Cisco Optical Network Planner Configuration Guide, Release 4.2

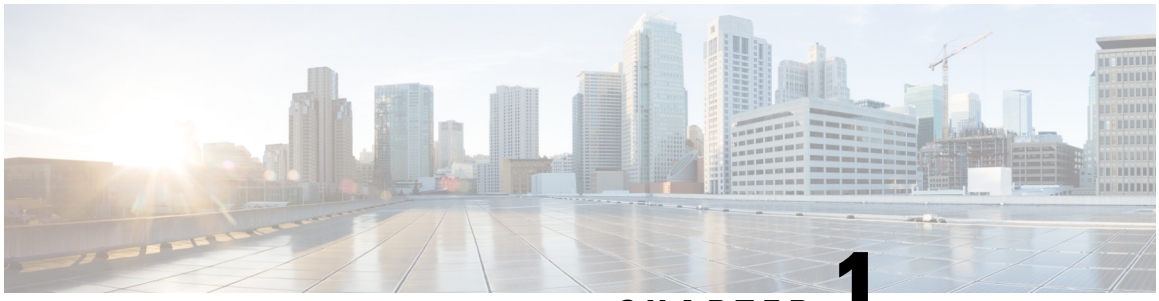
First Published: 2021-05-31

Last Modified: 2023-06-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 4



CHAPTER 1

Get Started with Cisco Optical Network Planner

Cisco Optical Network Planner

Cisco Optical Network Planner is a web application that

- models and tests Optical Transport Networks (OTN) and Dense Wavelength Division Multiplexing (DWDM) networks,
- provides a graphical environment for network design and validation, and
- supports creating and comparing multiple network instances.

Cisco ONP enables you to visualize their network designs. It allows you to generate bills of materials and access detailed reports for network planning and validation.

Purpose

The primary purpose of Cisco ONP is to design and validate networks for the NCS 1004, NCS 2000, and NCS 4000 series.

With Cisco ONP, you can create multiple instances of a network, modify various parameters for each instance, and perform comparisons. The tool generates a rack view of all the sites deployed in the network, highlights the differences between instances, and provides a complete Bill of Materials (BoM).

Detailed network information

Cisco ONP models the network and generates the BoM. You can view detailed reports, including:

- Cabling report
- Optical report
- Device Configuration file
- Traffic matrix

Features and compliance

You can use the features of Cisco ONP, including protection scenarios, topology and service support, to support protection scenarios, topology and service support, and compliance with the Cisco Secure Development Lifecycle (CSDL). You can also set up the graphical display.

Additional resources

For more detailed information about Cisco ONP, see the data sheet.

Supported platforms

Cisco ONP supports these platforms:

Table 1: Supported platforms and releases

Platforms	Recommended and Supported Releases
NCS 1004	7.0.1
NCS 2000	11.0.0, 11.1.0, 12.1.0, 12.2.0
NCS 4000	6.5.28

Supported topologies

Cisco ONP supports several network topologies, each offering different configurations and benefits.

Cisco ONP supports these platforms.

- Linear topology: In a linear topology, the nodes are arranged in a line and are connected to two adjacent nodes. However, the first and last nodes are not connected to each other.
- Mesh topology: In a mesh topology, each node is connected to one or more nodes. This configuration provides maximum redundancy to the network.
- Ring topology: In a ring topology, each node is connected to exactly two other nodes, forming a circular configuration. It requires at least three nodes to form a ring.

Supported protection schemes

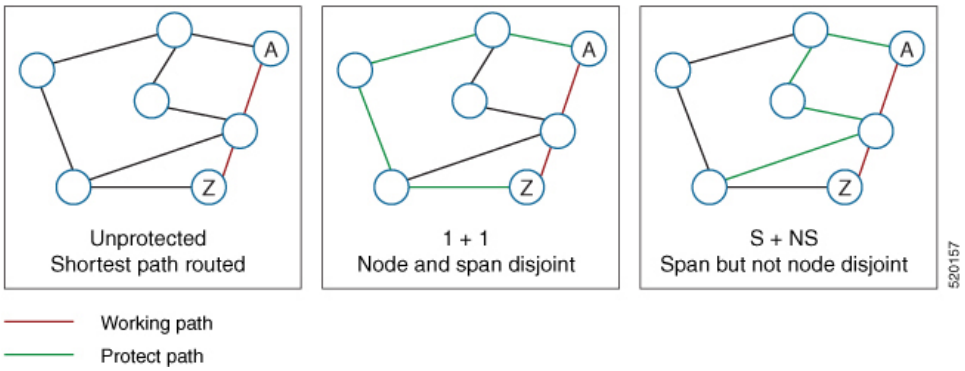
Cisco ONP offers a variety of protection schemes to enhance network reliability and resilience.

Table 2: Feature History

Feature Name	Release Information	Feature Description
Protection Types Supported	Cisco ONP Release 4.1	The following protection schemes are supported: • 1+R: For each service, Cisco ONP automatically finds one working path. You can define the restoration path. • 1+1+R: For each service, Cisco ONP finds one working path, and one protected path. You can define the restoration path. • 1+1+R+R: For each service, Cisco ONP finds one working path and one protected path. You can define the restoration paths.

Cisco ONP offers a variety of protection schemes to enhance network reliability and resilience.

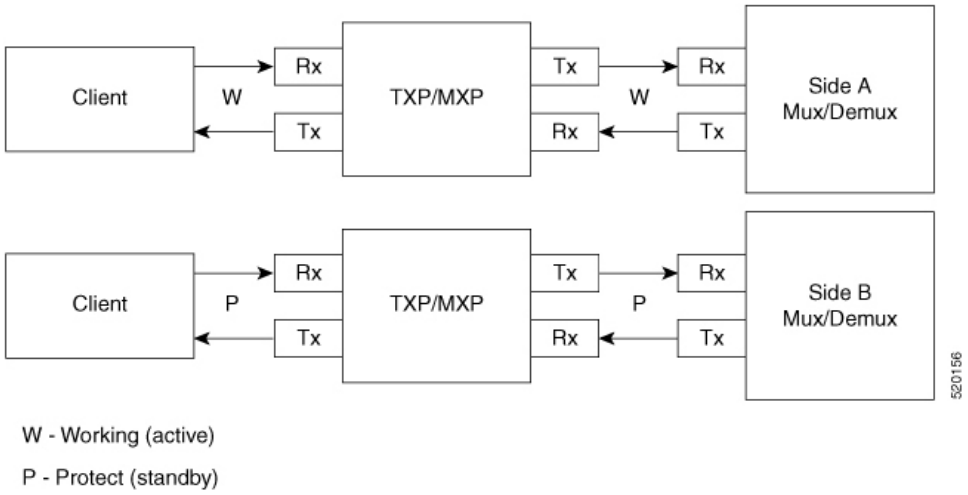
Figure 1: Protection schemes



Supported protection schemes include:

- Unprotected: In unprotected mode, the tool routes the service on the shortest path without any backup.
- 1+1: In this scheme, two client signals are transmitted to separate line cards or transponder cards, rather than using a Y-cable to split one client signal into two. Client 1+1 protection allows the client system to control failure events and to manage the switchover.

Figure 2: 1+1 protection



- 1+R: Supported on SSON networks, this scheme allows Cisco ONP to automatically find one working path for each service. You can define the restoration path.
- 1+1+R: Also supported on SSON networks, this scheme involves Cisco ONP finding one working path and one protected path for each service, and users can define the restoration path.
- 1+1+R+R: Supported on SSON networks, this scheme involves Cisco ONP finding one working path and one protected path. You can define additional restoration paths.
- S+NS: Supported on non-SSON network, Cisco ONP uses the shortest path for the working service and the next shortest path for protection. The paths are span-disjoint but not node-disjoint
- Unprotected disjoint: Supported on non-SSON network, this scheme provides two cards following two completely disjoint paths in the network to reach their destination.

Supported services

Cisco ONP supports these OTN, Ethernet, and STS services.

Cisco ONP supports these OTN demands and services.

- ODU demands:
  - ODU-1
  - ODU-2
  - ODU-3, and
  - ODU-4
- Ethernet services:
  - GE
  - 10GE

    - 100GE

- Synchronous Transport Signal (STS) services:
    - STS-3
    - STS-12
    - STS-48
    - STS-192
- Virtual Container (VC) services:
    - VC-4-4
    - VC-4-16
    - VC-4-64
- Synchronous Transport Module services such as STM-64.

Supported DWDM channel interfaces

Cisco ONP supports several DWDM channel interfaces that provide high-capacity optical transport and are compatible with industry-standard wavelengths. For more information about the DWDM channel interfaces supported by Cisco ONP, seeSupported Cards and Pluggables, on page 181 and Supported Optical Sources, on page 195.

Supported fiber types

Cisco ONP supports these fiber types.

- Standard single-mode fibers:
    - G652-SMF
    - G652-SMF-28E
- True Wave fiber series:
    - True Wave
    - TWR
    - TWPlus
    - TWMinus
    - TWClassic
- Other type of fibers:
    - MC

- FL
- LS
- TL
- ELEAF

Register a new user

Use this procedure to register a new account on Cisco ONP. This enables you to create a username and password to gain access to the system.

Procedure

Step 1 In the browser URL field, enter the IP address or hostname of the Cisco ONP instance.

Step 2 Click **Sign Up** in the Login page.

Step 3 Enter the **Username**, **Email**, **Password**, and **Confirm Password**, and click **Submit**.

Step 4 If you want a system-generated password, click **Generate**, and click **Submit**. The system fills the **Password**and **Confirm Password** fields with the generated password.

Step 5 Click **Ok** in the **Success** dialog box.

Log in to the Cisco ONP web interface

Use this task to log into the Cisco ONP web interface.

Procedure

Step 1 In the browser URL field, enter the IP address or hostname of the Cisco ONP instance.

If you are a new user, sign up. See Register a new user, on page 6.

Note
If the Google Chrome browser blocks your access to Cisco ONP due to self-signed certificate security, type **thisisunsafe** to proceed to the Login page.

Step 2 Enter the username and password in the **Username** and **Password** text boxes, and click **Login**.

Cisco ONP home page

This topic helps you understand the layout, key navigation elements, user and network information displayed in the Cisco ONP home page.

After you log in, the Cisco ONP home page displays several key elements that help users navigate and utilize the tool effectively.

- Menu bar: The menu bar includes several options: File, Network, Export, Import, Manage, Logs, Job Monitor, Control Panel, and Help. See Menu bar, on page 169.
- Last login: Displays the last date and time of user login to Cisco ONP.
- Last login IP: Shows the IP address from which the user previously logged into Cisco ONP.
- User name: Your user name appears here, for example, ADMIN.
- Reports tabs: Use these tabs to access different reports. The availability of reports depend on whether a network has been analyzed. You can also access reports in site properties after network analysis.
- Network tree: Displays the network name and its elements, such as Sites, Fibers, Waves or Media Channels, SRLGs, and Subnets. See Network Tree, on page 175.

Tip To expand the Cisco ONP workable area, click the horizontal and vertical arrows on the home page.

If you see an empty grey window, update your browser to the latest version. For detailed hardware and software requirements, refer to the Cisco ONP Installation Guide.

Change password

Follow these steps to change your password.

Procedure

Step 1 Click the Login icon in the home page, then select **Change Password**.

Step 2 In the **Change Password** dialog box, enter the **Old Password**, **New Password**, **Repeat New Password**, then click **Update**.

Reset your password

Use this procedure to reset your password for the Cisco ONP.

Procedure

Step 1 In the browser URL field, enter the IP address or hostname of the Cisco ONP instance.

Step 2 Click **Forgot Password?** on the Cisco ONP Login page.
The **Forgot Password** page appears.

Step 3 Enter your registered email address in the **Forgot Password** page, then click **Continue**.

A verification code is generated and sent to the registered email address.

Step 4 Enter the verification code, new password, and confirmation of your new password, then click **Continue**.

Sign out from Cisco ONP

Use this procedure to sign out of Cisco ONP.

Procedure

Click the Login icon in the top-right corner of the home page, and choose **Sign Out** to log out of the Cisco ONP tool.

CSDL compliance enhancements in Cisco ONP

The Cisco Secure Development Lifecycle (CSDL) compliance enhancements in Cisco ONP are security features that:

- display the last login IP address of the client,
- allow setting a passphrase for encrypting credentials during the installation of the LNI application and database, and
- incorporate several CSDL compliance measures to improve security and user management.

Table 3: Feature History

Feature Name	Release Information	Feature Description
CSDL Compliance Enhancements	Cisco ONP Release 4.1	The following CSDL compliance enhancements are supported: • Displays the last login IP address of the client. • Allows you to set a passphrase for encryption of credentials during the installation of LNI application and database.

Cisco ONP incorporates these CSDL compliances to enhance security and user management.

Passphrase security

Passphrase security features are security measures that:

- ensure new passphrases do not exist in a dictionary of common passwords.
- provide pop-up messages to alert users about upcoming passphrase expiration, and
- enable admin users or those with CONFIGURATION_MANAGEMENT permission to set the passphrase lifetime and grace period via the system configuration tab.

To create a valid passphrase, ensure it is between 8 and 127 characters and includes at least one lowercase letter, one uppercase letter, one number, and one special character.

Passphrase management

Passphrase management features are administrative controls that:

- prompt the admin to change the passphrase upon first login,
- allow setting a passphrase or key to encrypt credentials during the installation of the Live Network Import (LNI) application (the default key is used if unspecified), and
- let users set a passphrase between 8 and 64 characters during Cisco ONP and LNI database installation.

User login information

User login information features are user management tools that:

- display the last login date,
- display the last login time, and
- display the last login IP address in the Cisco ONP user interface.

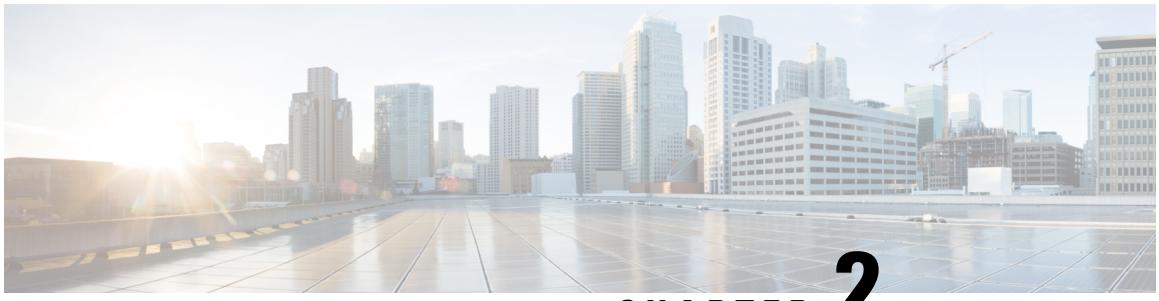
Additional security features

Additional security features are user-facing enhancements that:

- provide an option for users to generate a password using the Generate Password feature,
- display the strength of the password set by the user, and
- offer improved feedback on password creation.

Port details

The LNI application provides details of all ports used, enabling administrators to reference port usage information for enhanced network configuration and troubleshooting. See Ports Used in LNI, on page 31.



CHAPTER 2

Manage Users and Roles

User roles in Cisco ONP

Cisco ONP provides a structured approach to access control management through various user roles. Here's an overview of the default roles and their capabilities:

Administrator

As an administrator, you have these roles and responsibilities:

- **User activation**: Admin or users with admin access grant access by activating new users, who are then notified by email.
- **Group management**: Some user groups are predefined. These groups cannot be edited or deleted.
- **Role assignment**: Admins assign roles to groups, defining the actions a group can perform.

Designer

As a designer, you have these roles and responsibilities:

- **Network design**: Designers can create network topologies using either manual design or import design methods.
- **Capabilities**: They can design networks with various topologies (linear, ring, mesh) and assign fibers between sites, including Traffic, OLA, ROADM, and Passthrough sites.
- **Limitations**: Designers cannot analyze networks but can view reports shared by others after analysis.

Planner

As a planner, you have these roles and responsibilities:

- **Design and analysis**: Planners can both design and analyze networks. They evaluate network performance after creating sites, fiber spans, and service demands.

Reader

As a reader, you have these roles and responsibilities:

- **View-only access**: Readers can view users, user groups, roles, permissions, network topology, layout, connections, and the Bill of Materials (BOM).

  By default, users are assigned to the READ_ONLY_GROUP with the role called READER_ROLE.

To create a new role, see #unique_24.

Under **Control Panel** > **Roles** and **Control Panel** > **Permissions**, you can view the permissions applicable for each role and the actions that can be performed for each permission.

Assign a role to a user group

All users with the admin role receive an email notification about new user registration.

Follow these steps to assign a role to a user group:

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 You can change the state of a user from INACTIVE to ACTIVE in either of two ways.

- From the **State** field, click **INACTIVE** in the respective user row.
- Select the user row and click **Update**.
  - In the **Update User** dialog box, select the **Group** and **State** from the respective drop-down lists.
  - Click **Save**.

Step 3 Click **OK** in the **Success** dialog box.

Note

- After your access is granted by the admin, you receive an email notification at your registered email address. ou can log in after you get this email.
- The admin assigns a Role and Group to a newly created user. These assignments determine what actions the user can perform.

Remove access to a user

This section helps you to securely revoke a user's access for security, compliance, or resource management reasons.

Follow these steps to remove Cisco ONP access to a user.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Change the state of a user from ACTIVE to INACTIVE in either of two ways:

- In the **State** field, click **ACTIVE** in the user's row.
- Select the user row , and click **Update**.
  - In the **Update User** dialog box, select the **Group** and **State** from the drop-down lists.
  - Click **Save**.

Step 3 In the **Success** dialog box, click **OK**.

Delete a user

Follow these steps to delete a user.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with admin role.

Procedure

Step 1 Click **Control panel**.

The **Access Control Management** page appears.

Step 2 Delete a user:

a) Select the user to be deleted under the **USERS** tab, and click **Delete**.

b) Click **Yes** in the **Warning** dialog box.

The message **User deleted successfully** appears. You can delete another user only after this message appears.

Create a new user group

Follow these steps to create a new user group.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USER GROUPS** tab.

Step 3 Click **Create**.

a) In the **Create Group** dialog box, enter the **Group Name**.

b) Choose the appropriate role from the **Role** drop-down list. The available default roles are:

- ADMIN
- PLANNER
- DESIGNER
- READER

The **Role** drop-down list may also have user-defined roles listed under it.

c) Click **Save** to create the user group.

Step 4 In the **Success**dialog box, click **OK**.

Assign a user to a user group

This task guides an administrator to assign a user to a specific user group within the system. Organizing users into groups with defined roles and permissions streamlines access management and enhances security controls.

Follow these steps to assign a user to a user group.

Before you begin

Log in to the Cisco ONP web interface, on page 6 with Admin permission.

Procedure

Step 1 Click **Control panel**.

The **Access Control Management** page appears.

Step 2 Under the **USERS** tab, select the user who is to be assigned to the new group, and click **Update**.

In the **Update User** dialog box:

a) From the **Group** drop-down list, select the appropriate group.
b) From the **State** drop-down list, select **Active** to activate the user in the group, or **Inactive** to deactivate the user in the group.
c) Click **Save**.

Step 3 In the **Success** dialog box, click **OK**.

Note

a. A user can belong to only one group.

b. Only one role can be assigned to any group.

c. All users in a group have the group's role.

d. By default, a new user is assigned to the Read_Only_Group.

Set password expiration for individual user

This section explains how to set password expiration to help maintain user account security.

Follow these steps to set the expiration of the password set by the user.

Before you begin

Log in to the Cisco ONP web interface, on page 6 with Admin or Configuration_Management permission.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Select the user under the **USERS** tab., and click **Update**.

In the **Update User** dialog box:

a) Click the **PASSWORD EXPIRY** tab.
b) Enter values for the **Lifetime**, **Warning** and **Grace** fields.
c) Click **Save**.

Note
The password expiry settings like lifetime, warning and grace time, take effect after the existing password is changed by the user.

Step 3 In the **Success** dialog box, click **OK**.

Set password expiration for all users

This section explains how to set password expiration to help maintain user account security.

Follow these steps to set the password expiration for all users.

Before you begin

Log in to the Cisco ONP web interface, on page 6 with Admin or Configuration_Management permission.

Procedure

Step 1 Click **Control Panel**.
The **Access Control Management** page appears.

Step 2 Click the **System Configuration** tab.

a) Enter values for the **Lifetime**, **Warning**, and **Grace** fields.
b) Click **Update**.

Note
The password expiry settings such as lifetime, warning, and grace time, take effect after the user changes their existing password.

Lock and unlock an individual user account

This procedure enables administrators to ensure that only authorized users can access the system.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USERS** tab.

a) Select the user whose account you want to lock or unlock.

b) Click **Lock** to lock the user account, or click **Unlock** to unlock the account.

If your account is locked, contact your administrator to unlock your account.

Expire the password set by an individual user

This task allows an administrator to manually expire the password of a specific user to enhance security by ensuring compromised or outdated credentials are not used.

Follow these steps to expire the password set by an individual user.

Before you begin

Log in to the Cisco ONP web interface, on page 6 with Admin permission.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USERS** tab.

a) Select the user whose password you want to expire.

b) Click **Expire**.

Create a new role

This procedure guides an administrator in defining a new role, assigning appropriate permissions, and making the role available for users.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **ROLES** tab. Then click **Create**.

a) In the **Create Role** dialog box, enter the **Role Name**, select the **Permissions** for the role, and click **Save**.

Note
You can select more than one permission.

b) In the **Success** dialog box, click **OK**.

Assign a role to a user group

This procedure helps the administrator to assign or update a role for a user group in Cisco ONP, ensuring the group has appropriate access permissions within the system.

Follow these steps to assign a role to a user group.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the Admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **USER GROUPS** tab.

a) Select the user group you want to update, and click **Update**.
b) In the **Update Group** dialog box, select the desired role from the **Role** drop-down list, and click **Save**.
c) In the **Success** dialog box, click **OK**.

Manage password through Dictionary

The dictionary rejects any new password that exists in the predefined list of passwords under the **Content** column in the **DICTIONARY** tab.

The system performs this password verification check against the dictionary during these events:

- New user sign-up

- Password change
- Password reset using forgot password option

Use this task to verify whether the new password set by the user exists in the list of predefined passwords:

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Procedure

Step 1 Click **Control Panel**.

The **Access Control Management** page appears.

Step 2 Click the **DICTIONARY** tab.

a) Enable the **Rejection Mode** toggle button to verify the password against the dictionary.

By default, this toggle button remains disabled.

b) Enter the password in the **Enter Passphrase** text box.

c) To specify the maximum number of matching passphrases, enter the limit in the **Enter Limit** text box.

d) Click **Search**.

The system displays the matching passphrases.

Note
If you enter a limit, the system displays only that number of matching search results. If you do not enter a limit, the system displays all matching passphrases.

Retrieve system logs

This task guides administrators or authorized users through the steps to retrieve, filter, and manage system logs for a specified time interval on the **System Logs** page. For more information, see Logs , on page 172.

Follow these steps to retrieve the system logs.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as an admin, or a user with User Management and Network Management permissions.

Procedure

Step 1 Click **Logs**.

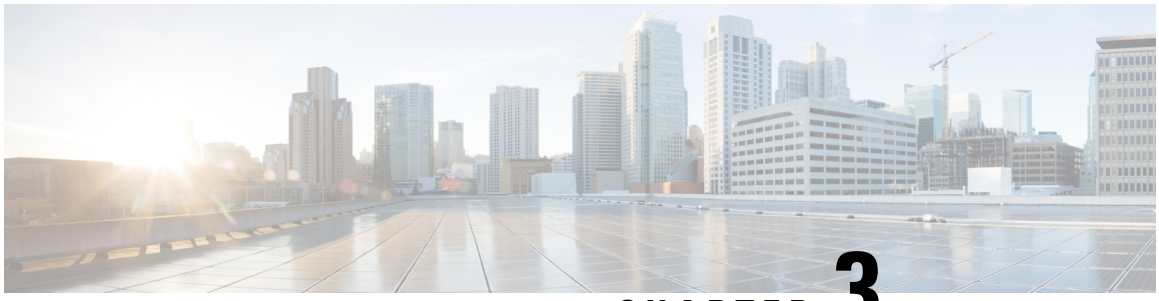
a) Click **Select Start Date**, and choose the start date. Similarly, click **Select End Date**, and choose the end date.

b) Choose the **Logs Category**.

c) Click **FILTER** to retrieve the logs.

Step 2 Perform the required actions in the **Logs** page.

If you want to.....	then...
export the system logs to an Excel sheet	click the **Export as CSV** icon.
export the system logs as a zip file	click the **Export Archive** icon.
import the zip file	click the **Import Archive** icon.
refresh the system logs page	click the **Refresh** icon.
delete the existing logs	click the **Clear Logs** icon.



CHAPTER 3

Design and Analyze Networks

Design a network using Cisco ONP

A network design using Cisco ONP is a network architecture planning process that

- allows users to create a new design manually or import an existing design,
- supports integration with various sources and tools, and
- provides flexibility in how network models are created and managed.

You can design a network in one of these ways:

- Manual design: Create a network design using the design palette.
- Import design: Import a network design from an Excel sheet, live network import, Cisco Transport Planner, or another instance of Cisco ONP.

Manually design a network using Cisco ONP

Table 4: Feature History

Feature Name	Release Information	Feature Description
Multi-Layer Platform (MLP) Greenfield Design with NCS 4k-1k-2k	Cisco ONP Release 4.1	This feature allows you to: • Support NCS 4K-1K-2K multiplatforms • Visualize new layout for Txp and SVO for NCS 2000 node • Support different OTN service types with protection • Edit layout for NCS 4000 and NCS 1004 nodes

Use this procedure to create a network in the Cisco ONP.

You can create any of these network designs:

- Spectrum Switched Optical Network (SSON) that uses flexible spectrum allocation, where the required minimum spectral resources are allocated adaptively based on traffic demand and network conditions.
- Non-SSON network that allocates single spectrum (fixed spectrum) irrespective of the traffic demand and network conditions.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Choose **File** > **New**.

Step 2 In the **Create New Network** dialog box, choose the required options to create a network.

Choose	To create...
NCS 2000	a non-SSON network that contains NCS 2000 and NCS 4000 nodes, or an SSON network including NCS 2000, NCS 1004, and NCS 4000 nodes
NCS1010	a network that contains only NCS 1010 nodes

a) If you want to create an SSON network, check the **SSON Network** check box. Otherwise, do not check the check box..

b) Choose the **System Release** for NCS 2K from the drop-down list.

You cannot change the system releases that are available for NCS 4K and NCS 1K.

c) Click **Create**.

The application displays a map and the design palette. For details, refer to Design Palette, on page 176.

Step 3 Click the **Drawing Tool** icon (pencil and ruler crossed), and add sites and other network elements.

a) Add sites to the map using the drawing tool.

Zoom in on the map to the desired level. Click any of the site icons (**ROADM**, **OLA**, or **Traffic**(4K-1K-2K)), and drag it to the sites on the map. Drag or click the map where a site has to be placed, when the cursor changes to the site icon.

Note

- SRLG is not supported in the SSON networks.
- Cisco ONP calculates the distance based on the x and y coordinates on the map. Before you create the design, zoom in the map to the maximum for an accurate distance, because the distance is used to calculate signal degradation.

b) Click the **Fiber** icon and drag it to connect from one site to another site. Continue this for all sites.

c) Create services between the sites.

Cisco ONP provides only OTN service.

d) Click **OTN Service** (green) and add the service between the existing Traffic sites on the map.

e) Click **Media channel** (purple), or **Waves** (red), and add media channel, or waves between the existing sites on the map.

In the left pane, you can view a network tree panel with a default network name. The network elements added are displayed in the tree panel.

Step 4 Choose **File** > **Save As**.

a) In the **Give a Network Name** dialog box, enter a network name and click **Save**.

Create shared risk link group

Use this procedure to create Shared Risk Link Group (SRLG) using the Cisco ONP GUI. The SRLG feature enables routing of protected services.

Note SRLG is supported only for non-SSON networks that include traffic nodes.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to create the SRLGs.

Step 2 Click the network tree panel.

Step 3 Expand **Fibers**, and check the check box next to each fiber that should be in the same SRLG.

Step 4 After selecting all fibers, right-click and choose **Create SRLG**.

Cisco ONP creates an SRLG with a unique name, which you can subsequently rename.

Import a network using an Excel sheet

Use this procedure to import a network into Cisco ONP, using an Excel sheet.

Follow these steps to import a network into Cisco ONP, using an Excel sheet.

Note By default, the system release of the Excel-imported network is 11.0.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Choose **File** > **Download Import Template** to download the Excel sheet template.

The template has tabs and fields that you must fill in the Excel sheet. For details about these tabs and fields, refer to Tabs available in the Excel sheet template, on page 24.

Step 2 Fill the network details in the template file or edit the current network file, and save the file.

Step 3 Choose **Import** > **Excel** .

Step 4 Browse for the file, select it, and click **Import**.

The selected network is imported.

If there are errors in the imported data, a pop-up error message is shown in case of new import, and the errors are available under the **Elements** > **Messages** tabs in case of updating the existing network.

Tabs available in the Excel sheet template

This table lists the various tabs available in the Excel sheet template used to import a network.

Table 5: Tabs available in the Excel sheet template

Tabs	Description
Network	Label (name of the network), Platform (NCS2000)
Sites	Site Label, Type, X coordinates, Y coordinates, Pre Equip Degree

Network imports from Cisco Transport Planner

The Cisco Transport Planner network import is a compatibility feature that

- allows you to import networks created and analyzed in Cisco Transport Planner into Cisco ONP, as `.mpz` files,
- prevents the need to recreate existing networks, and
- supports only networks from Release 11.0 or later for compatibility.

Supported hardware for CTP network import

Cisco ONP supports these hardware as part of CTP network import.

- Optical source files and transponders

  See Supported Optical Sources, on page 195, and Supported Cards and Pluggables, on page 181.
- Contentionless, colorless, and colored point-to-point demands
- Flex network
- Gain Equalizer

Note The Gain Equalizer node converts to a ROADM node when you unlock the site after a release upgrade.

- ROADM-SMR-9 and SMR-20
- All flex supported amplifiers, controller cards, and chassis types

Import an mpz design file from Cisco Transport Planner

Use this procedure to import an mpz file from Cisco Transport Planner to Cisco ONP.

Before you begin

- Log in to the Cisco ONP web interface, on page 6 as a user with network creation permission.
- Import the required optical source files and layout template using **Manage** > **Optical Source** and **Manage** > **Optical Source** options. For more information, refer to **Manage Alien**, and **Manage Layout** .
- Delete the unsupported parameters for Cisco ONP from the mpz file. For example, mpz networks with P-Ring and A2A demands are not supported for import. Delete these demands in Cisco Transport Planner, reanalyze the networks in Cisco Transport Planner, and import the mpz file into Cisco ONP.

