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 1001, 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. 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

Table 1: Feature History

Feature Name	Release Information	Feature Description
Support for NCS 1001 Network Creation	Cisco ONP Release 24.3.1	This release supports the design of C-band NCS 1001 networks. The NCS 1001 is a 1RU, DWDM line system optimized for data center environments. It includes support for amplifiers, PSM modules, and various colored add/drop modules such as MD-32-EVEN, FLD-4, MD-48-ODD, MD-48-EVEN, and MD-64. Cisco ONP supports unprotected, terminal section, and terminal path protection over the NCS 1001 network. Also, the NCS 1001 network is compatible with optical sources such as NCS 1004, CIM8, Bright ZR, QDD, and CFP2.

Feature Name	Release Information	Feature Description
Addition of new NCS 1020 Chassis for NCS 1010 Networks	Cisco ONP Release 24.3.1	NCS 1020 is a 10RU optical line system that supports the OLTs and NCS1K14-CCMD-16-C card in the NCS 1010 networks. The NCS 1020 chassis optimizes the NCS 1010 networks design, extending the reach of NCS 1010 networks. With OLTs and NCS1K14-CCMD-16-C, the NCS 1020 chassis provides a wide range of configuration options to NCS 1010 networks.

Cisco ONP supports these platforms:

Table 2: Supported platforms and releases

Platforms	Recommended and Supported Releases
NCS 1001	7.10.1, 25.4.1
NCS 1014	24.3.1, 25.1.1, 26.1.1
NCS 1010	7.10.1, 7.11.1, 24.3.1, 25.1.1, 26.1.1
NCS 2000	11.1.0, 25.1.1, 26.1.1
NCS 4000	6.5.33

Supported topologies

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

- 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

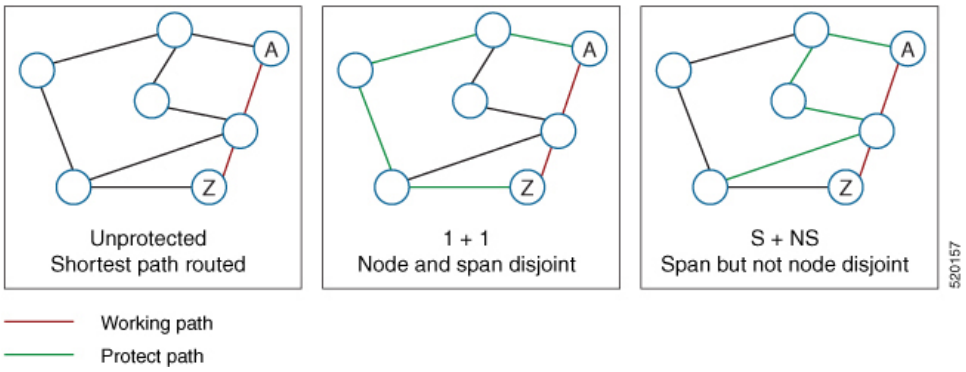
Cisco ONP offers a variety of protection schemes to enhance network reliability and resilience.

Table 3: 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.

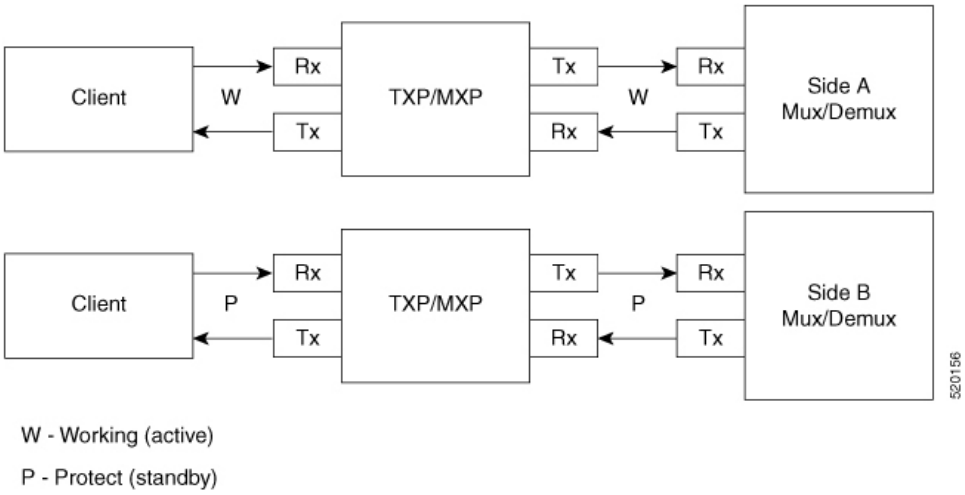
Figure 1: Protection schemes



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 both SSON and non-SSON NCS 4000 and NCS 2000 networks, 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 both SSON and non-SSON NCS 4000-NCS 2000 network, this scheme provides two cards following two completely disjoint paths in the network to reach their destination.
- PSM-Channel protection: This protection scheme is supported on NCS 2000 non-SSON networks.

Supported services

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

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

- 10GE
- 100GE
- 400GE

  The 400GE service is supported on the NCS 1010 networks.

- 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
  - SMF-28 ULL (only NCS 1010)
  - SMF28-Ultra (only NCS 1010)
- True Wave fiber series:
  - True Wave Reach
  - True Wave RS
  - True-Wave Plus

- True-Wave Minus
- True-Wave Classic

- Other type of fibers:
  - Free-Light
  - Tera-Light
  - Metro-Core
  - ELEAF
  - NDSF (only NCS 1010)
  - ALLWave (only NCS 1010)

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 procedure 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 7.

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.

The Cisco ONP home page displays key elements that help users navigate and utilize the platform effectively.

- Menu bar: Includes options such as File, Network, Export, Import, Manage, Logs, Job Monitor, Control Panel, and Help. For more information about menu options, 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: Indicates the current user (for example, ADMIN).
- Reports tabs: Provide access to various reports. The availability of reports depends on whether the network has been analyzed. Reports are also accessible from site properties after network analysis.
- Network tree: Displays the network name and its elements, including Sites, Fibers, Waves or Media Channels, SRLGs, and Subnets. For more information, see Network Tree.

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

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

Change password

Use this procedure 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

A CSDL compliance enhancement is a set of security features in Cisco ONP that

- display the last login IP address of the client in the user interface,
- allow administrators to set a passphrase for encrypting credentials during the installation of the Live Network Import (LNI) application and its database, and
- incorporate several Secure Development Lifecycle (CSDL) compliance measures to strengthen security and user management.

Table 4: 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.

Other security and user management improvements associated with CSDL compliance in Cisco ONP include:

Passphrase security features

- Ensure new passphrases do not match common passwords by checking against a dictionary.
- Notify users with pop-up alerts before passphrase expiration.
- Enable administrators or users with CONFIGURATION_MANAGEMENT permission to configure passphrase lifetime and grace period in the system configuration tab.
- Require passphrases to be 8–127 characters and contain at least one lowercase letter, one uppercase letter, one number, and one special character.

Passphrase management features

- Prompt administrators to change their passphrase upon first login.
- Allow setting a passphrase or encryption key for credentials during LNI application installation (using a default key if unspecified).
- Permit users to set a passphrase between 8 and 64 characters during Cisco ONP and LNI database installation.

User login information features

- Display the last login date and time.
- Show the last login IP address in the Cisco ONP user interface.

Additional security features

- Offer a “Generate Password” option, letting users create a password automatically.
- Display password strength as the user sets it.
- Provide improved feedback during password creation.