical connection.
5. Select the destination according to your network plan.
   a. If needed, change the connection arrow symbol.
   b. If you do not see the required destination, change the **Class** to display other selections.
   c. (optional) Enter **Description**.
6. Click **Apply & Exit**.
7. To access the physical connections, see the Physical Connections.

Adding Ports

After you create the relevant plug, complete these steps to add the plug ports.

	Some modules require that you provision a network port before you provision a client port.

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to configure.
4. In the main pane, click the **Ports** area.
5. Click **Add** to open the **Add Facility** window.
6. From the **Identifier** list, select the correct Identifier.
7. See your network plan to enter the required information.

8. Click **Add**.

   The **Ports** area will list the new port.

Using LEDs to Identify Equipment or Ports

You can cause an LED to blink green to help you locate equipment or ports. In the Configure Details view for ports, click **Identify** to cause the slot LED or port LED to blink green and help on-site personnel locate that module or port.

> If the port is in use by the Install Guide, the **Identify** button is unavailable.

Adding Data Channels

After you create the relevant plug and port, complete these steps to add data channels.

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to provision.
4. In the main pane, click the **Data Channels** area.
5. Click **Add End Point** to open the **Add Facility** window.
6. From the list, select the correct port and channel.
7. See your network plan to enter the required information.
8. Click **Add**.

   The new data channel will be listed in the **Data Channels** area **Details View**.

Adding Management Channels

Several different entity types, including SDCC, LDCC, GCC0, GCC1, GGC2, and EOC, support management channels, depending on the protocol.

To connect management channels to the management network:

1. Add the management channel to the supporting module.
2. Add an endpoint and connection to the NCU to connect the management channel to the management network.
3. Then, add the management channel to the module or port.

After you create the relevant plug and port, complete these steps to add management channels.

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to configure.
4. In the main pane, click the **Management Channels** area.
5. Click **Add** to open the **Add Facility** window.
6. From the **Identifier** list, select the correct identifier.
7. See your network plan to enter the required information.
8. Click **Add**.

   The new management channel displays in the **Management Channels** area.

To connect the management channel to the management network, add a management link on the NCU.

1. Select **Configure**, and then in the navigation tree, click shelf 1 to expand it.
2. Select the active NCU, slot 1, 3, or 18.
3. Add an end point to the NCU. In the **Management Links to Module Management Channels** area:
   a. Click **Add End Point**.
   b. Select a LINK identifier and other configuration information as described in your network plan.
   c. Click **Add**.
   d. Click **Add Connection**.
   e. Select an **Identifier**.
   f. Select a **Management Channel**.
   g. Click **Add**.
4. Restart the node as described in Restarting the NCU

Adding Management LANs

Use management LANs to connect certain management ports to the management network. NCU C ports connect to the management network by default.

Connect CEM/9HU and UTM C ports to a management LAN. Connect OSCM C ports to a management LAN if these port do not connect through an Ethernet cable.

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to configure.
4. If needed, add the C port to the module.
5. Navigate to the NCU in shelf 1, slot A, 3, or 18.
6. In the main pane, click the **Management LANs** area.
7. Click **Add** to open the **Add Facility** window.
8. Select a LAN **Identifier**.
9. See your network plan to enter the required information.
10. Click **Add**.

> Restart to activate the new settings.

Setting Up DHCP on Management Ports or LANs

To set **IP Operation** to **IPv4 and IPv6** you must set up the node to support IPv6. See: Provisioning IP Operation. Then:

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. Click the **Management Ports** or **Management LANs** area.
4. Click an **NCU** port or LAN row to open the **Details** window.
5. In the Internet Protocol (IPv6) area, **IP Operation** list, select **IPv4 and IPv6**.

Setting Up the DHCP Server

When you set up the DHCP Server, you can directly connect your computer to the port. Then the node provides an IP address for communication. You do not need to manually change your computer IP address.

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. Click the **Management Ports** or **Management LANs** area.
4. Click an **NCU** port or LAN row to open the **Details** window.
5. In the **DHCP** area, **DHCP Mode** field, select **Server**.
6. Change the settings in these fields if needed:
   - **DHCP Start Address**
   - **DHCP Stop Address**
   - **DHCP Mask**
   - **Direct Browser to NED**

> When you set the Direct Browser to NED, the software redirects all browser requests to NED. For example, if you enter http://google.com, the software redirects you to the NED login screen.

Click **Apply & Exit**. The NCU provides the IP address for communication. Restart the NCU for this action to take effect. Then, add a static route with a destination that can manage the subnet by using a relay agent address as the gateway.

> You can set up the DHCP server only for IPv4.

Enabling a DHCP Client

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. Select the **Management Ports** or **Management LANs** area.
4. Click an **NCU** port or LAN row to open the **Details** window.
5. In the **DHCP** area, **DHCP Mode** field, select **Client** or **Client Lite**.
6. Click **Apply & Exit**.

The NCU receives the IP address for communication. Restart the NCU for this action to take effect.

> The DHCP client supports all DHCP services. Therefore, only one port on the node can be a DHCP client at a time.
>
> DHCP Client Lite support is limited to receiving an IP address so that you can configure multiple ports can to DHCP client lite.

Enabling the DHCP Relay Agent

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. Select the **Management Ports** or **Management LANs** area.
4. Click an **NCU** port or LAN row to open the **Details** window.
5. In the **DHCP** area, **DHCP Mode** field, select **Relay Agent**.
6. In the **Relay Agent Server IP address** field, enter the appropriate IP address.
7. Click **Apply & Exit**.

The NCU forwards the client request. Restart the NCU for this action to take effect.

> The relay agent port and DHCP server must be in the same subnetwork.

Enabling the DHCP Relay-Client Agent

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. Select the **Management Ports** or **Management LANs** area.
4. Click an **NCU** port or LAN row to open the **Details** window.
5. In the **DHCP** area, **DHCP Mode** field, select **Relay-Client Agent**.
6. In the **Relay-Client Agent Server IP address** field, enter the appropriate IP address.
7. Click **Apply & Exit**.

The NCU receives the IP address for communication and forwards the client request. Restart the NCU for this action to take effect.

> The port works as both the DHCP relay and the DHCP client. The node receives an IP address from the DHCP server and forwards DHCP requests and responses from the DHCP server.

Adding Optical Lines

1. Select **Configure**.
2. Select **Optical Lines**.
3. Click **Add Optical Line**.
4. In the **Add Optical Line** dialog box, **Optical Line** list, select the correct optical line (OL) entity.
5. Click **Add** to apply your settings.
6. In the main pane, navigate to the new OL entity, and then click the entry to open **Configure Details**.
7. See your network plan to enter the required information.
8. In the **Attenuation Tx Fiber** [dB] and **Attenuation Rx Fiber** [dB] fields, enter the attenuation for the fiber segment in both directions.
9. (Optional) In the **Far End Location** field, enter the final location name.
10. Click **Apply & Exit**.

Adding an External Channel

Adding an External Channel to Channel Ports on CSM, PSM or 4-OPCM

> Channel ports on CSM, PSM and 4-OPCM support one channel per fiber.

1. Select **Configure > External Channels**.
2. In the **External Channels** area, click **Add**.
3. At the channel connection, select the slot and port for the CSM, PSM or 4-OPCM.
4. Enter the information for the external channel.
   –or–
   Select a profile that contains details about the channel.
5. In the **Transport Signal** area, **Channel** list, select a channel.
   –or–
   Select **Selected by System** for the control plane to determine the channel.
6. Click **Add**.

Adding an External Channel to an Optical Multiplex Ports on a PSM or CCM-C96/9 Module

> Optical multiplex ports on PSM, and CCM-C96/9 support one or more channels per fiber.

1. Select **Configure** > **External Channels**.
2. In the **External Channels in Optical Multiplex** area, click **Add**.
3. At the channel connection, select the slot and port for the CCM-C96/9 or PSM.
4. If this channel is first one that connects to this port:
   a. (Optional) In the **Identity** field, enter the **Host Device Name**.
   b. Click **Add**.
5. Select the **External Channel**.
6. Enter information for the external channel.
   –or–
   Select a profile that contains details about the channel.
7. In the **Transport Signal** area, select the **Channel**.
8. Click **Add**.

Adding Passive Units

Connect passive units to an identifier port on either a CEM9HU or PSCU module for detection. Each identifier port supports one passive unit. Before you can add a passive unit, you must add the identifier port that the unit connects to.

1. Select **Configure**.
2. Navigate to the corresponding shelf to display the CEM9HU or PSCU module.

> The system automatically adds the CEM/9HU module in the SH9HU shelves. To add a PSCU, see Adding Modules.

3. Click the CEM/9HU or PSCU module.
4. Click the **Passive Equipment Ports** area.
5. Click **Add** to add an identifier port.
6. In the **Add Facility** window, select the **Identifier**.
7. Click **Add** to activate your settings.
8. In the navigation tree, right-click **Passive Units**.

9. Click **Add Unit**.
10. In the **Unit** and **Equipment** type fields, select the correct types.
11. Click **Add**.

Port LEDs on Passive Equipment

Some passive equipment, including the 96CSM/2HU-#19600-#19125 or 16PSM4 module, supports port LEDs. These LEDs indicate that the port traffic status is actively carrying traffic, or if an issue with the traffic occurs.

Port LED	Description
Green	Traffic throughput is normal.
Yellow	Either local monitoring or the connected channel module detects an issue with the traffic.

Adding Passive Shelves

The node does not detect passive shelves, so you need to manually add them. You can add passive shelves to identify themselves, modules that you install in these shelves, and the physical connection entry to the modules. These shelves and their installed modules do not report alarms or inventory, which improves visibility of the installed equipment and supports physical connections to the modules. When you provision this equipment and its physical connections, the equipment tree supports the equipment, the physical connections, and the shelf views. The graphic representations help you install fiber, and you can track channel features.

The number of passive shelves that a node supports depends on the installed controllers:

Controllers	Passive Shelves Supported
NCU-S + SCU-S	2
NCU-II + SCU-II	30
NCU-II-P + SCU-II	30
NCU-II-P + SCU-II (redundant)	30
NCU-3 + SCU-II	30

1. Select **Configure**.
2. In the main pane, click **Add** to open the **Add Shelf/Unit** window.
3. From the **Shelf/Unit** list, select an available shelf or unit.

4. From the **Equipment** list, select **SH1HU/PASSIVE/FT**.
5. In the **User Label** field, enter the label.
6. In the **Admin State** field, specify the admin state according to your network plan. This equipment does not generate alarms.
7. In the **Location** area, complete these fields:
   - **Rack Number**
   - **Rack Description**
   - **Shelf Position [HU]**
8. In the **Information** area, complete these fields:
   - **Equipped**: Select **Yes**. After you complete the equipment installation, the system does not automatically detect the equipment.
   - (Optional) **Serial Number:** Enter the same serial number that is on the product label for inventory purposes.

> Use the Tooltips when you enter these parameters.

9. Click **Add** to add the new passive shelf.

After you add the passive shelves, you can provision modules in the passive shelves that do not require power for operation. For example, you can provision filters, power splitters/combiners, and protection modules.

Adding a Connection to a 16TCC-PCN-4GU+10G Module

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that corresponds to the 16TCC-PCN-4GU+10G module.
4. In the main pane, select the **Data Channels** area.
5. Click **Add Connection**.
6. Specify the direction.
   In a dual muxponder application, the direction should always be add-drop.
   In an ADM application, the direction can be pass-through or add-drop.
7. Select the source and destination endpoints for the connection.
8. Click **Add**.
   The new connection is listed in the **Data Channels** area **Details View**.

Adding Protection

The FSP 3000R7 offers equipment protection schemes.

- You must set the same options for all network facilities or virtual channel facilities in all protection schemes.
- You must connect network ports of the same type to form protection groups in these protection schemes:

Channel Protection

This section describes how to add channel protection for a service and contains these topics:

Requirements

To provision channel protection, you need two channel modules of the same type, each with two network interfaces. You must install one module in the near-end NE and one in the far-end NE. Provision both modules to operate in Transponder NE & NW or in Multiplexer NE & NW mode. For more information, see About Modes.

Setting Up Channel Protection

You first need to install the channel modules required for this protection scheme and correctly provision them.

1. Provision the two network pluggable transceivers in the near-end and far-end channel modules with the same plug equipment type.
2. Provision the two network channels in the near-end and far-end channel modules. Depending on the channel module type, set these options identically:
   - Facility type
   - Port usage
   - Error forwarding
   - Auto laser shutdown (ALS)
   - ALS hold-off
   - Laser Off Delay disabled, to meet the 50 ms switch time
   - SDH/SONET or OTN termination level
3. The client facilities in the near-end and far-end modules must be the same type. Set these options to identical values:

  - SDH/SONET or OTN termination level
  - Configuration of Tandem Connection Monitoring (TCM)
  - Configuration of Trace

4. Set up a protection group for two network facilities at the near end. See your network plan to enter the required information.
5. Set up a protection group for two network facilities at the far end. Specify the same settings as for the near-end protection group.

Setting Up Channel Card Protection

This section describes how to add channel card protection for a service and contains these topics:

Requirements

First install these required modules in the same shelf between slots 1 and 20. Then form a protection group:

- Four channel modules of the same equipment type.
- One pair of modules in every node.

After you install these modules, each module pair can form a protection group. Create channel card protection between normal and tunable variants. Provision the channel modules as follows:

- Provision the channel module pair in Transponder or Multiplexer mode. For more information, see About Modes.
- You must use a deployment scenario other than Back To Back or Client Layer Protection.

🗒	The combination of auto laser shutdown (ALS) in the client direction and channel card protection or client channel card protection is not supported. However, the system does not prevent you from provisioning this scenario. If you provision client-facing ALS in combination with a unidirectional client-channel card or channel-card protection, a signal failure will occur at the client interface receiver and might disrupt traffic.

Setting Up Channel Card Protection

Only certain modules support channel card protection. See the *Module and System Specification* to determine whether a particular module supports channel card protection.

1. You must provision the network channels in the two near-end modules and the two far-end modules.
2. Set these options in the same exact way if channel modules support them:
   - Facility Type
   - Port Usage
   - Error Forwarding
   - Auto laser shutdown (ALS)
   - ALS Hold-off
   - Laser Off Delay disabled, to fulfill the 50-ms switch time
   - Laser Off Hold
   - SDH/SONET or OTN termination level
3. Set these options in the same exact way in the same types of client facilities in the near-end and far-end modules:
   - SDH/SONET or OTN termination level
   - Configuration of Tandem Connection Monitoring (TCM)
   - Configuration of Trace
4. Set up a protection group for two network facilities in the near end. See Refer to your network plan to enter the required information.
5. Set up a protection group for two network facilities in the far end. Specify the same settings as for the near-end protection group.

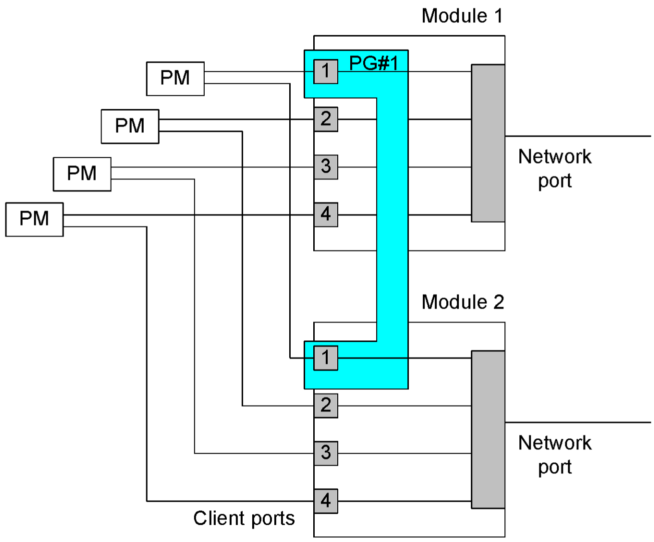
Using Client Channel Card Protection

Client Channel Card Protection (CCCP) provides 1+1 active equipment protection for supported channel modules. To provision CCCP, first set up a protection group for a pair of client ports on the same module type.

The figure that follows shows protection using network ports of the protection modules that connect to channel module client ports.

You can use a Y-cable instead of the protection module. The Y-cable contains an optical splitter/combiner and functions in the same way as a protection module. See the *Hardware Description* and *Module and System Specification* manuals for details about Y-cables.

Figure 36: Client Channel Card Protection Group Example



PG = Protection group
PM = Protection Module (optical splitter/combiner)

This section contains these topics:

Requirements

To form a protection group for CCCP:

- Install two channel modules of the same type on both nodes.
- Depending on the channel module type, you might need to install the channel modules in the same shelf.
- Connect the channel module client ports that you plan to use in a protection group to a protection module or Y-cable.
- Protection modules and Y-cables include:
    - 1 PM
    - 2 PM
    - All Y-cable models

You can then use the channel module client ports to form a protection group.

	The mode setting on some channel modules might prevent you from using CCCP. For more information, see About Modes.

> A combination of auto laser shutdown (ALS) in the client direction and CCCP is unsupported, but the software does not prevent you from provisioning this scenario.
>
> If you attempt to provision a client-facing ALS in combination with a CCCP, a signal failure will occur at the client port receiver and might disrupt traffic.

> After a fault in the working path, traffic might switch to the protection path. A protection path fault might then occur while the working path continues to have a fault. In this scenario, traffic will switch back to the working path, even though both paths are disrupted.

Setting Up Client Channel Card Protection

You can provision channel modules for CCCP on any client service type. However, not all channel modules support CCCP. See the *Module and System Specification* for more information about specific modules.

1. Ensure that you installed the required modules according to the requirements.
2. From the **Capability** list, select the correct module capability.
3. Provision the network ports on all four channel modules, both near-end and far-end. If applicable, complete these settings and use the same values for each of them:
   - Facility Type
   - Port Usage
   - Error Forwarding
   - Auto laser shutdown (ALS)
   - ALS Hold-Off
   - Laser Off Delay disabled (to meet 50 ms switch time)
   - Laser Off Hold
   - SDH/SONET or OTN termination level

1. Client facilities in the near-end and far-end channel modules must be the same. If applicable, complete these settings and use the same values for each of them:
   - SDH/SONET or OTN termination level
   - Tandem Connection Monitoring (TCM)
   - Trace Identifiers

4. Set up a protection group for two client ports for the near end. See your network plan to enter the required information.
5. Set up a protection group for two client ports for the far end. Specify the same settings that you used for the near-end protection group.

Path Protection

This section describes how to add path protection for a service and contains these topics:

Requirements

To provide path protection, create independent but identical paths between a network east facility and a network west facility to a single client facility. These paths are generally bidirectional connections. However, you can add a path at one end, drop a path at the other end, or create an add/drop path at both ends.

To create the cross-connections between the two independent and identical network facilities and the single client facility, follow the cross-connection rules so the software can create the cross-connections.

> For information about how to provision facilities for cross-connection services, see the Provisioning ADM Services section in the *Provisioning and Operations Manual.*

You must first delete a cross-connection protection group before you can delete the related cross-connections. After you delete the protection group, protection becomes inactive.

> See your network plan to enter the required information. The MDG: *Management Data Guide* describes options to provision each module.

Setting Up Path Protection

This procedure provides a generic description of how to configure a path-protected add/drop service between two NEs.

Configuring the Near-End NE

1. Create the module that will use the **Add-Drop Multiplexer** mode. For more information, see About Modes.
2. Create the client-side facility.
3. Create a network east facility and a network west facility.

   Both network facilities must be of the same service type and match the client-side service type.

4. Create a cross-connection between the client channel and the network east virtual channel.

5. Create a cross-connection between the client channel and the network west virtual channel.
6. Use the Cross-Connections Table to verify that you correctly defined the cross connections.
7. Correctly and successfully define the network-side virtual channels on both the east and west sides. Then create a protection group for the network east and network west virtual channels that cross-connect to the same client channel.
8. Use the Channel Protection Table to verify that you correctly defined the protection group.

Configuring the Far-End NE

1. For the NEs at the far ends, complete steps 1 to 6 inConfiguring the Near-End NE.
2. Fulfill these requirements:
   a. Ensure that the network facilities on both the near-end and far-end module are of the same type.
   b. If applicable, set these options, which you must set to the same values:
      - Port Usage
      - Error Forwarding
      - Auto Laser shutdown (ALS)
      - Laser Offf Delay disabled to fulfill the 50-ms switch time
      - Laser Off Hold

> When you change from a protected service to an unprotected service, deleting protection also deletes the cross-connection. You have to re-establish the cross-connection.
>
> When you re-establish the cross-connection path on the QuadFlex on the MP-2B4CT, ensure that the path is:
>
> - N1/odu4-1 to C1/odu4
> - N1/odu4-2 to C2/odu4
> - N2/odu4-1 to C3/odu4
> - N2/odu4-2 to C4/odu4

Versatile Protection

This section describes how to add versatile protection for a service and contains these topics:

Requirements

Make sure that you:

- Assign a system IP address to every node.
- Complete all network topology detection.
- Properly cable all VSM or OPPM (operating in VSM mode) network ports.

Configuring Versatile Protection

To configure a versatile protection scheme, you must first install and correctly provision the required channel modules:

- Versatile Switch Module (VSM)
- Optical Path Protection switch Module (OPPM) in VSM mode

> The User Label field is optional.

Configuring Versatile Protection Using a VSM

To configure versatile protection using VSM:

1. Select **Configure**.
2. In the navigation tree, right-click the shelf where the VSM module is located and select **Add**.
3. In the **Add Module** window, **Slot** field, select the slot number where you want to add versatile protection.
4. In the **Equipment** field, select **VSM**.
5. Click **Add**.

Continue with these steps:

1. In the navigation tree, expand the required shelf and select the slot number you just created.
2. In the **Ports** area, click **+**.
3. In the **Add Facility** window, **Identifier** field, select the NE port .
4. In the **Admin State** field, select **In Service**.
5. Click **Add**.
6. In the **Ports** area, click **+**.
7. In the **Add Facility** window, **Identifier** field, select the NW port.

8. In the **Admin State** field, select **In Service**.
9. Click **Add**.

Continue with these steps:

1. In the **Protection** area, click **+**.
2. In the **Add Facility** window, **Identifier** field, select the port that will support the working path.
3. In the **Protection** area, **Far End IP Address** field, enter the appropriate IP address.
4. Repeat this procedure for the VSM on the other end of the node span.

Configuring Versatile Protection Using an OPPM in VSM Mode

1. Select **Configure**.
2. In the navigation tree, right-click the shelf where the OPPM module is located and select **Add**.
3. In the **Add Module** window, complete these fields:
   a. **Slot**: select the slot number.
   b. **Equipment**: select **OPPM**.
   c. **Admin State**: select **In Service**.
4. Complete any additional required settings, and then click **Add**.
5. In the **Basic** area, complete these fields:
   a. **Capability**: select **1:VSM operation**.
   b. **Protection Switch Mode**: select **VSM Mode**.
6. In the navigation tree, expand the required shelf and select the newly created slot.
7. In the **Ports** area, click **+**.
8. In the **Add Facility** window, complete these fields:
   a. **Identifier**: select the **OM-*X*-*X*-C** port.
   b. **Admin State**: select **In Service**.
9. Click **Add**.

Continue with these steps:

1. Repeat the applicable steps to add the other ports.
2. In the **Protection** area, click **Add**.
3. In the **Add Facility** window, **Identifier** field, select the port that will support the working path.
4. In the **Far End IP Address** field, enter the appropriate IP address.
5. Complete any additional required settings, and then click **Add**.
6. Repeat this procedure for the OPPM on the node at the other end of the span.

Line Protection

This section describes how to add line protection for a service and contains these topics:

Requirements

- Install two switch modules of the same type — one in the near-end node and one in the far-end node. You can pre-provision the modules before you install them.
- For protection to work, place the cabling between the optical filter module and the switch module in both the near-end node and the far-end node. You can pre-provision the cables before you install them.
- If you use VSM or RSM modules in ROADM networks, ensure that the optical power difference between the two paths is 1 dB or less.
- Connect the RSM-OLM modules:
  - At the near-end, NW-T to NW-R.
  - At the far-end, NE-T to NE-R.

Setting Up Line Protection

To apply line protection, use one pair of switch modules. The optical transmission line protects all client signals. Use one of these switch module types to provision line protection:

- RSM-OLM, a remote switch module (RSM) with optical line monitoring.
- RSM-SF#1310 and RSM-SF#1510, RSMs for single fiber solutions without optical line monitoring.

Configuring the Near-End and Far-End Nodes

1. Create the switch module, and then set it to **Auto in Service**.
2. Create NW and NE ports, and then set them to **Auto in Service**.
3. Create the protection group for the two network ports.
4. Repeat steps 1 to 3 for the far-end node.

Viewing Protection Overview

You can view protection details in the **Protection Overview** area:

1. Select **Overview**.
2. Select **Protection**.
3. Click **Refresh**.
4. Click an area to view details.

Adding Existing Equipment

Complete these steps to add a pre-provisioned shelf, module, or plug.

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
    a. In the navigation tree, select the pre-provisioned slot or module that you want to add.
    b. To add the pre-provisioned plug, navigate to **Plugs**, and then select the plug.

The pre-provisioned **Shelf** or **Module** on the list is unavailable and appears dimmed, for example, **Slot 5 EDFA-DGC**.

In the **Plugs** area, the **Admin State** of the pre-provisioned **Plug** is listed as **Unassigned** / **Deleted**.

3. Click the relevant equipment to open the **Add Equipment** window. If the equipment already exists, the options display as pre-provisioned .
4. Click **Add**.

Provisioning an Optical Time Domain Reflectometer

This section includes instructions to provision an Optical Time Domain Reflectometer (OTDR) and contains these topics:

Background Information

First configure the OTDR by using the OTDR application. Then you can use the OTDR to acquire reference traces and monitor your fiber network. Open the OTDR from the Network Element Director (NED).

> In NED, the OTDR displays with the equipment name of 8-OTDR/3HU.

First create the OTDR shelf in the node database, and then connect to the OTDR. See Adding an OTDR to the Node Database. The only valid user name for the OTDR is *admin*, with password *xxx*.

See the *OTDR Installation, Provisioning, and Operations Manual*.

Requirements

Your node must have an NCU and two Ethernet ports.

Adding an OTDR to the Node Database

1. Select **Configure**.
2. Select **Shelf 1 > Slot A NCU**.
3. If Ethernet port C2 is already provisioned, delete it as follows.
   a. Click the **Ethernet Ports** area.
   b. Select **Edit**.
   c. Change the **Admin State** of port C2 (SC-1-A-C2) to **Management**.
   d. Click **Apply**.
   e. Select the **Delete** field for port C2, and then click **Apply**.
4. Complete the instructions in Adding Shelves.

Starting the OTDR

First create the OTDR shelf, and then start the OTDR.

1. Select **Configure**.
2. Select **SHELF OTDR 8-OTDR/3HU**.
3. Select **Access OTDR**.
   A new browser window opens with the login dialog box for the OTDR.
4. Enter the user name and password.
   To connect to the OTDR for the first time, in the User Name field enter *admin* and in the Password field enter *xxx*.
5. Click **Login**.

Using an OTDR with a RSM-OLM

The RSM-OLM is an optical switch module that you can use for network fiber protection. This module uses pilot Lasers associated with each network port to detect fiber cuts.

Complete these steps to temporarily disable protection switching. When you disable protection switching you also disable the pilot Laser on the network port if **Protection** is set to **Standby**.

1. Select **Maintain**.
2. Navigate to the shelf that contains the RSM-OLM.

3. Select the RSM-OLM module.
4. In the main pane, click to expand the **Ports** area.
5. Select **OTDR**.
6. In the **OTDR Operation Time** area, select a time period value that is required for an OTDR measurement:
   - Disabled
   - 5-Minutes
   - 20-Minutes
   - 40-Minutes
   - 60-Minutes
7. Click **Apply**.
8. Perform the OTDR operation. See *OTDR Installation, Provisioning, and Operations Manual*.

> After the RSM-OLM pilot Laser and protection switching return to normal operation, OTDR Remaining Time [min] displays.

Changing the Alarm Severity of an Item

1. Select **Configure**.
2. In the Navigation Tree, click the applicable module.
3. Select the item.
4. Click the row of the item to open the **Configure Details** window.
5. In the **Severities** field, select the severity for the alarm or event.
6. Click **Apply** or **Apply & Exit** to save the changes.

> To display the previous severity without saving the change, click **Refresh**.
> –or–
> To close the view without saving the change, click **Cancel**.

Copying and Pasting Channel Module Ports

Use this option to copy only optical channel (CH) ports. To copy a port, a plug must be provisioned. The software automatically selects the channel number based on the channel number of the plug. You can copy client-to-client ports and network-to-network ports.

> You can copy a port only if that port has a provisioned plug.

1. Select **Configure**.
2. In the navigation tree, select the shelf and module you want to configure.
3. Select the **Ports** area.
4. Right-click the port you want to copy, and then click **Copy**.
5. Select the **Destination Port**.
6. Click **Apply** to continue copying ports.
7. Click **Apply & Exit** to finish the procedure.

Configuring Remote Authentication

Complete these steps to set up remote authentication at the node.

1. Select **Node** > **Security** > **Access**.
2. In the **Remote Servers** area, enter up to three remote authentication servers.
3. Click **Add**, and then complete these settings:
    a. **IP Address**: enter the applicable IP address.
    b. **Remote Port**: enter the name of the remote port.
    c. **Remote Secret**: enter the shared secret key.
4. In the **Access Management** area, **Remote Authentication** field: select **TACACS+** or **RADIUS**.
5. In the **Authentication Protocol** field, select **PAP** or **CHAP**.
6. Click **Apply**.

Provisioning Encryption on Channel Modules

This section describes the provisioning and maintenance tasks related to channel modules that use encryption:

Provisioning Channel Modules to Use Encryption

To provision encryption, set the channel modules on both ends of the transport path to support the same encryption management.

- Users with the required privilege level can provision these channel modules.
- Only users with crypto officer privileges and the correct password can manage the encryption controls.
- Only crypto users with the correct password can approve software updates.

Provisioning Audio Engineering Society and European Broadcasting Union Channel Modules

Complete these steps to provision Audio Engineering Society (AES) and European Broadcasting Union (EBU) channel modules.

1. Add the channel modules. See Adding Modules.
2. Provision all required ports on each channel module. See Adding Ports.
3. If required, change the crypto officer password. See Changing the Crypto Officer Password.
4. Configure the authentication password on each encryption module. See Changing the Authentication Password

Provisioning Federal Information Processing Standard - F Channel Modules

Complete these steps to provision the Federal Information Processing Standard (FIPS) –F channel modules.

1. Add the channel modules. See Adding Modules.
2. Provision all required ports on each channel module. See Adding Ports.
3. If required, change the crypto officer password. See Changing the Crypto Officer

Password.

4. Pair the encryption keys for FIPS. See Pairing Encryption Modules.

Changing the Crypto Officer Password

The default crypto officer password on an encryption module is CHANGEME.1. Complete this procedure to change the crypto officer password.

Requirements

The crypto officer password:

- Must be 10 to 128 characters.
- Must contain at least one lowercase character, one uppercase character, and one numerical character.
- Can contain special characters.

Procedure

1. Select **Maintain**.
2. In the **Navigation Tree**, click the channel module that has encryption.
3. Click **Change Crypto Officer Password**.
4. In the **Change Crypto Officer Password** window, enter these options:
   - **Current Password**
   - **New password**
   - **Confirm password**
5. Click **Apply**.

Changing the Authentication Password

Channel modules that support encryption use an authentication password to establish a secure communication path.

Requirements

- You already provisioned the channel module that has the encryption N port.
- The channel module pair has the same authentication password.

The authentication password must:

- Be 10 to 128 characters.
- Contain at least one lowercase character, one uppercase character, and one numerical character.

Procedure

1. Select **Configure**.
2. In the **Navigation Tree**, select the channel module that has encryption.
3. Click the **Port Encryption** area.
4. Click the N port row.
5. In the **Configure Details** window, click **Change Authentication Password**.
6. In the **Change Authentication Password** window, enter these options:
   - **Current Password**, the crypto officer password
   - **Authentication Password**
   - **Confirm Authentication Password**
7. Click **Apply**.

> For FIPS-compliant AES modules see: Pairing Encryption Modules.

Setting Tag Error Values for the WCC-PCN-AES100GB-G

When you use the WCC-PCN-AES100GB-G channel card in a protection application with the OPPM:

- Set the Tag Error High Threshold to 100. The default is 3.
- Set the Tag Error Count Period(s) to 10 seconds. The default is 3600.

These values prevent loss of data traffic during protection switching.

Maintenance Operations on Channel Modules with Encryption

This section describes these maintenance tasks:

Modifying the Session Key Duration

The session key updates every 10 minutes during normal operation. The crypto officer specifies the maximum duration that the session key can be in use to manage communication failures such as a loss of signal.

Complete these steps to modify the session key duration.

1. Select **Configure**.
2. In the navigation tree, select the channel module with encryption.
3. In the **Data Channels** area, click the N port row. **Configure Details** window opens.
4. In the **Encryption Session** area, in the **Session Key Duration** field, select the application duration.
5. Click **Apply**.

Resetting the Encryption Options to the Default Values

After you reset the encryption options to the default values, the software makes these changes:

- Resets the crypto officer password to the default.
- Deletes the authentication password.
- Sets the session key duration to 1-day.
- Disables the FWP encryption update.
- Resets the FWP encryption release to 0.0.0.

Requirements

- Log in with an admin or provision-level user account.
- Set the administrative state of the encryption-capable channel module, and its ports and channels, to Maintenance.

Resetting the encryption options to their default values is service-affecting.

1. Select **Maintain**.
2. In the navigation tree, select the encrytion-enabled channel module.
3. Click the **Module Encryption** area.
4. In **the Encryption Passwords** field, click **Clear**.
5. In the dialog box that opens, enter the crypto officer password.
6. Click **Apply**.

Set **Admin State** to the previous or an applicable setting.

Running Encryption Tests

Run encryption tests for maintenance and troubleshooting purposes.

Requirements

- You must log in with an admin or provision-level user account.
- Set the administrative state of the channel module that has encryption, its ports, and its channels to Maintenance.

> Performing encryption tests is service-affecting.

To perform encryption tests:

1. Select **Maintain**.
2. In the navigation tree, select the channel module.
3. Click the **Module Encryption** area.
4. In the **Encryption Test** area, click **Start.**
5. In the dialog box that opens, enter the crypto officer password.
6. Click **Apply**.

> If the software detects a failure, the Mod LED becomes solid yellow, and the software updates the crypto log. Depending on the failed component, the module either operates in a degraded mode or no longer transmits.
>
> After the encryption tests complete, set **Admin State** to the previous setting or to another applicable setting.

Disabling Encryption

You might need to disable encryption to:

- Establish N port loopbacks.
- Reconfigure encryption modules.
- Establish an encryption link.

Encryption resumes in 30 minutes after you disable it. Or, you can manually enable encryption at any time.

Requirements

- You must log in with an admin or provision-level user account.
- Set the administrative state of the channel module, and its ports and channels, to Maintenance.

> Disabling encryption is not service-affecting. However, after encryption resumes, the generation and exchange of a new session key does affect service.

1. Select **Configure**.
2. In the navigation tree, select the channel module with encryption.
3. Click the **Port Encryption** area.
4. Click the N port row.
5. In the **Configure Details** window, set **Allow Encryption Bypass** to **Enable**.
6. Click **Apply**.
7. In the dialog box that opens, enter the crypto officer password.
8. Click **Apply**.

Encryption Operation should change to **Bypass**.

> After you complete the maintenance task, set the Admin State to the previous setting or to another applicable setting.

Enabling Encryption

To manually start encryption, disable bypass mode on the module. Encryption will automatically resume 30 minutes after you disable it. You can also manually enable encryption.

Requirements

- The crypto officer must first disable encryption.
- You must log in with an admin or provision-level user account.
- Set the administrative state of the channel module, and its ports and channels to Maintenance.
- Encryption automatically resumes after 30 minutes. Look at the Encryption Off Time setting to determine when you need to enable encryption.

> Enabling encryption is service-affecting.
>
> After this procedure completes, the generation and exchange of a new session key can take a few minutes.

1. Select **Configure**.
2. In the navigation tree, select the encryption module.
3. Click the **Port Encryption** area.

4. Click the N port row.
5. In the **Configure Details** window, set **Allow Encryption Bypass** to **Disable**.
6. Click **Apply**.
7. In the dialog box that opens, enter the crypto officer password.
8. Click **Apply**.
9. Wait for **Encryption Operation** to return to **Normal**.

> Set Admin State to the previous setting or to another applicable setting.

Provisioning Fiber Detection

You can set fiber detection on the node module and port to enabled or disabled.

To enable or disable fiber detection on a node:

1. Select **Node**.
2. Select **General > Controls**.
3. In the main pane **Functionality** area, select **Fiber Detect**. After you disable fiber detection, this setting remains disabled regardless of the fiber detection setting on the module or port.

To enable or disable fiber detection on a module:

1. Select **Configure**.
2. In the navigation tree, select the module you want to configure.
3. In the main pane equipment row, open the **Details** window.
4. In the **Port Function** area, select **Fiber Detect**. After you disable fiber detection, this setting remains disabled regardless of the fiber detection setting on the port.

To enable or disable fiber detection for a port:

1. Select **Configure**.
2. In the navigation tree, select the module.
3. In the main pane **Fiber Detection** area, click the port row to open the **Details** window.
4. In the **Physical Interface** area, select **Fiber Detect**.

Deleting Items

You can delete multiple items on a module. Delete items at the lower level of the configuration and work your way up the hierarchy — for example, delete ports before plugs.

> Before you can delete an item, set the Admin State of that item to Management or Disabled.

> Logical Interfaces (LIF) can only be deleted when the Admin State is set to Disabled.

Complete these steps:

1. Select **Configure**.
2. In the navigation tree, select the module to edit.
3. Open the area that contains the item you want to delete, and then click **Edit**.
4. Set the **Admin State** of the items you want to delete to **Disabled**.
5. Click **Apply**.
6. Next to the items you want to delete, select the **Delete** fields.
7. Click **Apply & Exit**.

Enabling Force Delete

1. Select **Node**.
2. Select **General** > **Controls**.
3. In the **Functionality** area, **Force Delete** field, select **Enable**.
4. Click **Apply**.

Using Network Intelligence

Use Network Intelligence to configure optical channels that exist across the network. You can use Network Intelligence with Service Manager on Ensemble Controller to create end-to-end services across the network.

A Network Intelligence controller runs on a centralized server and agents, which run on each node in the network. Set up the Network Intelligence agent on each the node so that the agent can communication with the controller. The Network Intelligence agent informs the controller which resources are available on the node.

After you set up the Network Intelligence agent, this change affects the operation of some aspects of Control Plane. Network Intelligence replaces the Control Plane after an upgrade from NCU-II to NCU-3. For a seamless operation across the network using Network Intelligence, enable the Network Intelligence agent on all nodes so that path computation can route the optimum path.

You should set up the Network Intelligence agent only if you also set up the Control Plane and the web interface.

To enable Network Intelligence agent on a node:

1. Select **Node**.
2. Select **General > Controls**.
3. In the **Control Network** window, select **Network Intelligence**.
4. Select **Enable**.
5. Click **Apply**.

Supporting Special Cables

This section contains these topics:

Provisioning Protection Cables

1. Select **Configure**.
2. Select **Special Cables > Protection**.
3. Click **Add Protection Cable**.
4. Enter a value of 1 to 2000.
5. In the **Protection Cable** area, select **Y-Cable Fiber/Connectors**.
6. Click **Add**.

Provisioning Filter Cables

1. Select **Configure**.
2. Select **Special Cables > Filter**.
3. Click **Add Filter Cable**.
4. Enter a value of 1 to 2000.

5. In the **Filter Cable** area, select **Filter Cable**.
6. Click **Add**.

Setting Up the Gateway Proxy Address Resolution Protocol

The NCU uses the Gateway Proxy Address Resolution Protocol (ARP) to respond to ARP requests for IP addresses. These requests originate outside the bridged IP sub-net without the need to set up static routes or use the Open Shortest Path First (OSPF) protocol to set up static routes. All NCU types support the Gateway Proxy ARP.

> You must set the OSPF and the Proxy ARP to disabled on all management links before you enable this gateway protocol.

1. Select **Overview**.
2. In the navigation tree, select **Management Network**.
3. In the main pane, select the **Management Ports** area.
4. Click the management port row to open **Configure Details** window.
5. In the **ARP Configuration** area, **Gateway Proxy ARP** field, select **Enable**.
6. Click **Apply & Exit**.

Provisioning for Flexgrid Channel Spacing

On certain modules, you can select channels based on channel spacing. The value you select for channel spacing determines the channels available for selection. You can space channels at 50 GHz, 100 GHz, or flexible for flexgrid operation. When channel spacing is flexible, you can also select the channel bandwidth. You can select channel spacing at the node level or on individual modules.

When you set channel spacing to flexible on the node level, the channel spacing setting on all modules that support flexible channel spacing change. If you set channel spacing to flexible, doing so has no affect on existing channels or services.

🗒	After you change channel spacing to flexible, you cannot reverse this setting. After you complete this operation, all flexgrid-capable modules will support only a flexgrid operation, including any flexgrid-capable modules you might install at a later time.

To configure all flexgrid-capable modules in the node for flexgrid operation, complete these steps.

1. Select **Node**.
2. Select **Controls > Functionality > Channel Spacing**.
3. Select **Flexible**.
4. Click **Apply**.

Configuration Modes

Option	Description
Transponder	The traffic path goes between the client and the network ports.
Transponder NE Only	The traffic path goes between the client port and the northeast port.
Transponder NW Only	The traffic path goes between the client port and the northwest port.
Transponder NE & NW	The traffic path goes between the client port and both the northeast and northwest ports to support channel protection. One network port is for the working path, and the other is for the protection path.
Multiplexer	Traffic on multiple client ports combines to transmit on the network port.
Multiplexer NE Only	Traffic on multiple client ports combines to transmit on the northeast port.
Multiplexer NW Only	Traffic on multiple client ports combines to transmit on the northwest port.
Multiplexer NE & NW	Traffic on multiple client ports combines to transmit on the both northeast and northwest ports to support channel protection. One network port is for the working path, and the other is for the protection path.
Regenerator 1-Way	Traffic converts to Optical-to-Electrical-to-Optical using a single port in each direction.
Regenerator 2-Way	Traffic converts to Optical-to-Electrical-to-Optical using two ports in each direction.
Add-Drop Multiplexer	The module supports traffic between a client and a network port — add-drop — and between two network ports — pass-through.
Dual Transponder	The module supports two traffic paths. Each path goes between a client port and a network port.
Dual Muxponder	The module supports two traffic paths. Each path goes between multiple client ports and a network port.

Option	Description
Degree Fixed	The ROADM module N port connects to a network degree and uses network fibers.
Degree Select	The ROADM module N port connects to channel add-drop equipment to support optical-channel routing to a network degree, in a directionless node.
Dual Port Add-Drop	The ROADM module N port connects to a network degree that uses network fibers, and two client ports support channel add-drop. The Cn port, where n equals the ROADM number, supports channels 19xx0, and the C8 port supports channels 19xx5.
Cross-Connect	The module supports traffic between any two ports.
Quad Transponder	The module supports four traffic paths. Each path goes between a client port and a network port.
Quintuple Transponder	The module supports five traffic paths. Each path goes between a client port and a network port.
Traffic C to N	Traffic is supported between Cx and Nx ports, where *x* is the same on both ports.
Traffic C to N+N Protect	Traffic is supported between Cx, Nx, and Nx+1 ports to support channel protection, where *x* is 1 or 3. One network port is for the working path, and the other is for the protection path.

Connecting to Juniper Network Routers

This use case explains how to set up interface edge nodes, located in a WDM network, with Juniper Network routers. This use case contains these topics:

Background Information

The objective of this use case is to create a point-to-point dataplane connection between two PTX5000 Juniper Network routers. These routers attach to nodes located at the edge of a WDM network.

The example use cases sets up the interface by using the GMPLS ENNI abstract link model. End-to-end service signaling uses the node and PTX5000 control planes. The node and

PTX5000 exchange routing information using OSPF. They exchange signaling information using RSVP messages through a dedicated Control Channel or GRE tunnel.

You can use these Juniper Network routers in this use case scenario:

- PTX3000
- MX80
- MX104
- MX240
- MX480
- MX960
- MX2010
- MX2020
- T640
- T1600
- T4000

Requirements

Fulfill these conditions.

Node	• The basic operational modules. • A cabling plan that shows all node-internal fiber jumpers is available. • All cables properly connect as specified in the Installation and Commissioning Manual. • You set up a configured and working control plane on the WDM layer.
Juniper PTX5000 Node	• All interfacing fibers properly connect. • You configured all interfacing routers, and they are operational as described in the Juniper Networks manual.

Click to return to the Connecting to Juniper Network Routers

Examples

The diagrams that follow show how the Juniper Networks PTX5000 Packet Transport Routers and edge nodes connect in a WDM network. These figures show a gray interface and a color interface with an external wavelength.

Figure 37: PTX5000 and Node Gray Interface

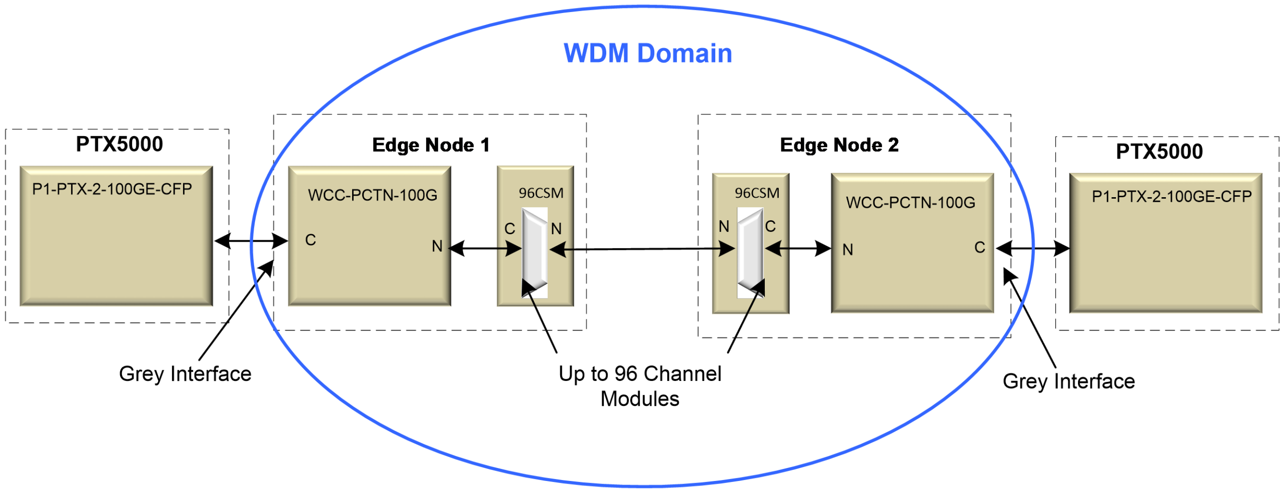
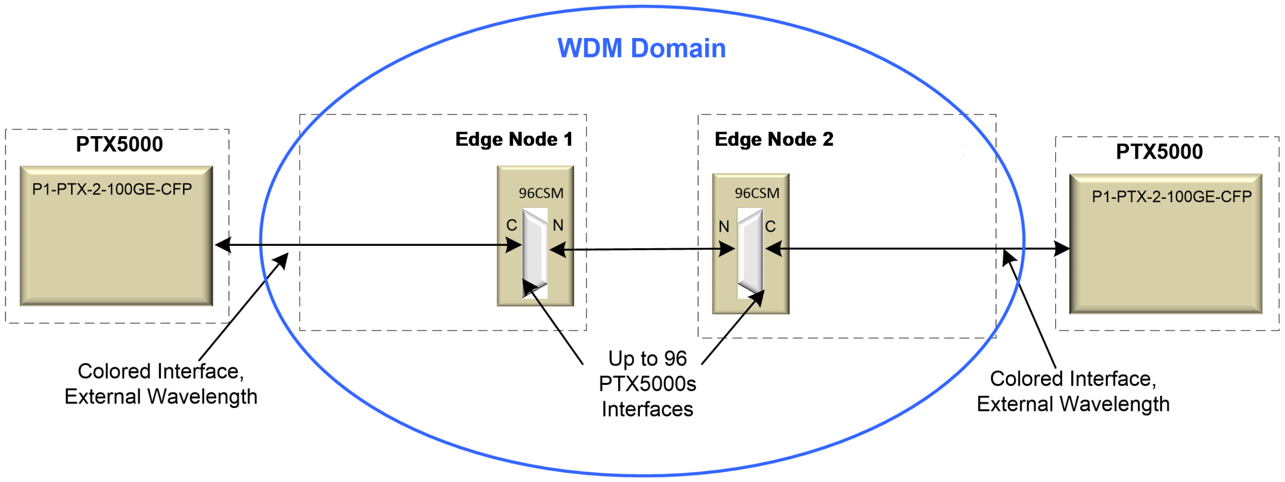


Figure 38: PTX5000 and Color Node Interface


WDM Domain
PTX5000
P1-PTX-2-100GE-CFP
Edge Node 1
96CSM
C
N
Edge Node 2
96CSM
N
C
PTX5000
P1-PTX-2-100GE-CFP
Colored Interface, External Wavelength
Up to 96 PTX5000s Interfaces
Colored Interface, External Wavelength

Click to return to the Connecting to Juniper Network Routers

Provisioning Nodes to Interface with Juniper Routers

The goal of this procedure is to provision two nodes located at the edge of a WDM network to connect two Juniper Networks routers located outside the WDM network. The supported Juniper Networks routers provisioned in the same way are the PTX5000, PTX3000, MX80, MX104, MX240, MX480, MX960, MX2010, MX2020,T640, T1600, and T4000.

We assume that you have the experience and information required to access the Juniper Networks routers.

Equipment

The listed equipment is an example. Ensure all nodes are populated with the optical transport modules. Your equipment might be different. Verify your design plan.

Edge Nodes 1 and 2 connected to Juniper Networks Routers with a Gray (1310/1550) Channel:

- WCC-PCTN-100G at each node: Client transceiver CFP/112G/LR4/SM/LC in each module.
- 96CSM/4HU-#19600-#19125 filter at each node.

Edge Nodes 1 and 2 connected to Juniper Networks Routers with DWDM Channels:

96CSM/4HU-#19600-#19125 filter at each node

Preparation

You must fulfill these conditions for this use case:

- All modules and plugs are installed in the node.
- You have a cabling plan that shows all internal node fiber connections. See the Examples diagram.
- All fibers and cables properly connect.

To provision the edge nodes, complete these steps:

Edge Node 1:

Provision the WCC-PCTN-100G channel module. Omit this step if the Juniper Networks router has a DWDM channel.

1. Select **Configure**.
2. Navigate to the relevant shelf.
3. Click **Add Module**.
4. Select the proper slot. A channel module that is plugged in displays.
5. Click **Add Module**.
6. Provision the client plug. Select the plug from the list.

Create a logical interface (LIF). This configuration is a control channel configuration.

1. Enable the Control Plane. Select **Node** > **General** > **Controls** > **Control Plane** area.

	Configure the control plane on the WDM layer. See Requirements

2. Set **Control Plane** to **Enable**, and then click **Apply**.
3. Select **Overview > Management Network > Logical Interfaces**, and then click **Add**. Select LIF.
4. Add the Management interface. This is the interface that attaches to the DCN or management network where the Juniper Networks router is reachable. See your DCN network plan.
5. Enter Encapsulation GRE or IP over IP.
6. OSPF routing is enabled for area 0.0.0.0. This is the default value, so no entry needed.
7. Enter the IP address: the tunnel local endpoint IP (inner IP). See your design plan for addressing scheme.
8. Enter the Subnet Mask: 255.255.255.252.
9. Add a Far End IP address. Add IP address:
   tunnel source/destination IP (outer IP – GRE encapsulation header).
   See your design plan for addressing scheme.

> After an upgrade from NCU-II to NCU-III, the control plane is disabled. Network Intelligence replaces the control plane.

If no route is available with the next hop from the LIF interface that you created in the previous steps, create a static route to the Juniper Networks route loopback IP address. If the route is available, omit this step.

1. Select **Overview > Management Network > Routes** area, and then click **Add**.
2. Enter the Destination: Juniper router loopback IP from Juniper router configuration.
3. Enter the Subnet Mask: 255.255.255.255.
4. Enter the Gateway: Juniper router GRE tunnel endpoint IP address from the Juniper Networks router configuration.
5. Enter the Interface: From the LIF you created earlier.
6. Click **Add** to create the route.

Provision an external channel for the DWDM channel. If the Juniper Networks router is a gray interface, omit this step.

1. Create an External Channel (ECH). Select **Configure > Node > External Channel**. Click **Add External Channel**.
2. Select an entity related to CSM client port location, which connects to the Juniper Networks router interface.
3. Select **Channel**.

Create a control plane LIF (LIF CP) for the access TE Link. See your design plan for TE link scheme.

1. Select **Overview > Control Plane > Logical Interfaces CP**. Click **Add**.
2. Enter LIF CP: Numbered TE link.
3. Enter IP address: a.b.c.X/30 (local link identifier).
4. Enter Remote address: a.b.c.Y/30 (TE link identifier on PTX5000 side)
5. Select Encoding: Ethernet.
6. Select Switching type: sub-lambda.
7. Select control plane type: GMPLS.
8. Enter Far End Datalink ID: Any non-zero value.
9. Enter OSPF routing: Passive, area 0.0.0.0.
10. Enter Trans Layer Termination Point. This is AID on the node corresponding to client interface created in previous steps. Examples: PTP-1-2-C1 for grey channel or ECH-3-FCU-I1-C1 for DWDM channel.

Create control plane LIF (LIF CP) for virtual TE Link. See your design plan for TE link scheme.

1. Select **Overview > Control Plane > Logical Interfaces CP**.
2. Click **Add**.
3. Select the LIF CP Numbered VTE link.
4. Select Encoding: Ethernet.
5. Select Switching type: lambda.
6. Select control plane type: internal.
7. Externally advertised: yes.
8. Enter the Trans Layer Termination Point: This is AID on the node that corresponds to the network interface that you created in the previous steps.
   Example: PTP-1-2-NW, MOD-2-2 for grey channel or ECH-3-FCU-I1-C1 for
   DWDM channel.
9. Enter the Far End Termination: This is AID, which corresponds to the network interface at the far end of the network.

Edge Node 2:

Go to edge node 2 and repeat steps for edge node 1.

Using TCM for Path Verification

You can use Tandem Connection Monitoring (TCM) for verification if the connection is properly configured on both ends. You must set both the near-end and far-end node TCM and Traces fields to the same values, for the TCM to work correctly. To enable TCM complete these steps:

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to configure.
4. In the main pane, click the **Data Channels** or **Ports** area.

    > You can set TCM on different levels, depending on module.

5. Click the channel / port that you want to configure.
6. In the **Configure Details** window, click the **Tandem Connection Monitoring (TCM)** to expand the area.
7. Set the fields according to your network plan:
    - **TCM_A**, **TCM_B** or **TCM_C**

    > To set these options, you need to change the Admin Status to Management and confirm the selection with Apply. After you set one of these options, additional selections will be available.

        - **Degrade Threshold**
        - **Degrade Period**
        - **LTC Action**
        - **Mode Rx**
        - **Mode Tx**
8. Click **Apply**.

Setting Traces

1. In the **Configure Details** window, click the **Traces** to expand area.
2. Set the fields according to your network plan:
    a. **Layer**
    b. **TIM Mode**
    c. **TIM Action**
    d. **Trace**
    e. **DAPI**
    f. **OPSP**
    g. **SAPI**.

3. Click **Apply**
   - or -
   Apply & Exit.

Using a Smartcard

You can use the NCU-3 smartcard chipset for cryptographic key protection. If you generate keys on the smartcard, the private key physically binds to the device and you cannot export that key. However, an administrator can export the public key. If someone requests a cryptographic function, the smartcard computes the request internally and does not expose the private key. This security feature protects keys from remote and physical attacks.

You can use the smartcard to:

- Authenticate RSA keys for SCP or SFTP file operations.
- Authenticate an SSH public key.
- Store a private key.

Initiating a Random Number Generator

1. Select **Configure** > **Node**.
2. In the navigation tree, select the applicable NCU module.
3. In the **Smartcard Applications** area, click the add icon to open the **Add Facility** window.
4. In the **Add Facility** window, set **Identifier** to **APPL-1-A-1**.
5. Click **Add**.

Initiating a Smartcard Cryptographic Function

1. Select **Configure** > **Node**.
2. In the navigation tree, select the applicable NCU module.
3. In the **Smartcard Applications** area, click the add icon to open the **Add Facility** window.
4. In the **Add Facility** window, set **Identifier** to **APPL-1-A-2**.
5. Click **Add**. In the **Smartcard Applications** area, an additional row displays.
6. Select the new row to open **Configure Details** window.
7. In the **Configure Details** window, **Operation** area, **Applet Operation**, click **Change**. The **Change - Applet Operation** window opens.
8. Select **Install**, and then click **Apply**.

After the installation completes, continue with these steps:

1. In the **Configure Details** window, **Configuration** area, **PIN/PUK** field, click **Change**.
2. Complete these fields:
   a. **New PIN**
   b. **Confirm PIN**
   c. **PUK**
   d. **Confirm PUK**
3. Click **Apply**.

Adding a Key to a Smartcard

To store a key in a smartcard, complete these steps:

1. Select **Node** > **Security** > **Certificates & Keys**.
2. In the **Keys** area, click the add icon to open the **Cryptographic Keys** window.
3. In the **Cryptographic Keys** window, **Identifier** field, select the relevant PKI_KEY.
4. In the **Cryptographic Key Configuration** area, set these parameters:
   a. **Key Length** to **2048**.
   b. **Key Algorithm** to **RSA**.
   c. **Key Profile** to **SSH/SFTP Authentication**.
   d. **Key Exportable** to **No**.
   e. **Key Storage** to **HSM on NCU-3**.
5. Click **Apply**.

To enable SSH authentication, see Enabling SSH Authentication.

Changing a Smartcard Cryptographic Function Applet PIN

1. Select **Configure** > **Node**.
2. In the navigation tree, select the applicable NCU module.
3. In the **Smartcard Applications** area, click the relevant applet identifier row.
4. In the **Configure Details** window, **Configuration** area, **PIN/PUK** field, click **Change**.
5. Complete these fields:
   a. **New PIN**
   b. **Confirm PIN**
   c. **PUK**
6. Click **Apply**.

Deleting a Smartcard Cryptographic Functions Applet

> Before you delete a smartcard cryptographic functions applet, deactivate and delete all stored keys.

1. Select **Configure** > **Node**.
2. In the navigation tree, select the applicable NCU module.
3. In the **Smartcard Applications** area, click relevant applet identifier row.
4. In the **Configure Details** window, **Operation** area, **Applet Operation**, click **Change**. The **Change - Applet Operation** window opens.
5. Select **Uninstall**, and then click **Apply**.

After the process completes, continue with these steps:

1. Click **Delete**. The Delete dialog box opens.
2. Select **Force Delete**, and then click **Delete**.

Alarm

The Alarm application allows you to view and change the severity of the current occurrences of alarms.

The handling and interpretation of the alarms are based on the severity as follows:

- **Not Reported** - Condition is not reported unless explicitly requested.
- ⓘ **Information** - Condition is reported but does not have a significant impact.
- ⚠ **Minor** - Condition requires a corrective action but generally does not impact service.
- ♦ **Major** - Condition requires an urgent correction action.
- 🛑 **Critical** - Condition requires an immediate corrective action.

The default severity for all alarms is listed in the *Management Data Guide*.

> Alarm reporting is suppressed when an item's **Admin State** is **Disable**, **Maintenance**, **Management**, or **Auto In-Service**.

To change the severity for an alarm, see Changing the Alarm Severity of an Item (in the Configure application). To change the alarm profile for the entire node, see Changing Alarm Severity for an Item Type (in the Node application).

This section contains these topics:

Viewing Alarms

Select **Alarm** to view alarms.

> To filter the table by the text that you enter in the field, use Search by all columns. For a more precise search, use Regular Expressions.

Changing Active Alarm Severities

1. Click **Alarm**.
2. In the main pane, right-click the row of the item whose alarm severity you want to change.
3. In the shortcut menu, select **Set <alarm name> on <equipment identifier>**, and then select the alarm severity from the list.

> The new alarm severity that displays applies to the current item in the current report occurrence.To apply changes to a module or the entire system, see Changing the Alarm Severity of an Item or Changing Alarm Severity for an Item Type.

Using the Monitor Application

Use the **Monitor** application to view performance monitoring information and associated thresholds. To change the thresholds, below the paramaters, click **Edit**.

To display performance monitoring data and manage thresholds, click **Monitor**.

To select equipment, in the Navigation tree, click an item.

These tabs display performance monitoring data.

- **Current** tab: the most recent data.
- **History** tab: the historical data.
- **Chart** tab: the historical data in a graphical view.
- **Reference** tab: representations of the physical data captured by user's requests.
- **Clear Counters** tab: reset data layer error counters.

Below **Current > Latest**, when you display Optical Power Receive and Transmit (OPR and OPT), if available, the optical power readings from the equipment display. OPR and OPT fields can also provide state information that indicate if the port is disabled or detected an outage.

> Invalid performance monitoring data displays in a light gray color. An asterisk * indicates a measurement interruption for part or all of the monitoring period. A loss of signal can cause measurment interruptions. A value of –99 indicates that the monitoring period recorded no valid values.

This section contains these topics:

Displaying Optical Power for All Ports

You can display and export the current optical-power levels that the system receives and transmits, OPR and OPT, for all equipped ports at the same time.

1. Select **Monitor**.
2. Click **Node**.
3. Click **Show All Ports**.

> In the **Show All Ports** dialog box, click **Export** to export the displayed information as a CVS file.

Changing Performance Monitoring Thresholds

> Some default thresholds are set as is, and you cannot change them.
>
> Find default values for performance monitoring thresholds in the *Management Data Guide*.

Most monitoring points have user-configurable thresholds that generate alarms. These are known as Threshold Crossing Alerts.

The threshold ranges are based on the equipment specifications. However, some threshold ranges support different equipment versions. For example, ports that support plugs have threshold ranges that manage all supported plugs.

Select **Show specification limits** to display the specification limits for the provisioned module or plug. Then you can specify that the thresholds be based on the equipment to be in use in this location.

1. Select **Monitor**.
2. In the **Navigation Tree**, select the applicable module.
3. Click **Show specification limits**.
4. Click the area for the item type you want to change.
5. Click **Edit**.

Click in the **Threshold** fields to display the allowable ranges.

6. Change the **Threshold**.
7. Click **Apply & Exit**.

Viewing Performance Monitoring Information

1. Select **Monitor**.
2. In the **Navigation Tree**, select one of these:
   - Node - to view total node **Input Power**.
   - Passive Units then a Unit - to view port OPR and OPT if supported.
   - Shelf - to view total shelf **Input Power**.
   - Module - to view supported performance monitoring values.

In the main pane, you can open a panel select one of these tabs:

Current	Current performance monitoring values in a numerical form. For example, the node power consumption mean value.
History	Historical performance monitoring values in a numerical form. For example, the shelf power consumption mean value and the shelf power consumption high value.
Chart	• Displays performance monitoring values in a chart for 1 or more data types. • You can see the thresholds and exact values by hovering over data points. • Use the labels above the chart to select and deselect the data types. • For the physical layer, the chart views the thresholds in the upper and lower regions.
Reference	Displays previously saved performance data for comparison to the current values.
Clear Counters	To clear the current and historical values.

To get valid power consumption historical values, you must provision all PSUs and PSMs.

You can select performance monitoring groups as desired to view more data. Most modules display the current temperature by default.

In the **Current**, **History** and **Chart** tab you can select the applicable time period:

- Latest
- 15 Minutes
- Daily
- Weekly

Also, if available, you can select:

- **Auto Refresh** to automatically update the performance data.
- **Thresholds** to display parameter thresholds.
- **Specification Limits** to display OPR Limit Min, OPR Limit Max, OPT Limit Min and OPT Limit Max.
- Performance monitoring groups, such as **Optical**, **OTU**, **TCM**, **SONET/SDH Line**.

In the **Reference** tab, you can select a related entry to display the previously stored data.

In the **Clear Counters** tab > **Current** or **History** area, you can select the counter you want to clear, and click **Clear Counters**.

Exporting and Printing Performance Monitoring Information

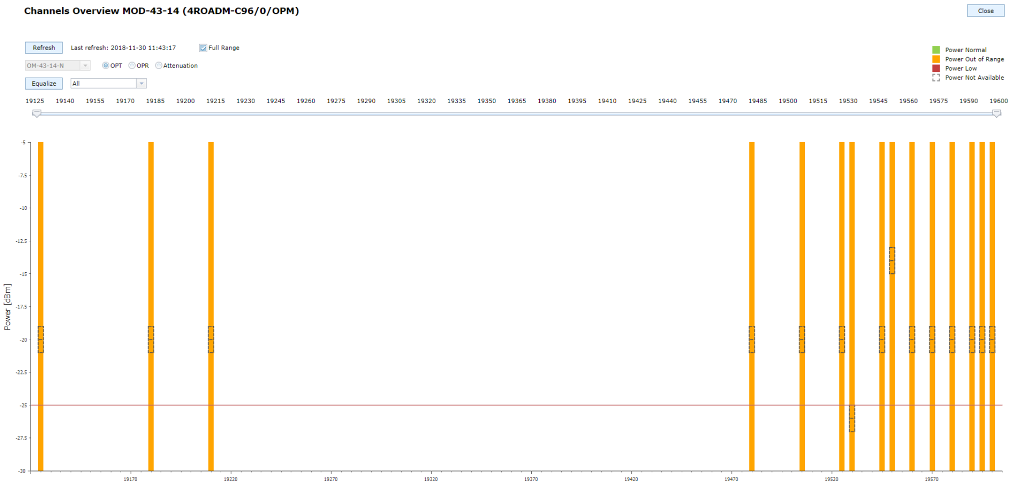
1. Click **Monitor**.
2. In the **Navigation Tree**, select or expand the applicable item or equipment.
3. In the main pane, select the applicable panel.
4. If needed, select **Current**, **History** or **Reference** tab.
5. If needed, select the applicable PM group, for example OTU or ODU.
6. Click:
   a. The export icon to export data.
   b. The print icon to print data.