The network must be in design-analyzed or upgrade-analyzed mode.

Procedure

Step 1 Choose **Import** > **MPZ**.

The **Import File (mpz)** dialog box appears.

a) Browse to the mpz file stored on your computer.

b) Click **Import**.

The mpz file is imported to Cisco ONP.

Note
If you view a blank screen when you click waves in the network tree, refresh the browser.

Step 2 Choose **Network** > **Upgrade** or **Network** > **Release Upgrade** to make any changes on the imported network.

Note
- You cannot go back to design mode on the imported mpz network.
- The wave label of imported mpz network in Cisco ONP is the service name present in the Cisco Transport Planner properties window.

Export the CPZ file

Cisco ONP saves the network design file as a .cpz file in its database. Use this process to export the design file to your computer.

The contents of the .cpz file depend on the network mode:

- In design mode, the .cpz file includes the design file, layout template, and optical source details.
- In analyze mode, the .cpz file contains several items: a design file, analyze file, ANS file, per-side ANS file, BOM, error messages, trace files, layout template, mpz, and report.
- For networks in upgraded mode, you can only export the last child in the parent-child hierarchy.

Note You can export only one network at a time.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network whose design file that you want to export.

The network opens.

Note
If a blank screen appears when you open a network, refresh the browser or log in to Cisco ONP again.

Step 2 Choose **Export** > **CPZ**.

Step 3 Inside the **Export .cpz file** dialog box:

a) Rename the file if necessary.

b) Click **Export**.

The design file is saved on your computer.

Import the CPZ file

Use this procedure to import the cpz network design files that are exported from another Cisco ONP instance.

Note You can import only the networks that are exported from the current release.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Choose **Import** > **CPZ**.

Step 2 In the **Import .cpz file** dialog box:

a) Click **Choose file**, and select a cpz network design file that you want to import into Cisco ONP, from your local system.

b) Click **Import**.

If the names of the optical source and layout template files in the database and the imported network file match, Cisco ONP prompts you to confirm whether you want to overwrite the existing file.

Note
The message **"Network already exists in the system with another user. New network will be created"**, you do not need to take any action. Cisco ONP automatically imports the network as a new network for you without changing the existing network.

c) If you want to overwrite the existing file, check the **Overwrite Network** check box.

If you do not check the box, Cisco ONP saves the imported network as a new network.

d) Choose the optical source files and layout template that you want to replace.

If you do not choose the optical source or the layout template file, the files will not be imported.

e) Click **Confirm**.

The imported network is saved in the Cisco ONP database.

Live Network Import

The Live Network Import (LNI) feature is a network import capability that:

- enables real-time import of deployed networks into Cisco ONP,

- supports networks with NCS 1004, NCS 2000, and NCS 4000 nodes , and
- allows you to view comprehensive deployed network details after import.

Table 6: Feature History

Feature Name	Release Information	Feature Description
Live Network Import	Cisco ONP Release 4.1	This feature allows you to import a live deployed network having NCS 1004, NCS 2000, and NCS 4000 nodes into Cisco ONP, using the LNI (Live Network Import) import template. This feature also allows you to view network topology, BOM, and layout report.

The Map displays the network topology, and you can check the node, fiber, OTN service, and media channel properties through the Network Tree and the Entity Editor.

Perform live network import

Use this procedure to perform live import of a network.

Before you begin

- Perform LNI only when the Cisco ONC is in a stable or running state. Do not perform LNI during the maintenance period for software upgrade.
- Configure all the mandatory parameters on the circuit.
- Make sure that the following Cisco IOS XR Software Maintenance Updates (SMUs) are loaded on the NCS 4000 devices on top of Cisco IOS XR Release 6.5.28:
  - ncs4k-6.5.28.CSCvu93045.tar
  - ncs4k-sysadmin-6.5.28.CSCvt67465.tar
  - ncs4k-6.5.28.CSCvv79518.tar
- Make sure that there is a provision for opening three TL1 sessions per NCS 2000 device for Live data collection. Avoid overloading NCS 2000 devices with TL1 sessions.
- Configure the fibers with the same channel numbers (Spectral Density, for example: 91.0/82.0) on both the source and destination ends.
- Check the card label set for these NCS 2000 cards and update it if they are not aligned.

PID	Card label
NCS2K-16-AD-CCOFS	AD-16-FS
NCS2K-20-SMRFS	SMR20-FS-CV
NCS2K-20-SMRFS-L	SMR20-FS

PID	Card label
NCS2K-9-SMR17FS	SMR9-17-FS
NCS2K-9-SMR24FS	SMR9-24-FS
NCS2K-9-SMR34FS	SMR9-34-FS
NCS2K-9-SMR34FS-L	SMR9-34-FS
15454-M-RAMAN-COP=	OPT-RAMP-COP
15454-M-RAMAN-CTP=	OPT-RAMP-CTP
NCS2K-OPT-EDFA-35	OPT-EDFA-35

- To open the Cisco ONP application, install Microsoft Excel on the client machine where you launch the browser.
- Log in to the Cisco ONP web interface, on page 6

.

Procedure

Step 1 Choose **Export** > **Download LNI Import Template**, and download the template which is in the form of an Excel sheet.

Step 2 Fill the template with the details of all the nodes belonging to the network to be imported and save the file.

These fields are mandatory:

- Node IP
- User Name
- Password
- Connectivity Type—TL1 for NCS 2000 nodes and NETCONF for NCS 1004 and NCS 4000 nodes
- Connectivity port—830 for NCS 4000 and NCS 2000 nodes

Note
Enter a value in the range of 60 to 180 in the Connectivity Timeout field or leave the field empty.

Step 3 Choose **Import** > **Live Import**.

a) Browse and choose the saved file.

b) If you want to clean the existing LNI database of the nodes and perform a fresh import, check the **Fresh Import (Cleanup LNI Database)** check box.

Note
We recommend performing a fresh import of the live network.

Leave this check box unchecked to import the details for only a few nodes that had issues during the previous import.

Note

LNI import is not user-specific. When you perform a fresh import, Cisco ONP overwrites all the LNI data that are imported by the other users.

c) Click **Import**.
d) In the **Device Onboarding** dialog box, click **OK**.

Note
If you try to import a network of unsupported version, the device collection does not happen,. An error message "device collection failed" appears. See Supported Hardware and Software for LNI, on page 32.

Step 4 View the status of the LNI operation:

a) Click **Job Monitor**, and click **Check Progress** for the IMPORT_LIVE_NETWORK task, to view the status of the LNI operation in the **LNI Progress** dialog box. Click **Refresh** to see the updated status.

After LNI is completed, the job is removed from the **Job Monitor** page.

b) Click **Logs** to view the list of events that are related to the LNI operation, as logs.

Step 5 After the completion of the LNI operation, choose **File** > **Open**.

The format of the LNI imported network filename is LNI_<Date>_<Time>.

Step 6 Click the imported network name to view the network under the **Map** tab and its corresponding network tree in the left panel.

The aggregated node that includes NCS 1004, NCS 2000, and NCS 4000 appears in purple, and the aggregated node that includes NCS 1004 and NCS 2000 appears in orange in the network tree. You can view the tag **Imported from Network** in the interface.

Note

- Even if errors occur during the LNI operation, the operation is not canceled. In this case, when you open the imported network, a warning message appears.
- You can view the errors under the **Elements** > **Messages** tab.
  - Device collection failure is listed under critical messages.
  - The reason for failure is listed under noncritical messages.
- If both NCS and Non-NCS PIDS are present in the inventory, Cisco ONP enables the **Enable NCS** option. You can edit this option during upgrade after unlocking the site, if necessary.
- Service path for the restored circuits is displayed as:
  - Primary Path: Working path before restoration
  - Secondary path: Protected path
  - Restoration path: Current work path after restoration

Note
If the circuit is not in the restored state, the restoration path is not shown.

- SSON circuits carrying protected OTN services are merged as Client 1+1 protected Media Channel. Due to this, you may see difference in total number of SSON circuits between the imported network in Cisco ONP and the actual network.

- If LNI is not installed properly, you may encounter the errors such as LNI failure or LNI not able to purge the data. In such cases, we recommend starting and stopping the LNI services in the server where Cisco ONP and LNI are installed using these commands:
  - Stop the LNI services.

    ```
    root:~/$ONP_HOME# cd LNI
    root:~/$ONP_HOME/LNI# bash ciscolniinstaller.sh -o stop -t update -m offlinemode
    ```

  - Start the LNI services.

    ```
    root:~/$ONP_HOME/LNI# bash ciscolniinstaller.sh -o start -t update -m offlinemode
    ```

Note
Wait at least 5 minutes after starting the services for LNI services to resume before triggering a new live network import.

What to do next

Click the **BOM** tab to view the BOM details of the network.

Note The PIDs of prototype cards are shown as "NA" in the BOM details of the LNI network.

You can export the CPZ, import the CPZ, and share the imported network. Use the **Entity Editor** to view network properties.

Ports Used in LNI

LNI application uses the following ports. If any port is shut down due to any failure, then the service is restarted by the Docker system.

Port	Service	Usage
8761	Eureka Service	Registration and discovery service, which holds the information about all microservice applications
8088	API Gateway	Receives all the incoming requests, and then delegates the requests to internal microservices like LNI Broker
8086	Collector Service	Collects metrics and operation data from the devices
8082	Device Manager	Responsible for device onboarding process
8083	Inventory Service	Provides inventory data
9975	TL1 plug-in Service	South bound interface plug-ins for TL1 protocol-based NCS 2000 devices
8898	NCS 2K Inventory Adapter Service	Adapter module to transform NCS 2000 device response from collector to Cisco ONP NCMS schema-based POJO

Port	Service	Usage
8899	NCS 4K Inventory Adapter Service	Adapter module to transform NCS 4000 device response from collector to Cisco ONP NCMS schema-based POJO
8900	NCS 1K Inventory Adapter Service	Adapter module to transform NCS 1004 device response from collector to Cisco ONP NCMS schema-based POJO
9976	NETCONF plug-in Service	South bound interface plug-ins for NETCONF based 1K/4K devices
8102	LNI Broker Service	Provides interfaces for Cisco ONP BE service to trigger live network import
8085	Topology Service	Provides network topology data
8090	Circuit Service	Provides network circuit data
8024	NETCONF Adapter Service	Common adapter for Topology and Circuit services
8091	Model Aggregator Service	Aggregates inventory, topology, and circuit details under NCMS schema-based networks
8092	TL1 Adapter Service	Common adapter for Topology and Circuit Service
5601	Kibana	Data visualization and exploration tool that is used for log and time-series analytics, application monitoring, and operational intelligence use cases **Note** The default Edge browser on Windows OS is not supported for viewing the Kibana logs. Cisco recommends using Firefox or Chrome browser for viewing the Kibana logs.
2181	Zookeeper	Keeps track of status of the Kafka cluster nodes, and also keeps track of Kafka topics, partitions publish-subscribe messaging system that enables inter service communication
9092	Kafka	Publish-subscribe messaging system that enables inter-service communication
27017	Mongo	Database to persist services data

Supported Hardware and Software for LNI

The following table describes the software versions and hardware requirements of the network imported through LNI.

Table 7:

Property	Values
Network	

Property	Values
Network Type	SSON
Platform	ETSI
System Release	NCS 2000: R11.1, and R11.1.1.2 NCS 1004: XR 7.0.1 NCS 4000: XR 6.5.2.8
Site/Node	
Site Type	4K-1K-2K: ADD/DROP, 1K-2K;Regen, 2K:ROADM/OLA
ROADM	SMR-20, SMR-9-17FS, SMR-9-34FS, SMR-9-24FS
Amplifier	RAMAN-CTP, RAMAN-COP, EDFA35-24, EDFA35-35
Degree Mesh Type	DEG-5/UPG-4
Chassis Type	4K: NCS4016, 2K:NCS2006, 1K:NCS1004
Power Supply	4K-DC, 1K-DC, 2K-DC40
ECU	ECU-S
Controller Card	TNCS-2, TNCS-2O
Channel Rule	82
Line Cards	NCS1K4-1.2T-K9=, NCS4K-4H-OPW-QC2
Evolved Mesh	ON and OFF
Node Protection	2K: Separated shelves, 4K: Single shelf
Mpo16Lc	MPO-16LC Unit
Mpo16ToMpo08	MPO16TO2MPO8Cable
Cascaded SMR	Yes
Enable NCS	Yes
Use Payg	No
Connection Verification	Yes, No
MF Unit	MF-6RU, MF6-10RU, or MF-1RU
Structure	Line, Multidegree, Terminal
Scalable upto degree	4, 8, 12

Property	Values
Power redundancy	Yes
IP Address	IPv4
Fiber	
OSC Frame Type	Auto
DCN Extension	Yes
ENE/GNE	Yes
Length	Yes
Loss	Yes
Measurement Unit	KM
Length based Loss	No
Raman Amplified	Yes
Fiber Type	G652-SMF-28E
Connector Loss A	Yes
Connector Loss B	Yes
Cross OSC and Parallel OSC	Yes
Media Channel	
Traffic Type	NCS1004_SP_16QAM_16QAM_300G_27%SDFEC_60GBd
Protection	Unprotected, and 1+R
Path	Actual Path
Regen	Regen site
Multicarrier	No
Contentionless	Yes
Circuit State	Restored, Unrestored
Service	
Service Type	100GE, 10GE, STM-64
Protection	1+1, Unprotected, 1+R, 1+1+R, 1+1+R+R
Path	Actual Path
Client Type (1K)	OTU4

Property	Values
Interface Type (1K)	BH
Trunk Mode (1K)	200G, 300G
Baud Rate (1K)	60 and 69 GBd
Client Pluggable	ONS-QSFP28-LR4=, QSFP-100G-SR4-S=,ONS-QSFP-4X10-MLR=

Limitations of LNI

These are the limitations, unsupported features, and known constraints of LNI, and scenarios where LNI may not function as expected and the available workarounds.

- Simultaneous import of multiple live networks and scheduled import are not supported. LNI does not support importing Non-SSON networks, Non-Contentionless configurations, circuits with NCS 2000 Transponder or Muxponder cards, or NCS1001, NCS1004, and NCS4000 devices.
- The chassis position in the layout may not be accurate in the live imported network. NCS 2000, NCS 1004, and NCS 4000 chassis are placed in separate racks to provide a clearer layout view.

  Workaround: You can edit the layout after network upgrade and analysis.
- If X, Y coordinates are not configured in the devices, nodes are overlapped in the Cisco ONP map.

  Workaround: Configure X, Y coordinates before importing the network for a better view of the topology in Cisco ONP map; otherwise, you can drag and drop the nodes in the Cisco ONP map and adjust the node position after importing.
- The Scalable upto degree parameter is not imported from the real device. Cisco ONP chooses the maximum scalable up to degree based on the number of line sides and contentionless sides present on the node.

  Workaround: Unlock the node after upgrading and change the scalable upto degree. After unlocking the site, use the layout template to rearrange the layout.
- Cisco ONP imports the proto-PID, if present in the inventory, and show as N/A PID in the Cisco ONP BOM. Duplicate media channel labels are not supported. If multiple media channels with the same label exist in the network, only one is imported; the rest are discarded.
- Fiber name, source, and destination names may not match between imports; source and destination site names may interchange for bidirectional fibers. Fibers may not associate with the correct optical subnet if channel numbers differ at source and destination, causing amplifier output power issues. Workaround: Correct channel numbers at both ends and re-import or associate fibers with the correct optical subnet after upgrade.
- If the regenerated demand is in restored state, the restored path is shown as working or protected path, and service protection is shown as 1+R in Cisco ONP. Restoration details will not be available. Service protection type is shown as 1+1+R or 1+1+R+R only if restoration path is available. Otherwise, it is shown as 1+1.

  Preprovisioned cards are not listed in the Cisco ONP BOM and are populated only after a successful upgrade and analysis of the LNI network. Ensure that the cards are equipped to retrieve the PID details.

Optical subnets and their role in networks

An optical subnet is a network structure that

- consists of a collection of spans with defined properties,
- is automatically created when a new network is set up in Cisco ONP, and
- must exist in at least one instance for every network.

When a new network is created, Cisco ONP links an optical subnet to it, ensuring that each network has its own optical subnet for proper operation.

Create optical subnet

Use this procedure to create an optical subnet in Cisco ONP for Non-SSON and SSON networks.

Note Check the **Current Subnet** check box in the properties window below the network tree, to make the subnet you created as the current subnet. You cannot uncheck the **Current Subnet** check box.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the required network (Non-SSON or SSON) in which you want to create a subnet.

Step 2 Expand **Subnet** in the network tree panel.

Step 3 Right-click **Optical Subnet**, and select **Create Optical Subnet**.

Step 4 In the **Create Optical Subnet** dialog box:

If you are creating optical subnet for...	Then...
non-SSON network	From the **Cband Rules** drop-down list, choose the C-band design rules for the new optical subnet, then click **Save**.

If you are creating optical subnet for...	Then...
SSON network	• From the **Band Type** drop-down list, choose either **C-Band** or **L-Band**. • From the **Spectral Density** drop-down list, choose the spectral density for the new optical subnet that you want to create. The selected spectral density determines the value of **Name**, **CBand Rules** or **LBand Rules**, and **Maximum Number of Channels** that appear in the **Create Optical Subnet** dialog box. • Click **Save**.

Step 5 (Optional) After the new optical subnet is created:

If you want to...	Then...
select a new spectral density	select a new spectral density from the **Spectral Density** drop-down list in the properties window displayed under the network tree.
add a fiber to a subnet	add a fiber to a subnet from the **Fiber links** drop-down list in the properties window. The fiber now appears in the **Fiber links** field. When you select the optical subnet, its corresponding fiber is highlighted in the map.
add a fiber to a subnet from the network tree panel	• Right-click the required optical subnet and select **Edit Fibers**. • In the **Info** dialog box, click **OK**. The user interface will freeze to allow fiber selection from the map. • Select the required fiber and click the **Done** button appearing near the zoom icon. **Note** When a fiber is added to one of the subnets, it is automatically removed from the other subnets. Only one subnet rule is associated with each fiber.

Cisco ONP creates the new optical subnet with your selected properties and places it under **OpticalSubnet** in the network tree panel.

Share a network

Use this procedure to share a network with one or more users or user groups.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network that you want to share.

Step 2 Choose **File** > **Share**.

Step 3 In the **Share Network** dialog box, select one or more users or user groups, and then click **Share**.

You can share the network with selected users or user groups in read-only mode.

Access a shared network

Use this procedure to open a network shared by another user and save an editable copy for your own work.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open a shared network.

a) Choose **File** > **Open Shared**.

b) In the shared network list, choose the network you want to open.
The shared network opens in read-only mode.

Step 2 Choose **File > Save As**.

Step 3 Enter a name for your copy and click **Save**.

A copy of the shared network is saved.

You now have your own editable copy of the shared network. You can work on it according to the privileges of your user role.

Step 4 (Optional) If you want, share your updated network with other users.

Unshare a network

Use this procedure to remove user or user group access to a previously shared network, ensuring only authorized individuals retain visibility and control of the network.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network you want to unshare.

Step 2 Choose > **Share**.

Step 3 In the **Share Network** dialog box, remove the name of one or more users or user groups from the list, then click **Share**.

The shared network is no longer available to the users or user groups that are removed.

Analyze the network

After completing the network design, use this procedure to analyze the network.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network that you want to analyze.

Step 2 Analyze the network:

a) Choose **Network** > **Analyze**.

The analysis progress indicator shows the current analysis status. After successful analysis, the network goes to **Analyze Mode**.

b) If you see the "Analysis Failed." message, navigate to the **Elements** > **Messages** tab to see the list of error details in the analyzed network.

By default, the system displays only the key messages when the **Critical Only** toggle button is enabled. If you want to view the entire network message, disable the **Critical Only** toggle button.

c) Resolve the error and analyze the network again. Continue until you resolve all errors.

Note
You may see the error message 'Unexpected Situation 999' if incorrect property values are entered or changed during network design. Contact Cisco TAC to identify the exact cause of the error. Afterwards, modify the suggested property value so that the network analysis completes successfully.

Bottom-up flow and network creation

A bottom-up flow is a network creation approach that

- enables incremental, step-by-step building of a network over several days,
- allows analysis and report generation at each phase without requiring all services or waves to be configured on the first day, and
- provides flexibility in the order of adding network elements such as services and waves.

How bottom-up flows work

Summary

The bottom-up flow process enables gradual, phase-based network creation and analysis, giving users flexibility in building and evaluating their network incrementally.

The key components involved in the process are:

- Network administrator: Builds and configures the network in stages.
- Network topology: Consists of sites and fibers initially added to form the network's structure.
- Services and waves: Additional network components that can be added over time for increased functionality and connectivity.

Workflow

The process involves the following stages:

1. On Day 0, the administrator creates the network by adding all sites and fibers to define the topology. They can analyze the network and view reports at this stage without configuring services or waves.
2. On Day 1, the administrator adds waves between sites (including both previously added and new sites/fibers), then re-analyzes and reviews updated reports.
3. On Day 2, the administrator adds services and tags the waves created in the previous stage, as well as incorporates additional sites and fibers as needed, with ongoing analysis and reporting.
4. After the initial topology is created, services or waves can be added in any order, without following a prescribed sequence.

Result

The bottom-up flow process supports flexible, staged network development and ongoing analysis, optimizing the configuration and deployment of Non-SSON networks.

Idle timeout in the Analyze mode

An idle timeout in analyze mode is a session management feature that

- logs users out of Cisco ONP if the browser is inactive for a default duration of 15 minutes,
- allows system administrators to disable or adjust the timeout through server configuration options, and
- affects ongoing network analysis by running it in the background if logout occurs during an active analysis cycle.

Idle timeout settings and session restoration behavior

The default idle timeout in Cisco ONP is 15 minutes. System administrators can disable this timeout by setting the enabled option to false in the configuration file, or adjust the timeout duration by editing the duration option.

If a session times out during an analysis, network analysis continues to run in the background. When the user logs in again:

- If the analysis is ongoing, the progress bar appears and no actions are allowed.
- If the analysis is complete, the network opens in Analyze mode.
- If the analysis failed, the network opens in Design mode and the failure reason can be viewed under **Elements** > **Messages**.

Upgrade the analyzed network

Use this procedure to upgrade an existing network that is in analyzed mode. You can change specific properties of a network element while keeping the network layout and design locked.

Upgrade is supported for both SSON and for non-SSON networks.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network that you want to upgrade.

Step 2 Upgrade the network:

a) Choose **Network** > **Upgrade**.

b) Click **Yes** .

The message “Network Upgraded Successfully” appears. The network goes into upgrade mode and network elements such as sites, fiber, waves (for non-SSON), and media channel (for SSON) are locked.

Step 3 To modify a network element in the network tree panel, right-click it, and click **Unlock**.

Unlock individual elements at the node, side, add/drop card, or amplifier level in the network tree hierarchy.

Make these modifications:

- Edit properties of network elements.
- Delete elements from the network.
- Add a new site, wave, service, demand, optical subnet, or fiber into the network map.

Step 4 Choose **File** > **Save**.

The newly added elements are automatically displayed in the network tree panel, and by default, remain unlocked.

Note
To insert a node in upgrade mode, unlock the fibers connected to that node, then add the node to the network.

Step 5 Choose **Network** > **Analyze**.

After the analysis is completed, the newly added elements are locked, and the optical reports and installation parameters of the upgraded network are updated.

When you add services or fibers while upgrading a network with an applied layout template, the template updates to include the new service or fiber. You can export the template, make changes, and reapply it to another network.

Step 6 Choose **Network** > **Design** to further upgrade the newly upgraded network design.

Each time you upgrade the network, Cisco ONP saves the new version as a child network and maintains the parent-child relationship.

Upgrade LNI network

Use this procedure to correct errors in your LNI network, modify ,and reanalyze it, and view updated BOM, layout, connections, and optical results.

Table 8: Feature History

Feature Name	Release Information	Feature Description
Upgrade LNI Network	Cisco ONP Release 4.1	This feature allows you to upgrade and modify the imported LNI (Live Network Import) network as required. You can also correct LNI errors, reanalyze the network, and view the updated parameters such as BOM, layout, connections, and optical results.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network imported through LNI that you want to upgrade.

Step 2 Upgrade the network:

a) Choose **Network** > **Upgrade**.

b) Click **Yes** .

The message “Network Upgraded Successfully” appears. After you upgrade the network, it enters upgrade mode, which locks elements such as sites, fiber, OTN services, and media channels.

Step 3 To modify a network element in the network tree panel, right-click it, and click **Unlock**.

Unlock individual elements at the node, side, add/drop card, or amplifier level in the network tree hierarchy.

Make these modifications:

- Edit the properties of network elements.
- Delete elements from the network.

- Add a new site, wave, service, demand, optical subnet, or fiber into the network map.

Step 4 Choose **File** > **Save**.

Each time that you upgrade the network, Cisco ONP saves the new version as a child network and maintains the parent-child relationship.

Step 5 Choose **Network** > **Analyze**.

Analysis succeeds only if the imported network is consistent and valid. If the analysis fails, perform the listed steps:

a) Check the reports under **Elements Messages** for failure reasons.
b) Resolve the issues by modifying the network manually in Cisco ONP or re-importing the network after correcting the errors.
c) Reanalyze the network.

Step 6 After analyzing the network:

a) Click the **Layout** tab and edit the layout manually to adjust chassis or card position for NCS 4000 and NCS 1004 platforms. See
b) Click the **BOM** tab and the **Results** tab to view the BOM and optical results.

Media channel unlocking scenarios

This table explains the various media channel conditions and the unlocking possibilities.

Table 9: Media channel unlocking scenarios

Conditions	Unlocking possibilities
The channel has OTN services. In 4K-2K cases, the service maps directly to the channel. In 4K-1K-2K, the service maps to the channel through the OTU4 trail.	Cisco ONP throws an error indicating that there are OTN services associated with the media channel. First, unlock the associated OTN services. Then, unlock and delete the media channel. You cannot update or delete the channel before unlocking the associated services.
Channel does not have OTN services going over it. For example, in the case of 4K-1K-2K, the media channel carries empty OTU4s.	Cisco ONP allows you to unlock the channel.When you unlock the channel, the properties of the channel and its child entities like Trail and Section are not cleared automatically, whether you or the system assigned them. You can only unlock the channel automatically if there are no associated OTU4s. After unlocking the channel, you can delete the channel. You cannot update the properties of the channel or its child entities. When the properties of the media channel or any of its child entities are auto-assigned, the system clears and sets only the wavelength to Auto. All other properties are not cleared.

Conditions	Unlocking possibilities
Channel has neither OTN services nor OTU4(s) going over it. In case of 4K-1K-2K networks, Media Channel does not carry even empty OTUs.	Cisco ONP allows you to unlock the channel and automatically clears auto-assigned properties. After unlocking you can perform these: • Update various properties of the channel and its child entities. • Delete the channel.

Possible error scenarios and the workarounds

This table provides the workarounds for the errors that are shown under the **Elements > Messages** tab.

Table 10: Error scenarios and the workarounds

Error message	Workarounds
Device Authentication failure	Check the username and password of the device provided in the LNI input Excel file. Retry the LNI import using valid device credentials.
Device collection failed or Device not reachable.	Check for any connectivity issues in the setup. Fix any identified issues and retry the LNI import.
In Site4.A, output power setting is not supported by the amplifier.	Unlock C-Band amplifiers for side A within Site4 in the Network tree, and set the correct output power. If you are unsure, choose Auto and analyze the result. Cisco ONP chooses the best value based on the configuration.
Cannot Route demand! Did not find any valid Omnidirectional Side.	For protected OTN or SSON services, ensure that at least two contentionless sides are present on both the source and destination sites. Add contentionless sides where necessary, then analyze the network configuration.
• **Demand OTU3 has unrecognized type [OTU3]** • **ServiceGroup does not support the demandType OTU3 for OTU3**	Only 100GE, 10GE, and STM-64 service rates are supported. If a different service rate exists in the network, unlock the specific service, change it to a supported service type, update the ODU time slot accordingly, and analyze the changes.
Primary OTN Demand [100GE_Flex] has invalid Timeslot ranges. Allowed ranges are [1-80]	100GE service type must have ODU time slot in the range of 1–80. If any other value is set, update the correct value or leave it blank so that Cisco ONP can set it to the correct value.
Cannot complete mesh connections at Site3.	Unlock the site and reanalyze.

Error message	Workarounds
No OTN demand found for NCS4K trunk port - NCS4016-B - OTU40/8/0/1.	No action required. This is an information message to the user.
Fiber between Node1.A and Node2.B has an invalid value in connector loss value	Unlock the corresponding fiber couple and update the connector loss value so that it is greater than zero. The typical value is 0.2.
Fiber between Nod1.C and Node2.C has an invalid value in Tot SOL Loss w/o Connectors.	Unlock the corresponding fiber couple and update the Tot SOL Loss w/o Connectors value so that it is greater than zero.
Span Fiber-2 is forced as Raman but no traffic is present.	Remove Raman forcing on the fiber, or force the path for a service to ensure it travels through a Raman-enabled span.
Couple Fiber-2 has Raman enabled on the duct but corresponding Raman Forcing is missing.	Force RAMAN-CTP or COP on the Fiber-2 connecting node interface, or remove RAMAN forcing on the Fiber-2.

Note No specific action is required for noncritical messages. These are just information messages to the user.

Upgrade the software release of a network

Table 11: Feature History

Feature Name	Release Information	Feature Description
Release Upgrade	Cisco ONP Release 4.1	This feature allows you to choose the NCS 2000 system release to the desired release (11.1.0, 12.0.1, or 12.1.0), while performing the release upgrade of CTP network, Cisco ONP network, network imported through Excel, and LNI network.

You can upgrade the software version of networks that are imported from CTP, created in Cisco ONP, LNI Network, or imported from Excel to any desired release version. The release upgrade is supported for both SSON and non-SSON networks that have NCS 2000 nodes with ROADM, OLA, Traffic, or Passthrough functionality.

Release upgrade is supported starting with NCS 2000 Release 11.1.0.

Note NCS 2000 supports SVO from the Release 12.1.0.

See Supported upgrade paths for network system releases, on page 46for the available upgrade releases for each network type.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network in which you want to perform the system release upgrade.

Step 2 Upgrade the software release of the network:

a) Choose **Network** > **Release Upgrade**.

b) From the NCS 2K drop-down list, choose the system release of NCS 2000, to which you want to upgrade.

c) Click **Submit**.

The upgraded network is saved as a child network.

Note If the PMD coefficient does not get updated with the expected value, update the fiber type first, followed by the PMD value when you edit the fiber properties.

What to do next

Unlock and modify network elements as needed.

