

Get Started with Cisco Optical Network Planner

- Cisco Optical Network Planner, on page 1
- Supported platforms, on page 2
- Supported topologies , on page 2
- Supported protection schemes , on page 2
- Supported services, on page 4
- Supported DWDM channel interfaces, on page 5
- Supported fiber types, on page 5
- Register a new user, on page 6
- Log in to Cisco ONP web interface, on page 6
- Cisco ONP home page, on page 7
- Change password, on page 7
- Reset your password, on page 7
- Sign out from Cisco ONP, on page 8
- CSDL compliance enhancements in Cisco ONP, on page 8

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 of Cisco ONP

The primary purpose of Cisco ONP is to design and validate networks for the NCS 1004, NCS 1010, 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. IYou can view detailed information about the network, including reports such as the Cabling report, Optical report, Device Configuration file, and 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 1010	7.7.1, 7.9.1
NCS 2000	11.0.0, 11.1.0, 12.1.0, 12.2.0, 12.3.1
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

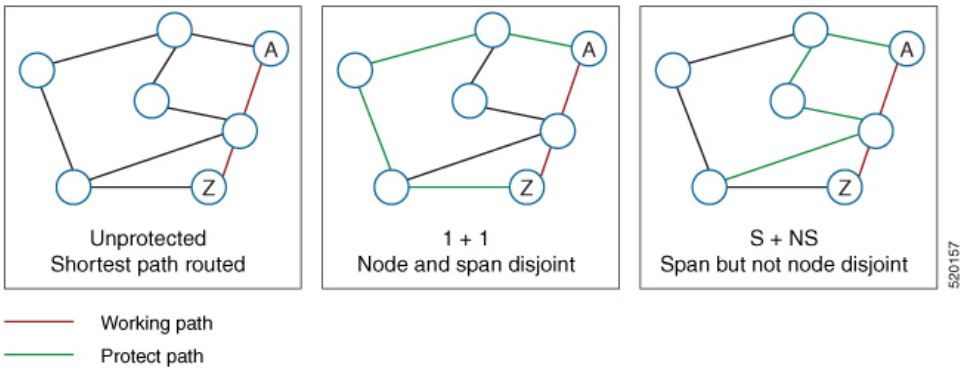
Cisco ONP offers a variety of protection schemes to enhance network reliability and resilience.

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.

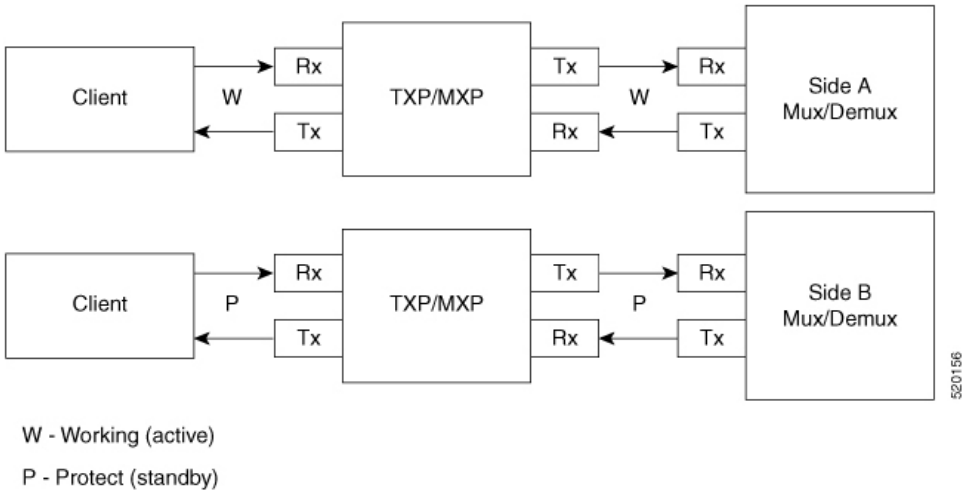
Figure 1: Protection schemes



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



W - Working (active)

P - Protect (standby)

- 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 and Supported Optical Sources.

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 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.
- 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.



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.