Overview of the Channels Window

In the **Channels Overivew** window, you can view all or part of the channel spectrum on reconfigurable, optical add-drop multiplexer (ROADM) equipment. This view displays the current or present channel power for configured channels on ROADM modules. This view also displays equipment that connects to MROADM P ports, such as MTP-OSC-C or PSM80-MROADM, where the system monitors all channels.

1. Select **Monitor**.
2. Navigate to the ROADM or associated equipment.
3. Click **Channels Overview**.

The **Channels Overview** window opens and displays the channel power of the provisioned channels.



Channels Overview MOD-43-14 (4ROADM-C96/0/OPM)

Last refresh: 2018-11-30 11:43:17

☑ Full Range

OM-43-14-N

● OPT ○ OPR ○ Attenuation

All

The view shows the time stamp of the last refresh. To update the channel powers, manually refresh the view.

For ports that support equalization, the view:

- Shows the low-power limit as a red line.
- Shows the set point and acceptable range as dashed lines.
- Provides access to the channel attenuation values.
- Is a method you can use to perform equalization for all channels or individual channels.

Select an individual channel to display the:

- Channel number
- Channel bandwidth
- Channel power or attenuation, depending on the selection
- Set point
- An alarm icon if the channel has an alarm

To equalize all channels, select **All** in the list, and then click **Equalize**.

To equalize an individual channel, select the channel in the list, and then click **Equalize**.

📄	The channel powers automatically refresh after equalization completes.

Maintain

This section contains these topics:

Restarting the NCU

1. Select **Maintain**.
2. In the **Navigation Tree**, select the active NCU.
3. Click **Restart**.
4. In the message box, click **Restart**.

Restarting a Module

1. Select **Maintain**.
1. In the **Navigation Tree**, select the relevant module.
2. In the **Restart Module** tab, click **Restart** to open the restart window.
3. Select **Warm Restart** or **Cold Restart**.

> **Warm Restart** does not affect traffic. **Cold Restart** interrupts traffic and raises the **Equipment Removed** alarm.

4. Click **Restart**.

> Modules require several minutes to complete a restart. To see all information after a restart completes, click Refresh.

Equalizing Ports and Channels

Equalizing is the process of adjusting the transmitted optical power of individual channels to a defined power level or set-point. You can equalize:

- On ROADM equipment, individual channels or all channels on the N port.
- On CCM equipment, individual channels or all channels on a C port or all channels on all C ports (module).

Support for equalization varies by equipment but all share a similar process. The Event and Equalization logs report the results. Below **Monitor**, you can find the transmitted power levels.

1. Select **Maintain**.
2. in the Navigation Tree, select the applicable module.
3. To equalize an entire module:
   a. Select the **Module** area.
   b. In the **Equalize** column, click **Start**.
4. To equalize all of the channels associated with a specific port:
   a. Select the **Port** area.
   a. In the **Equalize** column for the applicable port, click **Start**.
5. To equalize a specific channel:
   a. Select the **Optical Channels** area.
   b. In the **Equalize** column for the applicable channel, click **Start**.

Forcing or Releasing Lasers

You can force Lasers to transmit light on most channel module ports. You can also force the pump Lasers in RAMAN amplifiers to on.

> Use Force Laser On only for diagnostic or trouble shooting purposes

See the *Maintenance and Troubleshooting Manual* for more information about hazards and requirements.

1. Select **Maintain**.
2. In the Navigation Tree, select the applicable module.
3. In the **Ports** area, select the port.
   –or–
   In the **Amplifiers** area, select the RAMAN amplifier.
4. Select **Interface** for channel modules, or **Amplifier** for RAMAN Amplifiers, if needed.
5. Set the **Admin State** to **Maintenance**.
6. Click **Apply**. Remember the original setting so that you can revert to it when finished.
7. Choose the applicable option:
   - Select the **Force Laser On** field and click **Apply**.
     The software over-rides the Automatic Laser Shutdown (ALS) operation for the Laser.
   - Clear the **Force Laser On** field and click **Apply**.
     The ALS operation might turn off the Laser.
8. Set the **Admin State** to the previous value, or select **Auto In Service**.
9. Click **Apply**.

Applying Loopbacks

Most channel module ports support loopbacks that you can use to isolate failures. Use loopbacks only for installation and troubleshooting purposes because they interrupt the normal traffic flow. See the *Module and System Specification*, Appendix A, for detailed information about loopbacks that a module supports.

Loopbacks interrupt the normal traffic flow. Service for the user is down in one or both directions while loopbacks are active.

When loopbacks are active, the process can introduce bit errors on 4WCE-PCN-16GFC modules.

To apply a loopback, the port **Admin State** must be set to **Maintenance**. Ports with dependent items require the **Admin State** for all dependent items to be set to **Maintenance** before the port **Admin State** can be set to **Maintenance**.

You can apply loopbacks only to:

- Bi-directional services.
- Ports that are not part of a protection group.

1. Select **Maintain**.
2. In the Navigation Tree, select the applicable module.
3. Change **Admin State** of dependent entities to **Maintenance**. Remember the original setting, so you can set it to the original state when finished.
4. In the **Ports** area, set the port **Admin State** to **Maintenance**.
5. Click **Apply**. Remember the original setting, so you set it to the original state when finished.
6. Set **Loopback** to one of these options:
   - Facility - connects receive to transmit as close as possible to the port connector
   - Terminal - connects receive to transmit as close as possible to the linked port connector
   - None - removes the connection from receive to transmit and restores the normal traffic flow.
7. Click **Apply**.
8. After you test the module, set the Admin State of the port and any dependent back to the previous value.
9. Click **Apply**.

Pairing Encryption Modules

Complete these steps to pair encryption keys for FIPS-compliant AES modules. Pair modules first so that they can establish keys for encrypting data. The process generates a new key and sends it to the remote module that must accept it. Complete these steps on both the local and remote modules at the same time to start encryption.

1. Select **Maintain**.
2. In the Navigation Tree, select the applicable module.
3. Navigate to the **Port Encryption** area.
4. Select **Encryption Authentication Keys**.
5. Click **Start Pairing**.
6. In the **Crypto Officer Password** window password field, enter the applicable password.
7. Click **Apply**.

> The operation takes approximately 2 minutes to complete.

8. Click **Refresh**, and then compare the **Key Generated** and **Key Rx** on both modules to ensure the keys match.
9. If the generated key from the remote module matches the received key on the local module, in the **Authentication Key Rx** field, click **Accept**.
10. In the **Crypto Officer Password** window, password field, enter the applicable password.
11. Click **Apply** to confirm or **Cancel** to abort.

If both sides accept the fingerprints, pairing completes, and periodic key-establishment starts. As soon as a key is available, encryption of user data starts.

Performing Self-Tests

Encryption module self-tests execute automatically after power-on. You can also initiate self tests. On demand self-tests execute using the Network Element Director.

Requirements

- You must log in as Crypto Officer.
- Set the administrative state of the channel module to Maintenance.

Activating Self-Tests

> Self-test process will affect the traffic.

1. Select **Maintain**.
2. In the Navigation Tree, select the applicable module.
3. Navigate to the **Module Encryption** area.
4. In the **Self Test** table, click **Start**.
5. In the **Crypto Officer Password** window password field, enter the password.
6. Click **Apply**.

Viewing Self-Test Results

1. Select **Configure**.
2. In the Navigation Tree, select the applicable module.
3. In the **Equipment** table, click the applicable equipment to open the **Configure Details** window.
4. Compare the **Selftest Execute** and **Result of Selftest** parameters.
   - If the values are identical, all tests passed.
   - If the values differ, some or possibly all tests failed. If self-test failed contact ADVA Technical Service.

> You can see the self-test result in **Node** > **Logs** > **Crypto**.

Using PRBS for Test Path Performance

You can test the path configuration and performance by running a Pseudo Random Bit Sequence (PRBS) test. You can perform the PRBS test on new connections as well as the existing ones. This test is service affecting and during the test you must stop all the traffic. You can also use the PRBS test to ensure that the service path conforms with customer service level agreements. To enable the PRBS complete these steps:

1. Select **Maintain**.
2. In the navigation tree, navigate to the relevant shelf.
3. Click the slot that you want to configure.
4. In the main pane, click the **Ports** area.
5. Select one of the following options:
   - **PRBS** - allows you to enable or disable the **PRBS Rx Operation** and **PRBS Tx Operation**.

     > In most cases you need to use PRBS Lane 1 Monitoring. You can use other lanes when the Port supports an Ethernet Service with multiple lanes.

   - **PRBS Lane 1 Monitoring** - allows you to monitor different ports based on the channel configuration.
   - **PRBS Lane 2 Monitoring** - allows you to monitor different ports based on the channel configuration.

- **PRBS Lane 3 Monitoring** - allows you to monitor different ports based on the channel configuration.
- **PRBS Lane 4 Monitoring** - allows you to monitor different ports based on the channel configuration.

Node

This section contains these topics:

Express Setup

The first time you commission a node, complete the procedures in this section. Because the requirements for system operation can change over time, you will most likely need to configure the node at other times after the initial installation and commissioning.

This section contains these topics:

Requirements

To you complete this procedure you need to have a user account with ADMIN rights. However, all users can see the settings for a node after commissioning is complete.

First plan the node configuration details and requirements. These details include which services to configure, connections to protect, and connections that need regeneration, and how you want to implement the DCN.

Before you commission the node, install the master shelf and its NCU module. See the *Installation and Commissioning Manual* for installation instructions.

You can provision the remaining modules after you install the equipment, or pre-provision modules that you can install later.

Configuring the Node Using Express Setup

1. Access **Network Element Director** using the administrator account. See Connection Requirements.

2. Configure the node settings. See General Node Settings.
3. Configure the node security. See Node Security.
4. To configure the management network for this node, click **Overview**, and then select **Management Network**. See Provisioning the Management Network.
5. Provision all physical connections. See Adding Physical Connections.
6. Configure the amplifiers.
7. Configure the ROADM devices. See ROADM Provisioning.
8. To back up the database configuration, select **Node**, and then select **Database > Backup**.

Logging into the Network Element Director

To configure and monitor a node, you must log into the **Network Element Director**. This chapter provides the procedure and contains these topics:

Background Information

Before you can set a node to normal operation and apply traffic, you must first complete these steps:

- Log in to Network Element Director.
- Commission the node.
- Provision the node modules, plugs, ports, and any other applicable equipment.

The next section describes the how to access NED and provides references to supporting procedures for more detailed instructions, where relevant.

Requirements

You need the following to use NED:

- A computer (PC) or laptop with a screen resolution of 1920 x 1080 or higher.
- A web browser — the latest versions of Google Chrome, Microsoft Edge or Mozilla Firefox (or latest Extended Support Release).
- An IP connection to the node as follows:
  - If the NCU has no database or is reset to factory defaults, when you connect to NCU C1, the NCU issues an IP address through DHCP to your laptop.The

NED login page opens.

- A direct connection to NCU port C1 through a user-configured IP address or the default IP address of 192.168.1.1.
- A connection through an IP network with a minimum bandwidth of 256 kbps.

Configuration Procedure: Connection Requirements

To log in:

1. Open a browser window.
2. Type your node IP address into the address bar.
3. Press **Enter**.
4. Enter username.
5. Enter password.
6. Click **Login**.

The login process might include a two-factor authentication which means that the user needs to enter the username and a password, where the password consists of two blocks, i.e. a token code + PIN.

There is also a challenge process that might be included in the login process. This means that the user needs to answer a set of additional questions in order to log in.

Both login mechanisms can be used only for remote authentication (RADIUS or TACACS+).

Specifying General Settings on a Node

This section describes how to configure settings that you typically specify the first time you configure a node and contains these topics:

Setting the Node Parameters

To begin each of these procedures, select **Node** > **General**.

Setting the Node Information

1. Select **Information**.
2. In the **System ID** field, type a unique name to identify this node in the network. A Help window guides you to correctly enter this SID.

3. Complete the **Location** and **System Contact** fields as applicable.
4. Click **Apply**.

After you change the System ID and click Apply, the node disconnects all users and then restarts.

> If you use Internet Explore to run NED, how you set cookies can cause issues the next time you log in. If issues arise when you log in, try to log in again and make sure you enter the correct user name and password. If your login attempt continues to fail, clear the browser cookies and history, then retry.
>
> If you use Chrome or Firefox, this issue does not occur.

Setting the Node Controls

1. In the **Interfaces** area, you can enable or disable these interfaces:
   - SNMPv1 and v2c
   - SNMPv3
   - Web Redirector
   - TL1
   - CP REST
   - NETCONF
   - GNMI

   The Web Redirector provides a proxy functionality to redirect HTTP/HTTPS communication. The web redirector can pass the web traffic from a client PC to a far-end NE in case of a routed IP path between client and far-end NE does not exist. The proxy itself must have connectivity to both, client and far-end NE.

   The other interfaces support communication between the NE and an external server when enabled.
2. In the **Functionality** area, complete the appropriate fields, as applicable:
   a. **Force Delete**: select **Enable** or **Disable** to activate / deactivate the possibility to deprovision the module and all its dependent entities at once.
   b. **Admin State Change**: select **Selected Item Only** or **Item and dependents** to control if administrator changes are performed on selected entity only or also on all dependent entities.
   c. **Auto Provisioning**: select **Enable** or **Disable** to set auto or manual provisioning of equipment and facilities.
   d. **Auto Provisioning OL**: select **Enable** or **Disable** to set auto or manual OL provisioning and the fiber map between OL and OSFM N-Port.

   e. **Preferred Facility Type**: select **SDH** or **SONET**, as applicable. Default values for SDH are STM64, STM16; for SONET: OC48, OC192.

   f. **SCU Connections**: select **Ring** or **Linear**, based on the physical connections between the SCU and different shelves.

   g. **Fiber Detect**: select **Enable** or **Disable** to enable/disable fiber detection.

   h. **Amplifier Los Response**: select **Remain On** or **Auto off**.

      - **Remain On**: EDFA amplifier behavior under input LOS conditions will remain as it is.
      - **AUTO Off**: EDFA amplifier pumps remain off until the input LOS condition clears.

   i. **Ethernet CFM**: select **Hide** or **Show in Overview** to hide / show the Ethernet Connectivity Fault Management (CFM) feature in the Overview. See Overview.

   j. **Local Computer Transfer**: select one of these options:

      - **Disable**: Local computer transfer is disabled.
      - **Upload only**: You can only upload files to a local computer.
      - **Download only**: You can only download files to a local computer.
      - **Download and Upload**: You can download and upload files to a local computer.

   k. **Channel Spacing**: select **Flexible** or **Defined on Equipment**. See Provisioning for Flexgrid Channel Spacing.

3. In the **Remote Event Recipients (SysLog)** area, complete the appropriate fields as follows:

   a. Specify which external recipients receive information about events and database changes through the Syslog. You can also specify a port User Label.

   b. Complete any other settings as applicable.

   c. Click **Apply**.

> If you set **TLS** as the **Transport Protocol**, make sure that the remote event recipient has an applicable certificate.

4. In the **Control Network** area, complete these fields:

   a. Network Intelligence: select **Enable** to activate Network Intelligence mode.

   b. **NI Advertisement Mode**: select one of these options:

      - **Traffic Engineering**: Network Intelligence Controller behaves as a Path Computation Server (PCS). Control Plane service provisioning is done in distributed way using RSVP TE protocol.
      - **Multi-layer Agent**: all functions needed for Control Plane service establishment / management are handled by Network Intelligence Controller in a centralized way.

   c. Control Plane: select **Enable** to activate distributed Control Plane functions.

d. **SDN Interface**: select **None** or **RESTCONF**, as it apply to your node.

e. **Auto Provision LIF-CP**: select **Enable** or **Disable** to enable / disable auto LIF-CP provisioning using OSC communication.

f. **Node Name Syntax**: select **IP Address (IP)** or **Target Identifier (TID)**, as it apply to your node.

g. **Node PCE Ranking**: enter a number from range 0-255. Click on the **Node PCE Ranking** field to see a window with PCE ranking description.

Setting the Node Defaults

You can set these node defaults. This section includes instructions for the first four settings. The other two are self-explanatory.

- Alarm activation and deactivation schedule
- Severely errored seconds threshold (SES). The change affects only F7 modules.
- The laser force timer
- Automatic in-service
- Rack information
- NCU Flash read-write error automatic restart

1. Select **Defaults** > **Alarm**.
2. In the **Alarm Activation Time** and **Alarm Deactivation Time** fields, set the times to raise and clear alarms, respectively.
3. Click **Apply**.

> When you use FR-ALS, change the Alarm Activation Time and Alarm Deactivation Time only to a value that is greater than the pulse width.

Continue with these steps.

1. Select **Defaults** > **Severely Errored Seconds**.
2. Complete the **SDH Threshold** and **OTN Threshold** fields to set the thresholds for bit parity violations of errors per second. Specify this setting at a value higher than the value you set to increase the SES counter.

> You can set the SES parameter only for a F7 modules. Predefined values for a hybrid modules are:
>
> - 30% for SDH
> - 15% for OTN

Continue with these steps:

1. Select **Defaults** > **Laser Force Time**.
2. In the **Force Operation Release** field, set the time delay to return Lasers to normal operation. First set the Laser to force on. Then specify the value, but do not remove the force-on setting.

Continue with these steps:

1. Select **Defaults** > **Automatic In-Service**.
2. In the **Auto In Service Control** field, select Enable if you want the system to suppress alarms. The system then suppresses alarms for any uninstalled equipment until you install them and also for facilities until the time delay expires after the facility becomes operational.
   -or-
   Select **Disable** to disable and set the time delay for the Admin State Auto In Service feature.
3. Click **Apply**.

Setting the Node Date and Time

1. Select **General** > **Date & Time**.
2. In the **Date & Time** area, complete the fields to configure the data and time.
   –or–
3. In the **Network Time Protocols (NTP) Servers** area, specify a remote NTP server. See Configuring Date and Time.
4. Click **Apply**.

Provisioning the Date and Time

This section contains procedures to manually set the date, time, and time zone of the node, and to synchronize the node time using the Network Time Protocol (NTP).

> First enable and configure NTP synchronization on the node before you can run operations like scheduled equalization of ROADMs.

This section contains these topics:

Background Information

Adva advices that you change the date and time of the node, either directly, through the time zone, or through changes to the NTP configuration, when you commission the system.

> Any action that changes the date and time can affect the performance records in an operational system.

Actions that change date and time create an entry in the event log. The entry indicates whether the change was manual, including the user account that made the change, an NTP step correction, or a Daylight Saving Time action.

After an NTP step correction occurs, the NTP daemon automatically restarts. The "NTP Not Synchronized" alarm is raised and cleared. This behavior is normal and conforms to the standard RFC 5905 §11.2.3.

The intervals of the performance records that the system gathers when you change the time was will be incomplete. Therefore, those performance records will be marked as invalid. Additionally, if you set the time back in an operational system, multiple performance records will all have the same timestamp. To avoid confusion, we recommend that you retrieve the node performance records before you change the time. Performance records with identical timestamps display in the order the system gathers them.

Configuration Procedures

This section includes these procedures:

Manually Setting the Time, Date, and Time Zone

This procedure describes how to manually set the time, date, and time zone of the node.

> You can configure the node to operate as an NTP client with NTP Mode set to Client or Relay. This setting results in the node time being synchronized using NTP. With this setting, you cannot manually set the time or date for the node. You can, however, always change the time zone.

Before you change the date, time, time zone, or NTP configuration in an already operating system, ADVA suggests that you retrieve your performance record history from the node. Collect all performance records and store them in a safe place before you complete this procedure. Use NED to collect performance records.

1. Log in to NED with a user account that has ADMIN privileges.
2. Select **Node**.
3. Select **General > Date & Time**.
4. Set the **NTP Operation** to **Server** or **Disable**.
5. Enter the new date and time.
6. From the list, select the **Time Zone**.
7. Click **Apply**.

> If you enter a country or city, the resulting GMT offset will display in the **Time Difference from GMT** field. Whether the time zone contains information about Daylight Saving Time will be indicated in the **Daylight Saving Time** field. This field does not indicate whether **Daylight Saving Time** is currently in effect.

Synchronizing the Date and Time Using NTP

Network Time Protocol (NTP) is a standard protocol that distributes accurate time in a computer network. The synchronization status for remote NTP servers is described here.

This section describes how to configure the use of NTP and includes these topics:

Provisioning a Node for NTP

This procedure involves these aspects of configuring NTP:

- Provisioning a node to use NTP for date and time synchronization .
- Verifying that the node can reach the remote NTP servers.
- Verifying the synchronization status by using a remote NTP server.

This section contains these topics:

Requirements

Before you change the date, time, time zone, or NTP configuration in an operational system, back up your performance records and store them in a safe place.

- You need to know the IP addresses of the remote NTP servers that you plan to use.
- You must log in with a user account that has ADMIN rights.

Configuring NTP

Complete these steps according to your network plan specifications.

1. Log in to NED with a user account that has ADMIN rights.
2. Select **Node**.
3. Select **General** > **Date & Time**.
4. In the **Date & Time** area, set the time zone for this node.
5. Set the **NTP Operation** mode, and then click **Apply**.
6. To add the applicable NTP server, in the **Network Time Protocol (NTP) Servers** area:
   a. Click the add icon.
   b. Complete to relevant fields.
   c. Click **Add**.

> The NTP protocol contains mechanisms for an NTP client to determine which NTP servers provide the best quality time information. ADVA does not support overruling the automatic prioritization.

> You can configure up to three NTP servers.

7. To delete NTP server, in the **Network Time Protocol (NTP) Servers** area:
   a. Set **Admin State** to **Disabled**, and then click **Apply**.
   b. Click **Delete**, and then confirm.

> The software will use the NTP server for time synchronization only if you set it to **In Service**.
>
> The system uses the provisioned and in service NTP servers for time synchronization in order from top to bottom.

8. Ensure that the node can reach the NTP server. See Verifying the Node to the Remote NTP Server.

Adding an NTP Server

Complete the settings in these fields to add an NTP server to provide date and time information to the node.

1. Select **Node** > **General** > **Date & Time**.
2. In the **Network Time Protocol (NTP) Servers** area, click the add icon.
3. In the **Add NTP Server** window, complete the relevant fields.
4. Click **Apply**.

The software will use the NTP server for time synchronization only if you set it to **In Service**.

The system uses the provisioned and in service NTP servers for time synchronization in order from top to bottom.

5. Make sure that the node can reach the NTP server. See Verifying the Node to the Remote NTP Server.

Remote NTP Server Synchronization Status

Status Message	Description
No Data	The system established no contact with the remote peer. This message displays if, for example, if you enter the IP address of a host without NTP server capabilities, or if the system is unable to reach the remote NTP server through the DCN.
In Progress	The software sent packets to the remote peer, and the time-out to receive packets in response is not yet exceeded.
Discarded	The system discarded the remote NTP server as invalid by using the sanity test algorithm. For example, this message occurs because the remote NTP server sent packets with an invalid header or stratum.
False Ticker	The Clock Select Algorithm did not retain the remote NTP server as a truechimer . A truechimer clock maintains timekeeping accuracy to a previously published and trusted standard, while a falseticker is a clock that does not maintain this accuracy.
Candidate	The Clock Cluster Algorithm retained the remote NTP server. The Combine Algorithm uses this server clock information to calculate corrections to the local clock.
System Peer	The software selects this remote NTP as the system peer. Only one system peer can exists at any given time. Thererfore, in Relay mode, the local NTP server inherits system statistics from this remote NTP server to pass to any dependent NTP client. This system peer selection occurs even if the local node is operating in client mode. This system peer selection can change over time, especially if multiple remote NTP servers are of similar quality, which is a normal occurrence.

After you configure a new NTP server, or the software loses communication to a previously synchronized NTP server, the system can take a bit of time to update the synchronization status.

Configuring an NTP Server Authentication

You can add the authentication key and use it to secure the exchange with NTP time server. This authentication support allows the NTP client to verify that the server is trusted.

Complete these steps:

1. Select **Node** > **General** > **Date & Time**.
2. In the **Date & Time** area:
   a. In the **NTP Operation** field, select **Server**.
   b. Click **Apply**.
3. In the **Network Time Protocol (NTP) Key** area, click the add icon.
4. In the **Add NTP Key** window:
   a. Complete the relevant fields.
   b. Click **Add**.
5. In the **Network Time Protocol (NTP) Servers** area:
   a. If applicable, add the NTP server. See Adding an NTP Server.
   b. Left-click on the relevant NTP server.
6. In the **Edit NTP Server** window:
   a. In the **Admin State** field, select **In Service**.
   b. In the **NTP Authentication** field, select **Private Key**.
   c. In the **NTP Key Id**, select the applicable key id number.
   d. Click **Apply**.

Configuring SNMP

This section describes these aspects of SNMP:

SNMP Attributes

Authentication Traps

When an unsuccessful authentication via SNMPv1/SNMPv3 has taken place an Authentication Trap is sent according to RFC1907. The information associated with the trap/event is a time-stamp, IP address of the source that attempted to authenticate itself, and Node IP address.

Extended Authentication Traps

When successful or unsuccessful authentication takes place via any access method (http/https, SNMPv1/SNMPv3, telnet/SSH or TL1) an Extended Authentication Trap is sent. The information associated with the trap/event might be one of the following: a timestamp, type of protocol used, whether the access was successful or not, IP address and user account of the source that attempted to authenticate itself, and a node IP address.

If sending of authentication traps/logging of authentication security events is later disabled, the Security Log content will remain intact and accessible.

Identify Traps

Identify Traps enable adding additional information about User and Application in each Database Change trap.

Provisioning SNMP Access Authentication

This procedure describes how to provision the node to support SNMP access authentication. The node must be configured to match the SNMP management application.

1. Select **Node**.
2. Select **General > SNMP**.
3. In the **Configuration** area, specify the SNMP configuration to be used:
    a. **SNMPv1**
    b. **SNMPv3**

   c. **Authentication Traps**
   d. **Extended Auth Traps**
   e. **Identify Traps**
   f. **Secure SNMPv3 Access** (when enabled restricts SNMPv3 access to messages with security level AuthPriv)
   g. **UDP Port**, the default is 161, which should work for most applications
   h. **IPv6 UDP Port**, the default is 161
   i. Click **Apply**.

4. When using SNMPv1, specify the new communities:
   a. In the **Community** area, click **Add**.
   b. I then in the Add Community window, enter the following:
      a. **Community String**
      b. **IP Operation** (IPv4, IPv4 and IPv6, or IPv6)
      c. **Access Type**
      d. These are optional:
         - **IP Address**
         - **IP Mask**
         - **IPv6 Address**
         - **IPv6 Prefix Length**
   c. Click **Add**.

5. When using SNMPv3, add a new user account. When adding the user account, set the SNMPv3 security level as required by your plan. See Adding User Accounts.
6. Select **Add** in the **Trap Recipients** area then in the **Add Trap Recipients** window, enter the following:
   a. **SNMP Version**
   b. **Trap Host IP**
   c. **Trap Port** (UDP port the node use to send the traps, the default is 162.)
   d. **Name** (SNMPv1 only; enter an appropriate name for this recipient.)
   e. **Trap User** (SNMPv3 only; select the recipient from the drop-down menu.)
   f. **Duration** (Length of time node keeps the traps. The entry for the trap recipient is removed after this time if not refreshed.)

7. Click **Apply**.

Editing SNMP Trap Recipients

1. Select **Node**.
2. Select **General > SNMP**.
3. In the **Trap Recipients** area, click on the trap recipient that you want to edit.
4. In the Edit Trapsink Recipients window, you can edit the recipient in the **Trap User** list.
5. Click **Apply**.

Deleting SNMP Trap Recipients

1. Select **Node**.
2. Select **General > SNMP**.
3. In the **Trap Recipients** area, click on the trap recipient that you want to delete.
4. In the Edit Trapsink Recipients window, click **Delete**.
5. Click **Ok**.

Node Security

This section contains these topics:

Requirements

All security-related settings require admin rights.

Provisioning Node Security

To securely access network elements, you must authenticate the data origin, operators, access privileges, and standard protocols for secure communication and file transfer.

You must have a user account with admin rights to complete this procedure.

Complete these steps to provision your security requirements:

1. Click **Node**, and then select **Security** > **Access**.
2. In the **Password Management** area, complete these fields:
    a. **Security Mode**.
    b. **Min Password Length**.
    c. **Password History Length**, to prevent repeated use of previous passwords.

   d. **Login Failure Delay**, required delay after repeated incorrect password entry.
   e. **Show Last Success Login**.
   f. **Show Last Failed Login**.
   g. **Account Lockout**, to protect the last admin account from lockout.
   h. **Serial Access Lockout**, to preserve the serial access for admins.
   i. **Account Lockout Period [s]**.

> Change Security Mode to Enhanced only once. ADVA recommends that you do not revert to Basic, which is a complex process.

3. In the **Access Management** area, complete the applicable fields. Additional information for some of the options:
   a. **Login Presentation** displays or suppresses system identification information on the login screen.
   b. **Remote Authentication** for RADIUS or TACACS+.
   c. **Single Sign On 2-Factor**. The default is **Disable**. If you set this field to **Enable**, the software identifies users who require two-factor authentication. If you change this setting from **Enable** to **Disable**, the software logs off all users who use two-factor authentication.
4. In the **Warning Message** area, if applicable, enable and enter the warning message to be displayed at login.
5. In the **Timeouts** area, specify the values for session and login timeouts (see Security Timeouts).
6. In the **Remote Servers** area, click **Add** to specify the RADIUS or TACACS+ server.
7. In the **Controls** area, activate and set the length of time for removal of user names from logs, if applicable. After the specified time, the software replaces user names in the logs with XXXXX.
8. Set the SSH protocol for secure communication with the node. The NE supports only SSH version 2.
   a. Click **Node**, and then select **Security Applications > SSH Details**.
   b. To generate a new SSH host key, click **Activate Key,** select the key length and click **Activate.**
   c. To specify the SSH host, encryption type, and fingerprint, click **Add**.
9. Select **Security > SSL/TLS** to view the SSL certificate.
10. To provision secure SNMP access, see: Provisioning SNMP Access Authentication.

11. Add users to the local node:
    a. Click **Node**, and then select **Users**.
    b. Click **Add** to specify the user, password, and access level.

> You can set SSH to Disable only if you do not set Node > General > Controls TL1 Interface to encrypted mode.

Provisioning User Accounts

This section describes these aspects of user accounts:

Requirements

The management of user accounts requires admin rights.

Exception: Users that do not have admin rights can change their own passwords.

Viewing User Accounts

1. Select **Node**.
2. In the **Navigation Tree**, select **Users**.
3. To view active users or send messages to them, select **Active/Messenger**.
4. To view, add, or modify users accounts, select **Manage**.

> Only users with the admin privilege level can view, add, or modify local user accounts on the node.

Viewing Active Users or Messaging Other Users

NED displays the number of Active Users excluding SNMPONLY users, but does not automatically update them. NED updates the number of Active Users after you:

- Log in.
- Refresh the browser.
- Select Active User. Click or enter Active Users.
- Select **Node > Users > Active/Messenger**.
- Below **Node > Users > Active/Messenger**, select **Refresh**.

You can display other users who are logged in to the Node and send messages to those users.

1. Select **Node**.
2. Select **Users > Active/Messenger**.
3. The list of users currently logged in to the node, which are active users, displays.
   If the only user name in the list is yours, no other users are logged in to the node.
4. To send a message to another logged-in user:
   a. Click the row with that user's **Username**.
   b. In the NED Messenger window,type your message, and then press Enter.

> To access Node > Users > Active/Messenger, you can also click the number of displayed Active Users.

Broadcasting Messages to all Users

You can broadcast messages to users who are logged in to a node. To broadcast a message, at least three user sessions should be logged in.

1. Select **Node**.
2. Select **Users > Active/Messenger**.
3. Click **Broadcast**.
4. In the NED Messenger window, type your message, and then press Enter.

Adding User Accounts

1. Select **Node**.
2. Select **Users** > **Manage**.
3. Click **Add**.
4. Select the **User Privilege** level.
5. In the **User Name** field, enter a unique name according to requirements.
6. In the **Password** field, enter a password. Retype the password to confirm.
7. (optional) In the **Access** area, configure:
   - TL1 Timeout
   - TL1 Timeout Period [min]
   - Sudo Access

	After upgrade to the R22.1.1, all existing admin-account users get a sudo option enabled. Admin-account users with a sudo option enabled can create and edit all other admin accounts. Admin-account users with a sudo option disabled can only create and edit other admin accounts with disabled sudo option. The system always enforces that at least one admin account has a sudo option enabled. The account overview indicates each admin account with a sudo option enabled.

8. In the **SNMP** area:
   - Select the user access for SNMP.
   - Set the **Authentication Protocol** according to your requirements. Adtran Networks SE recommends that you use SHA-256 algorithm as a minimum.
   - Set the **Privacy Key Type** to **User Specified** if you want to use a specific key for encryption instead of using user password.
9. In the **Account** area, complete these fields:
   - **Login Fail Count**: Enter the number of failed login attempts that will lock the account. If the failed login attempts exceed this number, only a user with admin privileges can manually unlock the account.
   - **Password Age**: Enter the minimum and maximum values that will force users to change their password.
   - **Password Expire Warning**: Enter the number of days that must pass before the software warns users that their passwords will expire.
10. Click **Add** to save these settings and add the user.

	In the **Access Day/Time** area, you can create users with access restrictions based on time-of-day restrictions.

	Users who have admin privileges and the crypto office password for the AES encryption modules can perform crypto officer tasks.

Deleting User Accounts

1. Select **Node**.
2. Select **Users**.
3. Click the user that you want to delete.
   The Edit account window opens.
4. Click **Delete User**.
   The Delete account window opens.
5. Click **OK** to delete the user or **Cancel** to discontinue.

Editing User Accounts

1. Select **Node**.
2. Select **Users**.
3. Click the user account that you want to edit.
4. In the **Edit Account** window, edit the relevant fields.
5. Click **Apply** to save these settings.

> To use a specific key for encryption instead of a user password, in the SNMP area, SNMP Privacy Key Type, select User Specified.

> After you change the Authentication Protocol in the SNMP area, you must set a new password. If you do not set a new password, the software will force a change at the next login.

Temporarily Upgrading the User Privilege

Users with monitor privileges can request higher privilege levels on nodes that Network Manager (NM) manages. The monitor user logs in to the node, and then requests privilege upgrade. Users with admin privileges on Network Manager receive the request and can **Allow**, **Deny**, or **Ignore** it. If the admin user allows the request, the software upgrades the monitor user privilege to the allowed privilege level.

Requirements

NE Requirements:

- Enable **User Privilege Upgrade**.
- Enable **SNMPv3**.
- Configure Network Manager to be a SNMPv3 trap recipient.

Network Manager Requirements:

A user with admin privileges must allow the privilege upgrade.

Enabling User Privilege Upgrade

1. Select **Node**.
2. Select **General** > **SNMP**.
3. In the **Configuration** area, set **SNMPv3** to **Enable.**
4. In the **Trap Recipients** area, select **Add**.
5. Specify the information for Network Manager server:
   - SNMP Version = **SNMPv3**.
   - **IP Operation**.
   - **IP Address or IPv6 Address**.
   - **User Name**.
   - **Destination Port**.
   - **Duration**.
6. Select **Security** > **Access**.
7. In the **Access Management** area, set **User Privilege Upgrade** to **Enable**.

Forcing a Password Change

1. Select **Node**.
2. Select **Users**.
3. Select the user account.
4. In the **Edit Account** window, select the **Password** area.
5. In the **Require Password Change** field, select this field to require a password change. The software will then prompt users to change their passwords after their next successful log in.
6. Click **Apply** to save these settings.

Provisioning False Passwords

You can specify that the software will lock an account after a certain number of consecutive false passwords.

1. Select **Node**.
2. Select **Users**.
3. In the **Account** area, complete these fields:
   a. **Login Fail Count** specifies the number of consecutive false passwords before the software locks the account.
   b. **Max Password Age**.
   c. **Min Password Age**.
   d. **Password Expire Warning**.

4. Click **Apply**.

Manually Locking a User Account

1. Select **Node**.
2. Select **Users**.
3. Click the user account that you want the system to manually lock.
4. In the **Edit Account** window, select the **Account Lockout** area.
5. In the **User Access** list, select **Lock**.
6. Click **Apply**.

Provisioning User Account Inactivity

1. Select **Node**.
2. Select **Users**.
3. Click the user account that you want to configure.
4. In the **Edit Account** window, select the **Account Lockout** area.
5. In the **User Access** list, select which options should occur at the end of the inactivity period.
6. In the **Inactivity Period [day]** field, enter the number of days of inactivity before the software locks the account.
7. Click **Apply**.

Provisioning User Account Day or Time Access Restrictions

Complete these steps to restrict the day and time when users can access a node.

1. Select **Node**.
2. Select **Users > Manage**.
3. In the **Username** row, click the relevant user to open **Edit Account** window.
4. In the **Access Day/Time** area, select **Restrict Access**.
5. In the **Access Start Time** and **Access End Time** fields, enter the applicable times.
6. Select days of the week where time restrictions are active.
7. Click **Apply**.

> Only users with these privilege levels can have time restrictions:
>
> - Provision
> - Operator
> - Monitor
> - Crypto

> Only user accounts that do not use RADIUS or TACACS+ authentication support day and time restrictions.

Switching User Accounts

To switch from one user account to another:

1. Exit Network Element Director.
2. Log in, and then enter the new user account name and its corresponding password.

Changing Your Password

1. Select **Node**.
2. Select **Users**.
3. Select the user account.
4. In the **Edit Account** window, select the **Password** area.
5. In the **New Password** field, enter a password according to requirements.
6. In the **Confirm New Password** field, retype the new password.
7. Click **Apply** to save these settings.

Terminating Other Users' Sessions

If you have admin level user privileges, you can terminate sessions for other users.

1. Select **Node**.
2. Select **Users > Active/Messenger**.
3. Next to the session you want to terminate, select the **Access** field.
4. Click **Terminate**.

Security Timeouts

This section contains these topics:

Node Security Requirements

The software will terminate any incomplete login attempt or active session after a defined period of inactivity. This section describes how to configure the timeouts for different types of access to the system.

You must log in with admin rights to configure node security requirements.

This table lists the types of access that you can configure and the available range values.

- If you run the Craft interface over a serial line, the system prompts you for your login credentials again.
- If you run the Craft interface over a Telnet/SSH connection, the TCP connection terminates.
- If the Craft interface initiates a Linux command line shell, the software interprets any inactivity in the Linux command line shell as Craft interface inactivity. For any applications that start on the Linux command line and that the system sends to the background, the software regards as not being user activity.
- If you start a TL1 session from within the Craft interface, the TL1 login and session timeout listed in the table that follows will apply.

You do not need to configure a login timeout period parameter through NED. It is not possible to configure this period. A NED login timeout does not apply because the user name and password transfer to the NE in a single HTTP or HTTPS request.

Table 4: Session and Login Timeouts

Type of Access	Range in Seconds	Default
Serial or Telnet Login	5 to 300 s	30 s
SSH Login	5 to 300 s	30 s
TL1 Login	5 to 300 s	30 s

Type of Access	Range in Seconds	Default
Craft Console Session	30 to 3600 s If during the upgrade the system detects the current timeout value to be out of the limits, the system will correct it. If not, the system leaves it unchanged. If the current value is less than 30 seconds,the software will set the value to 30 seconds. The current value must be less than 3600 seconds. This limitation is also valid for web sessions.	900 s
Web Session	30 to 3600 s	900 s
TL1 Session Configure TL1 sessions at the user account level. See Provisioning User Accounts.	1 to 60 m	15 m
SNMP Session For all SNMPv1 communities and SNMPv3 users.	30 s to 3600 s	15 m
Write Access	100 to 3600 s	300 s

Configuring Security Timeouts

1. Select **Node**.
2. Select **Security > Access**.
3. In the main pane, select the **Timeouts** area.
4. Configure the timeout sessions or logins according to your requirements.
5. Click **Apply**.
6. Log out of the node, and then log in again to initialize the new timeout settings.

Packet Filtering

This section contains these topics:

Requirements

You must have a user account with admin rights to complete this procedure.

Background Information

When the Linux kernel receives a network packet, the kernel first determines whether the packet is addressed to the local host or if the kernel must route the packet to the next host. Packets for the local host must pass through the input filter before the kernel passes them to local processes. Packets that the kernel routes to the next host pass the forward filter.

Packets that local processes generate pass through the output filter before the kernel sends them through the network. To address defects, you can enable or disabled packet filtering.

Enabling Packet Filtering

You must have a user account with admin rights to complete this procedure.

1. Click **Node**.
2. Select **Security > Access**.
3. In the **Access Management** area, **Packet Filter** list, choose **Enable**.
4. Click **Apply**.

> After you disable packet filtering, packet controls in the Security > Packet window are also disabled. This message displays in the Security > Packet window:
>
> The Packet Controls (Filtering) are not executed. Packet Filter can be enabled in Security > Access.

Node Management IP Address Filters

You can define IP address ranges where management computers are located. Network management can occur only from these management stations. Node management IP-address filters block all traffic that does not originate from these stations. However, because the IP addresses are disabled by default, and the system blocks nothing. The node management IP address filter requires only an input filter. The NCU controls the output, which is secure by default.

The list of node management IP address filters can contain up to 25 network or host entries. You can either activate or deactivate these entries.

Enabling Node Management IP Address Filtering

You must have a user account with admin rights to complete this procedure.

1. Select **Node**.
2. Select **Security > Packet**.
3. In the **Node Management IP Address Filters** area, **Approved IP Filter** list, select

Enable.

4. Click **Apply**.

> Ports that connect to the management network through management LANs and management links do not support node management IP address filtering.

Adding Approved IP Addresses

For this procedure to be successful, you must enable the packet filter.

1. Select **Node**.
2. Select **Security > Packet**.
3. In the **Node Management Approved IP Addresses** area, click **Add**.
4. In the **Add Approved IP Address** window, **IP Operation** field, select **IPv4** or **IPv6**.
5. Set the **Admin State**.
6. Complete these fields:
   a. **IP Mask**: enter the correct mask address.
   b. **IP Address for IPv4**: enter the correct IPv4 address.
   c. **IPv6 Address**: enter the correct IP address for IPv6.
   d. **IPv6 Prefix Length**: enter the prefix length for this address.
7. Click **Add** to confirm.
8. In the **Node Management IP Address Filters** area, select whether the system will accept packets only to the System IP address.
9. In the **Node Management IP Address Filters** area, **Approved IP Filter** field, select **Enable**.
10. Click **Apply**.

Provisioning ICMP Filters

1. Select **Node**.
2. Select **Security > Packet**.
3. In the **Internet Control Message Protocol (ICMP)** area, select **Enable** or **Disable** for each of these messages:
   a. **ICMP Filter**
   b. **Drop Echo Requests**
   c. **Drop Source-Quench**
   d. **Drop Redirects**

   e. **Drop Timestamp Requests**
   f. **Drop Address Requests**

4. Click **Apply**.

Provisioning the Denial of Service Guard

1. Select **Node**, and then select **Security > Packet**.
2. In the **Controls** area, **Denial of Service Guard** menu, select **Enable** or **Disable**.
3. Click **Apply**.

Provisioning Packets Between Inband Channels

1. Select **Node**.
2. Select **Security > Packet**.
3. In the **Controls** area, **Isolate Inband Channels** list, select **Enable** or **Disable**.
4. Click **Apply**.

Enabling IP Forwarding

1. Select **Node**.
2. Select **Security > Packet**.
3. In the **Controls** area, **IP Forwarding** menu, select **Enable** or **Disable**.
4. Click **Apply**.

Preventing IP Attacks or Using Reverse Path Filtering

Reverse path filtering discards IP packets where the system cannot reach the source IP address within the same physical interface. If the IP path is not bidirectional and you enable this function, the network might lose connection to the node. Complete these steps to provision this protection mechanism.

1. Click **Node**.
2. Select **Security > Packet**.
3. In the **Controls** area, **Reverse Path Filter** field, select **Strict**.

Setting an NCU C2 Port to Node Management Only Mode

You can set the NCU C2 port to the **Node Management Only** mode to grant local access to the NE for encrypted-service end-users. This access allows for monitoring PMs and setting an encryption passwords.

Complete these steps:

1. Select **Node** > **Security** > **Packet**.
2. In the **Controls** area:
   a. In the **NCU Port C2** field select **Node Management Only**.
   b. Click **Apply**.

Generating SSL Certificates

1. Select **Node**.
2. Select **Security > SSL Details**.
3. In the **SSL Certificate Generation** area, specify the type of SSL configuration.
   a. **SSL Renew Mode**: Select between automatic and manual mode.
   b. **SSL Key Length**
   c. **SSL Validity Period [days)]**
   d. **SSL Certificate IP**
4. Click **Apply & Generate Certificate**.

Provisioning Write Access

This section contains these topics:

Write Access Requirements

To enable Write Access, you must be logged on with a user account that has ADMIN privileges.

To request Write Access, you must be logged on with a user account that has MONITOR privileges.

Write Access Usage

When this feature is enabled, the MONITOR user can request temporary "write access" to the network element.

When the user requests write access, the request is sent as an SNMP trap to all management stations. A receiver of this notification can allow or deny the request. If allowed, the MONITOR user is granted PROVISION rights for 1 - 480 minutes. Afterward, the MONITOR rights are restored.

Enabling Write Access

1. Select **Node**.
2. Select **Security > Access**.

3. Select the **Access Management** area.
4. From the **Central Write Access** list, select **Enable**.
5. Click **Apply**.

Anonymous Logging

The system removes all user identity from log entries that exceed the number of days admin users specify in the interval setting. The anonymization process occurs every midnight local time after each system reboot. By default, the log anonymization feature is disabled.

To set the deletion of user ID in logs:

1. Select **Node** > **Security** > **Access**.
2. In the **Log** area, select the **Mask User Name** field.
3. In the **Mask User Name Delay [day]** field, enter the time interval.
4. Click **Apply**.

> The system deletes ID logs from **System**, **Database Change** and **Crypto**.

Configuring an Audit Events

The system can generate an detailed audit record. See the audit events list in the table below.

Table 5: The List of Audit Events

Functionality	Audit Record
General functionalities	• Syslog service start • Syslog service stop • All configuration changes • Changing access banner • Changing authentication parameters • Changing SSH parameters • Changing TLS parameters

Table 5: The List of Audit Events

Functionality	Audit Record
System time	• Changing time parameters • Changing time manually • Changing NTP parameters • Changing time NTP update success • Changing time NTP update failure
Software upgrade	• Software upgrade initialization • Software upgrade success • Software upgrade failure
Accounts and sessions	• Changing account property • Resetting account password • Exceeding login count limit • Account locking • Account unlocking • Account session inactivity termination • Account session manual termination
Public key infrastructure	• Changing cryptographic functionalities • Changing trust anchor • Key create • Key import • Key changing parameters • Key delete • Certificate create • Certificate import • Certificate changing parameters • Certificate delete • Certificate validation failure

Table 5: The List of Audit Events

Functionality	Audit Record
SSH protocol	• SSH accepting TCP connection • SSH closing TCP connection • SSH establishing connection success • SSH establishing connection failure • SSH password authentication success • SSH password authentication failure • Public key authentication success • Public key authentication failure • SSH re-keying operation • SSH account session open • SSH account session close
TLS protocol	• TLS accepting TCP connection • TLS closing TCP connection • TLS establishing connection success • TLS establishing connection failure • TLS connection close • Certificate validation success • Certificate validation failure • NED password authentication success • NED password authentication failure • NED account session open • NED account session close
Syslog	• Changing syslog parameters • Syslog TCP connection failure • TLS establishing connection failure • Certificate authentication failure

If you enable audit logs, the log-data amount will increase significantly. Therefore, before enabling them, consider your network bandwidth and log collector capacities.

To enable the audit events logs, complete these steps:

1. Select **Node** > **Security** > **Access**.
2. In the **Log** area, in the **Audit Logs** field, select **Enable**.

3. Click **Apply**.

Public Key Infrastructure (PKI)

The FSP 3000R7 uses digital certificates for HTTPS encryption. These certificates require public key infrastructure support. If a valid certificate has not been added, users accessing the FSP 3000R7 using HTTPS are warned by the browser that the connection to the FSP 3000R7 is not secure.

This section contains these topics:

Workflows

This section contains example workflows to provision the NCU web server keys and certificates. Each workflow uses configuration examples that are described in next sections.

The example workflows are:

- Using manual operations to provision NCU web server key and certificates.
- Configuring the NCU to automatically provision NCU web server key and self-signed certificate.

Manual provisioning of the certificate chain

Perform these tasks to manually provision the NCU web server key and certificate chain so that the NCU secure web server can establish TLS sessions with clients:

- Obtain a copy of the Root Certificate Authority (CA) self-signed certificate in PEM format.
- Obtain a copy of the Subordinate CA's certificate in PEM format.
- Install Root CA certificate in web client. See: Installing the Root CA certificate in the web client.
- Configure NCU database to hold a new certificate chain. See: Configuring Certificate Authorities.
- Note the IP address and fully qualified domain name of the NCU.
- Choose user-assigned CSR values. See: Choosing user-assigned CSR values.
- Generate a private key and CSR on the NCU with Renewal Mode set to Manual (Certificate). See: Configuring Cryptographic Keys.
- Manually get an NCU certificate from an authority. See: Manually getting the NCU Certificate.
- Activate the certificate chain in the NCU. See: Activating the certificate chain in the NCU.

- Confirm the web client trust of NCU certificate chain. See: Confirming the web client trust of NCU certificate chain.

During normal operations, the workflow can use these additional tasks as needed:

- Manually update CSR with new attributes for existing key.
- Export a certificate.
- Delete a certificate from the NCU data store.
- Delete a private key from the NCU data store.
- Delete a certificate chain from the NCU data store.

Automatic provisioning of self-signed certificate

If organization policy allows trust of NCU web servers that present self-signed certificates, this alternate workflow is available:

- Automatically generate a self-signed NCU certificate. See: Automatically generating a self-signed NCU certificate.

Choosing User-Assigned CSR Values

Choose public key parameters and identification values to put in the NCU's Certificate Signing Request (CSR). Have these values ready for use when adding or changing cryptographic keys. See: Configuring Cryptographic Keys.

Optionally identify the NCU's Unique Serial Identifier to use in labels. Navigate to **Overview** > **Inventory**. Find the row for the NCU, and note the NCU's Unique Serial Identifier.

1. Choose values for the private key parameters:
   - RSA key modulus bit length [2048|3072|4096]
   - User Label text string to label the key (0 to 64 characters)
2. Choose values for the certificate signing request:
   - `subject.commonName` string (1 to 128 characters); one of:
     - IP Address, matching `subjectAltName.iPAddress`
     - fully qualified domain name, matching `subjectAltName.dNSName`
   - Choose values for at least one `subjectAltName` entry:
     - `subjectAltName.iPAddress`
     - `subjectAltName.dNSName` (a fully qualified domain name or wildcard FQDN)

> Ensure that the IP address and FQDN values in the CSR match actual NCU provisioning. Web clients typically compare the IP address and/or the fully qualified domain name shown in the certificate with the session values.

If complying with CA/Browser Forum baseline certificate requirements for best interoperability with widely available web clients:

- for the FQDN, do not use an internal name
- in the FQDN, do not use underscores

Configuring Certificate Authorities

In this procedure you configure the NCU database to create a chain of certification. Use this procedure if the NCU secure web server has no certificate chain, or if the existing certificate chain will be removed from service. Before you start the procedure, ensure that a database slot is available for an additional certificate chain.

To complete these steps you must have a Simple Certificate Enrollment Protocol (SCEP) that supports the Certificate Authority.

> Remember that SCEP supports only RSA-based cryptography.

Adding Certificate Authorities

1. Select **Node** > **Security** > **Certificate Authorities**.
2. In the **Certificate Authorities (CA)** area, click the **Add** icon. Select the applicable **Identifier**.
3. (Optional) Enter a **User Label**.
4. In the **CA Configuration** area, **Use IP Subnet** field, select one of these:
   - **System**: for the system IP address.
   - **Default Gateway**: for physical LAN I/F on the NCU.
5. In the **SCEP Configuration** area, set the **SCEP URL**.
6. In the **Certificate Revocation Configuration** area, complete these fields:
   a. **CRL Method** select one of these:
      - **Base CRL (end-entity)**: to verify only the certificates requested by the NE.
      - **Base CRL (all)**: to also verify the certificates that originate from the Certificate Authority.

   b. **CRL Distribution Point**, specify where the CRL is published on the Certificate Authority server.

   c. **CRL Update Interval** select one of these:
      - **Manual**: for a manual CRL request.
      - **Interval**: for an automated CRL request.
7. If the Certificate Authority server restricts certificate issuance to a dedicated user, in the **SCEP Authentication** area specify the:

   a. **Domain** of Certificate Authority server.
   b. **User Name** of SCEP user.
   c. **Password** of SCEP user.

8. In the **SCEP Advanced Configuration** area:
   a. Enter the **SCEP Query Message**.
   b. (Optional) Set the remaining parameters.
9. (Optional) In the **Certificate Validation Requirements** area, complete the relevant settings.
10. Click **Add**.

> To set SCEP queries, when you enter the **SCEP URL**, add the port IP address.

Authenticating Certificate Authorities

1. Select **Node** > **Security** > **Certificate Authorities**.
2. In the **Certificate Authorities (CA)** area, select the Certificate Authority server.
3. In the **Configure Details** window, **CA Authentication** area, click **Update**.
4. Select **Node** > **Security** > **Certificates & Keys** > **Certificates**.
5. In the **Certificates** area, select the certificate entity.
6. In the **Configure Details** window, complete these settings:
   a. **Certificate Identity**, use the SHA fingerprint to validate the authenticity of the certificate.
   b. **Certificate Configuration**, set the trust settings to trusted.
7. Select **Apply & Exit**.
8. If you receive certificates for the sub and root Certificate Authority, repeat the procedure for the second certificate.
9. Select **Node** > **Security** > **Certificate Authorities**.
10. In the **Certificate Authorities (CA)** area, select the Certificate Authority server.
11. In the **Configure Details** window, **CA Authentication** area, click **Update**.

> In the **CA Authentication** area, after you specify the **SCEP URL** in the **SCEP Configuration** area, the **Update** button becomes available.
>
> Click **Update** to automatically obtain Certificate Authority certificates.

Editing Certificate Authorities

1. Select **Node** > **Security** > **Certificate Authorities**.
2. In the **Certificate Authorities (CA)** area, click the proper identifier.
3. In the **Configure Details** window, edit these parameters:
   - **SCEP Configuration**
   - **SCEP Authentication**
   - **SCEP Advanced Configuration**
   - **CA Configuration**
   - **Certificate Revocation Configuration**
   - **Certificate Validation Requirements**
   - **Alarm Severities**
4. Click **Apply & Exit**.

In the **CA Configuration** area, **CRL Method** field, select **Base CRL (end-entity)**, so that certificate revocation validation can proceed.

See also Provisioning the Domain Name System

Configuring Cryptographic Keys

To enable the NCU secure web server to establish Transport Layer Security (TLS) sessions with clients, you must provision the NCU with a private key. Provision a private key if the NCU secure web server has no private key, or if you want to remove the existing private key from service. After you provision the private key, obtain an NCU certificate, which is also required to establish a TLS session.

After you complete this procedure, the NCU will have an RSA or ECDSA private key and a certificate signing request (CSR). The CSR shows the NCU public key and identity elements that you need for a certificate.

Adding Cryptographic Keys

1. Select **Node** > **Security** > **Certificates & Keys**.
2. In the **Keys** area, click add icon to open the **Cryptographic Keys** window.
3. Select **Identifier**.
4. (Optional) Enter the **User Label**.
5. In the **Cryptographic Key Configuration** area, complete these settings:
   a. **Key Algorithm**: select the applicable RSA or ECDSA algorithm. Keep in mind that SCEP supports only RSA-based cryptography.
   b. **Key Length**: select the applicable value, or select a value of greater length based on the local security policy.

c. **Key Profile**: select the profile where you plan to use the key.

d. **Key Exportable**: select **Yes** to later export the key from the NCU. The default is **No**. Be mindful that you cannot change this setting after you create the key.

6. In the **Key And Certificate Renewal** area:

a. Set the **Renewal Mode** according to your network plan:

Field	Description
Automatic (All)	The system renews the key, and then renews the certificate for the newly acquired key according to the period set in the Renewal Interval/Period.
Manual (All)	The software renews the key, and then renews the certificate for the newly acquired key. You must start this process manually.
Automatic (Certificate)	The software renews the certificate only for the existing key according to the period set in the Renewal Interval/Period.
Manual (Certificate)	The software renews the certificate only for the existing key. You must start this process manually.
Manual (CSR only)	not applicable

b. In the **Certificate Authority** list, specify the previously established value for this certificate chain, such as PKI_CA-1. If you set this field to **NONE** the CSR export will fail. Instead the software will automatically generate a self-signed NCU public key certificate.

If you set Renewal Mode to Automatic (All) or Automatic (Certificate), you must set the Renewal Interval/Period according to the certificate authority operator policy. Make sure that you set the Renewal Interval/Period length to be in effect for the validity period of the certificate that you plan to renew.

A single key can have only four associated certificates.

If the certificate-authority server experiences connection issues, the system will try to renew the certificate every 12 hours until the current certificate is no longer valid.

7. In the **Certificate Request Configuration** pane, complete these settings.

Field	Description
Common Name	Enter the IP address or the fully qualified domain name of the NCU.
Alternative Name (IP)	Enter the IP address that web clients use to reach the NCU web services. This option is unavailable if you use Module Authentication as the key profile.
Alternative Name (DNS)	Enter the IP address that web clients use to reach the NCU web services. This option is unavailable if you use the Module Authentication key profile.
Subject/Equipment Serial No	Enter the applicable information. This option is available only if you use the Module Authentication key profile.
Key Usage	Select None (Unspecified).
Extended Key Usage	• Server Authentication: select if you use a web service or the gRPC Network Management Interface (gNMI) service as the key profile. • Client Authentication: select if you use an authentication module or Quantum key distribution (QKD) authentication as the key profile.
Validity Period	Select the value defined in your network plan.
Request Challenge	Leave empty.

The Request Challenge option displays only if you previously configure and select the certificate authority. Some certificate authority operators require additional authentication for use with the Simple Certificate Enrollment Protocol (SCEP) protocol. Ask your certificate authority operator for information about this setting.

Continue with these steps.

1. In the **Advanced Renewal Configuration** area, complete these settings:
   a. **Renewal Retry Condition**: select **Any Failure** to instruct the system to retry the renewal after any failure. If you select **Resource Failure** the system retries a failure only for a resource failure. A resource failure occurs if the NCU has the maximum number of key entities.
   b. **Renewal Retry Interval**: select a value according to your network plan.
   c. **Renewal Retry User Limit**: select a value according to your network plan.
2. Click **Add** to confirm, or click **Cancel**.

Editing Cryptographic Keys

🗎	If the the authorization scheme for certificate renewal uses the certificate identity CSR values, do not change these values. If you change these values, the renewal process can fail. If you need to change certificate identity CSR attributes, use one of these options: • Change the authorization scheme for certificate renewal to use only the request challenge password. • Remove the current certificates before the certificate renewal.

1. Select **Node** > **Security** > **Certificates & Keys** > **Keys**.
2. In the **Keys** area, click the relevant **Identifier** to open the **Configure Details** window.
3. In the **Configure Details** window, edit the required parameters in these areas:
    - **Cryptographic Key Configuration**.
    - **Certificate Request Configuration**.
    - **Key And Certificate Renewal**.
4. Click **Apply & Exit** to confirm, or click **Cancel**.

Exporting Cryptographic Keys

🗎	You can export the cryptographic key if it is exportable. You can set the Key Exportable parameter only when you add a new key.

1. Select **Node** > **Security** > **Certificates & Keys** > **Keys**.
2. In the **Keys** area, click the relevant **Identifier** to open the **Configure Details** window.
3. In the **Key Import/Export** area, set the encryption password, and then click **Export**.
4. If you want to erase the cryptographic key export data, leave the password field empty, and then click **Erase**. This action will not erase the cryptographic key itself.

Manually Getting the NCU Certificate

Manually obtain a certificate from an authority outside the NCU to advertise the NCU secure web server public key and identity so that the NCU secure web server can establish TLS sessions with clients.

Use this if the NCU has no certificate or you want to take the existing certificate out of service. Use this when client and organization policies allow trust of servers that present certificates from a trusted certification authority.

Before performing this procedure:

- Ensure that the NCU has been provisioned to keep track of this chain of certificates. See: Configuring Certificate Authorities.
- Ensure that the NCU secure web server has a private key. See: Configuring Cryptographic Keys.
- Obtain the PEM text file that contains the NCU's Certificate Signing Request (CSR). See: Configuring Cryptographic Keys.

Submitting CSR to a Certificate Authority

Submit the NCU's CSR to the certification authority using the procedures established by that authority.

Receiving the NCU Certificate Chain from a Certificate Authority

From the certification authority, receive a copy of each certificate in the certificate chain, formatted as separate PEM files:

- NCU certificate
- Subordinate CA certificate
- Root CA certificate

Take note of identity information for each certificate, such as certificate serial number and issuer name. Optionally use a personal computer to view certificate information. For instance, on Windows computers, a certificate viewer is launched by clicking on a PEM certificate file that is named with the extension "crt" or "cer".

Configuring Public Key Certificates

To manually install the Root CA certificate on the NCU, use a text editor to view the file that contains the PEM-formatted Root CA certificate. Copy the contents of the file to the copy/paste buffer.

To manually install the Subordinate CA certificate on the NCU, use a text editor to view the file that contains the PEM-formatted Subordinate CA certificate. Copy the contents of the file to the copy/paste buffer.

To manually install the NCU certificate on the NCU, use a text editor to view the file that contains the PEM-formatted NCU certificate. Copy the contents of the file to the copy/paste buffer.

📝	The NCU applies some logic checks to certificate contents and indicates **Activation Status** of **Not Ready** for bad attributes. For the NCU certificate, if the keyUsage and sign extensions are present, the NCU checks to see that both the keyEncipherment and digitalSignature bits are set. For the NCU certificate, if the extKeyUsage extension is present, the NCU checks to see that the serverAuthentication bit is set.

Adding Public Key Certificates

1. Select **Node** > **Security** > **Certificates & Keys** > **Certificates**.
2. In the **Certificates** area, click the **Add** icon to open the **Public Key Certificates** window.
3. Select the **Identifier** from the list.
4. Enter the Certificate Data (PEM) in the **Certificate Import/Export** area.
5. In the **Certificate Attributes** pane, confirm that the Issuer and Serial Number values match the expected values.
6. In the **Certificate Configuration** pane, change the **Certificate Authority** selection from **NONE** to the previously established value for this certificate chain, for example: "PKI_CA-1".
7. For a CA certificate:
   - Verify authenticity of the CA certificate to be marked as trusted, comparing fingerprint from the **Certificate Identity** pane with the fingerprint you have obtained. See: Workflows.
   - In the **Certificate Configuration** pane, change the **Trust Setting** from **Not Trusted** to **Trusted**.
8. Click **Add** to confirm.
   -or-
   Click **Cancel** to abort.

For Root CA certificate confirm that:

- the **Certificates** pane on the web page has a new row for the Root CA certificate,
- the row shows **Validity Status** for the new certificate is **Valid**,
- the row shows **Trust Setting** for the new certificate is **Trusted (Root Authority)**.

For Subordinate CA certificate confirm that:

- the **Certificates** pane on the web page has a new row for the Subordinate CA certificate,

- the row shows **Validity Status** for the new certificate is **Valid**,
- the row shows **Trust Setting** for the new certificate is **Trusted (Authority)**.

For NCU certificate confirm that:

- the **Certificates** pane on the web page has a new row for the NCU certificate,
- the row shows **Validity Status** for the new certificate is **Valid**,
- the row shows **Activation Status** for the new certificate is **Ready**.

Editing Public Key Certificates

1. Select **Node** > **Security** > **Certificates & Keys** > **Certificates**.
2. In the **Certificates** area, click the relevant certificate to open the **Configure Details** window.
3. Edit the required parameters.
4. Click **Apply & Exit** to confirm
   or
   Click **Cancel** to abort.

Installing the Root CA Certificate in the Web Client

Use client-specific operations to load the Root CA certificate into the store of certificates that are trusted for web server authentication.

Before performing this procedure, obtain a copy of the Root CA certificate. See: Manually getting the NCU certificate.

Activating the Certificate Chain in the NCU

Activate the chain of certificates that the NCU will show a web client for subsequent TLS sessions.

Use this to change the credentials that the NCU shows to clients. Use this if a certificate in the previous chain is no longer valid or becomes untrusted.

Before performing this procedure, establish a private key and certificate in the NCU. See: Configuring Cryptographic Keys, Manually getting the NCU certificate and Installing the Root CA certificate in the web client.

1. Select **Node > Security > Certificates & Keys > Certificates**.
2. In the **Certificates** area, click therelevant NCU certificate to open the **Configure Details** window.
3. In the **Certificate Activation** area, click **Activate**.

The Activate button shows **In Progress** for a few moments. After that the **Activate** button is grayed out and the **Activation Status** is **Active**.

If the **Activation Status** indicates Key Duplicates Error:

- You might have added identical keys with different key profiles, but you did not assign the certificate purpose. Set the **Certificate Purpose** of the certificate to the same value as the **Key Profile** of the corresponding key.

- You might have added identical keys with the same key profile. Delete the duplicate key.

4. Close the Configure Details window.
5. In the **Keys** area, confirm that **Activation Status** is **Active** for the key that was created in Configuring Cryptographic Keys.

Confirming the Web Client Trust of NCU Certificate Chain

Use client-specific operations to open a fresh session to the NCU web server. For instance, close the web browser, then reopen it and navigate to the NCU. Examine the web browser's indications of web site security. Confirm that the web browser now trusts the NCU's certificate chain.