Supported upgrade paths for network system releases

This table shows the available upgrade releases for each network type.

Table 12: Supported upgrade paths for network system releases

Network	Upgrade Release
CTP network (.mpz)	• From 11.0.0 to 11.1.0, 12.1.0, and 12.2.0 • From 11.1.0 to 12.1.0., and 12.2.0
Cisco ONP network	• From 11.0.0 to 11.1.0, 12.1.0, and 12.2.0 • From 11.1.0 to 12.1.0., and 12.2.0 • From 12.1.0 to 12.2.0
Excel imported network	From 11.0.0 to 11.1.0, 12.1.0, and 12.2.0

Network	Upgrade Release
LNI network	11.1.0 to 12.0.1 and 12.1.0 11.1.0 to 12.1.0 and 12.2.0 **Note** You cannot directly release upgrade an LNI network. Perform the following: • #unique_73. • #unique_74. • Release upgrade the analyzed LNI network.

Plan mode

Plan mode is a feature that

- enables what-if analysis on existing network designs,
- simulates network behavior under failure scenarios, and
- determines the ability to reroute services without providing guidance for expanding network infrastructure.

Table 13: Feature History

Feature Name	Release Information	Feature Description
What-if Analysis for OTN Services	Cisco ONP Release 4.1	This feature extends the current implementation of What-if analysis for the OTN Services that are connecting the aggregated nodes. The failure report includes the number of failed services, restored services, and unrestored services. This feature is supported forsworn (4K-1K-2K and 1K-2K) and non-SSON (4K-2K) networks.

Advantages of plan mode

The advantages of the plan mode are:

- Simulates and analyzes potential network issues and solutions,
- focuses on rerouting capabilities, and
- avoids requiring physical changes to network infrastructure.

Supported network elements

Supported network elements in plan mode include:

- An NCS 2000 aggregated node that includes ROADM, OLA, and passthrough nodes
- Traffic nodes including1K-2K, 4K-2K, and 4K-1K-2K
- Nodes created in Cisco ONP
- Networks imported from Cisco Transport Planner in mpz format
- Networks imported from LNI

Limitations of plan mode

Plan mode has these limitations:

- Only users with PLANNER and ADMIN roles can access the Plan mode.
- Plan mode does not guide you in turning up new wavelengths or adding new network components.

Use this procedure to evaluate potential network failures and review restoration outcomes by simulating fiber and site outages in Plan mode.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with admin or planner role.

Follow these steps to perform a what-if analysis in Plan mode

Procedure

Step 1 Open the analyzed network.

Step 2 Choose **Network** > **Enter Plan Mode**.

The network switches to Plan mode. In this mode, you can perform what-if analysis by failing fibers and sites.

Step 3 Fail ne or more sites:

a) In the network tree, expand **Sites**.
b) Right-click the site, and select **Fail**. Alternatively, right-click a site on the map and select **Fail**.
c) To fail multiple sites, select them and choose **Fail**.

Step 4 Fail one or more fibers:

a) In the network tree, expand **Fibers**.
b) Right-click the fiber, and click **Fail**. Alternatively, right-click a fiber in the map and select **Fail**.
c) To fail multiple fibers, select them and choose **Fail**.

When a fiber fails, all media channels or waves, OTN services, and demands that pass through the failed fiber also fail. Symbols on the map indicate these failures:

- Failed channels: Red cross
- Fibers impacted due to site failure: Yellow cross
- Restored channels: Green check

d) To undo the fiber failure, right-click the fiber, and click **Undo Fail**.

Step 5 (Optional) Create a failure set if you wish to group selected failures. SeeCreate a failure set.

Step 6 After testing, restore the failed fibers by choosing **Restore**.

The restored channels are indicated by a green check mark in the network tree and map.

All media channels or waves, and demands that pass through the restored fiber are also restored. The Path Computation Element (PCE) restores OTN services based on optical feasibility and OTN constraints.

Step 7 Export the failure report:

a) Choose **Export** > **Failure Report** to export the failure report as an Excel file. The failure report includes the parameters described in Failure report , on page 50.

b) Alternatively, click **Export** in the **Failure Report** area under the map.

Review unrestored channels and reasons for restoration failure in the **Elements** > **Messages** tab.

Step 8 Exit Plan mode:

a) Choose **Network** > **Exit Plan Mode**.

The what-if analysis and failure report are completed and exported, providing insight into service impact and recovery.

Create a failure set

Use this procedure to create and manage failed fibers and sites as a failure set within a failure group. You can simulate or track network outages efficiently in a single action.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open a network and enter the Plan mode.

Step 2 Right-click the **Failure Groups** option in the network tree panel.

Step 3 Click **Add Failure Group**.

A failure group gets created.

Step 4 Add fibers and sites to the group.

a) Choose the **Fibers** and **Sites** to fail by selecting the check boxes next to them.

b) Right-click the chosen **Fibers** and **Sites**, and click **Fail**.

Step 5 Right-click to the network name and click **Add Failure Set**.

Step 6 Select the failure group to which the failed fibers or sites must be added.

The system creates the failure set under the failure group and adds the failed fibers or sites to it.

Note

If a network has dark fibers that do not carry traffic, the system does not consider those paths for restoration.

Failure report

This table describes the various parameters of the failure report.

Table 14: Failure report

Report	Description
Failed Fibers	Shows the failed fibers in the network.
Failed Sites	Shows the failed sites in the network.
Impacted Fibers	Shows the fibers that are impacted due to the site failure.
Total Channels	Shows the total number of media channels in the network.
Failed Channels	Shows the total number of media channels that are passing through the failed ducts or sites in the network.
Restored Channels	Shows the total number of media channels that are restored from the failure state.
Unrestored Channels	Shows the total number of media channels that are not restored from the failure state due to the unavailability of alternate paths.
Fiber HotZones	Shows the fibers that have utilized greater than or equal to 80% of the bandwidth. You can modify the threshold by updating the value in the Feature.Properties file. • **Fiber**: Shows the fibers that are listed under fiber hot zones. • **Utilization Before (%)**: Shows the percentage of bandwidth that is utilized before the channel restoration. • **Utilization After (%)**: Shows the percentage of bandwidth that is utilized after the channel restoration.
Total Services	Shows the total number of services going through the fiber that was failed.
Failed Services	Shows the number of failed services going through the fiber that was failed.
Restored Services	Shows the number of restored services going through the fiber that was restored.
Unrestored Services	Shows the number of unrestored services going through the fiber that was restored.

Import optical sources

Use this procedure to import an optical source

An Optical source wavelength is a way to connect a DWDM interface from any external element to a third-party optical network.

.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Create an optical source from an Excel template

Procedure

Step 1 Choose **Manage** > **Optical Source**.

The **Manage Optical Source** dialog box appears.

The default optical sources available in the server include:

- OpticalSources_NCS2K_400GXP-LC_NCS4K-4H-OPW-QC2
- NCS1004_OpticalSources_V3
- ONS-CFP2D-400G-C-OpticalSources-V2.mxd
- QDD-400G-ZRP-S-OpticalSources-V2.mxd

Note
By default, all existing optical source files are loaded in the server.

Step 2 Click **Add**.

The **Import Optical Source (.mxd)** dialog box appears.

Step 3 Click **Choose File**, browse to the .mxd file stored on your local system, and click **Import**.

After the optical source is imported, a list of related interfaces appears.

Step 4 Select the check box next to each interface you want to import.

After you import the optical sources and their interfaces, they appear in the Type drop-down list in the properties window of the network tree. Use these interfaces when you create waves in your network design.

What to do next

Go to Download optical sources, on page 51 to download the optical source for Cisco ONC.

Download optical sources

Use this procedure to download an optical source.

Procedure

Step 1 Choose **Manage** > **Optical Source**.

The **Manage Optical Source** dialog box appears.

Step 2 Select one or more optical sources to download.

The selected optical source data is downloaded in the chosen format.

Delete optical sources

Use this procedure to permanently remove unwanted optical sources from Cisco ONP.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Choose **Manage** > **Optical Source**.

The **Manage Optical Source** dialog box appears.

Step 2 Choose one or more optical sources to delete.

Step 3 Click **Delete**.

Cisco ONP permanently removes the selected optical sources or aliens.

Layout template

A layout template is a reusable configuration model that

- enables the design of consistent layout configurations for a network,
- applies fixed layout rules to multiple nodes, and
- saves time, reduces effort, and minimizes configuration errors.

Layout templates are especially useful when deploying NCS 2000 networks that require identical configuration across several nodes. Defining the layout once allows network engineers to ensure uniformity and compliance with network design standards during deployment.

Note Layout templates do not support configurations where there is a mix of TXP and Real card labels for transponders.

Export layout template

Table 15: Feature History

Feature Name	Release Information	Feature Description
Layout Template Enhancement	Cisco ONP Release 4.1	This feature allows you to export the layout template for an individual site or for all the sites. The layout template export is possible only if the network is analyzed in Cisco ONP Release 4.1. The export of layout template is supported on 4K, 4K-1K-2K, and 2K nodes.

Use this procedure to export the layout template for a specific site or for all sites.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network to export the network layout template.

Step 2 Choose **Network** > **Analyze**.

Note
Network must be successfully analyzed to proceed further.

Step 3 Click the **Layout** tab.

Step 4 Click the **Hierarchy** tab.

Step 5 Click the name of a site to download the layout template.

Step 6 Hover the mouse pointer over the **Export** icon and click **Layout Template** for current site or all Sites.

The **Export Layout Template** dialog box appears.

Step 7 Click **Export**.

Note

- Export the layout template only in the analyze mode. If you export layout templates in upgrade or release upgrade modes, the results may be inaccurate.
- You can export the layout template for nodes of type 4000 and 1000. However, the exported layout template includes only the layout for NCS 2000 nodes. To export the layout template for the node types NCS4K-1K-2K and NCS1K-2K, complete these steps:
  - Right-click the site name under the **Hierarchy** tab, and click **Export**.
  - Click **OK** to export the layout template in text format.

- The layout template for NCS 2000 is provided in XML format.

Import layout template for NCS 2000 network into Cisco ONP database

Use this procedure to import a template into the Cisco ONP database.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Choose **Manage** > **Layout Templates**.

Step 2 Click **Add** in the **Manage Layout Template** dialog box.

Step 3 Click **Choose Files** and select a template from your local system.

Step 4 Click **Import**.

The template is imported to the Cisco ONP database.

Download a layout template for NCS 2000 network

Use this procedure to download a template from the Cisco ONP database:

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Choose **Manage** > **Layout Templates**.

Step 2 Choose the template that you want to download and click **Download**.

You can also choose multiple templates.

The selected layout template is saved to your local system.

Delete Layout Template for NCS 2000 Network

Use this procedure to delete a NCS 2000 Network template from the Cisco ONP database:

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Choose **Manage** > **Layout Templates**.

Step 2 Choose the template that you want to download, and click **Delete** to delete the template from the Cisco ONP database.

You can also choose multiple templates.

Apply NCS 2000 layout template into a site

Use this procedure to configure the layout of the NCS 2000 section for a site. Although the site can be NCS4K-2K, NCS1K-2K-4K, or NCS1K-2K, you should apply the template only to the NCS 2000 section.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open a network that contains the site where you want to apply the layout template.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, expand **Sites** and choose the site.

Step 4 In the **Layout Template** drop-down list, choose the required template.

Note
Ensure that the other properties under the **Layout** section, such as **Chassis Type**, **Power Supply**, **Controller Card**, **Node Protection**, **Redundant Controller Card**, and **MF-Unit** are set to *Auto*. Otherwise, the **Layout Template** drop-down list remains disabled.

The NCS 2000 layout template is applied to the NCS 2000 section of the selected site.

Import layout templates into NCS1K-2K and NCS4K-1K-2K sites

Use this procedure to add exported layout templates for NCS 1000 and NCS 4000 into 4K-2K and 4K-1K-2K sites.

Note If you modify an exported template, rename it before reapplying in upgrade mode to ensure changes are visible in the layout view.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network that has the site to which you want to apply the layout template.
Step 2 Click the **Layout** tab.
Step 3 Click the **Hierarchy** tab.
Step 4 Click **Edit** to enable the edit mode.
Step 5 Right-click the site where you want to import the layout template, then click **Import**.
Step 6 Choose the layout template that you want to import into the site and click **OK**.

Cisco ONP applies the chosen layout template to the specified site.

Layout visualization

A network layout visualization is a graphical feature that

- displays the arrangement of racks, chassis, and cards in a network designed using Cisco ONP,
- allows users to interact with and highlight specific hardware components, and
- enables zooming in and out for detailed or broad views.

Table 16: Feature History

Feature Name	Release Information	Feature Description
Layout Visualization and Edit	Cisco ONP Release 4.1	This feature allows you to view and adjust the position of NCS 4016 and NCS 1004 chassis and cards in the layout. This feature is supported only on 4K-1K-2K and 1K-2K aggregated nodes and not supported on stand-alone NCS 2000 node.

When you click a particular rack, chassis, or card in the **Hierarchy** panel, the corresponding hardware component is highlighted in the layout image. This feature enhances the ability to understand and manage complex network physical topologies.

View network layout

Use this procedure to view the network layout.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network for which you want to view the layout.

Step 2 Choose **Network** > **Analyze**.

Note
The network must be successfully analyzed to proceed further.

Step 3 Click the **Layout** tab.

Step 4 In the **Hierarchy** panel, click the site.

Note
The OLA sites are highlighted in green, ROADM sites are highlighted in blue, and Aggregated nodes are highlighted in purple.

Passthrough sites are not listed in the layout.

Step 5 Click any rack under a site to view the rack view of the network under the **Layout** tab.

Step 6 Click any chassis under a rack to view the chassis view of the network.

Note
When you click the Aggregated node under **Hierarchy** panel, NCS 1004, NCS 2000, and NCS 4000 series chassis are placed in separate racks.

You can click the screenshot icon to capture images of all rack layouts of the selected site.

Edit the layout manually

Use this procedure to position the NCS 4016 and NCS 1004 chassis and cards by manually adjusting the layout.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where 4K-1K-2K and 1K-2K aggregated nodes are added.

This feature is not supported on NCS 2000 node.

Step 2 Choose **Network** > **Analyze**.

Note
To proceed, make sure the network has been successfully analyzed.

Step 3 Click the **Layout** tab.

Step 4 Click **Edit** to enter the Edit mode.

Step 5 Select a chassis (4K-1K-2K and 1K-2K) or card from a rack.

Step 6 Drag and drop the selected chassis or card from a particular rack to an empty slot in the same chassis, a different chassis, or a different rack.

Step 7 Add pluggables to a card.

Note
Make sure to add the required cards.

a) Select the Rack.

The cards available in the rack are displayed.

b) Select the card to which you want to add pluggables.

The ports available in the card are displayed.

c) Select the pluggable for each port.

These pluggables are displayed:

Card	Supported Pluggables
NCS4K-4H-OPW-QC2	• ONS-QSFP8-LR4= • QSFP-110G-SR4-S= • ONS-QSFP-4*10-MLR=
NCS4K-4H-OPW-LO	• ONS-QSFP8-LR4= • QSFP-100G-SR4-S= • ONS-QSFP-4*10-MLR=
NCS1K4-1.2T-K9=	• ONS-QSFP8-LR4= • QSFP-100G-SR4= • ONS-QSFP28-LR4-S= • QSFP-100G-CWDM4-S= • QSFP-100G-SM-SR=

d) Click the check mark.

Step 8 Click **Done**.

Your changes are saved in the layout. You can view any new chassis or card that has been added to the layout in the **BOM** tab.

After you manually edit the layout, you can view the regenerated BOM.

View layout details using tooltip

Use this procedure when you need to quickly access hardware and port information in the Rack display.

Procedure

Step 1 Hover over a rack, chassis, or card in the Rack display to view summary details in a tooltip.

Step 2 Click **See More Details** in the tooltip to view information such as port number, type, pluggables, and rates.

Cisco ONP displays the detailed information for the selected rack, chassis, or card.

Copy configurations from one node to another

Use this procedure to copy the configurations of a specific node to a node at a different site.

You can copy the configuration only during a manual 4K-1K layout movement.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network from which you want to copy the configuration.

Step 2 Choose **Network** > **Analyze**.

Note
Network must be successfully analyzed to proceed further.

Step 3 Click the **Layout** tab.

Step 4 Select the rack, chassis, or card of a particular site.

Step 5 Select the site that will receive the configurations from the **Copy To** drop-down list.

Step 6 Click **New Rack** to add a new rack. Cisco ONP copies the configuration to the new rack

Step 7 Click **Done** to save the changes in the layout.

Note
You can also cut, copy, and delete racks, chassis, and cards in the layout.

Export the IPC report

Use this procedure to export the connections of a current site or all sites to an Excel sheet.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network from which you want to export the connections of a current site or all sites to an Excel sheet.

Step 2 Choose **Network** > **Analyze**.

Note
The network must be successfully analyzed to proceed further.

Step 3 Click the **Layout** > **IPC** tabs.

You can view the patches that are listed in the left pane. Click each patch to view the details such as position, card, and port of the source and destination sites.

Step 4 Hover over the **Export** icon, and click **Current site** or **All Sites** option.

The **Export IPC** dialog box appears.

Step 5 Click **Continue** to export the connections of the current site or all sites.

Export port usage of an LNI network

Use this procedure to export the port usage details of an LNI network.

Table 17: Feature History

Feature Name	Release Information	Feature Description
Multi-Layer Connections Phase 1	Cisco ONP Release 4.1	This feature provides the connection trace of a service across various interfaces in a network. This feature allows you to export the following: • Consolidated port usage report based on network in addition to the internal port details which you can view by hovering the mouse pointer over the tooltip • Port usage report based on sites • Port usage report only for LNI imported networks

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the LNI network whose port usage you want to export.

Step 2 Choose **Network** > **Analyze**.

Note
To proceed, make sure the network has been successfully analyzed.

Step 3 Click the **Layout** tab.

Step 4 Click the **Hierarchy** tab.

Step 5 Select the site for which you want to export port usage.

Step 6 Hover the mouse over the **Export** icon and select **Port Usage** for either **Current site** or **All Sites**.

The **Export Port** dialog box appears.

Step 7 Click **Continue**.

Cisco ONP exports the port usage details in Excel format.

Note

- If you modify any services in the NCS 4000 node after upgrading the LNI network, the changes in the port usage details will not update.
- The demand labels shown for the trunk ports of the NCS4K-DWDM line card in the port mapping report are not logically related to the NCS 4000 trunk ports. They are related to NCS 1004 client ports.

Define multilayer connections for an SSON network

Use this procedure to define the Multilayer Connections (MLC) such as cards and pluggables for 4K-1K-2K and 1K-2K aggregated nodes in an SSON network.

Table 18: Feature History

Feature Name	Release Information	Feature Description
NCS4K-1K-2K Multilayer Connection Trace	Cisco ONP Release 4.2	You can define Multilayer Connections (MLC) such as cards and pluggables for NCS 4K-1K-2K and NCS 1K-2K aggregated nodes in an SSON network. This new tab in the **Layout** page helps to view end-to-end MLC trace for OTN service starting from **NCS4K IN** until **NCS2K** Add/Drop for LNI network. Also, it helps to define new traces for the newly added service and maintain the network design and deployment.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network where you want to define multilayer connections.

Step 2 Define the MLC:

a) Click the **Layout** tab.

b) Click the **MLC** tab.

Alternatively, you can navigate to the **MLC** page by right-clicking the service name in the network tree and clicking **View in MLC**

You can view the service properties in a table. See MLC details, on page 63.

c) Click the service name to switch to the layout view.

You will view the layout and the service details in the right pane.

d) Select the rack, shelf, card, and ports from the drop-down lists for NCS4K In, NCS4K Out, NCS 1K In, and NCS 1K out, for both **Source** and **Destination** sites.

The NCS 2000 chassis details appear automatically.

Note
For an LNI imported network, all details appear automatically. If you add a new service, you can update its details.

e) Click the check icon to save your changes.

Click the refresh icon to remove changes you made after saving.

The updated details are included in the BOM.

Step 3 To export the MLC details, perform these steps:

a) Click the table icon to switch to the table view.
b) Choose **Export** > **MLC Traces**to export all the details available in the MLC table.
c) Choose **Export** > **LMP/TTI Connections** to export the details of Link Management Protocol (LMP) connections, which are between NCS 1004 and NCS 2000 cards, and Trail Trace Identifier (TTI) connections, which are between NCS 4000 and NCS 1004 cards.

   All these connections are included in the BOM.

Step 4 To filter the services displayed in the left pane, click the Filter icon and choose one of these options:

- Source Site
- Destination Site
- Type of the traffic
- Trace Origin
  - LNI: imported through Import Live Network option
  - User Created: created through Cisco ONP UI
- Trace Status
  - Completed: User has defined all MLC details,
  - Partial: User has defined only partial MLC details, and
  - Empty: User has not defined any MLC details.

Step 5 Click the three vertical dots and choose the option you need.

- **Enable Multi Select**: You can select up to the card level for different OTN.
- **Expand All**: Expands the service tree.
- **Collapse All**: Collapses the expanded service tree.
- **Show Trace Status**: Shows the trace status icon next to the service name.

Step 6 Click the three horizontal dots next to the service trace and choose the option you need.

- **Delete Trace**: Deletes the respective trace.
- **Locate in Map**: Shows the service in the map view.

Note
You can enable the same port number on the primary and secondary **NCS4K IN** nodes for Client 1+1 and other protection scheme.

MLC details

This section describes the various fields available in the MLC tab in the Layout view of a network.

The MLC tab includes these fields.

Table 19: MLC details

Properties	Description
Name	Name of the service
Group Name	Name of the group to which the service belongs
Type	Traffic type
Src Site	Source site
Src NCS4K In	Details of the rack, slot, card, port in the input side of the NCS 4000 chassis in the source site
Src NCS4K Out	Details of the rack, slot, card, port in the output side of the NCS 4000 chassis in the source site
Src NCS1K In	Details of the rack, slot, card, port in the output side of the NCS 1004 chassis in the source site
Src NCS1K Out	Details of the rack, slot, card, port in the output side of the NCS 1004 chassis in the source site
Src NCS2K AddDrop	Add/Drop multiplexer and demultiplexer connected to the NCS 2000 chassis in the source site
Src NCS2K MPO	Media channel between the source and destination sites
Dst NCS4K In	Details of the rack, slot, card, port in the input side of the NCS 4000 chassis in the destination site
Dst NCS4K Out	Details of the rack, slot, card, port in the output side of the NCS 4000 chassis in the destination site
Dst NCS1K In	Details of the rack, slot, card, port in the input side of the NCS 1004 chassis in the destination site
Dst NCS1K Out	Details of the rack, slot, card, port in the output side of the NCS 1004 chassis in the destination site
Dst NCS2K AddDrop	Add/drop multiplexer and demultiplexer that is connected to the NCS 2000 chassis in the destination site
Dst NCS2K MPO	MPO cable connecting the NCS 2000 chassis in the destination site
Media Channel	Media channel between the source and destination sites
Notes	Additional notes, if applicable

Properties	Description
Trace Origin	Indicates whether the service connections are user-created or imported through LNI.

Add new pluggables, alarm cables and 100G client bandwidth licenses to BoM

Use this procedure to add new pluggables, alarm cables, and 100G client bandwidth licenses to an existing BoM for the NCS 1004 and NCS 4000 platforms.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network you want to update.

Step 2 Analyze the network by choosing **Network** > **Analyze**.

Note
Ensure the network is successfully analyzed before proceeding.

Step 3 Click the **BOM** tab.

Step 4 Start adding new items:

a) Click **Add**.

The **New** dialog box opens.

Step 5 Specify the details:

a) Enter the Cisco part number of the pluggable, alarm cable, or 100G bandwidth license in the **Cisco Part Number** field.

b) Click **Add** to confirm the additions.

The new pluggables, alarm cables, or 100G bandwidth licenses are now listed in the BoM.

Designing networks with SVO card

A SVO card is a network hardware component that

- provides licenses based on functionality for features such as alarm correlation, performance monitoring, connection verification, and OTDR,
- serves as the primary card for all networks starting from Release 12.1.0, and
- can be deployed in both ROADM and TRAFFIC nodes as part of network designs.

Features of the SVO card:

The SVO card offers these key features and configuration options:

- The SVO card occupies two slots.
- It serves as the primary card for all networks starting from Release 12.1.0.
- For high availability, a node can be equipped with two SVO cards, but they cannot be in the same chassis.
- Two 10G SFP+ pluggables can be used to connect two SVO cards within a node.
- You can connect a Cisco ASR 920 switch to the SVO cards during network design.
- The SVO can function as either a card or a UCS based solution.

SVO licenses

- SVO cards require either a Base License or an SVO Full License which covers High Availability, Connection Verification, and Flex Spectrum. If the SVO Full License is not selected, the SVO Base License and High Availability are enabled by default.
- Types of SVO licenses include:
  - Cisco NMS: Features High Availability, Connection Verification, Flex Spectrum, and OTDR.
  - Third-Party NMS: Includes North Bound Interface (NBI), Alarm Correlation, Performance Monitoring, and Circuit Provisioning.

Chassis licensing:

- Every chassis added to the network must be licensed from Release 12.1.0 onwards. For networks upgraded to Cisco ONP Release 4.0 or higher, a new chassis license is required after analysis.
- Chassis licenses come in variants such as 1-chassis, 5-chassis, 10-chassis, 20-chassis, 50-chassis, and others, chosen based on cost optimization.
- A license is required for each chassis added to the network after the first chassis.
- Chassis License Flush Out allows you to replace existing chassis licenses with new ones. The current license remains active if the site is unlocked. However, you can use flush out only during network upgrade mode.
- You can continue using existing licenses with changes to the chassis unless you opt for the Chassis License Flush Out option.

SVO associations

A SVO association is a network configuration mechanism that

- enables a ROADM node equipped with an SVO card to manage OLA and DGE that may not have their own SVO card, and
- allows both manual and automatic association of secondary nodes to a primary node based on network topology and configuration, and

Associate OLA or DGE sites with SVO cards

Use this procedure to associate OLAsites with the SVO cards:

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 In the network tree panel, right-click any ROADM or Traffic site with SVO card.

Step 2 Click **Edit** SVO **Associations**.

Step 3 Select the OLA sites on the map to toggle the SVO connections. To confirm your selection, click **Done** at the top-right corner.

You can open widgets in the map and select the top section to view the association.

Note
You can also right-click any ROADM or Traffic site from the map and click **Edit SVO Associations**. For the DGE sites, the **Edit** SVO **Associations** option is not displayed.

During network analysis, the tool automatically associates the sites you do not associate with the SVO card.

Upload NETCONF XML files on SVO web interface

Use this procedure to upload NETCONF XML files on the SVO web interface to configure and provision network nodes using exported configuration data.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 In the browser URL field, enter the IP address of the SVO line card.

The login page appears.

Step 2 Enter the username and password.

Step 3 Click **Login**.

Step 4 Click the hamburger icon and select **Node Configuration**.

Step 5 Click the **Node Setup** tab.

Step 6 Click **Select files** .

Step 7 Browse to the NETCONF XML files exported from the Cisco ONP GUI and upload them.

If the passive unit ID in the NETCONF file exceeds the range 1 to 126, SVO displays an error message. Validate the XML file and import it again.

Note
If the FEC mode provisioned in the 200G-CK-C line card does not match with the value in the NETCONF XML file, SVO displays an error message. Remove the provisioned FEC settings for this card and reimport the XML file.

Export NETCONF XML Files for individual sites

Use this procedure to export NETCONF XML files for individual sites from the Cisco ONP GUI.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 In the network tree panel, enable the **Stage** button.

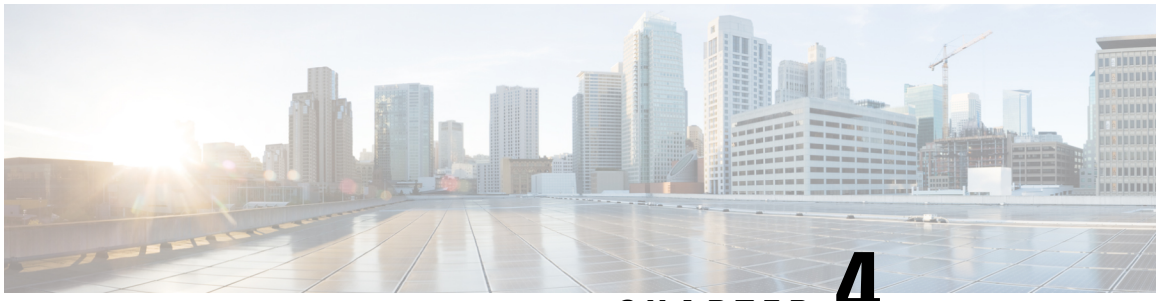
Step 2 Select the check box for the individual site.

You can select only one site at a time and download the NETCONF XML file for that site by enabling the **Stage** button.

Step 3 Right-click the site.

Step 4 Click **Generate NetConf XML**.

The message "Success. Netconf exported successfully" appears.



CHAPTER 4

Modify Network Properties

Modify network properties

Table 20: Feature History

Follow these steps to modify the properties of the network.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the network properties.

Step 2 Choose **Network** > **Entity Editor**.

Alternatively, click the network name in the network tree, and click **Show Advanced Properties** displayed under the network tree.

Step 3 In the **Entity Editor** window, click the **Site** tab.

Step 4 Click the network name, and modify the properties in the right pane. For the property descriptions, refer to:

- General properties of a network, on page 70
- System release properties, on page 72

Step 5 Click **Update**.

General properties of a network

This table describes various general properties of a network.

Table 21: General properties of a network

Property	Description	Available Options	Default option
Name	Displays the network name. You can modify the name.	—	—
Quick Analysis	This check box allows you to quickly analyze the network by using a less accurate algorithm. The quick analysis option does not optimize the DCU and amplifier placement algorithm, resulting in an approximate BoM. For an accurate BoM, uncheck the **Quick Analysis** check box.	—	—

Property	Description	Available Options	Default option
DWDM Interfaces	Cisco ONP supports 100G and 200G transceivers as DWDM interfaces. This option is applicable only for automatically created waves, when OTN services are present.	• 100G: The entire network chooses the 100G wavelength for transmission. • 200G: The entire network chooses the 200G wavelength for transmission. If you enable both 100G and 200G options, by default, the entire network chooses the 200G wavelength for transmission. If the 200G wavelength is not optically feasible, then it selects 100G automatically for transmission.	—
Customer Name	Enter the customer name.	—	—
Platform	Allows you to choose the platform type.	• ANSI • ETSI ANSI networks do not allow you to define SDH (ETSI) service demands. ETSI networks do not allow you to define SONET (ANSI) service demands.	ANSI
Measurement Unit	Displays the unit of measurement of span length. You cannot edit it.	km	km
A2A Mode	Any to Any (A2A) mode.	• A2A_None • A2A_FAST	A2A_None
A2A Power Output	The power output value is based on the chosen A2A mode.	—	—
A2A Demand Type	The demand type is based on the chosen A2A mode.	—	—

Property	Description	Available Options	Default option
A2A Channel TypeContentionless	Type of channel. You can choose multiple types.	• Contentionless: This property enables an N-degree ROADM node to accommodate N wavelengths of the same frequency from a single add or drop device. • Colorless: The colorless property enables tuning of channel wavelengths without changing the optical interface of the port. • Colored: The Colored property dedicates a separate port for each wavelength.	Contentionless
SSON	Indicates whether the network is an SSON network.	—	—
Use client Payg	This check box enables the Pay As You Grow feature on the client cards. The PAYG feature provides a cost-effective solution for fewer wavelength requirements. A standard card is configured to work on maximum supported wavelengths, whereas a PAYG license comprises license restricted cards and a base license. So, instead of purchasing a standard card, you can purchase a PAYG license.	—	—

System release properties

The table provides details about different system release properties of a network.

