

Get Started with Cisco Optical Network Planner

- Cisco Optical Network Planner Overview, on page 1
- Supported Platforms, on page 2
- Supported Topologies , on page 2
- Supported Protection Schemes , on page 3
- Supported Services, on page 4
- Supported DWDM Channel Interfaces, on page 5
- Supported Fiber Types, on page 5
- Register New User, on page 5
- Log in to Cisco ONP Web Interface, on page 6
- Cisco ONP Home Page, on page 6
- Change Password , on page 6
- Reset Your Password, on page 7
- Sign Out from Cisco ONP, on page 7
- Cisco Secure Development Lifecycle Compliance, on page 8

Cisco Optical Network Planner Overview

Cisco Optical Network Planner (Cisco ONP) is a tool to model and test Optical Transport Networks (OTN) and Dense Wavelength Division Multiplexing (DWDM) optical networks by using a graphical environment. The primary purpose of Cisco ONP is to design and validate networks of NCS 1004, NCS 1010, NCS 2000, and NCS 4000 series. Using the Cisco ONP tool, you create multiple instances of a network, modify different parameters at each instance, and compare. Cisco ONP generates a rack view of all the sites that are deployed in the network, shows the differences between the instances, and provides a complete Bill of Materials (BoM) for the network.

Cisco ONP models the network, generates the BoM, and provides detailed information about the network, such as Cabling report, Optical report, and Traffic matrix.

This chapter describes the features of Cisco ONP, protection scenarios, topology and service support, CSDL (Cisco Secure Development Lifecycle) compliance, and the setting up of the graphical display.

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

Supported Platforms

Cisco ONP supports the following platforms:

Table 1: Supported Platforms and Releases

Platforms	Recommended and Supported Releases
NCS 1004	7.11.1
NCS 2000	11.0.0, 11.1.0, 12.1.0, 12.2.0, 12.3.1
NCS 4000	6.5.33
NCS 1010	7.7.1, 7.9.1, 7.10.1, 7.11.1

Supported Topologies

Cisco ONP supports the following network topologies:

- Linear—In a linear topology, the nodes are arranged in a line and are connected to two other adjacent nodes. However, the first and last nodes are not connected.
- Mesh—In a mesh topology, each node is connected to one or more nodes. This configuration provides maximum redundancy to the network.
- Ring—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.

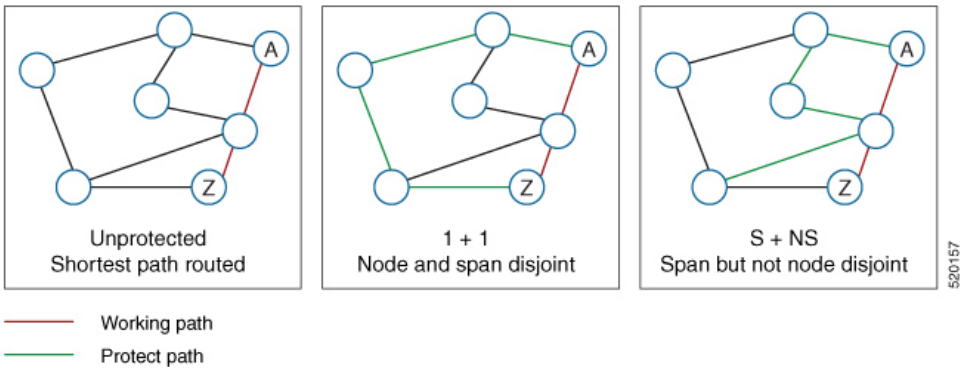
Supported Protection Schemes

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.

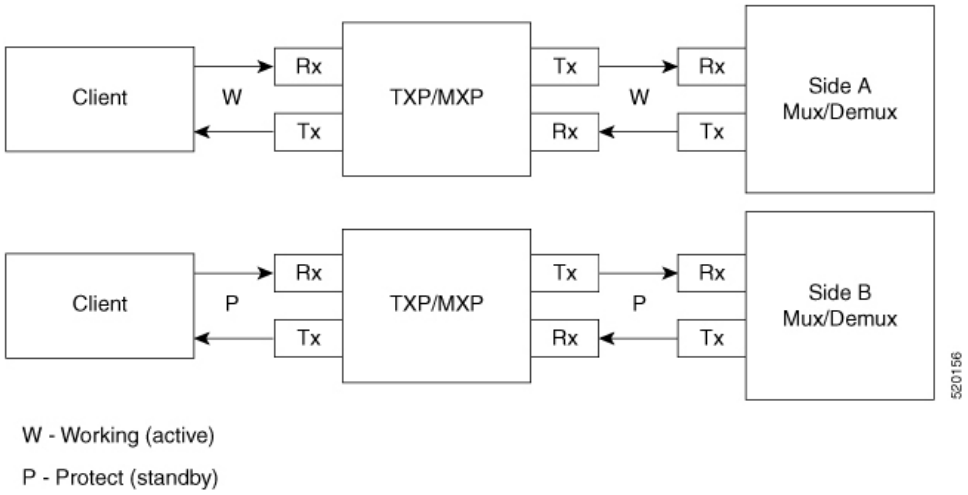
Cisco ONP supports the following protection schemes:

Figure 1: Protection Schemes



- **Unprotected**—In unprotected mode, the tool routes the service on the shortest path.
- **1+1**—Two client signals are transmitted to separate line cards or transponder cards instead of using Y-cable to split one client signal into two line cards or transponder cards. In client 1+1 protection, the failure and switchover are controlled by the client system. The following figure shows 1+1 protection.