Exporting a Certificate

Export a certificate from the NCU in PEM format.

Use this procedure to allow applications outside the NCU to examine a certificate's technical details. Use this procedure to export trusted certificates for installation on other hosts that are also to trust them.

1. Select **Node** > **Security** > **Certificates & Keys** > **Certificates**
2. In the **Certificates** area, click the row with the certificate to be exported to open the **Configure Details** window.
3. In the **Certificate Import/Export** area, select and copy the PEM text including the hyphens before "BEGIN CERTIFICATE" to the hyphens after "END CERTIFICATE".
4. Paste the text into a text editor and save the PEM text to a file, for example: `Exported_cert.crt`.

Deleting a Certificate from the NCU Data Store

Delete an unused certificate from the NCU data store.

Use this procedure when a certificate has expired and been replaced, or when a chain of certificates has been replaced.

1. Select **Node > Security > Certificates & Keys > Certificates**.
2. In the **Certificates** area, confirm that the row with the certificate shows **Activation Status** with any value other than **Active**.
3. Click the row with the certificate to be deleted to open the **Configure Details** window.
4. In the **Certificate Configuration** area, set the **Certificate Authority** to **NONE**.
5. Click **Apply** and wait a moment for the window to refresh.
6. Click **Delete**.
7. Click **Delete** to confirm.
   -or-
   Click **Cancel** to abort.

Deleting a Private Key from the NCU Data Store or Smartcard

Delete an unused private key from the NCU data store or Smartcard.

Use this procedure when a private key is retired from service and has been replaced.

Before performing this procedure, delete all associated certificates for this private key.

1. Select **Node** > **Security** > **Certificates & Keys** > **Keys**.
2. In the **Keys** area, confirm that the row with the certificate shows **Activation Status** with any value other than **Active**.
3. Click the row with the key to be deleted to open the **Configure Details** window.
4. In the **Key and Certificate Renewal** area, confirm that the list of **Associated Certificates** indicates **NONE**.
5. Click **Delete**. The message window opens.
6. In the message window, click **Delete** to confirm.

Deleting a Certificate Chain from the NCU Data Store

Delete an unused certificate chain from the NCU data store.

Use this procedure when a certificate chain is retired from service and has been replaced.

🗎	Network Element Director manages certificate chains in the **Certificate Authorities (CA)** pane.

1. Select **Node > Security > Certificate Authorities > Certificate Authorities (CA)**.
2. In the **Certificate Authorities (CA)** area, click the row with the certificate chain that is to be deleted to open the **Configure Details** window.
3. In the **CA Configuration** area, note any **Associated Certificates** that are listed.
4. In the **CA Authentication** area, note any **CA Certificates** that are listed.
5. Close the **Configure Details** window.
6. Select **Node > Security > Certificates & Keys > Certificates**.
7. In the **Certificates** area, for each associated certificate and CA certificate, click the row with the certificate top open the **Configure Details** window and then:
   - In the **Certificate Configuration** area, set **Certificate Authority** to **NONE**.
   - Click **Apply**.
   - After the window refreshes, confirm that the change happened, then click **Cancel** to close the window.
8. Click the row with the certificate chain that is to be deleted to open the **Configure Details** window.
9. Confirm that associated certificates and CA certificates now show **NONE**.
10. Click **Delete**.
11. Click **Delete** to confirm.
    -or-
    Click **Cancel** to abort.

Automatically Generating a Self-Signed NCU Certificate

Automatically provision the NCU with a self-signed certificate so that the NCU secure web server can establish TLS sessions with clients.

Use this when client and organization policies allow trust of servers that present self-signed certificates. Use this if you want the NCU to automatically generate a fresh certificate at the expiration of the current self-signed certificate.

1. Select **Node** > **Security** > **Certificates & Keys**.
2. In the **Keys** area, click add icon to open the **Cryptographic Keys** window.
3. Select **Identifier**.
4. (Optional) Enter the **User Label**.
5. In the **Certificate Request Configuration** pane:
   - Set **Common Name** to the IP address or fully qualified domain name of the NCU.
   - Set the **Alternative Name (IP)** to the IP address that web clients use to reach the NCU web services.
   - Set the **Alternative Name (DNS)** to the fully qualified domain name of the NCU.
   - In the **Key Usage** selection area, select **None/Unspecified**.

- In the **Extended Key Usage** selection area, select **Server Authentication**.
- Set the **Validity Period** according to your network plan.
- Leave **Request Challenge** blank.

6. In the **Cryptographic Key Configuration** pane:
   - Set the **Key Length** to **2048**.
   - Set the **Key Algorithm** to RSA or ECDSA.
7. In the **Key And Certificate Renewal** pane:
   - Set the **Renewal Mode** to **Automatic**.
   - Set the **Certificate Authority** to **NONE**.
8. Click **Add**.

Continue with these steps:

1. Click the **Refresh** button.
2. In the **Keys** area, confirm:
   a. The pane shows the new key row.
   b. The new key **Activation Status** is **Ready**.
3. In the **Certificates** area, confirm:
   a. The pane shows the new certificate row.
   b. The **Valid From (local)** and **Valid To (local)** values are correct.
4. Click the row with the new certificate. The **Configure Details** window opens.
5. In the **Configure Details** window, in the **Certificate Activation** area:
   a. Confirm that the **Activation Status** is **Ready**.
   b. Click **Activate**.
6. When the connection error window shows, refresh the web page.

> If the NCU web server uses a self-signed certificate, the web browser might shows the security warning.

7. If a browser security warning shows, accept the risks and proceed.
8. Log into the NCU and navigate to **Node** > **Security** > **Certificates & Keys**.
9. In the **Keys** area, in the new key row, confirm that the **Activation Status** is **Active**.

Configuring SSH Authentication

You can add SSH key-pair and a public key to authenticate remote entities.

Adding Cryptographic Keys

1. Select **Node** > **Security** > **Certificates & Keys**.
2. In the **Keys** area, click add icon to open the **Cryptographic Keys** window.
3. Select **Identifier**.
4. (Optional) Enter the **User Label**.
5. In the **Cryptographic Key Configuration** area,set these settings:
   - **Key Algorithm**: select RSA or ECDSA algorithm.
   - **Key Profile**: select **SSH/SFTP Authentication**.

> If you export the Privacy Enhanced Mail (PEM) version of the key, which you want to use while you create a key, use these steps.
>
> 1. In the **Key Import/Export** pane, **Key Data (PEM)** field, paste the key data.
> 2. Click **Add** to complete key creation process.

   - **Key Length**: select the applicable value unless the local security policy requires a key with a longer length.
   - **Key Exportable**: If you want the NCU to later export the key, select **Yes**. The default is **No**.

> After you create the key, the Key Exportable setting is set; you cannot change it.

6. Click **Add**.

Enabling SSH Authentication

1. Select **SSH Authentication**.
2. From the **SSH Authentication Key** list, select the key to use for ssh authentication.
3. Click **Apply**.

> After the completion of this procedure, a new **SSH Public Key** will be available. You can use this key to authenticate remote entities. To do so, you need to manually add this key to the trusted list on the remote servers.

Configuring Module Authentication

- Digital certificates enable each optical network line card in a communicating pair to authenticate the partner line card, and prove origin authenticity and integrity for key agreement messages that are exchanged between the pair. The currently supported modules are:

- 5TCE-PCN-10GU+AES10G
- 5TCE-PCTN-10GU+AES10G
- 10TCE-PCN-16GU+AES100G
- 4TCC-PCN-32GU+AES100GU
- WCC-PCN-AES100GB
- 9TCE-PCN-10GU+AES10G

> Before setting the module authentication make sure that in the **Node > Security> Certificates & Keys > Keys** area **Key Profile** of the key, that you want to use for module authentication, is set to **Module Authentication**. For more information refer to Configuring Cryptographic Keys.
>
> Furthermore, make sure that in the **Node > Security> Certificates & Keys > Certificates** area **Certificate Purpose** of certificate, that you want to use for module authentication, is set to **Module Authentication**. Only CA-signed certificates are accepted. For more information refer to Configuring Public Key Certificates.

1. Select **Node** > **Security Applications** > **Module Authentication**.
2. In the **Module Authentication** area, in the **Near End Certificate** list, select a certificate that you want to use for module authentication.
3. In the **Far End Default CA** list, select the Certification Authority to use for validation of Far-End certificates.
4. Click **Apply**.
5. Select **Maintain > Shelf** and select a module that you want to enable module authentication on.
6. In the **Module Encryption** area, click **Change** to open **Change - PKI Operation** window.
7. In the **Change - PKI Operation** window, select **Enable**, type the Crypto Officer Password and click **Change**.

> You must configure the Far-End Node in the same way in order to form a connection.

Configuring gRPC Network Management Interface (GNMI)

Before setting the GNMI service make sure that in the **Node > Security > Certificates & Keys > Keys** area **Key Profile** of the key, that you want to use for GNMI service, is set to **GNMI Service**. For more information refer to Configuring Cryptographic Keys.

Furthermore, make sure that in the **Node > Security > Certificates & Keys > Certificates** area **Certificate Purpose** of certificate, that you want to use for GNMI service, is set to **GNMI Service**. For more information refer to Configuring Public Key Certificates.

To provision GNMI, enable it under **Node > General > Controls** in the **Interfaces** area .

> To enable GNMI you have to enable NETCONF interface first. It is enabled by default starting with release 19.3.1. To enable it manually, navigate to **General > Controls** and in the **Interfaces** area set **NETCONF Interface** to **Enable**.

1. Select **Node > Security Applications > GNMI**.
2. In the **gRPC Network Management Interface (GNMI)** area, in the **Server Certificate** list, select the certificate that you want to use for GNMI service.
3. Click **Apply**.

Configuring the Transport Layer Security Protocol

Complete these steps to configure the Transport Layer Security (TLS) protocol.

Manually Generating a TLS Certificate

1. Select **Node** > **Security Applications** > **HTTPS**.
2. In the **Certificate Generation** area:
   a. **Renew Mode** field, select **Manual**.
   b. Click **Apply**.
   c. Complete these fields:
      - **Key Length** - select the relevant key length.
      - **Valid Period [years(s)]** - select a validation period for the certificate.
      - **Certificate IP** - select the valid IP address for the certificate.
   d. Click **Apply & Generate Certificate**.

Changing TLS Authentication

To change the supported TLS version:

1. Select **Node** > **Security Applications** > **SSL/TLS**.
2. In the **Transport Layer (TLS) Autentication** area, TLS Versions fields, select the applicable versions.
3. Click **Apply**.

Configuring TLS Ciphers

The FSP 3000R7 supports several Transport Layer Security (TLS) cipher versions.

> To meet high security standards, use the default or CSfC profile.

> If you remove all ciphers from the current TLS version, your next login might fail.

Complete these steps to configure TLS ciphers:

1. Select **Node** > **Security Applications** > **SSL/TLS**.
2. In the **TLS Ciphers** area:
   a. In the **TLS Ciphers Profile** field, select one of these options:
      - **Default**, the system resets to the default ciphers.
      - **Custom**, the system displays the installed ciphers for **TLS1 Algorithms**, **TLS 1.2 Algorithms** , and **TLS 1.3 Algorithms**. Select or clear ciphers as they apply to your network.
      - **CSfC** - To select this option, you must first select only TLS 1.2 version in **Transport Layer Security (TLS) Authentication** area. For this setting, the system uses only TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

   b. Click **APPLY**.

Configuring ECDHE Curves

> To meet high security standards, use the default or CSfC profile.

1. Select **Node** > **Security Applications** > **SSL/TLS**.
2. In the **ECDHE Curves** area:
   a. In the **ECDHE curves Profile** field, select one of these options:
      - **Default**, the system resets to the default curves.
      - **Custom**, the system displays the installed curves. Select or clear curves as they apply to your network.
      - **CSfC** - the system uses only NIST secp384r1.

   b. Click **APPLY**.

Configuring the Secure Socket Shell Protocol

Complete these steps to configure the Secure Socket Shell (SSH) protocol.

Setting the SSH Protocol

Set the SSH protocol to establish secure communication with the node. The NE supports only SSH version 2.

1. Select **Node** > **Security Applications** > **SSH**.
2. In the **Known Host IP Address** area, click the add icon.
3. In the **Add Fingerprint** window:
   a. Enter the **Known Host IP Address**.
   b. Select **SSH Key Encryption**.
   c. Enter the **Fingerprint** in hex format.
4. Click **Add**.

Configuring SSH Ciphers

The FSP 3000R7 supports several Secure Socket Shell (SSH) cipher versions.

🗎	To meet high security standards, use the default or CSfC profile.

🗎	If you remove all ciphers from the current SSH algorithm, your next login might fail.

Complete these steps to configure the SSH ciphers:

1. Select **Node** > **Security Applications** > **SSH**.
2. In the **SSH Ciphers** area:
   a. In the **SSH Ciphers Profile** field, select one of these options:
      - **Default** - the system resets to the default ciphers.
      - **Custom** - the system displays the installed ciphers for the **Host Key Algorithm**, **Key Exchange Algorithm**, **SSH Encryption Algorithm** and **SSH MAC Algorithm**. Select or clear ciphers as they apply to your network.
      - **CSfC** - the system uses only:
        - Host key: ecdsa-sha2-nistp384
        - Key exchange: ecdh-sha2-nistp384 and diffie-hellman-group15-sha512
        - Encryption + MAC: AEAD_AES_256_GCM

   b. Click **APPLY**.

Configuring Quantum Key Distribution (QKD)

This section contains these topics:

Configuring Certificates and Private Keys

The procedures described below must be performed for both modules (Master and Receiver), with proper end-entity certificates for each.

Provisioning Certificate Authority (CA)

1. Select **Node** > **Security** > **PKI** > **Certificate Authorities (CA)**.
2. Click **Add**.
3. In the Certificate Authorities window:
   a. From the **Identifier** list, select the first available value, e.g. "PKI_CA-1".
   b. Enter **User Label**.
   c. Leave all other parameters blank.
   d. Click **Add**.

Generating private key and Certificate Signing Request (CSR)

1. Select **Node** > **Security** > **PKI**.
2. In the **Keys** area, click **Add** to open the Cryptographic Keys window.
3. In the Cryptographic Keys window:
   a. From the **Identifier** list, select the first available value, for example: "PKI_KEY-2".
   b. Enter **User Label**.
4. In the **Certificate Request Configuration** area of that window:
   a. Set **Common Name** to the domain name of the NCU.
   b. Set **Alternative Name (IP)** to the IP address of NCU.
   c. Set **Alternative Name (DNS)** to the domain name of the NCU.
5. In the **Cryptographic Key Configuration** area of that window, set **Key Length** to 2048 unless local security policy requires longer length.
6. In the **Key And Certificate Renewal** area of that window, set **Certificate Authority** to the previously established value for this certificate chain, e.g. "PKI_CA-1".

> Setting this field to **NONE** will inhibit export of the CSR and instead generate a self-signed NCU certificate.

7. Leave all other parameters blank.
8. Click **Add**.
9. After a few moments delay, confirm that a new row appears in the list of keys.
10. Click on the row with the new key to open the Configure Details window.

11. From the **CSR Export** area, copy the entire PEM text contents (beginning and ending with hyphen characters) to a text editor.
12. Save the PEM text as a file, for example: new_csr.pem
13. Click **Cancel** to close the Configure Details window.

Obtaining a certificate from certificate authority outside the NCU

1. Submit the NCU's CSR to the certification authority using the procedures established by that authority.

Manually installing Root CA on the NCU

Use a text editor to view the file that contains the PEM-formatted Root CA certificate. Copy the contents of the file to the copy/paste buffer.

> Combined certificates chain for certificate authorities are not supported. RootCA and SubordinaryCA must be added as separate entities.

1. Select **Node > Security > PKI**.
2. In the **Certficates** area, click **Add**.
3. In the Public Key Certificates window, from the **Identifier** list, select the next available label, for example: "PKI_CERT-2".
4. In the **Certificate Import/Export** area, paste in the text for the PEM-formatted Root CA certificate to **Certificate Data (PEM)** field.
5. In the **Certificate Configuration** area, change **Trust Setting** from **Not Trusted (Root Authority)** to **Trusted (Root Authority)**.
6. Click **Add**.

Manually installing Subordinary CA on the NCU

1. Select **Node > Security > PKI**.
2. In the **Certficates** area, click **Add**.
3. In the Public Key Certificates window, from the **Identifier** list, select the next available label, for example: "PKI_CERT-3".
4. In the **Certificate Import/Export** area, paste in the text for the PEM-formatted certificate to **Certificate Data (PEM)** field.
5. In the **Certificate Configuration** area, change **Trust Setting** from **Not Trusted (Authority)** to **Trusted (Authority)**.
6. Click **Add**.

Manually installing an end-entity certificate on NCU

The certificate should be obtained from the certification authority outside the NCU. See: Obtaining a certificate from certificate authority outside the NCU.

Use a text editor to view the file that contains the PEM-formatted certificate. Copy the contents of the file to the copy/paste buffer.

1. Select **Node > Security > PKI**.
2. In the **Certficates** area, click **Add**.
3. In the Public Key Certificates window, from the **Identifier** drop-down list, select the next available label, for example: "PKI_CERT-4".
4. In the **Certificate Import/Export** area, paste in the text for the PEM-formatted certificate to **Certificate Data (PEM)** field.
5. In the **Certificate Configuration** area, set **Trust Setting** to **End Entity**.
6. Click **Add**.

Configuring Encryption Modules

1. Provision encryption modules on both sides.
2. Set the Crypto Officer password for both modules:
   a. Select **Maintain**.
   b. Select the proper shelf and slot.
   c. Expand the **Module Encryption** area.
   d. Confirm that the Change Crypto Officer Password window opens (the window will not open if the Crypto Officer password has already been set).
   e. Enter “CHANGEME.1” (default Crypto Officer password) in the **Current Crypto Officer Password** field.
   f. Enter a new Crypto Officer password and confirm the new Crypto Officer password.
   g. Click **Apply**.
3. Set the same Authentication Password on both modules:
   a. Select **Configure**.
   b. Select the proper shelf and slot.
   c. Click on the encryption module.
   d. Confirm that the Configure Details window opens.
   e. Click **Change Authentication Password**.
   f. Enter the Crypto Officer password.
   g. Enter a new Authentication Password and confirm the new Authentication Password.
   h. Click **Apply**.

4. Configure modules to be a part of QKD key-exchange:

> This must be performed for both modules (Master and Receiver), with proper end-entity certificates for each.

   a. Select **Maintain**.
   b. Select the proper shelf and slot.
   c. Expand the **Module Encryption** area.
   d. In the table under **QKD Operation**, click **Change** to open the Change QKD Operation window.
   e. Select the appropriate role for a module (Master or Receiver).
   f. Enter the **Crypto Officer Password**.
   g. Click **Change**.

5. Configure Target ID:
   a. Select **Configure**.
   b. Select the proper shelf and slot.
   c. Click on the encryption module.
   d. Confirm that the Configure Details window opens.
   e. Expand the **Encryption Connection** area.
   f. Enter the proper **QKD Target ID**, for example: "440110001".

> It is very important to enter the exact QKD Target ID that you have received with the QKD configuration. Without it the communication with the QKD Server will not work.

   g. Click **Apply & Exit**.

> Add Crypto Service operation is needed on configuration tab per enryption network for newly created CM/CM+ services.

Configuring Network Elements

The procedures described below must be performed for both modules (Master and Receiver).

Configuring Quantum Key Distribution (QKD)

1. Select **Node** > **Security** > **QKD**.
2. In the **Quantum Key Distribution** area:
   a. Set **QKD** to **Enable**.
   b. Enter the **QKD Server URL**.
   c. Set the **Client Key** from the list to previously configured entity of the private key, for example: "PKI_KEY-2".
   d. Set the **Client Certificate** from the list to previously configured entity of the end-entity certificate, for example: "PKI_CERT-5".
   e. Click **Apply**.

Checking the QKD Server Status

This functionality is only possible for the Master side.

1. Select **Node** > **Security** > **QKD**.
2. In the **QKD Server Status** area:
   a. Select the proper module AID from the **QKD Target ID for Module** list and confirm that **QKD Target ID** has been automatically set.
   b. Click **Start**.

Provisioning RADIUS or TACACS+

User access (log in) to a node can be supported from a RADIUS or a TACACS+ remote authentication server. Remote authentication requires:

- a network element configured to use RADIUS or TACACS+ authentication, as shown in the procedure below.
- at least one remote server configured for use and reachable from the network element.
- a shared secret for secure communication.
- user accounts with appropriate privilege mappings and passwords defined on the remote server.

NED supports up to 128 character password length.

Table 6: Privilege Level Mapping

NE	RADIUS		TACACS+
admin	Admin	4	12 - 14

Table 6: Privilege Level Mapping

NE	RADIUS		TACACS+
provision	Provision	3	8 - 11
operator	Operator	2	5 - 7
crypto	Crypto	6	4
monitor	Monitor	0	0 - 3

To provision RADIUS or TACACS+:

1. Click **Node**.
2. Select **Security > Access**.

> **Admin State** must be set to **In Service** for the node to access the remote server.

3. To change or delete a remote authentication server, in the **Remote Servers** area, select the server.
    a. In the Edit Server window, change the required information from your network plan and click **Apply**.
4. To add a remote authentication server, in the **Remote Servers** area, click **Add**,
    a. In the **Add Server** window, enter the required information from your network plan.
    b. Click **Add** to apply your settings.
5. In the **Access Management** area, set **Remote Authentication** to **RADIUS** or **TACACS+**.
6. Click **Apply**.

> When remote authentication is enabled, you will be logged out and must use the remote authentication user name and password to log in.

> Three remote servers are configured by default. These may be edited or new servers may be added by deleting previously configured ones.

Securing an HD Management Connection

To add an HD shelf map, complete these steps:

1. Select **Overview**.
2. In the navigation tree, select **Management Network** > **Interfaces**.
3. Select the **Management HD Shelves** area.
4. Click the add icon.
5. In the **Add Shelf Map** window, complete relevant fields according to your plan.
6. Click **Apply**.

To secure a connection to the HD shelf, complete these steps:

1. Select **Node**.
2. In the navigation tree, select **Security Applications** > **HD Shelves**.
3. In the **HD Secure Connection** pane, **HD Secure Connection** field, select **Enable**.
4. Click **Apply**.

Configuring a Pre-operational Self-Tests

The FSP 3000R7 performs a self-check procedure before starting the operating system. After each boot, the system uses SHA2-384 digests to validate the integrity of software files and validates the cryptographic functions using Known Answer Tests (KAT). You can select one of these expected system states in case of test failures:

- Operational
- Non-Operational

In the non-operational state, the Mod LED on the front NCU panel blinks with alternating yellow-red. The system does not provide any remote administration interface. However, you can still connect to the system through a serial RJ45 interface. Once you gain access, the system:

- Provides a POST execution report.
- Allows access to the system shell.
- Allows you to reboot the system.
- Allows you to try to reach the operational state.

Configuring POST Control

1. Select **Node** > **General** > **Controls**.
2. In the **Functionality** area, **Selftest Fail Control** field, select one of these options:

  - **Operational**
  - **Non-operational**

3. Click **Apply**.

Configuring TLS Mutual Authentication

You can configure mutual authentication for communication between a node and a client to:

- Secure the identity of node and client endpoints.
- Protect the data from disclosure.
- Detect data modification.

If you configure mutual authentication, according to RFC 5246:

- The node will send the TLS handshake protocol certificate request message.
- The client browser must respond with certificate and certificate verify messages.
- The node will validate the provided certificate and signature.

> Ensure that you configure the proper certificate in your browser before enabling mutual authentication. Failure to do so may cause you to lose connectivity to the NE.
>
> Ensure that end-entity certificate identifies the computer with a WEB browser, so NCU can recognize an authorized computer.

> For TLS mutual authentication, follow these guidelines:
>
> - To specify the IP address of the client using the certificate, you must define it either in the Subject Alternative Name (SAN) extension or the Common Names (CN).
>   If you choose to define the IP addresses in the SAN extension, the system will not perform a check on the CN.
>   You can define multiple IP addresses in the SAN extension.
> - To verify the Certificate Revocation List (CRL) for TLS mutual authentication, you need to set the CRL mode on the Certificate Authority (CA) entity to strict (all). This mode requires you to download all CRLs for the entire certificate chain. This ensures that the system can verify if any certificates in the chain have been revoked.
>
> Regarding the system:
>
> - The system takes into account CRL addresses defined in the CRL Distribution Points (CDP) extension on CA certificates.
> - The system considers one additional address on the CA entity.
> - The system does not consider CRL addresses in the CDP on end-user certificates.

To provision mutual authentication, complete these steps:

1. Add and authenticate certificate authorities. See Configuring Certificate Authorities.
2. Download CRLs:
   a. Select **Node** > **Security** > **Certificate Authorities**.
   b. Select the relevant CA.
   c. In the **Certificate Revocation Configuration** area:
      a. In the **CRL Method** field, select **Strict Base CRL (all)**.
      b. If necessary, in the **CRL Distribution Point**, enter an additional address for the CRL.
      c. Select the relevant **CRL Update Interval**. You can also click **Update** to manually update the CRL.
      d. Click **Apply**.
3. Set CA certificates **Trust Setting** to **Trusted**. See Configuring Public Key Certificates.
4. Import and install the required certificate files on your local computer.
5. Select **Node** > **Security Applications** > **HTTPS**.
6. In the **Client Authentication** area:
   a. Select the relevant **Client Authority**.
   b. Click **Apply**.
   c. In the **Client Authentication** field, select **Enable**.
   d. Click **Apply**.

Using Node Profiles

This section contains these topics about node profiles:

Background Information

You can save the settings for selected node level parameters in a Node Profile. The Node profile can be exported then imported on other nodes. The following parameters are included in the Node Profile.

Using node profiles requires ADMIN level user privileges.

Node Profile Parameters

NED Parameter Name	TL1
Security Mode = Basic	SECURITY-MODE=BASIC
NCU Boot Loader Access = Enable	BOOTLOADER_ACCESS=ENABLE
Login Presentation = Prompt/Product Details	SYSINFO-PRELOGIN=ENABLE
SNMPv1 and v2c = Enable	SNMP-V1=ENABLE
SNMPv3 = Enable	SNMP-V3=ENABLE
Authentication Traps = Disable	AUTH-TRAPS=DISABLE
Extended Auth Traps = Disable	EXT-AUTH-TRAPS=DISABLE
Secure SNMPv3 Access = Disable	SECURE-SNMP-V3=DISABLE
UDP Port = 161	UDPPORT=161
IPv6 UDP Port = 161	UDPPORTV6=161
FTP Client = Enable	FTPC=ENABLE
FTP Server = Disable	FTP=DISABLE
Telnet Interface = Enable	TELNET=ENABLE
SSH Interface = Enable	SSHD=ENABLE
Web Interface = Enable	WEB=ENABLE
TL1 Interface = Disable	TL1=DISABLE
Show Last Success Login = Disable	SHOW-LAST-LOGIN-SUCCESS=DISABLE

NED Parameter Name	TL1
Show Last Failed Login = Disable	SHOW-LAST-LOGIN-FAIL=DISABLE
Password History Length = 0	PID-HISTORY-SIZE=0
Min Password Length = 8	PID-MIN-LENGTH=8
Account Lockout Period = 86400	UNLOCK-TIME=86400
Account Lockout = Do Not Lock Last Admin	LOCK-SAFETY=ENABLE
Login Failure Delay = 2	LOGIN-FAIL-DELAY=2
Packet Filter = Disable	PACKET-FILTER=DISABLE
ICMP Filter = Disable	ICMP-FILTER=DISABLE
Denial of Service Guard = Enable	DOS-GUARD=ENABLE
Access Warning = Disable	ACCESS_WARNING=DISABLE
Access Warning = ""	ACCESS_WARNINGMSG=""

Generating a Node Profile

1. Select **Node**.
2. Select **Profiles** > **Node**.
3. In the **Generate Profile** area, click **Generate**.

The resulting file, node_profile.fcf, is stored on the NCU and the filename is displayed in the **Apply Profile** area.

Exporting a Node Profile

1. Select **Node**.
2. Select **Profiles** > **Node**.
3. In the **Export Profile** area, enter the information to save the node profile to the **Remote Port**.
   Follow any case-sensitive rules imposed by the remote server.
4. Click **Export**.

Importing the Node Profile

1. Select **Node**.
2. Select **Profiles** > **Node**.

3. In the **Import Profile** area, enter information to get a saved profile from the **Remote Port**.
   Follow any case-sensitive rules imposed by the remote server.
4. Click **Import**.

Applying a Node Profile

Apply a node profile to change the node level parameters to the values specified in the profile.

📝	Applying the node profile modifies multiple node level parameters in one step.

1. Select **Node**.
2. Select **Profiles > Node**.
3. In the **Apply Profile** area, select the desired profile.
4. Click **Apply**.

Managing Database

This section contains these topics:

Also see: Resolving ECM Database Mismatch

Manually Backing Up the Database

📝	To back up the database to your local computer, navigate to Node > General > Controls. In the Functionality area, Local Computer Transfer field, select Enabled.

1. Select **Node**.
2. Select **Database > Backup**.
3. In the **Manual Database Backup** area, select **Destination**.
4. Select other options as applicable.
5. Click **Backup**.

Scheduling Database Backup

You can schedule the database backup.

1. Select **Node**.
2. Select **Database > Backup**.
3. In the **Schedule Database Backup** area, select the **Destination** and other options as desired.
4. Click **Apply**.

When entering user name, the following characters are not allowed:

; | ` ' >

When entering password, the following characters are not allowed:

; | ` '>

When entering directory path name, the following characters are not allowed:

* ? ; | ` ' > < \t \\

When entering file name, the following characters are not allowed:

/ * ? ; | ` ' > < \t \\ ”

Encrypting Database Backup

You can encrypt the database backup file.

1. Select **Node**.
2. Select **Database > Backup**.
3. Select the **Destination** in the **Manual Database Backup** area.
4. Set **Encrypt Database Backup** to **Enable**.
5. Specify the encryption password and confirm.
6. Select other options as desired.
7. Click **Backup**.

Managing NCU Software

Update NCU software in the **Node** application under **Software > NCU**.

Users with ADMIN and PROVISION privilege level can:

- Transfer a new software release to the NCU standby area.
- Activate the NCU software in the NCU standby area.
- Schedule activation of the NCU software in the NCU standby area.
- Change a firmware package (FWP) to the active or standby area in the software release if required.

> First, the firmware package needs to be transferred to the Active NCU RAM using **Download** under **Node** > **File Storage**.

- Save descriptive comments about the active and standby software releases.

For detailed information about NCU software updates, refer to the *Maintenance and Troubleshooting Manual*.

Transferring Software to the NCU

This section describes how to transfer a software release from a remote server or local computer to the NCU. You must be logged on with an admin or provision privilege level account to continue.

> If the software version, you want to update, shows in the **Node** > **Software** > **NCU**, **Standby Software Release** area, the software is already installed and you need activate it.
>
> To perform an additional CON file signature validation, while the software is transferred to the standby area, under **Node** > **Software** > **NCU** in the **Software Standby Release** area, set the **Signature Validation** to **Enable**.

Remote Server

1. Select **Node**.
2. Select **Software** > **NCU**.
3. In the **Transfer Software to Standby Area** area, **Source Location** field, select **Remote Server**.
4. Select **FWP Download Mode** from the list:
    - **Required**, if you want to download only the firmware packages of equipped modules.
      -or-
    - **All**, if you want to download all the firmware packages for this software
5. Select **Transfer Protocol** from the list.

6. Select **Use IP Subnet** from the list:
   - **Default Gateway**, if the management network uses the range of the physical IP interfaces.
   - **System**, if the management network uses the range of the System IP addresses.
7. Enter the **IPv4/v6 Address** of the remote server.

Continue with these steps:

1. Enter **User Name** and **Password** to access the remote server.
2. (optional) Enter **Directory Path Name** on the remote sever.

> If the remote server is a GNE, set Directory Path Name to /cfdisk.

3. Enter **File Name** for the software configuration file (CON file).
4. Click **Transfer to Standby**.

The system transfers the software files to the NCU standby area. The transfer time depends on the connection bandwidth between the NE and remote server or local computer.

When the transfer is complete, the **Standby Software Release** area displays the software **Release**.

Local Computer

To enable software transfer from local computer, complete these steps:

1. Select **Node** > **General** > **Controls**.
2. In the **Functionality** area, **Local Computer Transfer** field, select:
   - **Download Only**
     -or-
   - **Upload & Download**
3. Click **Apply**.

To transfer software from local computer, complete these steps:

1. Select **Node**.
2. Select **Software** > **NCU**.
3. In the **Transfer Software to Standby Area** area, **Source Location** field, select **Local Computer**.

4. Click **Import** and then select the correct software configuration file (CON file).
5. For NCU-3, click **Import** and select the correct software configuration files:
   - E70*.PGM
   - S70*.PGM
6. For NCU-II, and NCU-II-P, click **Import** and select the correct software configuration files:
   - H70*.PGM
   - S70*.PGM
7. For NCU-S, click **Import** and select the correct software configuration files:
   - M70*.PGM
   - N70*.PGM

> Firmware M70*_FULL.PGM for NCU-S is not supported anymore.

8. If **Node** > **Software** > **NCU**, **Software Standby Release** area, **Signature Validation** field is enabled, click **Import** and then select the correct software configuration *.SIG files.
9. Click **Transfer to Standby**.

The system transfers the software files to the NCU standby area. The transfer time depends on the connection bandwidth between the NE and remote server or local computer.

When the transfer is complete, the **Standby Software Release** area displays the software **Release**.

> You can use any F7.CON for install. Transfer of native modules FWP to **Standby Software Area** will occur only if you use F7-FULL.CON with complete firmware package.
>
> For native modules FWP installation, see Transferring an Additional Firmware Packages to a NCU Standby Area.
>
> For HD-module firmware installation, see Transferring a FWPs of an HD Modules.
>
> This installation method does not handle or install firmware for AES cards.

Transferring a Firmware Package

You can download the firmware package (FWP) to the active NCU RAM, and then transfer the package to the active or standby area. The firmware package must have the release number compatible with the NCU software release.

1. Select **Node**.
2. Select **Software** > **NCU**.
3. In the **Transfer Firmware Package (FWP)** window:
   a. In the **Source Location** field, select **Active NCU RAM**.
   b. Select:
      - **Transfer to Active**.
        –or–
      - **Transfer to Standby.**
   c. Select a file.
   d. Click **Start**.

Start will be inactive until the system locates the PAK files on the active NCU RAM.

Transferring an Additional Firmware Packages to a NCU Standby Area

If you:

- Transfer software to the NCU,
- Set the **FWP Download Mode** to **Required** (see Transferring Software to the NCU),
- And then add shelves or modules to the node,

the firmware packages you need to update these shelves and modules might be absent from the NCU standby area. Complete these steps to transfer any additional FWPs to the NCU standby area from a remote server or from local computer.

You must log in with an admin or provision privilege-level account. The remote server or local computer must contain the required firmware packages in the FWP subfolder.

1. Select **Node**.
2. Select **Software** > **NCU**.
3. In the **Transfer Module Firmware Packages (FWP)** area:
   a. Make sure that **Encryption** is cleared.
   b. In the **Transfer to NCU Area** field, select **Standby**.

If you want to transfer FWP from a remote server, continue with these steps:

1. In the **Transfer Module Firmware Packages (FWP)** area:
    a. In the **Source Location** field, select **Remote Server**.
    b. In the **FWP Download Mode** field, select:
        - **Required**: to download only the firmware packages of equipped modules.
          -or-
        - **All**: to download all the module firmware packages for this generic software.
    c. Select the **Transfer Protocol** from the list.
    d. Select the **Use IP Subnet** from the list:
        - **Default Gateway**: if the management network uses the range of the physical IP interfaces.
        - **System**: if the management network uses the range of the system IP addresses.
    e. In the **IPv4/v6 Address** field, enter the IP address of the remote server.
    f. Enter **User Name** and **Password** to access the remote server.
    g. (optional) Enter **Directory Path Name** on the remote sever.
    h. Click **Transfer**.

If you want to transfer FWP from a local computer, continue with these steps:

1. In the **Transfer Module Firmware Packages (FWP)** area:
    a. In the **Source Location** field, select **Local Computer**.
    b. In the **FWP Download Mode** field, select:
        - **Required**, if you want to download only the firmware packages of equipped modules.
          -or-
        - **All**, if you want to download all the firmware packages for this software
    c. Click **Import & Transfer** and select the correct software directory.

Transferring a FWPs of an HD Modules

1. Select **Node**.
2. Select **Software** > **NCU**.
3. In the **Transfer HD Module Firmware Packages (FWP)** area:
    a. In the **Transfer to NCU Area** field, select **Active** or **Standby**.
    b. In the **Source Location**, select:
        - **Remote Server**, then complete the relevant parameters and click **Transfer**.
          -or-

- **Local Computer**, then click **Import & Transfer** and select the correct software directory.

Transferring a Firmware Packages to All Native Modules from a NCU Standby Area

The system downloads FWPs to the NCU as part of the software release. See Transferring Software to the NCU.

You must initiate the firmware update process, which includes the installation and activation of FWP. Firmware updates typically take about five minutes to complete, but some modules can take considerably longer. To reduce downtime during a software release update, you can transfer the FWP to native modules from the NCU standby area, then activate them during or after the NCU software activation. On legacy modules, you must transfer and activate the firmware after the NCU software activation is complete.

> If you remove modules, or they lose power during a firmware update, the module firmware might be corrupted. Native modules revert to the FWP that you installed in the backup area.
>
> Some FWP updates can be service-affecting, and if so, the UI indicates the update effect. Take the necessary precautions for a service interruption before you begin a service-affecting update or activation.
>
> You can downgrade the FWP to an earlier release, but only to release 9.1 or later. Downgrades are service-affecting for all FSP 3000R7 modules. However, the software marks as not service-affecting any downgrades to a FWP earlier than release 9.3 on FSP 3000R7 modules that you upgraded to an FWP from release 9.3 or later.
>
> Only the standby module in a channel-card protection configuration updates if a firmware update is service-affecting. You must perform a protection switch, and then activate the other module. Modules in client channel-card protection configurations always accept FWP updates. The update process does not block the FWP update if the module is active, even if the update is service-affecting.
>
> Some modules that support fiber detection might raise a hardware degrade (HWANR) condition for up to five minutes during the firmware update.

To check the number of modules that require firmware installation or activation, complete these steps:

1. Select **Node** > **Software** > **Module**. The **Firmware Package (FWP) Release Status** opens.

Log in with an admin or provision privilege-level account. You must install the applicable software release on the NCU to continue. Complete these steps.

1. Select **Node**.
2. Select **Software** > **Module**.
3. Click **Transfer** to open the **Firmware Package Transfer** window.
4. In the **Transfer from NCU Area** field, select **Standby**.
5. Click **Transfer**.

After the transfer is complete, the **FWP Version (Standby)** for each native module indicates the same FWP version as the **FWP on NCU (Standby)**.

Managing a Firmware of a Module

Update module firmware packages (FWP) in the **Node** > **Software** > **Module**. You can update module firmware if you have admin or provision privilege level.

The **Firmware Package (FWP) Release Status** table displays the firmware status of each installed module. You can access this information, under **Node** > **Software** > **Module**. You can filter the table by these criteria by selecting the corresponding **Show**:

- Modules with FWP
- Modules at Release
- Modules not at Release
- Modules waiting for activation
- Modules that must be updated with Transfer & Activate

> If the node contains HD equipment:
>
> - HD modules are updated by the software manager on the ECM in the HD shelf/subsystem.
> - All of the HD modules with transferred FW will be updated, once you click the ECM **Activate** button. To update only selected HD modules, you must transfer the FW and update the modules one at a time.
> - HD shelf row represents the software manager status. These rows not included in the Firmware Package (FWP) Release Status counts.
> - HD Software Manager Status is located in FWP Version (Standby) column.
> - HD Software Manager is in **Idle** state when column contains n/a.
> - HD Software Manager is in **Installed** state when release number is the same as FWP on ECM (Active), some modules can be activated.
> - HD Software Manager is in **Installed** state when release number is different than FWP on ECM (Active), ECM can also be activated.

You need to transfer the module firmware packages from the active NCU to the modules then activate. Use **Transfer**, **Activate,** and **Transfer & Activate** buttons for these actions.

Button	Action
Transfer	Transfers the firmware package from the NCU active (**Active Software Release**) or standby area (**Standby Software Release**) to the module standby area. **Transfer** works for native modules (FSP 3000 dedicated).
Activate	Causes modules to start using the firmware package that was transferred to the module standby area. **Activate** works for native modules (FSP 3000 dedicated).
Transfer & Activate	Transfers the firmware package then immediately activates the firmware package in 1 step. **Transfer & Activate** works for all modules.

You can update module firmware packages for all modules, all modules of the same type, or an individual module.

- All modules - In the **Module** tab, click **Transfer & Activate** or **Transfer** then **Activate**.
- All modules of the same type - In the **Type** tab, click on the row with the module type you want to update. Then, use the buttons in the overlay window.
- Individual module - In the **Module** tab, click on the row with the module you want to update. Then, use the buttons in the overlay window.

> FIPS compliant and WCC-PCN-AES-100GB encryption modules firmware update procedure requires the restart to be done from **Maintain** > **Module Encryption** > **Encryption Restart** with the selection of **Cold with Standby FWP**. This restart requires the entry of the crypto officer password.

You can update the FWP on modules automatically, to align to the NCU software release when modules are installed. If you enable this feature, the NCU will check the module FWP version after detection and if needed:

- Transfer and activate the FWP from the NCU.
  -or -
- Download FWP from the set server.

If there is not a FWP on the NCU for the module, you must update the software manually.

Provisioning an Automatic Module FWP Update

1. Select **Node**.
2. Select **Software** > **NCU**.

3. In the **Active Software Release** area, set **Update FWP on Install** to **Enable**.

For detailed information about module firmware updates, refer to the *Maintenance and Troubleshooting Manual*.

Provisioning an Automatic FWP Download to NCU

Enables the automatic download of FWP to NCU at software updates from previously specified servers.

1. Select **Node**.
2. Select **Software** > **NCU**.
3. In the **Automatic Module Firmware Package (FWP) Transfer on Install** area, set **Download FWP on Install** to **Enable**.
4. Select **Transfer Protocol** from the list:
   - **FTP**
   - **SCP**
   - **SFTP**
5. Select **Use IP Subnet** from the list:
   - **Default Gateway**, if the management network is configured to route IP addresses in the range of the physical IP interfaces.
   - **System**, if the management network is configured to route IP addresses in the range of the System IP addresses.
6. Enter the **IPv4/v6 Address** of the remote server.
7. Enter **User Name** and **Password** to access the remote server, following any case-sensitive rules imposed by the remote server.
8. Enter **Directory Path Name** on the remote sever, if needed.
9. (optional) To test your settings, click **Test**.
   The software provides the test result on the screen and saves it in the event log.
10. Click **Apply**.

Managing File Storage

You can view and manage files for the Active NCU RAM, Active NCU permanent memory, and SCU.

This section contains these topics:

Transferring Files to a Local Computer

You can import and export files to your local computer from the Active NCU RAM.

This functionality requires you to enable **Local Computer Transfer** in the **Functionality** area under **Node > General > Controls**.

Importing

1. Select **Node**.
2. Select **File Storage**.
3. Set **Location** to **Active NCU RAM**.
4. Click **Import** and select **Local Computer**.
5. Select a file on your computer and click **Open**.

Exporting

1. Select **Node**.
2. Select **File Storage**.
3. Set **Location** to **Active NCU RAM**.
4. Click the file name you wish to export.
5. The file is downloaded to the directory specified as the browser default.

Viewing Logs

This section contains these topics about viewing logs:

Background Information

The node stores logs for troubleshooting purposes. The logs available depend on how the node is used. The following is a list of all supported logs:

- *Event Log*: This log contains a history of all standing and transient conditions (events) generated on the node. The events provide a history of faults and other activities that occurred on the node. The event log stores up to 2000 entries, after which the oldest entries are overwritten. For more information about events, refer to the Maintenance and Troubleshooting Manual. The Event Log includes the following fields:

  - **Timestamp**: The date and time the event occurred, with a format of *yyyy-mm-dd*.
  - **Severity**: The notification code associated with the event (Critical, Major, Minor, Information, Not Reported).
  - **Status**: Indication of the standing condition transition, raised (SET) or cleared (CLEAR).

- *System Log*: This log contains information about authentication on the node and the addition/removal of users.
  - Successful authentication (login) via any interface method (http/https, SNMPv1/SNMPv3, telnet/SSH or TL1) results in a log entry with an associated time stamp, the user account, the protocol used, the source IP address, and the session ID.
  - An unsuccessful authentication attempt results in a log entry with the associated time stamp, authentication result, the user account, the protocol used, and the source IP address.
  - A logout leads to a log entry with an associated time stamp, the user account, the protocol used, and the session ID.

  The System Log may display the following fields:
  - **Timestamp**: The date and time the event occurred, with a format of *yyyy-mm-dd*.
  - **Message**: The user ID, protocol, source IP address, and session ID.

- *Database Change Log*: This log contains parameter changes saved to the database. It includes the following fields:
  - **Timestamp**: The date and time the database change occurred, with a format of *yyyy-mm-dd*.
  - **Command**: The action that caused the database change.
  - **Application**: The source of the database change.
  - **User**: The User ID of the session which originated the database change.

- *Equalization Log*: This log contains equalization events generated by ROADMs and CCMs. The events provide information about channel power changes that occur on equipment. The Equalization Log includes the following fields:
  - **Timestamp**: The date and time the event occurred, with a format of *yyyy-mm-dd*.
  - **Message**: The equalization event type (for example, EQLZ-START, EQLZ-COMPL, EQLZ-PASS). The events EQLZ-PASS, EQLZ-AUTO, EQLZ-RAMAN, and EQLZ-FAIL are followed by up to three numbers:
    - The channel output power at completion of the equalization process
    - The maximum deviation from the set-point during the equalization process

        - If present, the third number indicates the channel input power at completion of the equalization process

- *Control Plane Log*: This log contains information related to the control plane operation, when enabled. It contains the following fields:
    - **Timestamp**: The date and time the event occurred, with a format of *yyyy-mm-dd*.
    - **Message**: Details relevant for debugging.
- *Crypto Log*: This log contains events related to encryption actions and changes. It contains the following fields:
    - **Timestamp**: The date and time the event occurred, with a format of *yyyy-mm-dd*.
    - **Status**: Indication of the standing condition transition, raised (SET) or cleared (CLEAR).
    - **Location**: The location on the link that the condition/event occurred.
    - **Direction**: If applicable, the signal flow direction for the condition/event.
    - **Severity**: The notification code associated with the event (**Critical**, **Major**, **Minor**, **Information**, **Not Reported**).

Viewing Logs

Follow these steps to view a log file:

1. Select **Node**.
2. Select **Logs** to display the log types.
3. Select the log file you wish to view.

In the **Event** and **Database Change** logs, double click an event (row) to display the detail view of the log entry.

You can filter the log by entering all or part of the information you want to find in the **Search by all columns** field. You can also limit the date range by selecting **dates** in the **calendar** fields.

Exporting Logs

The node stores log files which can be exported to an external location for troubleshooting purposes. The log files available on a node depend on the node configuration. The following is a list of all supported log files:

- Event
- System
- Database Change
- Equalization
- Control Plane
- Crypto

Follow these steps to export a log file from the node:

1. Select **Node**.
2. In the **Navigation Tree**, click the "+" sign adjacent to **Logs** to display all available log files.
3. Select the log file you wish to export.
4. Click **Export** (in the **Main Pane** on the upper right) to download this log file.
5. Enter relevant details in the PC dialog to save this log file to your PC or an external file server.

All parameters available are exported in one CSV file. File name contains information about the entity, the module and the ID (shelf, slot) location.

For exporting all parameters in the Configure Details window see Configure Details.

Collecting Support Data

Support Data can be easily collected for analysis by technical experts.

> Support Data collection may take up to 2 hours depending on the size of the node.

1. Select **Node**.
2. Select **Tools**.
3. If desired, in the **Data For Technical Support Analysis** area, select up to 10 modules to collect PM data by selecting shelf and module.
4. Select the check box(es) depending on required file destination:
   a. **Export to Local Computer**
   b. **Transfer File to Remote Server**
      - Set the **Transfer Protocol**
        - FTP
        - SCP

   - SFTP
   - SCP-KEYBASED
   - SFTP-KEYBASED
- Set the **Use IP Subnet**
   - Default Gateway
   - System
- Enter **IPv4/v6 Address**
- Enter **User Name**
- Enter **Password**
- Enter **Directory Path Name**

5. Click **Start** next to **Data collection**.

Pinging an IP Address

Use ping to determine whether an IP connection exists to other equipment. Ping supports IPv4 and IPv6 addresses.

1. Select **Node**.
2. Select **Tools**.
3. Select **Ping** in the **Ping/Traceroute** area.
4. Enter the **IPv4/v6 Address**.
5. Click **Start**.
6. Click **Clear** to delete the resulting ping information.

> The ping response may take up to 10 seconds to be displayed.

Performing Traceroute

Use the traceroute utility to determine the IP route to other equipment. Traceroute supports IPv4 and IPv6 addresses.

1. Click **Node**.
2. Select **Tools**.
3. In the **Ping/Traceroute** area, select **Traceroute**.
4. Enter the **IPv4/v6 Address**.

5. Click **Start**.
6. Click **Clear** to delete the resulting traceroute information.

🗎	The system supports traceroute through UDP, and some networks might block this operation.

Importing Planner Information

When your network has been planned using FSP Network Planner (Planner), information from Planner can be imported to the node using NED. The Planner file format is XML. Planner supports importing Equipment and Physical Connections.

To import network information from the Planner:

1. Select **Node**.
2. Select **Profiles > Planner**.
3. Click the **Import from Planner** button at the top of the window.
4. Browse the File Manager and select the Planner file for the node. Click **Open**.
    - Check the **Configure** column in the **Planned Equipment from Import** area.
    - Check for any errors listed in the **Planned Physical Connections from Import** area.
5. Resolve any errors found.
6. Click **Refresh**.
7. Click **Add** to add imported network information.

Using the Alarm Profile

This section contains these topics about alarm profiles:

Exporting Active Profile

Complete these steps to export the active profile.

1. Select **Node**.
2. Expand **Profiles**.
3. Select **Alarm**.
4. In the **Export Active Profile** area, following your network plan:
    a. Set the **Destination**
        - Remote Server
        - Active NCU RAM
        - Local Computer

    b. Set the **Transfer Protocol**
        - FTP
        - SCP
        - SFTP

    c. Set the **Use IP Subnet**
        - Default Gateway
        - System

    d. Enter **IPv4/v6 Address**

    e. Enter **User Name**

    f. Enter **Password**

    g. Enter **Directory Path Name**
5. Click **Export**.

Importing Standby Profile

Complete these steps to import a standby profile.

1. Select **Node**.
2. Expand **Profiles**.
3. Select **Alarm**.
4. In the **Import as Standby Profile** area, following your network plan:
    a. Set the **Source Location**
        - Remote Server
        - Active NCU RAM
        - Local Computer

    b. Set the **Transfer Protocol**
        - FTP
        - SCP
        - SFTP

   c. Set the **Use IP Subnet**
      - Default Gateway
      - System
   d. Enter **IPv4/v6 Address**
   e. Enter **User Name**
   f. Enter **Password**
   g. Enter **Directory Path Name**
   h. Enter **File Name**

5. Click **Import**.

Changing Alarm Severity for an Item Type

Complete these steps to change alarm severities system wide.

1. Select **Node**.
2. Expand **Profiles**.
3. Select **Alarm**.
4. In the **Modify Active Profile Severity** area, select the **Alarm Group** for the alarm severities to be changed.
5. Select the desired severity in the **Severity Provisioned** column [**Critical**, **Major**, **Minor**, **Information**, **Not Reported**].
   Use **Not Defined** to reset the severity to the system default.
6. Click **Apply** to save changes.

> Click **Refresh** to display the previous severity without applying any changes.

7. Repeat steps 4-6 to change alarm severities for other alarm groups.
8. At the top of the **Main Pane**, click **Update Alarm Severities** to apply the changes to the system.

Using the Master Profile

This section contains these topics about node profiles:

Creating the Master Profile

Set the parameters on the node as you want to be set for the Master profile for other node.

1. Select **Node**.
2. Select **Profiles > Master**.
3. Open the **Master Profile** area.
4. Click **Create**.
   - Enter **Master Profile Name**
   - Enter **Version Number**
   - Enter **Comment** (Optional).
5. Click **Apply**.

	License Server, License Backup Server and the Use IP Subnet are included in the Master Profile. See Using Licenses for more details.

Exporting the Master Profile

1. Select **Node**.
2. Select **Profiles > Master**.
3. Open the **Export Master Profile** area.
4. Choose the **Destination** from the list.
5. If needed, set the parameters to perform the profile transfer:
   - Transfer Protocol
   - Use IP Subnet
   - IPv4/v6 Address
   - User Name
   - Password
   - Directory Path Name
6. Click **Export**.

Importing the Master Profile

1. Select **Node**.
2. Select **Profiles > Master**.
3. Open the **Import Master Profile** area.
4. Choose the **Source Location** from the list.
5. If needed, set the parameters to perform the profile transfer:
   - Transfer Protocol
   - Use IP Subnet
   - IPv4/v6 Address
   - User Name
   - Password
   - Directory Path Name
   - File Name
6. Click **Import**.

Activating the Master Profile

Activating the Master Profile locks the node configuration, parameters associated with the Master profile cannot be changed without deactivating the master profile.

1. Select **Node**.
2. Select **Profiles > Master**.
3. Click **Activate** in the **Master Profile** area.

Deactivating the Master Profile

1. Select **Node**.
2. Select **Profiles > Master**.
3. Click **Deactivate** in the **Master Profile** area.
4. In the Confirm Deactivation window:
   - Click **Yes** to confirm,
     or
     Click **Cancel** to abort.

Deleting the Master Profile

The Master Profile must be deactivated in order to be deleted.

1. Select **Node**.
2. Select **Profiles** > **Master**.
3. Click **Deactivate** in the **Master Profile** area.
4. In the Confirm Deleting window:
    - Click **Yes** to confirm,
      or
      Click **Cancel** to abort.
5. Click **Delete** in the **Master Profile** area.
6. In the Confirm Deleting window:
    - Click **Yes** to confirm,
      or
      Click **Cancel** to abort.

Using the Threshold Profile

Threshold profiles allow you to change thresholds node wide for all equipment that uses the profile. These profiles can be exported then imported to other nodes to have consistent settings across all of the equipment in the network. You can see the threshold profile(s) used by an entity in the Monitor application by selecting the monitor group (i.e. Optical) then clicking the row in the table to open Monitor Details.

> Optical power transmit and receive (OPT/OPR) threshold profiles are listed on an equipment basis (module/port or plug). Be careful to select the profile for intended port type which is indicated by the letter after the module name.

This section contains these topics about threshold profiles:

Exporting Threshold Profile

This procedure requires a user account with PROVISION or ADMIN rights.

> You can only export the active threshold profile.

Complete these steps to export the threshold profile.

1. Select **Node**.
2. Select **Profiles > Threshold**.
3. Open the **Export Active Profile** area.
4. Choose the **Destination** from the list.
5. If needed, set the parameters to perform the profile transfer:
   - Transfer Protocol
   - Use IP Subnet
   - IPv4/v6 Address
   - User Name
   - Password
   - Directory Path Name
6. Click **Export**.

Importing Standby Profile

This procedure requires a user account with PROVISION or ADMIN rights.

Complete these steps to import a standby profile.

1. Select **Node**.
2. Select **Profiles > Threshold**.
3. Open the **Import as Standby Profile** area.
4. Choose the **Source Location** from the list.
5. If needed, set the parameters to perform the profile transfer:
   - Transfer Protocol
   - Use IP Subnet
   - IPv4/v6 Address
   - User Name
   - Password
   - Directory Path Name
   - File Name
6. Click **Import**.

Changing and Applying Threshold Profiles

Complete these steps to apply a threshold profile system wide.

1. Select **Node**.
2. Select **Profiles > Threshold**.
3. Select an Item Type from the list.
4. Click **Edit**.
5. Enter the parameters following your network plan.
6. Click **Apply**.
7. Click **Apply Threshold Profile**.
8. In the **Apply Threshold Profile** window, click **Apply**.

Clearing All Changes

The Threshold Profile contains various specific threshold profiles for individual parameters. Clearing all changes resets any user modifications to the default threshold profile values.

1. Select **Node**.
2. Expand **Profiles**.
3. Select **Threshold**.
4. In the **Active Profile** area, click **Clear All Changes**.
5. In the **Clear All Changes** window, click **Clear All Changes**.

Using Licenses

HD equipment requires a license to use these features:

- Non-ADVA plugs.
- Cross connection functionality.
- Access to additional client ports on a module.

To obtain a license, contact your sales representative.

You can manage licenses in two ways:

- Floating (server-based) - A license server provides a license that is stored on the node in trusted storage. For more efficient license management across the network, the server provides centralized license access.

- Fixed (shelf-based) - Install the licenses on the HD shelf or subsystem where you plan to use them. The HD shelves or subsystems cannot share these licenses.

> First configure an ECM on the relevant HD shelf to activate license management.

> If you connect HD shelves using an HDSCM optical interconnection, the system will show that the HD shelf connected by ECM consumes all HD module licenses.

> In case the T-MP-M8DCT or T-MP-2D8DCT module requires GCC communication to access the DCN network and the license server, and no F8-RTU-T-100G-CAPACITY license is available before connection, the system:
>
> - Allows the creation of a single client without raising **configure fail-license** error to enable the establishment of a GCC connection to a DCN network.
> - Raises a **no license** alarm.
> - Clears the **no license** alarm after acquiring licenses from a license server.

Using a Server-Based License

1. Select **Node**.
2. Select **General** > **License**.
3. In the **License Management** area, click any column to manage your licenses.
4. In the **Configure Details** window, **Manager** area, **License Management** field, select **Floating (Server Based)**.
5. Click **Apply**.
6. In the **License Server** field, enter the applicable IP address.

> For applicable IP address format:
>
> 1. (optional) Enter https:// to use the HTTPS protocol. License manager uses the HTTP protocol without encryption as the default.
> 2. Enter the URL.
> 3. (optional) Enter colon followed by port ID. By default, the license manager uses ports 7070 for HTTP and 7071 for HTTPS.
>
> Example: https://1725.27.X.X:8000

7. Change any additional required settings, and then click **Apply**.

Using a Shelf-Based License

1. Select **Node**.
2. Select **General** > **License**.
3. In the **License Management** area, click any column to manage your licenses.
4. In the **Configure Details** window, **Manager** area, **License Management** field, select **Fixed (Shelf Based)**.
5. Click **Apply**.
6. In the **Licenses per Shelf** area, in the applicable license manager row, click any column other than the **Identifier**.
7. In the **License Import** area, specify the data required to import a license file.
8. Click **Import & Install** to import a license file from a specified location and install the licenses on the shelf.
9. After the license file installation completes, in the **Configure Details** window, click **Apply**.

Exporting and Printing Node Related Information

1. Select Node.
2. In the **Navigation Tree**, expand the relevant items.
3. Select the item for that you want to export information.
4. In the **Main Pane**, select the area with the related information.
5. Click 📤 to export information, or click 🖨 to print information.

Services

The **Services** application provides a simplified approach to configuring equipment paths in a node to carry data. You can provision optical channels and/or client services through the node.

This section contains these topics:

Background Information

A service is the end-to-end path across a network to carry end user data. The **Services** application is used to setup a service segment on a node. Under **Services**, you can create the following bi-directional service segment types.

- **Passthrough Optical Channels** - Optical Line (OL) to Optical Line
- **Add-Drop Optical Channels** - Channel module network port to an Optical Line
- **Client Service** - Channel module client port to an Optical Line

Service segments provide a number of advantages. They:

- Reduce the number of configuration steps compared to direct equipment configuration.
- Provide a higher level view of services or channels provisioned on a node.
- Allow easy removal of the client service and/or optical channel on the node.

Services does **not** support:

- discontinued equipment
- cascaded channel modules
- regeneration
- uni-directional channels or services
- service protection.

Configuration of services through 4TCA-PCN-4GU+4G and 4TCA-PCN-4GUS+4G modules may be incomplete and prevent traffic flow.

Requirements

To use the **Services** application:

- All equipment must be provisioned, including **Optical Lines** and **External Channels**
  - See Adding Optical Lines for more information.
  - See Adding an External Channel for more information.
- **Physical Connections** (fiber map) must be imported or entered
  - See Adding Physical Connections for more information.
- User must know service-level details
  - **(A --> B) Node in Path**
  - **(B --> A) Node in Path**
  - Network (Optical Channel) **Facility**
  - Client F**acility**
  - If required, **ODU ID** and **Slot(s)** or **Channel ID**

Setting up an Optical Passthrough Segment

1. Select **Services**.
2. Click **Add Service**.
3. Select **Optical Channel**.
4. If desired, enter a **User Label**.
5. In the **(A) - End Point** area:
   a. Select an OL in the **(A):** menu.
   b. Select a **Channel**.

   c. In the **Optical Channel** area, select a **Channel Group** option. Choose **Yes** when a channel is transported using four optical lanes.
   d. In the **(A) - End Point** area, select a **Facility**. If you chose **Yes** in the Channel Group menu, the **Facility** option will not be available.

6. In the **(B) - Line** area:
   a. Select an OL in the **(B):** menu. If the selection is inactive, no options are available.
7. Select **(A --> B) Node in Path**.
8. Select **(B --> A) Node in Path**.
9. If needed, select **Channel Bandwidth**.
10. Click **Add Optical Channel** to create an optical service segment.
11. Click the row for new the Optical Segment Supervisor (OSS) in the table at the top of the page.
12. In the OSS area, click the **Enable** button.
13. Continue to Setting up an Optical Passthrough Segment.

Setting Up an Optical Add-Drop Segment

1. Select **Services**.
2. Click **Add Service**.
3. Select **Optical Channel**.
4. If desired enter **User Label**.
5. In the **(A) - End Point** area:
   a. Select an channel module port or external channel in the **(A):** menu.
   b. Select a **Channel**, if available. If no **Channel** is available, proceed to Step 6.
   c. Select a **Facility**.
6. In the **(B) - Line** area, select an OL in the **(B):** menu. If the selection is inactive, no options are available. Return to Step 5C, if you advanced here from Step 5B.
7. Select **(B --> A) Node in Path**
8. If needed, select **Channel Bandwidth**
9. Click **Add Optical Channel** to create an optical service segment.
10. Click the row for new the Optical Segment Supervisor (OSS) in the table at the top of the page.
11. In the OSS view, click the **Enable** button.
12. Continue to Equalizing Optical Service Segments.

Equalizing Optical Service Segments

Equalizing is the process of adjusting the transmitted optical power of individual channels to a defined power level or set-point. Optical service segments allow equalization of all ROADMs and CCM in the channel path to be equalized in one step. However, light must be present to perform the equalization. During service setup, the entire path needs to be equalized in each direction separately.

Equalization results are reported in the Event and Equalization logs and transmitted power levels are displayed under **Monitor** for the ROADMs and CCM.

1. Select **Services**.
2. Click the desired Optical Segment Supervisor (OSS) row in the table.
3. Click **Equalize** in the **Maintain** area.
4. Confirm the request by clicking **Equalize**.
5. Wait for the equalization to complete.

This procedure needs to be repeated on each node (A to Z) in the forward path and then on each node (Z to A) in the reverse path.

Setting Up a Client Service Segment

Client services start at a client port and connect to an Optical Segment Supervisor (OSS). The OSS may be created before or as part of the client service segment process.

1. Select **Services**.
2. Click **Add Service**. **Service** is selected by default.
3. Enter a **User Label**.
4. In the **(A) - End Point** area:
   a. Select a channel module port in the **(A):** menu.
   b. If needed, select the **Route Through Port**.
   c. Select the client **Facility**.
5. In the **(B) - Line** area:
   a. Select an OL in the **(B):** menu. If selection is inactive no options are available.
6. If the **Optical Channel** needs to be configured, enter the required information. See Setting Up an Optical Add-Drop Segment.
7. In the **Service Segment** area enter the required information, which may include.
   a. **Termination Level**
   b. **Payload Type**

   c. **Auto Laser Shutdown**
   d. **Error Forwarding Mode**
   e. **Flow Control**
   f. **(A) Slots**
   g. **(A) ODU ID**
   h. **(B) Slots**
   i. **(B) ODU or Channel ID**

8. Click **Add Service**.

If the **Optical Channel** has not been equalized, continue to Setting Up a Client Service Segment after the entire path as been added.

Releasing a Segment

Releasing a service segment deletes the segment supervisor, which manages the entities associated with the segment. Traffic is not affected, but the optical channel or client service can no longer be managed as a segment. You must manage each entity individually.

To release a segment, click **Release Segment**.

Deleting a Segment

Deleting a service segment deletes the segment supervisor and all associated entities. The path is removed and traffic is blocked.

To delete a segment, click **Delete**.

Network

You can access other nodes in the **Network** application, either directly or by gateway access. Select **Network** to access other nodes in the network.

- In the **Direct Access** column, click a link to access a node.
- In the **Gateway Access** column, click a link to access a node through a proxy server.

Management

This section describes details for managing the Fiber Service Platform 3000R7.

Fault management includes:

- Conditions.
- Events and defects.
- Administrative and operational states.
- Special alarms.

Configuration management includes:

- Loopbacks.
- Connectivity.
- Consequent actions.

Performance management includes:

- Counters.
- Record types.
- Record content.

Security management includes:

- User accounts.
- Passwords.
- Security features.

Procedures for managing the Fiber Service Platform 3000R7 are collected in this user guide and also in the Provisioning and Operations Manual.

This section includes the following topics:

Fault Management

The Fiber Service Platform 3000R7 system detects and identifies conditions that could decrease the efficiency of transport.

NE stores conditions in two lists. One list is a log of conditions, representing a history, the other is a list of the currently present standing conditions.

Depending on the notification code/severity of the condition and the administrative state of the reporting entity, the system sends the notification of the condition from the NE to the NMS.