Table 22: System release properties

Property	Description	Options available	Default
NCS 4K	Displays the system release of the NCS 4000 node in the network.	—	—
NCS 2K	Displays the system release of the NCS 2000 node in the network.	—	—
NCS 1K (Available only on the SSON network)	Displays the system release of the NCS 1004 node in the network.	—	—
Previous NCS 2K (Available only on the Release upgraded network)	Displays the system release of the NCS 2000 node in the network, before the Release upgrade.	—	—
Naming Convention Enabled	Naming Convention Enabled is automatically turned on when networks are created in Cisco ONP, and cannot be edited. By default, the sides are named from T, S, R, Q, P, O, N, M, L, K, J, I, H, G, F, E, and index, depending on the used Scalable Upto parameter. • You can import a mpz network without naming convention enabled, but the Cascaded SMR option remains disabled. • You cannot edit the label name of the side.	—	—
SVO	Type of network management solution.	• SVO: Chooses SVO card. • UCS: Chooses SVO application that is hosted on a server. • Auto: Chooses SVO card as default, for SVO solution.	Auto

Modify site properties

Table 23: Feature History

Feature Name	Release Information	Feature Description
Shared SMR Port	Cisco ONP Release 4.2	You can enable the **Colored Add/Drop** property. This feature supports the use of contentionless and colored demands that are connected to the same port of an SMR card. With the **Shared SMR Port** enabled, you can create and validate the contentionless and colored configuration on a 16-degree SMR-20 node.

Use this procedure to modify the properties of the site.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the site properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, navigate to **Sites** > **Site**

Step 4 Choose the site and modify the properties in the next pane. For the property descriptions, refer to:

- General site properties, on page 75
- C-Band properties, on page 78
- Layout properties, on page 79
- Cisco NMS properties, on page 83
- Third party NMS properties, on page 83
- Map properties, on page 84
- Bill of materials properties, on page 85
- SVO properties, on page 88

Step 5 Click **Update**.

General site properties

This table describes the descriptions of various general properties for sites.

Table 24: General site properties

Property	Description	Available options	Default
Name	Enter the site name, either alphanumeric or numeric.	—	—
Type	Choose the type of site.	• ROADM • OLA • Traffic • Passthrough **Note** • You can add a passthrough site as a place holder. You cannot add services or waves to this site and therefore cannot generate the report. Later, you can convert the passthrough site to a ROADM, OLA, or the Traffic site in the design mode. • OLA is an optical line amplifier site that is used only for amplification. You cannot add service or waves on this site. • You cannot add a Traffic site of the type 4K-2K into an SSON network.	The site type that you chose while designing.
Node Type	This field is noneditable.	FLEX NG-DWDM	FLEX NG-DWDM

Property	Description	Available options	Default
Equipment Configuration	Choose the configuration from the drop-down list. This option is available only for the Traffic site.	• Large CO - NCS 4016 • Small Site - NCS 4016 • Small Site - NCS 4009	Large CO - NCS 4016
Traffic Type	Choose the traffic type. This option is available only for the Traffic site.	• 4K_1K_2K (for SSON) • 1K_2K (for SSON) • 4K_2K (non- SSON)	• 4K_1K_2K (for SSON) • 4K_2K (non- SSON)
SSON	Indicates whether the network is an SSON network.	—	—
CLLI Code	Enter a string holding the CLLI code.	—	—
Site Address	Enter the site address.	—	—
Evolved Mesh	By default, this option is unchecked. When you enable this feature on the network, it is automatically enabled on the associated sites of the network.	—	This option remains enabled.
Status	Displays the status of the network. It shows whether the network is **Up** or **Down**.	—	—
Weight Lbs	Displays the weight of all the units of the site, in pounds.	—	—
Node Protection	Choose the Node Protection.	• Same shelf • Separated shelves	Same shelf

Property	Description	Available options	Default
Mpo16Lc	Displays the fan-out module.	MF-MPO-16LC The MPO-16 to 16-LC fan-out module is a double slot module with one MPO-16 connector (COM) and eight LC duplex connectors. The MPO-16 connector is compatible with the SMR20 FS EXP and 16-AD-CCO FS units.	MF-MPO-16LC
Mpo16ToMpo8	Choose the required Mpo16 to Mpo8 converter.	• MPO16ToMPO8Cable • MF-2MPO_ADP	MPO16ToMPO8Cable
Cascaded SMR	Enable this option to add Layer-2 contentionless sides.	—	—
Flex Spectrum	By default, this check-box remains checked for a newly created network. You cannot edit it.	—	This check-box remains checked for a newly created network.
Grooming Site	When you enable this option, it indicates that OTN traffic can be groomed at this site.	—	—
MR-MXP BreakOut Cable	Check this check box to use the ONS-MPO-MPOLC-10 breakout cable to interconnect the client ports of the MR-MXP card with the NCS2K-MF-MPO-20LC passive module.	—	—
8X10G-FO	Check this check box to use the NCS2K-MF-8X10G-FO passive module only for 10G on the client-side of the NCS2K-400G-XP card. By default, this passive module is enabled.	—	—

C-Band properties

This table describes the descriptions of various C-Band properties under sites.

Table 25: C-band properties

Property	Description	Available options	Default
Structure	Displays the structure of the site: Multi degree and Terminal for ROADM and Traffic sites, and Line for OLA and Passthrough sites. This field is noneditable.		
Functionality	Displays the site functionality. This field is noneditable. Thee functionalities available for each type of site are: • Optical Cross Connect (OXC) for ROADM and traffic site • Auto for OLA site, Cisco ONP downgrades OLA site to passthrough if OLA is not required. • Passthrough for passthrough site	—	—
Scalable up to Degree	This parameter determines the maximum number of degrees, ducts, or line sides that can be supported by the site. The available options are 2, 4, 8, 12, and 16. The default option is 4. The network is scalable up to 16 degrees for ROADM and Traffic sites. Choose 2 to have a LINE ROADM site. For OLA and passthrough, the value is 2 and is noneditable.		
Site Type	Choose the type of site.	• Auto **Note** When you choose Auto, the default option is SMR-20. • SMR-20 • SMR-9 The Site type is Line for the OLA site.	Auto

Property	Description	Available options	Default
Shared SMR Port	Check this check box to connect Contentionless unit 16-AD-CCOFS and Colored unit MD-48-ODD/Even to the same MPO port of SMR-20. When Shared SMR port is enabled, MD-48-ODD/EVEN unit connects to the specific side of SMR-20 through MPO-8LC and UPG-4 instead of directly connecting to SMR-20 through MPO-16LC. **Note** Shared SMR port becomes disabled, if • **Degree Mesh Type** property is *PPMESH8-5AD* • Or, **Site Type** property is *SMR-9* and **Scalable Upto Degree** property is *8*	—	—
Degree Mesh Type	Choose the mesh type for the Flex NG-DWDM site.	• DEG-5/UPG-4 • PPMESH8-5AD	DEG-5/UPG-4
Site Type	Displays the type of the site. For example, OLT.	—	—
L0 Platform	Displays the platform.	—	—
Degree Type	Displays the type of degree. For example, BRK-8.	—	—
Pre Equip Degree	This parameter determines the number of degrees to be considered for the site hardware placement on day 0.	• None • Auto • 4 • 8 • 12 • 16	None If you choose None, only the sides that are present in the Cisco ONP GUI are shown. The values in the drop-down list are populated based on the value of scalable up to degree parameter.

Layout properties

This table describes the descriptions of various layout properties under sites.

Table 26: Layout properties

Property	Description	Available options	Default
Chassis Type	Choose the type of chassis. Chassis type is supported for all the sites except the passthrough.	• M6 Chassis • M15 Chassis • Auto M15 is the default option when you choose Auto.	Auto
Power Supply	Choose the type of Power Supply	• Auto • AC Power • DC Power	DC Power
Chassis Type	Choose the type of chassis. The available options are: **Note** Chassis type is not supported for the passthrough site.	• M6, and M15 Chassis for OLA • M6 Chassis for ROADM and Traffic • M15 Chassis for ROADM and Traffic • Auto for all nodes	Auto
Power Supply	Choose the type of Power Supply.	• Auto for all types of chassis • AC Power, DC power for M15 and M2 chassis • AC Power, DC Power, AC2 Power, DC40 Power, and DC20 Power for M6 chassis	Auto
Controller Card	Choose the type of the controller card.	• Auto • TNC/TSC, TNC-E/TSC-E, TNCS, TNCS-0, TNCS-2, and TNCS-20 for M2 chassis • TNC/TSC, TNC-E/TSC-E, TNCS, TNCS-0, TNCS-2, and TNCS-20 for M6 chassis • TNCS, TNCS-0 TNCS-2, TNCS-20 for M15 chassis	For an NCS 2000 site controller card is TNC available options are b chassis type chosen. E controller cards that a M15 chassis are listed
Redundant Controller Card	Choose whether to use a redundant controller card. This property is editable in NCS 1010 only when the chassis type is 1020.	—	—

Property	Description	Available options	Default
Layout Template	Choose the required layout template. **Note** After the chosen layout template is applied, all layout properties will be reset and disabled. **Note** After design analysis, if the applied layout template is not considered for card placement in the layout, check for the error message (noncritical) under the **Elements > Messages** tab. If you see a template-related error which indicates that there is a mismatch between the cards that are defined in the template and the cards that are created on the site, perform these steps: • Export the template from the **Layout** page, and modify it as required. • Import the modified template using the **Manage > Layout Template** option. • Switch to Design mode and apply the template to the site using the **Entity Editor**. • Reanalyze the network to get the correct layout populated.	List of available layout templates	—
UTS AC Power Cables	Choose the type of cables to be used for the AC power supply.	Cables are listed based on the country type and the Chassis type selected.	—
Redundant Power Scheme	Choose the redundant power scheme from the drop-down list to configure the number of working and protected power units for the chassis.	For an NCS 2000 site, the options available are based on the chassis type. For M15 chassis, the options available are 1+0, 1+1, 2+0, 2+1, 3+0, 3+1, 2+2. For example, if you choose 3+1 redundant power scheme, there are 3 working power units and 1 protected power unit. For M6 chassis, the options available are Auto, Yes, and No.	3+1 is the default scheme for M15 D the default redund for M15 AC chass

Property	Description	Available options	Default
Raman Adapter Share	This option is available only for the OLA site. This option indicates that MF-2LC-ADP can be shared with EDRA amplifiers and not with RAMAN amplifiers irrespective of the default selection.	—	By default, this check checked.
ECU Type	Choose the External Connection Unit (ECU) type.	The options available are based on the chassis type. • ECU—Has 12 USB 2.0 ports and supports IEEE1588v2 PTP, time-of-day (ToD), and pulse-per-second (PPS) inputs. • ECU-S—Similar to ECU except that it has eight USB 2.0 ports and two USB 3.0 ports. • ECU60-S—Variant of ECU-S introduced for the NCS 2006 when the shelf is powered at –60VDC nominal input voltage. ECU-S and ECU60-S are supported only for M6 chassis.	By default, the ECU ap is listed.
MF Unit	Choose the mechanical frame for the passive optical modules from the drop-down list.	• Auto • MF-6RU/MF-10RU • MF-1RU • The NCS2K-MF-1RU has four slots for the passive optical modules. • The NCS2K-MF-6RU supports up to 14 single-slot passive optical modules such as any combination of NCS2K-MF-DEG-5, CS2K-MF-UPG-4, or Connection Verification (CV) units. • The NCS2K-MF10-6RU supports up to 10 double-slot passive optical modules such as NCS2K-MF-MPO-16LC=.	Auto
Chassis Disaggregation	If you check this check-box, ROADM and transponder cards are placed in different chassis.	—	—

Cisco NMS properties

This table describes the descriptions of various Cisco NMS properties under sites.

Table 27: Cisco NMS properties

Property		Available options	Default
SVO Full License	Enable this check box to add High Availability (Feature and License), Connection Verification license, Flex Spectrum license, and OTDR license packaged in it.	—	—
High Availability	Enable this check box to add the High Availability feature to the license package.	—	—
Connection Verification License	Enable this check box to add the Connection Verification feature to the license package.	—	—
Flex Spectrum License	Enable this check box to add the Flex Spectrum feature to the license package. For SSON networks, the Flex Spectrum license is enabled by default.	—	—
OTDR License	Enable this check box to add the OTDR feature to the license package.	—	—

Third party NMS properties

This table describes the descriptions of various Third party NMS properties under sites.

Table 28: Third party NMS properties

Property		Available options	Default
3rd party Full License	Enable this check box to add NBI (North Bound Interface), Alarm Correlation, Performance Monitoring, and Circuit Provisioning features to the license package.	—	—
NBI	Enable this check box to add the NBI feature to the license package.	—	—
Alarm Correlation	Enable this check box to add the Alarm Correlation feature to the license package.	—	—
Performance Monitoring	Enable this check box to add the Performance Monitoring feature to the license package.	—	—
Circuit Provisioning	Enable this check box to add the Circuit Provisioning feature to the license package.	—	—

Map properties

This table describes the descriptions of various map properties under sites.

Table 29: Map properties

Properties	Description	Available options	Default
X Coordinate	It represents the longitudinal location of the site. Longitude can be positive or negative (-180 to 180). Negative is west of Greenwich, and positive is eastward.	—	—

Properties	Description	Available options	Default
Y Coordinate	It represents the latitudinal location of the site. Latitude can be positive or negative (- 90–90), north and south of the Equator.	—	—
Position Lock	Check this check box to lock the site position on the map.	—	—

Bill of materials properties

This table describes the descriptions of various layout properties under sites.

Table 30: Bill of materials properties

Properties	Description	Available options	Default
Bill of Material			
Enable NCS	This feature enables NCS features on all sites in the network.	—	—
Use PAYG	The Pay As You Grow (PAYG) functionality significantly reduces the initial setup cost and enables the purchase of another wavelength capacity on a need basis. PAYG enables port-based cost or licensing for SMR-9 and SMR-20 cards.	—	—

Properties	Description	Available options	Default
Connection Verification	Enable this check box to: • Validate the correct optical interconnection between the optical cards inside a Flex ROADM. • Measure the insertion loss of the external passive path. • Validate the quality of the connections to the patch panel. • Check if the insertion loss is within the expected value. These cards support connection verification: • SMR20 FS CV • MF-DEG-5-CV • MF-MPO-16LC-CV • MF-UPG-4-CV	—	—
New FS-SMR PID	By default, this check-box remains checked for a newly created network. You cannot edit it. This option enables displaying of the new SMR-20 PID in the BOM page. You can enable this option when you unlock an mpz network where SMR-20 is selected, during an upgrade or release upgrade.	—	—

Table 31: Bill of materials properties

Property	Platform	Description	Available options	Default
Enable NCS	NCS 2000	This feature enables NCS features on all sites in the network.	—	—

Property	Platform	Description	Available options	Default
Use PAYG	NCS 2000	The Pay As You Grow (PAYG) functionality significantly reduces the initial setup cost and enables the purchase of another wavelength capacity on a need basis. PAYG enables port-based cost or licensing for SMR-9 and SMR-20 cards.	—	—
Connection Verification	NCS 2000	Enable this check box to: • Validate the correct optical interconnection between the optical cards inside a Flex ROADM. • Measure the insertion loss of the external passive path. • Validate the quality of the connections to the patch panel. • Check if the insertion loss is within the expected value. The following cards support connection verification: • SMR20 FS CV • MF-DEG-5-CV • MF-MPO-16LC-CV • MF-UPG-4-CV	—	—

Property	Platform	Description	Available options	Default
New FS-SMR PID	NCS 2000	You cannot edit this option. This option enables displaying of the new SMR-20 PID in the BOM page. You can enable this option when you unlock an mpz network where SMR-20 is selected, during an upgrade or release upgrade.	—	This check-box remains checked for newly created network.

Enhanced face plate properties

This table describes the descriptions of various Enhanced face plate properties under sites.

Table 32: Enhanced face plate properties

SVO properties

This table describes the descriptions of various **SVO** properties of a site.

Table 33: SVO properties

Properties	Description	Available options	Default
Chassis License Flush Out	Allows you to flush out the existing chassis license and purchase new chassis license.	—	—
SVO Pluggables	Choose the pluggable. **Note** The SVO pluggables are not applicable for UCS-based SVO network design.	• Auto • ONS-SC +- 10G-SR • ONS-SC +-10G-LR	Auto When you choose Auto, ONS_SC+-10G_SR is the default option.

Add contentionless side to a site

Contentionless functionality on a site refers to the contentionless add or drop ability of an N-degree ROADM node to accommodate N wavelengths of the same frequency from a single add or drop device. A ROADM is contentionless when the number of drop units equals the number of ROADM degrees.

Use the following procedure to add contentionless sides to a ROADM or traffic site.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network in which you want to add contentionless sides to a site.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 Click the site to which you want to add contentionless sides.

Step 4 Click the **Add Contentionless Side** icon.

Step 5 Enter the appropriate value in the **Enter number of contentionless sides** field.

The number of contentionless sides you can add to a site depends on the site type and the **Scalable Upto Degree** property.

If you want to add contentionless sides to	Then..
Layer-1 SMR site	Enter the appropriate value in the **Enter number of contentionless sides** field.
Layer-2 SMR-20 site	• Check the **Evolved Mesh** check box. • Select **Site Type** as *SMR-20* or *Auto*. • Check the **Cascaded SMR** check box. • Select **Degree Mesh Type** as *DEG-5/UPG-4*. • Click **Update**. • Enter the appropriate value in the **Enter number of contentionless sides** field. See Contentionless sides for Layer-1 SMR, on page 90.

If you want to add contentionless sides to	Then..
Extended Layer-2 SMR-20 site	• Choose the **Reserve Cascaded SMR Port** value. **Note** The **Reserve Cascaded SMR Port** drop-down property is available for NCS 2000 networks from R11.1.x. Based on the N-degree and Layer-2 SMR, you can add more contentionless sides on each site for the extended layer-2 SMR, but this will reduce the number of Layer-1 contentionless sides. • Click **Update**. • Enter the appropriate value in the **Enter number of contentionless sides** field. See Contentionless sides for extended Layer-2 SMR, on page 91.

Step 6 Click **OK**.

Contentionless sides for Layer-1 SMR

This table explains how many contentionless sides you can add to a site based on the site type, and the **Scalable Upto Degree** property.

Table 34: Contentionless sides for Layer-1 SMR

Site type	Scalable upto degree	Number of contentionless sides
SMR-20	4	16
SMR-20	8	12
SMR-20	12	8
SMR-20	16	4
SMR-20	Line	8
SMR-20	Terminal	8
SMR-9	4	5
SMR-9	8	1

Contentionless sides for extended Layer-2 SMR

This table shows how many contentionless sides you can add to each site for the extended layer-2 SMR site. The number depends on the N-degree and Layer-2 SMR configuration

Table 35: Contentionless Sides for extended Layer-2 SMR

Reserve cascaded SMR port	Site type	Scalable upto degree	No. of contentionless sides for Layer-1 side	No. of contentionless sides with 1st Port Layer-2	No. of contentionless sides with 2nd Port Layer-2	No. of contentionless sides with 3rd Port Layer-2
1	SMR-20	4	16	20	Not supported	Not supported
	SMR-20	8	12	20	Not supported	Not supported
	SMR-20	12	8	20	Not supported	Not supported
	SMR-20	16	4	20	Not supported	Not supported
2	SMR-20	4	Not supported	Not supported	Not supported	Not supported
	SMR-20	8	11	20	20	Not supported
	SMR-20	12	7	20	20	Not supported
	SMR-20	16	3	20	20	Not supported
3	SMR-20	4	Not supported	Not supported	Not supported	Not supported
	SMR-20	8	Not supported	Not supported	Not supported	Not supported
	SMR-20	12	6	20	20	20
	SMR-20	16	2	20	20	20

Modify the number of contentionless side ports at a site

Follow these steps to modify the number of contentionless ports for a side in a ROADM site.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network in which you want to modify the number of contentionless ports for a side in a site.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 Expand a ROADM site, and select a contentionless side.

The properties of the side are displayed in the right panel.

Step 4 From the **Contentionless Ports** drop-down list, select the required number of ports.

Click **Update**.

Modify fiber properties

Use this procedure to modify the properties of a fiber.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network where you want to modify the fiber properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 Click the **Fiber** tab in the **Entity Editor** window.

Step 4 Choose the fiber and modify the required properties. For the property descriptions, refer to:

- General fiber properties, on page 92
- Physical and Raman amplification properties of fiber, on page 97
- Factors properties of fiber, on page 95
- Extended and totals properties of a fiber, on page 96

Step 5 Click **Update**.

General fiber properties

This table describes various general properties of the optical fiber connected between the sites.

Table 36: General fiber properties

Property	Description	Available options	Default
Name	By default, the name of the fiber is based on the number of fibers between the source and destination sites. You can edit the name.	—	—
Source	Displays the source site name. This field is noneditable.	—	—

Property	Description	Available options	Default
Destination	Displays the destination site name. This field is noneditable.	—	—
Bidirectional	Indicates whether a standard single fiber is used to transmit the data in both directions.	—	—
Fiber Type	Select the fiber type.	• G652-SMF-28E • TWR • MC • TWPlus • TWMinus • TWClassic • FL • TL • G652-SMF • ELEAF • True wave	G652-SMF

Property	Description	Available options	Default
Length	Displays the span length of the fiber connecting a source and destination site. If necessary, change the span length manually. • The Cisco ONP tool automatically updates the fiber length based on the actual geographical map. If you change the fiber length, then the Cisco ONP tool updates the same in the network tree and the map accordingly for the first time. Later, the fiber length does not change, when you drag and drop the sites in the map. • In the network tree pane, expand **Fiber** and select the fiber couple, A-Z and Z-A. The properties pane displays the fiber couple name, source side, destination side, its span length, loss, and, Polarization Mode Dispersion (PMD) value. • You can enter the different span length and loss values for the individual fibers in a fiber couple.	—	—
Network status	Displays the status of the network, whether the network is being deployed or not. If the network is not deployed, it shows the status as UNDISCOVERED.	—	—

Property	Description	Available options	Default
Business status	Displays the status of the fiber in a business perspective view. If fiber is not deployed, it shows the status as FUTURE. This field is noneditable.	—	—
Measurement Units	Choose the measurement unit .You can set the measurement unit only for the duct, but not for the fiber pair (couple) or fiber.	• Km • Miles	Km
Aging Loss [dB]	Enter the aging loss value for the fiber.	—	—
DCN Extension	Check this check box to enable the default use of a data connection network (DCN) extension on each span in the project. This setting implies that the optical service channel (OSC) channel is not used to connect the two nodes.	—	—
OSC FrameType	Choose the OSC frame type. Cisco ONP uses FE Frame as the preferred frame type.	• Auto • OC3 Frame • GE Frame • FE Frame	Auto
Aging Factor	Enter the number to factor fiber aging. This factor is multiplied by the SOL total span loss without connectors.	—	—

Factors properties of fiber

This table describes various factors properties of the optical fiber.

Table 37: Factors properties of fiber

Property	Description	Available options	Default
Loss Coefficient [dB/km]	Loss is calculated based on the loss coefficient.	—	—

Property	Description	Available options	Default
QD C-Band	Displays the secondary order dispersion for C-band.	—	—
CD C-Band	Displays the secondary order dispersion for L-band.	—	—
RD Factor	Displays the random dispersion value.	—	—

Extended and totals properties of a fiber

This table describes various extended and totals properties of the optical fiber.

Table 38: Extended and totals properties

Property	Description	Available options	Default
Extended			
Effective Mode Area	Displays the effective mode area [µm^2]	—	—
SRS tilt coefficient	Displays the Stimulated Raman Scattering tilt coefficient on the band.	—	—
DRBS coefficient	Displays the Rayleigh Scattering capture coefficient.	—	—
N2	Nonlinear index of refraction [1e-16 cm^2/W]	—	—
LFBR	Length of individual fibers for sigmaDSP [Km]	—	—
Totals **(The properties under Totals are noneditable)**			
PMD	Displays the Polarization Mode Dispersion (PMD) value.	—	—
Loss EOL	Displays the total loss EOL calculation.	—	—
Loss SOL	Displays the total loss SOL calculation.	—	—
CD C-Band	Displays the total chromatic dispersion for the C-band.	—	—
QD C-Band	Displays the secondary order dispersion for C-band.	—	—
RD	Displays the random dispersion value.	—	—

Physical and Raman amplification properties of fiber

This table describes various physical and Raman amplification properties of the optical fiber.

Table 39: Physical and Raman amplification properties of fiber

Property	Description	Available options	Default
Physical			
Length-Based Loss	The fiber loss value is automatically calculated based on length and loss coefficient, when you check this option.	—	—
Tot SOL Loss w/o connectors	Enter the start of life fiber loss value for each span, excluding the connector concentrated loss.	—	—
Connector Loss A	Connector Loss at Source Site [dB]	—	—
Connector Loss B	Connector Loss at Destination Site [dB]	—	—
Raman Amplification			
Raman Amplified	Enable Raman Amplification on the ducts. **Note** When you enable Raman amplification, the side property *Enable C+L Band S/C* is automatically disabled.	—	—

Modify fiber couple properties

Use this procedure to modify the properties of a fiber couple.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network where you want to modify the fiber couple properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 Click the **Fiber** tab in the **Entity Editor** window.

Step 4 Choose the fiber and drill down to the fiber couple, and modify the required properties. For the property descriptions, refer to:

- General properties of a fiber couple, on page 98
- Physical and factors properties of a fiber couple, on page 99
- Totals properties of a fiber couple, on page 99

Step 5 Click **Update**.

General properties of a fiber couple

This table describes various general properties of an optical fiber couple.

Table 40: General fiber couple properties

Property	Description	Available options	Default
Name	By default, fiber couple is named based on the fiber name followed by COUPLE-AZ or COUPLE-ZA. The sides that are connected by the fiber couple are indicated inside brackets. The name is noneditable.	—	—
Source Side	Displays the source side name. This field is noneditable.	—	—
Destination Side	Displays the destination side name. This field is noneditable.	—	—
Length	Automatically displays the span length of the fiber connecting a source and destination side. Change the span length manually, if necessary. You can enter the different span length and loss values for the individual fibers in a fiber couple.	—	—

Physical and factors properties of a fiber couple

This table describes various physical and factors properties of an optical fiber couple.

Table 41: Physical and factors properties of a fiber couple

Property	Description
Physical	
Tot SOL Loss w/o connectors	Enter the start of life fiber loss value for each span, excluding the connector concentrated loss.
Connector Loss A	Connector Loss at Source Site [dB]
Connector Loss B	Connector Loss at Destination Site [dB]
Factors	
Loss coefficient [dB]	Enter the value of the SOL fiber loss per kilometer used to calculate the loss of each span in the network.
PMD coefficient	Displays the PMD coefficient.

Totals properties of a fiber couple

This table describes various Totals properties of an optical fiber couple. The properties under Totals are noneditable

Table 42: Totals properties

Property	Description	Available options	Default
PMD	Displays the Polarization Mode Dispersion (PMD) value.	—	—
Loss EOL	Displays the total loss EOL calculation.	—	—
Loss SOL	Displays the total loss SOL calculation.	—	—
CD C-Band	Displays the total chromatic dispersion for the C-band.	—	—
QD C-Band	Displays the secondary order dispersion for C-band.	—	—
RD	Displays the random dispersion value.	—	—

Modify service properties

Use this procedure to modify the properties of the service.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the service properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, click the **Service** tab.

Step 4 Choose the service under the **Serives** tab, and modify the properties in the right pane. For the property descriptions, refer to:

- General service properties, on page 100
- Primary and secondary paths forcing properties, on page 101

Note

- Force both primary and secondary path fiber or channel to enable protected service. Ensure the wave type matches for both paths.
- Apply path forcing end-to-end, from the source to the destination. If you force only a partial path, the analysis fails.
- Force the wave path tagged to the service.
- For protection types 1+1+R+R, 1+1+R, and 1+R, you can force a path in restoration path1 or restoration path2. Fiber can also be forced in the primary or secondary path.

Step 5 Click **Update.**

General service properties

Table 43: General service properties

Property	Description		
Name	The service name is based on the source and destination sites and the number of services between them. You can edit the name. For example, if there are two services between site 1 and site 2, the names of the services are Site-1-Site-2-1 and Site-1-Site-2-2, respectively.	—	—
Client Type	Choose the type of service.	• 10GE • 100GE • STM-64	100GE

Property	Description		
Protection	Choose the protection type from the drop-down list. For more information on protection types, see #unique_135.	• Unprotected • 1+1 • Disjoint • S+NS • 1+R • 1+1+R • 1+1+R+R	1+1
Source	Displays the source site name.	—	—
Destination	Displays the destination site name.	—	—
Tertiary Source	From the drop-down list, select the possible site as a tertiary source.	Lists the available sites	—
Tertiary Destination	From the drop-down list, select the possible site as a tertiary destination. Tertiary source and tertiary destination are enabled only when you select the protection scheme as Unprotected Disjoint. You can select either tertiary destination or both tertiary source and tertiary destination. • If you select only the tertiary destination, the demand is created between the source and destination and between the source and tertiary destination. These do not have common fibers in the path, which are disjoint. • If you select both tertiary source and tertiary destination, two unprotected demands are created between the source to destination, and tertiary source to tertiary destination. The demands are disjoint to each other.	Lists the available sites	—

Primary and secondary paths forcing properties

These tables describe the primary and secondary paths forcing properties for services. Secondary path is available only for (1+1) .