Figure 2: 1+1 Protection



- **1+R**—Supported on SSON network. For each service, Cisco ONP automatically finds one working path. You can define the restoration path.
- **1+1+R**—Supported on SSON network. For each service, Cisco ONP finds one working path, and one protected path. You can define the restoration path.
- **1+1+R+R**—Supported on SSON network. For each service, Cisco ONP finds one working path and one protected path. You can define the 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-disjointed but not node disjointed.
- **Unprotected Disjoint**—Supported on non-SSON network. Cisco ONP provides two cards following two completely disjoint paths in the network to reach their destination.

Supported Services

Cisco ONP supports the following OTN demands:

- ODU-1,ODU-2,ODU-3,ODU-4
- GE – Gigabit Ethernet
- 10GE – 10-Gigabit Ethernet
- 100GE –100-Gigabit Ethernet
- STS-3
- STS-12
- STS-48
- STS-192
- VC-4-4

- VC-4-16
- VC-4-64
- STM-64

Supported DWDM Channel Interfaces

See Supported Cards and Pluggables and Supported Optical Sources for the DWDM channel interfaces supported by Cisco ONP.

Supported Fiber Types

Cisco ONP supports the following fiber types:

- G652-SMF
- G652-SMF-28E
- True Wave Reach
- True Wave RS
- True-Wave Plus
- True-Wave Minus
- True-Wave Classic
- Free-Light
- Tera-Light
- Metro-Core
- ELEAF
- NDSF (only NCS 1010)
- ALLWave (only NCS 1010)
- SMF-28 ULL (only NCS 1010)
- SMF28-Ultra (only NCS 1010)

Register New User

Use this task to register yourself as a user.

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**, and **Password**, and click **Submit**.

Click **Generate** if you want a system-generated password. Copy and paste the system-generated password in the **Password** field.

Step 4 Click **Ok** in the **Success** dialog box.

Log in to Cisco ONP Web Interface

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

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 New User, on page 5, for more information.

Note If 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.

Step 3 Click **Login**.

Cisco ONP Home Page

After your login, Cisco ONP displays its home page. The home page comprises the following elements:

- Menu bar—Includes various menus such as File, Network, Export, Import, Manage, Logs, Job Monitor, Control Panel, and Help. See Menu Bar.
- Last Login—Shows the last date and time when the user logged in to the Cisco ONP tool.
- Last Login IP—Shows the IP address of the client through which the user logged into the Cisco ONP tool previously.
- User name—Shows the name of the user, who has currently logged in to the Cisco ONP tool, for example: ADMIN.
- Reports tabs—Shows various reports under each tab. Report availability depends on whether a network is analyzed or not. Reports are also available in site properties after analyzing the network.
- Network tree—Displays the network name, and network elements, such as Sites, Fibers, Waves or Media Channels, SRLGs, and Subnet. See Network Tree.

Change Password

The procedure to change your existing password is:

Before you begin

Log in to Cisco ONP Web Interface, on page 6.

Step 1 Click the login icon in the top-right corner of the home page.
Step 2 Click **Change Password** to change the existing password.
Step 3 In the **Change Password** dialog box, enter the **Old Password**, **New Password**, **Repeat New Password**.
Step 4 Click **Update**.

Reset Your Password

The following procedure shows how to reset the password.

Step 1 In the browser URL field, enter the IP address or hostname of the Cisco ONP instance.
Step 2 Click **Forgot Password ?** in the Cisco ONP login page. The **Forgot Password** page appears.
Step 3 Enter the registered email ID in the Forgot Password page.
Step 4 Click **Continue**.

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

Step 5 Enter the verification code, new password and confirm password.
Step 6 Click **Continue**.

Sign Out from Cisco ONP

The procedure to sign out of Cisco ONP is:

Step 1 Click the login icon in the top-right corner of the home page.
Step 2 Click **Sign Out** to log out of the Cisco ONP tool.

Cisco Secure Development Lifecycle Compliance

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.

The following Cisco Secure Development Lifecycle (CSDL) compliancies are implemented:

- Check for the existence of new passphrases against a dictionary.
- Display of the last login date and time of the user in the user interface of the Cisco ONP tool.
- Display of the last login IP: The IP address of the client through which the user logged into the server, previously.
- Warning the users through pop-up messages about the impending passphrase expiration.
- Option to allow an admin user or any user with CONFIGURATION_MANAGEMENT permission to set the lifetime of a passphrase and the grace period to change the passphrase through the system configuration tab.
- Prompt for user to change the passphrase through the passphrase change dialog box, when the admin user logs in for the first time.
- Option to allow the user to set a passphrase with a minimum of eight characters and a maximum of 127 characters as the length.
- The passphrase must include at least one lowercase alphabet, one uppercase alphabet, one number, and one special character.
- Option to allow the user to set a passphrase or key for encryption of credentials during the installation of Live Network Import (LNI) application. If not specified Cisco ONP uses the default key.
- Option to allow the user to set a passphrase with a minimum of eight characters and a maximum of 64 characters as the length, during the installation of Cisco ONP and LNI database.
- LNI application provides the details of all the ports used. See Ports Used in LNI.
- Option to allow the user to generate a password using **Generate Password** option.
- Display of the strength of the password set by the user.