This section includes the following topics:

Condition Notification Code/Severity Level

In accordance with ITU CCITT X.733, each condition is assigned a notification code, or a severity level. Severity levels are defined by the urgency of the action to be taken by the maintenance engineers.

You can change the default assigned severity for a condition type for all applicable entities either manually or by applying an alarm profile.

Overview of Severity Levels

See the severity levels listed in this table:

Severity Level	Description
Critical	Indicates occurrence of a service-affecting condition which requires an immediate corrective action. It can be reported when a managed object goes out of service and you must restore its capability.

Severity Level	Description
Major	Indicates occurrence of a service-affecting condition which requires an urgent corrective action. It can be reported in case of severe degradation of a managed object capability and you must restore its full capability.
Minor	Indicates occurence of a non-service affecting condition. It can be reported when the detected alarm condition is not currently degrading the capacity of the managed object. However, you should correct this condition to prevent a more serious fault, such as service affecting issue.
Not Alarmed	Indicates an informative event, or the detection of a potential or impending service-affecting fault condition. You should diagnose and, if necessary, correct the problem before a service affecting fault condition occurs.
Not Reported	Indicates an event that will not be reported. The current standing condition list shows this condition, but the condition log on the NE does not.

Severities and Alarm Profiles

Apart from the following descriptions also refer to Figure 39 for a better understanding of how alarms and their severities are processed when using profiles.

Default Alarm Severity

The default severity for every alarm is hard-coded in NE software (cserver) and is written to the database during provisioning.

Alarm Profile (AP)

The default AP is empty. "Not-Defined" severity in AP means no severity modification made in the database based on the AP. This "Not-Defined" setting *cannot* be turned back to factory default. Severity modifications made in AP overwrite alarm severity settings of the cserver. These modifications are stored in the database for every entity. The AP modifies severity settings based on AID types independent of the entity.

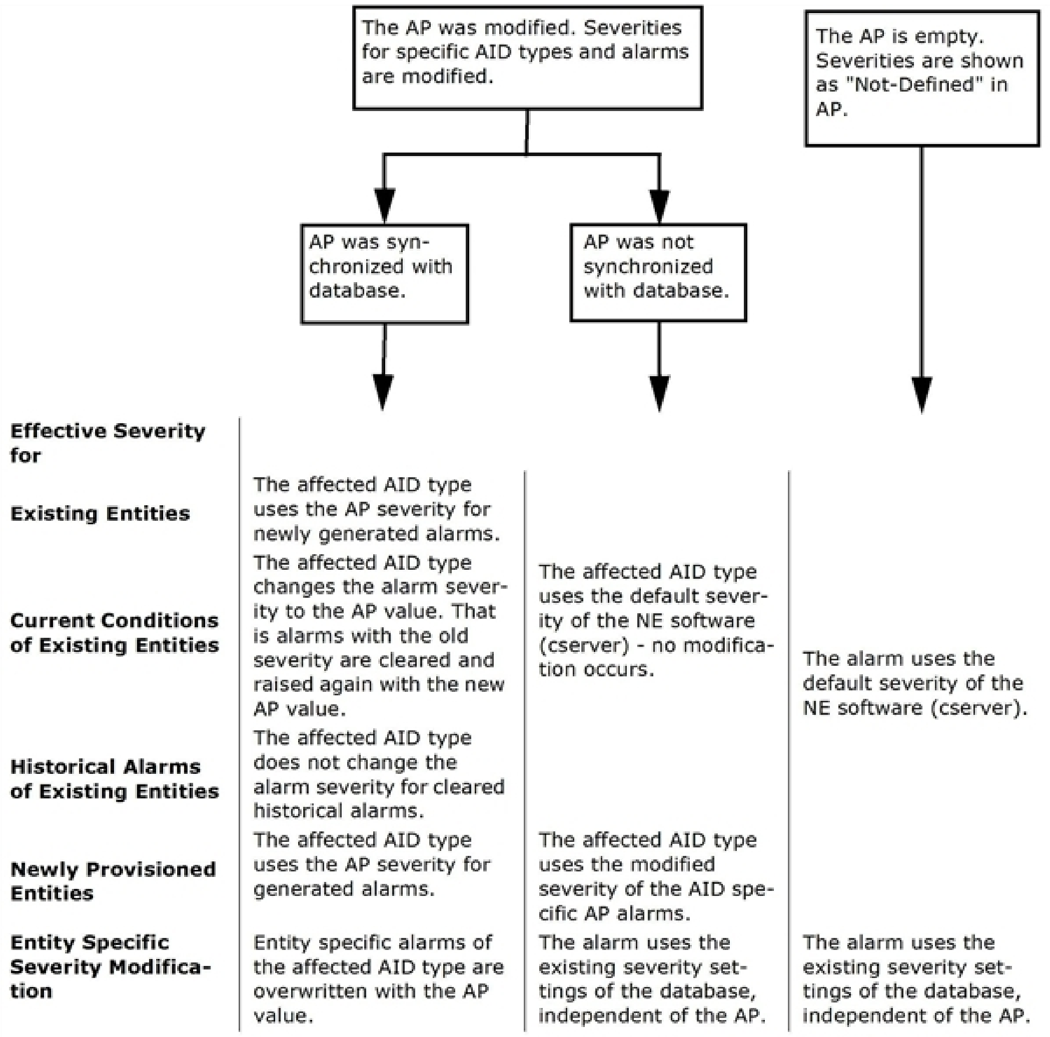
Effective Severity for Alarms

The effective alarm severity for each individual alarm is taken from the database.

Entity Specific Severity Modification

The alarm severity for every entity/AID type can individually be modified for every alarm. Modifications are written to the database for each alarm and entity.

Figure 39: Severities and Alarm Profiles


The AP was modified. Severities for specific AID types and alarms are modified.
AP was synchronized with database.
AP was not synchronized with database.
The AP is empty. Severities are shown as "Not-Defined" in AP.

Effective Severity for	AP was synchronized with database.	AP was not synchronized with database.	The AP is empty. Severities are shown as "Not-Defined" in AP.
Existing Entities	The affected AID type uses the AP severity for newly generated alarms.	The affected AID type uses the default severity of the NE software (cserver) - no modification occurs.	The alarm uses the default severity of the NE software (cserver).
Current Conditions of Existing Entities	The affected AID type changes the alarm severity to the AP value. That is alarms with the old severity are cleared and raised again with the new AP value.		
Historical Alarms of Existing Entities	The affected AID type does not change the alarm severity for cleared historical alarms.		
Newly Provisioned Entities	The affected AID type uses the AP severity for generated alarms.	The affected AID type uses the modified severity of the AID specific AP alarms.	
Entity Specific Severity Modification	Entity specific alarms of the affected AID type are overwritten with the AP value.	The alarm uses the existing severity settings of the database, independent of the AP.	The alarm uses the existing severity settings of the database, independent of the AP.

Transient Conditions

A transient condition is a temporary, or passing, phenomenon, and is of a brief duration. Transient conditions are reported immediately.

Transient conditions have the severity Not Alarmed (NA), and the user cannot change this severity.

Standing Conditions

Standing conditions are raised and remain active until they are autonomously cleared. Standing conditions can further be divided into:

- Alarms, when the severity is Critical (CR), Major (MJ), or Minor (MN).
- Events, when the severity is Not Alarmed (NA).
- Informational indicators, when the severity is Not Reported (NR) or Cleared (CL). The network element assigns the severity Cleared when it clears standing conditions.

Fault Cause Persistency Filtering

The network element applies a fault cause persistency filter (FCPF) to many of the standing conditions, for example standing conditions related to SDH, SONET, and OTN. Fault cause persistency is particularly relevant for standing conditions in the data plane.

- If the standing condition persists for a certain time period, an alarm is raised. This time period is called the activation time. Although reporting of the alarm is delayed by the activation time, the time stamp of the alarm reflects the first observation of the standing condition.
- After the alarm has been raised and the associated standing condition has been absent a certain time period, the alarm is cleared. This time period is called the de-activation time.

The effect of the activation and de-activation time periods is that the standing condition is "soaked" for a while before any alarm is reported as either raised or cleared. This prevents reporting of fluctuating alarms.

The activation and deactivation time periods are configurable, and are effective for all modules in the NE. The default alarm activation and de-activation time is 2.5 seconds and 10 seconds respectively. The sum of the activation and de-activation time must always be greater than or equal to 1 second to ensure that the frequency of a single alarm is not higher than 1 second. Changing the activation or de-activation time period is not service affecting, does not require a reboot and is effective across all modules in the NE within 60 seconds. Changes affect both new standing conditions as well as conditions that were under supervision before the change. Changes are logged in the database change log.

The network element does not apply the fault cause persistency filter to alarms related to the SC interface (NCU, OSCM, UTM).

Information Associated With Conditions

For all conditions, the following information is associated:

- The access identifier (AID) of the entity that reported the condition.
- The condition type, so that the condition can be distinguished from other conditions reported from the same entity.
- Indication of whether the condition is related to signal flow direction or not. The following indicators are used: transmit (Tx), receive (Rx) or not applicable (NA).

- At which end of a link the defect that causes the condition occurred: the near-end NE (NEND) or the far-end (FEND) NE.
- The notification code corresponding to that condition name. The notification code (NC) indicates the severity of the condition, which influences whether the condition is transient, an alarm, an event or an informational indicator.
- Alarms provide an indication of whether the condition interrupts a provisioned service (SA) or not (NSA).

Condition Reporting

When standing conditions are raised or cleared, this is signaled to the management system as SNMP traps or TL-1 reports. However, traps/reports are only sent if the severity/notification code of the condition is different from “Not Reported”.

In some situations it is practical to disable reporting of all conditions from a module or interface, or to inhibit a specific condition associated with a piece of equipment, an interface or a facility. When reporting is disabled for this condition, the following is true:

- An SNMP trap or TL-1 report is not sent.
- The condition is not logged in the event history on the NE.

This might be relevant, for example, when a client interface of a TCC module is unused, or during maintenance work on the NE.

When reporting of a condition on an entity is disabled, it is automatically disabled also for its dependent entities. For example, when condition reporting is disabled at the module level, it is automatically disabled also for the interfaces and facilities supported by that module. Disabling condition reporting for a whole shelf supersedes any condition reporting configuration on modules and facilities. Re-enabling condition reporting for the shelf restores the former settings for modules, ports and facilities.

The administrative state also influences whether conditions are reported. When the administrative state of an entity is set to **Management** or **Maintenance**, all conditions for that entity are treated as if they had severity/notification code **Not Reported**. When the administrative state is set to **In Service**, all conditions on that entity are reported in accordance with their notification codes/severity again.

In channel card protection and channel protection scenarios, alarm de-escalation is supported. A service-affecting condition on the standby entity is de-escalated and reported as non-service affecting, unless the active entity gets a service-affecting condition as well. When the service-affecting condition on the active entity is cleared, the standby entity’s service-affecting condition is de-escalated and reported as non-service affecting again.

Condition Lists

In the NE, conditions are collected and presented in two lists.

Fault Management Table

All standing conditions that are present on the NE are listed in a Fault Management Table regardless of their severity level/notification code. When the cause of the condition is cleared, the condition is removed from the list. Thus this list does not represent history, but the present only.

Event Log Table

All conditions, except those with severity level/notification code “Not Reported”, are logged in an Event Log Table.

The operator can retrieve these lists via the management interface.

Defects

The NE detects defects based on monitoring of parameters on a number of layers. The parameters that are used to detect defects vary for each layer. The monitored layers comprise:

- OTN FEC
- OTN TCM A, TCM B and TCM C connections
- OTN ODU layer
- OTN OTU layer
- OTN physical layer
- SDH physical layer
- SDH Regeneration Section/Section layer
- SDH Multiplex Section/Line layer
- GFP layer
- Equipment layer (e.g. internal faults, power, fan)

Defects may for example be Loss Of Signal or Loss of Frame. Also, analogue values for transmitted laser power and received power allow detection of fiber cuts, intrusion and degradations on the optical layer.

State Overview

This section gives an overview of the administrative and operational states of the Fiber Service Platform 3000R7.

Administrative States

Users can set the administrative state, which determines the extent to which each entity can be configured and operated. When the administrative state changes to any state other than

In Service, an informative condition is raised to indicate that the administrative state changed. These condition names all begin with OOS for Out of Service.

In Service

When an entity is in the administrative state of In Service (IS), normal surveillance is occurring.

- The software reports equipment and facility alarms to the management system.
- Performance records are valid.
- You are unable to perform any operation or configuration that affects service.
- You can set the administrative state to In Service if the entity that supports it is also In Service.

Auto In Service

When an entity is in administrative state Auto In Service (AINS):

- The software does not report the respective equipment or facility alarms to the management system.
- Performance monitoring records are invalid.
- You are unable to perform any operation to configuration that affects service.
- Transition from this state to In Service occurs automatically when all alarms on the respective module, pluggable transceiver, or facility clear, or the operational state of the associated port or facility is Normal.
- You can set the administrative state of an entity to Auto In Service only if the entity that supports it is also Auto In Service or In Service, and the entity that it supports is not In Service.

Management

When an entity is in the administrative state Management (MGT):

- The software does not report the respective equipment or facility alarms to the management system.
- Performance monitoring records are invalid.
- You can perform service-affecting configurations.
- You can set the administrative state of an entity to Management only if the entity that supports it is not Disabled, and the entity that it supports is not In Service or Auto In Service.

🗒	Some service-affecting configurations that you initiate can cause service interruption or loss. Because the software does not report alarms and performance monitoring records are invalid, consider the consequences while in this state. Contact your local technical support team if you are uncertain about the consequences.

Maintenance

When an entity is in the administrative state Maintenance (MT):

- The software does not report the respective equipment or facility alarms to the management system.
- Performance monitoring records are invalid.
- You can perform service-affecting operations.
- You can set the administrative state of an entity to Maintenance only if the entity that supports it is not Disabled, and the entity that it supports is not In Service or Auto In Service.

> Some service-affecting configurations that you initiate can cause service interruption or loss. Because the software does not report alarms and performance monitoring records are invalid, consider the consequences while in this state. Contact your local technical support team if you are uncertain about the consequences.

Disabled

When an entity is in the administrative state of Disabled (DSBLD):

- All alarm notifications from the entity stop.
- Performance monitoring is disabled.
- The OOS Tx Disabled (OFF) or OOS Rx Disabled condition indicate any traffic interruption on this entity.
- You can set the administrative state of an entity to Disabled only if the entity it supports is Disabled or Unassigned.

Unassigned

When an entity is installed but not yet provisioned in the internal database, the software automatically sets the administrative state to unassigned (UAS). Therefore:

- Only inventory information is available for this entity.
- In the management system, the administrative state is displayed in parenthesis next to the entity name in the list of entities.

Operational States

An entity operational state is influenced by the administrative state and current conditions.

Normal

This operational state indicates that the entity is running normally.

Abnormal

This operational state indicates that a signal degrade condition is present on the entity.

Outage

This operational state indicates that service is affected on this entity.It will be accompanied by a secondary state, and together with this and the current list of conditions, the cause for the outage can be found.

Unavailable

This operational state indicates that the entity cannot pass traffic.It is entered when the entity’s administrative state is “Disabled”, and there is no secondary state present.

Secondary States

In addition to the operational state, the NE displays a secondary state.

Basic Autonomous States

Unequipped

This autonomous state (UEQ) indicates that the equipment it is associated with is not present in the NE. Provisioning is allowed according to the current administrative state for the entity. For the entity with the associated Unequipped state, all autonomous standing conditions except “Removed” are cleared and performance monitoring records are nulled and invalid. For supporting equipment, all autonomous standing conditions are cleared and performance monitoring records are nulled and invalid.

Mismatch

This autonomous state (MEA) indicates that the equipment it is associated with does not match the equipment that was assigned during provisioning, or that this equipment is disallowed in this position. Provisioning is allowed according to the current administrative state for the entity. For the entity with the associated Mismatch state, all autonomous standing conditions except MEA are cleared and performance monitoring records are nulled and invalid. For supporting equipment, all autonomous standing conditions are cleared and performance monitoring records are nulled and invalid.

Fault

This state (FLT) indicates that the associated equipment has a fault. The equipment, and the equipment supported by this equipment, is unable to perform their provisioned tasks. The equipment supported by this equipment will have the SGEO state associated with it. The list of conditions for this equipment will detail the fault.

Supporting Entity Outage

This autonomous state (SGEO) has a variety of root causes, for example:

- The supporting equipment is unequipped.
- The supporting equipment does not match the assigned supporting equipment.
- The supporting equipment has a fault condition.
- The entity has an outage of management communication

Port-Related Secondary States

Busy

This state (BUSY) indicates that an ECC is provisioned, and cross-connected to a PPP/IP entity on the NCU module.

Idle

This state (IDLE) indicates that an ECC is provisioned, but not cross-connected to a PPP/IP entity on the NCU module.

Facility Failure

This state (FAF) indicates that the associated facility has a failure, the list of conditions for this facility will detail the failure.

Auto Shutdown

This state (LKDO) indicates that the associated facility is autonomously suspended. This facility enters this state as a consequence of an event. This specific event can be found in the Current Conditions list, the condition name begins with “LKDO”.

Protection-Related Secondary States

Active

This state (ACT) indicates that the associated protection group is active.

Standby Hot

This state (STBYH) indicates that the entity is part of a protection group, and is the hot standby entity.

Inhibit SwitchToProtect

When this state (PSI) is true, it indicates that switching from the working to the protection facility is inhibited. This state is associated with the working facility.

Inhibit SwitchToWorking

When this state (PRI) is true, it indicates that switching from the protection to the working facility is inhibited.

Operation-Related Secondary States

Loopback

This state (LPBK) indicates that a loopback is set on the associated facility.

Forced On

This state (FRCD) indicates that the laser transmitter of the entity is forced on.

Diagnostic

This state (DGN) indicates that service affecting diagnostic activity is being performed on the port.

Configuration Management

This section contains detailed descriptions of some of the Fiber Service Platform 3000R7 functions that can be configured. The intent is to describe facts/behavior that is common across several module types, and is useful to know as background information when using these functions.

These functions are:

Loopbacks

When a link does not work as it should, the best way to investigate the fault is to perform loopback tests. In complex systems it is often difficult to determine the point of failure. Different loopback settings allow you to isolate failed components or fiber connections and test them separately. It is also possible to test a complete fiber link at one time.

A loopback is a channel connection with only one endpoint. Therefore, the channel itself immediately receives any signal transmitted through that channel. This function can be used to test each segment of the optical link within the system.

External loopbacks, using patch cables, is one method for investigating faults. Another method is using internal loops.

External loopbacks and internal loopbacks can be performed in unprotected and protected optical links. In a system with protected links, set loopbacks on the protection path to prevent service interruption on the working path. Always begin loopback tests on the customer premises equipment (CPE) with client port loopback tests. Then proceed on to loopback tests that involve other selected portions of the link.

> Be aware that all loopback testing is intrusive to the relevant optical link. Therefore, while you test a portion of a network or only a circuit, you will be unable to pass traffic across that link.

External Loopbacks

External loopbacks are formed by attaching a patch cable and an appropriate attenuator between the receiving and transmitting connectors of the specified port of a channel module. The attenuator is mandatory to prevent overloading or damaging the receiver.

Depending on which interface the patch cable is attached to, one differentiates between the following types of loopbacks:

- External client port loop
- External network port loop

Each of these types are described in the following.

External Client Port Loop

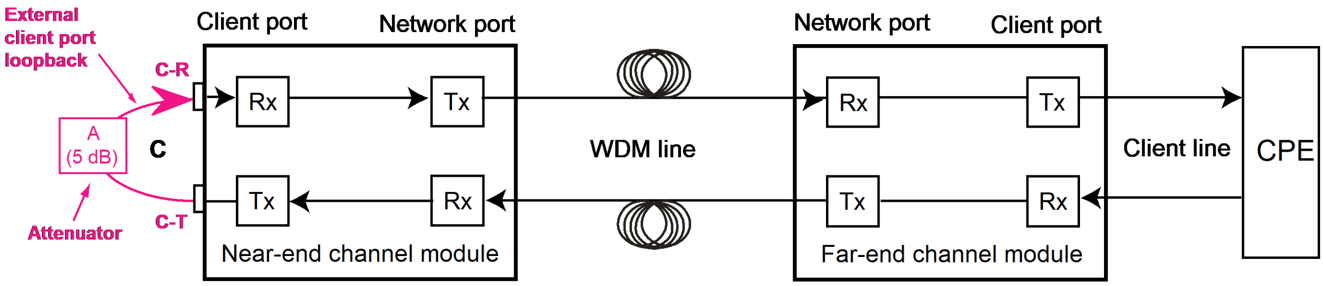
In this type of loopback, a patch cable is directly connected to the client port of the channel module itself.

Traffic that is transmitted from the client port C-T is returned to the client port C-R of the same module (Figure 40). The recommended attenuation on the client port is 5 dB. Using an external client port loop requires the ALS on the network port to be temporarily disabled.

The client port is disconnected from the near-end CPE, and the signal will be returned to CPE of the far-end network element provided that the WDM line and the client line are established.

This loop type can be used to test the connection between the client port of the near-end channel module and the far-end CPE as shown in Figure 40.

Figure 40: Example of a WDM Channel Module External Client Port Loopback



External client port loops must be established individually for each client port of a TDM channel module. The type of patch cable (single-mode or multimode) used for the external loop depends on the client interface of the channel module.

External Network Port Loop

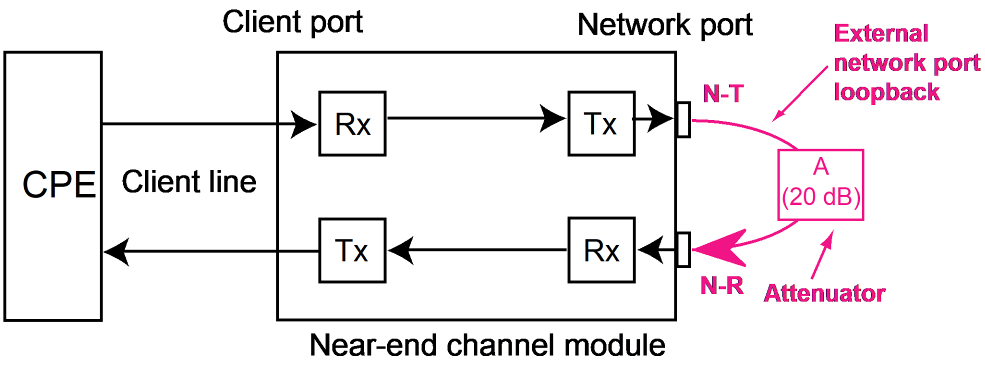
In this type of loopback, a single-mode patch cable is directly connected to the network port of the channel module.

Traffic that is transmitted from the network port N-T is returned to the network port N-R of the same module (Figure 41). To prevent a receiver overload a 20-dB single-mode attenuator between the N-T and N-R ports must be inserted.

The network port is disconnected from the WDM line and the signal will be returned to the near-end CPE provided that the client line is established.

This loop type can be used to test the connection between the near-end CPE and the network port of a near-end channel module as shown in Figure 41.

Figure 41: Example of a WDM Channel Module External Network Port Loopback



External network port loops must be established individually for each network port of a channel module with dual network interfaces.

Internal Loopbacks

Internal loopbacks are executed via the network element control unit (NCU) software and can be configured from a local management station or from a remotely connected management station using either of the management tools supported for the Fiber Service Platform 3000R7.

The Fiber Service Platform 3000R7 channel modules support two types of internal loopbacks on the client and network ports: facility loopbacks and terminal loopbacks. Four different internal loopback settings can be activated, deactivated, and monitored:

- Client interface facility loop
- Network interface terminal loop

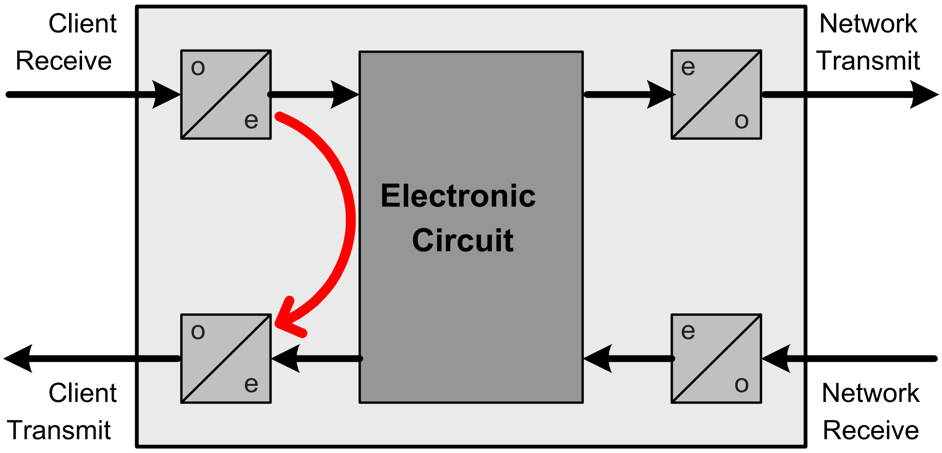
- Network interface facility loop
- Client interface terminal loop

For information about configuring internal loopbacks, refer to the Maintenance and Troubleshooting Manual.

Client Interface Facility Loopback

A facility loopback on a client interface can be used to test the connection between the CPE and the client port of the near-end channel module. Figure 42 illustrates this type of loopback.

Figure 42: Example of a Facility Loopback on a Client Interface



When a facility loopback on a client interface is configured, the incoming signal at the client port receiver Rx is looped back to the client port transmitter output Tx and directly retransmitted to the CPE.

Facility loopback characteristics for WCCs:

- traffic is interrupted
- the corresponding slot status LED indicator on the shelf blinks yellow.

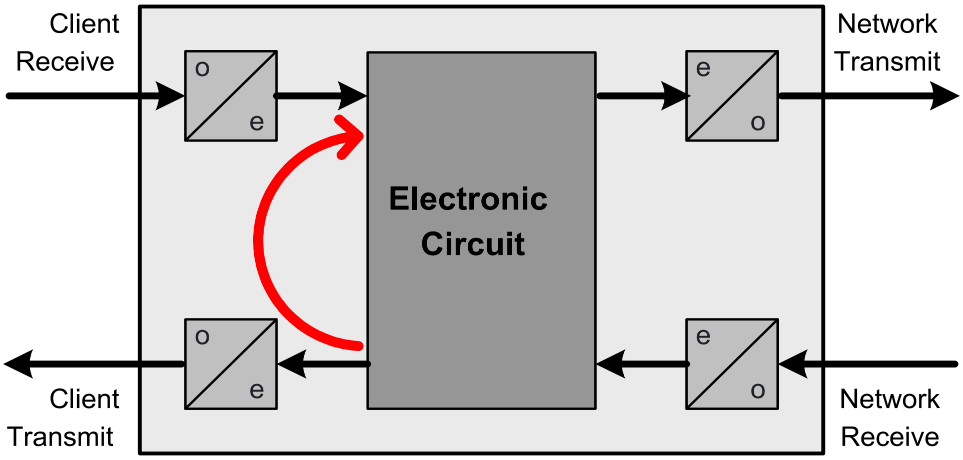
Facility loopback characteristics for multi-client port TCCs:

- performed individually for each client port
- the laser of the network port functions normally
- interrupts traffic only for the port that is being looped
- the corresponding slot status LED indicator on the shelf blinks yellow.

Client Interface Terminal Loopback

A terminal loopback on the client interface of a far-end channel module enables the testing of the complete communications link between the CPE and the client port of the far-end module. Figure 43 illustrates this.

Figure 43: Terminal Loopback on the Client Port



The signal from the near-end CPE is passed through the near-end channel module and the WDM line. At the far-end NE, the corresponding channel module receives signals via its network port. When a terminal loopback is configured at the far-end module, the incoming signal is looped back via the WDM line to the near-end CPE.

Terminal loopback characteristics for WCCs:

- traffic is interrupted
- the corresponding slot status LED indicator on the shelf blinks yellow.

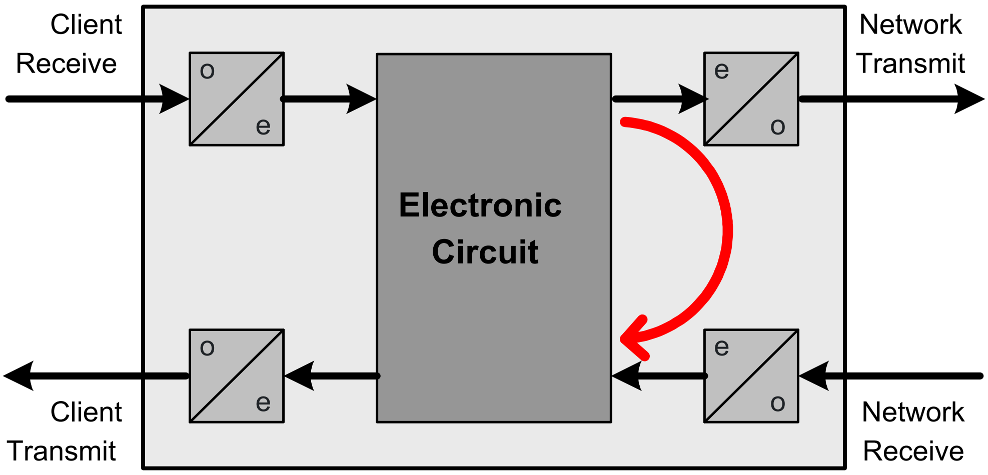
Terminal loopback characteristics for multi-client TCCs:

- performed individually for each client port
- the laser of the client port is switched off
- interrupts traffic only for the port that is being looped
- the corresponding slot status LED indicator on the shelf blinks yellow.

Network Interface Terminal Loopback

A terminal loopback on the network interface can be used to test the connection between the CPE and the network port of the near-end channel module. Figure 44 illustrates this.

Figure 44: Terminal Loopback on a Network Interface



Traffic from the CPE enters the channel module via the client port and passes through the module. When a terminal loopback is configured, the module is disconnected from the network line, and traffic is looped back via the client line to the CPE.

Terminal loopback characteristics:

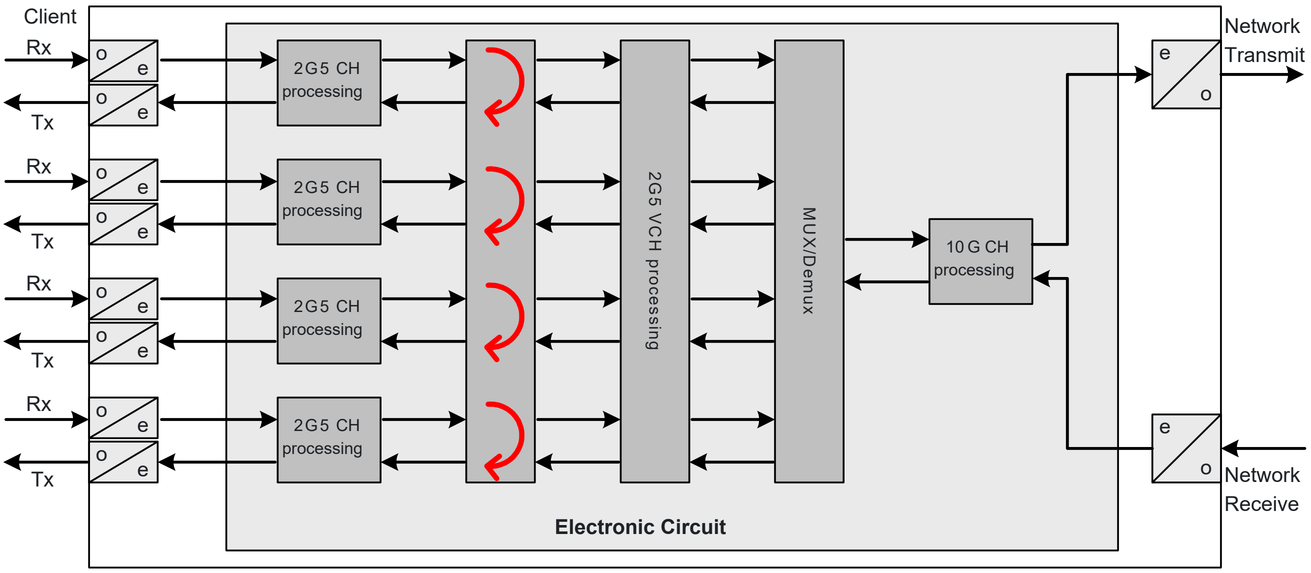
- traffic is interrupted
- the corresponding slot status LED indicator on the shelf blinks yellow

Terminal loopback characteristics for channel modules with dual network interfaces:

- performed individually for each network port
- the laser of the client port is switched off
- interrupts traffic only for the network port that is being looped
- the corresponding slot status LED indicator on the shelf blinks yellow.

For the 4TCC-PCTN-2G7+10G-V#D01-32, the network interface terminal loopback is a little different, see Figure 45.

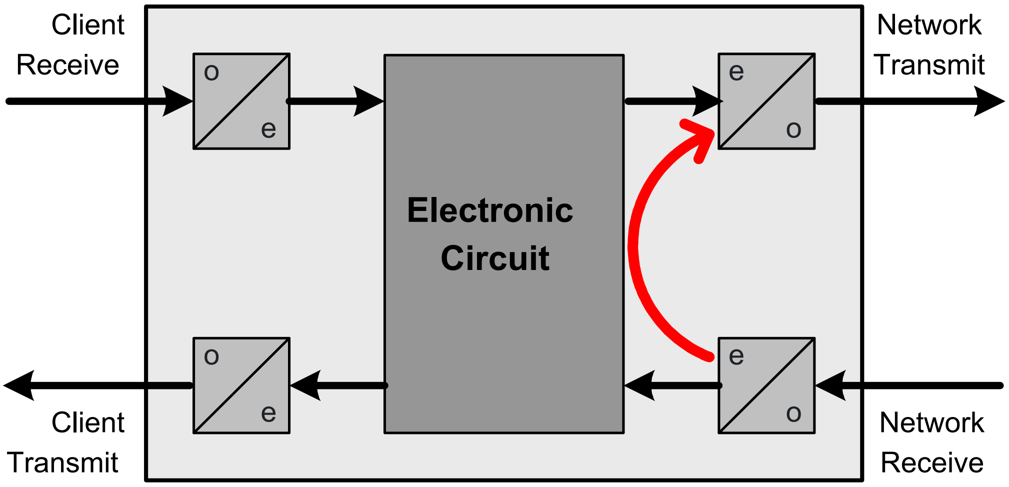
Figure 45: Terminal Loopback on a 4TCC-PCTN-2G7+10G-V#D01-32 Network Interface



Network Interface Facility Loopback

A facility loopback on the network interface of a far-end channel module enables the testing of the connection between the CPE and the network port of the far-end channel module. Figure 46 illustrates this type of loopback.

Figure 46: Facility Loopback on the Network Port of a Far-End Module



Signal from the CPE is received by the network port of the far-end module. Incoming signal at the receiver input Rx is looped back to the transmitter output Tx and directly retransmitted to the CPE. Reception of a signal at the network port receiver is required for the network port laser to switch on after the test.

Facility loopback characteristics:

- traffic is interrupted
- the corresponding slot status LED indicator on the shelf blinks yellow

Facility loopback characteristics for TCC, TCA and channel modules with dual network interfaces:

- traffic is interrupted
- performed individually for each network port.

Overview of Loop Functionality Support

For loop back behavior of the modules see the table below.

Table 7: Loop Back Behavior of Modules

Module	Port	Terminal Tx Data Continues	Facility Tx Data Continues	Terminal Tx Data Terminated	Facility Tx Data Terminated
5WCA-PCN-16GU	N			X	X
	C			X	X
WCC-PCN-100G	N	X	X		
	C	X	X		
WCC-PCN-100GB	N	X	X		
	C	X	X		
WCC-PCN-AES100GB	N				
	C	X	X		
WCC-PCN-AES100GB-F	N				
	C	X	X		
WCC-PCN-AES100GB-G	N				
	C	X	X		
4TCC-PCN-32GU+AES100GU	N				
	C	X	X		
4TCC-PCN-32GU+AES100G-S	N				

Table 7: Loop Back Behavior of Modules

Module	Port	Terminal Tx Data Continues	Facility Tx Data Continues	Terminal Tx Data Terminated	Facility Tx Data Terminated
	C	X	X		
10TCC-PCN-40GU+100G	N	X	X		
	C	X	X		
10TCC-PCTN-10G+100GB	N			X	X
	C			X	X
10TCC-PCN-3GSDI+10G	N		X		
	C		X[1]		
16TCC-PCN-4GUS+10G	N	X	X		
	C	X	X		
2TWCC-PCN-2G7UB	N	X	X		
	C	X	X		
2WCC-PCN-10G	N	X	X		
	C	X	X		
4WCC-PCN-10G	N	X	X		
	C	X	X		
10TCE-PCN-16GU+100G	N	X	X		
	C	X	X		
10TCE-PCN-16GU+AES100G	N	X[2]			
	C	X	X		

[1] Supported for bidirectional services only.

[2] Supported only if AES disabled.

Table 7: Loop Back Behavior of Modules

Module	Port	Terminal Tx Data Continues	Facility Tx Data Continues	Terminal Tx Data Terminated	Facility Tx Data Terminated
10TCE-PCN-16GU+AES100G-BSI	N				
	C	X	X		
10TCE-PCN-16GU+AES100G-F	N				
	C	X	X		
9TCE-PCN-10GU+10G	N	X			
	C	X	X		
9TCE-PCN-10GU+AES10G	N				
	C	X	X		
9TCE-PCN-10GU+AES10G-F	N				
	C	X	X		
9TCE-PCN-10GU+AES10G-G	N				
	C	X	X		
6WCA-PCN-28GU	N		X		
	C		X		

Verifying Connectivity by Using Trace

Trace is a way to check proper connectivity within a network by using the trace bytes. The principle is that an expected trace message is defined for a connection. The transmitter enters this message in the trace overhead bytes when sending. The receiver checks the message received in the trace bytes against the expected message. A mismatch indicates that the sender and receiver that were supposed to be connected, may not be correctly connected. A Trace Identifier Mismatch (TIM) alarm can be raised upon detection of such a mismatch, this is configurable per trace message.

Trace is supported on SDH, SONET and OTN interfaces.

- SDH/SONET interfaces support Regenerator Section (RS)/Section trace (J0). The RS/Section trace will be supported in accordance with G.707, G.783 and GR253.
- OTN interfaces support trace in OTU SM, ODU PM and activated ODU TCMs in accordance with [G.709] and [G.798].

The channel modules support trace monitoring as follows:

- The received trace message for a protocol layer is read from the module, when the module is configured to monitor that protocol layer.
- The expected trace message for a protocol layer can be configured, when the module is configured to monitor that protocol layer.
- The transmitted trace message for a protocol layer can be configured, when the module is configured to terminate that protocol layer.

For SDH/SONET, the J0 trace byte may contain a whole message, or successive bytes may be concatenated to contain a longer message. The supported message lengths in Fiber Service Platform 3000R7 are:

- 1 byte. The 1 byte shall contain one of the codes 0-255.
- 16 byte frame. The first byte in this frame should consist of a CRC-7 calculation over the previous frame, and the following 15 bytes transport T.50 characters.
- 64 byte frame. In the 64 byte frame the last two bytes are carriage return (0x0d) and a line feed (0x0a). This particular combination of values must not be used in other places in the message.

For OTN, the trace comparison process in the Fiber Service Platform 3000R7 is based only on the SAPI, as Fiber Service Platform 3000R7 connections are Point-to-Point connections only. The message is contained in a 64-byte string.

- The first byte is fixed to all 0s.
- The next 15 bytes contain the Source Access Point Identifier (SAPI).
- The 16th byte is fixed to all 0s.
- The next 15 bytes contain the Destination Access Point Identifier (DAPI).
- The last 32 bytes are operator specific.

The length and format of the trace string is the same for all layers in OTN. The SAPI and DAPI may consist of a 3-byte country code and a 12-byte National Segment code.

TIM Consequent Actions

Some channel modules may be provisioned to trigger consequent actions following the detection of a trace identifier mismatch. The TIM Mode, independently available for each OTU, ODU, and TCM layer of supporting channel modules, may be provisioned to trigger consequent actions.

> To determine whether a module supports traces, refer to the Management Data Guide. The TIM Mode is listed for each applicable layer for modules that support traces.

The TIM Mode may be set independently at any layer to any of these values:

- When set to disabled (DSBLD), a TIM alarm is not raised for the respective layer, even if a trace identifier mismatch is detected.
- When set to enabled with AIS insertion (ENBLD_AIS), a TIM alarm is raised for the given layer when a trace identifier mismatch is detected. Additionally, an alarm indication signal (AIS) is inserted into the ODU layer of the incoming signal[1]. The incoming ODU-AIS then results in a consequent action for any downstream ports that receive the ODU-AIS signal. For example, if the TIM is detected on the network port of a transponder, then these actions may be expected at the client:
  - For OTU clients, the outgoing client signal is replaced with an ODU-AIS.
  - For Ethernet clients, the outgoing client signal is replaced with LOCAL_FAULT.
  - For SONET/SDH clients, the outgoing client signal is replaced with an AIS-L.
- When set to enabled without AIS insertion (ENBLD_AISDSBLD), a TIM alarm is raised for the given layer when a trace identifier mismatch is detected. However, ODU-AIS does not replace the incoming signal.

Error Forwarding

As a consequence of detecting a failure on a port receiver, a channel module will indicate this to the channel modules in the downstream NEs. How this error is forwarded depends on which layer the failure is detected on. Generally, the Fiber Service Platform 3000R7 forwards errors according to the relevant standard for the layer the failure is detected on. In the case of proprietary interfaces, the error forwarding is proprietary.

For SDH, SONET and OTN signal types, error propagation in Fiber Service Platform 3000R7 is implemented according to the following standards:

- For SDH: ITU-T G.783
- For SONET: GR253
- For OTN: ITU-T G.798

For GbE and FC signal types, error code propagation in Fiber Service Platform 3000R7 is implemented according to ITU-T G.7041.

[1] The ENBLD_AIS feature is not supported on all modules or at all layers. Currently, this option is only available on the network ports of WCC-PCTN-100GB and 10TCC-PCTN-10G+100GB modules, at the ODU and OTU layers.

Forwarding of Errors Detected on Client Port

As an illustration of the possibilities that are supported, an error detected on a channel module's client port receiver could be forwarded as follows:

- A transponder channel module deactivates its network port laser.[1]
- A transponder channel module generates AIS as an error propagation code, and inserts it downstream of the failure (via the network port).
- A muxponder channel module could apply one of the following methods:
  - Use of GFP Control Management Frames (CMF).
  - Use of AIS or PN11.
  - Proprietary use of overhead.

Forwarding of Errors Detected on Network Port

As an illustration of the possibilities that are supported, an error detected on a channel module network port could be forwarded as follows:

- The channel module deactivates its client port laser.[2]
- When the client port is equipped with an SFP-E, the channel module deactivates the SFP-E transmitter (electrical).
- The channel module generates AIS[3] [4]as an error propagation code, and inserts it downstream of the failure (via the client port).
- The channel module generates an error propagation code (EPC) according to G7041, and inserts it downstream of the failure (the client port).

Error Forwarding Examples

Error forwarding is accomplished differently depending on the channel module you use. Take a typical point-to-point network between node A and node B. If no signal is detected at the client receive port at node A, no data can be sent out on the client transmit port at

[1] For relevant signal types it is possible to enable or disable application of a delay before port laser deactivation (Laser-Off Delay). The delay itself (Laser-Off Delay Timer) is not configurable. For GbE services the default is ENABLED while other service types the default is DISABLED. The system applies the relevant value for the transported signal type and provisioned parameters. When enabled, the delay is always 250 ms. In channel and channel card protection scenarios, the delay must be disabled (this is the default setting). In this case, the delay is 10 ms.

[2] For relevant signal types it is possible to enable or disable application of a delay before port laser deactivation (Laser-Off Delay). The delay itself (Laser-Off Delay Timer) is not configurable. For GbE services the default is Enable while other service types the default is Disable. The system applies the relevant value for the transported signal type and provisioned parameters. When enabled, the delay is always 250 ms. In channel and channel card protection scenarios, the delay must be disabled (this is the default setting). In this case, the delay is 10 ms.

[3] The multi-frame alignment signal is not included when creating ODU-AIS on 4TCC40G channel modules. A LOM will be raised and any allowed traces are not usable during ODU-AIS insertion.

[4] The 16TCC-PCN-4GUS+10G module does not use AIS-L as the error forwarding code for SDH/Sonet clients. It uses PN11 (Generic-AIS).

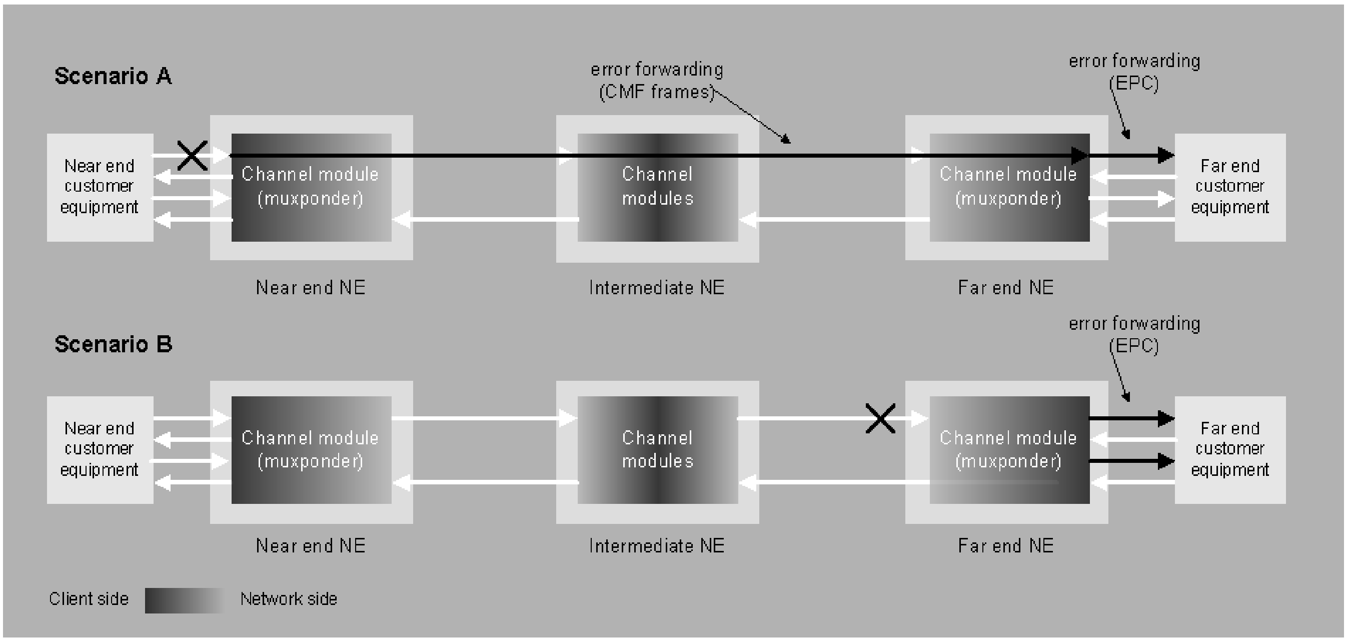
node B because no data is being received from the opposite side. The same thing occurs if the network link is down between node A and node B. Some channel modules use error forwarding measures like Alarm Identification Signal (AIS) and Error Propagation Code (EPC) to send error data to the node B transmitter and others turn off the transmitter at node B. You can see if your channel module supports error forwarding when the channel module is created.

This section contains example scenarios for various error-forwarding methods.

Error Propagation Code Example

For a 2TWCC2G7 muxponder channel module that transports GbE, two scenarios are useful for illustrating error forwarding, see Figure 47.

Figure 47: Example 1 - 2TWCC Error Forwarding Behavior

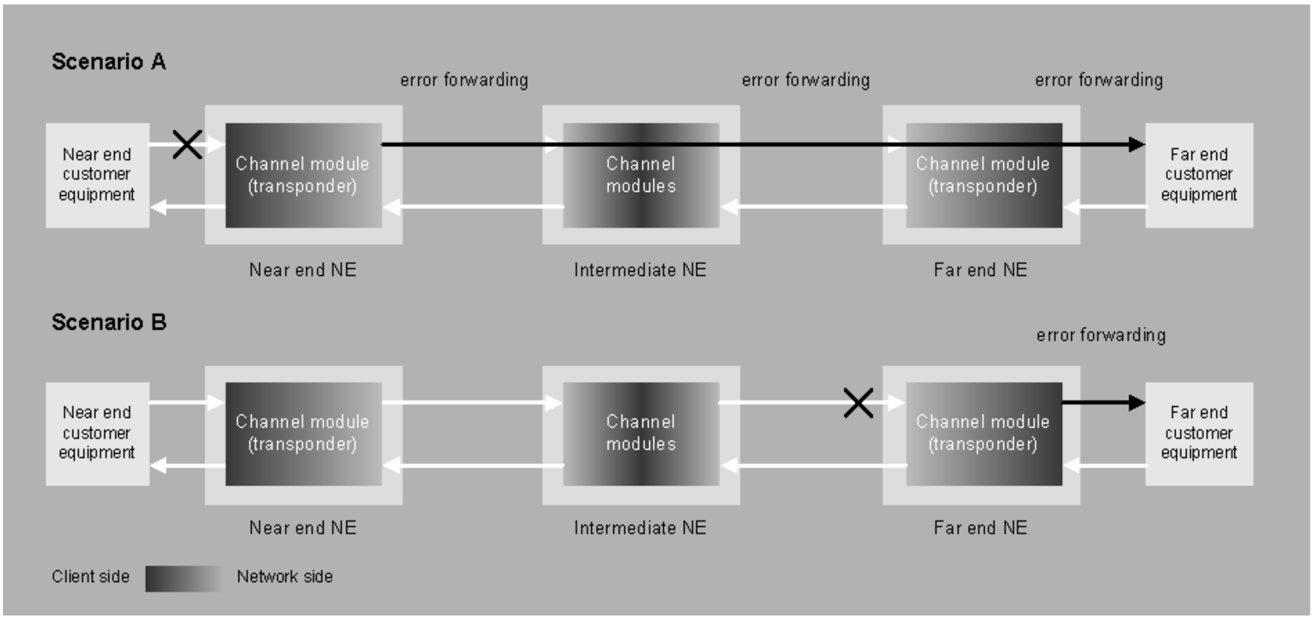


Scenario	Description
A	The 2TWCC2G7 multiplexes the client signals before it transports the signal to the far-end NE. When the system detects a failure on a client port, it is a requirement for it to first indicate this failure to the corresponding client port of the far-end muxponder channel module. The near-end muxponder channel module uses client management frames (CMF) to forward the error to the corresponding client port on the far-end muxponder channel module. The far-end muxponder channel module then inserts an error propagation code (EPC) in the client transmitter to forward the error to the corresponding far-end client equipment receiver.
B	The failure on the far-end network receiver results in the far-end channel module forwarding the error to both of the far-end client equipment receivers by inserting a 10BERR error propagation code (EPC).

AIS Example

For a WCC-PCTN-10G transponder channel module that transports STM-64 on both the client and network side, two scenarios are useful for illustrating error forwarding, see Figure 48.

Figure 48: Example 2 - WCC-PCTN-10G Error Forwarding Behavior

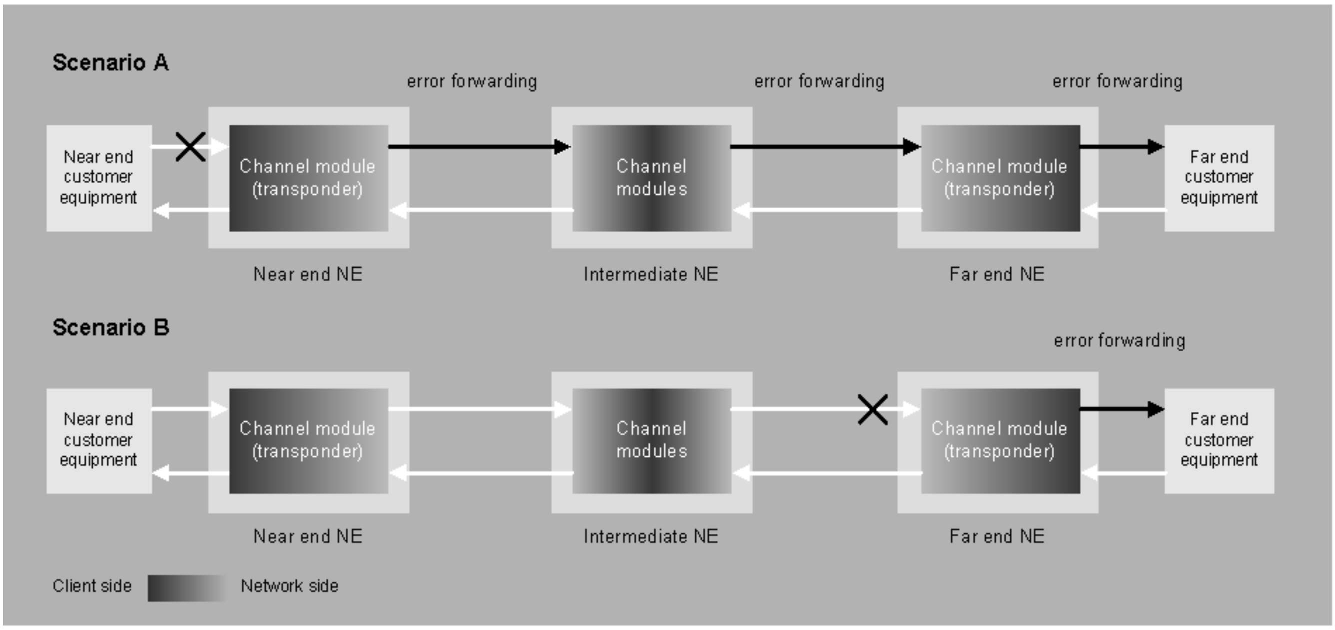

Scenario A
error forwarding
error forwarding
error forwarding
Near end customer equipment
Channel module (transponder)
Channel modules
Channel module (transponder)
Far end customer equipment
Near end NE
Intermediate NE
Far end NE
Scenario B
error forwarding
Near end customer equipment
Channel module (transponder)
Channel modules
Channel module (transponder)
Far end customer equipment
Near end NE
Intermediate NE
Far end NE
Client side
Network side

Scenario	Description
A	The failure on the near-end client receiver results in the near-end channel module inserting an AIS on its network transmitter. The channel modules in the intermediate NE perform no error forwarding. The AIS is transported through them and thus reaches the client equipment receiver.
B	The failure on the far-end network receiver causes the far-end channel module to insert an AIS on the client transmitter, which reaches the client equipment client receiver.

Laser Deactivation Example

For a WCC-PCTN-10G transponder channel module that transports 10GbE on both the client and network side, two scenarios are useful for illustrating error forwarding, see Figure 49.

Figure 49: Example 3 - WCC-PCTN-10G Error Forwarding Behavior


Scenario A
error forwarding
error forwarding
error forwarding
Near end customer equipment
Channel module (transponder)
Channel modules
Channel module (transponder)
Far end customer equipment
Near end NE
Intermediate NE
Far end NE
Scenario B
error forwarding
Near end customer equipment
Channel module (transponder)
Channel modules
Channel module (transponder)
Far end customer equipment
Near end NE
Intermediate NE
Far end NE
Client side
Network side

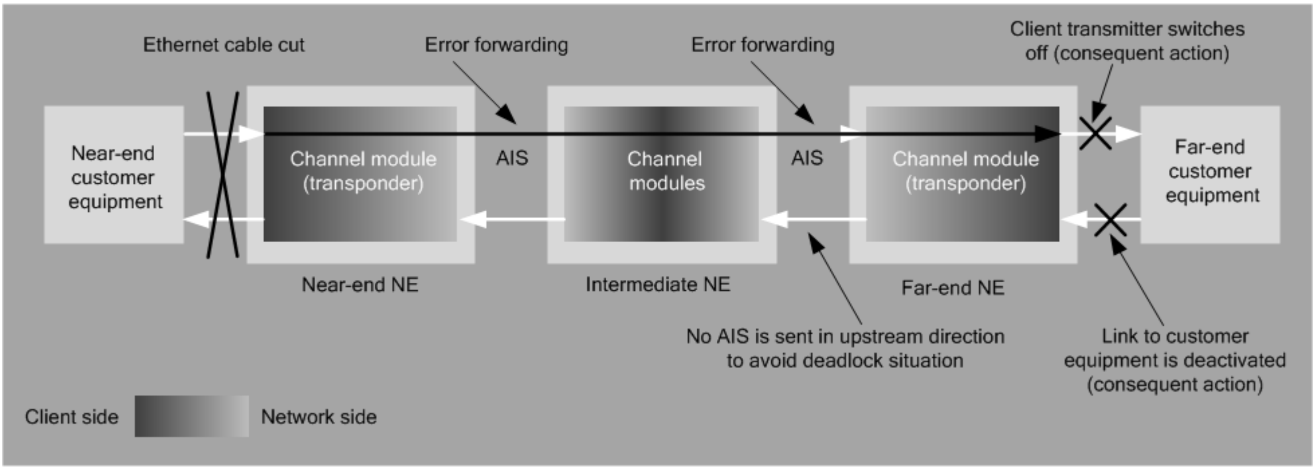
Scenario	Description
A	The failure on the near-end client receiver causes the near-end channel module to turn off its network transmitter. The intermediate NE detects a failure on its client receiver port and consequently turns off its network port laser. This scenario also takes place at the far-end NE, and the client equipment receiver detects the failure.

Scenario	Description
B	The failure on the far-end network receiver results in the far-end channel module turning off its client transmitter. The client equipment receiver then detects the failure.

Transmitter Deactivation Example for Electrical Links

The 4TCA-PCN-4GU+4G, 4TCA-PCN-4GUS+4G, and 10TCC-PCN-2G7US+10G modules equipped with SFP-E transmitters support client transmitter deactivation at the far-end channel module. This error forwarding feature is illustrated in Figure 50.

Figure 50: Example 4 - 4TCA-PCN-4GU+4G Error Forwarding Behavior


Ethernet cable cut
Error forwarding
Error forwarding
Client transmitter switches off (consequent action)
Near-end customer equipment
Channel module (transponder)
AIS
Channel modules
AIS
Channel module (transponder)
Far-end customer equipment
Near-end NE
Intermediate NE
Far-end NE
No AIS is sent in upstream direction to avoid deadlock situation
Link to customer equipment is deactivated (consequent action)
Client side
Network side

If an operator cuts an Ethernet cable that carries a 1GbE client signal, an external-link failure alarm is raised on the client channel port. After the near-end module detects this failure on its client channel port, the module inserts into its network transmitter an AIS, which is an error indication signal that the affected card supports. The channel modules in the intermediate NE forward the AIS to the far-end channel module, which detects the failure and stops its client transmitter. This client channel port also raises the auto shutdown (OFF) alarm because the system forwards the error to that client channel. The system deactivates the external-link failure alarm, which is the link to the far-end customer equipment. The system then deactivates the alarm because the far-end channel module is unable to synchronize with it.

To support reliable Auto Negotiation, the system does not insert an error-indication signal for E10-100TX and E10-1000T client signals in order to prevent a failure on the client receiver. This behavior is independent from Auto Negotiation configuration. For that reason, after the far-end channel module receives an external link failure that the near-end channel module detects, the far-end module continues to operate its transmitter.

After the system restores the connection to the near-end channel module, it ceases to transmit AIS. This action prompts the far-end module to activate its client transmitter. The client channel port also clears the auto shutdown (OFF) alarm and begins to resynchronize with the far-end customer equipment in order to activate the link. After the channel port completes this task, it clears the external-link failure alarm.

> The software prevents a deadlock or impasse situation when transponders at both ends are equipped with SFP-Es, and their error forwarding modes are set to **TxOff**. If the system switches off both the near-end and far-end client transmitters, the customer equipment will also switch off its transmitter. This situation causes a deadlock because the link remains deactivated. A special state machine ensures that no one can switch off both the near-end **and** far-end client transmitters. This precaution is why only the External Link Failure alarm is raised at the near-end client channel port.

About the 16TCC-PCN-4GUS+10G module

Deadlock prevention is not needed for the 16TCC-PCN-4GUS+10G module because the module does not support client failure end to end error forwarding. The module equipped with SFP-E transmitters supports client transmitter deactivation at the far-end channel module. Consequent actions are implemented with these rules:

In mode 1GbE both electrical and optical SFP is supported.

- In mode 1GbE with electrical SFP-E equipped.
  - On RX: External Link Fail (removed cable) doesn’t trigger any CA (no aCSF).
  - On RX: Plug removed triggers CA (aCSF).
  - On TX: ODU and OPU defects (AIS, OCI, LCK, OPU-PLM, OPU-CSF) detected on VCH triggers CA (Auto Shutdown Forward).
- In mode 1GbE with optical SFP equipped.
  - On RX: LOS and Plug removed triggers CA (aCSF).
  - On TX: ODU and OPU defects (AIS, OCI, LCK, OPU-PLM, OPU-CSF) detected on VCH triggers CA according to error forwarding mode (EPC or OFF).

In mode E10-100TX and E10-1000T electrical, only SFP is supported.

- On RX: External Link Fail (removed cable) doesn’t trigger any CA (no aCSF).
- On RX: Plug removed triggers CA (aCSF).
- On TX: ODU and OPU defects (AIS, OCI, LCK, OPU-CSF) detected on VCH triggers CA (Auto Shutdown Forward).
- On TX: OPU-PLM doesn’t trigger any CA (no Auto Shutdown Forward).
  - Different rates set by Auto Negotiation are communicated to far-end by OPU payload type:
    - 0x81 – 10Mbit/s
    - 0x82 – 100Mbit/s
    - 0x83 – 1000Mbit/s

    - To support reliable operation of Auto Negotiation, an error indication signal is not inserted when OPU-PLM is detected.

Using the Threshold Profile

Use threshold profiles to set equipment thresholds for an entire node. You can then export these profiles and use them in other nodes. By using these equipment settings across nodes, the network will have consistent threshold settings.

These user interfaces support threshold profile management:

- TL1
- SNMP
- Craft
- NED

Only one threshold profile can be active, and one remains in the standby area. Software or database changes in the node have no effect on the standby area.

When you use threshold profiles, you can change threshold values for each performance monitoring group. You can divide each group into several sub-profiles that are identified by numeric index. The system manages OPR and OPT thresholds differently and divides their sub-profiles by module or plug type and numeric index.

These performance monitoring groups support the use of threshold profiles:

- OTU
- FEC
- Ethernet Tx (ETH-TX)
- Ethernet Rx (ETH-RX)
- SONET/SDH-Line/MS (SONET-L)
- ODU
- PCS
- SONET/SDH-Section/RS (SONET-S)
- TCMA
- TCMB
- TCMC
- Polarization Rate (SOPT)
- Alignment Delta (SKEW)
- Round Trip Delay (RNDTRPDLY)
- Attenuation Tx (ATTRMT)
- Diff Group Delay (DGD)

- Quality Factor (QFACT)
- OSC Power Rx (OSCPWR)
- Carrier Offset (CFOT)
- Round Trip Latency (LATENCY)
- Attenuation Rx (ATRCV)
- Back Reflection Rx (BR)
- CD Compensation (CD)
- CD Compensation 40G (CDC)
- Signal-to-Noise Ratio (SNR)
- Optical Power Received(OPR) and Optical Power Transmitted (OPT)

You can edit thresholds in a threshold profile only when the threshold profile is part of the active database. The software applies threshold profile changes only after you activate the profile. You can also manually edit thresholds for each module, but the threshold profile will not reflect these changes. If you want the threshold profile to reflect changes, you need to edit it explicitly. When you add a new item to the related performance monitoring group, the process uses the thresholds in the active threshold profile as default values.

Only one threshold profile can be active in the NCU. You can export only the active profile from the NCU. After the export, the process creates the new threshold profile file on the NCU RDISK/. You can then copy the profile to other NCUs. Imported and activated profiles overwrite all thresholds that you specified in the threshold profile and currently set on the NCU.

During a database restore, the restore process replaces the active threshold, and the new profile from the database becomes the active profile. If the standby profile is more recent than the release profile, or no standby profile exists, the restore process uses the default profile.

Performance Management

Performance management includes configuration of performance monitoring, viewing, and reporting of performance data. This section contains detailed descriptions of the performance counters and records that the Fiber Service Platform 3000R7 supports.

The Fiber Service Platform 3000R7 provides monitoring of performance at module level, client interface level, and network interface level.

The network element collects the following information:

- Physical layer measurements
- Data layer counters

The collected information is stored in records. A number of these records are stored in order to provide a history.

In addition, the Fiber Service Platform 3000R7 provides current measurements of some physical-layer parameters, such as transmit/receive optical power, which are not logged in records. They are thus only viewable as instantaneous measurements.

The performance parameters measured and/or recorded may depend on the module type. To find out exactly which measured parameters/counters that are available for a certain module type, please look up that module type in the Management Data Guide.

The performance data, supported record types, record content, and record storage are described in the following sections:

Physical-Layer Performance

Physical layer performance is monitored at module and port level, this includes monitoring of the optical layer as supported by the optical line monitoring functionality. For a list of modules supporting the optical line monitoring functionality, refer to the *Module and System Specification*.

The Fiber Service Platform 3000R7 provides measurements of physical layer parameters in two ways:

- recorded measurements
- non-recorded, current measurements

For these measurements you can set thresholds so that a Threshold Crossing Alarm (TCA) is generated if the measurement reaches or crosses a threshold.

In addition, Fiber Service Platform 3000R7 offers one error counter to monitor the entire physical layer.

Recorded Measurements

Every second the system measures and records the physical layer parameters listed in Table 8. Which parameters are measured on a module or module port depends on the module type. The *Management Data Guide* provides a per module overview of which parameters are measured for which ports.

At the end of the recording interval, the average value is calculated and stored in the record. In addition, the lowest and highest values that were measured during the recording interval are added to the record. The recording intervals are 15 minutes, 1 day, and 1 week.