Table 44: Primary path forcing properties

Property	Description	Available options	Default
Path	Cisco ONP automatically selects the shortest path as working path and also allows you to force the path manually.	—	—

Property	Description	Available options	Default
Fiber	Primary path fiber is forcing path for working trail.	—	—
Regeneration Platform	Displays the platform of the regeneration site	—	—
Regen Sites	Choose the regeneration site.	Lists the available regeration sites	—
Wavelength	Click **Edit** to choose the wavelength.	Displays multiple wavelength options.	Auto
ODU Timeslot	Enter the ODU timeslot value.	—	—
Section Wavelength(s)	Displays the selected **Wavelength**.	—	—
Src Channel Type	Choose the type of source channel.	• Auto: Auto option is the contentionless demand. • Contentionless • Colorless • Colored	Auto
Dst Channel Type	Choose the type of destination channel.	Auto-populated based on the Src channel type.	—

Table 45: Secondary path forcing properties

Property	Description	Available options	Default
Path	Secondary path is the protected path when the primary path fails. This path is the second best path after the primary path.	—	—
Fiber	Secondary path fiber is for protected service, forcing path for the protected trail.	—	—
Regeneration Platform	Displays the platform of the regeneration site	—	—
Regen Sites	Choose the regeneration site.	Lists the available regeneration sites.	—
Wavelength	Click **Edit** to choose the wavelength.	Displays multiple wavelength options.	—

Property	Description	Available options	Default
ODU Timeslot	Enter the ODU timeslot value.	—	—
Section Wavelength(s)	Displays the selected **Wavelength**.	—	—
Src Channel Type	Choose the type of source channel.	• Auto: Auto option is the contentionless demand. • Contentionless • Colorless • Colored	Auto
Dst Channel Type	Auto-populated based on the Src channel type. You can still change the type. When you change the Dst channel type, Src channel type also changes to the same.	• Auto: Auto option is the contentionless demand. • Contentionless • Colorless • Colored	Same as the Src channel type.

NCS1K domain properties

This table describes the various NCS1K domain properties for services.

Table 46: NCS1K domain properties

Property	Platform	Description	Available options	Default
Client Type	NCS 2000	Displays the client type. By default, client type is OTU4.	—	—
Interface Type	NCS 2000	Displays the interface type. By default, interface type is BH.	—	—
Trunk Mode	NCS 2000	Choose the trunk mode. **Note** Based on the selected trunk mode, Baud rates are filtered.	• 200G • 300G	200G

Property	Platform	Description	Available options	Default
Baud Rate	NCS 2000	Choose whether the Baud rates mode as 60 or 69GBd.	• 60GBd • 69GBd	60GBd

Services aggregation

Table 47: Feature History

Feature Name	Release Information	Feature Description
Services Aggregation	Cisco ONP Release 4.1	The services aggregation feature allows two or more services to share the same trunk port or channel. By default, the services are added to the DefaultGroup. You can export aggregation reports.

You can use services aggregation to allow multiple services to share the same connection point, such as a trunk port or channel. This ability to share is determined by the characteristics defined in their **Service Group**.

Specifically, when you add services to a 1K-2K-4K Traffic site within an **SSON network**, the system automatically creates a **DefaultGroup** under **Services** in the network tree. All the services you add are then automatically associated with **DefaultGroup**.

Create a new service group

Follow these steps to create a new service group.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network where you want to create a new service group.

Step 2 Right-click **Services** under the network tree and choose **Create Service Group**.

A new service group appears under Services.

Modify service group properties

Follow these steps to modify the properties of a service group.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the service group properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, click the **Services** tab, and click a service group.

Step 4 Modify the service group properties as required.

See Service group properties, on page 105.

Step 5 Click **Update**.

Service group properties

This table describes various service group properties.

Table 48: Service group properties

Property	Description	Available options	Default option
General			
Name	By default, Cisco ONP provides a servive group name. For example, Group-1. Edit the name if needed. For example, if there are two services between site 1 and site 2, the name of the services are Site-1-Site-2-1 and Site-1-Site-2-2, respectively.	—	Group-1
Demand Types	Select the demand type. For default group all demand types are available, and you cannot edit them.	—	—
Default Group	Indicates whether the service group is a default group or a user created group.	—	—
NCS 4 K			
Exclusive LC Usage	Indicates whether the services belonging to this group must have an exclusive Line Card (LC). For example, when you check this check box, neither the Client LC nor the Trunk LC of the services belonging to this group can be shared by services belonging to any other groups.	—	—

Property	Description	Available options	Default option
Symmetric Aggregation	Indicates whether this group allows aggregation of only symmetric services. Services are symmetric if they have same protection scheme. • Unprotected • 1+R • 1+1 • 1+1+R • 1+1+R+R For Example, all "1+1" services are symmetrical. If you check this check box, this service group allows aggregation of only symmetrical services. For example, "Unprotected" can be aggregated only with "Unprotected", "1+R" only with "1+R", "1+1" only with "1+1", and so on. If this check box is unchecked, this service group allows aggregation of symmetrical and unsymmetrical services together. For example, "Unprotected" can be aggregated with either "Unprotected", "1+R", "1+1" "1+1+R" or "1+1+R+R". See Rules for aggregating services, on page 106	—	—
NCS 1 K			
Exclusive LC Usage	Same as NCS 4 K.	—	—
Symmetric Aggregation	Same as NCS 4 K.	—	—

Rules for aggregating services

These rules must be satisfied for any two services, whether symmetrical or non-symmetrical, to be aggregated:

1. Both services must have identical source and destination points.
2. The paths of the two services must align for the same path types.

- Example for symmetric aggregation:

  When aggregating two "1+1" services, the working path of the first service must match the working path of the second service, and similarly, the protection paths of both services must also match.

- Example for non-symmetric aggregation:

  When aggregating a "1+1" service with a "1+1+R" service, the working path and protection path of the first service must match the corresponding paths of the second service. However, the restoration path of the second service can differ.

3. Both services must use the same wavelength for the same path types.
   - If the wavelength is set to "auto," it can be aggregated with either another "auto" wavelength or a fixed wavelength.
4. Both services must have the same trunk mode configuration for the same path types.
5. The regeneration sites for both services must align for the same path types.
6. The demand type is not a constraint for aggregation, except when considering trunk capacity availability.

Associate a service with the newly created group

By default, the services are associated with the **DefaultGroup**. However, you can change the group.

Follow these steps to associate a service to the newly created group.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 In the network tree, click the service that you want to associate to a group.

You can view the properties of the network at the bottom of the network tree.

Step 2 Selct the group from the **Service Group** drop-down list.

Step 3 Click **Update**.

Note
For an LNI-imported network, all services are in the Default group by default. When you upgrade the LNI-imported network for the first time, you can move the services to other newly created Service Groups without unlocking them. For later upgrades, unlock the services before moving them between Service Groups. The Service Groups stay locked during upgrade mode unless you perform a complete network-level unlock.

Export aggregation reports

Follow these steps to export the service aggregation reports.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open an analyzed network to export the aggregation reports.
Step 2 Choose **Export** > **Service Aggregation**.
Step 3 Save the aggregation report as an Excel file to your local system.

Modify wave properties

Follow these steps to modify the properties of the wave.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the wave properties.
Step 2 Choose **Network** > **Entity Editor**.
Step 3 In the **Entity Editor** window, click the **Services** tab, and click a wave.
Step 4 Modify the wave properties as required.

See Wave properties, on page 108.

Step 5 Click **Update**.

Wave properties

This table describes various wave properties.

Table 49: Wave properties

Property	Description	Available options	Default option
General			

Property	Description	Available options	Default option
Label	Displays the wave name.	—	By default, the wave is named based on the source and destination sites and the number of waves between them. For example, if there are two waves defined between site 1 and site 2, the waves are named as Site-1-Site-2-1 and Site-1-Site-2-2, respectively. Edit the name if required.
Source Site	Displays the source site name.	—	—
Destination Site	Displays the destination site name.	—	—
Traffic Type	Select the traffic type.	• Optical Source • 100GE • 10GE LAN PHY • 40GE LAN PHY • Fiber Channel 10G • Fiber Channel 16G • Fiber Channel 8G • OC-192/STM-64 • OTU2 • OTU2e • OTU4 • Pluggable Card	Optical Source

Property	Description	Available options	Default option
Protection Type	Choose the protection type. For more information on protection types, see #unique_135. For Client 1+1, ensure that the sites have contentionless sides for the analysis to be successful. By default, Cisco ONP finds both span and node disjoint path for Client1+1 protected waves, but it allows you to force span and node disjoint path.	• Unprotected • Client 1+1	Unprotected
Forecast	Check this check box to change a present wave to a forecast wave.	—	—
Encryption	Check this check box to enable encryption.	—	—

Modify media channel properties

Follow these steps to modify properties of the media channel.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the media channel properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, click the **Services** tab, and click a media channel.

Step 4 Modify the media channel properties as required.

See Media channel properties, on page 110.

Step 5 Click **Update**.

Media channel properties

This table describes various media channel properties.

Table 50: Media channel properties

Property	Description	Available options	Default option
General			
Label	Displays the media channel name.	—	By default, the media channel is named based on the source and destination sites and the number of media channels between them. For example, if there are two media channels between site 1 and site 2, they are named as Site-1-Site-2-1 and Site-1-Site-2-2, respectively. Edit the name if required.
Source Site	Displays the source site name.	—	—
Destination Site	Displays the destination site name.	—	—
Traffic Type	Select the traffic type.	• Optical Source • 100GE • 10GE LAN PHY • 40GE LAN PHY • Fiber Channel 10G • Fiber Channel 16G • Fiber Channel 8G • OC-192/STM-64 • OTU2 • OTU2e • OTU4 • Pluggable Card	Optical Source

Property	Description	Available options	Default option
Protection Type	Select the protection type. For more information on protection types, see #unique_135. For Client 1+1, ensure that the sites have contentionless sides for the analysis to be successful. By default, Cisco ONP finds both span and node disjoint path for Client1+1 protected waves, but allows you to force span and node disjoint path.	• Unprotected • Client 1+1	Unprotected
Forecast	Check this check box to change a present wave to a forecast wave.	—	—
Encryption	Check this check box to enable encryption.	—	—

Modify trail properties

Follow these steps to modify the properties of the trail.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the trail properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, click the **Services** tab.

Step 4 Expand **Waves**, or **Media Channels**.

Step 5 Navigate to the required trail and click it.

Step 6 Modify the trail properties as required. See

- General trail properties, on page 113
- OTN trail properties, on page 114
- Source and destination trail properties, on page 114

Step 7 Click **Update**.

General trail properties

This table describes various general trail properties.

Table 51: General trail properties

Property	Description	Available options	Default option
Label	Displays the name of the trail. You can edit the name.	—	Available options
Path of Wave	Select a fiber.	Displays the fibers available in the network.	—
Regen Sites	Select the regeneration site.	Displays the regeneration sites available in the network.	—
Source Site	Displays the source site name.	—	—
Destination Site	Displays the destination site name.	—	—
Wavelength	Click **Edit** to choose the wavelength.	Diaplys multiple wavelengths.	Auto
Central Wavelength	Click **Edit** to choose the central wavelength.	Displays multiple wavelengths.	Auto
Multicarrier	Indicates whether the transmission is a multicarrier transmission.	—	—
Trunk Mode	Select the trunk mode.	See Supported Cards and Pluggables, on page 181	—
OSNR Forward [dB]	Displays the forward optical signal to noise ratio.	—	—
OSNR Reverse [dB]	Displays the reverse optical signal to noise ratio.	—	—
Colorless	Indicates whether colorless functionality is enabled on the trail.	—	—
Omnidirectional	Indicates whether omnidirectional functionality is enabled on the trail.	—	—
Contentionless	Indicates whether contentionless functionality is enabled on the trail.	—	—

Property	Description	Available options	Default option
Filtering Penality	Displays the value of the penalties that are caused by the different filter types (OADM, and ROADM).	—	—

OTN trail properties

This table lists and defines OTN trail properties.

Table 52: OTN trail properties

Property	Description	Available options	Default option
First ODU	Displays the first Optical Data Unit.	—	—
Last ODU	Displays the last Optical Data Unit.	—	—
SRLGs	Displays the SRLGs associated with the trail.	—	—
OTN Hops	Displays the number of OTN hops.	—	—
Quantity	Displays the number of OTN services on the trail.	—	—

Source and destination trail properties

This table lists and defines various source and destination trail properties.

Table 53: Source and destination trail properties

Property	Description	Available options	Default option
Source			
Src Card Type	Select the card used in the source site.	See Supported Cards and Pluggables, on page 181 and Supported Optical Sources, on page 195 for more details about the list of supported cards.	200G-SD-FEC

Property	Description	Available options	Default option
Src Client Interface	Select a pluggable from the drop-down list.	The pluggables suitable for the chosen card type are displayed. Supported Cards and Pluggables, on page 181 for more information on the list of supported pluggables. The pluggable FR-1(QSFP-100G-FR-S) is supported on the client ports of the 400G-XP LC starting from NCS 2000 Release 11.1.0.	Auto
Src Channel Type	Select the type of source channel.	The available options are: • Auto • Contentionless • Colorless • Colored	Auto
Src Trunk Type	Select the trunk type from the drop-down list.	See Supported Cards and Pluggables, on page 181	Auto
Src Contentionless Side	Select the contentionless side from the drop-down list.	Displays the available contentionless sides.	Auto
Destination			
Dst Card Type	The destination card type is auto populated based on the source card type chosen.	—	—
Dst Client Interface	Select a pluggable from the drop-down list. The pluggables suitable for the chosen card type are displayed.	See Supported Cards and Pluggables, on page 181	Auto
Dst Trunk Type	Select the trunk type from the drop-down list.	See Supported Cards and Pluggables, on page 181	Auto
Dst Channel Type	Select the type of the destination channel.	The available options are: • Auto • Contentionless • Colorless • Colored	Auto

Property	Description	Available options	Default option
Dst Contentionless Side	Select the contentionless side from the drop-down list.	Displays the available contentionless sides.	Auto

Modify section properties

Follow these steps to modify properties of the section.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the section properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, click the **Services** tab.

Step 4 Expand **Waves**, or **Media Channels**.

Step 5 Navigate to a trail and select a section within the trail.

Step 6 Modify the section properties.

The section and the trail have the same properties. See these references for descriptions of the properties.

- General trail properties, on page 113
- OTN trail properties, on page 114
- Source and destination trail properties, on page 114

Step 7 Click **Update**.

Modify side properties

Table 54: Feature History

Table 55: Feature History

Feature Name	Release Information	Feature Description
Support for NCS2K-MF-CL-SC (C and L-band combiner and splitter)	Cisco ONP Release 4.2	Cisco ONP supports the passive module, NCS2K-MF-CL-SC (C and L-band combiner and splitter), starting from the NCS 2000 system release 12.2 for SSON and non-SSON networks. This feature enables combining C and L band wavelengths.

Use this procedure to modify the properties of a side in a site.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the side properties of a site.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, navigate to **Sites** > **Site** > **Side**.

Step 4 Modify the side properties as required. See these references for the property descriptions.

- General side properties, on page 117

Step 5 Click **Update.**

General side properties

This table describes various general properties for the sides of a site.

Property	Description	Available options	Default
Label	Displays the label of the side.	—	—
Type	Displays the type of the side: Line or Contentionless	—	—

Property	Description	Available options	Default
Colorless Ports (Displayed for Line side)	Enter the number of colorless ports. From Release 24.3.1, this property is enabled for SMR-9 card	—	—
Contentionless Ports (Displayed for Contentionless side)	Choose the number of contentionless ports.	—	—

Property	Description	Available options	Default
Enable C+L Band S/C (Displayed for Line side type)	Cisco ONP supports the passive module, NCS2K-MF-CL-SC (C and L-band combiner and splitter), starting from the NCS 2000 system release 12.2 for SSON and non-SSON networks. Check this check box to enable the NCS2K-MF-CL-SC card. This card is supported for ROADM, OLA, and traffic nodes, but not on the passthrough node. **Note** When you enable this option on a side: • It is automatically enabled on the side that is connected to the selected side through a fiber. • The fiber property *Raman Amplified is* automatically disabled, and the opposite way. • This card introduces a certain amount of attenuation and insertion loss that is reflected in the ANS parameters. The NCS2K-MF-CL-SC module does not appear in the layout.	—	—

Modify C-band amplifier properties

Use this procedure to modify the properties of C-band amplifiers in a site.

Table 56: Feature History

Feature Name	Release Information	Feature Description
Manual Editing of Raman COP values	Cisco ONP Release 4.1	This feature allows you to edit the crosstalk values of the Raman COP amplifier in the SSON network, starting from NCS 2000 Release 11.1.

Table 57: Feature History

Feature Name	Release Information	Feature Description
Inline Amplifier	Cisco ONP Release 4.2	The **Inline Amplifier** option allows you to enable an inline amplifier in the network. You can simulate the optical feasibility of the network with and without an inline amplifier. Based on the colorless or colored add/drop type selected and the QSFP-DD pluggable status, a default inline amplifier is enabled for the network.

Note Make sure that SMR card is forced on the site before you update the c-band amplifier properties.

Before you begin

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network where you want to modify the C-band properties.

Step 2 Choose **Network** > **Entity Editor**.

Alternatively, click the network name in the network tree, and click **Show Advanced Properties** displayed under the network tree.

Step 3 In the **Entity Editor** window, click the **Site** tab.

Step 4 Choose **Sites** > **Site** > **Site domain** > **Side** > **C-Band**.

Step 5 Click **C-Band Amplifier** and modify the properties. For detailed property descriptions, refer to:

- General properties of a C-band amplifier, on page 121
- C-band amplifier and attenuator options, on page 124
- Raman amplification properties of a C-band amplifier, on page 127

General properties of a C-band amplifier

This table lists the general properties of a C-band amplifier.

Table 58: General properties of a C-band amplifier

Options	Description	Available options	Default
Raman COP Tilt	Enter a value.	—	Auto
Pre Tilt	Enter a value.	—	Auto
Raman Tilt	Enter a value.	—	Auto
Booster Tilt	Enter a value.	—	Auto

Options	Description	Available options	Default

Inline Amplifier		• Yes—EDFA17 or EDFA35 amplifier is chosen as the default amplifier when you choose colored add/drop module MD-64-C or colorless add/drop MF-6AD-CFS, respectively. See Modify Add/Drop multiplexer properties, on page 129.
		• No—No amplifier can be forced.
		• Auto
		  • EDFA17 amplifier is chosen as the default amplifier when any one of the demands aggregated in MD-64-C has low launch power optical resource or QSFP-DD pluggable is forced.
		  • EDFA35 amplifier is chosen as the default amplifier when any one of the demands aggregated in MF-6AD-CFS has low launch power optical resource or QSFP-DD pluggable is forced.
			Auto

Options	Description	Available options	Default
	Choose whether inline amplifier can be forced. **Note** When you configure MF-6AD-CFS+EDFA35 in an SSON or non-SSON network, the optical results show system error for the demands of the same or different types. This error affects the what-if analysis. Hence we recommend choosing the appropriate channel and client attenuators so that the inline amplifier works at the proper gain range. You can view the amplifier added in the **IPC**, **BOM**, and **Layout** tabs, after the successful analysis. **Note** • When you add a QDD demand while upgrading a network where the Inline Amplifier property is set as *no*, the inline amplifier can be included in the network only if you unlock the side and set the Inline amplifier property as *Auto* or *Yes*. • Default colorless configuration does not require inline amplifier. • When there are no demands passing through the colored or colorless Add/Drop device,		

Options	Description	Available options	Default
	the forced Inline amplifier is not placed.		

C-band amplifier and attenuator options

This table describes the various C-band amplifier and attenuator options you can choose in the C-band proeprties.

Table 59: C-band amplifier and attenuator options

Options	Description		
From Fiber			
Pre Amp	Choose a preamplifier from the drop-down list. The default value is Auto. To enable this field for ROADM and Traffic nodes, you must choose SMR-9 or SMR-20 from the **Site Type** drop-down list under the Site properties. If you choose SMR-9, the available options are: • SMR9-FS-EDFA17-PRE • SMR9-FS-EDFA24-PRE • SMR9-FS-EDFA24-PRE If you choose SMR-20, the available options are: • SMR20-FS-EDFA17-PRE • SMR20-FS-EDFA24-PRE For the OLA site, the available options are: • EDFA35-35-PRE • EDFA35-24-PRE • OPT -EDFA-17 • OPT -EDFA-24		

Options	Description		
Output Power	The default value is Auto. You can enter a value.		
Attenuator In	This field is enabled only when you choose a preamplifier. Choose an attenuator from the drop-down list. The available options are: • ATT-LC-2 • ATT-LC-3 • ATT-LC-5 • ATT-LC-7 • ATT-LC-10 • ATT-LC-12 • ATT-LC-15 • ATT-LC-18		
Attenuator Out	This field is enabled only when you choose a preamplifier. Choose an attenuator from the drop-down list. The available options are: • ATT-LC-2 • ATT-LC-3 • ATT-LC-5 • ATT-LC-7 • ATT-LC-10 • ATT-LC-12 • ATT-LC-15 • ATT-LC-18		
To Fiber			

Options	Description		
Booster	The default value is Auto. To enable this field for ROADM and Traffic nodes, you must choose SMR-9 or SMR-20 from the **Site Type** drop-down list under the Site properties. If you choose SMR-20, the default booster is 20SMR-FS-BST. If you choose SMR-9, default booster is SMR9-FS-EDFA-BST. For the OLA node, the available options are: • EDFA35-35-BST • EDFA35-24-BST • OPT -EDFA-17 • OPT -EDFA-24		
Output Power	The default value is Auto. You can enter a value.		
Attenuator In	This field is enabled only when you choose a booster. Choose an attenuator from the drop-down list. The available options are: • ATT-LC-2 • ATT-LC-3 • ATT-LC-5 • ATT-LC-7 • ATT-LC-10 • ATT-LC-12 • ATT-LC-15 • ATT-LC-18		

Options	Description		
Attenuator Out	This field is enabled only when you choose a booster. Choose an attenuator from the drop-down list. The available options are: • ATT-LC-2 • ATT-LC-3 • ATT-LC-5 • ATT-LC-7 • ATT-LC-10 • ATT-LC-12 • ATT-LC-15 • ATT-LC-18		

Raman amplification properties of a C-band amplifier

This table describes the Raman amplification properties of a C-band amplifier.

Table 60: Raman amplification properties of a C-band amplifier

Options	Description		
Raman Amp	Choose the Raman amplifier from the drop-down list. **Note** To force the RAMAN amplifier, you must enable **RAMAN amplified** on the fiber, else the **Raman Amp** is disabled, and network analysis fails.	The available options for ROADM and Traffic sites are: • Auto • RAMAN-CTP • RAMAN-COP-CTP Raman Amp can be forced only between two nodes. The available options for the OLA site are: • Auto • EDRA1-26 • EDRA1-35 • EDRA2-26 • EDRA2-35 • RAMAN-CTP	Auto
Raman CTP Gain	Enter a value.	—	—
Raman COP Gain	Enter a value. This field is enabled only when you choose RAMAN-COP-CTP.	—	—
Static Data	By default, this option is disabled. Enable it to edit the crosstalk values of the Raman COP amplifier. **Note** Static data is supported from Release 11.1 for SSON network.	—	—
Linear XT Avg	Edit the value of average linear crosstalk.	-99.0	-99.0
Linear XT Six	Edit the value average linear crosstalk sigma.	0.0	0.0

Options	Description		
NonLinear XT Avg	Edit the value of average nonlinear crosstalk.	-99.0	-99.0
NonLinear XT Sig	Edit the value of average nonlinear crosstalk sigma.	0.0	0.0

Note Raman crosstalk values are present in the ANS file under *logoparameters* section.

Modify Add/Drop multiplexer properties

Table 61: Feature History

Feature Name	Release Information	Feature Description		
Modify Properties of Add/Drop Multiplexer and Demultiplexer	Cisco ONP Release 4.2	You can create and validate network designs by choosing colored and colorless add/drop multiplexers and demultiplexers, and interlever under **C-Band** > **Add/Drop**. The following options are supported in this release:		
		Type of Add/Drop	Options	Network Supported
		Colorless	• Direct SMR • MF-6AD-CFS	• SSON • Non-SSON
		Colored	• MD-64-C • MD-48-ODD • MD-48-EVEN • MD-48-ODD + MD-48-EVEN	• SSON • Non-SSON
		Interlever	• MpoCable • MD-48-CM	• Non-SSON

Use this procedure to modify the properties of the add/drop multiplexer in a site.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to modify the Add/Drop multiplexer properties.

Step 2 Choose **Network** > **Entity Editor**.

Step 3 In the **Entity Editor** window, navigate to **Sites** > **Site** > **Site domain** > **Side** > **C-Band**

Step 4 Click **Add/Drop** and modify the properties in the next pane. For the property descriptions, refer to Add/Drop multiplexer properties, on page 130.:

Step 5 Click **Update**.

Add/Drop multiplexer properties

This table describes the general properties of the Add/Drop multiplexers.

Table 62: Add/Drop multiplexer properties

Options	Description	Available options	Default
Colored Add/Drop	Choose the colored add/drop multiplexer and demultiplexer. To mix 16-AD-CCOFS and MD-48-ODD/EVEN on the same MPO port of SMR-20, and connect MD-48-ODD/EVEN to SMR-20 by using MPO-8LC and UPG-4, enable the Shared SMR port and select the required colored Add/Drop.	• MD-64-C: Passive optical multiplexer and demultiplexer module (for SSON network) • None • Auto Cisco ONP adds some options automatically based on the colored demands created and the wavelengths you configure in the non-SSON network. These options include: • MD-48-ODD • MD-48-EVEN • MD-48-ODD + MD-48-EVEN	Auto

Options	Description	Available options	Default
Colorless Add/Drop	Choose the colorless add/drop multiplexer and demultiplexer.	• Auto • Direct SMR: SMR-20 card that is directly connected to the colorless channels through MF-MPO-16-LC. **Note** If the **Site Type** property is set to *SMR-9*, the **Colorless Ports** property under the Side will be disabled. • MF-6AD-CFS: 6 Port Add/Drop Module (supported only for ROADM starting from NCS 2000 system release 11.0, and traffic site). **Note** If you choose MF-6AD-CFS for a side, we recommend you to choose the same for other sides of the site.	Auto
Interlever Type	Choose the interlever type from the drop-down list. **Note** **Interlever Type** property is visible and editable only for Line sides of Multi-Degree nodes having **Site Type** property as *SMR-9* and **Scalable Upto Degree** property as *8* under the C-Band tab at the Site level.	• Auto • MpoCable • MD-48-CM	Auto

Table 63: Add/Drop multiplexer properties

Options	Platform	Description	Available options	Default
Colored Add/Drop	NCS 2000	Choose the colored add/drop multiplexer and demultiplexer. To mix 16-AD-CCOFS and MD-48-ODD/EVEN on the same MPO port of SMR-20 and connect MD-48-ODD/EVEN to SMR-20 via MPO-8LC and UPG-4, enable the Shared SMR port and select the required colored Add/Drop.	• MD-64-C: Passive optical multiplexer and demultiplexer module (for SSON network) • None • Auto Cisco ONP adds some options automatically based on the colored demands created and the wavelengths you configure in the non-SSON network. These options include: • MD-48-ODD • MD-48-EVEN • MD-48-ODD + MD-48-EVEN	Auto
	NCS 1010	Choose the colored add/drop multiplexer and demultiplexer for NCS 1010.	• Auto • None • MD-32-EVEN • MD-32-ODD • MD-32-ODD+MD-32-EVEN	Auto
	Colorless Add/Drop	NCS 2000	Choose the colorless add/drop multiplexer and demultiplexer for NCS 2000.	Auto

Options	Platform	Description	Available options	Default	
				• Auto • Direct SMR: SMR-20 card that is directly connected to the colorless channels through MF-MPO-16-LC. **Note** If the **Site Type** property is set to *SMR-9*, the **Colorless Ports** property under the Side will be disabled. • MF-6AD-CFS: 6 Port Add/Drop Module (supported only for ROADM starting from NCS 2000 system release 11.0, and traffic site). **Note** If you choose MF-6AD-CFS for a side, choose the same for other sides of the site.	
		NCS 1010	Choose the colored add/drop multiplexer and demultiplexer for NCS 1010. **Note** QDD optical sources are not supported (both as optical source and pluggable) with colorless BRK-8, BRK-16, or BRK-24 configurations.	• Auto • None • BRK-8 • BRK-16 • BRK-24	Auto

Options	Platform	Description	Available options	Default
Colorless Ports	NCS 1010	Enter the number of colorless ports. The default value is 0. If you do not change the default value, Cisco ONP automatically calculates the number of colorless ports based on the number of circuits added and colorless add/drop units forced.	—	—
Interlever Type	NCS 2000	Choose the interlever type from the drop-down list. **Note** **Interlever Type** property is visible and editable only for Line sides of Multi-Degree nodes having **Site Type** property as *SMR-9* and **Scalable Upto Degree** property as *8* under the C-Band tab at the Site level.	• Auto • MpoCable • MD-48-CM	Auto

MPO connector properties

This table describes the properties of MPO connectors that are used in Add/Drop multiplexers.

Table 64: MPO connector Add/Drop properties

LC connector properties

This table describes the properties of LC connectors that are used in Add/Drop multiplexers.

Table 65: LC connector Add/Drop properties

Modify client properties

Use this task to modify the properties of a client-side attenuator in a site.

Before you begin

Table 66: Feature History

Feature Name	Release Information	Feature Description
Channel Attenuators	Cisco ONP Release 4.2	You can set up channel attenuators for QSFP-DD demands. You can choose different channel attenuators based on the specific configuration and check for the optical feasibility of the channel.

Log in to the Cisco ONP web interface, on page 6

Procedure

Step 1 Open the network where you want to modify the client properties.

Step 2 Choose **Network** > **Entity Editor**.

Alternatively, click the network name in the network tree, and click **Show Advanced Properties** displayed under the network tree.

Step 3 In the **Entity Editor** window, click the **Site** tab.

Step 4 Choose **Sites** > **Site** > **Site domain** > **Side** > **Clients** > **Channel-Attenuators**.

Step 5 In the right pane of the **Entity Editor** window, modify properties of the client-side attenuator.

See Client properties, on page 135 for the descriptions.

Step 6 Click **Update**.

Client properties

This table describes various System Release properties under the Network properties.