The average value over the recording interval is calculated by adding together all recorded measurements and dividing by the number of seconds in the recording interval. Notice that for parameters measured in dBm, this average, which is displayed as the “mean” value, is not the average of the power level received within the 15 minute recording interval. It is only the average value of the recorded power level measurements expressed in dBm within the 15 minute period.

Table 8: Table 1: Monitored Physical Layer Parameters

Physical Parameter	Unit
Attenuation Rx Fiber	dBm
Attenuation Tx Fiber	dBm
Current	mA
Optical Power Rx	dBm
Optical Power Tx	dBm
OSC Gain	dB
Back Reflection Rx	dB
Pump Power	dBm
OSC Power Rx	dBm
Estimated Gain	dB
Dispersion Compensation	ps/nm
Link Attenuation	dB

Instantaneous Measurements

The network element system measures the physical layer parameters listed in Table 9. Which parameters are measured on a module, or module port, depends on the module type. The RSM-OLM provides a per module overview of which parameters are measured and whether they are measured at the module or port. These parameters are not recorded.

Table 9: Instantaneous Measurement Parameters

Physical Parameter	Unit	Description
Laser Bias Current	mA	Real time Laser Bias Current
Laser Bias Current Average	mA	Averaged Laser Bias Current 10 second window
Temperature[1]	°C	Module or Plug Temperature
Temperature 2	°C	Temperature second monitored point
Laser Temperature[2]	°C	Real time Laser Temperature
Current	mA	
Pump Power	dBm	
Pump-{1|2} Laser Temp	°C	
Pump-{1|2} Laser Bias Current	mA	
Attenuation	dB	
External Loss	dB	Attenuation in dB from 1 stage transmit to 2 stage receive
Hours of Operation	h	Accumulated total of operating hours
Average measured BER		Average measured Bit Error Rate for the PRBS test signal
Maximum measured BER		Maximum measured BER for the PRBS test signal during monitored time
Error free time for PRBS	Sec	Error free time for PRBS since last detected error.
Elapsed Time	Sec	Elapsed time since PRBS test signal start
OTDR Remaining Time	Min	Monitors the remaining OTDR operation time[1]
Max Output All PSUs	dB	Total power output (supplied)

[1] Module or plug temperature

[2] Network port

Table 9: Instantaneous Measurement Parameters

Physical Parameter	Unit	Description
Max Power All Equipment	dB	Total power uptake (consumption)

1. The "OTDR Operation Time" can be set to "disable", "5 minutes", "20 minutes", "40 minutes" or "60 minutes. In case it expires all settings are reset in normal operation mode. If the "OTDR Operation Time" is set the switching option of the RSM-OLM is inhibited and the pilot laser is disabled.

Physical-Layer Counter

The Fiber Service Platform 3000R7 offers one counter for monitoring of the physical layer, depending on the type of module. The supported performance counter is described in Table 10.

Table 10: Physical Layer Counter Descriptions

Counter name	Description
Defect Seconds (DS)	Increased for each second in which an error on the physical layer occurs

Data-Layer Performance

Data layer performance is monitored at the interface level. The Fiber Service Platform 3000R7 offers performance for monitoring of the following data layers:

- OTN (OTU, ODU, FEC)
- SDH/SONET
- Sub-aggregate layer
- GFP
- Ethernet
- Physical conversion layer

Which data layers are monitored for each module depends on the module type. For each data layer a set of counters are recorded. The current values as well as historic values are stored in records for 15-minute and 1-day time periods. For the SDH/SONET or OTN layers, you can set thresholds for each performance counter. Then a threshold crossing alert (TCA) is generated if the performance counter reaches or crosses a specified threshold.

When an SDH, SONET or OTN layer is terminated, the modules handle the overhead for this layer as follows:

- In a port’s receive direction, the overhead bytes are read, and processed according to the standards.
- In a port’s transmit direction, the channel module generates content and inserts this in the overhead bytes.

When an SDH, SONET or OTN layer is not terminated, it is non-intrusively monitored. The modules handle the overhead for this layer as follows:

- In a port’s receive direction, the overhead bytes are read, and processed according to the standards for non-intrusive monitoring.
- In a port’s transmit direction, no processing takes place.

The following sections list the supported counters for each of the data layers.

SDH/SONET Performance

The supported set of performance counters for the Regeneration Section/Section and Multiplex Section/Line are shown in Table 11. Sec/RS indicates a Section/Regenerator Section counter, while Line/MS indicates a Line/Multiplex Section counter.

> There is no distinction in counter names for SDH and SONET counters. The counter name may suggest a SONET counter, but is an SDH counter if your system is SDH.

Table 11: SDH/SONET Counter Descriptions

Counter Name	Description
Errored Second	Increased for each second in which one or more CV/BBEs, traffic disruptive defects, connection defects, or BIP-8 violations are detected.
Severely Errored Second	Iincreased for each second in which the number of bit parity violations is higher than a configurable threshold, or in the case of traffic disruptive or connection defects. The SES threshold is by default set to 30% of the transmitted frames. This threshold applies to all relevant entities in the Network Element.
Severely Errored Framing Second	Increased for each second with Out of Frame (OOF)/Several Errored Framing (SEF) or traffic disruptive defects.
Coding Violations Background Block Errors	Increased for each parity violation/background block error. Given one second for which the SES counter is increased, the parity violations registered in this second are not counted.

Table 11: SDH/SONET Counter Descriptions

Counter Name	Description
Unavailable Seconds	When more than 10 consecutive seconds of SES are recorded, the unavailable second (UAS) state is entered. The UAS counter is increased for each second this state persists. These 10 consecutive seconds are added to the counter. To exit the UAS state, more than 10 consecutive seconds without SES must be recorded. These 10 seconds are considered available seconds

> A Trace Identifier Mismatch (TIM) alarm is considered a traffic disruption.

The MDG provides a per module overview of which counters are supported for which ports, as well as the maximum value that can be recorded and the record type.

OTN Performance

The Fiber Service Platform 3000R7 provides a set of performance counters for the OTU, ODU and FEC sublayers. The OTN counters are listed in Table 12.

Table 12: OTN and FEC Counter Descriptions

Counter type	Description	Displayed counter names
Errored Second (ES)	Increased for each second in which one or more CV/BBEs, traffic disruptive defects, connection defects, or BIP-8 violations are detected.	OTU ES, ODU ES, TCM-A ES, TCM-B ES, TCM-C ES, OTU FEC ES[1]

[1] The OTU FEC PM record is extended with the counters ES (Errored seconds), SES (Severely errored seconds) and UBE (Uncorrected Block Errors) as compared to the ITU-T G.798 standard. This means that when FEC is disabled, the ES/SES counters in the FEC PM record will still contain valid values. ES is counted if corrected blocks are detected. Both ES and SES are counted if any SSF-resulting defects have occurred. Such defects include: SSF from physical layer (from root cause LOS, LOC), LOF, LOM or OTU-AIS detected at this termination level.

Table 12: OTN and FEC Counter Descriptions

Counter type	Description	Displayed counter names
Severely Errored Second (SES)	Increased for each second in which the number of bit parity violations is higher than a configurable threshold, or when one or more traffic disruptive or connection defects are detected. The SES threshold is set to 15% of the transmitted frames. The SES threshold for each protocol applies to the whole NE.	OTU SES, ODU SES, TCM-A ODU SES, TCM-B ODU SES, TCM-C ODU SES, OTU FEC SES[1]
Background Block Errors (BBE)	Increased for each parity violation. Given one second for which the SES counter is increased, the parity violations registered in this second are not counted.	OTU BBE, ODU BBE, TCM-A BBE, TCM-B BBE, TCM-C BBE
Unavailable Seconds (UAS)	When more than 10 consecutive seconds of SES are recorded the unavailable second (UAS) state is entered. The UAS counter is increased for each second this state persists. These 10 consecutive seconds are then added to the counter. To exit the UAS state, more than 10 consecutive seconds without SES must be recorded. These 10 seconds are considered available seconds.	OTU UAS, ODU UAS, TCM-A UAS, TCM-B UAS, TCM-C UAS
Corrected Errors (CE)	Increased for each error that is corrected. The error itself results in an ES, even though it is corrected. CE is not counted when FEC is disabled. In the 15min interval during which FEC was disabled, CE retains the status it displayed when FEC was disabled.	FEC Corrected Errors
Uncorrected Block Errors (UBE)	Increased for each byte with an error that is not corrected. UBE is not counted when FEC is disabled. In the 15min interval during which FEC was disabled, UBE retains the status it displayed when FEC was disabled.	FEC UBE[1]
Bit Error Rate (BER)	Computed in 15 minute and 24 hour intervals. The rate increases with each corrected error in the given interval. Bit Error Rate ignores CEs that occur during seconds when a UBE occurs. The formula uses only CEs occurring in seconds that do not contain UBEs.	BER before FEC

The *Management Data Guide* provides a per module overview of which counters are supported for which ports. It also provides information about the maximum value that can be recorded and the record type.

Physical Coding Sublayer (PCS) Performance

The Fiber Service Platform 3000R7 provides a set of performance counters for the physical coding sublayer of Ethernet and Fibre Channel.

This set of counters are described in Table 13, however, not all modules supporting these services support all of these counters. The *Management Data Guide* gives a per module overview of which counters are supported for which ports, as well as the maximum value that can be recorded and the record type.

In the column Counter Name, the counter name abbreviations that are displayed in the management tool are shown in parentheses.

Table 13: PCS Counter Descriptions

Counter Name	Description
Errored Second (PCS ES)	Increased for each second in which one or more CV/DE/SEs or traffic disruptive alarms are detected
Disparity Errors (PCS Disparity Errors)	Reports the number of detected 8B/10B disparity errors (DE)
Coding Violations (PCS CV)	Reports the number of detected code words violating the 8B/10B or 64B/66B coding rules, depending on the module type
Sync Header Errors (PCS SE)	Increased if more than 15 sync header errors are detected inside a 125 µs time slot
Coding Violations and Disparity Errors (PCS CV+DE)	Reports the number of detected disparity errors (DE) and coding violations (CV). This counter is only applicable to interfaces with 8B/10B coding.

Sub-aggregate Layer Performance

The 4TCA4GUS and 2TCA2G5 channel modules use a proprietary protocol on the network port when operating in multiplexer mode. These channel modules provide a set of performance counters for the sub-aggregate data layer at egress from de-multiplexing. This set of counters is described in Table 14.

Table 14: Sub-aggregate Layer Counter Descriptions

Counter Name	Description
Errored Second	Increased for each second in which one or more CRC or traffic disruptive alarms are detected
Severely Errored Second	Increased for each second in which the number of CRC errors is higher than a fixed threshold, or when traffic disruptive alarms are detected[1]
Cyclic Redundancy Check	Increased for every frame with an invalid CRC check sum

The *Management Data Guide* gives a per module overview of which counters are supported for which ports, as well as the maximum value that can be recorded and the record type.

Encryption Sublayer Performance

Encryption channel modules provide a set of performance counters for the encryption data layer at egress from de-multiplexing. This set of counters is described in Table 15.

Table 15: Encryption Sublayer Counter Descriptions

Counter Name	Description
Encryption Operation	Increased for every second in which data is encrypted
Encryption Degrade Time	Increased for every second in which data is encrypted using a “degraded or limited encryption” mode. The module uses degraded mode when, e.g. the key exchange between the encryption modules failed three times. Data transmission is nevertheless safe.
Encryption ES	Increased for every second in which data is not encrypted

The *Management Data Guide* gives a per module overview of which counters are supported for which ports, as well as the maximum value that can be recorded and the record type.

Ethernet Performance

Ethernet service counters (transmit and receive) are described in Table 16.

[1] For the 4TCA4GUS modules, this fixed threshold is 100. For the 2TCA2G5 module, this fixed threshold is 800.

Table 16: Ethernet Counter Descriptions

Counter name	Description
Broadcast Frames Rx	Number of received broadcast frames
Bytes Rx	Number of received bytes
CRC Errors Rx	Number of Ethernet MAC frames with CRC errors in the receive direction
Frames Rx	Number of successfully received Ethernet MAC frames
Frames Rx Discarded	Number of discarded Ethernet MAC frames due to buffer overflow in the receive direction
Multicast Frames Rx	Number of received multicast frame.
Oversized Frames	Number of received frames that are oversized
Pause Frames Rx	Number of received Ethernet MAC Pause frames
Undersized Frames	Number of received frames that are undersized
Utilization Rx	Calculated utilization in percentage (0% to 100%) for received Ethernet traffic (the current, high, mean, and low values are displayed)
64 Byte Frames Rx	Number of received frames of length 64 Bytes
65-127 Byte Frames Rx	Number of received frames of length 65-127 Bytes
128-255 Byte Frames Rx	Number of received frames of length 128-255 Bytes
256-511 Byte Frames Rx	Number of received frames of length 256-511 Bytes
512-1023 Byte Frames Rx	Number of received frames of length 512-1023 Bytes
1024-1518 Byte Frame Rx	Number of received frames of length 1024-1518 Bytes

Table 16: Ethernet Counter Descriptions

Counter name	Description
1519+ Byte Frames Rx	Number of received frames of length 1519 Bytes or more
Broadcast Frames Tx	Number of transmitted broadcast frames
Bytes Tx	Number of transmitted bytes
CRC Errors Tx	Number of Ethernet MAC frames with CRC errors in the transmit direction
Frames Tx	Number of transmitted Ethernet frames
Multicast Frames Tx	Number of transmitted multicast frames
Oversized Frames	Number of transmitted frames that are oversized
Pause Frames Tx	Number of transmitted Ethernet Pause frames
Undersized Frames	Number of transmitted frames that are undersized
Utilization Tx	Calculated utilization in percentage (0% to 100%) for transmitted Ethernet traffic (the current, high, mean, and low values are displayed)
64 Byte Frames Tx	Number of transmitted frames of length 64 Bytes
65-127 Byte Frames Tx	Number of transmitted frames of length 65-127 Bytes
128-255 Byte Frames Tx	Number of transmitted frames of length 128-255 Bytes
256-511 Byte Frames Tx	Number of transmitted frames of length 256-511 Bytes
512-1023 Byte Frames Tx	Number of transmitted frames of length 512-1023 Bytes
1024-1518 Byte Frame Tx	Number of transmitted frames of length 1024-1518 Bytes
1519+ Byte Frames Tx	Number of transmitted frames of length 1519 or more Bytes

The *Management Data Guide* gives a per module overview of the counters supported for each port, as well as the maximum value that can be recorded and the record type.

GFP Frame Performance

The service counters supported for GFP-F frames are described in Table 17. The service counters supported for GFP-T frames are described in Table 18.

Table 17: Framed GFP Frame Counter Descriptions

Counter name	Description
CHEC Frames Corrected	The GFP Core Header consists of a 16-bit PDU Length Indicator (PLI) and a 16-bit HEC (cHEC) protecting the Core Header. The cHEC corrects single bit errors and this counter reports the number of successfully corrected GFP Core Headers.
THEC Frames Corrected	The GFP frame Type field is protected by a HEC (the tHEC). The tHEC corrects single bit errors. This counter reports the number of successfully corrected Type Fields.
THEC Frames Discarded	This counter reports the number of Type Fields that were discarded due to correction not being successful.

Table 18: Transparent GFP Frame Counter Descriptions

Counter name	Description
CHEC Frames Corrected	The GFP Core Header consists of a 16-bit PDU Length Indicator (PLI) and a 16-bit HEC (cHEC) protecting the Core Header. The cHEC corrects single bit errors and this counter reports the number of successfully corrected GFP Core Headers.
CHEC Frames Discarded	This counter reports the number of Type Fields that were discarded due to correction not being successful.
GFP Valid Frames	This counter reports the number of received GFP frames that were valid.

Table 18: Transparent GFP Frame Counter Descriptions

Counter name	Description
THEC Corrected Frames	The GFP frame Type field is protected by a HEC (the tHEC). The tHEC corrects single bit errors. This counter reports the number of successfully corrected Type Fields.
THEC Discarded Frames	This counter reports the number of Type Fields that were discarded due to correction not being successful.
Discarded Super Blocks	This counter reports the number of discarded superblocks due to errors detected in the superblock CRC-16 error check.

The *Management Data Guide* gives a per module overview of which counters are supported for which ports, as well as the maximum value that can be recorded and the record type.

Performance Records

The Fiber Service Platform 3000R7 records physical-layer measurements in 15-minute, 24-hour and 1-week intervals, and records data-layer performance and service counters in 15-minute and 24-hour intervals. 15-minute intervals always start at a whole hour, a quarter past, half past or a quarter to an hour. For example, 02:00, 02:15, 02:30 and 02:45. The 24-hour intervals always start at midnight. The 1-week intervals always start at 00:00 on the night from Saturday to Sunday.

When the secondary state of an entity is “Unequipped”, “Mismatch” or “Fault”, performance recording for that entity is disabled and the content of the record so far is discarded. This is, for example, the case when an SFP transceiver is unplugged.

For each of the record types you can do the following:

- View the content of the current record while it is being created. This is called the Current Record.
- View the records after the recording interval has ended. A number of these records are stored. The collection of these records is called the History Record.
- For the data-layer records only, reset the Current Record or the Current and History Record list, if relevant.

Record Types

Current 15 Minute Record

The Current 15 Minute record contains the measurements or counters for the ongoing 15 minute interval as well as the elapsed time of the ongoing interval. When the ongoing 15 minute interval is completed, the content of this record is transferred to the Historic 15 Minute record, together with a timestamp to identify it. Then the counter content is reset and a new Current 15 Minute Record is started.

History 15 Minute Record

The History 15 Minute record contains the previous 15 minute records, as well as information about the validity of each of these records. A maximum of ninety-six previous 15 minute records are stored. The ninety-seventh 15 minute record will overwrite the oldest stored record. Thus, the Historic 15 Minute records together represent a 24 hour history.

Current 24 Hour Record

The Current 24 Hour record contains the measured contents of the counter for the ongoing 24-hour interval as well as the elapsed time of the ongoing interval. When the ongoing 24 hour interval is completed, the content of this record is transferred to the Historic 24 Hour record together with a timestamp to identify it. Then the counter content is reset and a new Current 24 Hour record is started.

History 24 Hour Record

The History 24 Hour record contains the previous 24 hour records, as well as information about the validity of each of these records. A maximum of thirty-one previous 24 hour records are stored. The thirty-second 24 hour record will overwrite the oldest stored record. Thus the Historic 24 Hour records together represent a 1 month history.

Current 1 Week Record

The Current 1 Week record contains the measured contents of the counter for the ongoing 24-hour interval as well as the elapsed time of the ongoing interval. When the ongoing week interval is completed, the content of this record is transferred to the Historic 1 Week record together with a timestamp to identify it. Then the counter content is reset and a new Current 1 Week record is started.

History 1 Week Record

The History 1 Week record contains the counter contents for the previous 1 Week record, as well as information about the validity of each of these records. A maximum of fifty-two previous 1 week records are stored. The fifty-third 1 week record will overwrite the oldest stored record. Thus, the Historic 1 Week records together represent a 1 year history.

Record Content

Physical Layer

Each record contains the average value of the parameter over the recording interval, the lowest and highest value measured in the interval, and an indication of the validity of the record.

If optical performance monitoring is interrupted by an LOS or other failure in a monitoring period, a value other than -99.0 dBm is displayed and the record is marked as invalid (Valid = no). When the failure persists for an entire record, -99.0 dBm is displayed and the record is marked as invalid.

Data Layer

Each record contains the count of events during the monitoring period.

If the performance monitoring is interrupted by an LOS or other failure in a monitoring period, the record is marked as invalid (Valid = no).

Record Validity

A record is Invalid in the following situations:

- When the recording period is shorter than the record interval. For example, the first record is usually shorter than the interval unless it starts exactly at the interval start time.
- When the administrative state has not been in “In Service” during the whole interval. For example, setting a loopback requires the entity to be in administrative state “Management”.
- When a threshold or measurement period has been changed during the recording interval.

Record Storage

Records are located as follow:

- The 15-minute records are saved in RAM on the NCU. During a controlled shut down of the NE (via the management interface), the records are stored on the CompactFlash (CF) on the NCU. Upon start up of the NE, the 15-minute records stored on the CF are restored to the RAM. If the NE is powered off, or the NCU is extracted, these records cannot be stored on the CompactFlash. The records are lost in this situation, and a gap in the History 15 min record will be seen.

- The 24-hour records are stored in the CF on the NCU.
- The 1-week records are stored on the CF on the NCU.

This means that if there is an uncontrolled shutdown, for example, if you re-seat the NCU, the 15-minute records are lost. The 24-hour and 1-week records, however, are maintained.

Streaming Telemetry

The FSP 3000R7 supports streaming telemetry, as defined by OpenConfig and based on gNMI/gRPC protocols. This feature uses the Subscribe method of gNMI service. The method uses a subscribe request, which is a structured protobuf message. The supported fields of this message are listed in the table that follows.

Table 19: The request supported fields

Request Message Type	Supported Field
SubscribeRequest	subscribe (subscription list)
SubscriptionList	subscription
	mode (STREAM only)
Subscription	path
	mode (ON_CHANGE and SAMPLE)
	sample_interval
	heartbeat_interval

> STREAM:ON_CHANGE subscriptions work only for alarms.

The response to a subscription is a structured message. This feature supports the response fields listed in the table that follows.

Table 20: The response supported fields

Response Message Type	Supported Field
SubscribeResponse	update
Notification	timestamp
	update
Update	path
	val

Errors are indicated using a Status message in the RPC return trailers. This message has this content:

- code - the gRPC error code.
- message - a string that describes the error condition.
- details - a repeated field of protobuf or any messages that carry error details.

License Management

License management for Fiber Service Platform 3000R7 nodes with high density shelves is supported by two solutions.

- Node based (licenses are installed directly on the node)
- License Server based (licenses reside on license server connected to the FSP 3000R7 management network)

Node-Locked

Node-Locked licenses do not use a license server, licenses are distributed directly to nodes in the network. See Node-Locked Licensing presentations located in the ADVA License Management library on the ADVA Customer Portal.

License Server

Licenses are distributed with a software package named Flexnet which is provided by the Flexera company. Flexnet runs on a server connected to the Fiber Service Platform 3000R7 management network and distributes licenses as they are required.

Here are ways to install the License Server software for license management.

- **Installed with ENC:** The License Server software is installed together with the Ensemble Controller (ENC) as part of the installation package.
  - Linux OS: In ENC 10.4 the License Server was installed by default, and starting with ENC 10.5 it is optional
  - Windows OS: Starting with ENC 10.4 the License Server installation is optional

For information about installation of the License Server together with the Ensemble Controller, see the Ensemble Controller Administrator Manual, Installing on a Windows Operating System (from release 10.4) or Installing on a Linux Operating System (from release 10.5). Also see Embedded License Server licensing presentation located in the ADVA License Management library on the ADVA Customer Portal.

- **Standalone Installation:** The License Server is installed as a standalone application with the Embedded License Server installation package. For more information about the Embedded License Server, see Embedded License Server Administrator Manual, located on the documentation portal at https://advadocs.com.

Channel Numbers

This chapter contains the following sections:

C-Band Wavelengths

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19640	1526.44	196.4000		
19635	1526.82	196.3500		
19630	1527.21	196.3000		
19625	1527.60	196.2500		
19620	1527.99	196.2000		
19615	1528.38	196.1500		
19610	1528.77	196.1000		
19608	1528.93	196.0800		
19607	1529.00	196.0700		
19606	1529.08	196.0600		
19605	1529.16	196.0500		
19603	1529.32	196.0300		
19602	1529.39	196.0200		
19601	1529.47	196.0100		
19600	1529.55	196.0000	D01	E01
19598	1529.71	195.9800		
19597	1529.79	195.9700		
19596	1529.86	195.9600		
19595	1529.94	195.9500		
19593	1530.10	195.9300		
19592	1530.18	195.9200		
19591	1530.25	195.9100		
19590	1530.33	195.9000	D02	1
19588	1530.49	195.8800		
19587	1530.57	195.8700		
19586	1530.64	195.8600		
19585	1530.72	195.8500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19583	1530.88	195.8300		
19582	1530.96	195.8200		
19581	1531.04	195.8100		
19580	1531.11	195.8000	D03	E02
19578	1531.27	195.7800		
19577	1531.35	195.7700		
19576	1531.43	195.7600		
19575	1531.50	195.7500		
19573	1531.66	195.7300		
19572	1531.74	195.7200		
19571	1531.82	195.7100		
19570	1531.90	195.7000	D04	2
19568	1532.05	195.6800		
19567	1532.13	195.6700		
19566	1532.21	195.6600		
19565	1532.29	195.6500		
19563	1532.44	195.6300		
19562	1532.52	195.6200		
19561	1532.60	195.6100		
19560	1532.68	195.6000	DC1	E03
19558	1532.84	195.5800		
19557	1532.91	195.5700		
19556	1532.99	195.5600		
19555	1533.07	195.5500		
19553	1533.23	195.5300		
19552	1533.31	195.5200		
19551	1533.38	195.5100		
19550	1533.46	195.5000	D05	3

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19548	1533.62	195.4800		
19547	1533.70	195.4700		
19546	1533.78	195.4600		
19545	1533.86	195.4500		
19543	1534.01	195.4300		
19542	1534.09	195.4200		
19541	1534.17	195.4100		
19540	1534.25	195.4000	D06	E04
19538	1534.40	195.3800		
19537	1534.48	195.3700		
19536	1534.56	195.3600		
19535	1534.64	195.3500		
19533	1534.80	195.3300		
19532	1534.88	195.3200		
19531	1534.95	195.3100		
19530	1535.03	195.3000	D07	4
19528	1535.19	195.2800		
19527	1535.27	195.2700		
19526	1535.35	195.2600		
19525	1535.43	195.2500		
19523	1535.58	195.2300		
19522	1535.66	195.2200		
19521	1535.74	195.2100		
19520	1535.82	195.2000	D08	
19518	1535.98	195.1800		
19517	1536.06	195.1700		
19516	1536.13	195.1600		
19515	1536.21	195.1500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19513	1536.37	195.1300		
19512	1536.45	195.1200		
19511	1536.53	195.1100		
19510	1536.61	195.1000	DC2	
19508	1536.76	195.0800		
19507	1536.84	195.0700		
19506	1536.92	195.0600		
19505	1537.00	195.0500		
19503	1537.16	195.0300		
19502	1537.24	195.0200		
19501	1537.32	195.0100		
19500	1537.39	195.0000	D09	
19498	1537.55	194.9800		
19497	1537.63	194.9700		
19496	1537.71	194.9600		
19495	1537.79	194.9500		
19493	1537.95	194.9300		
19492	1538.03	194.9200		
19491	1538.10	194.9100		
19490	1538.18	194.9000	D10	5
19488	1538.34	194.8800		
19487	1538.42	194.8700		
19486	1538.50	194.8600		
19485	1538.58	194.8500		
19483	1538.74	194.8300		
19482	1538.82	194.8200		
19481	1538.89	194.8100		
19480	1538.97	194.8000	D11	E05

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19478	1539.13	194.7800		
19477	1539.21	194.7700		
19476	1539.29	194.7600		
19475	1539.37	194.7500		
19473	1539.53	194.7300		
19472	1539.61	194.7200		
19471	1539.68	194.7100		
19470	1539.76	194.7000	D12	6
19468	1539.92	194.6800		
19467	1540.00	194.6700		
19466	1540.08	194.6600		
19465	1540.16	194.6500		
19463	1540.32	194.6300		
19462	1540.40	194.6200		
19461	1540.48	194.6100		
19460	1540.55	194.6000	DC3	E06
19458	1540.71	194.5800		
19457	1540.79	194.5700		
19456	1540.87	194.5600		
19455	1540.95	194.5500		
19453	1541.11	194.5300		
19452	1541.19	194.5200		
19451	1541.27	194.5100		
19450	1541.35	194.5000	D13	7
19448	1541.51	194.4800		
19447	1541.58	194.4700		
19446	1541.66	194.4600		
19445	1541.74	194.4500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19443	1541.90	194.4300		
19442	1541.98	194.4200		
19441	1542.06	194.4100		
19440	1542.14	194.4000	D14	E07
19438	1542.30	194.3800		
19437	1542.38	194.3700		
19436	1542.46	194.3600		
19435	1542.54	194.3500		
19433	1542.70	194.3300		
19432	1542.77	194.3200		
19431	1542.85	194.3100		
19430	1542.93	194.3000	D15	8
19428	1543.09	194.2800		
19427	1543.17	194.2700		
19426	1543.25	194.2600		
19425	1543.33	194.2500		
19423	1543.49	194.2300		
19422	1543.57	194.2200		
19421	1543.65	194.2100		
19420	1543.73	194.2000	D16	E08
19418	1543.89	194.1800		
19417	1543.97	194.1700		
19416	1544.05	194.1600		
19415	1544.13	194.1500		
19413	1544.28	194.1300		
19412	1544.36	194.1200		
19411	1544.44	194.1100		
19410	1544.52	194.1000	DC4	

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19408	1544.68	194.0800		
19407	1544.76	194.0700		
19406	1544.84	194.0600		
19405	1544.92	194.0500		
19403	1545.08	194.0300		
19402	1545.16	194.0200		
19401	1545.24	194.0100		
19400	1545.32	194.0000	DC9	
19398	1545.48	193.9800		
19397	1545.56	193.9700		
19396	1545.64	193.9600		
19395	1545.72	193.9500		
19393	1545.88	193.9300		
19392	1545.96	193.9200		
19391	1546.04	193.9100		
19390	1546.12	193.9000	DC5	
19388	1546.28	193.8800		
19387	1546.36	193.8700		
19386	1546.44	193.8600		
19385	1546.52	193.8500		
19383	1546.67	193.8300		
19382	1546.75	193.8200		
19381	1546.83	193.8100		
19380	1546.91	193.8000	D17	E09
19378	1547.07	193.7800		
19377	1547.15	193.7700		
19376	1547.23	193.7600		
19375	1547.31	193.7500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19373	1547.47	193.7300		
19372	1547.55	193.7200		
19371	1547.63	193.7100		
19370	1547.71	193.7000	D18	9
19368	1547.87	193.6800		
19367	1547.95	193.6700		
19366	1548.03	193.6600		
19365	1548.11	193.6500		
19363	1548.27	193.6300		
19362	1548.35	193.6200		
19361	1548.43	193.6100		
19360	1548.51	193.6000	D19	E10
19358	1548.67	193.5800		
19357	1548.75	193.5700		
19356	1548.83	193.5600		
19355	1548.91	193.5500		
19353	1549.07	193.5300		
19352	1549.15	193.5200		
19351	1549.23	193.5100		
19350	1549.31	193.5000	D20	10
19348	1549.47	193.4800		
19347	1549.55	193.4700		
19346	1549.63	193.4600		
19345	1549.71	193.4500		
19343	1549.87	193.4300		
19342	1549.95	193.4200		
19341	1550.03	193.4100		
19340	1550.11	193.4000	DC6	E11

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19338	1550.27	193.3800		
19337	1550.35	193.3700		
19336	1550.43	193.3600		
19335	1550.51	193.3500		
19333	1550.68	193.3300		
19332	1550.76	193.3200		
19331	1550.84	193.3100		
19330	1550.92	193.3000	D21	11
19328	1551.08	193.2800		
19327	1551.16	193.2700		
19326	1551.24	193.2600		
19323	1551.48	193.2300		
19322	1551.56	193.2200		
19321	1551.64	193.2100		
19325	1551.32	193.2500		
19320	1551.72	193.2000	D22	E12
19318	1551.88	193.1800		
19317	1551.96	193.1700		
19316	1552.04	193.1600		
19315	1552.12	193.1500		
19313	1552.28	193.1300		
19312	1552.36	193.1200		
19311	1552.44	193.1100		
19310	1552.52	193.1000	D23	12
19308	1552.68	193.0800		
19307	1552.76	193.0700		
19306	1552.84	193.0600		
19305	1552.92	193.0500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19303	1553.09	193.0300		
19302	1553.17	193.0200		
19301	1553.25	193.0100		
19300	1553.33	193.0000	D24	
19298	1553.49	192.9800		
19297	1553.57	192.9700		
19296	1553.65	192.9600		
19295	1553.73	192.9500		
19293	1553.89	192.9300		
19292	1553.97	192.9200		
19291	1554.05	192.9100		
19290	1554.13	192.9000	DC7	
19288	1554.29	192.8800		
19287	1554.37	192.8700		
19286	1554.45	192.8600		
19285	1554.53	192.8500		
19283	1554.70	192.8300		
19282	1554.78	192.8200		
19281	1554.86	192.8100		
19280	1554.94	192.8000	D25	
19278	1555.10	192.7800		
19277	1555.18	192.7700		
19276	1555.26	192.7600		
19275	1555.34	192.7500		
19273	1555.50	192.7300		
19272	1555.58	192.7200		
19271	1555.66	192.7100		
19270	1555.74	192.7000	D26	13

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19268	1555.91	192.6800		
19267	1555.99	192.6700		
19266	1556.07	192.6600		
19265	1556.15	192.6500		
19263	1556.31	192.6300		
19262	1556.39	192.6200		
19261	1556.47	192.6100		
19260	1556.55	192.6000	D27	E13
19258	1556.71	192.5800		
19257	1556.79	192.5700		
19256	1556.88	192.5600		
19255	1556.96	192.5500		
19253	1557.12	192.5300		
19252	1557.20	192.5200		
19251	1557.28	192.5100		
19250	1557.36	192.5000	D28	14
19248	1557.52	192.4800		
19247	1557.60	192.4700		
19246	1557.68	192.4600		
19245	1557.77	192.4500		
19243	1557.93	192.4300		
19242	1558.01	192.4200		
19241	1558.09	192.4100		
19240	1558.17	192.4000	DC8	
19238	1558.33	192.3800		
19237	1558.41	192.3700		
19236	1558.49	192.3600		
19235	1558.58	192.3500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19233	1558.74	192.3300		
19232	1558.82	192.3200		
19231	1558.90	192.3100		
19230	1558.98	192.3000	D29	15
19228	1559.14	192.2800		
19227	1559.22	192.2700		
19226	1559.31	192.2600		
19225	1559.39	192.2500		
19223	1559.55	192.2300		
19222	1559.63	192.2200		
19221	1559.71	192.2100		
19220	1559.79	192.2000	D30	E15
19218	1559.95	192.1800		
19217	1560.04	192.1700		
19216	1560.12	192.1600		
19215	1560.20	192.1500		
19213	1560.36	192.1300		
19212	1560.44	192.1200		
19211	1560.52	192.1100		
19210	1560.60	192.1000	D31	16
19208	1560.77	192.0800		
19207	1560.85	192.0700		
19206	1560.93	192.0600		
19205	1561.01	192.0500		
19203	1561.17	192.0300		
19202	1561.25	192.0200		
19201	1561.34	192.0100		
19200	1561.42	192.0000	D32	E16

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19198	1561.58	191.9800		
19197	1561.66	191.9700		
19196	1561.74	191.9600		
19195	1561.82	191.9500		
19193	1561.99	191.9300		
19192	1562.07	191.9200		
19191	1562.15	191.9100		
19190	1562.23	191.9000		
19188	1562.39	191.8800		
19187	1562.47	191.8700		
19186	1562.56	191.8600		
19185	1562.64	191.8500		
19183	1562.80	191.8300		
19182	1562.88	191.8200		
19181	1562.96	191.8100		
19180	1563.04	191.8000		
19178	1563.21	191.7800		
19177	1563.29	191.7700		
19176	1563.37	191.7600		
19175	1563.45	191.7500		
19173	1563.62	191.7300		
19172	1563.70	191.7200		
19171	1563.78	191.7100		
19170	1563.86	191.7000		
19168	1564.02	191.6800		
19167	1564.10	191.6700		
19166	1564.19	191.6600		
19165	1564.27	191.6500		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19163	1564.43	191.6300		
19162	1564.51	191.6200		
19161	1564.59	191.6100		
19160	1564.68	191.6000		
19158	1564.84	191.5800		
19157	1564.92	191.5700		
19156	1565.00	191.5600		
19155	1565.08	191.5500		
19153	1565.25	191.5300		
19152	1565.33	191.5200		
19151	1565.41	191.5100		
19150	1565.49	191.5000		
19148	1565.66	191.4800		
19147	1565.74	191.4700		
19146	1565.82	191.4600		
19145	1565.90	191.4500		
19143	1566.07	191.4300		
19142	1566.15	191.4200		
19141	1566.23	191.4100		
19140	1566.31	191.4000		
19138	1566.48	191.3800		
19137	1566.56	191.3700		
19136	1566.64	191.3600		
19135	1566.72	191.3500		
19133	1566.88	191.3300		
19132	1566.97	191.3200		
19131	1567.05	191.3100		
19130	1567.13	191.3000		

Channel	Wavelength [nm]	Frequency [THz]	"D" Channel	"E" Channel
19128	1567.29	191.2800		
19127	1567.38	191.2700		
19126	1567.46	191.2600		
19125	1567.54	191.2500		
19123	1567.70	191.2300		
19122	1567.79	191.2200		
19121	1567.87	191.2100		
19120	1567.95	191.2000		

L-Band Wavelengths

Channel	Wavelength [nm]	Frequency [THz}	"D" Channel	"E" Channel
19100	1569.59	191.0000	D33	E17
19090	1570.41	190.9000	D34	17
19080	1571.24	190.8000	D35	E18
19070	1572.06	190.7000	D36	18
19060	1572.89	190.6000	DL1	E19
19050	1573.71	190.5000	D37	19
19040	1574.54	190.4000	D38	E20
19030	1575.37	190.3000	D39	20
19020	1576.19	190.2000	D40	
19010	1577.02	190.1000	DL2	
19000	1577.85	190.0000	D41	
18990	1578.68	189.9000	D42	21
18980	1579.52	189.8000	D43	E21
18970	1580.35	189.7000	D44	22
18960	1581.18	189.6000	DL3	E22
18950	1582.02	189.5000	D45	23

Channel	Wavelength [nm]	Frequency [THz}	"D" Channel	"E" Channel
18940	1582.85	189.4000	D46	E23
18930	1583.69	189.3000	D47	24
18920	1584.52	189.2000	D48	E24
18910	1585.36	189.1000	DL4	
18900	1586.20	189.0000	DL9	
18890	1587.04	188.9000	DL5	
18880	1587.88	188.8000	D49	E25
18870	1588.72	188.7000	D50	25
18860	1589.57	188.6000	D51	E26
18850	1590.41	188.5000	D52	26
18840	1591.25	188.4000	DL6	E27
18830	1592.10	188.3000	D53	27
18820	1592.94	188.2000	D54	E28
18810	1593.79	188.1000	D55	28
18800	1594.64	188.0000	D56	
18790	1595.49	187.9000	DL7	
18780	1596.34	187.8000	D57	
18770	1597.19	187.7000	D58	29
18760	1598.04	187.6000	D59	E29
18750	1598.89	187.5000	D60	30
18740	1599.74	187.4000	DL8	E30
18730	1600.60	187.3000	D61	31
18720	1601.45	187.2000	D62	E31
18710	1602.31	187.1000	D63	32
18700	1603.17	187.0000	D64	E32

CWDM Wavelengths

Channel	Wavelength [nm]	Frequency [THz]
C1270	1270	236.00
C1290	1290	232.50
C1310	1310	229.00
C1330	1331	225.50
C1350	1351	222.00
C1370	1371	218.50
C1430	1431	209.50
C1450	1451	206.50
C1470	1471	203.50
C1490	1491	201.00
C1510	1511	198.50
C1530	1531	196.00
C1550	1551	193.50
C1570	1571	190.85
C1590	1591	188.50
C1610	1611	186.09

Protocols and Rates

Some modules have full protocol support, while others carry protocols transparently. Facility types under Protocol-Full Support, support protocol performance monitoring, indicators and overhead. Facility types under Protocol-Transport Only support transparent transmission of protocols at the specified rate.

Table 21: Protocols and Rates

Protocol-Full Support	Protocol-Transport Only	Rate	Comments
Ethernet 1G	Ethernet 1G (F1250)	1.250 Gbps	1 GbE

Table 21: Protocols and Rates (continued)

Protocol-Full Support	Protocol-Transport Only	Rate	Comments
Ethernet 10G WAN	STM-64/OC-192 (F9953)	9.953 Gbps	
Ethernet 10G LAN	Ethernet 10 LAN (F10312)	10.3125 Gbps	10 GbE
Ethernet 25G LAN	Ethernet 25G LAN (F25781)	25.781 Gbps	line rate
Ethernet 25G LAN	Ethernet 25G LAN (F25800)	25.781 Gbps	fixed rate, supports transport of Ethernet 25G LAN
Ethernet 40G	Ethernet 40G (F41250)	41.25 Gbps (4x 10.3125 Gbps)	40 GbE
Ethernet 100G	Ethernet 100G (F103125)	103.125 Gbps (10x 10.3125 Gbps)	100 GbE
Ethernet 400G		425 Gbps	
Fast Ethernet	FE/MADI (F125)	125 Mbps	
Fibre Channel 1G	Fibre Channel 1G (F1062)	1.0625 Gbps	
Fibre Channel 2G	Fibre Channel 2G (F2125)	2.125 Gbps	
Fibre Channel 4G	Fibre Channel 4G (F4250)	4.25 Gbps	
Fibre Channel 8G	Fibre Channel 8G (F8500)	8.5 Gbps	
Fibre Channel 10G	Fibre Chan 10G (F10518)	10.51875 Gbps	
Fibre Channel 16G	Fibre Chan 16G (F14025)	14.025 Gbps	
Fibre Channel 32G	Fibre Chan 32G (F28050)	28.05 Gbps	

Table 21: Protocols and Rates (continued)

Protocol-Full Support	Protocol-Transport Only	Rate	Comments
Fibre Channel 128G	Fibre Chan128G (F112200)	112.200 Gbps	
Infini Band 2.5G	InfiniBand 2G5 (F2500)	2.5 Gbps	
InfiniBand 5G	InfiniBand 5G (F5000)	5.0 Gbps	
InfiniBand 10G	InfiniBand 10G (F10000)	10.0 Gbps	
OC-3	STM-1/OC-3 (F155)	155.52 Mbps	STM-1/OC-3 (F155) also supports transport of ATM 155 Mbps
OC-12	STM-4/OC-12 (F622)	622.08 Mbps	STM-4/OC-12 (F622) also supports transport of ATM 622 Mbps
OC-48	STM-16/OC-48 (F2488)	2.488 Gbps	
OC-192	STM-64/OC-192 (F9953)	9.953 Gbps	
OC-768	STM-256/OC-768 (F39813)	39.813 Gbps	
STM-1	STM-1/OC-3 (F155)	155.52 Mbps	
STM-4	STM-4/OC-12 (F622)	622.08 Mbps	
STM-16	STM-16/OC-48 (F2488)	2.488 Gbps	
STM-64	STM-64/OC-192 (F9953)	9.953 Gbps	
STM-256	STM-256/OC-768 (F39813)	39.813 Gbps	
OTU1	OTU1 (F2666)	2.666 Gbps	
OTU1e	OTU1e (F11049)	11.0491 Gbps	OTU2 carrying 10 GbE LAN without stuffing

Table 21: Protocols and Rates (continued)

Protocol-Full Support	Protocol-Transport Only	Rate	Comments
OTU2	OTU2 (F10709)	10.7092 Gbps	
OTU2e	OTU2e (F11095)	11.0957 Gbps	OTU2 carrying 10 GbE LAN with stuffing
OTU2f	OTU2f (F11318)	11.3176 Gbps	OTU2 carrying 10G Fibre Channel with stuffing
	OTU2fc (F8500)	10.9750 Gbps	Proprietary OTU2 carrying 8G Fibre Channel
	OTU2p (F10664)	10.6642 Gbps	Proprietary OTU2 carrying STM-64 or OC-192 without stuffing
	OTU2v IB (F10759)	10.7595 Gbps	Proprietary OTU2 carrying 10G InfiniBand
	OTU2v FC (F10974)	10.9747 Gbps	Proprietary OTU2 carrying 8G Fibre Channel
OTU3		43.01841 Gbps	
OTU4		111.8 Gbps	
OTU (200 Gbps)			Proprietary OTU format carrying 2 ODU4
OTU (300 Gbps)			Proprietary OTU format carrying 3 ODU4
OTU (400 Gbps)			Proprietary OTU format carrying 4 ODU4
OTU (500 Gbps)			Proprietary OTU format carrying 5 ODU4
OTU (600 Gbps)			Proprietary OTU format carrying 6 ODU4
	ESCON (F200)	200 Mbps	
	2xCPRI (F1228)	1.2288 Gbps	
	4xCPRI (F2457)	2.4576 Gbps	

Table 21: Protocols and Rates (continued)

Protocol-Full Support	Protocol-Transport Only	Rate	Comments
	5xCPRI/4xOBSAI (F3072)	3.072 Gbps	
	8xCPRI (F4915)	4.9152 Gbps	
	10xCPRI8xOBSAI (F6144)	6.144 Gbps	
	16xCPRI (F9830)	9.8304 Gbps	
	20xCPRI (F10137)	10.1376 Gbps	
	3G-SDI/1 (F2967)	2.967 Gbps	
	ED-SDI (F540)	540 Mbps	SMPTE 344M
	HD-SDI/1 (F1483)	1.4835 Gbps	
	HD-SDI (F1485)	1.485 Gbps	SMPTE 292
	3G-SDI (F2970)	2.970 Gbps	HD-SDI Dual Link
	SD-SDI A (F143)	143.2 Mbps	SMPTE 259M-A
	SD-SDI B (F177)	177.3 Mbps	SMPTE 259M-B
	SD-SDI C (F270)	270 Mbps	SMPTE 259M-C/ DVB-ASI
	SD-SDI D (F360)	360 Mbps	SMPTE 259M-D
	Video-10G (F10754)	10.754 Gbps	
	Video-166M (F166)	166 Mbps	
	Video-666M (F666)	666 Mbps	

Module and Plug Compatibility

See the *FSP 3000R7 Compatibility Matrix* to determine module and pluggable transceiver compatibility.

Use Cases

This section contains these topics:

Securing the Node

In the **Node** application, complete these tasks:

Disable Telnet

1. Select **Security** > **Access**.
2. In the **Access Management** area, **Telnet Interface** field, select **Disable**.
3. Click **Apply**.

Disable SNMP

1. Select **General** > **Controls**.
2. In the **Interfaces** area, **SNMPv1 and v2c** field, select **Disable**. In the **SNMPv3** field, select **Enable**.
3. Click **Apply**.

Disable TL1

1. Select **General** > **Controls**.
2. In the **Interfaces** area, set **TL1 Interface** to **Disable**.
3. Click **Apply**.

Disable FTP

1. Select **Security** > **Access**.
2. In the **Access Management** area, **FTP Client** and **FTP Server** fields, select **Disable**.
3. Click **Apply**.

Disable TLS v1.0 and TLS v1.1

1. Select **Security Applications** > **SSL/TLS**.
2. In the **Transport Layer Security (TLS) Authentication** area, **TLS Versions** field, select **1.2** and **1.3**.
3. Click **Apply**.

Configure TLS Ciphers Profile

1. Select **Security Applications** > **SSL/TLS**.
2. In the **TLS Ciphers** area, set the **TLS Ciphers Profile** to **Default** or **CSfC**.
3. Click **Apply**.

Configure SSH Ciphers Profile

1. Select **Security Applications** > **SSH**.
2. In the **SSH Ciphers** area, set the **SSH Ciphers Profile** to **Default** or **CSfC**.
3. Click **Apply**.

Enable SSH

1. Select **Security** > **Access**.
2. In the **Access Management** area, **SSH Interface** field, select **Enabled**.
3. Click **Apply**.

You cannot set SSH to disable if the Node > General > Controls TL1 Interface is set to encrypted mode.

Enable Security Enhanced Mode and Change ADMIN Password

1. Select **Security** > **Access**.
2. In the **Password Management** area, **Security Mode** field, select **Enhanced**.
3. Click **Apply**.
4. In the **Security Mode** window, click **Apply**. The system logs out the user.
5. Log back in to the Node.
6. Enter the current password
7. In the **Password Change** window, **New Password** field, enter the new password. The system logs out the user.
8. Log back in to the Node, and change the password to one that meets this criteria:
   - Contains at least two lowercase alphabetic characters.
   - Contains at least two uppercase alphabetic characters.
   - Contains at least two numeric characters.
   - Contains at least two of these special characters:
     ! , @ , # , $, % , ^ , (,) , _ , + , | , ~ , { , } , [,] , - , .
   - Is a minimum of 15 characters long.

Enable Security Banner

1. Select **Security** > **Access**.
2. In the **Warning Message** area, **Access Warning Message** field, enter the warning message.
3. Set **Access Warning** to **Enable**.
4. Click **Apply**.

> Exemplary Access Warning Message:
>
> WARNING TO UNAUTHORIZED USERS: This system is for authorized users only. Disconnect immediately if you are not an authorized user!

Configure SysLog

1. Select **General** > **Controls**.
1. In the **Remote Event Recipients (SysLog)** area, click the add icon.
2. In the **Add Remote Event Recipients (SysLog)** window, **IPv4/v6 Address** field, enter the applicable IP address.

3. (optional) Select categories of events that the system sends to system log:
   - Alarms
   - Database Changes
   - Security Events
4. Click **Add**.

	To add a port user label to SysLog information, in the **Remote Event Recipients** area, **Message Extension** field, select **Add User Label**.

Regenerate the SSH Certificate

1. Select **Security Applications** > **SSH**.
2. In the **Host Keys** area, select the relevant key.
3. Click **Activate Key**.
4. In the **Generate and Activate SSH Host Key** window, complete the relevant fields.
5. Click **Generate and Activate**.

Disable NTP

1. Select **General** > **Date & Time**.
2. In the **Date & Time** area, **NTP Operation** field, select **Disable**.

Disable Boot Loader Access

1. Select **Security** > **Access**.
2. In the **Access Management** area, **NCU Boot loader Access** field, select **Disable**.
3. Click **Apply**.

Hide Login Presentation

1. Select **Security** > **Access**.
2. In the **Access Management** area, **Login Presentation** field, select **Prompt**.
3. Click **Apply**.

Disable NCU Serial Port

1. Select **Configure** > **Node** > **Shelf 1**.
2. Select **Slot A NCU-II**.
3. In the **Serial Port** area, click the relevant port.
4. In the **Configure Details** window, **Admin State** field, select **Disable**.
5. Click **Apply & Exit**.

> Network Element Director supports HTTP Strict Transport Security (HSTS). This feature is enabled by default. You cannot disabled this setting.

Disable NETCONF

1. Select **Node** > **Controls**.
2. In the **NETCONF Interface** area, select **Disable**.
3. Click **Apply**.

Enable PKI certificate using a trusted CA

1. Select **Node** > **Security** > **Certificate Authorities (CA)**.
2. In the **Certificate Authorities (CA)** area, click the add icon.
3. In the **Certificate Authorities** window:
   a. Select a **Identifier**.
   b. In the **SCEP Configuration** area, enter **SCEP URL**.
   c. In the **SCEP Advanced Configuration** area, complete the relevant fields.
4. Click **Add**.

> Some servers require NTLM authentication. In that case, in the **SCEP Authentication** area, enter **Domain**, **User Name** and **Password** then click **Apply**.

5. In the **Certificate Authorities (CA)** area, select the PKI server identifier.
6. In the **Configure Details** window:
   a. In the **CA Authentication** area, click **Update**.
   b. Click **Apply and Exit**.
7. Select **Node** > **Security** > **Certificates & Keys**.

8. In the **Certificates** area:
    a. Select the PKI identifier.
    b. In the **Configure Details** window, in the **Certificate Configuration** area, set **Trust Settings** to **Trusted**.
9. In the **Keys** area, click the add icon.
    a. In the **Cryptographic Keys** window:
        a. Select the **Identifier**.
        b. In the **Cryptographic Key Configuration** area, **Key Algorithm** field, select one of these:
            - **RSA**
            - **ECDSA**

            Keep in mind that SCEP supports only RSA-based cryptography.
        c. In the **Key And Certificate Renewal** area, select the **Certificate Authority**.
        d. In the **Certificate Request Configuration** area, complete relevant fields.
        e. Click **Add**.
10. In the **Certificates** area, select the **Identifier**.
11. In the **Configure Details** window,
    a. In the **Certificate Activation** area, click **Activate**.
    b. Click **Apply & Exit**.

4WCC-PCN-10G

The 4WCC-PCN-10G is a quad 10G core channel module with four SFP+ type pluggable client interfaces and four SFP+ type pluggable network interfaces. It provides four fully functional 10 Gbps transponders.

FEC must be set for all network ports at time of 4WCC-PCN-10G configuration. If its changed after a service is configured, it will impact the existing services

16TCC-PCN-4GUS+10G

The 16TCC-PCN-4GUS+10G module transports up to 16 client signals over two 10 Gbps channels. This section contains these topics:

Background Information

The 16TCC-PCN-4GUS+10G module transports up to 16 client signals from 125 Mbps to 4.25 Gbps over two 10 Gbps network channels. This section describes how to use 16TCC-PCN-4GUS+10G modules for the following applications:

- Dual Muxponder
  In this application multiple client port signals are multiplexed to one of the network ports. A client port signal may be connected to either network port provided bandwidth is available.
- Add-Drop Multiplexer (ADM)
  In this application, multiple client port signals are multiplexed to one of the network ports but signals can also be passed between network ports. This application allows an OTU2 ring to be established which overlays the optical network. Each 16TCC-PCN-4GUS+10G network port is connected to another 16TCC-PCN-4GUS+10G network port at a different site. Client signals may be added and dropped or passed through at each 16TCC-PCN-4GUS+10G. Pass-through channels may limit the number of client signals that can be added and dropped.

Refer to the Examples.

Back to 16TCC-PCN-4GUS+10G.

Requirements

- Common equipment is installed, configured and operational.
- The 16TCC-PCN-4GUS+10G module and required plugs are installed, supports up to 16 client ports which use SFP plugs and 2 network ports which use SFP+ plugs.
- Fiber (cable) plan with physical connections for modules.
- Fibers are connected as specified in the fiber plan.

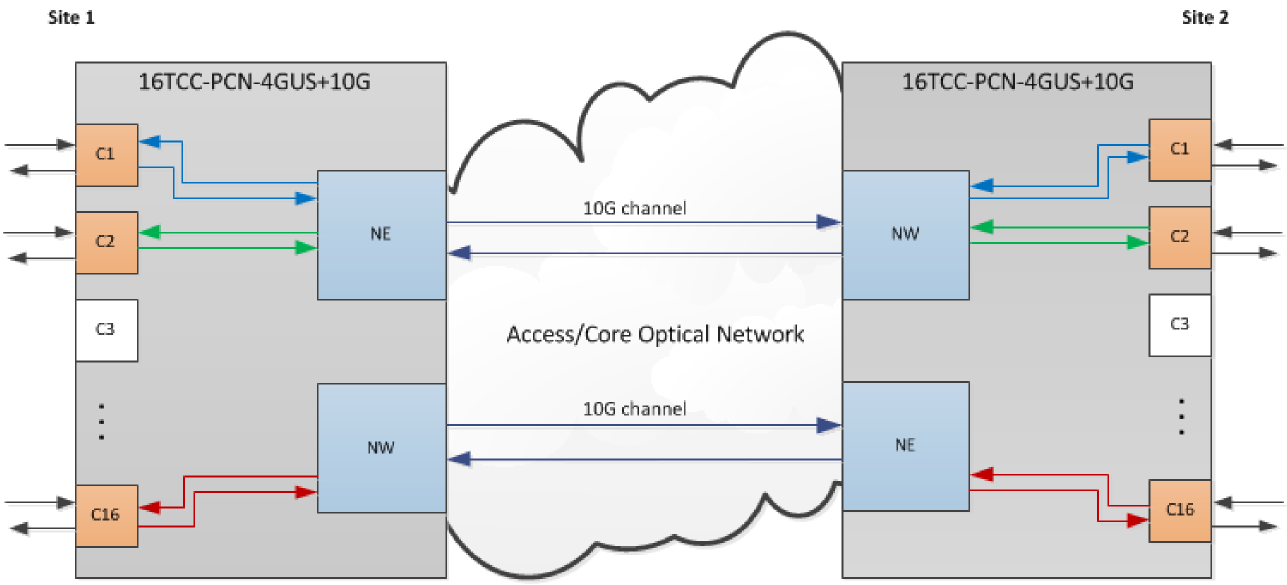
Back to 16TCC-PCN-4GUS+10G.

Provisioning the 16TCC-PCN-4GUS+10G

The 16TCC-PCN-4GUS+10G modules operate as dual muxponders or add-drop multiplexers as shown in Examples.

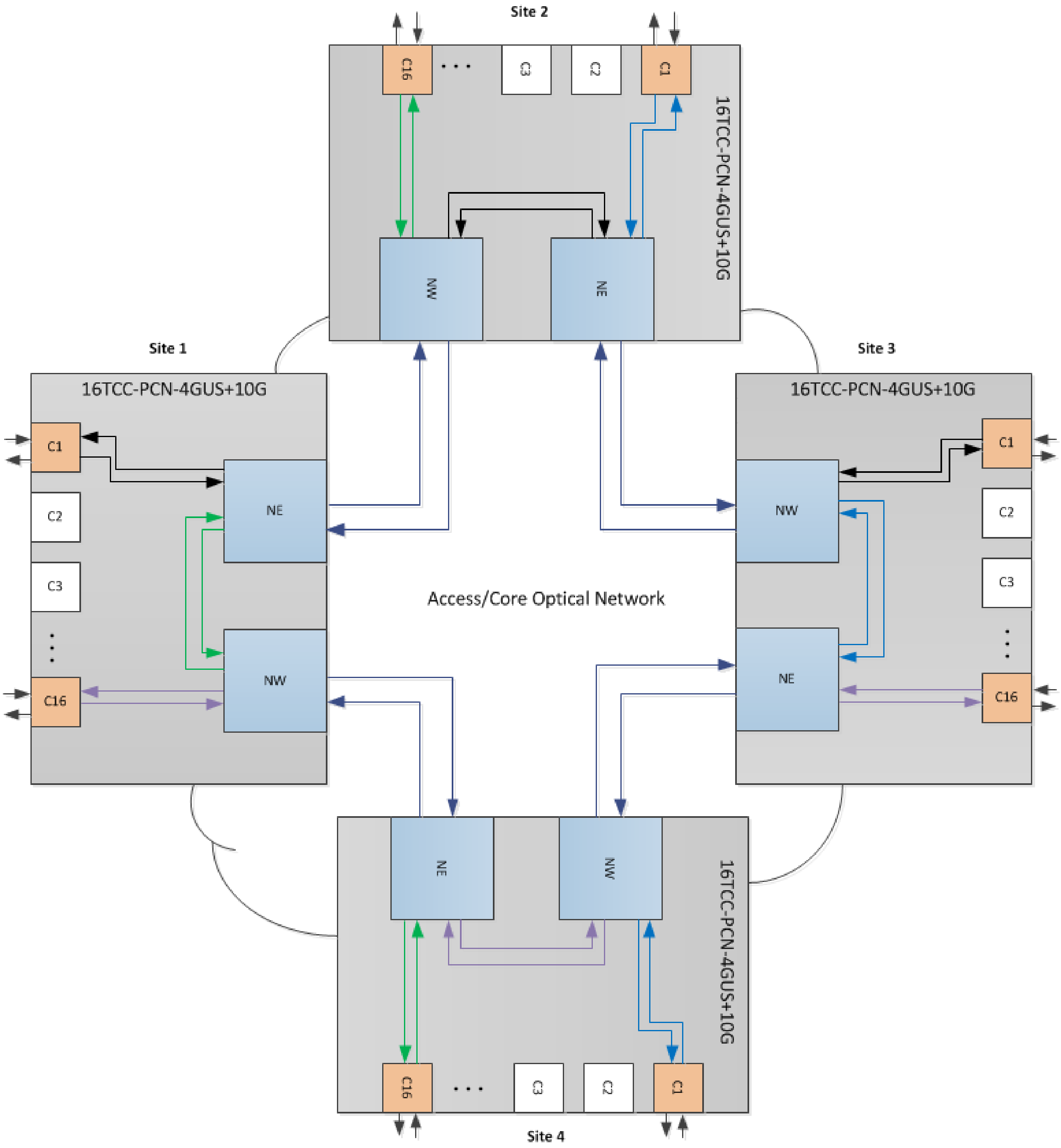
When the 16TCC-PCN-4GUS+10G is used as a dual muxponder service provisioning is only required at the add and drop sites.

Figure 51: Dual Muxponder



When the 16TCC-PCN-4GUS+10G is used as part of an OTU2 add-drop multiplexer ring, service provisioning must be performed at each site supporting the service (add, drop or pass-through).

Figure 52: OTU2 Ring



Add the module

1. Select **Configure**.
2. Select the relevant shelf from the **Navigation Tree**.
3. In the **Main Pane** of the shelf, click **Add Module**.
4. From the list, select the correct slot and equipment type.
5. Refer to your network plan to enter the required information.

   The module is listed in the **Navigation Tree**.

Add plugs to support the client and network ports

1. Select **Configure**.
2. Navigate to the relevant shelf in the **Navigation Tree**.
3. Click the slot that you want to configure.
4. In the **Main Pane**, click the **Plugs** area.
5. Click **Add** to open the Add Plug window.
6. From the list, select the correct plug and equipment type.
7. Refer to your network plan to enter the required information.
8. Click **Add**.

   The plug is listed in the **Plugs** area.

Add Physical Connections

1. Select **Overview**.
2. Select **Physical Connections**.
3. Click the **Filter** area.
4. Select your preferences for the search filter and click **Update**.
   Allow time for the query to execute. The in-progress icon indicates that the software is retrieving information from the equipment.
5. Select the relevant identifier, and click the item to open the Physical Connection - Create window.
6. Refer to your network plan to enter the required information.
7. After setting up the options, click **Apply & Exit**.

Add Port to support services

1. Select **Configure**.
2. Navigate to the relevant shelf in the **Navigation Tree**.
3. Click the slot that you want to configure.
4. In the **Main Pane**, click the **Ports** area.
5. Click **Add** to open the Add Facility window.
6. From the list, select the correct **Identifier**.
7. Refer to your network plan to enter the required information.
8. Click **Add**.

   The port is listed in **Ports** area.

Add Endpoints for service as required

1. Select **Configure**.
2. Navigate to the relevant shelf in the **Navigation Tree**.
3. Click the slot that you want to provision.
4. In the **Main Pane**, click the **Data Channels** area.
5. Click **Add End Point** to open the Add Facility window.
6. From the list, select the correct port and channel.
7. Refer to your network plan to enter the required information.
8. Click **Add**.

   The data channel is listed in the **Data Channels** area.

Add Connections

1. Select **Configure**.
2. Navigate to the relevant shelf in the **Navigation Tree**.
3. Click the slot corresponding to the 16TCC-PCN-4GUS+10G module.
4. In the **Main Pane**, click the **Data Channels** area.
5. Click **Add Connection**.
6. Set the direction.
   In a Dual Muxponder application, the direction should always be Add-Drop.
   In an ADM application, the direction may be Pass-Through or Add-Drop.
7. Select the source and destination endpoints for the connection.
8. Click **Add**.

   The service path is listed in the **Data Channels** area.

Back to 16TCC-PCN-4GUS+10G.

Aggregating Traffic Using a 4TCA-PCN-4GU (S)+4G Module

Traffic may be aggregated into a 16TCC-PCN-4GUS+10G from a 4TCA-PCN-4GU(S)+4G.

1. Install 16TCC-PCN-4GUS+10G and 4TCA-PCN-4GU(S)+4G modules.
2. Install matching 4GU plugs on the 16TCC-PCN-4GUS+10G client port and the 4TCA-PCN-4GU(S)+4G network port to be connected.
3. Connect a fiber between the 16TCC-PCN-4GUS+10G client port Tx and the 4TCA-PCN-4GU(S)+4G network port Rx.
4. Connect a fiber between the 16TCC-PCN-4GUS+10G client port Rx and the 4TCA-PCN-4GU(S)+4G network port Tx.

5. Add physical connections as described in Adding Physical Connections
6. Provision the 16TCC-PCN-4GUS+10G as described in Provisioning the 16TCC-PCN-4GUS+10G with the client port **Facility** set to **Fixed Clock 4.250 Gbps**.
7. Add the 4TCA-PCN-4GU(S)+4G module as described in Adding Modules
8. Add the 4TCA-PCN-4GU(S)+4G plugs, select the **Plugs** area, right-click on each plug, and then select **Add**.
9. Add the 4TCA-PCN-4GU(S)+4G network port. The **Facility** is **Fixed Clock 4.250 Gbps**.
10. Add the 4TCA-PCN-4GU(S)+4G client ports to support the desired client facilities.

Examples

16TCC-PCN-4GUS+10G modules may be deployed in multiple configurations. The most common are dual muxponder or add-drop multiplexer (ADM) supporting an OTU2 ring.