Options	Description	Available options	Default option
General			
Wavelength	This column displays the selected wavelength.	—	—

Options	Description	Available options	Default option
New Wavelength - Auto	Click **Edit** to select a Flex Grid or Fixed Grid wavelength. **Note** Select **Fixed Grid (64-Chs)** for SSON network with NCS1K-MD-64-C card. **Note** NCS1K-MD-64-C card has First Channel limitation for Colored sites. First Channel (196.1 THz) in Fixed Grid (64-Chs) wavelength supports only Terminal Add/Drop sites and not ROADM sites.		
RX-Attenuator	Choose an RX-Attenuator from the drop-down list. **Note** You must select a wavelength to edit this field.	• Auto • None • ATT-LC-2 • ATT-LC-3 • ATT-LC-5 • ATT-LC-7 • ATT-LC-10 • ATT-LC-12 • ATT-LC-15 • ATT-LC-18	Auto

Options	Description	Available options	Default option
TX-Attenuator	Choose a TX-Attenuator from the drop-down list. **Note** You must select a wavelength to edit this field.	• Auto • None • ATT-LC-2 • ATT-LC-3 • ATT-LC-5 • ATT-LC-7 • ATT-LC-10 • ATT-LC-12 • ATT-LC-15 • ATT-LC-18	Auto

Sort the Network Elements

You can sort the sites, services, fibers, waves, and SRLG in ascending or descending order. This feature is useful for huge networks, making it quick to locate the required site, fiber, wave, or SRLG names.

Follow these steps to sort the network elements in the network tree.

Procedure

Step 1 Open the network where you want to sort the network elements.

Step 2 Right-click the network element in the network tree, such as **Sites**, and choose **Ascending** or **Descending**.

The network elements are sorted based on the alphabets, numbers, and, alphanumeric.

Regeneration support

Signal degradation in optical networks

As the fiber length increases in an optical network, unavoidable issues such as attenuation and dispersion lead to signal loss and power degradation. These problems can significantly affect the network's performance over long distances, necessitating the need for regenerators to maintain efficient signal transmission.

Role of regenerators

To address signal degradation, regenerators are used at specific points in the network to recover and strengthen optical signals. They achieve this through Optical-Electrical-Optical (OEO) conversion, which involves:

- Converting the weak optical signal into an electrical signal.
- Cleaning and amplifying the electrical signal.
- Converting the restored signal back into an optical format, known as Optical-Electrical-Optical (OEO) conversion.

Cisco ONP and regeneration sites

Cisco ONP supports the establishment of regeneration sites within optical networks. These sites are essential in maintaining signal integrity over long distances by utilizing regenerators to enhance the network's overall performance.

Note A regenerator site can only be a ROADM site.

Create a regeneration site

Table 67: Feature History

Feature Name	Release Information	Feature Description
Wavelength Forcing at the Section Level	Cisco ONP Release 4.1	This feature enables you to assign distinct wavelengths to various sections of the Regen sites

Follow these steps to create a regeneration site in the network.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the network where you want to create a regeneration site.

Step 2 In the network tree, expand **Waves**, select a wave and drill down to its trail.

Note
If the network is an SSON network , you see **Media Channels** instead of waves. Expand **Media Channels** , and drill down to its trail.

Step 3 Click the trail to view its properties.

Step 4 From the **Regen Sites** drop-down list, select a regeneration site.

Note
If you select a fiber from the **Path of Wave** drop-down list, you cannot select any regeneration site to force a path. Similarly, if you select a regeneration site, you cannot force a path for the wave. However, if you want to force a fiber, select the fiber from the **Path of Wave** drop-down list available under the section properties.

Step 5 If required, select the wavelength of each section in the properties for non-SSON network.

Note
For the SSON network, you can select the wavelength only at the trial level.

Step 6 Click **Update**.

Whenever a regeneration site is created, a new section is added along with the existing section under the trail. Regeneration can be performed using any two cards back-to-back or with a dedicated regenerator card.

Step 7 Click **Analyze** to analyze the network.

After analysis, if you click trail or section in the network tree, the map highlights the trail in orange color and the section in green color.

Note
You can assign different wavelengths for different sections. The **Wavelength** property under trail is denoted as "*", when different wavelengths are assigned for different sections.

You can also add a regeneration site when you are designing a new network or upgrading a network.

Multidegree ROADM

A multidegree ROADM is a network node configuration that

- enables a site to connect to two or more fiber spans,
- allows flexible routing of wavelengths across multiple paths in a mesh network, and
- supports higher degrees than simpler ROADMs, which typically connect only two directions.

You can design a multidegree ROADM configuration in Cisco ONP using cascaded SMR .

Design a multidegree ROADM site using cascaded SMR

Use this procedure to design a multidegree ROADM site in your network, using cascaded SMR modules.

When designing a multidegree ROADM site using cascaded SMR, be aware of these limitations:

- The configuration only supports contentionless add/drop demands.
- Layer-2 SMR is supported only for the SMR-20 card.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

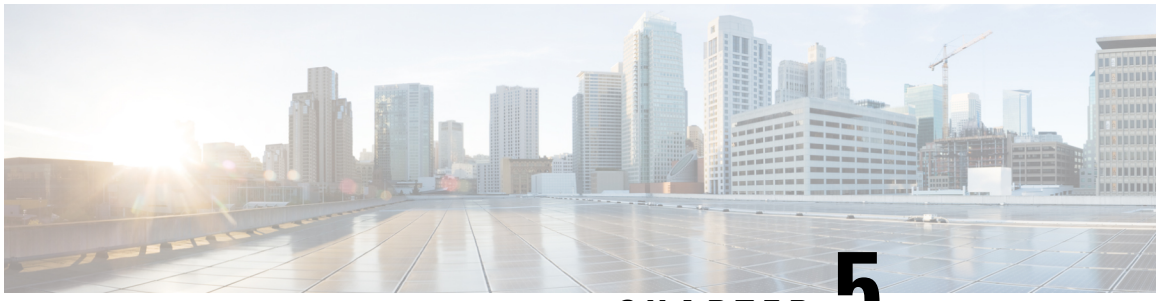
Step 1 Design a network. For detailed instructions, see the Manually design a network using Cisco ONP, on page 22 task.

Step 2 Modify these site properties.

- Set the **Structure** to *Multidegree* in the **C Band** section.
- Set the **Site Type** to *SMR-20* in the **C Band** section.
- Set **Degree Mesh Type** to *Auto* or to *DEG-5/UPG-4* in the **C Band** section.
- Check the **Evolved Mesh** and **Cascaded SMR** check boxes in the **General** section.
- Set the **Mpo16TOMpo8** to *MPO16To2MPO8* cable in the **General** section.

Step 3 Add a contentionless side to the site. For detailed steps, see the Add contentionless side to a site, on page 88 task.

Step 4 Modify the number of contentionless side ports for the site as needed. For detailed steps, see the Modify the number of contentionless side ports at a site , on page 91 task.



CHAPTER 5

Configure a Network

This chapter describes the various ways of configuring the network designed through Cisco ONP.

Configure a network for contentionless functionality

Use this procedure to configure contentionless functionality in a network.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Procedure

Step 1 Create a network design. See #unique_172.

Step 2 Add contentionless sides to the required sites. See Add contentionless side to a site, on page 88.

Step 3 Set the channel type for the demands:

a) In the **Entity Editor** window, click the **Services** tab.

b) Click the service connecting the site and set the **Src Channel Type** property as *Auto* or *Contentionless*. Then, click the trail under the wave (for non-SSON) or Media Channel (for SSON) and set the **Src Channel Type** property to *Auto* or *Contentionless*.

Note
Contentionless is the default option when you select *Auto*.

c) Click **Update**.

Step 4 Analyze the network by choosing **Network** > **Analyze.**

Configure a network for colorless functionality

This procedure guides you through the process of configuring colorless functionality in an NCS 2000 optical network.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Procedure

Step 1 Create a network design. See #unique_172 .

Step 2 Set the channel type for the demands:

a) In the **Entity Editor** window, click the **Services** tab.

b) Click the service connecting the site. Set the **Src Channel Type** property as *Colorless*. For non-SSON click the trail under the wave. For SSON, click the Media Channel (for SSON). Set the **Src Channel Type** property as *Colorless*.

c) Under the **Site > Side** properties, choose the Line type side from which you want to create the colorless demand, and enter the number of **Colorless Ports**.

From Release 24.3.1, you can select the colorless ports for the SMR-9 card.

The number of colorless ports for MF-6AD-CFS depends on the **Scalable Upto Degree** property. See Colorless ports for SSON and Non-SSON networks, on page 142.

d) Click **Update**.

Step 3 Under the **C-Band** properties, choose *MF-6AD-CFS* or *Direct SMR* as the **Colorless Add/Drop**.

Step 4 Click **Update.**.

Step 5 Analyze the network by choosing **Network** > **Analyze.**

You can see the colorless Add/Drop unit getting added in the layout and BOM.

Colorless ports for SSON and Non-SSON networks

This table explains the maximum number of colorless ports that can be added based on the **Scalable Upto Degree** property for the MF-6AD-CFS card.

Table 68: Colorless ports for SSON and Non-SSON networks

Site type	Scalable upto degree	Maximum number of colorless ports for SSON	Maximum number of colorless ports for non-SSON
SMR-20	4	72	72
SMR-20	8	72	72
SMR-20	12	24	24
SMR-20	16	24	24

Site type	Scalable upto degree	Maximum number of colorless ports for SSON	Maximum number of colorless ports for non-SSON
SMR-20	Line	96	96
SMR-20	Terminal	120	96

Configure a network for colorless functionality

Configure a network for colored functionality

This procedure guides you through the process of configuring colored functionality in an NCS 2000 optical network.

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Procedure

Step 1 Create a network design. See #unique_172 .

Step 2 Set the channel type for the demands:

a) In the **Entity Editor** window, click the **Services** tab.

b) Click the service connecting the site and set the **Src Channel Type** property as **Colored**. For non-SSON click the trail under the wave. For SSON, click the Media Channel (for SSON). Set the **Src Channel Type** property as **Colored**.

c) Click **Update**.

Step 3 For an SSON network, complete these steps.

a) Under the **C-Band** properties, choose **MD-64-C** as the **Colored Add/Drop**.

Note
MD-64-C is supported from NCS 2000 Release 12.x.

b) Click **Update.**.

By default, the system adds **MD-48-ODD** or **MD-48-EVEN**as the **Colored Add/Drop** when **Share SMR Port** is not enabled.

Note
If you choose **MD-48-EVEN** or **MD-48-ODD**, select an even wavelength for the **Wavelength** property under **Trail**.

Step 4 When **Share SMR Port** port is enabled, you can select the **Colored Add/Drop** by using these steps:

a) Under the **C-Band** properties, choose **MD-48-ODD**, **MD-48-EVEN**, or **MD-48-ODD+MD-48-EVEN** as the **Colored Add/Drop**.

Note
These Add/Drop units are supported from NCS 2000 Release 11.x.

b) Click **Update**.

Step 5 Analyze the network by choosing **Network** > **Analyze**.

The colored Add/Drop unit appears in the layout and BOM.

Configure a network with mixed Add/Drop multiplexers and demultiplexers

Use the following procedure to configure mixed wavelengths in a network:

Before you begin

Log in to the Cisco ONP web interface, on page 6 as a user with the admin role.

Table 69: Feature History

Feature Name	Release Information	Feature Description
Support for Mixed Add/Drop Configuration	Cisco ONP Release 4.2	You can configure different functionalities in the network created in Cisco ONP. Mixed wavelengths such as colorless and contentionless, colored and contentionless, can be added/dropped on the same side or direction. The following mixed configurations are supported: • Colored (MD-48-ODD/MD-48-EVEN) and Contentionless (16-AD-CCOFS) without shared SMR port • Colored and Contentionless (MD-64-C and 16-AD-CCOFS) • Colored (MD-64-C) and Colorless (Direct SMR) • Colored (MD-48) and Contentionless (16-AD-CCOFS) with Shared SMR Port • Colorless and MD-48-ODD/MD-48-EVEN • Colorless and 16-AD-CCOFS

Procedure

Step 1 Create a network design. See #unique_172.

Step 2 Set the properties of the network under the **Entity Editor** for different combinations of the functionalities, as described in Supported and unsupported mixed configurations, on page 145.

Note
You cannot mix the MF-6AD-CFS colorless configuration with any other configuration.

Supported and unsupported mixed configurations

This section describes the list of mixed configurations that are supported and unsupported by Cisco ONP.

Table 70: Supported mixed Configurations

Supported network type	Possible mixed configurations	Properties to be set
Non-SSON	Colored (MD-48-ODD/MD-48-EVEN) and Contentionless (16-AD-CCOFS) without shared SMR port	• Add required number of contentionless sides. • **Channel Type—**Set the **Src Channel Type** and **Dst Channel Type** to be **Colored** for one wave. Set the **Src Channel Type** and **Dst Channel Type** to be **Contentionless** for the second wave created on the same site. Both wavelengths must add/drop in the same side or direction. • By default, MD-48-ODD or MD_48-EVEN is added as the Colored Add/Drop in the BOM and layout when you set the **Channel Type** as **Colored** and when **Shared SMR Port** is disabled. By default, 16-AD-CCOFS is added in the BOM and layout when you set the **Channel Type** as **Contentionless**.

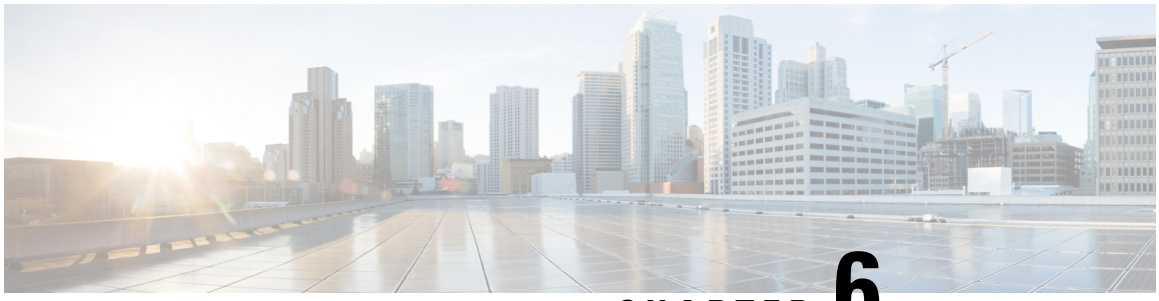
Supported network type	Possible mixed configurations	Properties to be set
SSON	Colored and Contentionless (MD-64-C and 16-AD-CCOFS)	• Add required number of contentionless sides. • **Channel Type—**Set the **Src Channel Type** and **Dst Channel Type** to be **Colored** for one media channel. Set the **Src Channel Type** and **Dst Channel Type** to be **Contentionless** for the second media channel created on the same site. Both channels must add/drop in the same side or direction. • **Colored Add/Drop—**MD-64-C under the side.
SSON	Colored (MD-64-C) and Colorless (Direct SMR)	• **Channel Type—**Set the **Src Channel Type** and **Dst Channel Type** to be **Colored** for one media channel. Set the **Src Channel Type** and **Dst Channel Type** to be **Colorless** for the second media channel created on the same site. Both channels must add/drop in the same side or direction. • Enter the number of **Colorless Ports** under the **Line Side** properties. • **Colored Add/Drop—**MD-64-C **Colorless Add/Drop—**Direct SMR

Supported network type	Possible mixed configurations	Properties to be set
Non-SSON	Colored (MD-48) and Contentionless (16-AD-CCOFS) with Shared SMR Port	• Add required number of contentionless sides. • **Channel Type—**Set the **Src Channel Type** and **Dst Channel Type** to be **Colored** for one wave. Set the **Src Channel Type** and **Dst Channel Type** to be **Contentionless** for the second wave created on the same site. Both wavelengths must add/drop in the same side or direction. • Check the **Shared SMR Port** check box, under the **Site** properties. • **Colored Add/Drop—**MD-48-ODD, MD-48-EVEN, or MD-48-ODD and MD-48-EVEN • If you choose **MD-48-EVEN**, make sure to select an even wavelength for the **Wavelength** property under **Trail**.
Non-SSON	Colorless and MD-48-ODD/MD-48-EVEN	• **Channel Type—**Set the **Src Channel Type** and **Dst Channel Type** to be **Colorless** for the wave. • Enter the number of **Colorless Ports** under the **Line Side** properties. • • • By default, MD-48-ODD/MD-48-EVEN is added as colored Add/Drop in the BOM and layout, when any colored demand is added in the non-SSON network.

Supported network type	Possible mixed configurations	Properties to be set
SSON	Colorless and Contentionless (16-AD-CCOFS)	• Add required number of contentionless sides. • **Channel Type—**Set the **Src Channel Type** and **Dst Channel Type** to be **Colorless** for the wave or media channel. • **Channel Type—Colorless** for one wave and **Contentionless** for another wave created on the same site. Both wavelengths must add/drop in the same side or direction.

Table 71: Unsupported mixed configurations

Network type	Mixed configurations
SSON	Colored (MD-64-C) and Colorless (MF-6AD-CFS)
SSON	Contentionless and Colorless (MF-6AD-CFS)
SSON	Colored (MD-64-C), Contentionless, and Colorless (MF-6AD-CFS)
SSON	Colored (MD-64-C) and Layer-2 Contentionless
Non-SSON	Contentionless and Colorless (MF-6AD-CFS)
Non-SSON	Colored (MD-48) and Colorless (MF-6AD-CFS)
	Colorless (Direct SMR) and Colorless (MF-6AD-CFS)
Non-SSON	Colored, Contentionless, and Colorless (MF-6AD-CFS)



CHAPTER 6

View Network Reports

Network reports

The Cisco ONP home page has multiple tabs to access the reports of the analyzed network. You can also view the reports for specific site, fiber, or wave properties by clicking the respective report in the Network Tree pane. The tabs are:

- Dashboard
- Elements
- Map
- BOM
- Layout
- Results

View reports in the Dashboard tab

Follow these steps to view various reports of an analyzed network under the **Dashboard** tab.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the analyzed network for which you want to view the network summary.

Step 2 Click the **Dashboard** tab.

The **Network Summary** tab displays this information about the network:

- Total count of sites
- Total count of fibers

- Total count of SRLGs (Shared Risk Link Groups)
- Total count of services
- Total count of waves/media channels/circuits
- Total count of messages

View reports in the Elements tab

The **Elements** tab provides comprehensive reports of network elements and any associated messages.

Follow these steps to view the network elements report and messages.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the analyzed network for which you want to view the network summary.

Step 2 Click the **Elements** tab.

You can view the reports described in this table.

Table 72: Reports under Elements

Report	Description
Sites	Shows the site information, which consists of the name of the sites, their types, and their X and Y coordinate values.
Fibers	Shows the information about the fiber length between the source and the destination for the corresponding sites.
Services	Shows the service type, source and destination sites for particular service, quantity, protection type, and status. For each service, the report shows the primary path, secondary path, and their status.

Report	Description
Waves	The Waves report shows the number of waves available in the network and the wave utilization. Click each wave to view the following details: • Wave: Consists of a wave UID and its source and destination sites. • Wave Details: Provides details of wave OSNR, channel path, OTN services associated to wave and excluded channels. • Channels: Port details of the source and destination cards, the wavelength that is used, and its utilization demands. • Optical Results: Provides details of optical parameters such as OSNR, SOL, EOL, power margin, CD, and PMD.
SRLGs	Lists the names of created SRLGs and their fiber details. Click **Export** at the bottom to export the report in .xlsx format.
Messages	Shows messages that relate to errors that occurred while analyzing the network. By default, only critical messages for the analyzed network are listed here. You can disable the **Critical Only** toggle button to view all messages.

Step 3 Click each tab to view the respective report.

Step 4 Click the Pop-up icon to view the reports in a larger, resizable window.

View details of the BOM report

Table 73: Feature History

Feature Name	Release Information	Feature Description
MLP Brownfield with Diff BOM	Cisco ONP Release 4.1	This feature allows you to perform the following: • Compare the BOMs of two or more LNI imported networks. • Upgrade brownfield network. • Upgrade the Cisco ONP network with traffic sites.

The Bill of Materials (BOM) report includes these components:

- Detailed price lists for each site.
- The overall BOM for the entire network.

Follow these steps to view the BOM report for an analyzed network.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the analyzed network for which you want to view the BOM.

Step 2 Click the **BOM** tab.

The BOM details are displayed.

To view the BOM details for OTN and DWDM separately, click each site. See Licensed PIDs available in the BOM report, on page 152for the list of licensed PIDs added into the BOM report.

See for the list of licensed PIDs added into the BOM report.

Step 3 View the BOM details for any particular site.

a) In the network tree, expand **Site** and right-click the required site.

b) Click **Open BOM**

Cisco ONP opens the **BoM** tab and provides the BoM details of the selected site.

c) Expand the Site to view the PID information.

Step 4 Click **Export** to export the BOM details in the form of a spreadsheet, and save it into your local system.

We recommend that you export the BOM report only in analyze mode. Exporting the reports in the upgrade and release upgrade modes may lead to inaccuracies..

Step 5 Compare the BOM of the existing network with other networks:

a) Click **Compare with: Other Networks**.

b) From the **Other Networks** dialog box, choose the network that you want to be compared with.

You can view both BOM reports displayed on the same page for comparison.

Licensed PIDs available in the BOM report

Table 74: Feature History

Feature Name	Release Information	Feature Description
Support for New PIDs for SMR-20 Card	Cisco ONP Release 4.2	The following new licensed PIDs for the SMR-20 card are displayed on the BOM page so that you can view the price details and consider ordering. • NCS2K-FSSMR-2LIC= • E-NCS2K-1P-LIC= • E-NCS2K-5P-LIC= • E-NCS2K-10P-LIC=

Cisco ONP introduces new licensing PIDs with each platform release to incorporate the latest updates and features.

This table lists the licensed PIDs included in the BOM report for different Cisco ONP releases.

Table 75: Licensed PIDs added to BOM report

Cisco ONP release supported from	Platform	PIDs and description
4.2	NCS 2000	• **NCS2K-FSSMR-2-LIC=** : 20-port FS-SMR licensed to enable two ports • **E-NCS2K-1P-LIC=** : Software license to enable one port on licensed 20-port FS-SMR • **E-NCS2K-5P-LIC=** : Software license to enable five ports on licensed 20-port FS-SMR • **E-NCS2K-10P-LIC=** : Software license to enable ten ports on licensed 20-port FS-SMR
5.2	NCS 1010 from Release 7.11.1	• **NCS1K10-ATO=** : NCS 1010 ATO • **SF-NCS1K10-7111K9S=** : Software license to download the COSM NETCONF XML file for the COSM UI. • **NCS1K4-CCMD-C=** : 16-port, C-Band Colorless Coherent Multiplexer/Demultiplexer with an EDFA • **NCS1K4-CCMD-L=** : 16-port, L-Band Colorless Coherent Multiplexer/Demultiplexer with an EDFA

View details of layout and internal connections

Follow these steps to obtain the layout details and internal connections of an analyzed network.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Click the **Layout** tab on the Cisco ONP homepage.

Step 2 Type the site name in the search box.

The site layout is displayed with its racks and cards.

a) Hover the mouse pointer over the transponder card to view the details of the slot, the PID of the card, and the ports.
b) Expand the Ports to view details, such as wavelength and trunk mode.
c) Hover the mouse pointer over the chassis to view the total power consumption.

SVO supports up to 50 UIDs; beyond which, the site layout displays incorrect UID for the chassis.

Step 3 Click the Orange-Colored Double Arrow symbol close to the search box to view internal connections. You can also view the patch details of every site.

Step 4 Click **Export as png** to export the layout as an image file.

Export Internal connections

Cisco ONP allows you to export internal fiber connections in two ways: either at site-level or network-level.

Follow these steps to export internal fiber connections.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

View details of layout and internal connections, on page 153

Procedure

Step 1 Click the **Ellipsis** icon available in the right side of the internal fiber connection or site.

Step 2 Click **Export**.

View the results of analyzed network

Follow these steps to view the details of optical reports, installation parameters, traffic reports, and cabling reports.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Open the analyzed network for which you want to view the optical results.

Step 2 Click the **Results** tab on the Cisco ONP home page.

By default, the **Optical Report** tab appears. Each row in the tab shows the performance of one optical path. See Optical Report, on page 156.

Step 3 Click the **Installation Parameters** tab.

The Installation Parameters report specifies the values to be provisioned at installation for each site in the network.

To view the installation parameters for Automatic Node Setup (ANS) and Automatic Node Provisioning (ANP), click the respective tabs. See Installation parameters, on page 159

Step 4 Click the **Traffic Report** tab.

You can view the aggregated demand channel data in the form of the traffic reports. See Traffic reports, on page 160.

To view the traffic report for any particular optical path:

a) In the network tree, expand **Circuit** and right-click the required optical path.
b) Click **Open Results**.

The Cisco ONP displays the traffic report for the selected optical path.

Note
By default, **Optical Result** appears under the **Results** tab. Click **Traffic Report** to view traffic reports.

c) Expand the optical path to view the wave information.

Step 5 Click the **Cabling Report** tab. See Cabling report , on page 161

You can view the patch cord connections related to multishelf management. This report is available for the networks starting from NCS 2000 system Release 12.1.0.

Step 6 Click **Export Report** to export the optical reports details in an Excel sheet.

We recommend exporting the optical report only in analyze mode. Exporting reports in upgrade and release upgrade modes may be inaccurate.

Compare installation parameters of two networks

Table 76: Feature History

Feature Name	Release Information	Feature Description
UI Revamp of Optical Reports	Cisco ONP Release 4.1	This feature improves the user experience while comparing the installation parameters and optical reports of two networks.

Use this task to compare the installation parameters of two networks.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Click the **Results** tab on the Cisco ONP home page.

Step 2 Click **Installation Parameters**.

Step 3 Click **Other Networks**.

Step 4 From the list of networks, select the network with which to compare.

FInd a new parameter called **diffBy**.

Step 5 To stop comparing the two networks, click **Clear**.

Compare the optical reports of two networks

Follow these steps to compare the optical reports of two networks.

Before you begin

Log in to the Cisco ONP web interface, on page 6.

Procedure

Step 1 Click the **Results** tab on the Cisco ONP home page.

Step 2 Click **Optical Report**.

Step 3 Click **Other Networks**.

Step 4 From the list of networks, select the network with which to compare.

The optical parameters display two values.

Step 5 To stop comparing the two networks, click **Clear**.

Optical Report

From Release 24.3.1, you can filter the results by any column available in the report for more precise data analysis. For reports represented as colored icons, you can use the first letter of the color (e.g., "g" for green) to filter the results.

Table 77: Optical Report

Optical Parameter	
Name	Displays the ID number of the wave and aggregated waves. ID is automatically generated based on the site name.
Protection	Displays the protection type of the wave.

Optical Parameter	
Protection Type	Displays whether the path type is Protected or Working path for NCS 1001.
SOL	Displays an icon indicating the results summary of the analysis that is run with Start of Life (SOL) fiber loss values: • Green indicates success. • Yellow indicates success with a marginal failure risk. • Orange indicates that the channel has a higher risk of failure. • Red indicates failure.
EOL	Displays an icon indicating the results summary of the analysis that is run with End of Life (EOL) fiber loss values. The indicator shows the optical performance for the path at the end of the fiber life: • Green indicates success. • Yellow indicates success with a marginal failure risk. • Orange indicates that the channel has a higher risk of failure. • Red indicates failure.
SE	Indicates a system-related error that may impact the analysis of the design. If the indicator is red, review the messages that are reported at the end of the analysis or determine which units or sites have a problem.
P/F	Displays the present or forecast services indication.
Source	Displays the name of the source site and side; for example, Site 1-E.
Src Colorless	Displays whether the colorless functionality is enabled on source ports.
Src Contentionless	Displays whether the contentionless functionality is enabled on source ports.
Destination	Displays the name of the destination site and side; for example, Site 1-E.
Dst Colorless	Displays whether the colorless functionality is enabled on destination ports.
Dst Contentionless	Displays whether the contentionless functionality is enabled on destination ports.
Wavelength	Displays the wavelength of the optical channel.
Src Tx Type	Displays the type of DWDM unit or pluggable port module that is used at the source of the specific Optical Channel (OCH) trail. The class of the DWDM unit is also displayed.
Dst Tx type	Displays the type of DWDM unit or pluggable port module that is used at the destination of the specific OCH Trail. The class of the DWDM unit is also displayed.
Span	Displays the total span length (source to destination) for this path in kilometers.
Suggested Regen Locations	Displays the regeneration locations.

Optical Parameter	
BER Target	Displays the bit error rate (BER) target for this channel, based on the capability of the channel's optical interface. It is 1.0E-15 for the interfaces using forward error correction (FEC) and 1.0E-12 for interfaces without FEC.
SOL OSNR	Displays the start of life average Optical Signal to Noise Ratio (OSNR) value at the receiver.
EOL OSNR	Displays the end of life average OSNR value at the receiver.
SOL OSNR margin	Displays the SOL OSNR margin calculation. It is the difference between the OSNR value at certain power of the working point of the receiver client and the working area boundary.
EOL OSNR margin	Displays the EOL OSNR margin calculation, which is the difference between the OSNR value at a certain power of the working point of the receiver client and the working area boundary.
SOL RX	Displays the SOL average power that is received at the destination site in dBm.
EOL RX	Displays the EOL average power that is received at the destination site in dBm.
SOL Power Margin	Displays the SOL power budget margin at the receiver in decibels. It is defined as the offset between the receiver working point and the BER curve with margin. A positive value indicates that there are no power problems.
EOL Power Margin	Displays the EOL power budget margin at the receiver in decibels. It is defined as the offset between the receiver working point and the BER curve with margin. A positive value indicates that there are no power problems.
SOL Overload	Displays the SOL overload margin at the receiver in decibels. A positive value indicates that there are no overload problems.
EOL Overload	Displays the EOL overload margin at the receiver in decibels. A positive value indicates that there are no overload problems.
Residual CD	Displays the chromatic dispersion (CD) margin of the demand.
CD robustness	Displays the robustness to chromatic dispersion of the receiver.
Single-Channel NLE Status	Displays the status of alarms if any nonlinear effect (NLE) is present in the demand.
Multi-Channel NLE Status	Provides the status of the nonlinear effect (NLE) on a particular channel or demand due to other channels or demands.
Min GB	Displays the minimum Guard Band (GB) requirement between channels on the 40G CP-DQPSK MXP and 40G CP-DQPSK ME MXP cards, and other transponders in a mixed any-to-any connectivity.
Filtering Penalty	Displays the value of the penalties that are caused by different filter types (OADM, ROADM, and arrayed waveguide grating (AWG)).
PMD	Displays the calculated total Polarization Mode dispersion (PMD) for each circuit. If the overall PMD for the link overcomes the maximum that is allowed, the PMD value is displayed in a red-colored font. The maximum allowed value depends on the client interface. For these special cases, the network must be manually resolved by contacting a Cisco TAC team.

Optical Parameter	
RX Atten	Displays the attenuation at the input of the receiver.
TX Atten	Displays the attenuation at the output of the receiver.
Encryption	Displays the encryption type of the channel. Possible values are N/A, Yes, No.

Installation parameters

This table outlines the installation parameters for the ANS component.