Figure 53: Dual Muxponder

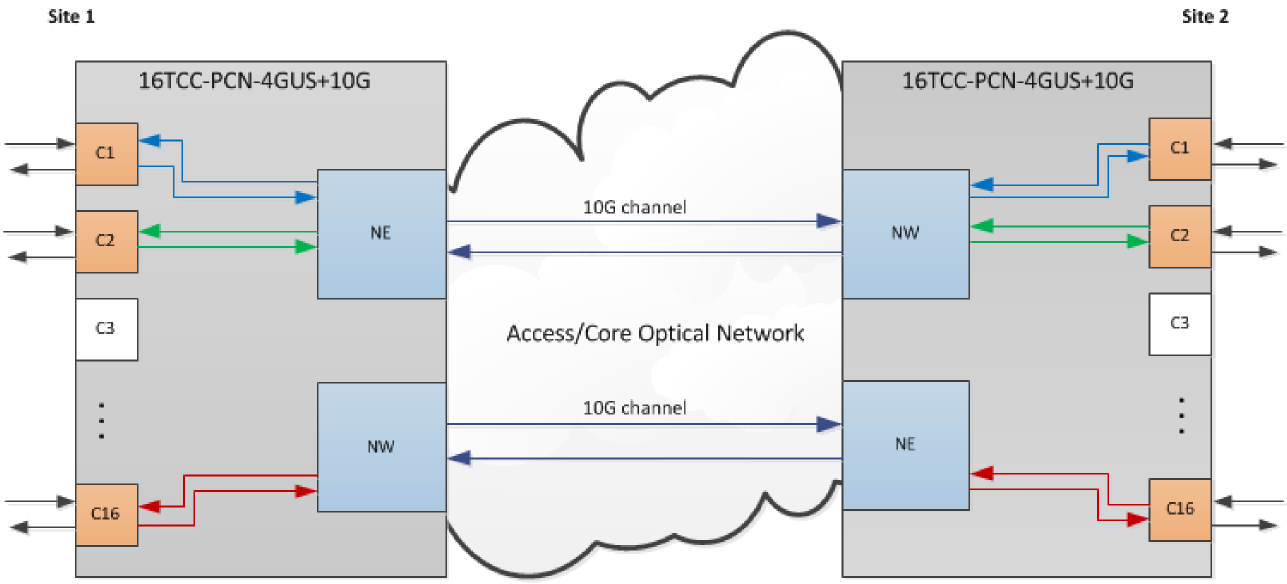
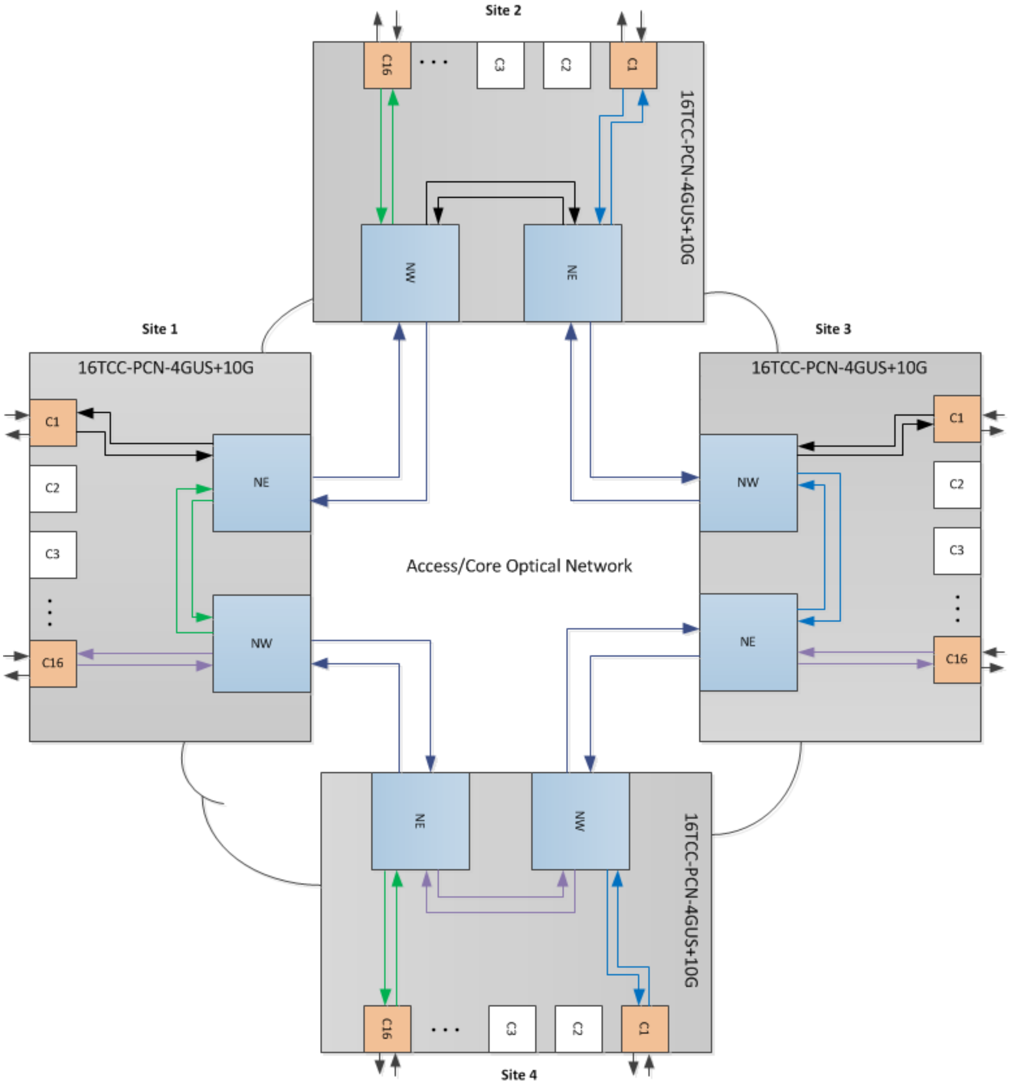


Figure 54: OTU2 Ring



Back to 16TCC-PCN-4GUS+10G.

9ROADM-RS

The 9ROADM-RS is based on the route-and-select, reconfigurable optical add-drop multiplexer (ROADM) architecture. This architecture incorporates a 1 x 9 wavelength selective switching (WSS) component. The product uses this component after the network-port input that routes each network-port service or wavelength receives a signal to any of the 9 client-port output signals. One or more of the client- port output signals can connect to an add-drop structure that directs the individual drop services to channel cards, or to external channels. One or more of the client-port output signals can connect to client ports on other 9ROADM-RS modules to pass services through to another degree.

This architecture also incorporates a 9 x 1 WSS component after the 9 client-port inputs. This component selects between pass-through services and add-services from each of the 9 client-port inputs. It can also multiplex the selected services on the network-port output signal and equalize all channels at the network-port output.

This section contains these topics:

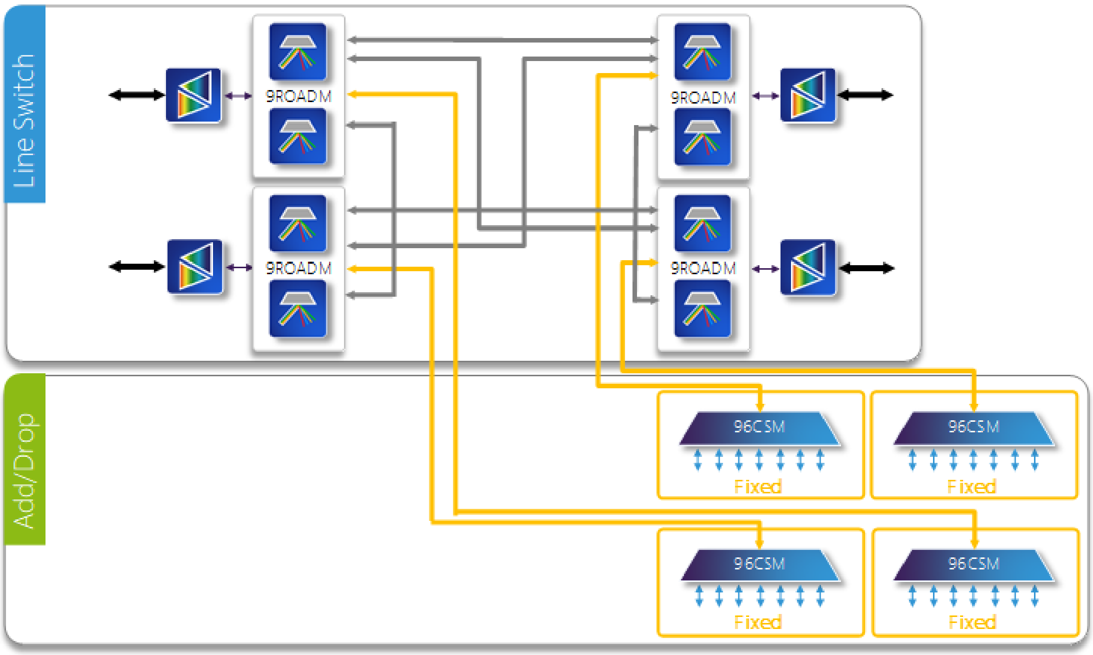
Background Information

You can configure the 9ROADM-RS for any combination of degrees and add-drop structures. The use cases in this section focus on a basic N-degree fixed, add-drop structure and colorless directionless add-drop structures that use coherent transceivers. The illustrations that follow are simplified and omit some client port connections.

N-Degree Fixed Add-Drop Using 96CSM

In this application, the 9ROADM-RS uses 96CSM passive-filter shelves as a fixed-wavelength add-drop filter that supports up to 96 add-drop channels per degree. Eight client ports on each 9ROADM-RS module connect to client ports on different 9ROADM-RS modules. The remaining client ports on each 9ROADM-RS module connect to a 96CSM shelf. The 96CSM shelf provides a 96-channel wavelength-multiplexer function in the add-channel direction and a 96-channel wavelength de-multiplexer function in the drop-channel direction.

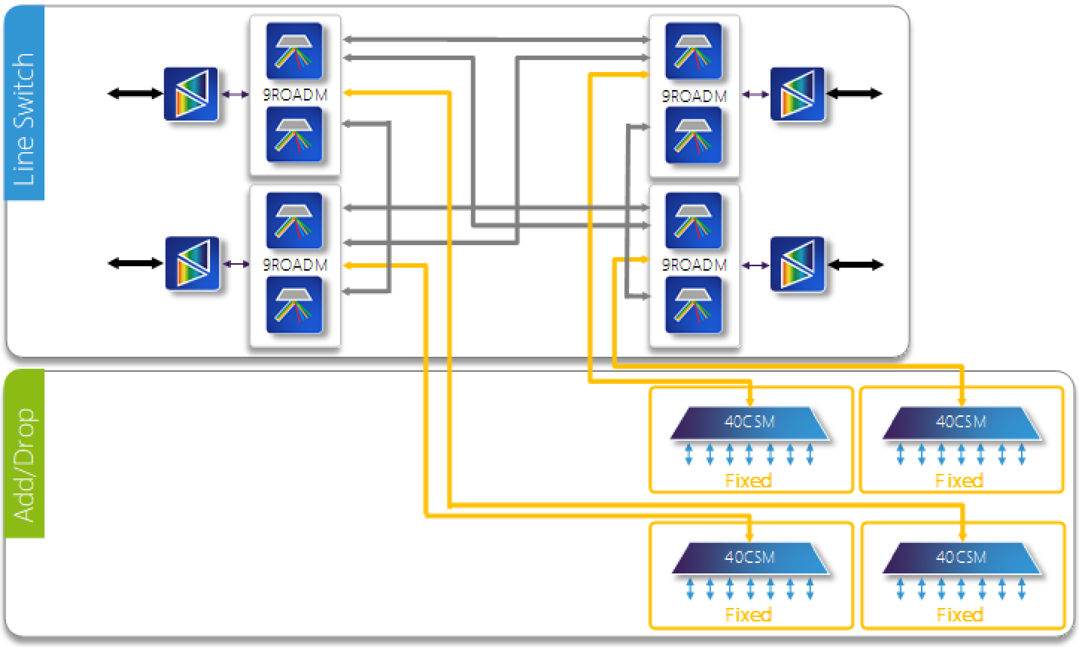
Figure 55: N-Degree Fixed Add-Drop With 96CSM



N-Degree Fixed Add-Drop Using 40CSM

This application is similar to the 96 Channel Splitter Module (CSM) application, but it uses 40CSM passive-filter shelves that connect to 9ROADM-RS client ports. These 40CSM shelves can also support up to 80 add-drop channels per degree if the configuration uses an Interleaver Module (ILM) to aggregate two 40-channel filter modules into 80 channels. An example is shown here.

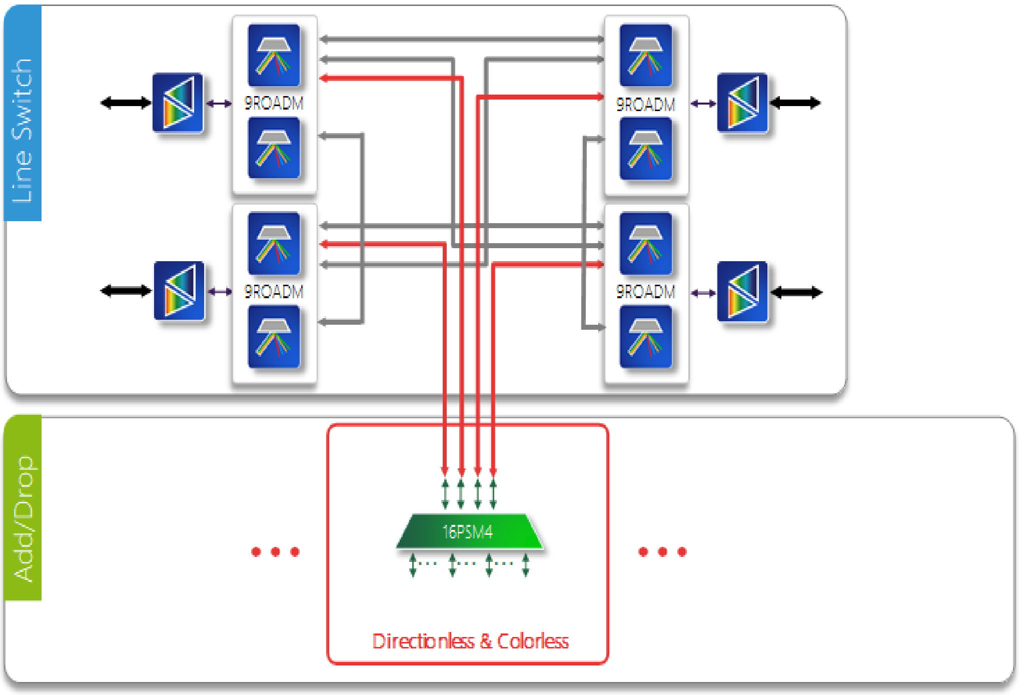
Figure 56: N-Degree Fixed Add-Drop With 40CSM



4-Degree Colorless Directionless Add-Drop for Coherent Signals

In this application, the 9ROADM-RS uses 16PSM4 filter modules to provide a 4-degree colorless directionless add-drop structure. Up to 96 add-drop channels total can be routed to or from any of the degrees.

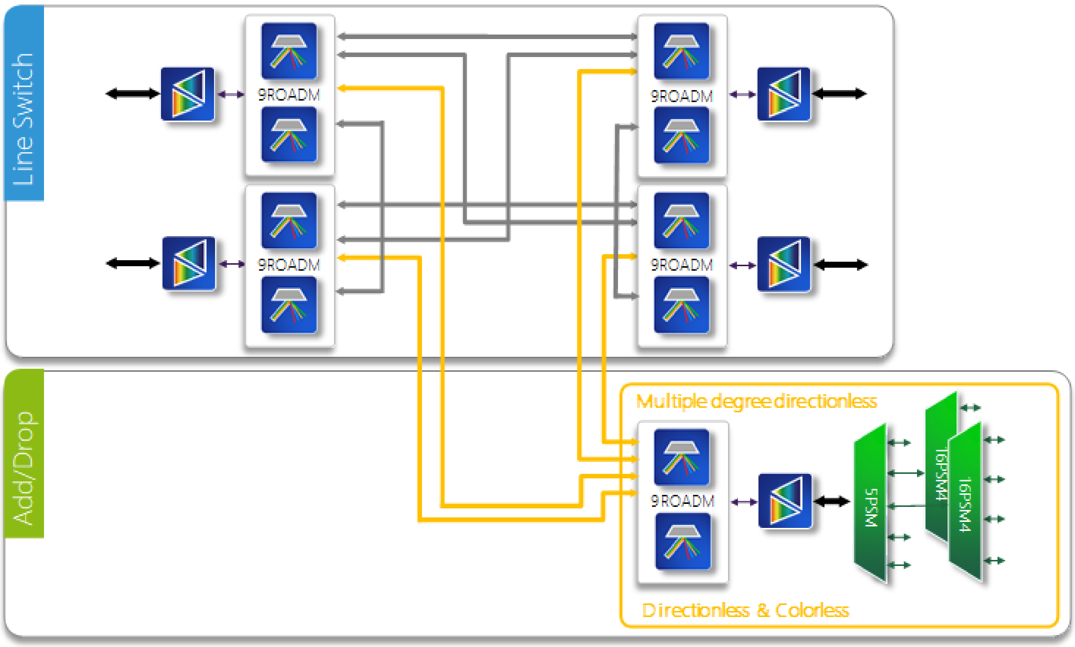
Figure 57: 4-Degree Colorless Directionless Add-Drop Structures



Colorless Directionless Add-Drop for More than 4 Degrees

In this application, multiple 9ROADM-RSs are set for Degree Fixed, and one 9ROADM-RS is set for Degree Select (steerable). Also, a 5 channel Power Splitter Module (PSM), 8PSM, and or 16PSM filter module can connect to multiple 16PSM4 filter modules to provide up to 9-degree colorless directionless add-drop capability. Up to 96 add-drop channels can be routed to and from any of the degrees.

Figure 58: Up to 9-Degree Colorless Directionless Add-Drop



Requirements

- The node is populated with the required modules, including an NCU-II or NCU-II-P.
- All modules are added, and their admin states are set to **In Service**.
- A fiber (cabling) plan is available.
- Amplifier ports are added, and their admin states are set to **In Service**.
- The ROADM ports are added, and their admin states are set to **In Service**.
- Channel module network ports are added, and their admin states are set to **In Service**.

9ROADM-RS Provisioning Steps

The purpose of this procedure is to configure the 9ROADM-RS and related filters for N-degree fixed add-drop structures and colorless directionless add-drop applications.

Provisioning equipment to support N-degree fixed add-drop branches involves provisioning the 9ROADM-RS, 96CSM, or 40CSM as detailed in this section. Provisioning is the same for the 96CSM and 40CSM configurations. See N-Degree Fixed Add-Drop With 96CSM and N-Degree Fixed Add-Drop With 40CSM figures.

To provision equipment that supports a 4-degree colorless directionless add-drop configuration, you must configure four 9ROADM-RSs and one 16PSM4 filter module. See 4-Degree Colorless Directionless Add-Drop Structures figure.

To provision equipment to support multiple-degree colorless directionless add-drop configurations, you must provision multiple 9ROADM-RSs for Degree Fixed and one 9ROADM-RS for Degree Select. Also, you need to provision a 5PSM filter and multiple 16PSM4 filter modules if more than four degrees are required. See Up to 9-Degree Colorless Directionless Add-Drop figure.

1. Ensure that all 9ROADM-RS modules, ports, and physical connections are added to the nodes. If not, see Adding Modules, Adding Ports, and Adding Physical Connections in the NED online Help.
2. Change the admin state of all added modules and ports to In-Service. To change the admin state of the module, you have to change the admin states of the provisioned entities (plugs, ports, and so on). See Adding Modules in the NED online Help.
3. Determine the pass-through and add-and-drop channels.
    a. Determine the specific pass-through channel between each 9ROADM-RS C port. You can identify the pass-through channels from the physical connections between the 9ROADM-RS C ports.
    b. Determine the add-and-drop channels between each 9ROADM-RS N port and C port. You can identify the add-and-drop channels from the physical connections between the CSM C ports and the channel modules.

> ROADM modules require that optical-channel power is present for proper operation. Therefore, when the channel passes through the ROADM modules, you must set channel modules as described here:
>
> - You must set **Auto Laser Shutdown** to **Disable**.
> - You must set **Error Forwarding Mode** to **Laser On**.
>
> These parameters can cause the channel-module laser to be turned off.

4. Add pass-through channels (determined in the previous step) by using the NED optical channel add wizard between the C port on a 9ROADM-RS module and the C port on the other 9ROADM-RS module. See Adding an Optical Channel in the NED online Help.

5. Add add-and-drop channels (determined in the previous step) by using the NED optical channel add wizard between the 9ROADM-RS N and C ports. See Adding an Optical Channel in the NED online help.

   > The NED optical channel add wizard automatically adds all necessary VCHs on the ports and the cross-connections between VCHs when each channel is added.

6. Change the admin state of the pass-through and add-and-drop cross-connections to In-Service. See Adding Modules in the NED online Help.
   a. From the Equipment list, select the 9ROADM-RS, and then change the admin state of the pass-through cross-connects to **In-Service**.
   b. From the Equipment list, select the 9ROADM-RS, and then change the admin state of the add-and-drop cross-connects to **In-Service**.
7. Initiate a port equalization on all 9ROADM-RS module N ports. See Equalizing Ports and Channels in the NED online Help.
8. Change the admin states for all VCHs to **In-Service** on all 9ROADM-RS N ports. See Provisioning a ROADM Channel in the NED online Help.
   a. Select **Configure** > **9ROADM-RS module** > **Optical Channels** > **Edit**.
   b. From the **Admin State** list, for each VCH select **In-Service**.

   > When you change the admin states to In-Service, any VCH alarms will be visible to the user.

9. Ensure that all services are fully established.
10. Verify the alarm status for all VCHs on all of the 9ROADM-RS N ports.

Click this link to return to use cases for 9ROADM-RS

10TCC-PCN-2G7US+10G

The 10TCC-PCN-2G7US+10G module transports up to 10 client signals over two 10 Gbps network channels. This section contains these topics:

Provisioning the 10TCC-PCN-2G7US+10G

Adding Module

1. Select **Configure**.
2. Navigate to the relevant shelf in the **Navigation Tree**.
3. In the **Main Pane**, click **Add Module**.
4. From the **Slot** list, select the slot number.
5. From the **Equipment** list, select 10TCC-PCN-2G7GUS+10G.
6. Enter **User Label** (optional) and select the **Admin State** from the list (**Auto In Service** is the default state).
7. Click **Add**.

   The module is listed in the **Navigation Tree**.

> If you want to edit the default options, navigate to the module in the **Navigation Tree** then click the row to access the **Details View**.

Adding Plugs

Add the plugs that support the service.

1. In the **Main Pane** of the slot that you want to configure, click the **Plugs** area.
2. Click **Add** to open the Add Plug window.
3. From the list, select the correct plug and equipment type.
4. Refer to your network plan to enter the required information.

Adding Ports

Add ports that support the service.

1. In the **Main Pane** of the slot that you want to configure, click the **Ports** area.
2. Click **Add** to open the Add Facility window.
3. From the list, select the correct **Identifier**.
4. Refer to your network plan to enter the required information and click **Add**.

   The ports are listed under the **Ports** area.

Adding Data Channels

Add the data channel to establish the service path:

1. In the **Main Pane** of the slot that you want to configure, click the **Data Channels** area.
2. Click **Add End Point** to open the Add Facility window.
3. From the list, select the correct port and channel.
4. Refer to your network plan to enter the required information and click **Add**.

> You have to select ODU ID and slot number when adding data channels on network plugs.

5. In the **Data Channels** area, click **Add Connection**.
6. Select **Add-Drop** connection.
7. Choose the end points.
8. Click **Add**.

The data channels are listed under the **Data Channels** area.

Adding Protection

If you need to protect the service:

1. In the **Protection** area, click **Add**.
2. From the list, select the correct **Identifier**.
3. Refer to your network plan to enter the required information.
4. If the far-end module for the protected service is not a 10TCC-PCN-2G7U+10G module, then set **APS Far End Module** to **Other** for correct operation.
5. Click **Add**.

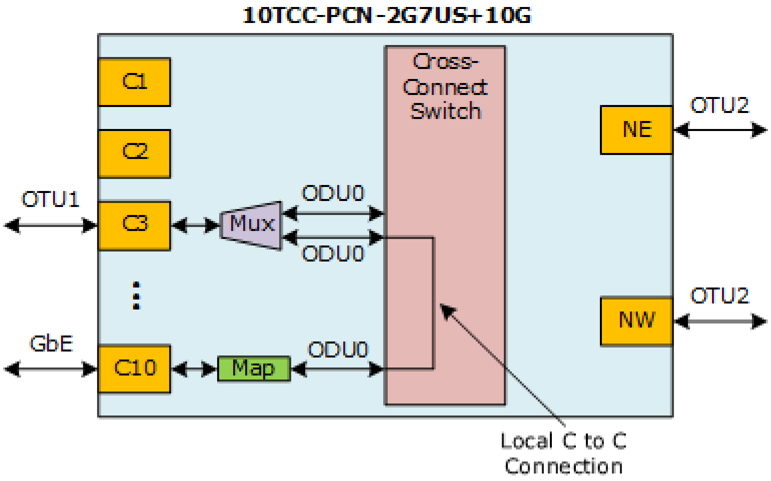
The protected path is listed under the **Protection** area.

Provisioning Local Client-to-Client Services

This example shows how to provision the 10TCC-PCN-2G7US+10G to connect services between two client ports on the same module.

OTU1 (with ODU0 carrying GbE) to GbE

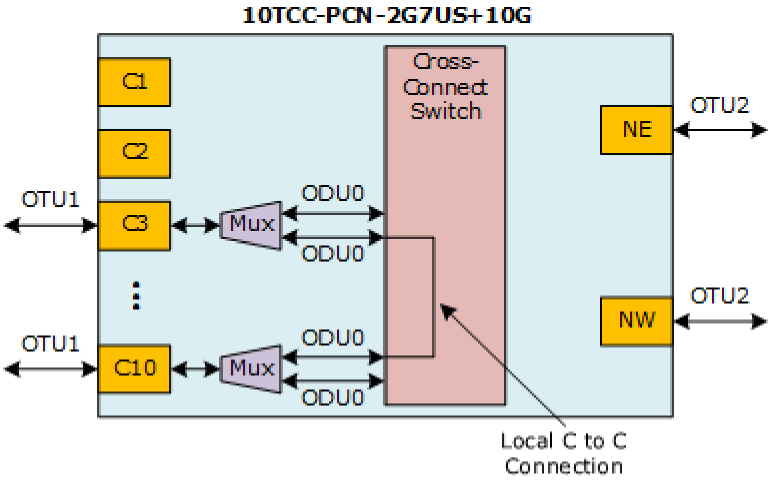
An OTU1 service can carry 2 multiplexed ODU0s, each of which may contain a service (i.e. GbE). Each ODU0 can be routed to a different port. In this case one ODU0 is connected to another client port and the GbE service is dropped.



1. Add the **10TCC-PCN-2G7US+10G** module.
2. Add the client plug supporting the OTU1 service.
3. Add the client port supporting the OTU1 service.
   - **Termination Level** must be set to **OPU**.
4. Add the client plug supporting the GbE service.
5. Add the client port supporting the GbE service.
   - Select **Facility** (**Ethernet 1G**).
6. Add Data Channel.
   - Click **Add End Point**.
   - Select the port supporting the OTU1 service.
   - Select the channel (ODU0 carrying the GbE service).
   - Click **Add**.
   - Select the port supporting the GbE service.
   - Select the channel.
   - Click **Add**.
   - Click **Add Connection**.
   - Select **Local C to C**.
   - Select **End Point** added to port supporting the OTU1 service with GbE in ODU0.
   - If required, select **End Point** added to port supporting the GbE service.
   - Click **Add**.

OTU1 (with ODU0) to OTU1 (with ODU0)

An OTU1 service can carry 2 multiplexed ODU0s, each of which may contain a service. Each ODU0 can be routed to a different port. In this case one ODU0 is connected to another client port and multiplexed into an OTU1 service.



1. Add the **10TCC-PCN-2G7US+10G** module.
2. Add the client plug supporting the first OTU1 service.
3. Add the client port supporting the first OTU1 service.
   - **Termination Level** must be set to **OPU**.
4. Add the client plug supporting the second OTU1 service.
5. Add the client port supporting the second OTU1 service.
   - **Termination Level** must be set to **OPU**.
6. Add the Data Channel
   - Click **Add End Point**.
   - Select port supporting the first OTU1 service.
   - Select the channel (ODU0 to be routed to other client port).
   - Click **Add**.
   - Select the port supporting the second OTU1 service.
   - Select the channel (ODU0 to be routed to other client port).
   - Click **Add**.
   - Click **Add Connection**.
   - Select **Local C to C**.
   - Select end point for first OTU1 service.
   - If required, select end point for second OTU1 service.
   - Click **Add**.

Back to 2TWCC-PCN-2G7U.

10TCC-PCN-3GSDI+10G

The 10TCC-PCN-3GSDI+10G module can transport video services (SDI) from a remote site to a studio. This section contains these topics:

Background Information

The 10TCC-PCN-3GSDI+10G module transports up to 20 client signals over two 10 Gbps network channels. This module offers transport of video services at a high port density. The module network ports (NE) and (NW) can be configured to route video services in diverse fiber paths from one node to another or around a ring network. The module is capable of delivering a range of raw and uncompressed video and audio formats.

Supported unidirectional client formats include:

- SD-SDI (270 Mbit/s)
- HD-SDI (1.4835 Gbit/s)
- HD-SDI/1.001 (1.485 Gbit/s)
- 3G-SDI (2.967 Gbit/s)
- 3G-SDI/1.001 (2.970 Gbit/s)
- DVB-ASI (270 Mbit/s)
- MADI digital audio (125 Mbit/s)

Supported bidirectional client formats include:

- GbE (1.250 Gbit/s)

The module can be configured to automatically adapt to respective SD-SDI, HD-SDI or 3G-SDI video formats present at a client port. The module does not automatically adapt to DVB-ASI, MADI digital audio, or GbE services.

The module supports Client Channel Card Protection (CCCP) and inter-shelf Client Channel Card Protection (inter-shelf CCCP). With inter-shelf CCCP, two video modules provisioned in a CCCP group can be placed in different shelves without regard for the slot position within a shelf and location of the shelves within the network element (NE). Inter-shelf CCCP is supported in high availability environments as well as non-high availability environments. To further increase reliability in high availability environments, redundant System Control Units (SCU) are interconnected between shelves, and video modules in the CCCP group are placed in shelves located in different rooms with separate power sources.

The module supports unidirectional Path Protection.

Back to 10TCC-PCN-3GSDI+10G

Requirements

- The node is populated with the required modules.
- All modules have been added and their admin states are set to **In Service**.
- A fiber (cabling) plan is available.
- Fibers are represented under **Overview > Physical Connections**.

Auto Configuration Feature

There are two facility types listed on the menu, ADAPT1485 and ADAPT2970, that allow the video module to adapt automatically to the video format present at the client port. To use this feature, select one of these facility types:

- If ADAPT1485 is selected, the port adapts to SD-SDI, HD-SDI/1.001, and HD-SDI video formats.
- If ADAPT2970 is selected, the port adapts to SD-SDI, HD-SDI/1.001, HD-SDI, 3G-SDI/1.001, and 3G-SDI video formats.

If a connected client video service in adapted mode changes types at the client port (for example, from SD to HD), and the service has an active, uninhibited CCCP or path protection configuration, the changed service is not active until at least 10 seconds after the service has been re-established. During that 10-second time frame, a protection switch event may occur.

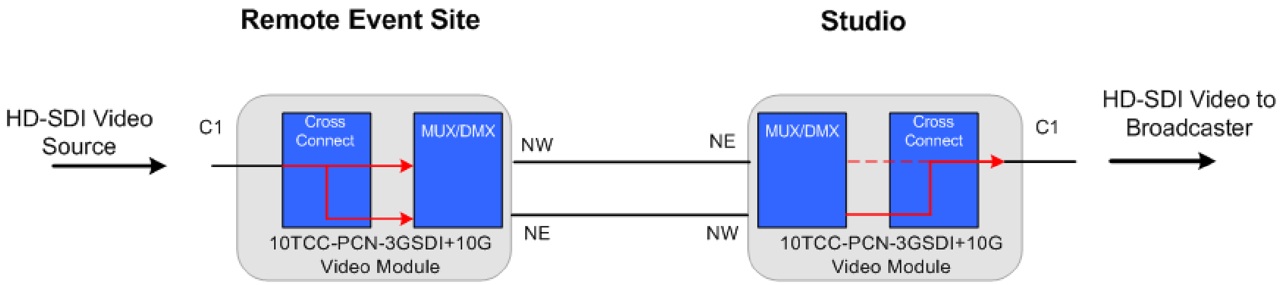
These requirements must be met before provisioning a port for auto-configuration:

- The facility type must match everywhere the video format is present.
- At least one monitor path must be free because that path must be reassigned.
- A path is available in the desired direction with sufficient bandwidth to accommodate the largest potential video format, i.e. HD-SDI (ADAPT1485) or 3G-SDI (ADAPT2970).
- Adaptive service might reduce the number of available paths because the system treats it like a bidirectional service.

Back to 10TCC-PCN-3GSDI+10G

Provisioning 10TCC-PCN-3GSDI+10G Module for Path Protection

The 10TCC-PCN-3GSDI+10G module supports path protection at the Remote Event and Studio nodes. The two nodes are connected in a point-to-point configuration. A protected drop cross-connection is provisioned at each node.



Equipment

The equipment listed is an example. Ensure remote event and studio nodes are populated with the required modules. Your equipment may be different. Check your design plan.

Remote Event Node:

- 10TCC-PCN-3GSDI+10G module.
- SFP-2RX/x/G client plug (dual receive).
- 2 XFP/x/D network plugs. Plugs must match in remote event and studio nodes but can be different for each fiber path.

Studio Node:

- 10TCC-PCN-3GSDI+10G video module.
- SFP-2TX/x/G client plug (dual transmit).
- 2 XFP/x/D network plugs. Plugs must match in remote event and studio nodes but can be different types for each fiber path.

Follow these steps:

Remote Event Node:

1. Select **Configure**.
2. Navigate to the shelf and slot.
3. Click **Add Module**.
4. Select the proper slot. If the 10TCC-PCN-3GSDI+10G card is plugged in, it will be displayed.
5. Click **Add**.

6. Provision the Client plug and select the **Rx** type.
7. Provision the Network plugs for NE and NW.
8. Provision the Client ports. Choose the frequency 2970 and UNI channel.
9. Provision Network ports, select frequency if the plug tunable.
10. For Network ports, click **Add Network End Point** to add the end points for connection in Data Channels:

- Select **Identifier** for the data channel
- The desired **Facility**
- Enter a **Channel ID**
- Set **Traffic Direction** to Cross-Connect Tx

11. Click **Add Connection** and select **Multicast Add** and then add VCH for NE and NW.
12. Click on **+** at NE VCH, then open new created cross connection and modify cross connect type to “1-Way DC Protection”. Click **Apply and Exit**.

Studio Node:

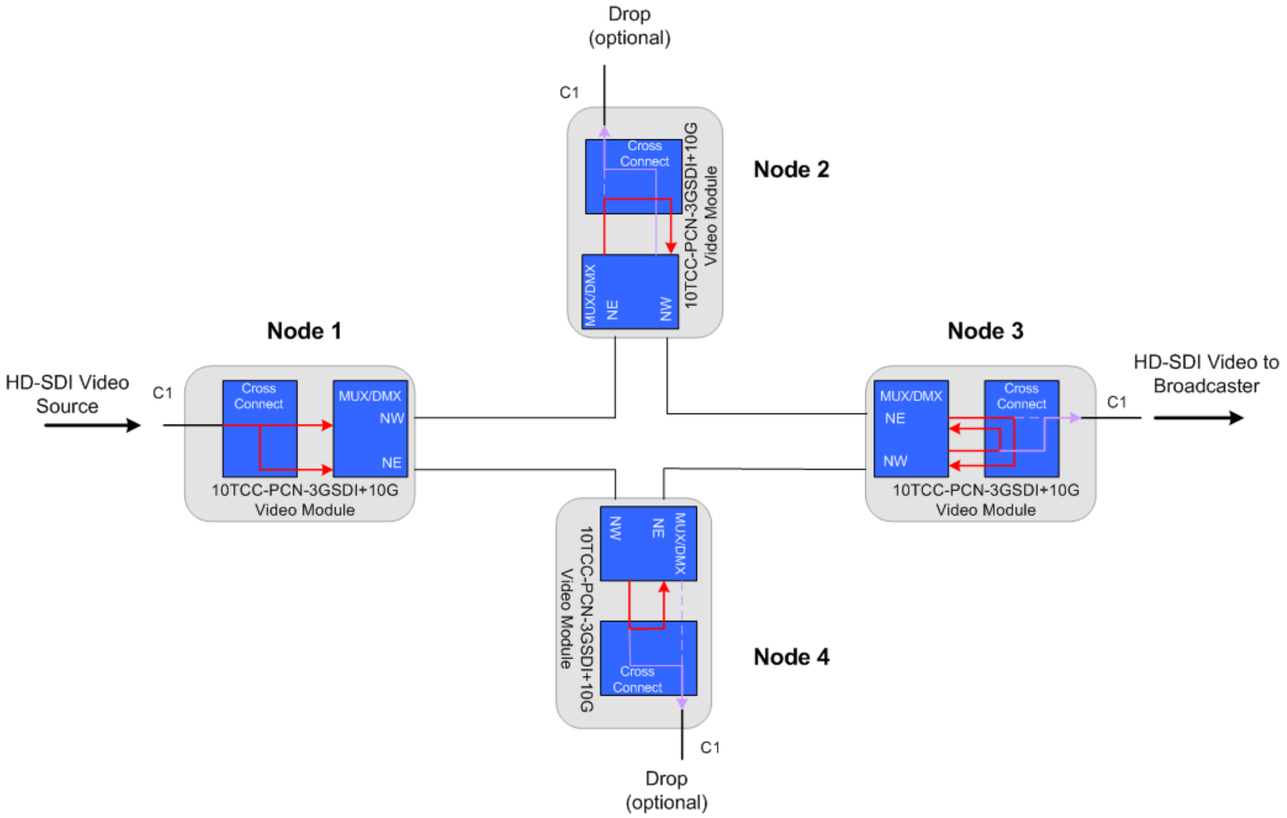
13. Repeat steps 1 to 5.
14. Provision Client plug and select the **Tx** type.
15. Provision the Network plugs for NE and NW.
16. Provision Client port and select facility 2970.
17. Provision Network ports NE and NW.
18. For NE and NW ports, Click **Add End Point** in **Data Channels** and select traffic direction **Rx** and facility type as Client port frequency 2970. Enter the same channel ID (channel 01 for this example) as you have for the Remote Event node.
19. Click **Add Connection** and select **Protected Multicast Drop** and then for this example VCH...NE. The field **(C) Secondary** should report your VCH-NW. In the field **(B) Destination** select your Client. Select working side. Check UCH B for this example.
20. Select **Protection**, your designated working field -> FFP-CH...NE. Finish by selecting **Add**.

Back to 10TCC-PCN-3GSDI+10G

Provisioning Path Protection in a Ring Network

The 10TCC-PCN-3GSDI+10G video module can use path protection when 4 nodes are connected in a ring. In this configuration, you must provision different types of cross connections:

- Add cross connection
- Drop cross connection
- Pass-through cross connection
- Drop with continue cross connection
- Path protection



Equipment

The equipment listed is an example. Ensure nodes are populated with the modules.

Node 1 (source) (add cross connection):

- 10TCC-PCN-3GSDI+10G video module.
- SFP-2RX/x/G client receive plug.
- 2 each, XFP/x/D network plugs (fixed frequency, for NE and NW ports) Plugs in module must match with neighbor nodes. They can be different types for each fiber link.

Node 2 (pass-through):

- 10TCC-PCN-3GSDI+10G video module.
- 2 each, XFP/x/D network plugs (fixed frequency, for NE and NW ports). Plugs in module must match with neighbor nodes. They can be different types for each fiber link.

Node 3: (broadcaster) (drop cross connection):

- 10TCC-PCN-3GSDI+10G video module.
- SFP-2TX/x/G client transmit plug.

- 2 each, XFP/x/D network plugs (fixed frequency, for NE and NW ports). Plugs in module must match in source and broadcaster nodes. They can be different types for each fiber link.

Node 4 (drop with continue):

- 10TCC-PCN-3GSDI+10G video module.
- SFP-2TX/x/G client transmit plug.
- 2 each, XFP/x/D network plugs (fixed frequency, for NE and NW ports). Plugs in module must match with neighbor nodes. They can be different types for each fiber link.

Preparation

The use case assumes these conditions:

- All modules and plugs have been plugged into node.
- You have a cabling plan showing all node-internal fiber jumpers.Examples, Path Protection Ring diagram.
- All fiber and cable connections are properly connected.

To provision the video module for path protection, follow these steps:

1. Select **Configure**.
2. Navigate to the relevant shelf.
3. Click **Add Module**.
4. Select the proper slot. If the 10TCC-PCN-3GSDI+10G card is plugged in, it will be displayed.
5. Click **Add**.

Node 1 (source) (add cross connection)

1. Provision the Client plug and select the **Rx** type.
2. Provision the Network plugs for NE and NW.
3. Provision the Client ports. Select your UCH channel and choose frequency 2970.
4. Provision Network ports NE and NW. Select frequency if tunable.
5. Create NE and NW virtual channels for Network cross connection by clicking **Add Network End Point** in **Ports** area. Select VCH-xxx- 1, facility client frequency 2970 and traffic direction **Tx**. Choose channel ID **01** for this example.
6. In **Data Channels** area click **Add Connection** and select **Multicast Add**. Then add VCH for NE and NW.
7. Click on **+** at NE VCH, then open new created cross connection and modify cross connect type to **1-Way DC Protection**. Click **Apply & Exit**.

Node 2 (pass-through)

1. Repeat steps 1 to 5.
2. Provision the Network plugs for NE and NW.
3. Provision Network ports NE and NW.
4. For NE and NW ports, click **Add Network End Point** in **Ports** area. Select VCH-xxx- 1, facility client frequency 2970 and traffic direction (NE is Rx and NW is Tx). Enter channel ID **01**. Same channel as for Node 1 (source).
5. Click **Add Connection** in **Data Channels** area, select **Pass-Through A - C** and then for this example VCH...NE. The field **(A) Local** should report your VCH-NE. The field **(C from A)** should report your VCH-NW.
6. Click **Add**.

Node 3 (broadcaster) (drop cross connection)

1. Repeat steps 1 to 5.
2. Provision Client plug and select the **Tx** type.
3. Provision the Network plugs for NE and NW.
4. Provision Client port and select facility 2970.
5. Provision Network ports NE and NW.
6. For NE and NW ports, click **Add Network End Point** in **Ports** area. Select VCH-xxx-1, facility client frequency 2970 and traffic direction **Rx**. Enter channel ID **01**. Same channel as for Node 1 (source).
7. Click **Add Connection** and select **Protected Multicast Drop** and then for this example VCH...NE. The field **(C) Secondary** should report your VCH-NW. In the field **(B) Destinations** select your Client. Select working side. Check UCH B for this example.
8. Select **Protection**, your designated working field -> FFP-CH...NE.
9. Click **Add**.

Node 4 (drop with continue)

1. Repeat steps 1 to 5.
2. Provision Client plug and select the **Tx** type.
3. Provision the Network plugs for NE and NW.
4. Provision Client port and select facility 2970.
5. Provision Network ports NE and NW.
6. For NE and NW ports, click **Add Network End Point** in **Ports** area. Select VCH-xxx- 1, facility client frequency 2970 and traffic direction (NW is Rx and NE is Tx). Enter channel ID **01**. Same channel as for Node 1 (source).
7. Click **Add Connection** and select **Multicast Drop With Continue** and then for this example in **C from A** section, select VCH...NE. In **B (destinations)** section, select your

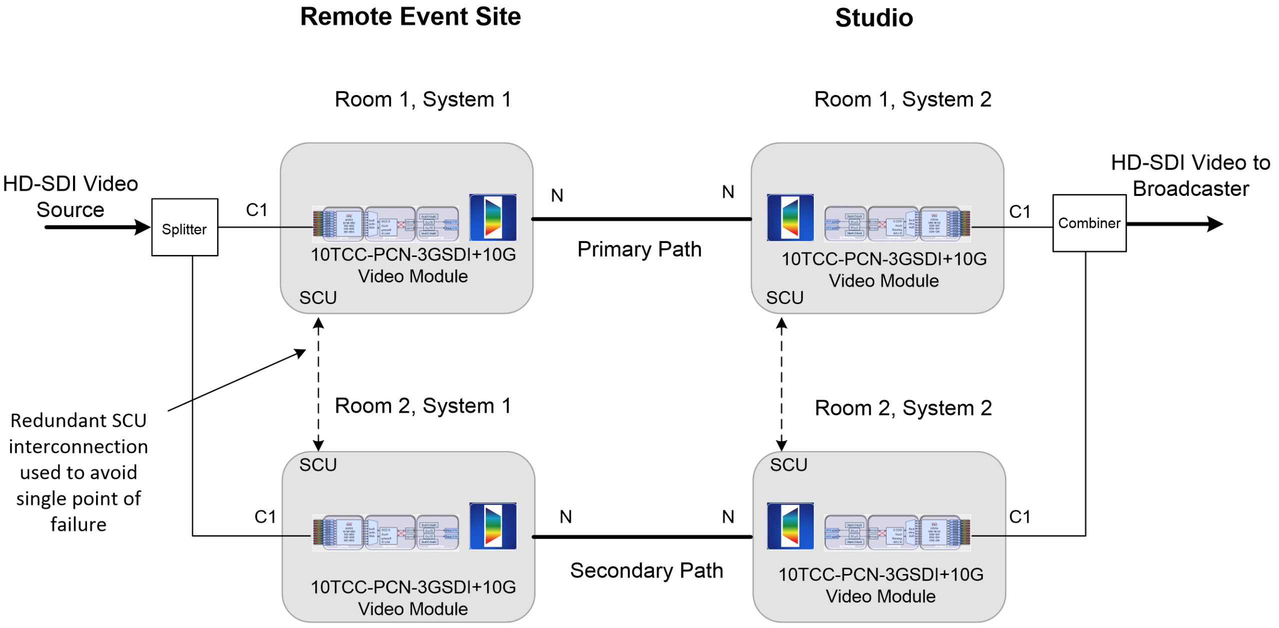
client UCH. Field **(A) Local** should report your VCH-NW. The field **(C from A)** should report your VCH-NW. The field **B (Destinations)** should report the UCH.

8. Select **Protection**, your designated working field -> FFP-CH...NE.
9. Finish by selecting **Add**.

Back to 10TCC-PCN-3GSDI+10G

Provisioning Client Channel Card Protection

The 10TCC-PCN-3GSDI+10G video module can support client channel card protection at the Remote Event and Studio nodes. The two nodes are connected in a point-to-point configuration.


Remote Event Site
Studio
Room 1, System 1
Room 1, System 2
HD-SDI Video Source
Splitter
C1
10TCC-PCN-3GSDI+10G Video Module
SCU
N
Primary Path
N
10TCC-PCN-3GSDI+10G Video Module
SCU
C1
Combiner
HD-SDI Video to Broadcaster
Redundant SCU interconnection used to avoid single point of failure
Room 2, System 1
Room 2, System 2
SCU
C1
10TCC-PCN-3GSDI+10G Video Module
N
Secondary Path
N
SCU
10TCC-PCN-3GSDI+10G Video Module
C1

Equipment

The equipment listed is an example for this use case. Ensure the remote event and studio FSP-3000R7 nodes are populated with the basic operational modules. Your equipment may be different. Check your design plan.

Remote Event Node:

- 2 each, 10TCC-PCN-3GSDI+10G video modules.
- 2 each, SFP-2RX/x/G client receive plugs.
- 2 each, XFP/x/D network plugs (fixed frequency, for network port) Plugs in module must match in remote event and studio nodes. They can be different types for each fiber link.

Studio Node:

- 2 each, 10TCC-PCN-3GSDI+10G video modules.
- 2 each, SFP-2TX/x/G client transmit plugs.
- 2 each, XFP/x/D network plugs (fixed frequency, for network ports). Plugs in module must match in remote event and studio nodes. They can be different types for each fiber link.

Preparation

The use case assumes these conditions:

- All modules and plugs have been plugged into node.
- You have a cabling plan showing all node-internal fiber jumpers (For this example, see CCCP Point-to-Point diagram).
- All fiber and cable connections are properly connected.

To provision the video module for CCCP, follow these steps:

1. Click **Configure**.
2. Navigate to the relevant shelf.
3. Click **Add Module**.
4. Select the proper slot for first module. If the 10TCC-PCN-3GSDI+10G card is plugged in, it will be displayed.
5. Click **Add**.
6. Click **Add Module**.
7. Select the proper slot for second module. If the 10TCC-PCN-3GSDI+10G card is plugged in, it will be displayed.
8. Click **Add**.

Remote Event Node: first module, room 1 system 1

9. Provision the Client plug and select the **Rx** type.
10. Provision the Network plug for NE.
11. Provision the Client port. Choose the frequency 2970.
12. Provision the Network port NE.
13. Click **Add End Point** for Network cross connection in **Data Channels** and select **Traffic direction Tx** and Facility **Client**.
14. Click **Add Connection** and select **Multicast Add** and then add VCH for NE.

Remote Event Node: second module, room 2 system 1

15. Provision the Client plug and select the **Rx** type.
16. Provision the Network plug for NW.
17. Provision the Client port. Choose the frequency 2970.

18. Provision the Network port NW.
19. Click **Add End Point** for Network cross connection in **Data Channels** and select **Traffic direction Tx** and Facility **Client**.
20. Click **Add Connection** and select **Multicast Add** and then add VCH for NW.

Studio Node

21. Repeat steps 1 to 8.

Studio Node, first module, room 1, system 2

22. Provision client plug and select the **Tx** type.
23. Provision network plug for NW.
24. Provision client port and select facility 2970.
25. Provision network port NW.
26. Click **Add End Point** in **Data Channels** and select traffic direction **Rx** and facility type as **Client** port 2970. Enter the same channel ID as you have for the remote event site, first module.
27. Click **Add Connection** and select **Multicast Drop**. Use (A) for the VCH from step 26 and (B) for the UCH from step 24.

Studio Node, second module, room 2, system 2

28. Provision client plug and select the **Tx** type.
29. Provision the network plug for NE.
30. Provision client port and select facility 2970.
31. Provision network port NE.
32. Click **Add End Point** in **Data Channels** and select traffic direction **Rx** and facility type as **Client** port 2970. Enter the same channel ID as you have for the remote event site, first module.
33. Click **Add Connection** and select **Multicast Drop**. Use (A) for the VCH from step 32 and (B) for the UCH from step 30.

Create CCCP, Studio Node, first module

34. Select the **Protection** from first module.
35. Click **Add** and select in the Identifier dialog the **FFP** from the client port from step 24. The dialog window opens. Fill out Working and Protection Partner.
36. Finish with **Add** to create CCCP.

Back to 10TCC-PCN-3GSDI+10G

Examples

The diagrams below illustrate how the 10TCC-PCN-3GSDI+10G Video Module can be used in protection applications.

10WXC-PCN-10G

This section describes the 10-port ODUk cross-connect interface module, the 10WXC-PCN-10G, for the Node. It contains these topics:

Background Information

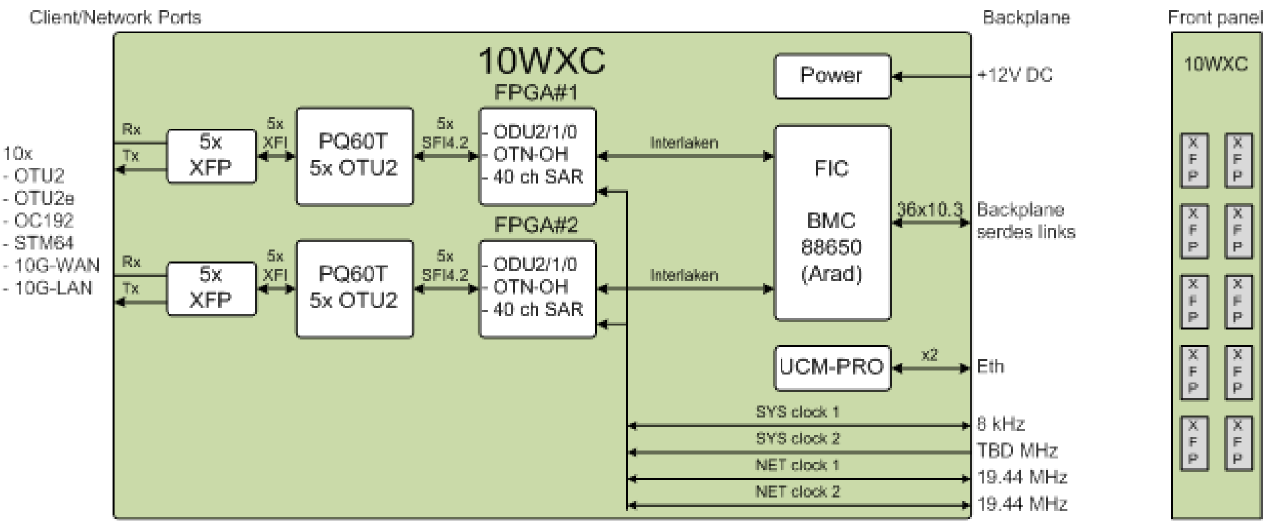
A 10WXC-PCN-10G supports cross connection of up to 100 Gbps of services at different ODU levels and/or SDH/SONET/Ethernet mapped into ODU. The module may be alone or in an interconnected group with two other 10WXC-PCN-10G modules to cross connect up to 300 Gbps of services. When interconnected in a group the three modules must be inserted into slots 4, 6, 8 or in slots 12, 14, and 16 in a SHX9HU shelf. The module may interface to any equipment supporting ITU-T G.709 OTU2/2e signals with OTN structures at ODU2/2e/1/0. The 10WXC-PCN-10G may also be used as demarcation point in multi-vendor/operator domain configurations in which OTN services are passed from one network domain to another.

Requirements

- The node controller must be an NCU-II and NCU-II-P.
- The 10WXC-PCN-10G module can be installed in a SH9HU or SHX9HU shelf.
- The CEM in the SH9HU shelf must have firmware version 121.2.1 or higher.
- The 10WXC-PCN-10G module(s) must have firmware version 121.6.3 or higher.

Examples

This simplified functional block diagram illustrates the signal path through the 10WXC-PCN-10G module:



Provisioning the 10WXC-PCN-10G Module

Adding the Module

1. Select **Configure**.
2. Click on the shelf where the module will be installed.
3. Click **Add Module** in the **Main Pane**.
4. Select the **Slot**.
5. Select **10WXC-PCN-10G** from the **Equipment** list.
6. Enter **User Label** (optional).
7. Select the desired **Admin State**.
8. Select the **Capability Level**.
9. Click **Add**.

If you want to edit the default options, navigate to the new module in the **Navigation Tree** and click it to view the **Details View**.

Adding Plugs

1. Click the **Plugs** area in the **Main Pane**.
2. Click **Add**.
3. Select the plug location and type.
4. Refer to your network plan to enter the required information.
5. Click **Add**.

Adding Ports

> Port usage can be either a **Client** or **Network**.
>
> Transport parameters determine type of data channel(s) that can be supported.

1. Click the **Ports** area in the **Main Pane**.
2. Click **Add**.
3. Select the Port Identifier.
4. Select the **Facility**.
5. Select other parameter as specified in your network management plan.
6. Click **Add**.

Adding Data Channels

Data Channels on this module require two end points to be added then a connection between them.

1. Click the **Data Channels** area in the **Main Pane**.
2. Click **Add End Point**.
3. Select an **Identifier** associated with the desired port.
4. Select the desired **Facility**.
5. Select other parameter as specified in your network management plan
6. Click **Add**.
7. If needed, repeat steps 1-6 for the other port.
8. Click **Add Connection**.
9. Select the connection type, ports and end points.
10. Click **Add**.

2TWCC-PCN-2G7U

The 2TWCC-PCN-2G7U and 10TCC-PCN-2G7US+10G ADM channel modules can transport SONET and OTN services. This section describes common use cases for transporting OTN services. It contains these topics:

Examples

Refer to the example network diagrams below:

- Example Network: Subtended Nodes, illustrates how two subtended nodes feed into a 10G ADM access ring.
- Client Channel Card Protection (CCCP) illustrates how to configure a 2TWCC-PCN-2G7U module for CCCP.

Set up the example networks by using interconnecting fibers. The network must contain these characteristics:

- 2TWCC-PCN-2G7U module.
- 10TCC-PCN-2G7US+10G ADM module.
- 1PM Protection modules or Y-cables.
- Active GbE services.

You may also use your own network and configure it. Refer to your engineering plan.

Prerequisites

The use cases assume these conditions:

- All cables are properly connected.
- Each node is populated with the required modules, all modules have been created, and all modules are set to In Service.
- All EDFA OM ports are set to In Service (if used).
- All transponder network ports are set to In Service.
- For each node in the network configuration, you will need a cabling plan showing all node-internal fiber jumpers.
- All physical cable connections are represented in the node databases by valid PTP (fibermap) connections in the PTP & Physical Connections Table.
- All nodes have been configured properly for optical supervisory channel (OSC) DCN channel traffic, and the OSC is in service between nodes, with no alarms.
- An overview of the network configuration, in the form of a figure showing the node's relative position to each other.
- A DCN plan for the network configuration.

Figure 59: Example Network: Subtended Nodes

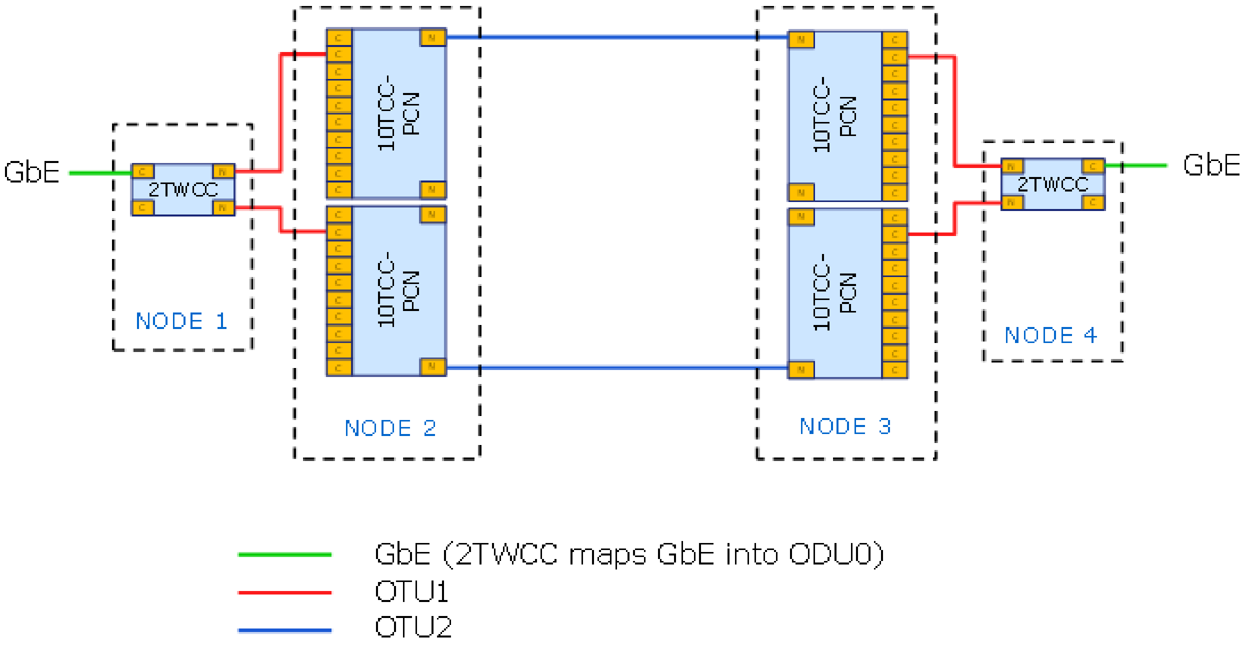
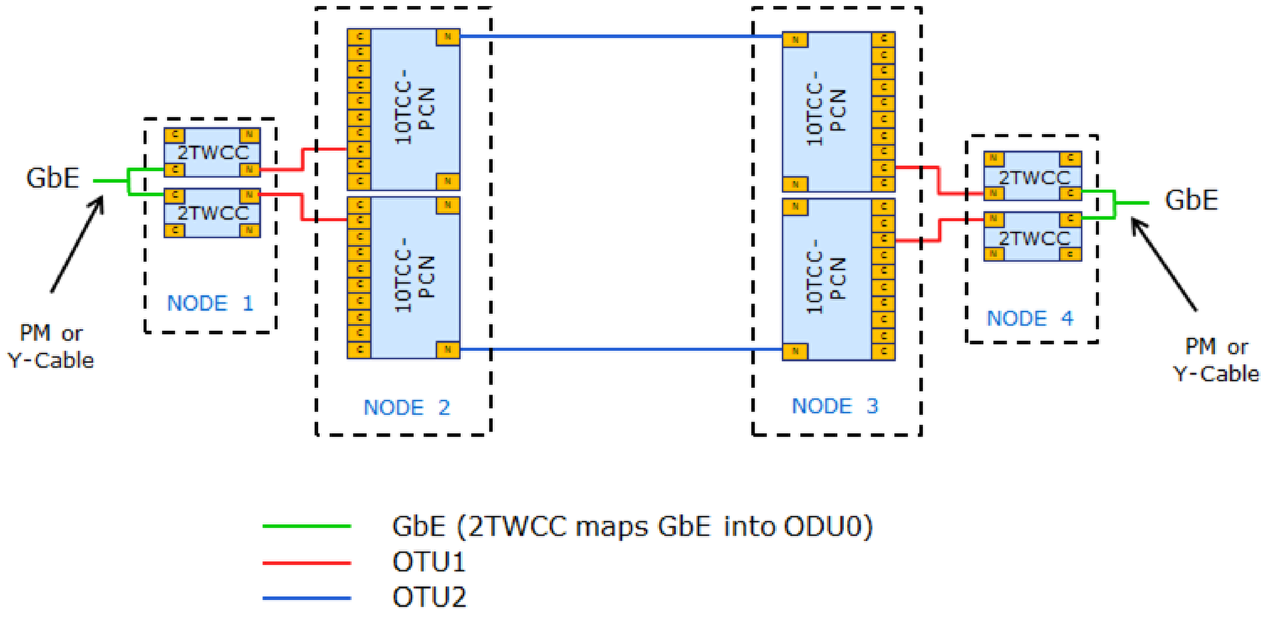


Figure 60: Example Network: Client Channel Card Protection



Back to 2TWCC-PCN-2G7U.

Provisioning as a Subtended Node

This user example scenario explains how to configure the 2TWCC-PCN-2G7U channel module as a subtended node, feeding its output into a 10G ADM access ring. Although the 2TWCC-PCN-2G7U channel module can transport SONET and OTN services, this use case explains how to transport OTN services.

In this example, GbE services are mapped by the 2TWCC-PCN-2G7U module into ODU0s to ODU1s and output as OTU1 services. The OTU1 services are input to the 10TCC-PCN-2G7US+10G ADM modules at the 10G ADM access ring network. Refer to Example Network: Subtended Nodes. Follow these steps to provision the 10TCC-PCN-2G7US+10G ADM and 2TWCC-PCN-2G7U modules to transport GbE services.

Provisioning Requirements

- See Examples, Refer to "Example Network: Subtended Nodes". (Either 1PMs or Y-cables can be used at the 2TWCC-PCN-2G7U module client ports). Refer to the *Hardware Description* and *Module and System Specification* for details about Y-cables.
- See Requirements and ensure that the channel modules are installed in the correct shelves and slots.

At the 10TCC-PCN-2G7US+10G ADM Module

1. Provision the 10TCC-PCN-2G7US+10G ADM modules at nodes 2 and 3.
2. Provision the four network ports where OTU1 services will be added and dropped:
   - Select OTU2 with OPU termination, and payload type 21 (to create VCHs with an ODU1 facility).
3. Create a VCH1 entity (data channel). Select **Add End Point** function in Data Channels panel:
   - Select the ODU1 facility.
   - Use the tributary port and slot according to your network plan.
4. Ensure that your network port links are operational.
5. Provision the client ports:
   - Select OTU1 with OTU termination.
   - Most other parameters are set as default. Select other parameters as required in your engineering plan.
6. Create cross-connections between the client ports (CH) and the network ports (VCH1):
   - Select **Add Connection** function in Data Channels panel (Add-Drop).

At the 2TWCC-PCN-2G7U Module

1. Provision the 2TWCC-PCN-2G7U modules at nodes 1 and 4.
2. Set the Multiplexing Method to OTN on both modules.
3. Provision the client ports on both nodes:
   - Set the facility type to Ethernet 1G.
   - Most other parameters are set as default. Select the other parameters as required in your engineering plan.

4. Provision the network ports on both nodes:
   - Ensure that the network facilities are assigned.
   - The service should be OTU1 with OPU termination, payload type 20.
5. Create the VCH entities (data channel):
   - Set the VCH entities to facility type ODU0.
   - In the case of transparent service (no rate limiting), these are fixed, and you need only to click apply.
   - In the case of framed service (rate limiting enabled), committed bit rate must be considered. (Refer to your engineering plan.)
   - If rate limiting is enabled, consider auto-negotiation. (Refer to your engineering plan.)
   - If client channel card protection is used in your network plan, auto-negotiation must be disabled.
6. Verify traffic is operational in GbE channel, all the way through the network.

Back to 2TWCC-PCN-2G7U.

Provisioning for Client Channel Card Protection

This user example scenario explains how to provision 2TWCC-PCN-2G7U channel modules in near-end and far-end subtended nodes. Although the 2TWCC2G7 channel module can transport SONET and OTN services, this use case explains how to transport OTN services. The channel modules are provisioned to protect GbE services using Client Channel Card Protection (CCCP).

Provisioning Requirements

- Refer to Examples "Client Channel Card Protection". (Either 1PMs or Y-cables can be used at the 2TWCC2G7 module client ports). Refer to the *Hardware Description* and *Module and System Specification* for details about Y-cables.
- Refer to Requirements section and ensure channel modules are installed in correct shelves and slots.

At the Channel Module

1. Ensure modules exist (are assigned but not necessarily equipped).
2. Set equipment type to 2TWCC2G7.
3. Ensure modules are of the same MODE type: Multiplexer NE only or Multiplexer NW only (not Multiplexer NE & NW). For more information, see About Modes.
4. Provision one protection partner for Multiplexer NE only and the other for Multiplexer NW only.
5. Set Capability Level to 1.

6. Set Capability description to 1 (for ODU0/ODU1, CCCP, and Rate Limiting (check design plan for rate limiting or no rate limiting).
7. Provision Multiplexing Method for OTN (which means ODU0 on the VCH).
8. Check that DEPLOY parameter is defaulted to STANDARD.