Table 78: ANS Parameters

Parameter	Description
Name	Displays the name of the site
Side	Displays the line side
Position	Displays the rack number, shelf number, and slot position of the card where the patch cord originates.
Unit	Displays the name of the card.
Port	Displays the port number where the patch cord originates.
Port ID	Displays the port ID.
Port Label	Displays the name of the port.
Parameter	Displays the name of the parameter to be set, such as RX Power Low.
Value	Displays the name of the value to be set for the parameter.
Measurement Unit	Displays the measurement unit for the related installation parameter value, such as dBm.
Manual Set	Indicates with a Yes or No which parameters must be manually set using the Cisco Transport Controller (CTC) interface.

This table outlines the installation parameters for the ANP component.

Table 79: ANP Parameters

Parameter	Description
Name	Displays the name of the site.
Unit ID	Displays the unit (slot number) of the passive units in the shelf.
Shelf ID	Displays the shelf identifier.
Rack Number	Displays the rack number.
Rack Position	Displays the rack position in the shelf.

Parameter	Description
Slot Position	Displays the slot position in the shelf for the card.
Equipment Type	Displays the card type.
Description	Displays the details of the card type.

Traffic reports

This table displays the aggregated data of demand channel in the traffic report for the analyzed network.

Table 80: Traffic Reports

Traffic report	Description
Demand	Categorizes each demand type. Each demand is further categorized into service, trails, and sections.
Section	Displays the sections under every service.
Src Site	Displays the site name for the optical channel source.
Src Position	Displays the rack, shelf ID, and slot identifiers for the source of the optical channel.
Src Card	Displays the unit name for the optical channel source.
Dst Site	Displays the site name for the optical channel destination.
Dst Position	Displays the rack, shelf ID, and slot identifiers for the destination of the optical channel.
Dst Card	Displays the unit name for the optical channel destination.
Client Service Type	Displays the client service type of the demand; for example, OC-48.
Protection Type	Displays the protection type of the demand
Encryption	Displays whether the demand is encrypted with values: NA, Yes, or No.
Wavelength	Displays the wavelength value of the optical channel, and the serial number of the wavelength in the wavelength band.
Max Latency	Displays the latency time for the current circuit. This value includes all the latency components for the circuit, including fiber and DWDM units on the path.

Cabling report

This table shows patch cord connections related to internal patch connections and multishelf management.

Table 81: Cabling

Cabling Report	Description
Name	Displays the name of the site.
Src Unit Type	Displays the source unit.
Src Position	Displays the rack, shelf, and slot position of the card from which the patch cord originates.
Src ID	Displays the source unit ID.
Src Port Label	Displays the name of the port.
Cable Type	Displays the type of cable.
Dst Unit Type	Displays the source unit.
Dst Position	Displays the rack, shelf, and slot position of the card from which the patch cord terminated.
Dst ID	Displays the destination unit ID.
Dst Port Label	Displays the name of the port.
W/P	Indicates whether the connection relates to a present or forecast circuit.

Confidential banner in exported reports

Table 82: Feature History

Feature Name	Release Information	Feature Description
Confidential Banner	Cisco ONP Release 4.1	This feature indicates the confidentiality of the reports or results generated by Cisco ONP for a network. The CONFIDENTIAL banner is placed in all the exported reports. It is placed in the first row and first cell of the Excel sheet, followed by a blank row and the contents of the exported report.

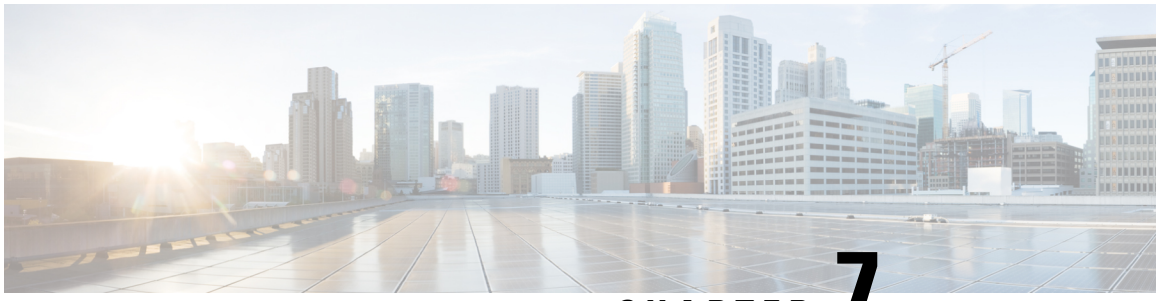
Table 83: Feature History

Feature Name	Release Information	Feature Description
Customizable Confidential Banner	Cisco ONP Release 4.2	The Confidential Banner string can be customized as required. An admin user can modify the banner string when the *confidentialBanner.enabled* field is set to true in the *feature.properties* file.

The "CONFIDENTIAL" banner appears in all exported reports. In Excel files (.xlsx), it is located in the first cell of the first row, followed by a blank row, and then the report contents. If the .xlsx file contains multiple sheets, the banner is included on each sheet.

The "CONFIDENTIAL" banner is updated only when reports are exported in .xlsx format.

Server administrators can customize the "CONFIDENTIAL" banner text by modifying the `confidentialBanner.content` field. To enable banner customization, the `confidentialBanner.enabled` field must be set to `true` in the `feature.properties` file. By default, this field is set to `false`.



CHAPTER 7

Backup and Restore Cisco ONP Database

Backup Database

The database backup configuration on the server, set by the system administrators, allows backups of the entire database to be taken daily, weekly, or monthly. Only system administrators have access to the backup folders and can perform restorations. Backup archives are stored on a highly durable NFS share. The available backup archives include:

- Daily archives for the last 7 days
- Weekly archives for the last 4 weeks
- Monthly archives for the last 6 months

Note You can change the duration for monthly archives.

Setup Backup

Before you begin

- Ensure that a highly durable 2 TB NFS storage is available to store database archives.
- Ensure that the storage is accessible from the Cisco ONP environment.
- Set up rules as defined by the Cisco ONP network and configure the appropriate Access Control List (ACL) to permit or deny access to the storage as needed.

Procedure

Step 1 Log into the Cisco ONP server, where you have installed Cisco ONP by using the tar archive.

Step 2 Create a folder for backup. Ideally it should be mounted on a reliable object storage such as NFS.

Step 3 Copy `restore_mongo.sh` from `/ONP/images/`.

Perform manual backup

Follow these steps to back up the Cisco ONP database.

Procedure

Step 1 Browse to the location where the backup_mongo.sh script is stored.

Step 2 Use the `bash backup_mongo.sh` command to execute the script.

Example:

```
user@server:~/cnp_backups$ bash backup_mongo.sh
```

The backup file is stored in the daily backup folder (backup.daily) with the current time stamp.

Schedule a backup

You can schedule a backup in either of these two ways:

- Schedule a backup using script, on page 164
- Schedule a backup, on page 165

Schedule a backup using script

Follow these steps to schedule the backup operation using a script.

Procedure

Step 1 Log in to the Cisco ONP server.

Step 2 Use the command `bash rotation.sh` to execute the rotation.sh script.

Example:

```
user@server:~/cnp_backups$ bash rotation.sh
```

This command creates the necessary folder structure.

Step 3 Use the command `bash backup_postgres.sh` to execute the backup_postgres.sh script.

Example:

```
user@server:~/cnp_backups$ backup_postgres.sh
```

The backup file is stored in the daily backup folder (backup.daily) with the current time stamp.

Step 4 Enter the path at the user prompt to store the file.

Backup files are stored in your required file path as shown in this example.

Example:

```
/user-defined path/backups/backup.daily
```

Schedule a backup

Follow these steps to schedule the backup operation using Crontab.

Procedure

Step 1 Log in to the Cisco ONP server.

Step 2 Use the command `sudo crontab -e` to configure the Crontab job.

```
user@server~/cnp_backups$ sudo crontab -e
```

Step 3 Update the `Crontab.sh`script with the required cron job entries using the Syntax to schedule the backup using Crontab, on page 167, to schedule backup operations.

Example:

This example shows the scheduling of the backup operation at 3:00 a.m daily.

```
0 3 * * * /home/ciscocnp/cnp_backups/backup_mongo.sh
```

Syntax to schedule the backup using Crontab

Use this syntax to schedule a backup in Crontab:

```
m h dom mon dow
```

Where:

- m: Minutes (0–59)
- h: Hours (1–23)
- dom: Day of the month (1–31)
- mon: Month of the year (1–12)
- dow: Day of the week (0–6, where 0 represents Sunday)

To specify the time, you can provide exact values for the minute (m), hour (h), day of the month (dom), month (mon), and day of the week (dow). Alternatively, you can use the wildcard character `*` in these fields to indicate "any value."

Note The backup jobs are initiated according to the system daemon's understanding of time and time zones as defined by the cron scheduler.

Restore the database manually

Follow these steps to restore the database manually.

Procedure

Step 1 Check the Cisco ONP Database.

Example:

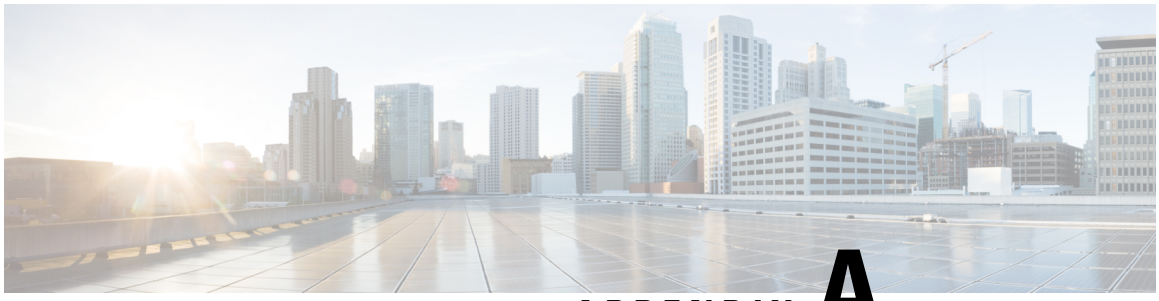
```
$ mongo CnpDB

MongoDB shell version: 2.6.10
 connecting to: CnpDB
 Server has startup warnings:
 2019-01-31T12:17:39.354+0000 I STORAGE [initandlisten]
 2019-01-31T12:17:39.354+0000 I STORAGE [initandlisten] ** WARNING: Using the XFS filesystem is
strongly recommended with the WiredTiger storage engine.
 2019-01-31T12:17:39.354+0000 I STORAGE [initandlisten] ** See
http://dochub.mongodb.org/core/prodnotes-filesystem
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten]
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten] ** WARNING: Access control is not enabled
for the database.
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten] ** Read and write access to data and
configuration is unrestricted.
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten]
 > show collections
 NetworkEntity
 SystemLog
 BOM
 fs.files
 Users
 fs.chunks
 ErrorInfo
 NetworkObject
 UserGroups
 TaskInfo
 ActionGroups
 Roles
 >
 ```
```

**Step 2** Remove the Cisco ONP back-end and front-end Docker services,"docker service rm cnp_cnp cnp_cnp_frontend" and check again:

**Example:**

```
```

$ mongo CnpDB

 MongoDB shell version: 2.6.10
 connecting to: CnpDB
 Server has startup warnings:
 2019-01-31T12:17:39.354+0000 I STORAGE [initandlisten]
 2019-01-31T12:17:39.354+0000 I STORAGE [initandlisten] ** WARNING: Using the XFS file system is
strongly recommended with the WiredTiger storage engine.
 2019-01-31T12:17:39.354+0000 I STORAGE [initandlisten] ** See
http://dochub.mongodb.org/core/prodnotes-filesystem
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten]
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten] ** WARNING: Access control is not enabled
for the database.
```

```
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten] ** Read and write access to data and
configuration is unrestricted.
 2019-01-31T12:17:40.013+0000 I CONTROL [initandlisten]
 > show collections
 >
 ```
```

**Step 3** Copy the database to the folder that is mapped to MongoDB container's volume:

**Example:**

```
 $ sudo cp backups/2019-02-01-04-29.archive /var/lib/mongodb_cnp/
```

Step 4 Restore the database and check.

Example:

```
 $ docker exec -t cnp_mongo.1.$(docker service ps -f 'name=cnp_mongo.1' -f 'desired-state=running'
cnp_mongo -q) bash -c "mongorestore -u \$(cat \$MONGO_INITDB_ROOT_USERNAME_FILE) -p \$(cat
\$MONGO_INITDB_ROOT_PASSWORD_FILE) --authenticationDatabase admin --port 27017 -h localhost --db
CnpDB --gzip --archive=/data/db/2019-02-01-04-29.archive"
```

Restore database using script

You can restore the database using a script, which is available at this location:

`Images/DB_backup/restore_mongo.sh`

Follow these steps to restore the database using a script:

Procedure

Use the command `sudo bash restore_mongo.sh` to restore the database

Example:

```
 $ sudo bash restore_mongo.sh DB backup archive file path.
$ sudo bash restore_mongo.sh /backups/backup.daily/2019-05-05-23-58.archive
```

The database backup is created, and a confirmation prompt appears that asks whether to delete the database. `(y/n)`.

Enter `y` to delete the database.

Enter `n` to not delete the database.

Enter `No` to not delete the database and apply only missing data(s) from backup file.

Syntax to schedule the backup using Crontab

Use this syntax to schedule a backup in Crontab:

```
m h dom mon dow
```

Where:
```

- m: Minutes (0-59)
- h: Hours (1-23)
- dom: Day of the month (1-31)
- mon: Month of the year (1-12)
- dow: Day of the week (0-6, where 0 represents Sunday)

To specify the time, you can provide exact values for the minute (m), hour (h), day of the month (dom), month (mon), and day of the week (dow); alternatively, you can use the wildcard character * in these fields to indicate "any value."

Note The backup jobs are initiated according to the system daemon's understanding of time and time zones as defined by the cron scheduler.



APPENDIX A

Cisco ONP UI Reference

This appendix chapter describes the various options available in the Cisco ONP UI.

Menu bar

This table lists all options available in your Cisco ONP GUI menu bar.

Table 84: Menu options and descriptions

Options	Description
File	Performs common file operations such as New, Open, Open Shared, Save, Save As, Share, and Delete
Network	Opens Entity Editor, analyzes the network, and converts non-SSON to SSON networks
Export	Exports reports of CPZ, sites, fibers, SRLGs, services, waves, media channels, optical results, service aggregation, BOM, and messages. Export allows you to download Excel and LNI templates
Import	Imports CPZ, Excel, LNI, and MPZ to design a network in Cisco ONP
Manage	Manages Layout Templates and Optical Sources
Logs	Displays log events initiated during a specific period, such as user login, user logout, password change, and LNI - start, failed, and completed
Job Monitor	Monitors background tasks
Control Panel	Manages users, user groups, user roles, permissions, system configuration, and dictionary
Help	Displays the Cisco ONP version
Last Login	Shows the last date and time you logged in to Cisco ONP including the last login IP details
Username	Displays the name of the user who has currently logged in to Cisco ONP

File

The **File** menu includes common file options such as New, Open, and Delete.

Options	Description
New	Creates a new network. You can check the **SSON Network** check box and select **System Release** for NCS 2K to create an SSON network.
Open	Opens a saved network. The network name in blue-colored font indicates that the network is in the Design mode, and the network name in green-colored font indicates that the network is in the Analyze mode. **Note** If you view a blank screen when you open a network, refresh the browser, or log in to Cisco ONP again.
Open Shared	Opens a shared network.
Save	Saves a network.
Save As	Saves the network with a new name.
Share	Shares a network or networks.
Delete	Deletes a network or networks.

Network

The **Network** menu includes options such as Entity Editor, Analyze, and SSON Convert in the design mode. It includes options such as Entity Editor, Design, Upgrade, and Enter Plan Mode in the Analyze mode.

Options	Description
Entity Editor	Use this option to edit various properties of an element in the network
Analyze	Analyzes the network after completing the design
SSON Convert	Converts a Non-SSON network to an SSON network
Design	Switches from Analyze mode to Design, Upgrade, or Release Upgrade mode
Upgrade	Upgrades an existing network that is in the Analyze mode
Release Upgrade	Upgrades the NCS 2K System Release of a network
Enter Plan Mode	Switches to the Plan mode
Exit Plan Mode	Exits the plan mode
Restore	Restores failed fibers and nodes

Export

The **Export** menu includes options to export reports of Sites, Fibers, Services, SRLG, Waves, Messages, and BOM.

Options	Description
CPZ	Export the .cpz design file of a network into your local system.
Sites	Exports site details such as x and y coordinates, grooming site flag, CLLI code, site address, site type, and site name.
Fibers	Exports fiber details such as length, loss to fiber, source and destination site, source and destination edge.
Services	Exports service details such as name, type, path, quantity, and protection.
SRLGs	Exports details about created SRLGs.
Waves (Available for non-SSON network)	Exports wave details such as Label, Source and Destination sites, Card Type, Wavelength, Utilization, Source port, Destination port, Demands, OTN Hops, OSNR, OSNRMarginEOL, StatusEOL, Excluded Channels, and Path of Wave.
Media Channels (Available for SSON network)	Exports media channel details such as Media Channel Label, Media Carrier Label, Source and Destination sites, Card Type, Wavelength, Utilization, Source port, Destination port, Demands, OTN Hops, OSNR, OSNRMarginEOL, StatusEOL, Excluded Channels, and Path of Media channel.
Messages	Shows the complete log of the analysis, including critical errors.
Excel Template	Download sample Excel file that can be used as a reference for creating networks using the Import Excel feature.
LNI Template	Download sample LNI file that can be used as a reference for creating networks using the Import feature.
BOM	Exports details about pricing and quantity of the network equipment
Failure Groups	This option is available only in the plan mode. You can add failed fibers to a failure group.
Failure Report	This option is available only in the plan mode. It shows the failed fibers, total channels, failed channels, restored channels, and fiber hotzones.
Optical Results	Exports details such as protection type, SOL, EOL, source, and destination

Import

The Import menu imports an Excel file, a CPZ file, or an MPZ file.

Options	Description
CPZ	Imports the .cpz network design files that are exported from another Cisco ONP instance

Options	Description
Excel	Imports an Excel file containing all the design parameters
Live	Imports a live deployed network by retrieving configurations of the nodes, provided in the LNI input Excel sheet
MPZ	Imports the .mpz network design files from CTP to Cisco ONP, to avoid recreating the networks that are already created in CTP

Manage

You can manage layout templates and optical sources.

Options	Description
Layout Templates	Imports reusable templates to design layout configurations for a network
Optical Sources	Imports an optical source from your local system

Logs

The System Logs option allows an admin user, or user with USER MANAGEMENT, and NETWORK MANAGEMENT permissions to view at logs the events that are initiated during a specific time interval. Examples of events are user login, user logout, password change, Live Network Import (LNI)-start, failed, completed and analysis-start, and failed.

The **SYSTEM LOGS** page includes the following fields:

Field	Description
Time Stamp	Provides the date and time of the specific event
Event Type	Shows the type of event, which includes user login, user logout, password change, and so on
Description	Describes the event, which includes user login success, user logout success, and so on
Username	Shows the user who has initiated specific events
Event Source	Shows the IP address of the device from where the event is initiated

Events that are captured in the System Logs are:

Event	Description
SIGNUP	New user sign-up for Cisco ONP
LOGIN	User log in to Cisco ONP
USER STATE CHANGE	User state change from Active to Inactive and the converse

Event	Description
USER ROLE CHANGE	User role change, such as admin to planner, and so on
LOGOUT	User log out from Cisco ONP
USER DELETION	Deletion of a particular user
UNAUTHORIZED	User enters invalid login credentials
LNI_START	Successful initiation of Live Network Import
LNI_COMPLETE	Successful completion of live import of a network
LNI_CANCEL	Cancellation of Live Network Import
LNI_PURGE	Imported Live network data is successfully purged
ANALYZE_LNI_START	Analysis of LNI network started successfully
ANALYZE_LNI_END	Analysis of LNI network completed successfully
LNI_POPULATE_DESIGN_DATA	Populating of L0 DesignData initiated
ANALYZE START	Starting of the network analysis
ANALYZE END	Completion of the network analysis
ANALYZE CANCEL	Cancellation of the network analysis
UPGRADE NETWORK	Entering the Upgrade mode
PLAN_INIT	Entering the Plan mode
PLAN_END	Exiting the Plan mode
PLAN_REROUTE	Checking for alternate paths to restore failed media channels or waves
PLAN_PROGRESS	Restoration of failed media channels or waves in progress
RELEASE_UPGRADE_NETWORK	Upgrading the system release of the network is in progress.

Job Monitor

The **Job Monitor** menu checks and manages tasks running in the background.

You can access this menu if you have ADMIN, NETWORK_MANAGEMENT, or NETWORK_PLANNING role.

The **JOB MONITOR** page has the following options:

Options	Description
Refresh	Refreshes the display information.

Options	Description
Filter	Applies one or more of the following filter options: Task Type: Filters the display information based on the task type. Select Start Date: Filters the display information based on the start date of the task. Select End Date: Filters the display information based on the end date of the task. Username: Filters the display information based on the username.
Created Date	The date on which the task is started by the user.
Network Name	Name of the network on which the task is running.
Task Type	The type of background task: Valid values are ANALYZE and EPNM_IMPORT.
Messages	The current state of the task.
Cancel	Enables you to cancel or stop an ongoing background task: • The Admin can cancel any of the running background tasks. Other valid users can cancel only their own tasks. • If you want to cancel your ongoing network analysis, you can open Cisco ONP at the browser in incognito mode, or contact the Admin. • After a task is cancelled, it gets removed from the job monitor. You can check the status of a cancelled task from **System logs** page. Click **Logs** to open the **System logs** page.
Check Progress	Enables you to view the status of the LNI operation.

Control Panel

Apart from designing, analyzing, and creating BOM for a network, a user with admin rights can activate, manage, and delete users and their roles.

To navigate to the control panel page, click **Control Panel**.

The admin or any user with USER_MANAGEMENT role can lock, unlock an individual user account, and manually expire the individual user password. For more information, see Manage Users and Roles, on page 11.

Preferences

This menu contains the General Settings option to customize Cisco ONP settings such as the default map view and spectrum utilization percentage.

Field	Description
General Settings	Allows choosing the default map view and applying color codes for spectrum usage percentage • **Default Map**: Choose the **Detailed** or **Minimal** map from the drop-down list. • **Spectrum Utilization Percentage**: Click and drag to change the color code to indicate spectrum usage.

Help

This menu provides information about the Cisco ONP version.

Field	Description
About	Provides the Cisco ONP version.

Network Tree

The left pane of the Cisco ONP home page comprises a network tree. The network tree includes various network elements. When you click each element, the respective property is displayed under the network tree. You can edit the properties. For more information on editing the network properties, see Modify Network Properties, on page 69.

Table 85: Network Tree Elements

Network Tree Elements	Description
Network name	Displays the name of the network.
Sites	Customer premise equipment that is located in a rack within a building.
Fiber	Optical fiber connecting two sites.
Fiber Couple	A fiber couple consists of two different fibers (clockwise and counterclockwise), one for transmission and another for reception.
Services	Service is the circuit through which traffic flows between nodes. When you add services to the Traffic site (of the type 1K-2K-4K) in an SSON network, a DefaultGroup is created under the Services in the network tree. You can also create a new service group.

Network Tree Elements	Description
Waves or Medial Channel	The wave or Media channel represents a DWDM channel. In a wave hierarchy, for each wave, there is a trail. When you expand a trail, there is a section under each trail. The trail is an optical path or a network section joining two traffic nodes. It can have more than one section depending on whether the trail has a regenerator site. For more information on regeneration, see Regeneration support, on page 137.
SRLG	Shared Risk Link Group (SRLG) is useful for routing the protected services. If there are Fiber 1 and Fiber 2 in the network, they are assumed to be diverse and are used as alternates for protection purposes. If Fiber 1 and Fiber 2 are in an SRLG, they are not true alternates, and they share the same risk of failure. Therefore, if Fiber1 fails, Fiber 2 also fails, and Fiber 2 cannot be used as a protected path.
Optical subnet	An optical subnet is a collection of spans with certain associated properties. When you create a new network, Cisco ONP automatically creates an optical subnet that is associated to the network. At least one optical subnet must exist for each network.
Stage button	Visible only in the Analyze mode.

Use the Search box on top of the network tree to search for any specific site, fiber, or wave in the network tree panel. Click the Refresh icon to refresh your search.

Design Palette

Table 86: Feature History

Feature Name	Release Information	Feature Description
Intuitive Map Display	Cisco ONP Release 5.2	The new intuitive map display allows you to virtually rearrange networks for a clutter-free view without impacting the original design. This display simplifies adding new nodes to complex networks. Save the last modified network in the new view to retain the latest rearrangement. The new icons in the Design Palette that enable the intuitive display are: • **Switch to Intuitive Arrangement**/**Switch to Coordinates Arrangement**—Toggles the map between the intuitive and original displays. • **Rearrange nodes**—Overrides node coordinates and rearranges the map in a presentable manner.

At the right of the Cisco ONP home page, there is the design palette. You can use this design palette to create a network design. It consists of the following six icons:

Icons	Description
Zoom In	Click this icon to magnify the map.
Zoom Out	Click this icon to minimize the map.
Reset Zoom	Click this icon to reset the map to its original size.
Drawing Tool	The Drawing Tool consists of the following icons: • **Traffic Site**: Select this icon, and click the working area to create traffic sites in the network. • **ROADM Site**: Select this icon, and click the working area to create ROADM sites. • **OLA Site**: Select this icon, and click the working area to create OLA sites. • **Passthrough Site**: Select this icon, and click the working area to create passthrough sites. • **Link**: Click this icon, and drag and drop between sites to create a fiber link. • **OTN Service**: Click this icon to create OTN service between sites. • **DWDM channel**: Click this icon to add a wave or medial channel between sites. • **Select**: The **Select** icon looks similar to the cursor tool. Click this icon to select a node, link service, and so on.
Layers Window	Use this icon to view or hide layers such as fiber link, service, text, and channel. The following are the four toggle icons: • **Toggle Fiber**: Click this icon to view or hide fiber link details from the network. • **Toggle Service**: Click this icon to view or hide service details from the network. • **Toggle Wave**: Click this icon to view or hide the channel or wave details from the network. • **Toggle Text**: Click this icon to view or hide the text from the network. • **Toggle SVO associations**: Click this icon to remove or add SVO associations. • **Expand/Collapse All Demands**: Click this icon to expand the waves or media channels so that you can view them clearly. Click this icon again to collapse the waves and media channels to their original shape and position. The eye symbol in the icon indicates that you are currently viewing the respective details.

Icons	Description
Zoom Tool	The icon below the **Drawing Tool** is the **Zoom Tool**. You can change the display of the working area by using this function. Click the arrow to view two sliders. • **Map Fade**: Move the **Map Fade** slider from right to left to fade the map from the background. • **Zoom In/Out**: To magnify the map, move the Zoom in or out slider from left to right.
Zoom Elements	Click the **Zoom Elements** icon to view four sliders. • **Media Channel Width**: Move this slider from left to right to increase the channel width. • **Path Spread**: Move this slider from left to right to increase the space between the paths. • **Fiber Width**: Move this slider from left to right to increase the fiber width. • **Service Width**: Move this slider from left to right to increase the service width.
Show Failed (available only in plan mode)	This icon shows the failed media channels in the map. Failed ones are marked with a red cross mark.
Traffic Monitor (available only in plan mode)	This icon shows the total number of impacted media channels, demands, or services that are working or failed in the entire network.

Entity Editor

The **Entity Editor** allows you to edit various properties of an element in the network. Choose **Network** > **Entity Editor** to open the **Entity Editor** window.

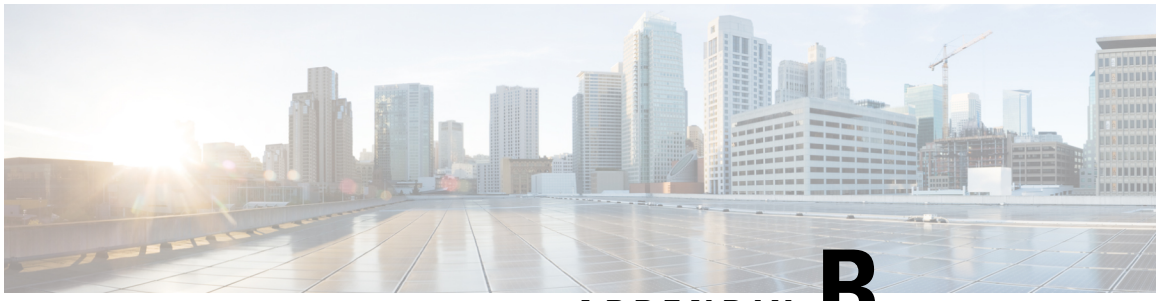
The **Entity Editor** enhances some properties with descriptions in the form of tooltips.

The table lists the operations that you can perform in the **Entity Editor** window.

Options	Description
Left pane filter	Includes check boxes to filter the network elements displayed under each tab: • For the **SITE** tab, you can choose whether to display OTN (only traffic node), DWDM (ROADM, OLA, or pass-through) node, or both. • For the **FIBER** tab, you can choose the fiber connecting a particular source and destination sites. • For the **SERVICE** tab, you can choose to display either services, waves, or both.

Options	Description
Right pane properties	Displays all properties of the selected network element. You can modify the properties as required.
Search	Searches for a particular network element.
Refresh	Refreshes the list of network elements displayed under each tab.
Expand/Collapse	Expands or collapses the network elements available in the network tree under each tab.
Select Similar	Selects similar network elements available in the network tree. For example, select a ROADM site, and click the **Select Similar** icon. All ROADM sites are selected. You can change a property in all the selected sites at the same time. This option allows you to identify and compare the property difference. For example, if a property is different among the selected sites, that property is dimmed. You can select an option that is applied to all the selections.
Un-Select All	Deselects all selections that you make under the network tree.
Delete	Deletes the selected network elements.
Add Contentionless Sides (available only under the **Site** tab)	Adds contentionless sides to NCS 2000 networks. Contentionless functionality on a site refers to the contentionless add/drop ability of an N-degree ROADM node to accommodate N wavelengths of the same frequency from a single add/drop device. For a ROADM to be contentionless, the number of drop units have to be equal to ROADM degrees. • Click the ROADM site to add contentionless sides. • Click the **Add Contentionless Side** icon. • Enter an appropriate value in the **Enter number of contentionless sides** field. • Click **OK**. After adding the contentionless side, you can edit the contentionless port property of the side at the right pane. You can select any of the values ranging from 1 to16. The default value is 16.
Copy (available only under the **Service** tab)	Clones a service or wave that is connected between two sites. To clone a service, • Select a wave and click **Copy**. • Enter the quantity in the **Clone Service/DWDM Channel** dialog box, and click **OK**. –1 is added at the end of the label of the cloned wave. An example label of a cloned wave is Site-2-Site3-1-1. The original wave is Site-2-Site3-1. You can rename the label. You can also clone a service in a similar way.