At the Client Port

1. Ensure the client plugs exist (are assigned) and are equivalent.
2. Ensure client (C) facilities exist (are assigned):
   - Set facility type to Ethernet 1G.
   - Set client (C) facilities for the same Facility Type.
   - Ensure client (C) TERM, behavior, and Error Forwarding are the same.
3. Set ADMIN state to automatic In-service (any assigned ADMIN state is valid, including DSBLD).
4. Check that client (C) facilities are physically on separate modules:
   - If rate limit is used, ensure both modules are provisioned the same for rate limit and flow control.
   - Auto negotiate must be disabled when using CCCP.

At the VCH

1. Ensure VCH facilities exist (are assigned).
2. Provision VCH facilities for the same FACILITY TYPE, TERM, PAYLOAD, and PT:
   - Facility type should be ODU0 as defined by selecting Multiplexer Method for OTN in an earlier step.
   - If Rate limit is used, CIR settings should be the same.

At the Network Port

1. Ensure network facilities exist (are assigned) and are equivalent:
   - Verify ODU1 with termination level OPU is set.
2. Ensure Network facilities are the same FACILITY TYPE and TERM level.
3. Set the N ports for the same ALS mode.
4. Set ADMIN state to automatic In-service (any assigned ADMIN state is valid, including DSBLD).

Create Facility Fault Protection (FFP)

1. Create FFP at the client (C) entities:
   - At the channel module (CH-x-x-Cx 1GBE), Config tab 3, set Protection Role to P for Protect.

- Set Revertive Protection to no for no revert or yes for wait to restore (refer to your design plan).
- Verify Working Partner and Protection Partner are selected and correct.
- At client interface, any existing loopbacks should be released when FFP is created. The software will not allow establishment of a loopback if an FFP exists.

2. Release any Force LASER operation when FFP is created:
   - At client interface, a forced LASER condition is released when FFP is created.
   - Forced FFP provisioning per EOU documents is applicable.

See Setting Up Client Channel Card Protection in this manual for more information.

At this point, all nodes have been configured properly for client channel module protection, wavelengths and services. OSC and DCN channel traffic should be in service between nodes, with no alarms.

Back to 2TWCC-PCN-2G7U.

Connecting OPPM for Point-to-Point Operation

This use case explains how to provision channel modules to operate with the Optical Path Protection Switch Module (OPPM). The configuration in this use case protects 100Gbit services in a point-to-point connection between two nodes.

This section contains these topics:

Background Information

The OPPM is an optical broadcast and selection device for optical protection. You use the module in multiple ways to provide optical protection in access, metro, and core-meshed networks.

The OPPM provides optical path protection for a single optical channel or multiple optical channels.To accomplish this task, the module splits the client-receive optical signal that broadcasts to both network transmit ports and creates working and protection paths. At the network receive ports, NE and NW, the OPPM selects and switches one of the network paths to the client transmit optical port.

The system monitors the optical signal power independently at each network receive port, which is the primary criteria that applies to path selection. In addition, you can initiate the OPPM through a digital-signal fail from a single channel module or a group of channel modules known as protection trigger partners. The protection trigger partner group can contain up to four channel modules.

You can use amplifiers, such as boosters, pre-amplifiers, or inline amplifiers, between channel modules and the OPPM. You can also use amplifiers in the optical path between peer OPPMs. Make sure that these amplifiers do not exceed the maximum input power level specified for the respective OPPM interface.

You can provision the OPPM for either unidirectional or bidirectional protection switching. Use an Automatic Protection Switching (APS) channel that a protection trigger partner provides to communicate local switch information for bidirectional switching peer OPPMs.

Return to Connecting OPPM for Point-to-Point Operation

Requirements

These are the required conditions for Connecting OPPM for Point-to-Point Operation. Make sure that you:

- Populate all nodes with the basic operational modules.
- Have a cabling plan that shows all internal node-fiber jumpers.
- Properly connect all cables that the Installation and Commissioning Manual specifies.

> To configure revertive switching, you must disable EPTE triggering. You can provision revertive switching only if you set the EPTE triggering field to DISABLED.

Return to Connecting OPPM for Point-to-Point Operation

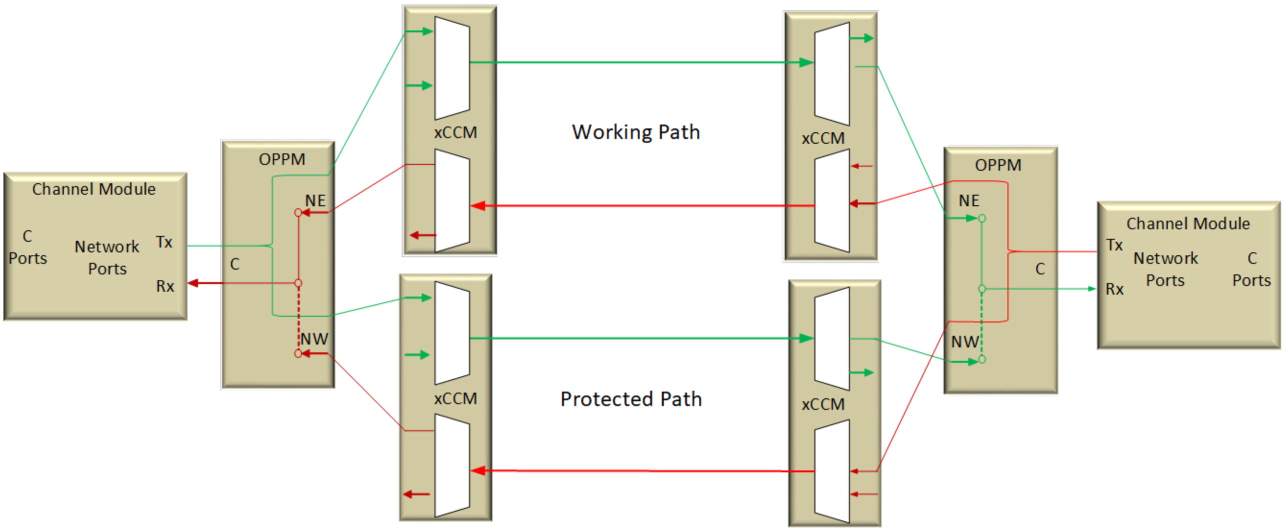
Examples

The diagram in Figure 61 illustrates how OPPM and channel modules in a point-to-point protection application transport up to 100 Gbit services. The OPPM is always located in front of any channel module. These are the three types of switching methods that the OPPM performs for any module types that connect to it:

- Switching is based on OPPM defects like LOS.
- Switching is based on a signal fail feature known as protection trigger partners from a single or group of channel modules.
- Switching takes place on APS, where switching occurs based on the defects from the APS feature of the channel module.

This example shows the use of amplifiers, such as booster, pre-amplifiers, or inline amplifiers, according to node system guidelines.

Figure 61: OPPM: Point to Point Protection Configuration



Return to Connecting OPPM for Point-to-Point Operation

Provisioning OPPM for Point to Point Connection

The goal of this procedure is to provision the OPPM and channel modules for path protection between two nodes. The channel modules use coherent network CFPs. Follow these guidelines to provision working and protected paths.

Equipment

The equipment listed is an example for this use case. Ensure that you popluate all FSP 3000R7 nodes with the basic operational modules. Also make sure that you equip and provision the client interfaces to establish traffic. Your equipment might be different. Refer to your specific design plan.

Client-side optics do not participate in OPPM switching. Only network-side protection triggers exist. OPPM-based protection switching times depend on the channel-module network interfaces. If the channel-module network interfaces are plugs, overall protection switching performance time varies based on the network optics. See the FSP 3000R7 Pluggable Transceiver Module Specification for information about switching times.

Nodes 1 and 2

Follow these guidelines for 10TCE-PCN-16GU+100G modules:

You need:

- One 10TCE-PCN-16GU+100G module for each node.
- Up to ten client SFP+ transceivers. For example, SFP+CDR/11GU/1310S/SM/LC or SFP+CDR/10GU/850I/MM/LC for each node.

- One network CFP coherent transceiver. For example, CFP/112G/#DCTC/SM/LC for each node. The transceiver should be in module-matching neighbor nodes.
- One OPPM for each node.
- Two CSM filters. For example, 96CSM/4HU-#19600-#19125 for each node.

Follow these guidelines for WCC-PCN-100G Family Type modules:

The same processes apply to the WCC-PCN-100GB, WCC-PCN-AES100GB, WCC-PCN-AES100GB-F, and WCC-PCN-AES100GB-G. However, the client interfaces differ for the various module types. You need:

- One WCC-PCN-100G module for each node.
- One client CFP transceiver. For example, CFP/112G/LR4/SM/LC or CFP/112G/SR10/MM/MPO for each node.
- One network CFP coherent transceiver. For example, CFP/112G/#DCTC/SM/LC for each node. Transceiver should be in module-matching neighbor nodes.
- One OPPM for each node.
- Two CSM filters, for example, 96CSM/4HU-#19600-#19125, for each node.

Preparation

You should meet these conditions:

- All modules and transceivers are plugged into the node.
    - If you use plug optics for a Transponder of one client and one network, you need transceivers at each interface.
    - If you use plug optics for a Muxponder of many clients and one network, the minimum requirements is one client and network transceiver.
- The cabling plan shows all internal-node fiber jumpers.Examples Examples, OPPM, and the point-to-point diagram.
- All fiber and cable connections properly connect.

⚠	**CAUTION** Do not enable a network side loopback on an interface protected by the OPPM if that interface is provisioned as a Protection Trigger Partner. This setting will prevent the OPPM from switching.

Complete these steps using NED to provision the modules:

Node 1, Channel module:

1. Select **Configure**.
2. Navigate to the relevant shelf and click **Add Module**.

3. Select the slot. If channel module 10TCE-PCN-16GU+100G or WCC-PCN-100G is plugged in, it is displayed.
4. Click **Add**.
5. Provision the **Client** transceivers:
   - Click **Add**.
   - Select the client port, plug type, and data rate.
6. Provision the **Network** transceiver. Select the coherent type transceiver.
7. Provision the **Client** ports and select the facility.
8. Click **Add**.
9. Provision the **Network** port:Click **Add** to select a channel.

Node 1, OPPM:

1. Select **Configure**.
2. Navigate to the relevant shelf.
3. Click **Add Module**.
4. Select the slot. If OPPM is plugged in, it is displayed.
5. Click **Add**.
6. Navigate to module level and select the **Ports** area.
7. Click **Add** to add client and network ports for NE and NW.
8. Define protection:
   a. Select NE or NW port as the working port.
   b. Set the **Protection Type** and **Protection Switch Mode** as necessary.
      For bidirectional protection switching:
      Set the **Protection Type** to **SNC-N** and
      the **Protection Switch Mode** to **Bidirectional**.
   c. Click **Add**.
   d. Select the protection partner if needed or available. Below Equipment, select the OPPM to add a protection partner. Bidirectional switching is the default setting and applies only if you provisioned protection partners. If you do not use protection partners, the protection switch functions in a unidirectional mode even if you provisioned bidirectional mode.
   e. If you use bidirectional protection switching, select an APS channel partner. Set Assigned APS Channel to a valid protection partner. See the Module and System Specification for a list of channel modules that support APS channels.

Node 2, Channel module:

9. Repeat channel module steps for Node 1.

Node 2, OPPM:

10. Repeat OPPM steps for Node 1.

Provisioning Coherent Colorless Directionless Add-Drop

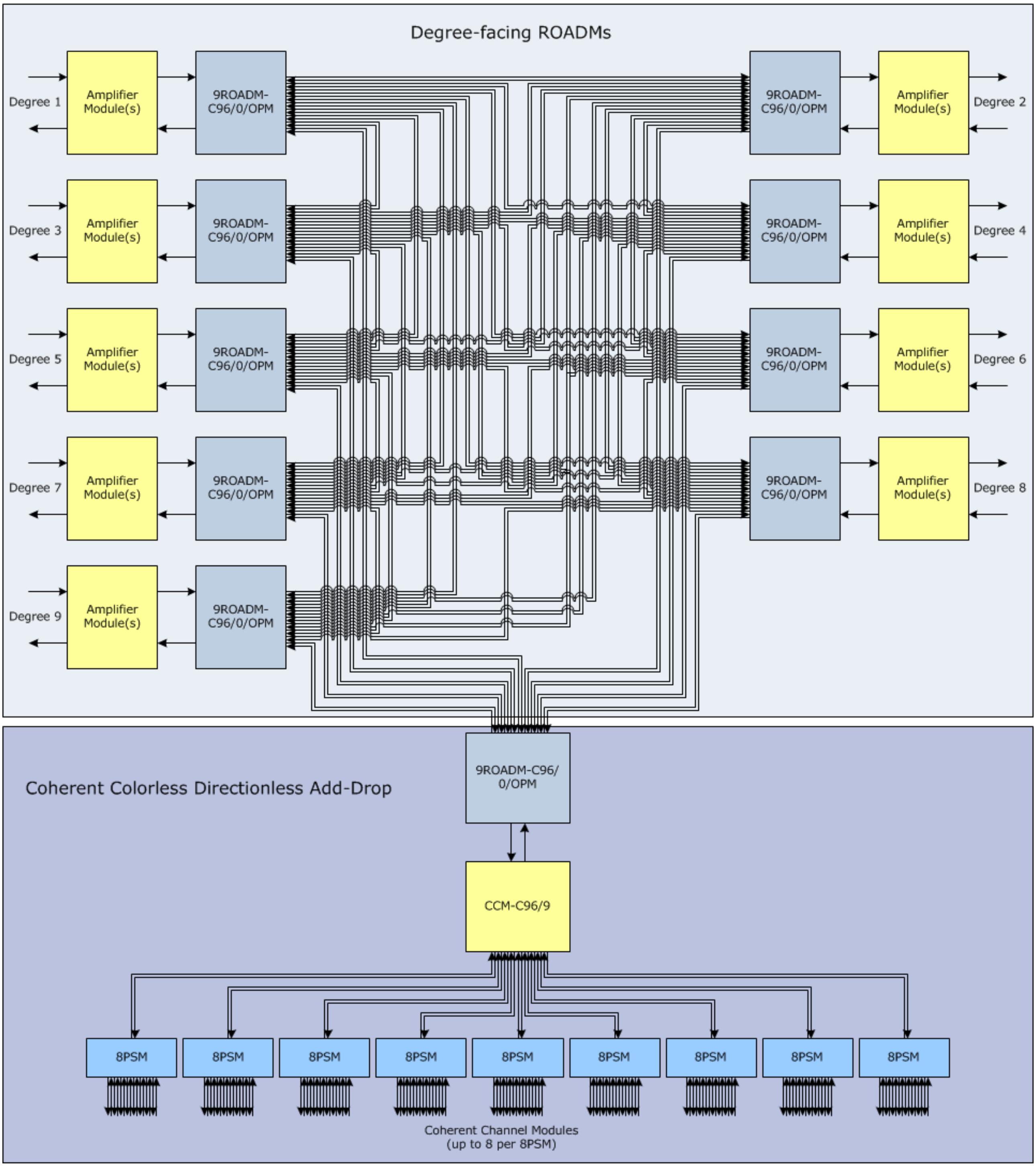
ROADM nodes may support coherent colorless directionless add-drop. A coherent colorless directionless add-drop branch supports up to 72 channels which can be added and/or dropped to any degree. Each channel (wavelength) may only be added once in the branch. This section describes the coherent colorless directionless add-drop supported by 9ROADM-C96, CCM-C96/9 and 8PSM modules. It contains theses topics:

Background Information

ROADM nodes can support various numbers of degrees and directionless or colorless, directionless add/drop branches. For example, the maximum number of degrees and add/drop branches using 9ROADM-C96 modules is 10. The following figure shows a 9-degree ROADM node with one coherent colorless directionless add-drop branch. This configuration supports the maximum number of degrees with eight C ports from each degree-facing 9ROADM-C96 connected to a C port of the other degree-facing 9ROADM-C96 modules. The remaining C port of each degree-facing 9ROADM-C96 is connected to a 9ROADM-C96 used for coherent colorless directionless add/drop, allowing channels to be added and/or dropped from any degree. A coherent colorless directionless add-drop branch supports up to 72 channels.

In the drop direction, the user can selectively route up to 8 channels from the CCM-C96/9 to the 8PSM, which directs the 8 channels to all 8PSM C ports. Each 8PSM C port can be connected to coherent channel modules, which must be provisioned to receive one of the channels. In the add direction, the 8PSM combines the channels from the connected coherent channel modules. The CCM-C96/9 combines all channels from the connected 8PSM modules which are routed to the directionless 9ROADM-C96. The directionless 9ROADM-C96 forwards the channels to the degree-facing 9ROADM-C96 modules. The cross connects on the degree-facing 9ROADM-C96 determine which channels are connected to each degree. You must ensure each coherent channel module in the coherent colorless directionless add-drop branch is provisioned for a different channel.

Figure 62: 9-Degree ROADM Coherent Colorless Directionless Add-Drop



Back to Provisioning Coherent Colorless Directionless Add-Drop.

Requirements

- The node is populated with the required modules, including an NCU-II or NCU-II-P.
- All modules have been added and their admin states are set to **In Service**.

- A fiber (cabling) plan is available.
- Fibers are represented under **Overview > Physical Connections**.
- Amplifier ports have been added and their admin states are set to **In Service**.
- ROADM ports to be used have been added and their admin states are set to **In Service**.
- CCM ports to be used have been added and their admin states are set to **In Service**.
- Channel module network ports to be used have been added and their admin states are set to **In Service**.

Back to Provisioning Coherent Colorless Directionless Add-Drop.

Provisioning

Provisioning equipment to support Coherent Colorless Directionless Add-Drop branches involves provisioning the ROADM, CCM-C96/9, and 8PSM modules, as detailed below.

Provisioning ROADM modules

Provision the ROADM modules, as specified in Provisioning ROADM , including ROADM modules that are part of the coherent colorless directionless add-drop branches.

Provisioning CCM-C96/9 modules

Provision the CCM-C96/9 module in each coherent colorless directionless add-drop branch, as detailed in Provisioning CCM-C96/9.

Provisioning 8PSM modules

Provision the 8PSM as detailed in Adding Modules or Adding Passive Units, depending on placement.

Back to Provisioning Coherent Colorless Directionless Add-Drop.

UTM-S

The UTM-S (Utility Module for 1HU shelves) provides centralized management access to a single network element (NE) in any configuration. It features a telemetry interface (TIF) with dry contacts for 5 opto-isolated alarm input signals and 5 alarm output signals. The use case contains these topics:

Background Information

The telemetry interface enables the user to connect the NE to alarm inputs of other devices of the system or directly control external alarm devices. TIF input and output alarm triggers the acoustic alarm. The alarm status of these input/output alarm signals is visualized to the user via five yellow TIF input LEDs and five yellow TIF output LEDs.

The UTM-S is intended for installation into 1HU shelves (slimline shelves) and is managed by the NCU-S and SCU-S only. It supports a maximum of two 1HU shelves, managed by one NCU-S (SHELF-1) and one SCU-S (SHELF-2). The UTM-S should be placed in the same shelf as NCU-S (SHELF-1).

Refer to Examples.

Refer to UTM-S

Requirements

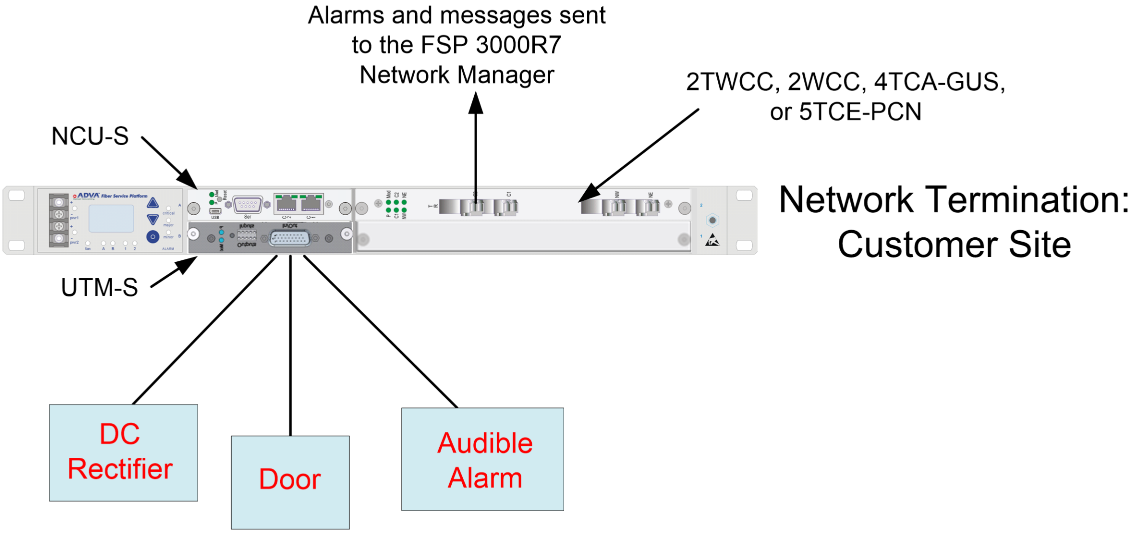
- SH1HU shelf
- One UTM-S
- One NCU-S
- One channel module (2TWCC, 2WCC, 4TCA-GUS, or 5TCE-PCN)
- All fibers and cables are properly connected as specified in the Installation and Commissioning Manual

Back to UTM-S

Examples

Below is an example of how the UTM-S is used in a network.

Figure 63: UTM-S Network Connection



Back to UTM-S

Provisioning TIF Alarms on the UTM-S

Follow this procedure to add the UTM-S module and configure the TIF alarm contacts.

Click each step to view the details of the steps.

Add Module

1. Select **Configure**.
2. Click on the shelf where the module will be installed.
3. Click **Add Module** in the **Main Pane**.
4. Select the slot.
5. Select UTM-S from the equipment list.
6. Select desired **Admin State**.
7. Click **Add**.

Configure Input Telemetry Alarms

1. Click the **Telemetry Input** area in the **Main Pane**.
2. Click **Edit**.
3. Select telemetry alarm 1 through 5.
4. Enter alarm type (door, DC Rectifier, audible alarm, etc) and message.

5. Select alarm logic (alarm when open or closed).
6. Click **Apply & Exit**.

Configure Output Telemetry Alarms

1. Click the **Telemetry Output** area in the **Main Pane**.
2. Click **Edit**.
3. Select output alarm type (NE Minor, PSU Major, etc).
4. Click **Apply & Exit**.

Back to UTM-S

Provisioning ROADM

This section contains these topics:

Node Topologies using ROADM Modules

Nodes that contain ROADM modules, ROADM nodes, can be deployed at any or every location in a network. The ROADM modules are used to add, drop, and/ or pass-through optical channels and control the channel power. ROADM modules are used to reduce power variation across optical channels which can increase the channel reach in a network.

Modules that support transmission of channels to/from a network fiber pair are referred to as a *degree*. The type and number of modules associated with the degree varies, depending on the application. The ROADM module type determines the maximum number of degrees supported.

ROADM modules do not provide equipment protection. If one unit fails, the other module (s) do not automatically take over the traffic of the failed unit. However, end-to-end service path protection, using other unidirectional and bidirectional 1+1 protection mechanisms, is supported.

- ROADM modules support **Mode** and **Number** parameters to specify usage.
- Some ROADM modules support either fixed grid 50 GHz/100 GHz channel resolution or flexgrid with 12.5 GHz channel resolution.
- ROADM modules with the N port connected toward the network fibers must have the mode set to **Degree Fixed**. These ROADM modules are referred to as degree facing.

- ROADM modules with the N port connected to or toward a filter must have the mode set to **Degree Select**. These ROADM modules are referred to as "directionless".

Node topologies using ROADM modules:

- *Fixed add-drop* is a configuration where channel modules are connected to a filter (CSM) which is then connected to a ROADM module C port. The channels can only be routed toward the degree connected to the ROADM N port. Depending on the ROADM module type, 1, 2 or more C ports can be connected to filters. ROADM modules that support 96 channels allow any C port(s) to be used for fixed add-drop. ROADM modules that support 40 or 80 channels must have the filter connected to the C or Cx port (where x matches the ROADM number). When an 8ROADM-C80 is configured with Mode set to "Dual Port Add-Drop" then port C8 can also be connected to a filter that supports channels with channel numbers that end with 5 (19xx5).
- *Directionless add-drop* (also called *Steerable add-drop*) is a configuration where channel modules are connected to a filter (CSM) which is then typically connected through an amplifier to a directionless ROADM module N port. The Client ports of a Degree Select ROADM module are connected to the Client ports of each Degree Fixed ROADM in the node. The Degree Select ROADM module is used to “steer” or direct a channel from a channel module to any degree. Cross Connects determine the channel routing. Steerable (Directionless) nodes have a minimum of three ROADM modules.
- *Coherent, Colorless add-drop* is a configuration where xPSM (5PSM and 8PSM) and xPSMy (16PSM4, 16PSM8 and 8PSM8) modules are used in a fixed add-drop configuration.
- *Coherent, Colorless, Directionless add-drop* is a configuration where xPSMy (16PSM4, 16PSM8 and 8PSM8) modules are used in a fixed add-drop configuration. This configuration requires the channel modules to have coherent receivers (for example, WCC-PCTN-100GB and 10TCC-PCTN-10G+100GB modules).

The different topologies can be used alone or in combination. However, only ROADM modules of the same type can be interconnected.

Provisioning a ROADM Channel

Add a ROADM channel as follows:

> ROADM and CCM modules require optical channel power to be present for proper operation. Therefore, channel modules must be set as follows when the channel passes through ROADM or CCM modules:
>
> - **Auto Laser Shutdown** must be set to **Disable**
> - **Error Forwarding Mode** must not be set to **Laser Off**.
>
> These parameters can cause the channel module laser to be turned off.

1. If necessary, add ROADM modules to each node where the channel will be added, passed through or dropped, as detailed in Adding a ROADM Module.
2. If necessary, add the required ports to each ROADM module the channel enters or exits to reach its destination, as detailed in Adding a ROADM Port.
   - Required ports include: Network (N), Upgrade (U), and Client (C).
   - Add-Drop channels require the N port and C port at which the channel is added/dropped.
   - Pass-through and Steerable Add-Drop channels require two N ports and two U or C ports.
3. Ensure the administrative state of the module(s) and ports associated with the channel are set to "In Service".
4. Add the channel, as detailed in Adding an Optical Channel.
5. Some ROADM modules support Fiber Detection. Refer to Provisioning Fiber Detection to modify the Fiber Detection settings for these ports, if needed.

> Any add operation may be aborted by selecting Cancel.

Adding a ROADM Module

1. Select **Configure**.
2. In the **Navigation Tree**, right-click on the shelf where the ROADM module will be located, and select **Add Module**.
3. In the Add Module window, select **Slot**, and then select the **Equipment** type.

Selection of the desired module may not be possible if the required slots are unavailable to support the module.

4. Refer to your network plan to set the additional options that appear based on the ROADM type you selected.

5. Click **Add**.

Adding a ROADM Port

1. Select **Configure**.
2. In the **Navigation Tree**, select the ROADM module.
3. Click the **Ports** area to display and/or add ROADM ports.
4. Click **Add**.
5. In the Add window, select the relevant port from the **Port** list.
6. Additional options appear based on the port type. Refer to your network plan to configure these options.

7. Click **Add**.

Adding an Optical Channel

ROADM devices support pass-through, fixed add-drop, and steerable (directionless) add-drop optical channels.

1. Select **Configure**.
2. In the **Navigation Tree**, click the ROADM module.
3. Select the **Optical Channels** area to add the channel.
4. Click **Add End Point**.
5. In the Add facility window, select the relevant port from the **Port** list.
6. Choose the channel from the **Channel** menu, based on your network plan.
7. Additional options appear based on the port type. Configure them according to your network plan.
8. Click **Add** to activate your settings.
9. Repeat the above steps for the end point on the other port.

The other port may be on a different module for **Pass-through** and **Steerable Add-Drop** channels for some ROADM types.

10. Click **Add Connection**.
11. In the Wizard for Cross Connection window, select the **Direction** as follows:
    - **(A) <-> (B)** signifies a bidirectional connection.
    - **(A) -> (B)** signifies a unidirectional connection.

12. Select the connection type based on your network plan.

13. If the **Channel Number** is accessible, select the desired channel number.
14. Refer to your network plan to configure additional options that appear.
15. Click **Add**.
16. Click **Edit**, then expand the "+" sign adjacent to the desired channel to display the **Admin State** for the associated channel components.
17. Set the **Admin State** for each channel component to **In Service** and click **Apply**.
18. The following actions take place upon successfully adding and enabling a channel:
    - The path is established.
    - The system attempts to adjust the channel power based on the set-point and tilt provisioned on the N port.
    - Alarms are enabled.
    - Performance Monitoring is enabled.

Adding an Optical Channel in 96-channel ROADM modules

ROADM devices support pass-through, add and drop optical channels. Steerable (Directionless) ROADM Add/Drop configurations are supported by the **Steerable Add-Drop** selection when the channel is added. See Node Topologies using ROADM Modules for more information about Steerable (Directionless) ROADMS. This procedure adds an optical channel in a single step through one or two 96-channel ROADM modules.

This procedure applies to 9ROADM-C96, 4ROADM-C96 and 4ROADM-E-C96 modules.

You can select the channel configuration:

BIDIRECTIONAL

- (A) <--> (B) **Pass-Through**
- (A) <--> (B) **Add-Drop**
- (A) <--> (B) **Steerable Add-Drop**

UNIDIRECTIONAL

- (A) -> (B) **Pass-Through**
- (A) -> (B) **Add**
- (A) -> (B) **Drop**
- (A) -> (B) **Steerable Add**
- (A) -> (B) **Steerable Drop**

Requirements

For the following procedure to work, fiber map connections (PTPs) between ROADM C ports must be entered in Physical Connections.

1. Select **Configure**.
2. Navigate to the relevant slot in the **Navigation Tree**.
3. Click the **Optical Channels** area.
4. Click **Add**. The optical channel window is displayed.

   Using your network plan:

5. Select the **Add Channel** type from the list.
6. Select either the **Local Port** or the port it will be linked to **(Linked Port)**.
7. Select the **Channel**.
8. Select the **Node in Path** for each direction.
9. Click **Add**.

Configuring the Individual Wavelength Set-Point Delta

You can establish the set-point per individual channel as a positive or negative deviation from the set-point set on the network port of the reconfigurable optical add-drop multiplexer (ROADM) device. The range is –6dBm to +6dBm, and 0.0 dBm indicates no deviation from the network value.

1. Select **Configure**.
2. In the **Navigation Tree**, click the ROADM module whose wavelength you want to adjust.
3. Select the **Optical Channels** area.
4. Ensure that you select the N port (for example, OM-1-9-N).
5. To select the channel to adjust it, click that row.
6. In the details window, **Channels** area, change the **Setpoint Delta** to the applicable value.
7. Select **Apply**, and then **Exit**.
8. To equalize the channel, select **Go To**, and then **Maintain**.

9. Select the **Optical Channels** area.
10. To select the channel to adjust it, click that row.
11. Select **Equalize**.

Provisioning Fiber Detection

1. Select **Configure**.
2. In the **Navigation Tree**, click the module.
3. Click the **Fiber Detection** area to display ports supporting Fiber Detection.
4. Click the row corresponding to the desired port.
5. In the **Details View**, modify options according to your network plan.
6. Click **Apply & Exit** to activate your settings.

Provisioning a ROADM with Internal Amplifier

Provision a ROADM with an internal amplifier as follows:

> ROADM and CCM modules require optical channel power to be present for proper operation. Therefore, channel modules must be set as follows when the channel passes through ROADM or CCM modules:
>
> - **Auto Laser Shutdown** must be set to **Disable**
> - **Error Forwarding Mode** must not be set to **Laser Off**.
>
> These parameters can cause the channel module laser to be turned off.

1. Follow the procedure for Provisioning a ROADM Channel.
2. The amplifier is automatically added to the ROADM module. Adjust the amplifier gain as indicated in Adjusting the Amplifier Gain in a ROADM.
3. Some ROADM modules support fiber detection. Refer to Provisioning Fiber Detection to modify the Fiber Detection settings if needed.

Adjusting the Amplifier Gain in a ROADM

1. Select **Configure**.
2. In the **Navigation Tree**, click the ROADM module.

3. Click the **Amplifier** area to display the amplifier in this ROADM.
4. If the gain needs to be reduced due to a high input power and span equalization is not being used, click the row with the amplifier.
5. In the **Details View**, set **Admin State** to **Management**.
6. Click **Apply** to activate the **Admin State** change.
7. Set **Gain** per your network plan.
8. Click **Apply** to activate the **Gain** setting.
9. Set **Admin State** to the original setting.

10. Click **Apply & Exit**.

Provisioning an MROADM with MTP Amplifier

Provision a MROADM with an internal amplifier as follows:

> MROADM and CCM modules require optical channel power to be present for proper operation. Therefore, channel modules must be set as follows when the channel passes through MROADM or CCM modules:
>
> - **Auto Laser Shutdown** must be set to **Disable**
> - **Error Forwarding Mode** must not be set to **Laser Off**.
>
> These parameters can cause the channel module laser to be turned off.

1. Follow the procedure for Provisioning a ROADM Channel.

2. The amplifier is automatically added to the ROADM module. Adjust the amplifier gain as indicated in Adjusting the Amplifier Gain in a ROADM.
3. Some ROADM modules support fiber detection. Refer to Provisioning Fiber Detection to modify the Fiber Detection settings if needed.

Provisioning a Multicast Optical Channel

Multicast optical channels may be provisioned on 4ROADM-C96, 8ROADM-C40, 8ROADM-C80, and 9ROADM-C96 modules.

- On 8ROADM-C40 and 8ROADM-C80 modules, multicast channels are provisioned by creating unidirectional connections between network ports of the respective ROADMs (between multiple nodes).

- On 4ROADM-C96 and 9ROADM-C96 modules, multicast channels are provisioned by creating unidirectional connections between the network port and multiple client ports on the same ROADM module.

Follow these steps to provision a multicast optical channel:

1. Follow the procedure for Provisioning a ROADM Channel, except the **Direction** must be (A) -> (B) .
2. Add all of the required ports on the ROADM modules the multicast channel passes through: network (N), upgrade (U) and client (C) based on your application.
3. Proceed to Adding a ROADM Port to add each port for the multicast channel.
4. Add the channel for each unidirectional path in the multicast channel setup, as detailed in Adding an Optical Channel.

> For multicast optical channels, the same channel is assigned on all of the required ports.

5. Add unidirectional connections, as detailed in Adding an Optical Channel

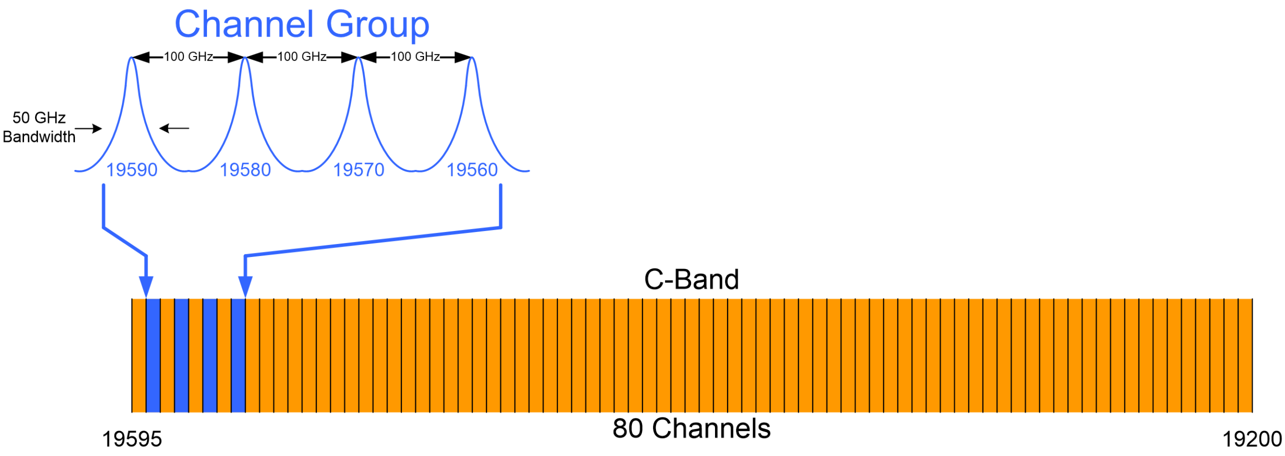
Provisioning an Enterprise 100 Gbps Service through a Network

This section describes how to provision Enterprise 100 Gbps channel modules, ROADM modules, and optical lines to support services from Enterprise 100 Gbps channel modules. It contains these topics:

Background Information

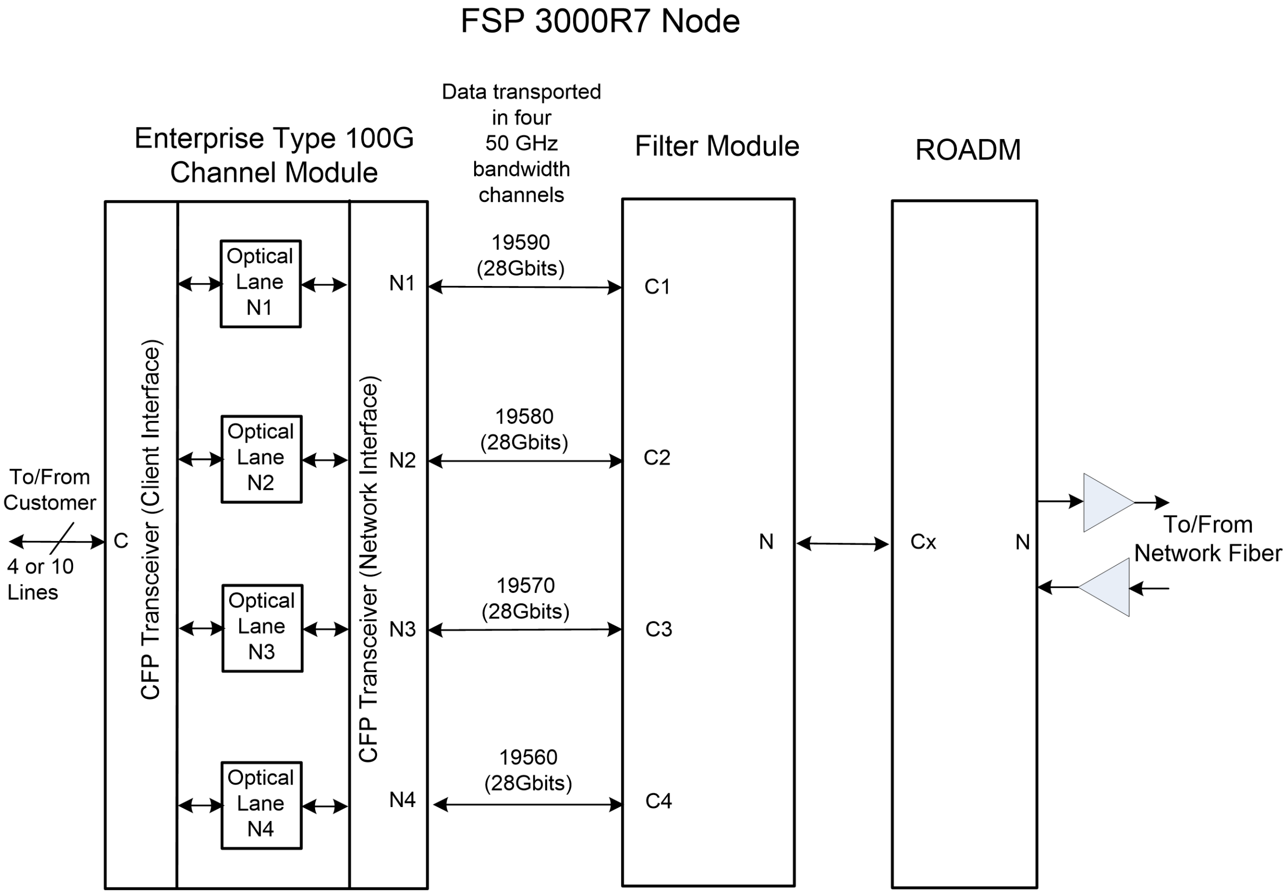
Some Enterprise channel modules support a 100 Gbps service which have four optical channels (or lanes). These four channels are referred to as a channel group. The channel group must follow the same path through the node and network path. The channels within the channel group are 100 GHz spaced and have a bandwidth of 50 GHz. All four channels must be available through the node and network path to support the channel group. Simplified provisioning for channel groups is supported on ROADM modules and optical lines.

Figure 64: Channel Grouping Example



A channel group originates at a 100 Gbps Enterprise channel module. The filter module combines the four channels onto a single fiber. If the path contains a ROADM, then the channels can be provisioned as a channel group through the ROADM modules. A channel group can also be provisioned on optical lines to indicate channel usage on network fibers. The diagram below shows the four 28 Gbps (including payload and overhead) channels supported and routed to the network fiber at the add or drop nodes.

Figure 65: Channel Group Flow Diagram



Provisioning an Enterprise 100 Gbps Service through a Network

Provisioning an Enterprise 100 Gbps Channel Module

Follow this procedure to provision an Enterprise 100 Gbps channel module:

1. Add the Enterprise 100 Gbps channel modules to the nodes where service will be added and dropped, as detailed in Adding Modules.
2. Add the N plug , select parameters as specified by your network plan.
3. Add the C plug(s), select parameters as specified by your network plan.
4. Add the N port, select parameters as specified by your network plan.
5. Add the C port(s), as specified by your network plan.
6. If necessary, add the data channel(s).
7. If a management channel will be used, add the management channel as specified by your network plan.

Provisioning an Enterprise 100 Gbps Service through a Network

Provisioning a Channel Group on a ROADM

> A service supported by a channel group requires:
>
> - Enterprise 100 Gbps channel modules to be provisioned at the service endpoints (see Provisioning 100G Enterprise Channel Modules).
> - Filter modules to be provisioned at the service endpoint nodes, as outlined in Adding Modules or Adding Passive Units.

Follow this procedure to provision a channel group on a ROADM:

1. If necessary, add ROADM modules to each node where the channel group will be added, passed through, or dropped, as detailed in Adding a ROADM Module.
2. If necessary, add the required ports to each ROADM module that the channel group enters or exits to reach its destination, as detailed in Adding a ROADM Port.
    - Required ports include: Network (N), Upgrade (U), and Client (C).
    - Add-Drop channels require the N port and C port at which the channel is added/dropped.
    - Pass-through and Steerable Add-Drop channels require two N ports and two U or C ports.

3. Ensure the Admin state of the module(s) and ports associated with the channel group are set to "In Service."
4. Provision the Channel Group, as detailed in Adding a Channel Group on a ROADM .

Provisioning an Enterprise 100 Gbps Service through a Network

Adding a Channel Group on a ROADM

1. Select **Configure**.
2. In the **Navigation Tree**, click the ROADM module.
3. Select the **Optical Channels** area.
4. Click **Add End Point**.
5. In the Add window, select the relevant port from the **Port** list.
6. Select the **Channel Group** check box.
7. Select the **Channel** number associated with the first channel of the group.
8. Additional options appear based on the port type. Configure them according to your network plan.
9. Click **Add** to activate your settings.

   Expanding the "+" sign next to this row displays the 4 optical channels in this channel group.

10. Repeat the above steps to add the channel group on the other port, which may require navigating to another ROADM module.
11. Click **Add Connection**.
12. In the Add window, select the **Direction** as follows:
    - **(A) <-> (B)** signifies a bidirectional cross connection.
    - **(A) -> (B)** signifies a unidirectional connection.
13. Select the **Channel Group** check box.
14. Select the connection type based on your network plan.
15. Select the **Channel** number associated with the first channel of the group. If the channel number is not available, one or more of the channels resources in the group is in use. Another path must be determined or resources de-provisioned to continue. If the **Channel Number** is accessible, select the desired channel number.
16. Refer to your network plan to configure additional options that appear.
17. Click **Add**.

    The individual channels for the channel group are listed in the **Optical Channels** area.

18. Click **Edit**, and then expand the "+" sign adjacent to the desired channel to display the **Admin State** for the associated channel components.
19. Set the **Admin State** for each channel component to **In Service** and click **Apply & Exit**.
20. If the channel group spans two ROADM modules, return to the first ROADM module and repeat steps 18 to 19.

Provisioning a Channel Group on a ROADM

Adding an Optical Channel Group on an Optical Line

> This procedure is optional, but allows the channels present on an Optical Line to be displayed for easy reference when needed:
>
> - Enterprise 100 Gbps channel modules must be provisioned at the service endpoints (see Provisioning 100G Enterprise Channel Modules).
> - Filter modules must be provisioned at the service endpoint nodes, as outlined in Adding Modules or Adding Passive Units.
> - If present, ROADM modules in the path between the Enterprise 100 Gbps channel modules must be provisioned.

1. Select **Configure**.
2. In the **Navigation Tree**, select **Optical Lines**.
3. Select the **Optical Channels** area.
4. Click **Add End Point**.
5. In the Add Endpoint window, select the relevant port (Optical Line) from the **Port** list.
6. Select the **Channel Group** check box.
7. Select the **Channel** number associated with the first channel of the group.

   You may enter information to identify the channel for future reference in the **User Label** field.
8. Click **Add**.

   Expanding the "+" sign next to this row displays the 4 optical channels in this channel group.

9. Repeat the above steps to add the channel group on the other Optical Line.

10. Click **Add Connections**.
11. In the Add window, select the **Direction** as follows:
    - **(A) <-> (B)** signifies a bidirectional cross connection.
    - **(A) -> (B)** signifies a unidirectional connection.

13. Select the **Channel Group** check box.
14. Select the connection type based on your network plan.
15. Select the **(A) Optical Line**.
16. Select the **Channel** number associated with the first channel of the group.
17. Select the **(B) Optical Line**.
18. Select the **Channel** number associated with the first channel of the group.

19. Click **Add**.

Provisioning a Channel Group on a ROADM

Delete this text and replace it with your own content.

Provisioning CCM-C96/9

Provision a CCM-C96/9 module as follows:

> CCM-C96/9 modules must be installed in SH9HU shelves.
>
> CCM-C96/9 does appear in the **Equipment** list when the slots required to install the module are not available based on the selected slot.

> ROADM and CCM modules require optical channel power to be present for proper operation.Therefore, channel modules must be set as follows when the channel passes through ROADM or CCM modules:
>
> - **Auto Laser Shutdown** must be set to **Disable**.
> - **Error Forwarding Mode** must not be set to **Laser Off**.
>
> These parameters can cause the channel module laser to be turned off.

1. If necessary, add the CCM-C96/9 module, as detailed in Adding Modules.
   All network and client ports of the CCM-C96/9 module are automatically added.

2. Ensure the **Admin State** of the module and ports associated with the channel are set to **In Service**.
3. Add the channel, as detailed in Adding Optical Channels in CCM-C96/9 Modules.

Adding Optical Channels in CCM-C96/9 Modules

1. In the **Navigation Tree**, click the CCM-C96/9 module.
2. Select the **Optical Channels** area.
3. Click **Add End Point**.
4. In the Add End Point window, select the N port from the **Port** list.
5. Select the channel from the **Channel** list, based on your network plan.
6. Click **Add**.
7. Click **Add End Point**.
8. In the Add End Point window, select the C port from the **Port** list, based on your network plan.
9. Select the channel from the **Channel** list, based on your network plan.
10. Click **Add**.
11. Click **Add Connection**.
12. In the Add Connection window, select the **Direction**:
    - **(A) <-> (B)** signifies a bidirectional connection (both add and drop)
    - **(A) -> (B)** signifies a unidirectional connection (either add or drop)
      If **Direction** is **(A) -> (B)**, select **Add** or **Drop** based on your network plan.
13. Click **Add**.
14. Click **Edit**, then expand the "+" sign adjacent to the desired channel to display the **Admin State** for the channel components.
15. Set **Admin State** for each channel component to **In Service** and click **Apply**.
16. Repeat steps 3 to 15 for each channel to be provisioned on the CCM-C96/9.

> The following actions take place upon successfully adding and enabling a channel:
>
> - The optical path for the channel is established.
> - The module attempts to adjust the channel power to the set-point provisioned on the C port.
> - Alarms are enabled.
> - Performance Monitoring is enabled.

Provisioning 100G Enterprise Channel Modules

Follow this procedure to provision 100G Enterprise channel modules:

1. Add the 100G Enterprise channel module at the designated node, as described in Adding Modules
2. Add plugs for the client and network ports, as described in Adding Plugs.

> For DWDM transport, the network port on these modules requires four channels that are spaced 100 GHz apart. These channels are referred to as a **Channel Group**. The first lane channel selected determines the **Channel Group**. Select the first lane channel according to your network plan.

3. Add ports, as described in Adding Ports.
4. If necessary, add data channels, as detailed in Adding Data Channels.

Provisioning Optical Amplifiers

Background Information

Optical amplifiers include EDFA and RAMAN amplifiers. Most optical amplifiers support setting the amplifier gain, while some amplifiers also allow the tilt across the band to be specified.

Provisioning Optical Amplifiers

1. Select **Configure**.
2. Select the **Shelf**for the amplifier in the **Navigation Tree**.
3. Click **Add Module**.
4. In the Add Module on Shelf window:
   a. Select the **Slot** for the amplifier.
   b. Select the desired optical amplifier type from the **Equipment** list.
   c. Click **Add**.

Provisioning a RAMAN-C10

If the node contains a RAMAN-C10 module which has a Raman amplifier, it must be calibrated with the network fiber before being used. This section explains how to perform the Raman amplifier calibration process. The two nodes at each end of the fiber span are referred to as Node A and Node B.

This section contains these topics:

Background Information

Raman amplifiers utilize the network fiber to amplify the incoming optical signal.

Part of the Raman amplifier provisioning process is to build the Amplified Spontaneous Emission (ASE) table which is stored on the RAMAN-C10 module. The ASE table is used for performance monitoring and to estimate the Raman amplifier gain. To build the ASE table, the fiber span must only contain the OSC signal. While building the ASE table, infra-red light is driven into the network fiber. Without the ASE table, the Raman amplifier will not become operational.

> A fiber span that does not contain any channel except the OSC is referred to as “dark” in the following sections.

During system operation, the RAMAN-C10 module subtracts the noise power level stored in the ASE table to calculate the optical power in the fiber span.

> **NOTICE**
>
> Raman amplifiers output high power levels. Always disable Raman amplifiers before removing fiber-optic cables. Failure to disable Raman amplifiers can result in damage to the optical connector. On the RAMAN-C10, the amplifier is controlled by Admin state of the N port.

"Forced On" Mode

The OSC signal is amplified when the Raman amplifier is on. The Raman amplifier has a special mode where it can be forced on. All relevant safety checks are performed to ensure laser safety class 1M operation. If the optical path to the network fiber is open, the Raman amplifier will not operate, the detected back reflection will be too high and the OSC signal will not be detected.

This "forced on" mode is useful when the ASE table build fails because of the following:

- The fiber span is not dark.
- The OSC is the only method to communicate with the remote NE where the channels must be shut down.
- The OSC requires additional gain to support communication to the remote NE.

You may use the OSC connection to shut down channels preventing ASE table generation, then generate the ASE table. Without this mode, a technician would be required at the remote site to shut down the channels.

The "forced on" mode can also be used to verify the cabling is correct by sending light to the other end of the fiber span for detection.

Requirements

- The following equipment is required at each node:
  - RAMAN-C10 amplifier module
  - Optical Supervisory Channel Module (OSCM-PN) with an SFP (SFP/FE/D1528.77.SM/LC)
  - An EDFA amplifier (pre-amplifier)
  - An EDFA amplifier (post-amplifier)
  - Channel Module
- All modules are installed according to the planning document and Installation and Commissioning Manual.
- All ports and fiber-optic connectors are cleaned before making connections. Fiber-optic connectors must be cleaned before every connection.
- When ROADM equipment is used, channels and cross-connects may be provisioned but the cross-connects' Admin state must be disabled.
- Far-end post-amplifier Admin state must be set to Disable before and during the calibration process for the near-end Raman amplfier.

> When using Raman amplification, minimize the number of Fiber Distribution Panels (FDPs) to reduce fiber loss and back reflections.

> Raman amplifiers use the network fiber as the gain medium and must be longer than 40 km. The RAMAN-C10 N port must be connected to the network fiber for calibration and operation.

> Raman amplifiers require the discrete back reflection levels to be below -32 dB. The network fiber and FDP must have discrete back reflection levels below -27 dB. The back reflection levels can be measured with an optical time-domain reflectometer (OTDR). Higher back reflection levels cause BER penalties due to in-band crosstalk generated by multi-path interference. OTDR measurements need to be made with a fiber spool having a length exceeding the OTDR measurement “dead-zone”. One end of the fiber spool is connected to the OTDR and the other end to the FDP. The fiber spool is required to make reliable back reflection and loss measurements. OTDR measurements should be made for both network fibers.

> When using RAMAN-C10 amplifiers, discrete loss elements such as connectors on fiber-optic cables, patch panels, or fiber splices should total less than 2.0 dB in the first 20 km of fiber connected to the Raman amplifier.
>
> Losses higher than 2.0 dB from the discrete loss elements can prevent Raman amplifier operation, to prevent connector damage and to ensure the gain in the network design can be reached.

Provisioning a RAMAN-C10

Follow these steps to provision a RAMAN-C10. The two nodes at each end of the fiber span are referred to as Node A and Node B.

1. Setup the RAMAN-C10 at Node A, proceeding in the **Node B -> Node A** direction. Execute these procedures in the sequence specified, noting that Node A is the **near-end** node, while Node B is the **far-end** node:
    a. Establishing an OSC Connection
    b. Verifying the Fiber Span is Dark
    c. Building the ASE Table
    d. Enabling the Amplifier
2. Setup the RAMAN-C10 at Node B, proceeding in the **Node A -> Node B** direction. Execute these procedures in the sequence specified, noting that Node B is the **near-end** node, while Node A is the **far-end** node:

   a. Establishing an OSC Connection
   b. Verifying the Fiber Span is Dark
   c. Building the ASE Table
   d. Enabling the Amplifier

3. Once the RAMAN-C10 modules are activated in both directions, enable the channel modules as described in Enabling Channel Modules.

Establishing an OSC Connection

The two nodes are connected at each end of the fiber span as shown below.

- When setting up the Raman amplifier at Node A, Node A is the **near-end** node, while Node B is the **far-end** node.
- When setting up the Raman amplifier at Node B, Node B is the **near-end** node, while Node A is the **far-end** node.

Figure 66: Network Diagram

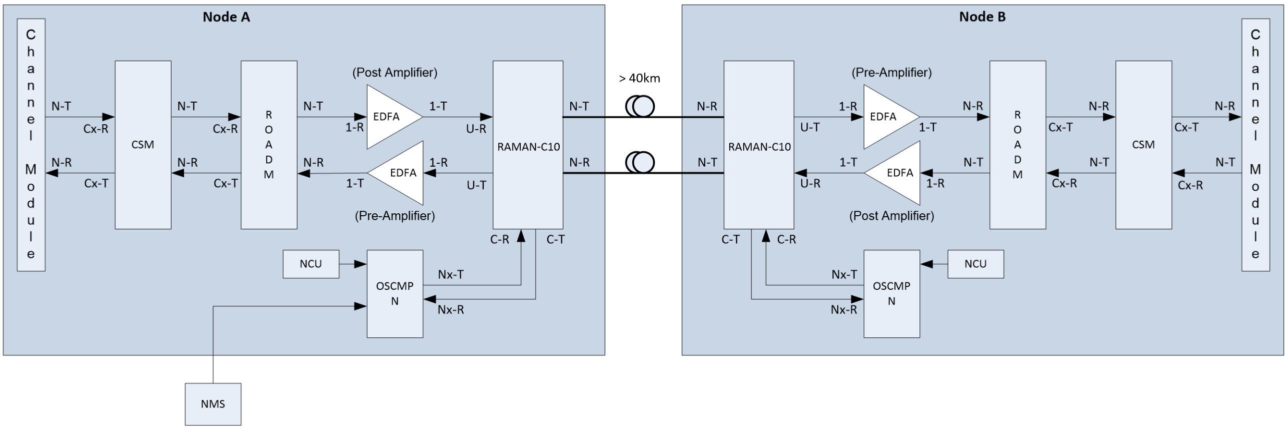
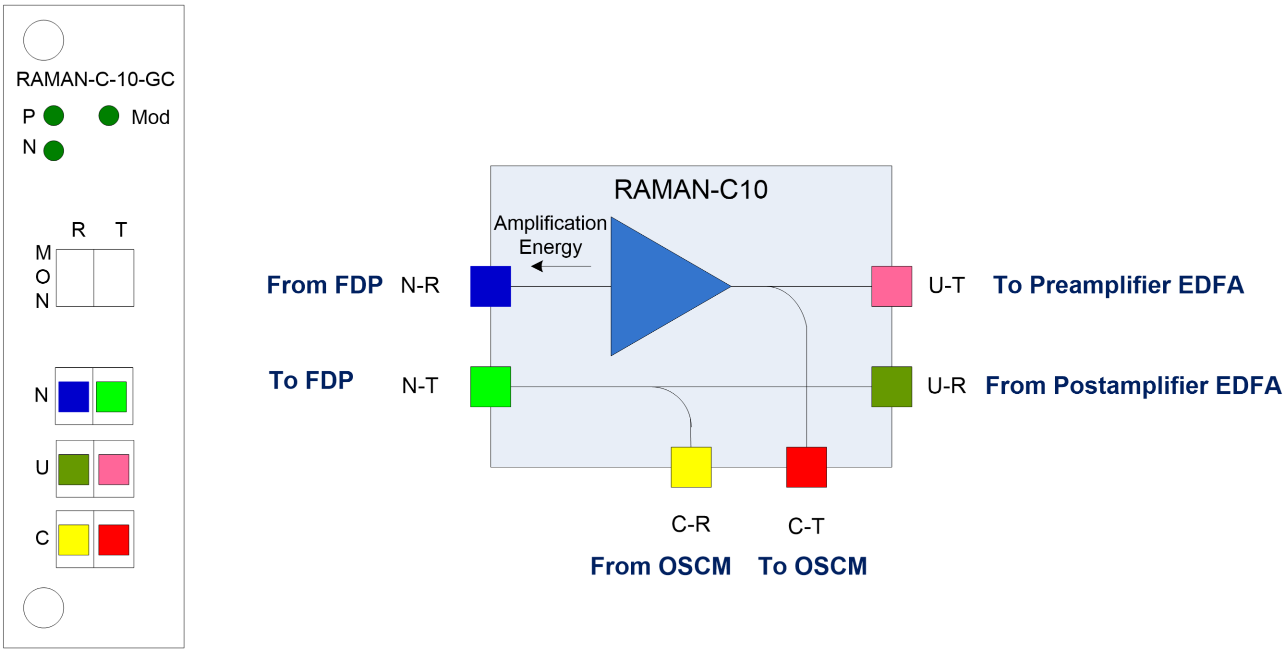


Figure 67: Raman Connection Diagram



> If the OSC power is too low to establish OSC communication between the two nodes, use the Raman amplifier Force On mode.

To establish an OSC connection:

1. **Far-end Node**: Prepare the OSCM.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   c. In the **OSC Ports** area, select the corresponding N port (NW or NE).
      The Configure Details window for the N port opens.
   d. Set the **Admin State** to **Maintenance**, then click **Apply**.
   e. Set the **Auto Laser Shutdown** to **Disable**, then click **Apply & Exit**.
   f. Verify the OSC channel is 19610 (1528.77 nm) on the corresponding N port.
   g. Select **Monitor**.
   h. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   i. In the **Ports** area, **Current** tab, view the **OPT** value for the N port.
      The optical power transmitted by the OSCM-PN can be from +2 to +7 dBm.
   j. Verify the N port is OSCM port is +2 to +7 dBm.

2. **Far-end Node:** Disable the post-amplifier.
    a. Select **Configure**.
    b. In the **Navigation Tree**, select **Shelf > Post-amplifier** slot.
    c. In the **Ports** or **Amplifier** area, select the N port or amplifier.
    The Configure Details window for the port opens.
    d. Set the **Admin State** to **Disabled**, then click **Apply & Exit**.

3. **Far-end Node**: Place the Raman amplifier in maintenance mode.
    a. In the **Navigation Tree**, select **Shelf > Raman** slot.
    b. In the **Ports** area, select the N port.
    The Configure Details window for the N port opens.
    c. Set the **Admin State** to **Maintenance**, then click **Apply & Exit**.

4. **Near-end Node**: Place the Raman amplifier in maintenance mode.
    a. Select **Configure**.
    b. In the **Navigation Tree**, select **Shelf > Raman** slot.
    c. In the **Ports** area, select the N port.
    The Configure Details window for the N port opens.
    d. Set the **Admin State** to **Maintenance**, then click **Apply & Exit**.

5. **Near-end Node**: Check OSC receive power.
    a. Select **Monitor**.
    b. In the **Navigation Tree**, select **Shelf > Raman** slot.
    c. In the **Ports** area, select **OSC**.
    OSC Power Rx is displayed for the N port.

6. **Near-end Node**: Verify the OSC is present at the desired OSCM port.
    a. Select **Monitor**.
    b. In the **Navigation Tree**, select **Shelf > OSCM** slot.
    c. In the **Ports** area, **Current** tab, verify the **OPR** value for the N port is greater than **-45 dBm**.

    The OSC has now been verified in the **far-end node -> near-end node** direction.

> If you disable the OSCM-PN port, a warning message appears: “Disabling the port may cause loss of management connectivity to remote nodes. Note: laser will remain on. Do you wish to continue? [Apply | Cancel]”.

Verifying the Fiber Span is Dark

To build an ASE table, only the OSC can be present (In-Service).

> Ensure the far-end post-amplifier Admin state is disabled, to prevent damage to the optical connectors.

1. **Near-end Node**: Connect an OSA to the network fiber to be connected to the RAMAN-C10 module N port receive (N-R).
2. **Near-end Node**: Verify only the OSC signal (1528.77 nm) is present.

Building the ASE Table

Build an ASE table at the near-end node to operate the Raman amplifier. If you change the Raman amplifier performance, rebuild the ASE table to overwrite the existing one.

Requirements

- Connect the RAMAN-C10 module U-T port.
- Disable the post amplifier module N port or amplifier administrative state at the far-end node.
- Set the post amplifier N port or the far-end node amplifier admin state to **Disabled**.

Procedure

1. Ensure the back reflection is less than the threshold.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf** > **RAMAN-C10**.
   c. In the **Ports** area,**Current** tab, select **Tresholds** and **Interface**.
      The **Back Reflection Rx** level displays for the N port.
   d. Ensure that the back reflection is less than the **High Threshold**.
2. Build the ASE table.
   a. Select **Maintain**.
   b. In the **Navigation Tree**, select **Shelf** > **RAMAN-C10**.
   c. In the **Port** area, **Calibrate** section, click **Start**.

> If an ASE table already exists for this Raman amplifier link, a dialog opens.
>
> Complete one of these actions.
>
> - To rebuilt the ASE table, click **Apply**. The system overwrites the existing ASE table. Continue with the next step.
> - Click **Cancel** to use the existing ASE table.

3. Verify the new ASE table build.
    a. Select **Alarm**.
    b. In the **Navigation Tree**, select **Shelf** > **RAMAN-C10**.
    c. In the **Main Window**, select **Include Not Reported**.
    If the system raises any of the following alarms against the RAMAN-C10 module N port, the ASE table build fails.
        - Pump Shutdown (ASE Low)
        - ASE Table-Fail (ASE Low)
        - ASE Table-Fail (BR)
        - ASE Table-Fail (OSC)
        - ASE Table-Fail (Signal)
        - ASE Table-Not Available
    d. Refer to the Maintenance and Troubleshooting Manual, Appendix A, to resolve these alarms.
4. Verify Raman pump power.
    a. Select **Monitor**.
    b. In the **Navigation Tree**, select **Shelf** > **RAMAN-C10**.
    c. In the **Ports** area, **Current** tab, select **Pump**.
    Pump Power displays for the N port.

Enabling the Amplifier

Once the ASE table is built and the 'ASE Table-Not Available' alarm has cleared, follow this procedure to turn on the post-amplifier, if applicable, and verify the amplifier configuration.

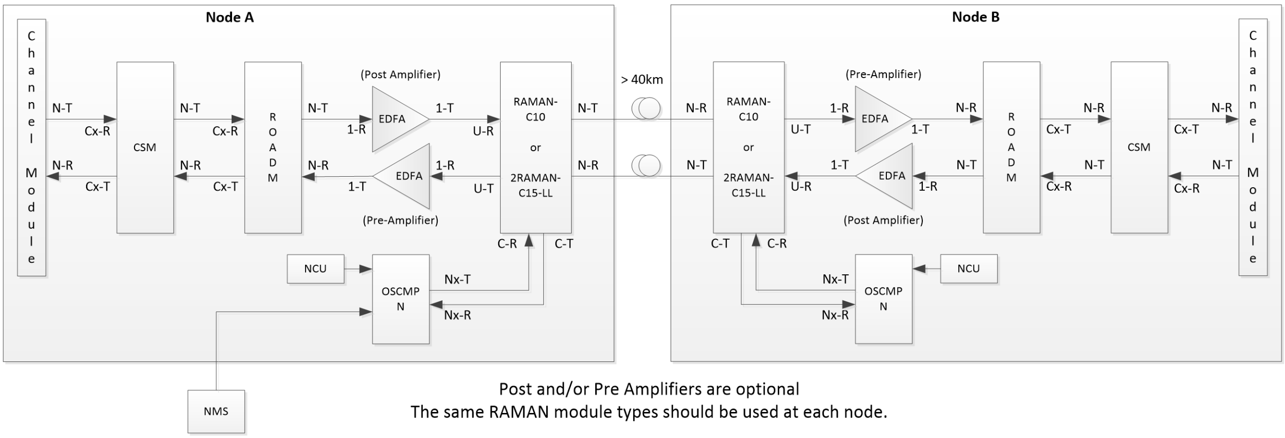
1. **Far-end Node**: Enable the post-amplifier, if applicable.
    a. Select **Configure**.
    b. In the **Navigation Tree**, select **Shelf > Post-amplifier** slot.
    c. In the **Ports** or **Amplifier** area, select the N port or post-amplifier.
    The Configure Details window for the port or amplifier opens.
    d. Set the **Admin State** to **Auto In Service**, then click **Apply**.
2. **Near-end Node:** Check the Raman N port for alarms.
    a. Select **Alarm**.
    b. In the **Navigation Tree**, select **Shelf > Raman** slot.
    c. Set **Alarm Severity** to **Not Reported.**
    d. The LOS alarm will clear when channels are present.
    Maintenance alarms are still present because the Raman N port is in maintenance.

    This completes the set up of the Raman at the near-end node.

Enabling Channel Modules

Once the Raman amplifiers are activated in both directions, the channel modules can be enabled. This procedure applies to channel modules routed to RAMAN-C10 or 2RAMAN-C15-LL amplifiers.

Figure 68: Enable Channel Modules routed to RAMAN-C10 or 2RAMAN-C5-LL Amplifiers



Post and/or Pre Amplifiers are optional
The same RAMAN module types should be used at each node.

NOTICE	**EQUIPMENT DAMAGE MAY RESULT IF:** Ensure the channel modules are transmitting at the proper level to prevent damaging the receive port of the channel module at the far-end node!

This procedure activates the channel module at Node B going to Node A and verifies it is transmitting at the proper level. Then the channel module in the other direction is checked.

> The channel modules may be routed through a ROADM or CSM. Refer to your planning document and Installation and Commissioning Manual.

1. **Node B**: Enable the channel module N port.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Ports** area, select the N port.
   The Configure Details window for the port opens.
   d. Set the **Admin State** to **In Service**, then click **Apply**.
2. **Node B**: Check the channel module N port transmit.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Network Ports** area, select **Optical** under the **Current** tab.
   OPT displays the optical power transmitted.

3. **Node A**: Check the channel module N port at Node A.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Network Ports** area, select **Optical** under the **Current** tab.
      OPR displays the optical power received.
4. **Node B:** Use an OSA to check the Optical Signal-to-Noise Ratio (OSNR) at the post-amplifier output port. Verify the OSNR meets the requirements in your planning document.
5. Repeat Step 1 to Step 3 to activate the N port of the channel module in Node A and check the channel module levels in the opposite direction (***Node A to Node B).***
6. **Node A:** Use the OSA to check the OSNR at the post-amplifier output port. Verify the OSNR meets the requirements in your planning document.
7. **Node A**: Place the Raman amplifier(s) in service:
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > Raman** slot.
   c. In the **Ports** or **Amplifiers** area, select the N port or Amplifier.
      The Configure Details window for the N port/amplifier opens.
   d. Set the **Admin State** to **In Service**, then click **Apply**.
8. **Node B**: Repeat Step 7 to place the Raman amplifier(s) in service.

Provisioning an AMP module

If the node contains an AMP-S20H-C15 or an AMP-S20L-C15 module which has a Raman amplifier, it must be calibrated with the network fiber before being used. This section explains how to perform the Raman amplifier calibration process and make the initial setting for the EDFA. The two nodes at each end of the fiber span are referred to as Node A and Node B.

This section contains these topics:

Background Information

The AMP modules contains two amplifiers, a Raman amplifier (BRMN) in the N to U direction and an EDFA in the U to N direction. The Raman amplifier utilizes the network fiber to amplify the incoming optical signal.

EDFA amplifiers perform amplification within the module. The AMP-S20L EDFA gain is adjustable from 4 dB to 13 dB, while the AMP-S20H EDFA gain is adjustable from 11 dB to

20 dB. For more information about the AMP specifications, refer to the Module and System Specification.

Part of the Raman amplifier provisioning process is to build the Amplified Spontaneous Emission (ASE) table which is stored on the AMP module. The ASE table is used for performance monitoring and to estimate the Raman amplifier gain. To build the ASE table, the fiber span must only contain the OSC signal. While building the ASE table, infra-red light is driven into the network fiber. Without the ASE table, the Raman amplifier will not become operational.

> A fiber span that does not contain any channel except the OSC is referred to as “dark” in the following sections.

During system operation, the AMP module subtracts the noise power level stored in the ASE table to calculate the optical power in the fiber span.

> **NOTICE**
>
> Raman amplifiers output high power levels. Always disable Raman amplifiers before removing fiber-optic cables. Failure to disable Raman amplifiers can result in damage to the optical connector. The amplifiers are controlled by their Admin state.

Requirements

- The following equipment is required at each node:
  - AMP-S20L-C15 or AMP-S20H-C15 amplifier module (Refer to your design plan)
  - Optical Supervisory Channel Module (OSCM-PN) with an SFP (SFP/FE/D1528.77.SM/LC)
  - Channel module
- All modules are installed according to the planning document and Installation and Commissioning Manual.
- All ports and fiber-optic cable connectors are cleaned before making connections. Fiber-optic connectors must be cleaned before every connection.
- When ROADM equipment is used, channels and cross-connects may be provisioned but the cross-connects' Admin state must be disabled.
- Far-end AMP module EDFA Admin state must be set to Disable before and during the calibration process for the near-end Raman amplfier.

> When using Raman amplification, minimize the number of Fiber Distribution Panels (FDPs) to reduce fiber loss and back reflections.

> Raman amplifiers use the network fiber as the gain medium and must be longer than 40 km. The AMP module N port must be connected to the network fiber for calibration and operation.

> Raman amplifiers require the discrete back reflection levels to be below -32 dB. The network fiber and FDP must have discrete back reflection levels below -27 dB. The back reflection levels can be measured with an optical time-domain reflectometer (OTDR). Higher back reflection levels cause BER penalties due to in-band crosstalk generated by multi-path interference. OTDR measurements need to be made with a fiber spool having a length exceeding the OTDR measurement “dead-zone”. One end of the fiber spool is connected to the OTDR and the other end to the FDP. The fiber spool is required to make reliable back reflection and loss measurements. OTDR measurements should be made for both network fibers.

> When using AMP-S20L-C15 or AMP-S20-C15 amplifiers, discrete loss elements such as connectors on fiber-optic cables, patch panels, or fiber splices should total less than 1.5 dB in the first 20 km of fiber connected to the Raman amplifier.
>
> Losses higher than 1.5 dB from the discrete loss elements can prevent Raman amplifier operation, to prevent connector damage and to ensure the gain in the network design can be reached.

Provisioning an AMP Module

Follow these steps to provision an AMP module. The two nodes at each end of the fiber span are referred to as Node A and Node B.

1. Setup the AMP at Node A, proceeding in the **Node B -> Node A** direction. Execute these procedures in the sequence specified, noting that Node A is the **near-end** node, while Node B is the **far-end** node:

   a. Establishing an OSC Connection
   b. Verifying the Fiber Span is Dark
   c. Building the ASE Table
   d. Enabling the Amplifier

2. Setup the AMP at Node B, proceeding in the **Node A -> Node B** direction. Execute these procedures in the sequence specified, noting that Node B is the **near-end** node, while Node A is the **far-end** node:
   a. Establishing an OSC Connection
   b. Verifying the Fiber Span is Dark
   c. Building the ASE Table
   d. Enabling the Amplifier
3. Once the AMP modules are activated in both directions, enable the channel modules as described in Enabling Channel Modules associated with AMP modules.

Establishing an OSC Connection

The two nodes are connected at each end of the fiber span as shown below. The Raman amplifiers are part of the AMP modules which provide amplification in the N to U direction using the network fiber.

- When setting up the Raman amplifier at Node A, Node A is the **near-end** node, while Node B is the **far-end** node.
- When setting up the Raman amplifier at Node B, Node B is the **near-end** node, while Node A is the **far-end** node.

Figure 69: Network Diagram

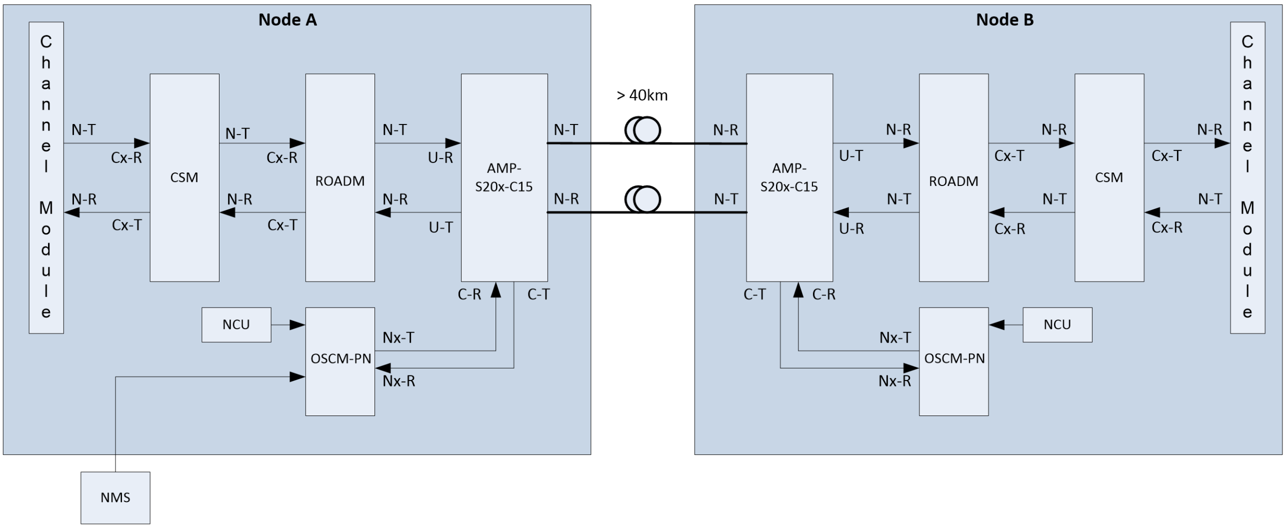
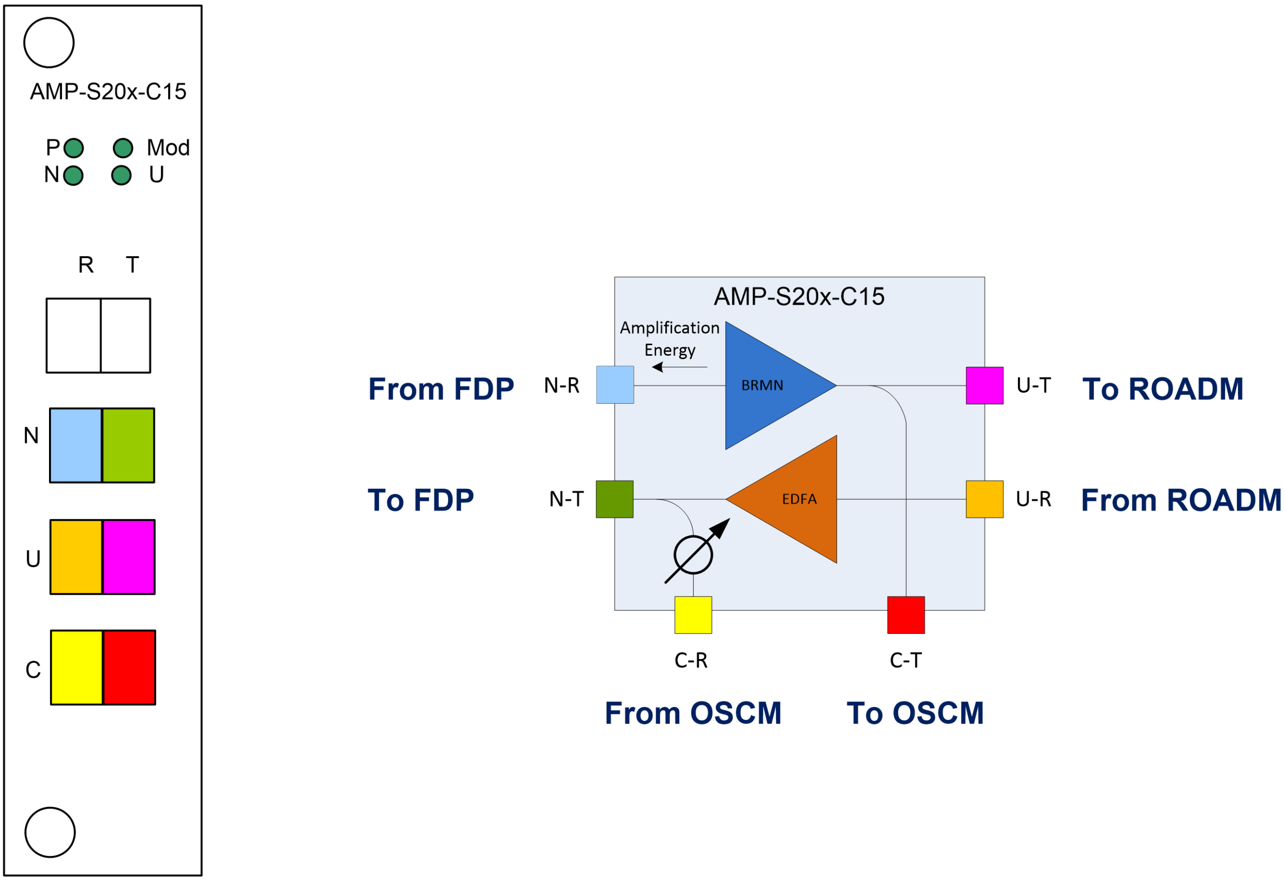


Figure 70: AMP Connection Diagram



Setup example: The OSC Tx level at the AMP N port is user provisionable. The default level is -6 dBm when the OSC signal at the C port transmit (C-T) is +5 dBm. When the span loss is less than 30 dB (recommended), the far-end OSCM-PN N port should receive the OSC signal at approximately -36 to -39 dBm. The level must be greater than -45 dB for the Raman amplifier to build the ASE table. You can set the OSC launch power at the AMP module N port up to +2 dBm, when more power is needed at the far end or to minimize cross talk between the OSC signal and channel at the low end of the C-band. Refer to your design plan for setting the correct OSC level.

The AMP module OSC launch power is user provisionable, changes may cause the fiber attenuation estimate made by the OSCM-PN to be inaccurate.

The AMP module N port at the near-end and far-end must have their administrative state set to **Maintenance**, **Management**, **In Service**, or **Auto In Service** to establish OSC communication. If the N port administrative state is Unassigned or Disabled, the OSC transmit signal is blocked and the OSC cannot be used for communication across the network fiber span.

To establish an OSC connection:

1. **Far-end Node:** Prepare the OSCM-PN.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > OSCM-PN** slot.
   c. In the **OSC Ports** area, select the corresponding N port (NW or NE) to open the Configure Details window for the N port.
   d. Set the **Admin State** to **Maintenance**, then click **Apply**.
   e. Set the **Auto Laser Shutdown** to **Disable**, then click **Apply & Exit**.
   f. Verify the OSC channel is 19610 (1528.77 nm) on the corresponding N port.
   g. Select **Monitor**.
   h. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   i. In the **Ports** area, **Current** tab, view the **OPT** value for the N port.
      The optical power transmitted by the OSCM-PN can be from +2 to +7 dBm.
   j. In the **Navigation Tree**, select **Shelf > AMP** slot.
   k. In the **Ports** area, **Current** tab, verify the **OPT** value for the N-T port is in the range **-6 to +2 dBm.**
2. **Near-end Node:** Check the OSC receive power.
   a. Select **Monitor**
   b. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   c. In the **Ports** area, **Current** tab, verify the **OPR** value for the N port is greater than **-45 dBm**.

The OSC has been verified in the **far-end node > near-end node** direction.

> If you disable the OSCM-PN port, a warning message appears: “Disabling the port may cause loss of management connectivity to remote nodes. Note: laser will remain on. Do you wish to continue? [Apply | Cancel]”.

Verifying the Fiber Span is Dark

To build an ASE table, only the OSC can be present (In-Service).

> Ensure the far-end AMP module EDFA Admin state is disabled, to prevent damage to the optical connectors.

1. **Near-end Node**: Connect an OSA to the network fiber to be connected to the AMP module N port receive (N-R).
2. **Near-end Node**: Verify only the OSC signal (1528.77 nm) is present.

Building the ASE Table

Build an ASE table at the near-end node to operate the Raman amplifier of an AMP module. If you change the Raman amplifier performance, rebuild the ASE table to overwrite the existing one.

Requirements

- Connect the amplifier U-T port.
- Set the Raman amplifier N port admin state to **Disabled**.

Procedure

1. Ensure the back reflection is less than the threshold.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf** > **AMP** slot.
   c. In the **Amplifiers** area,**Current** tab, select **Tresholds** and **Interface**. For the **BRMN** port, the **Back Reflection Rx** level displays.
   d. Ensure the back reflection is less than the **High Threshold.**
2. Build the ASE table.
   a. Select **Maintain**.
   b. In the **Navigation Tree**, select **Shelf** > **AMP** slot.
   c. In the **Amplifiers** area, **Calibrate** section, click **Start**.

> If an ASE table already exists for this Raman amplifier link, a dialog opens.
>
> Complete one of these actions.
>
> - To rebuilt the ASE table, click **Apply**. The system overwrites the existing ASE table. Continue with the next step.
> - Click **Cancel** to use the existing ASE table.

3. Verify the new ASE table build.
   a. Select **Alarm**.
   b. In the **Navigation Tree**, select **Shelf** > **AMP** slot.
   c. In the **Main Window**, select **Include Not Reported**.
   If the system raises any of the following alarms against the AMP module Raman amplifier, the ASE table build fails.
   - Pump Shutdown (ASE Low)
   - ASE Table-Fail (ASE Low)
   - ASE Table-Fail (BR)
   - ASE Table-Fail (OSC)

- ASE Table-Fail (Signal)
- ASE Table-Not Available

d. Refer to the Maintenance and Troubleshooting Manual, Appendix A, to resolve these alarms.

4. Set the Raman amplifier gain.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf** > **AMP** slot.
   c. In the **Amplifiers** area, **BRMN** port, set **Gain** to **+15 dB**.

Enabling the Amplifier

Once the ASE table is built and the 'ASE Table-Not Available' alarm has cleared, follow this procedure to verify the AMP module configuration.

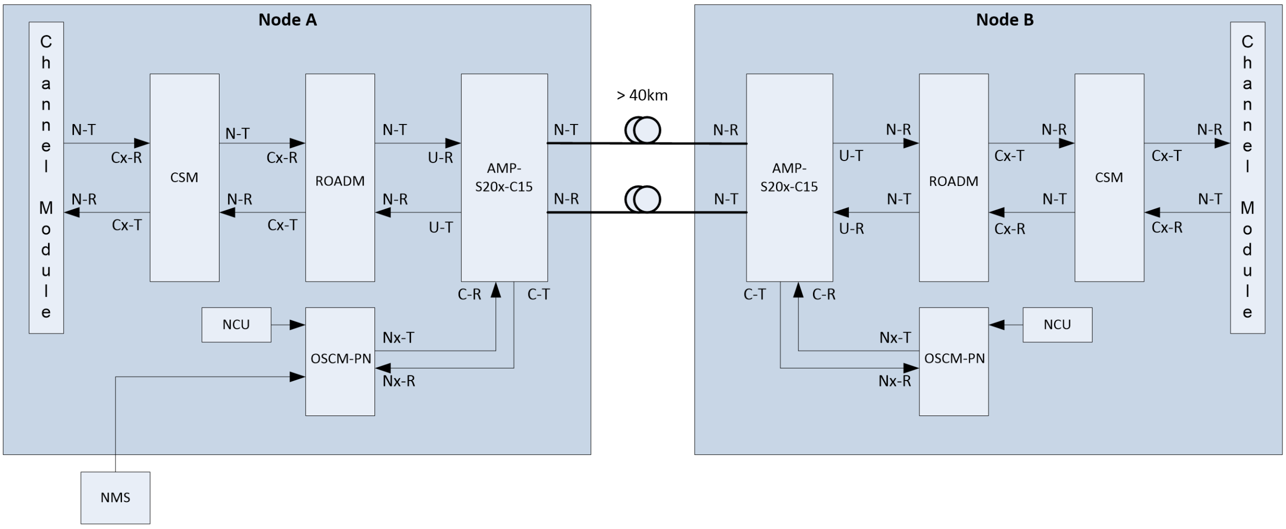
1. **Far-end Node**: If necessary, clean and connect the fiber to the AMP U port receive (U-R).
2. **Far-end Node:** Place the EDFA in maintenance mode, then set the gain equal to the span loss.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > AMP** slot.
   c. In the **Amplifiers** area, select the EDFA.
      The Configure Details window for the EDFA opens.
   d. Set the **Admin State** of the EDFA to **Maintenance**, then click **Apply**.
   e. Set the EDFA **Gain** to equal the span loss, then click **Apply & Exit**.
3. **Near-end Node:** Check the AMP module for alarms.
   a. Select **Alarm**.
   b. In the **Navigation Tree**, select **Shelf > AMP** slot.
   c. The LOS alarm will clear when channels are present.
      Maintenance alarms are still present because the amplifiers are in maintenance.

      This completes the set up of the AMP module at the near-end node.

Enabling Channel Modules associated with AMP modules

Once both AMP modules have been successfully calibrated and provisioned in both directions, the channel modules can be enabled.

Figure 71: Enabling Channel Modules associated with AMP Modules



NOTICE	**EQUIPMENT DAMAGE MAY RESULT IF:** Ensure the channel modules are transmitting at the proper level to prevent damaging the receive port of the channel module at the far-end node!

🗎	The channel modules are generally routed through a ROADM or CSM. Refer to your planning document and Installation and Commissioning Manual. If the channel module is routed through a ROADM, enable the corresponding channel after the channel module N port is enabled.

1. **Node A:** Enable the channel module N port.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Ports** area, select the N port.
   The Configure Details window for the N port opens.
   d. Set the **Admin State** to **In Service**, then click **Apply**.
2. **Node B:** Repeat Step 1 to enable the channel module routed to the AMP module.
3. **Node B:** Check the channel module transmit and receive power levels in the **Node B -> Node A** direction.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.

   c. In the **Network Ports** area, select **Optical** under the **Current** tab.
      OPT displays the optical power transmitted and **OPR** displays the optical power received.

4. **Node B**: Check the AMP module's U port receive level.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > AMP** slot.
   c. In the **Ports** area, select **Optical** under the **Current** tab.
      OPR displays the optical power received at the U port.

5. **Node A:** Check the channel module transmit and receive power levels in the **Node A -> Node B** direction.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Network Ports** area, select **Optical** under the **Current** tab.
      OPT displays the optical power transmitted and **OPR** displays the optical power received.

6. **Node A:** Place the EDFA and Raman amplifiers on the AMP module in service.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > AMP** slot.
   c. In the **Amplifiers** area, select the EDFA.
      The Configure Details window for the EDFA opens.
   d. Set the **Admin State** to **In Service**, then click **Apply**.
   e. In the **Amplifiers** area, select the Raman amplifier (BRMN).
      The Configure Details window for the Raman amplifier opens.
   f. Set the **Admin State** to **In Service**, then click **Apply & Exit**.

7. **Node B:** Repeat Step 6 to place the EDFA and Raman amplifiers on the AMP module in service.

Provisioning the 2RAMAN-C15-LL

If the node contains a 2RAMAN-C15-LL amplifier which has Raman amplifiers in the transmit and receive directions, they must be calibrated to the network fibers before being used. This section explains how to perform the Raman amplifier calibration process. The two nodes at each end of the fiber span are referred to as Node A and Node B.

This section contains these topics:

Background Information

The 2RAMAN-C15-LL module has two Raman amplifiers. Raman amplifiers utilize the network fiber to amplify the incoming optical signal. The Raman amplifier (BRMN) in the N to U direction drives energy into the receive network fiber.The Raman amplifier (FRMN) in the U to N direction drives energy into the transmit network fiber.

Part of the Raman amplifier provisioning process is to build the Amplified Spontaneous Emission (ASE) table which is stored on the 2RAMAN-C15-LL module. The ASE table is used for performance monitoring and to estimate the Raman amplifier gain. To build the ASE table, the fiber span must only contain the OSC signal. While building the ASE table, infra-red light is driven into the network fiber. Without the ASE table, the Raman amplifier will not become operational.

When 2RAMAN-C15-LL amplifiers are set up, the Network Receive ASE table (for the BRMN) must be built first. To build the Network Transmit ASE table, the Network receive Raman amplifier (BRMN) must be in operation.

🗒	The Network receive Raman amplifier (BRMN) must always be used and must always have an ASE table. Use of the Network transmit Raman amplifier is optional. When the Network transmit Raman amplifier is not used, it must be **Unassigned** or **Disabled** and it's ASE table is not required. During any ASE build process, the network fiber must be dark.

🗒	If the network fibers or connections change, the Raman amplifier ASE table must be rebuilt. Changes would include fiber cuts, switched fibers, different patch panel configurations, an increase in connector loss, or removal and re-connection of a fiber. Failure to rebuild the ASE table after changes can result in performance errors in the 2RAMAN-C15-LL.

During system operation, the RAMAN module subtracts the noise power level stored in the ASE table to calculate the optical power in the fiber span.

NOTICE

EQUIPMENT DAMAGE MAY RESULT IF:

Raman amplifiers output high power levels. Always disable Raman amplifiers before removing fiber-optic cables. Failure to disable Raman amplifiers can result in damage to the optical connector. The amplifiers are controlled by their Admin state.

Requirements

- The following equipment is required at each node to set up a fiber span that requires Raman amplification:
    - 2RAMAN-C15-LL amplifier module
    - Optical Supervisory Channel Module (OSCM-PN) with an SFP (SFP/FE/D1528.77.SM/LC)
    - One or two EDFA amplifiers (pre-amplifiers), depending on network application
    - Channel module
- All modules are installed according to the planning document and Installation and Commissioning Manual.
- All ports and fiber-optic cable connectors are cleaned before making connections. Fiber-optic connectors must be cleaned before every connection.
- The fiber to the Raman's U-R port must be disconnected.
- When ROADM equipment is used, channels and cross-connects may be provisioned but the cross-connects Admin state must be disabled.

When using Raman amplification, minimize the number of Fiber Distribution Panels (FDPs) to reduce fiber loss and back reflections.

Raman amplifiers use the network fiber as the gain medium and must be longer than 40 km.

Raman amplifiers require the discrete back reflection levels to be below -32 dB. The network fiber and FDP must have discrete back reflection levels below -27 dB. The back reflection levels can be measured with an optical time-domain reflectometer (OTDR). Higher back reflection levels cause BER penalties due to in-band crosstalk generated by multi-path interference. OTDR measurements need to be made with a fiber spool having a length exceeding the OTDR measurement “dead-zone”. One end of the fiber spool is connected to the OTDR and the other end to the FDP. The fiber spool is required to make reliable back reflection and loss measurements. OTDR measurements should be made for both network fibers.

When using 2RAMAN-C15-LL amplifiers, discrete loss elements such as connectors on fiber-optic cables, patch panels, or fiber splices should total less than 1.0 dB in the 20 km of fiber connected to the Raman amplifier.

Losses higher than 1.0 dB from the discrete loss elements can prevent Raman amplifier operation, to prevent connector damage and to ensure the gain in the network design can be reached.

Provisioning a 2RAMAN-C15-LL

Follow these steps to provision a 2RAMAN-C15-LL module, The two nodes at each end of the fiber span are referred to as Node A and Node B.

1. Setup the 2RAMAN-C15-LL at Node A, proceeding in the **Node B -> Node A** direction. Execute these procedures in the sequence specified, noting that Node A is the **near-end** node, while Node B is the **far-end** node:
   a. Establishing an OSC Connection
   b. Verifying the Fiber Span is Dark
   c. Building ASE Tables
   d. Enabling the Amplifier
2. Setup the 2RAMAN-C15-LL at Node B, proceeding in the **Node A -> Node B** direction. Execute these procedures in the sequence specified, noting that Node B is the **near-end** node, while Node A is the **far-end** node:

   a. Establishing an OSC Connection
   b. Verifying the Fiber Span is Dark
   c. Building ASE Tables
   d. Enabling the Amplifier

3. Once the 2RAMAN-C15-LL modules are activated in both directions, enable the channel modules as described in Enabling Channel Modules.

Establishing an OSC Connection

The two nodes are connected at each end of the fiber span as shown below.

- When setting up the 2RAMAN-C15-LL at Node A, Node A is the **near-end** node, while Node B is the **far-end** node.
- When setting up the 2RAMAN-C15-LL at Node B, Node B is the **near-end** node, while Node A is the **far-end** node.

Figure 72: 2RAMAN-C15-LL Network Diagram

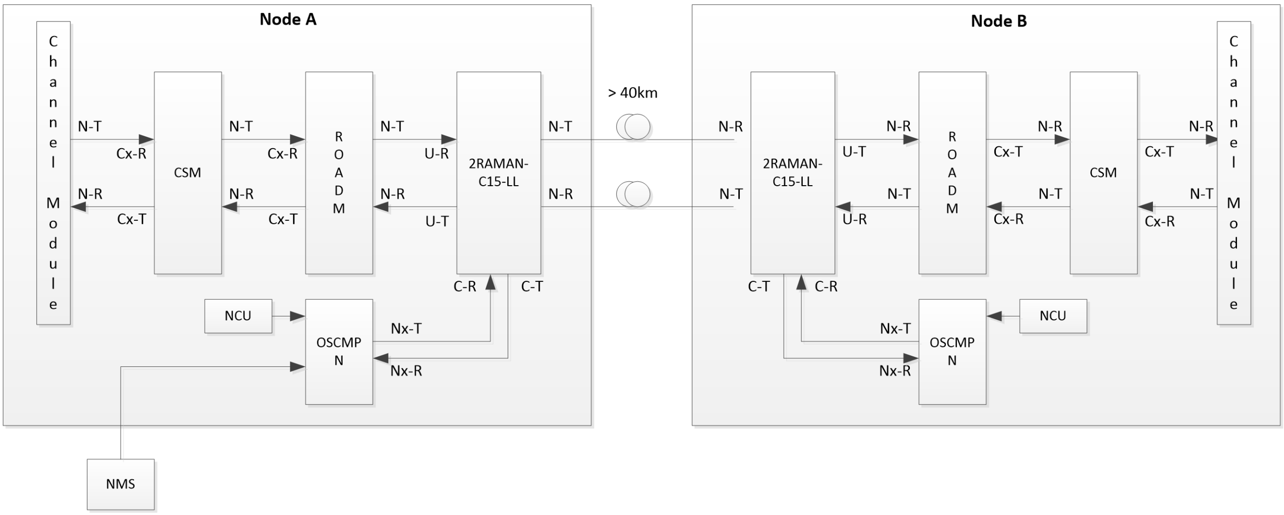
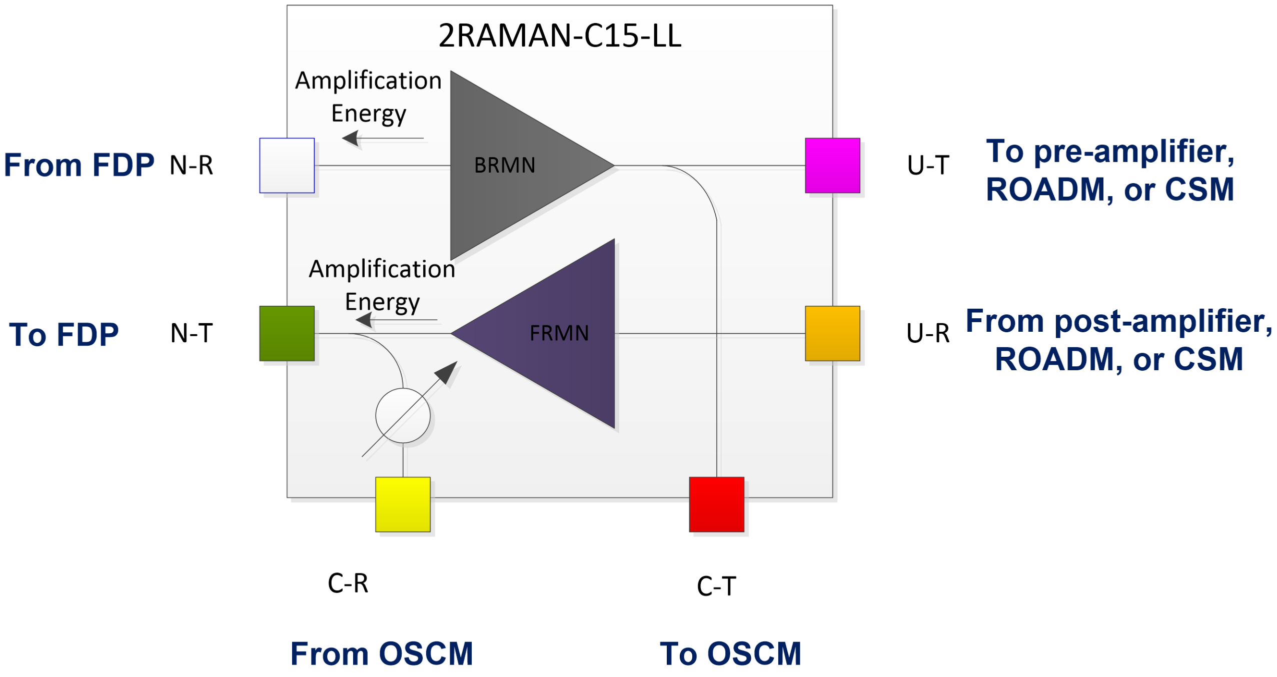


Figure 73: 2RAMAN-C15-LL Connection Diagram



To establish an OSC connection:

1. **Far-end Node**: Prepare the OSCM-PN.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   c. In the **OSC Ports** area, select the corresponding N port (NW or NE).
   The Configure Details window for the N port opens.
   d. Set the **Admin State** to **Maintenance**, then click **Apply**.
   e. Set the **Auto Laser Shutdown** to **Disable**, then click **Apply & Exit**.
   f. Verify the OSC channel is 19610 (1528.77 nm) on the corresponding N port.
   g. Select **Monitor**.
   h. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   i. In the **Ports** area, **Current** tab, view the **OPT** value under the N port.
   The optical power transmitted by the OSCM-PN can be from +2 to +7 dBm.
2. **Near-end Node**: Repeat Step 1 to prepare the OSCM-PN.
3. **Far-end Node**: Disable the post-amplifier. If your network fiber span is not equipped with a post-amplifier, skip to Step 4.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > Post-amplifier** slot.
   c. In the **Ports** or **Amplifiers** area, select the port or amplifier.

   The Configure Details window for the port/amplifier opens.

   d. Set the **Admin State** to **Disabled**, then click **Apply & Exit**.

4. **Far-end Node**: Configure the OSC level at the 2RAMAN-C15-LL N transmit port (N-T).
   a. In the **Navigation Tree**, select **Shelf > 2RAMAN-C15-LL** slot.
   b. In the **Ports** area, select the N port.
      The Configure Details window for the N port opens.
   c. Set the **Admin State** to **Maintenance**, then click **Apply**.
   d. Set the **OSC Setpoint** per your network plan, then click **Apply & Exit**.
5. **Near-end Node**: Check OSC receive power.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > 2RAMAN-C15-LL** slot.
   c. In the **Ports** area, select **OSC**.
      The **OSC Power Rx** is displayed for the N port.
6. **Near-end Node**: Check the OSC receive power at the OSCM-PN N port.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > OSCM** slot.
   c. In the **Ports** area, **Current** tab, verify the **OPR** value for the N port is greater than **-45 dBm**.
      The OSC has now been verified in the **far-end node -> near-end node** direction.

> If you disable the OSCM-PN port, a warning message appears: “Disabling the port may cause loss of management connectivity to remote nodes. Note: laser will remain on. Do you wish to continue? [Apply | Cancel]”.

Verifying the Fiber Span is Dark

To build an ASE table, only the OSC can be present (In-Service). The Network Receive ASE table (for the BRMN) must be built first.

> Ensure the Raman amplifier Admin state is disabled, to prevent damage to the optical connectors.

1. **Near-end Node**: Connect an OSA to the fiber connected to the 2RAMAN-C15-LL N port receive (N-R).
2. **Near-end Node**: Verify only the OSC signal (1528.77 nm) is present.
3. **Near-end Node**: Clean and re-connect the fiber.

Building ASE Tables

To operate the Raman amplifier first build the network receive ASE table, and then the network transmit ASE table at the node. If you change the Raman amplifier performance, rebuild the ASE tables to overwrite the existing ones.

Requirement

- On the near-end and far-end Raman amplifiers set the **Fiber Brand**, **Gain**, and **Tilt** parameter as the network plan specifies.
- Set the Raman amplifier N port admin state to **Disabled**.

> Do not set gains higher than 13.5 dB when the link uses SMF transmission fiber and the patch panel loss is the maximum of 1 dB.
>
> You can change the Raman gain at any time. If you change the tilt or fiber type parameters, you must rebuild the ASE table.

Procedure

1. On the near-end node, build the network receive ASE table.
   a. Select **Maintain**.
   b. In the **Navigation Tree**, select **Shelf** > **2RAMAN-C15-LL**.
   c. In the **Ports** area, **Calibrate** section, **BRMN** port, click **Start**.

> If an ASE table already exists for this Raman amplifier link, a dialog opens.
>
> Complete one of these actions.
>
> - To rebuilt the ASE table, click **Apply**. The system overwrites the existing ASE table. Continue with the next step.
> - Click **Cancel** to use the existing ASE table.

2. On the near-end node, verify the new network receive ASE table build.
   a. Select **Alarm**.
   b. In the **Navigation Tree**, select **Shelf** > **2RAMAN-C15-LL**.
   c. In the **Main Window**, select **Include Not Reported**.
   If the system raises any of the following alarms against the 2RAMAN-C15-LL, the ASE table build fails.
      - Pump Shutdown (ASE Low)
      - ASE Table-Fail (ASE Low)
      - ASE Table-Fail (BR)

        - ASE Table-Fail (OSC)
        - ASE Table-Fail (Pilot)
        - ASE Table-Fail (Signal)
        - ASE Table-Not Available

    d. Refer to the Maintenance and Troubleshooting Manual, Appendix A, to resolve one of these alarms.

3. On the far-end node, enable the pilot for network transmit ASE table build.
    a. Select **Maintain**.
    b. In the **Navigation Tree**, select **Shelf** > **2RAMAN-C15-LL**.
    c. In the **Port** area, **BRMN** port, set the **Pilot Operation** to **Force On**, then click **Apply**.
4. On the near-end node, repeat steps 1 and 2 to build the network transmit ASE table, selecting the FRMN.
   On successfully building the Network Transmit ASE table, the FRMN will be in Auto Pump Shutdown mode until a valid channel is received. The "ASE Table-Not Available" condition should clear.
5. On the near-end node, build the network transmit ASE table.
    a. Select **Maintain**.
    b. In the **Navigation Tree**, select **Shelf** > **2RAMAN-C15-LL**.
    c. In the **Ports** area, **Calibrate** section, **FRMN** port, click **Start**. The FRMN port is in Auto Pump Shutdown mode until a valid channel receives. The ASE Table-Not Available condition clears.

> If an ASE table already exists for this Raman amplifier link, a dialog opens. Click **Apply** to restore the link service operation on the new ASE table. The system overwrites the previous ASE table with the new one.

6. On the near-end node, verify the network transmit ASE table build.
    a. Select **Alarm**.
    b. In the **Navigation Tree**, select **Shelf** > **2RAMAN-C15-LL**.
    c. In the **Main Window**, select **Include Not Reported**.
       If the system raises any of the following alarms against the 2RAMAN-C15-LL, the ASE table build fails.
        - Pump Shutdown (ASE Low)
        - ASE Table-Fail (ASE Low)
        - ASE Table-Fail (BR)
        - ASE Table-Fail (OSC)
        - ASE Table-Fail (Pilot)

    - ASE Table-Fail (Signal)
    - ASE Table-Not Available

  d. Refer to the Maintenance and Troubleshooting Manual, Appendix A, to resolve these alarms.

7. On the far-end node, disable the pilot for network transmit ASE table build.
   a. Select **Maintain**.
   b. In the **Navigation Tree**, select **Shelf** > **2RAMAN-C15-LL**.
   c. In the **Port** area, **BRMN** port, set the **Pilot Operation** to **Normal**, then click **Apply**.

Enabling the Amplifier

Once the ASE table is built and the 'ASE Table-Not Available' alarm has cleared, follow this procedure to turn on the post-amplifier, if applicable, and verify the amplifier configuration.

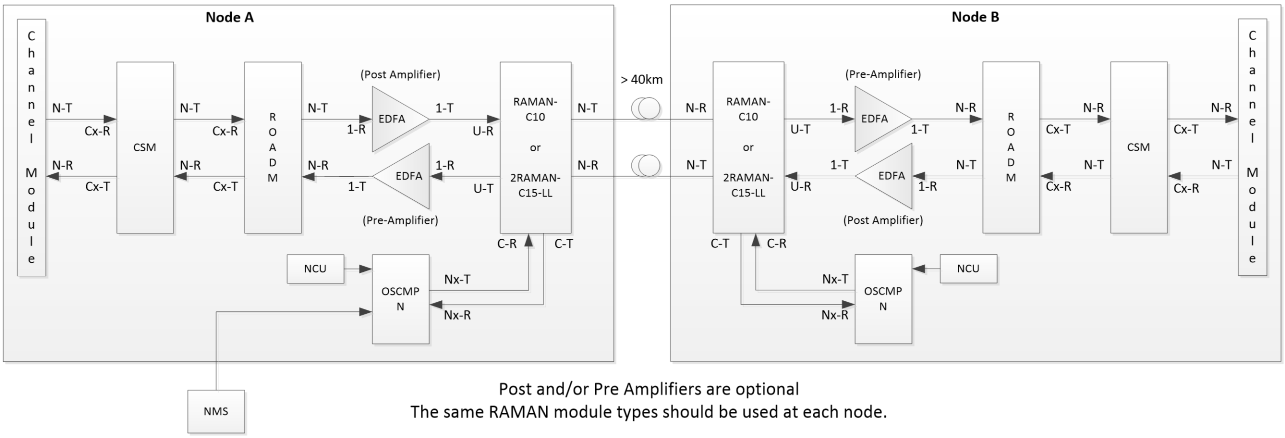
1. **Far-end Node**: Enable the post-amplifier, if applicable.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf** > **Post-amplifier** slot.
   c. In the **Ports** or **Amplifier** area, select the N port or post-amplifier.
      The Configure Details window for the port or amplifier opens.
   d. Set the **Admin State** to **Auto In Service**, then click **Apply**.
2. **Near-end Node:** Check the Raman N port for alarms.
   a. Select **Alarm**.
   b. In the **Navigation Tree**, select **Shelf** > **Raman** slot.
   c. Set **Alarm Severity** to **Not Reported.**
   d. The LOS alarm will clear when channels are present.
      Maintenance alarms are still present because the Raman N port is in maintenance.

      This completes the set up of the Raman at the near-end node.

Enabling Channel Modules

Once the Raman amplifiers are activated in both directions, the channel modules can be enabled. This procedure applies to channel modules routed to RAMAN-C10 or 2RAMAN-C15-LL amplifiers.

Figure 74: Enable Channel Modules routed to RAMAN-C10 or 2RAMAN-C5-LL Amplifiers



Post and/or Pre Amplifiers are optional
The same RAMAN module types should be used at each node.

NOTICE

EQUIPMENT DAMAGE MAY RESULT IF:

Ensure the channel modules are transmitting at the proper level to prevent damaging the receive port of the channel module at the far-end node!

This procedure activates the channel module at Node B going to Node A and verifies it is transmitting at the proper level. Then the channel module in the other direction is checked.

The channel modules may be routed through a ROADM or CSM. Refer to your planning document and Installation and Commissioning Manual.

1. **Node B**: Enable the channel module N port.
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Ports** area, select the N port.
   The Configure Details window for the port opens.
   d. Set the **Admin State** to **In Service**, then click **Apply**.
2. **Node B**: Check the channel module N port transmit.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.
   c. In the **Network Ports** area, select **Optical** under the **Current** tab.
   OPT displays the optical power transmitted.
3. **Node A**: Check the channel module N port at Node A.
   a. Select **Monitor**.
   b. In the **Navigation Tree**, select **Shelf > Channel Module** slot.

   c. In the **Network Ports** area, select **Optical** under the **Current** tab.
      OPR displays the optical power received.

4. **Node B:** Use an OSA to check the Optical Signal-to-Noise Ratio (OSNR) at the post-amplifier output port. Verify the OSNR meets the requirements in your planning document.
5. Repeat Step 1 to Step 3 to activate the N port of the channel module in Node A and check the channel module levels in the opposite direction (***Node A to Node B*).**
6. **Node A:** Use the OSA to check the OSNR at the post-amplifier output port. Verify the OSNR meets the requirements in your planning document.
7. **Node A**: Place the Raman amplifier(s) in service:
   a. Select **Configure**.
   b. In the **Navigation Tree**, select **Shelf > Raman** slot.
   c. In the **Ports** or **Amplifiers** area, select the N port or Amplifier.
      The Configure Details window for the N port/amplifier opens.
   d. Set the **Admin State** to **In Service**, then click **Apply**.
8. **Node B**: Repeat Step 7 to place the Raman amplifier(s) in service.

Provisioning the T-MP-2D12CT

The T-MP-2D12CT is a multi-rate muxponder with twelve client ports and two network ports. Each client interface supports 10GE, 100GE, or OTU4, while each network interface supports 100 to 600G.

These types of DWDM filter modules are compatible with multiple T-MP-2D12CT traffic modules:

- FD-64W with 64 channels
- FD-48E-W with 48 channels
- FD-48E-2 with 48 channels
- FD-48E with 48 channels
- 40CSM with 40 channels
- 48CSM with 48 channels
- 96CSM with 96 channels (supports up to 300-400G with limited distance)

This section contains these topics:

Requirements

You must install this equipment on both the near end and far end of the network:

- T-MP-2D12CT modules (only supported in T=SH1R-2 shelves).
- QSFP28 plugs in T-MP-2D12CT module client ports. To support Ethernet 10G client services, you must use MicroMux Plugs (QSFP28/10x10G/850I/MM/MPO or QSFP28/10x10G/1310S/SM/MPO) for the client ports.
- FD-64W, FD-48E-W, FD-48E-2, FD-48E, 40CSM, 48CSM or 96CSM filters.
- Connect equipment according to your fiber plan.

Provisioning T-MP-2D12CT1

Complete these steps to configure the T-MP-2D12CT.

Adding or Configuring the Module

By default, the T-MP-2D12CT is automatically configured when installed.

If desired, you can configure the module before installation byselecting Add then the slot and Equipment (T-MP-2D12CT).

Configuring Client Plugs

By default, the client plugs are automatically configured when installed.

If desired, you can configure the module before installation by selecting the plug to be installed.

Configuring the Client Port

To configure the client port, you must first configure or install the plug.

1. Select **Configure**.
2. Navigate to the proper **Node > Shelf > Slot**.
3. Select the **Cx** port and set the parameters following your network plan.
4. Click **Add**.

Configuring the Network Port

To configure the network port,

1. Select **Configure**.
2. Navigate to the proper **Node > Shelf > Slot**.

3. Select the **N1 or N2** port and set the parameters following your network plan.
4. Click **Addy**.

Configuring Client and Network Services

The T-MP-2D12CT client port supports the Ethernet 100G (ET100), OTU4 and Ethernet 10G (ET10) services. The network ports support OTU4, OTU (200 Gbps), OTU (300 Gbps), OTU (400 Gbps0), OTU (500 Gbps) or OTU (600 Gbps) services.

Provision Ethernet 100G or OTU4 client services - add plugs, ports and connections. Specify the parameters following your network plan.

Provisioning the Network Port Modulation Type

To configure the network port modulation type, you must first set the network port to Out of Service.

1. Select **Configure**.
2. Navigate to the proper **Node > Shelf > Slot**.
3. Select the **N1** port and set the parameters following your network plan
4. Click **Apply**.
5. Repeat the procedure for the **N2** port.

Setting Forward Error Correction on the Client Port

The forward error correction (FEC) on the client port is enabled by default.

An appropriate client FEC setting depends on the bit error rate (BER) performance of the client port plugs in use. These plugs provide the BER in the range of 10–6:

- QSFP28/112G/SR4/MM/MPO
- QSFP28/112G/AOC/xxxx
- QSFP28/112G/DAC/yy/xxxx QSFP28/103G/PSM4/SM/MPO

This value is insufficient for a proper link performance of 10–9 to 10–12. For these plugs, we recommend that you enable FEC for both 100 GBE and OTU4 client protocols. You can configure and run traffic with an FEC-disabled setting, but only as an exception.

For ET100 services, you can set FEC on the ety6-100g layer. The default FEC value is 802-3bj.

Provisioning Teraflex Modules

Teraflex modules include multiple types with different capabilities.

Teraflex Module	Description
T-MP-2D12CT	• 2 network ports support rates up to 600 Gbps. • 12 client ports support rates up to 100Gbps.
T-MP-2D8CT	• 2 network ports support rates up to 400 Gbps. • 8 client ports support rates up to 100Gbps.
T-MP-2D3DT	• 2 network ports support rates up to 600 Gbps. • 3 client ports support rates up to 400Gbps.
T-MP-M8DCT	• 1 network port supports rates up to 800 Gbps. • 8 client ports support rates up to 400Gbps.

You can use Teraflex modules with various DWDM filter modules. The filter bandwidth might limit the reach of DWDM filter modules.

This section contains these topics:

Requirements

Install this equipment on both the near and far end of the network:

- Teraflex modules
- QSFP28 plugs for the client ports. Ethernet 10G client services require MicroMux plugs:
  - QSFP28/10x10G/850I/MM/MPO
    -or-
  - QSFP28/10x10G/1310S/SM/MPO
- FD-64W, FD-84E-W, FD-48E-2, FD-48E, 40CSM, 48CSM or 96CSM filters.
- Cabling according to you fiber plan.

Install Teraflex modules only in Teraflex shelves T-SH1R-2.

Configuring the Teraflex Modules

Complete the steps in this section to configure the Teraflex modules. These procedure use the T-MP-2D12CT as an example.

You can add the Teraflex modules, a client plugs, and a client ports. ADVA automatically configures these elements with the default settings so they are ready to use when you insert them. You can also manually configure these elements with your specific details before you insert them. After you add a plug, the system automatically creates the corresponding client port. See:

- Adding Modules
- Adding Plugs
- Adding Ports

Configuring Client and Network Services

1. Provision client and network services.
2. Specify the parameters following your network plan.

Table 22: Teraflex Modules and Supported Protocols

Teraflex Module	Client Port Protocols	Network Port Protocols
T-MP-2D12CT	• 100GbE • OTU4 • 10GbE - using MicroMux	• Proprietary 100 Gbps transport signal (OTU4V-like) • Proprietary 200 to 600 Gbps high-speed transport signal
T-MP-2D8CT	• 100GbE • OTU4 • 10GbE - using MicroMux	• Proprietary 100 Gbps transport signal (OTU4V-like) • Proprietary 200 to 600 Gbps high-speed transport signal
T-MP-2D3DT	• 400 GbE	• Proprietary 200 to 600 Gbps high-speed transport signal

Table 22: Teraflex Modules and Supported Protocols

Teraflex Module	Client Port Protocols	Network Port Protocols
T-MP-M8DCT	• 100GbE • OTU4 • 10GbE - using MicroMux • 400 GbE	• Proprietary 400 to 800 Gbps high-speed transport signal

Provisioning the Network Port Modulation Type

To configure the network port modulation type, you must first set the network port to Out of Service.

1. Select **Configure**.
2. Navigate to the proper **Node** > **Shelf** > **Slot**.
3. Select the **N1** port and set the parameters following your network plan
4. Click **Apply**.
5. Repeat the procedure for the **N2** port.

Setting Forward Error Correction on the Client Port

The forward error correction (FEC) on the client port is enabled by default.

An appropriate client FEC setting depends on the bit error rate (BER) performance of the client port plugs in use. These plugs provide the BER in the range of 10–6:

- QSFP28/112G/SR4/MM/MPO
- QSFP28/112G/AOC/xxxx
- QSFP28/112G/DAC/yy/xxxx
- QSFP28/103G/PSM4/SM/MPO

This value is insufficient for a proper link performance of 10–9 to 10–12. For these plugs, we recommend that you enable FEC for both 100 GBE and OTU4 client protocols. You can configure and run traffic with an FEC-disabled setting, but only as an exception.

For ET100 services, you can set FEC on the ety6-100g layer. The dafault FEC value is 802-3bj.

Provisioning T-MP-2D12CT1

Complete these steps to configure the T-MP-2D12CT.

Adding or Configuring the Module

By default, the T-MP-2D12CT is automatically configured when installed.

If desired, you can configure the module before installation byselecting Add then the slot and Equipment (T-MP-2D12CT).

Configuring Client Plugs

By default, the client plugs are automatically configured when installed.

If desired, you can configure the module before installation by selecting the plug to be installed.

Configuring the Client Port

To configure the client port, you must first configure or install the plug.

1. Select **Configure**.
2. Navigate to the proper **Node > Shelf > Slot**.
3. Select the **Cx** port and set the parameters following your network plan.
4. Click **Add**.

Configuring the Network Port

To configure the network port,

1. Select **Configure**.
2. Navigate to the proper **Node > Shelf > Slot**.
3. Select the **N1 or N2** port and set the parameters following your network plan.
4. Click **Addy**.

Configuring Client and Network Services

The T-MP-2D12CT client port supports the Ethernet 100G (ET100), OTU4 and Ethernet 10G (ET10) services. The network ports support OTU4, OTU (200 Gbps), OTU (300 Gbps), OTU (400 Gbps0), OTU (500 Gbps) or OTU (600 Gbps) services.

Provision Ethernet 100G or OTU4 client services - add plugs, ports and connections. Specify the parameters following your network plan.

Provisioning the Network Port Modulation Type

To configure the network port modulation type, you must first set the network port to Out of Service.

1. Select **Configure**.
2. Navigate to the proper **Node > Shelf > Slot**.
3. Select the **N1** port and set the parameters following your network plan
4. Click **Apply**.
5. Repeat the procedure for the **N2** port.

Setting Forward Error Correction on the Client Port

The forward error correction (FEC) on the client port is enabled by default.

An appropriate client FEC setting depends on the bit error rate (BER) performance of the client port plugs in use. These plugs provide the BER in the range of 10–6:

- QSFP28/112G/SR4/MM/MPO
- QSFP28/112G/AOC/xxxx
- QSFP28/112G/DAC/yy/xxxx QSFP28/103G/PSM4/SM/MPO

This value is insufficient for a proper link performance of 10–9 to 10–12. For these plugs, we recommend that you enable FEC for both 100 GBE and OTU4 client protocols. You can configure and run traffic with an FEC-disabled setting, but only as an exception.

For ET100 services, you can set FEC on the ety6-100g layer. The default FEC value is 802-3bj.

Configuring Management Connection between FSP 3000 C Channel Modules

> When FSP 3000 C channel module is in an FSP 3000R7 node:
>
> - **MTU [Byte]** set up to 1472.
> - **Time to Live** set to at least 1 higher than the number of hops.
> - If using IPv4:
>   - **IP Configuration** set to **Numbered**.
>   - **IP Mask** enter 255.255.255.252.

Configuring Management Links

1. Select **Overview** > **Management Network** > **Interfaces**.
2. In the **Management Links to Module Management Channels** area, click **Add End Point**.
3. In the **Add Facility** window:
   a. Select the **Identifier** based on your network plan.
   b. Set the **Facility** to **HD PPP/IP**. You must set both facilities to HD PPP/IP if at least one module is HD module.
   c. Enter **User Label** (optional).
   d. Set the **Admin State** to **In Service**.
   e. In the **Management Link** area:
      - Enter the **Max Tx Rate [kbps]** based on your network plan.
      - Enter the **MTU [Byte]** based on your network plan.
   f. In the **IPv4 Configuration** area:
      - Set the **IP Configuration** to **Unnumbered**.
      - Enter the **Far End IP Address** based on your network plan.
   g. Click **Add** to confirm.
4. Repeat steps 1 to 3 for the second Management Link.
5. In the **Management Links to Module Management Channels** area, click **Add Connection**.
6. In the **DCN Connection Cross** window:
   a. Select the **Identifier** based on your network plan.
   b. Select the GCC in the **Management Channel** based on your network plan.
   c. Click **Add** to confirm.

Creating a Logical Interface

OSPF Routing is disabled for HD PPP/IP facilities. If you want to use OSPF instead of static routes, you need to create a logical interface.

1. Select **Overview** > **Management Network** > **Interfaces**.
2. In the **Logical Interfaces** area, click **Add**.
3. In the **Add Logical Interface** window:
   a. Select the **Identifier** based on your network plan.
   b. Enter **User Label** (optional).
   c. In the **Internet Protocol (IPv4)** area:
      - In the **IP Address** enter IP Address based on your network plan.
      - In the **IP Mask**, enter based on your network plan.

   d. In the **Management LAN** area, select the **Management Interface** based on your network plan.
   e. In the **OSPF Routing** area, set **OSPF Routing** to **Enable**.
   f. Set the **Admin State** to **In Service**.
   g. In the **IP Encapsulation** area:
      - Set **Encapsulation** to **Generic Routing (GREIP)** or **IP in IP**.
      - Enter the **IP Address**.
      - Enter the **Far End IP Address**.

   h. Click **Add** to confirm.
4. Repeat steps 1 to 3 for the second entity.

Flexgrid with PSM80 and Raman Supported Amplification

This section contains these topics:

Requirements

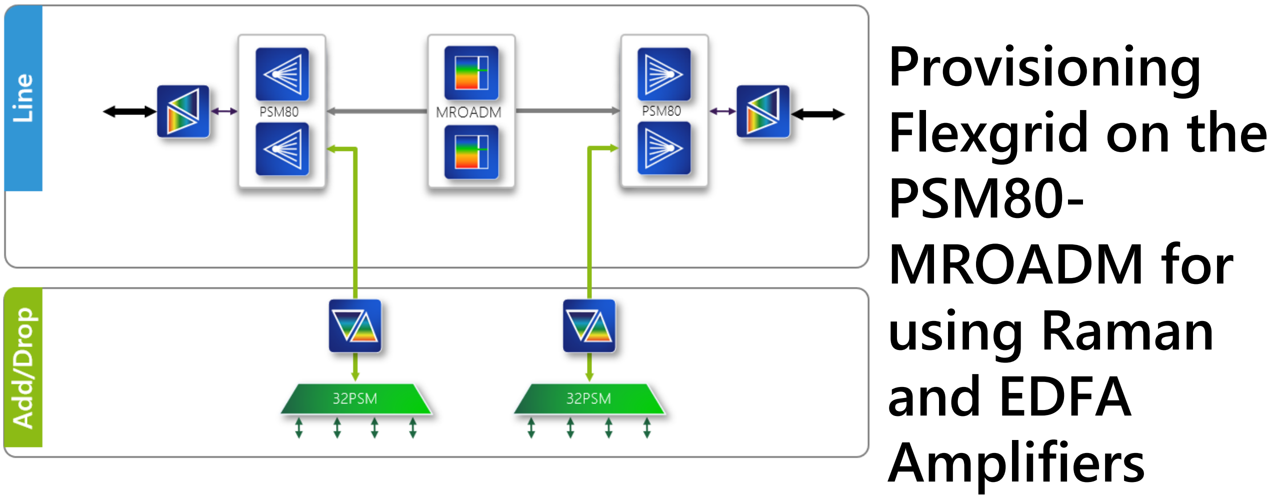
- A node is populated with the required modules:
  - RAMAN-C10
  - EDFA-C-D20-VLGC-DM
  - PSM80-MROADM

  - MROADM-C96
  - 32PSM-1HU

- A fiber (cabling) plan is available, that shows all internal node-fiber jumpers.

Example

Figure 75: Example Flexgrid Add-Drop using PSM80-MROADM and 32PSM-1HU.



Provisioning Flexgrid on the PSM80-MROADM for using Raman and EDFA Amplifiers

You can provision Flexgrid configuration using MROADM-C96, PSM80-MROADM and RAMAN-C10 supported amplifiers. Only west-side configuration is shown, east-side configuration procedure is similar. Follow the procedure steps to provision the mentioned structure:

Provisioning the RAMAN-C10 and EDFA-C-D20-VLGC-DM on the receiving side

1. Provision the RAMAN-C10. Refer to Provisioning a RAMAN-C10.
2. Provision the EDFA-C-D20-VLGC-DM booster. Refer to Provisioning Optical Amplifiers.

Provisioning EDFA-C-S26-VGC-DM on the transmitting side

1. Provision the EDFA-C-S26-VGC-DM. Refer to Provisioning Optical Amplifiers.

Provisioning the PSM80

1. In the **Main Pane** select **Add Module**.
2. In the **Add Module** window:
   a. In the **Equipment** list, select the **PSM80-MROADM**.
   b. In the **Channel Spacing** list, select **Flexible**.
3. Click **Add**.

Provisioning the MROADM-C96

1. Provision the MROADM-C96. Refer to Adding Modules.

Provisioning the add / drop structure

> You must provision the add amplifier and drop amplifier according to your network plan and the specific needs of your network.

1. Provision the add amplifier. Refer to Provisioning Optical Amplifiers.
2. Provision the drop amplifier. Refer to Provisioning Optical Amplifiers.
3. Provision the 32PSM-1HU. Refer to Adding Passive Units.

Provisioning Physical Connections

Provision physical connections according to your fiber plan available. Refer to Adding Physical Connections.

Provisioning Optical Channels

Add optical channels for the pass-through and add-drop services:

1. Navigate to **PSM80-MROADM > Optical Channels** area.
2. Click **Add**.
3. In the **Wizard for optical channel** window, set these fields according to your network plan:
   a. **Add Channel**
   b. **Channel**
   c. **Channel Bandwidth**
   d. **Facility**
   e. **Setpoint Delta**

f. **(A->B) Node in Path**

g. **(B->A) Node in Path**

h. **User Label** (optional).

4. Click **Add**.

Provisioning the OF-2D16DCT

This section contains these topics:

Background Information

The OF-2D16DCT, or OpenFabric™1200, is a core-type, add-drop multiplexer traffic module that can add or drop up to 36 optical client signals from one or two optical network signals.

The OF-2D16DCT supports these applications:

- Muxponder with a maximum of 600G traffic using one or two CFP2 network ports.
- Add-drop multiplexer with a maximum of 300G traffic using two CFP2 network ports.

The OF-2D16DCT client ports support 10 GbE, 100 GbE, 400 GbE, OTU2, OTU2e, and OTU4 signals for a maximum of 600G. The OF-2D16DCT network ports support OTUC2, OTUC3, and OTUC4 signals for a maximum of 600G.

> See the FSP 3000 C Hardware Guide for details on services and service configurations that the OF-2D16DCT supports.
>
> See the FSP 3000 C Compatibility Matrix for a list of pluggable transceivers and services that the OF-2D16DCT supports.

Requirements

Install this equipment on the near and far-end nodes:

- OF-2D16DCT modules.
- QSFP or SFP pluggable transceivers in OF-2D16DCT modules.
- Fibers (cables) as specified in the fiber plan.

Provisioning the OF-2D16DCT

To configure the OF-2D16DCT on the near and far-end nodes:

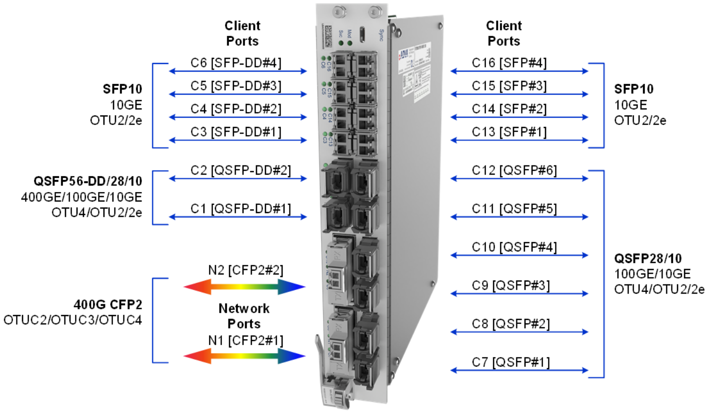
1. Create the module and set the OF-2D16DCT operational mode to single-module configuration (single-card-cross-connect) or dual-module configuration (dual-card-crossconnect). The OF-2D16DCT supports only the single-module configuration in the current release. In a future release, the OF-2D16DCT also supports the dual-module configuration. The dualmodule configuration provides up to 600G add-drop multiplexer and extended client signal support for muxponder and add-drop multiplexer applications. Two OF-2D16DCT modules interconnect through the two QSFP-DD ports and the Sync port.

> If you set the operational mode to single-module configuration:
>
> - A later upgrade to dual-module configuration requires a reboot.
> - You cannot use the SFP C15 and C16 ports.
>
> If you set the operational mode to dual-module configuration:
>
> - The OF-2D16DCT operates as a single module in the current release. In a future release, the module can upgrade to dual-module configuration without a reboot.
> - You can use the QSFP-DD C1 and C2 ports only to interconnect modules. For example, the module will not support 400 GbE traffic.

> By default, the system automatically creates the OF-2D16DCT module type after you insert it in a slot. The default operation mode is single-module configuration.

2. (Optional) Configure the client and network pluggable transceivers.

This diagram shows the plugs you can install in specific client and network ports of the OF-2D16DCT:



3. Configure the client and network interfaces.
4. Provision the network port frequency.
5. Create services and cross-connections.

Retrieving Tributary Ports and Slots Information

To retrieve the available and used tributary slot counts:

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant module.
3. In the **Ports** area, click the relevant N port. The **Configure Details** window opens:
   a. Click **ODU Tributary Slots**.
   b. Read the relevant fields:
      - **Slots Available**
      - **Slots in Use**

To retrieve the service (LO) tributary port and slots:

1. Select **Configure**.
2. In the navigation tree, navigate to the relevant module.
3. In the **Data Channels** area, click the relevant channel. The **Configure Details** window opens:
   a. Click **Transport**.
   b. Read the relevant fields:
      - **ODU ID**
      - **Slot(s)**