Cisco ONP UI Reference



APPENDIX B

Supported Cards and Pluggables

Supported Transponder Cards and Pluggables

Table 87: Feature History

Feature Name	Release Information	Feature Description
Pluggable Support	Cisco ONP Release 4.1	QSFP-100G-FR-S= pluggable is supported on the QSFP ports of the 400G-XP LC transponder card with 100GE data rate.

Cisco ONP supports the following transponders and pluggables:

Table 88: Supported Transponder Cards and Pluggables for NCS 2000 Network

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
200G-CK-LC + MR-MXP (200G MXP mode)	• 100GE • OTU4	SD-FEC_20	• SR-1(CPAK-100G-SR10) • SR-1(CPAK-100G-SR4) • LR-1(CPAK-100G-LR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	Yes (only for 100GE)	No	Auto, TRK_200G
200G-CK-LC + MR-MXP (100G TXP mode)	100GE	SD-FEC_20	• SR-1(CPAK-100G-SR10) • SR-1(CPAK-100G-SR4 • LR-1(CPAK-100G-LR4)	Yes	Yes	Auto, TRK_100G

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
200G-CK-LC + MR-MXP (100G TXP mode)	100GE	SD-EFEC	• SR-1(CPAK-100G-SR10) • SR-1(CPAK-100G-SR4 • LR-1(CPAK-100G-LR4)	Yes	Yes	Auto, TRK_100G
200G-CK-LC + MR-MXP (100G TXP mode)	100GE	SD-FEC	• SR-1(CPAK-100G-SR10) • SR-1(CPAK-100G-SR4 • LR-1(CPAK-100G-LR4)	Yes	Yes	Auto, TRK_100G
200G-CK-LC + MR-MXP (100G MXP mode)	• 10GE • 10GE LAN PHY • OC192 • OTU2	SD-FEC_20	• LR-1(ONS-QSFP-4*10G-MLR) • LR-1(QSFP-4*10G-MLR) • SR-1(QSFP-40G-SR4) • SR-1(ONS-SC+10G-SR) • LR-1(ONS-SC+10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x)	Yes	Yes	Auto, TRK_100G
200G-CK-LC + MR-MXP (100G MXP mode)	• 10GE • 10GE LAN PHY • OC192 • OTU2	SD-EFEC	• LR-1(ONS-QSFP-4*10G-MLR) • LR-1(QSFP-4*10G-MLR) • SR-1(QSFP-40G-SR4) • SR-1(ONS-SC+10G-SR) • LR-1(ONS-SC+10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x)	Yes	Yes	Auto, TRK_100G
200G-CK-LC + MR-MXP (100G MXP mode)	• 10GE LAN PHY • 10GE • OC192 • OTU2	SD-FEC	• LR-1(ONS-QSFP-4*10G-MLR) • LR-1(QSFP-4*10G-MLR) • SR-1(QSFP-40G-SR4) • SR-1(ONS-SC+10G-SR) • LR-1(ONS-SC+10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x)	Yes	Yes	Auto, TRK_100G

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
200G-CK-LC + MR-MXP (100G MXP mode 2*10G 2*40G MODE)	• 10GE • 10GE LAN PHY • 40GE	SD-FEC_20	• SR-1(ONS-SC+10G-SR) • LR-1(ONS-SC+10G-LR) • DWDM(ONS-SC+-10G-C) • LR-1(QSFP-40G-LR4) • DWDM(ONS-SC+-10GEPxx.x) • SR-1(QSFP-40G-SR4) • SR-1(QSFP-40G-SR-BD)	Yes	Yes	Auto, TRK_100G
200G - CK-LC + MR - MXP (100G MXP mode 2*10G 2*40G MODE)	• 10GE • 40GE	SD-EFEC	• SR-1(ONS-SC+10G-SR) • LR-1(ONS-SC+10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • SR-1(QSFP-40G-SR4) • LR-1(QSFP-40G-LR4) • SR-1(QSFP-40G-SR-BD)	Yes	Yes	Auto, TRK_100G
200G - CK-LC + MR -MXP (100G MXP mode 2*10G 2*40G MODE)	• 10GE • 40GE	SD-FEC	• SR-1(ONS-SC+10G-SR) • LR-1(ONS-SC+10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • SR-1(QSFP-40G-SR4) • LR-1(QSFP-40G-LR4) • SR-1(QSFP-40G-SR-BD)	Yes	Yes	Auto, TRK_100G
200G - CK-LC +10x10G -LC	• 10GE • OC192 • OTU2 • OTU2e	SD-FEC_20	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR (ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	Yes for OTU2e	No	Auto, TRK_100G

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
200G - CK-LC +10x10G -LC	• 10GE • OC192 • OTU2 • OTU2e	SD-EFEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER (ONS-SC+-10G-ER) • ZR (ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	Yes for OTU2e	No	Auto, TRK_100G
200G-CK-LC + 10x10G -LC	• 10GE • OC192 • OTU2 • OTU2e	SD-FEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	Yes for OTU2e	No	Auto, TRK_100G
200G - CK-LC + MR-MXP (200G Mxp 100G+10*10G Mode)	• 100GE • 10GE • OC192 • OTU2	SD-FEC_20	• SR-1(CPAK-100G-SR10) • SR-1(CPAK-100G-SR4) • LR-1(CPAK-100G-LR4) • SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	Yes for 100GE and OTU2	No	Auto, TRK_200G

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
200G-CK-LC + MR-MXP + MR-MXP (200G Mxp 4*40G + 4*10G Mode)	• 10GE • 10GE LAN PHY • 40GE	SD-FEC_20	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • SR-1(QSFP-40G-SR4) • LR-1(QSFP-40G-LR4) • SR-1(QSFP-40G-SR-BD)	Yes	Yes	Auto, TRK_200G
200G-CK-LC + 10x10G -LC + MR-MXP	• 10GE • OC192 • OTU2	SD-FEC_20	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x) • LR-1(ONS-QSFP-4*10G-MLR) • ZR(ONS-SC+-10G-ZR)	Yes	Yes	Auto, TRK_200G
200G-CK-LC + MR-MXP + MR-MXP	• 10GE • OC192 • OTU2	SD-FEC_20	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x) • LR-1(ONS-QSFP-4*10G-MLR) • ZR(ONS-SC+-10G-ZR)	Yes	Yes	Auto, TRK_200G

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
100GS - CK-LC + 10x10G-LC	• 10GE • OC192	EFEC, SD-FEC_20	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto, TRK_100G
100G - LC-C + 10x10G-LC	• 10GE • OC192 • Fiber Channel 10G • Fiber Channel 8G • OTU2 • OTU2e	FEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto
100G - LC-C + 10x10G-LC	• 10GE • OC192 • Fiber Channel 10G • Fiber Channel 8G • OTU2 • OTU2e	EFEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER (ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
100G - LC-C + 10x10G-LC	• 10GE • OC192 • Fiber Channel 10G • Fiber Channel 8G • OTU2 • OTU2e	HG-FEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER (ONS-SC+-10G-ER) • ZR (ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto
100G - CK-LC-C + 10x10G-LC	• 10GE • 10GE LAN PHY • OC192 • Fiber Channel 10G • Fiber Channel 8G • OTU2 • OTU2e	FEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
100G -CK-LC-C + 10x10G-LC	• 10GE • 10GE LAN PHY • OC192 • Fiber Channel 10G • Fiber Channel 8G • OTU2 • OTU2e	EFEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto
100G - CK-LC-C + 10x10G-LC	• 10GE • 10GE LAN PHY • OC192 • Fiber Channel 10G • Fiber Channel 8G • OTU2 • OTU2e	HG-FEC	• SR-1(ONS-SC+-10G-SR) • LR-1(ONS-SC+-10G-LR) • DWDM(ONS-SC+-10G-C) • DWDM(ONS-SC+-10GEPxx.x) • ER(ONS-SC+-10G-ER) • ZR(ONS-SC+-10G-ZR) • DWDM(ONS-SC+-10G-xx.x)	No	No	Auto

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
400G-XP-LC	• 100GE • 10GE LAN PHY • 10GE • 40GE • Fiber Channel 10G • Fiber Channel 16G • Fiber Channel 8G • OC192 /STM64 • OTU2 • OTU2e • OTU4	SD-FEC_25-NO_DE	• SR-1(QSFP-100G-SR4-S) • LR-1(QSFP-100G-LR4-S) • LR-1(QSFP-28-LR4) • SR-1(QSFP-100G-SM-SR) • SR-1(QSFP-40/100G-SRBD) • LR-1(ONS-QSFP-4*10G-MLR) • LR-1(QSFP-4*10G-LR) • SR-1(QSFP-40G-SR4) • ER(ONS-QSFP-4*10G-MER) • LR-1(QSFP-40G-LR4) SR-1(QSFP-40G-SR-BD • LR-1(ONS-QC16GFC-LW) • LR-1(ONS-QC16GFC-SW) • LR-1(ONS-QSFP28-LR4) • FR-1 (QSFP-100G-FR-S) (only for 100GE)	Yes	Yes	TRK_100G, TRK_200G

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
400G-XP-LC	• 100GE • 10GE LAN PHY • 10GE • 40GE • Fiber Channel 10G • Fiber Channel 16G • Fiber Channel 8G • OC192 /STM64 • OTU2 • OTU2e • OTU4	SD-FEC_15 -NO_DE	• SR-1(QSFP-100G-SR4-S) • LR-1(QSFP-100G-LR4-S) • LR-1(QSFP-28-LR4) • SR-1(QSFP-100G-SM-SR) • SR-1 (QSFP-40/100G-SRBD) • LR-1(ONS-QSFP-4*10G-MLR) • LR-1(QSFP-4*10G-LR) • SR-1(QSFP-40G-SR4) • ER(ONS-QSFP-4*10G-MER) • LR-1(QSFP-40G-LR4) • SR-1(QSFP-40G-SR-BD • LR-1(ONS-QC16GFC-LW) • LR-1(ONS-QC16GFC-SW) • LR-1(ONS-QSFP28-LR4) • FR-1 (QSFP-100G-FR-S) (only for 100GE)	Yes	Yes	TRK_100G, TRK_200G
100G-LC-C	• 100GE • OTU4	FEC	SR-1(CPAK-100G-SR10)	No	No	Auto
100G-LC-C	• 100GE • OTU4	EFEC	SR-1(CPAK-100G-SR10)	No	No	Auto
100G-LC-C	• 100GE • OTU4	HGFEC	SR-1(CPAK-100G-SR10)	No	No	Auto
100G - CK-LC-C	• 100GE • 40GE • OTU4	FEC	• SR-1(CPAK-100G-SR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	No	No	Auto

Transponder/ Muxponder	Traffic Type	FEC mode	Pluggables Supported	Encryption SSON	Encryption Non-SSON	Trunk Mode
100G - CK-LC-C	• 100GE • 40GE • OTU4	EFEC	• SR-1(CPAK-100G-SR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	No	No	Auto
100G - CK-LC-C	• 100GE • 40GE • OTU4	HGFEC	• SR-1(CPAK-100G-SR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	No	No	Auto
100GS - CK-LC	100GE	FEC	SR-1(CPAK-100G-SR10)	Yes	No	Auto, TRK_100G
100GS - CK-LC	100GE	EFEC	LR-1(CPAK-100G-LR4)	YEs	No	Auto, TRK_100G
100GS - CK-LC	100GE	SD-FEC_20	SR-1(CPAK-100G-SR10)	Yes	No	Auto, TRK_100G
200G - CK-LC (100G Mode only)	• 100GE • OTU4	FEC	• SR-1(CPAK-100G-SR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	Yes (for 100GE)	No	Auto, TRK_100G
200G - CK-LC (100G Mode only)	• 100GE • OTU4	EFEC	• SR-1(CPAK-100G-SR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	Yes (for 100GE)	No	Auto, TRK_100G
200G-CK-LC (100G Mode only)	• 100GE • OTU4	SD-FEC_20	• SR-1(CPAK-100G-SR4) • SR-1(CPAK-100G-SR10) • LR-1(CPAK-100G-LR4)	Yes (for 100GE)	No	Auto, TRK_100G

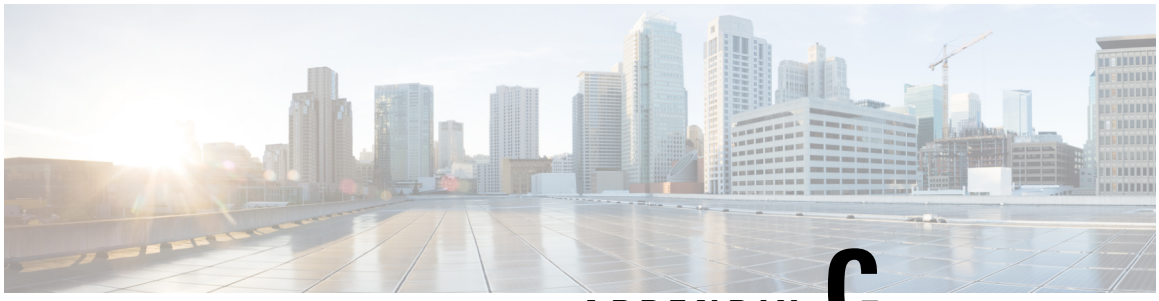
Cisco ONP supports the following transponders and pluggables:

Table 89: Supported Transponder Cards and Pluggables for NCS 1010 Network

Transponder / Muxponder	Traffic Type	FEC mode	Pluggables Supported		Encryption	Trunk Mode
			Client Pluggables	Trunk Pluggables		
NCS1K14-2.4T-K9	100GE 400GE	SD_FEC_15	• Auto • QDD-400G-FR4-S • QDD-400-AOC1M • QDD-400G-DR4-S • QDD-4x100G-LR-S	• Auto • CIM8-C-K9	No	• Auto • 400G • 500G • 600G • 700G • 800G • 900G • 1000G • 1100G • 1200G
NCS1K14-2.4T-X-K9	100GE 400GE	SD_FEC_15	• Auto • QDD-400G-FR4-S • QDD-400-AOC1M • QDD-400G-DR4-S • QDD-400G-LR4-S • QDD-4x100G-LR-S • QDD-4x100G-FR-S	• Auto	Yes	• Auto • 400G • 500G • 600G • 700G • 800G • 900G • 1000G • 1100G • 1200G

Transponder / Muxponder	Traffic Type	FEC mode	Pluggables Supported		Encryption	Trunk Mode
			Client Pluggables	Trunk Pluggables		
NCS1K4-QXP-K9	100GE	OFEC CFEC	• Auto	• Auto • QDD400G-ZRP-S • QDD400G-ZR-S	Yes	• Auto
			• QSFP-100G-DR-S • QSFP-100G-LR4-S • QSFP-100G-LR-S • ONS-QSFP-28-LR4 • QSFP-100G-CWDM4-S • QSFP-100G-FR-S • QSFP-100G-SR4-S			• 100G
			• QDD-4x100G-LR-S			• 100G • 200G • 300G • 400G
	400GE		• QDD-400G-FR4-S • QDD-400-AOC1M • QDD-400G-DR4-S			• 400G

Supported Cards and Pluggables



APPENDIX C

Supported Optical Sources

Supported Optical Sources

Table 90: Feature History

Feature Name	Release Information	Feature Description
New Optical Source and Pluggable Support	Cisco ONP Release 4.2	Optical Sources enable you to simulate the optical feasibility of the network with the 400G and other interfaces that are not natively modeled in Cisco ONP. The following Optical Sources are introduced in this release: • ONS-CFP2D-400G-C-OpticalSources-V 2.mxd • QDD-400G-ZRP-S-OpticalSources-V2.mxd

Cisco ONP supports the following optical sources:

Note From Release 24.3.1, the optical sources for NCS 2000 networks are tagged with System Release to indicate from when the optical sources support the network release.

- OpticalSources_NCS2K_400GXP-LC_NCS4K-4H-OPW-QC2 DWDM Line Card
  - 400GXP_100G_25%_DE
  - 400GXP_200G_15%_DE
  - 100G-SD-FEC
  - 400GXP_100G_15%_DE
  - 200G-SD-FEC
  - 400GXP_100G_15%

- 400GXP_200G_15%
- 400GXP_200G_25%DE

- NCS1004_OpticalSources_V3
  - NCS1004_QPSK_SP_16QAM_200G_27%SDFEC_60GBd
  - NCS1004_SP_16QAM_300G_27%SDFEC_69GBd
  - NCS1004_QPSK_200G_27%SDFEC_69GBd
  - NCS1004_16QAM_32QAM_400G_27%SDFEC_62GBd
  - NCS1004_16QAM_400G_27%SDFEC_69GBd
  - NCS1004_SP_16QAM_16QAM_300G_27%SDFEC_60GBd
  - NCS1004_32QAM_500G_27%SDFEC_69GBd

- QDD and CFP2-DCO variants
  - **ONS-CFP2D-400G-C-OpticalSources-V2.mxd**[1]
    - CFP2_200OR_TXP_FOIC2_OFEC_15_DE_ON_4Q_1S_BR63_1
    - CFP2_300OR_TXP_FOIC3_OFEC_15_DE_ON_8Q_1S_BR63_1
    - CFP2_400OR_TXP_FOIC4_OFEC_15_DE_ON_16Q_1S_BR63_1
  - **ONS-CFP2D-400G-C-OpticalSources-V2.mxd**[2]
    - CFP2_300ZR+_MXP_GAUI8_OFEC_15_DE_ON_8Q_0S_BR60_1
    - CFP2_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_8Q_1E_BR40_1
    - CFP2_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_16Q_1E_BR30_1
    - CFP2_400ZR_TXP_GAUI8_CFEC_15_DE_ON_16Q_0S_BR59_8
    - CFP2_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_4Q_0S_BR60_1
    - CFP2_100ZR+_TXP_GAUI2_OFEC_15_DE_ON_4Q_1S_BR30_1
    - CFP2_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_4Q_1S_BR60_1
    - CFP2_400ZR+_TXP_GAUI8_OFEC_15_DE_ON_16Q_1E_BR60_1
    - CFP2_300ZR+_MXP_GAUI8_OFEC_15_DE_ON_8Q_1E_BR60_1
    - CFP2_400ZR+_TXP_GAUI8_OFEC_15_DE_ON_16Q_0S_BR60_1
    - CFP2_100OR_TXP_FOIC1_OFEC_15_DE_ON_4Q_1S_BR31_6
    - CFP2_200OR_TXP_FOIC2_OFEC_15_DE_ON_8Q_1S_BR42_1
    - CFP2_200OR_TXP_FOIC2_OFEC_15_DE_ON_16Q_1E_BR31_6

[1] The optical source interfaces are supported for SSON networks.
[2] The optical source interfaces are supported for SSON and non-SSON networks.

- **QDD-400G-ZRP-S-OpticalSources-V2.mxd**[2]
  - QDD_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_4Q_1S_BR60_1
  - QDD_400ZR_TXP_GAUI8_CFEC_15_DE_ON_16Q_0S_BR59_8
  - QDD_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_4Q_0S_BR60_1
  - QDD_400ZR+_TXP_GAUI8_OFEC_15_DE_ON_16Q_1E_BR60_1
  - QDD_400ZR+_TXP_GAUI8_OFEC_15_DE_ON_16Q_0S_BR60_1
  - QDD_300ZR+_MXP_GAUI8_OFEC_15_DE_ON_8Q_1E_BR60_1
  - QDD_400ZR+_TXP_GAUI8_OFEC_15_DE_ON_16Q_0E_BR60_1
  - QDD_300ZR+_MXP_GAUI8_OFEC_15_DE_ON_8Q_0E_BR60_1
  - QDD_100ZR+_TXP_GAUI2_OFEC_15_DE_ON_4Q_1S_BR30_1
  - QDD_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_16Q_1E_BR30_1
  - QDD_300ZR+_MXP_GAUI8_OFEC_15_DE_ON_8Q_0S_BR60_1
  - QDD_200ZR+_MXP_GAUI2_OFEC_15_DE_ON_8Q_1E_BR40_1

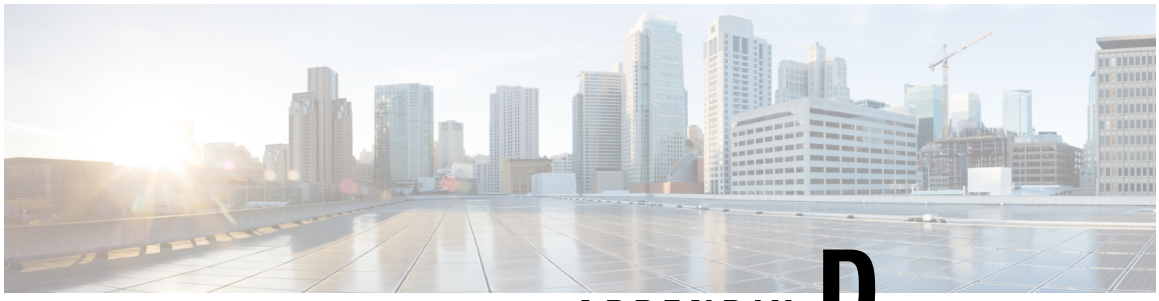
Note NCS 1004 is supported as an optical source.

Note The following optical source files are not supported in NCS 2000 Release 11.0:

- NCS1004_16QAM_32QAM_400G_27%SDFEC_62GBd
- NCS1004_QPSK_SP_16QAM_200G_27%SDFEC_60GB

Hence, we recommend you to upgrade the system release of the network to Release 11.1, or force the optical source files that are supported for the Release 11.0.

Supported Optical Sources



APPENDIX D

Supported Amplifiers

Supported Amplifiers

Cisco ONP supports the following amplifiers:

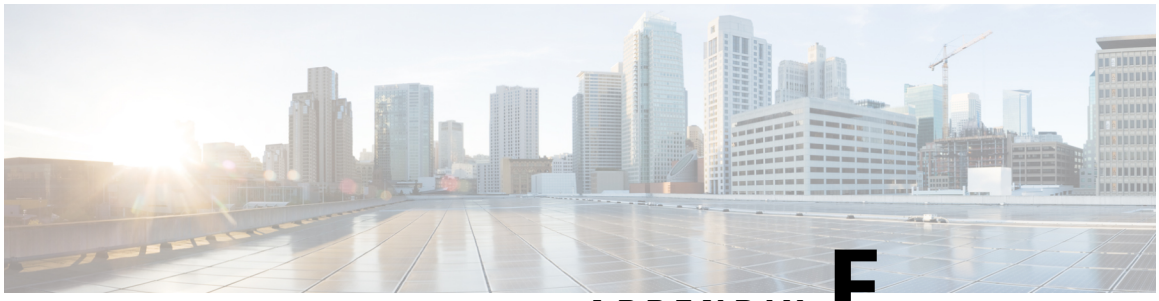
Table 91: Cisco ONP Supported NCS 2000 Amplifiers

Amplifier	Description
15454-M-RAMAN-CTP	Raman Amp C-Band
15454-M-RAMAN-COP	Raman Amp C-Band
EDFA 35 for OLA node	Erbium Doped Fiber Amplifier (EDFA) that can function in dual gain with maximum gain of 35 dB
NCS2K-EDRA2-26C	21dBm EDFA + Bst 26dB Span - C-Band
NCS2K-EDRA1-26C	21dBm EDFA 26dB Span - C-Band
NCS2K-EDRA2-35C	21dBm EDFA + Bst 35dB Span - C-Band
NCS2K-EDRA1-35C	21dBm EDFA35dB Span - C-Band

Note

- RAMAN-CTP is supported on all nodes.
- EDRAs are supported on the OLA node.
- For ROADM and Traffic nodes, the booster amplifier and preamplifier are in-built. The booster is 20SMR-FS-BST.

Supported Amplifiers



APPENDIX E

Troubleshoot

Troubleshooting Tasks

The following table describes the common error messages that are related to Cisco ONP configuration and the workarounds:

Table 92: Troubleshooting Tasks for Cisco ONP Configuration

Warning Message or Error	Probable Reason for the Error	Workaround
Cannot Route demand. Did not find any valid omnidirectional side.	Required contentionless sides are not created on add/drop sites. For protected service or wave, minimum two contentionless sides are required on the add/drop sites.	Check and add the required number of contentionless sides on the target service or wave source and destination sites.
Error: No valid path from <*source*> to <*destination*>	Disjoint path is not available for protected demand. Or Forced wavelength may be already used for other demand in the same path. Or The number of colorless demands created is more than the colorless ports forced on the interfaces.	For linear topology, change the demand protection to unprotected. For ring topology, ensure that at least two nodes and fiber-disjoint paths are available and the forced wavelength is unconfined in the end-to-end path. Force the required number of colorless ports.
Error: Traffic subnet constraints prevent routing of section.	Disjoint path is not available for protected demand. Or Forced wavelength may be already used for other demands in the same path.	For linear topology, change the demand protection to unprotected. For ring topology, ensure that at least two nodes and fiber-disjoint paths are available and the forced wavelength is unconfined in the end-to-end path.

Warning Message or Error	Probable Reason for the Error	Workaround
Error: The sum of CoDem and Non-CoDem colorless ports and ports that are used for Omnidirectional and Contentional sides cannot exceed 20 when the TYPE is SMR-20.	The number of contentionless sides, colorless ports that are forced, and colored demand exceed SMR-20 port capacity. Or The Cascaded SMR flag is enabled, and colored or colorless demand is created.	If the Cascaded SMR flag is enabled, create only contentionless demands on those nodes. Else, reduce the number of contentionless sides, colorless ports, or colored demands that are created, to get successful network analysis.
Couple between <*source*>.<*side*> and <*destination*>.<*side*> is of invalid type.	The fiber connecting these sides is not supported by Cisco ONP.	Change the fiber type to the one that is supported by Cisco ONP.
Unconnected nodes or sites are present in the network.	Any of the sites are connected to the fiber in the Ring/Linear network.	Connect the fiber to the nodes in the ring network.
Unfeasible forcing	Wrong path has been forced on the wave or media channel.	Force the correct path on the Wave/Media Channel.
E11000 duplicate key error collection: CnpDB.dbchangelog index: _id_ dup key: { : ObjectId(') }	Restore database script attempts to write data in the mongo database, but the data with the same index is already present.	Clear the contents of mongodb_cnp folder before running the restore command: **rm -rf /var/lib/mongodb_cnp/***cannot
Cannot complete mesh connection.	There is an issue with setting up connection in the lock mode.	Unlock the mentioned entity or unlock the complete site.
Path constraints prevent routing.	Invalid path has been forced.	Check the path and choose the correct primary path and secondary path fibers. Or Remove all the fibers that are forced to set the **Path of Wave** property as *Auto*.
Traffic subnet constraints prevent routing.	Forced Wavelength is not part of the Optical subnet rule.	Force the wavelength as per optical subnet rule or change the optical subnet rule.
MF Unit value MF1-RU is not supported in RPT, so resetting the value to default for <*site name*>.	Template is applied when properties such as **ECU**, **MF Unit** are forced.	Set the property **MF Unit** to *Auto* and then force the template.

Warning Message or Error	Probable Reason for the Error	Workaround
Please force MD-48-CM as Interlever Type for {0}.	In non-SSON traffic, the ROADM site with the properties (DEG-8, SMR-9, number of contentionless sites is equal to 1) has 96 colored waves. The **Interlever Type** is property set to *Auto* or *MpoCable.*	Modify the Interlever forcing on the line side to MD-48-CM.
The sum of forced CoDem and Non-CoDem colorless ports and colored demands can't be greater than 9 for type SMR-9.	During upgrade or Release upgrade, colorless port is forced on SMR-9, and more than one contentionless side is added in the imported MPZ network.	Delete the extra contentionless sides.
No Route Found.	Plan mode restoration fails because the presence of dark fiber in the restoration path makes it difficult to find it.	Check the restoration path. It must not have any dark fiber.
Wavelength Forced {0} in this {1} is already in use / not as per current optical subnet channel rule.	Two fibers are occupied by a wave with the same wavelength. The fiber belongs to a subnet where the wavelength is not supported. For example, a wave with an even wavelength is forced through a fiber belonging to the C40 channel or C48 channel subnet rules.	Correct the wave such that the wavelength is supported by the optical subnet C-band rule.
tm.unsupported_client_pluggable.msg =Incompatible Client Interface forcing.	ROADM sites having waves with optical source other than 100, 200SDFEC are converted to traffic sites.	Before you convert the site type to traffic, modify the optical source wave to be feasible.
Error Message	Slow internet connectivity, or idle session.	Refresh the browser and try again.
Please provide a valid .mpz network file.	The MPZ file that you are trying to upload does not have a valid file extension.	Upload proper .MPZ file.
Failed to import mpz file, please make sure the MPZ file is not in use and retry.	MPZ file remains open in the CTP tool.	Close MPZ file in the CTP tool before uploading it to Cisco ONP .
Cannot connect to Server;(Password).	Failed to connect to Mongo DB on opening **Control Panel** tab.	Restart the Mongo database container or reinstall the Build.

Warning Message or Error	Probable Reason for the Error	Workaround
Null pointer exception	The applied layout template file has syntax error such as extra SPACE, TAB, missing symbols such as <, >.	Fix the syntax and reapply the template.
Object not found in cache.	Intermediate network disconnection.	Refresh the browser or log in again to Cisco ONP.
Session does not exist.	Idle time-out	Log in again to Cisco ONP.
Forced/Locked wavelength is not feasible for spectrum to be allocated for the demand/MCH <*Site-1-Site-3-1*>. Insufficient spectrum around the forced central wavelength.	Forced wavelength is not a feasible central wavelength based on the configuration.	Force another wavelength that is next to the currently forced one.
Route could not be found/Alternate path not found/<Optically not feasible>.	Insufficient spectral width due to the following reasons: • The alternate path has no waves (dark fiber). • Optical parameters are not feasible. • Wavelength dos not have sufficient bandwidth.	Make sure that the alternate path has waves associated with the fiber and has sufficient bandwidth available.
Error: Could not find any valid flex configuration for the traffic matrix defined at <*Site-1.A*> This could be because of configuration limitations, invalid forcings, or equipment restrictions.	Check if it is 8 degrees, SMR-9 node with Evolved Mesh ON and contentionless and colorless/colored mixed add/drop configuration.	Change Evolved Mesh to Off, reduce Scalable upto degree to 8, change Site Type to SMR-20, or Remove contentionless or colorless forcing.
Single hop path Site-1~Site-3 needs regeneration but has no regenerator hosting sites.	Check if **Quick analysis** under Network property is disabled.	• Enable **Quick analysis**. • After successful analysis, check the optical report and look for the waves that require regeneration. • Split the long haul demand between the intermediate short distance nodes that are equivalent to regen site. • Disable **Quick analysis** and analyze.