Get Started with Cisco Optical Network Planner

Cisco Optical Network Planner

Introduction to Cisco Optical Network Planner

Cisco Optical Network Planner (Cisco ONP) is a web application designed to model and test Optical Transport Networks (OTN) and Dense Wavelength Division Multiplexing (DWDM) optical networks using a graphical environment.

Purpose of Cisco ONP

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.

Network design and comparison

With Cisco ONP, users 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 not only models the network and generates the BoM but also offers detailed information about the network. This includes reports such as the Cabling report, Optical report, Device Configuration file, and Traffic matrix.

Features and compliance

This chapter outlines the features of Cisco ONP, including protection scenarios, topology and service support, and compliance with the Cisco Secure Development Lifecycle (CSDL). It also covers setting up the graphical display.

Additional resources

For more detailed information about Cisco ONP, please refer to 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
NCS 1014	25.1.1
NCS 1010	7.7.1, 7.9.1, 7.10.1, 7.11.1, 24.3.1, 25.1.1
NCS 2000	11.0.0, 11.1.0, 12.1.0, 12.2.0, 12.3.1, 25.1.1
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.

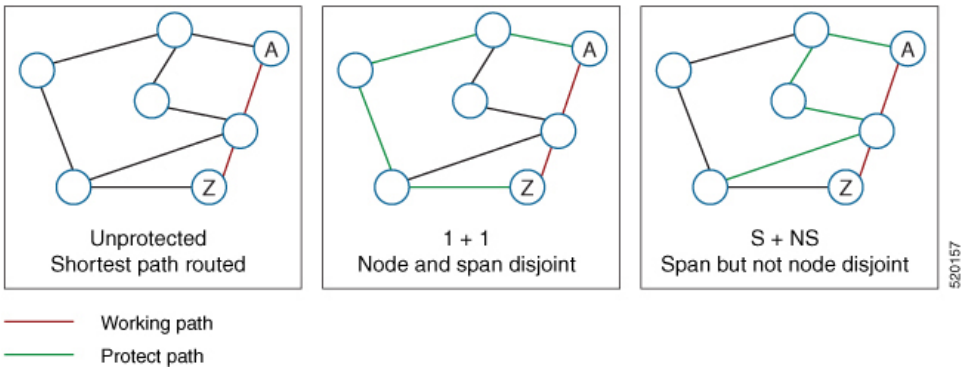
Supported protection schemes

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



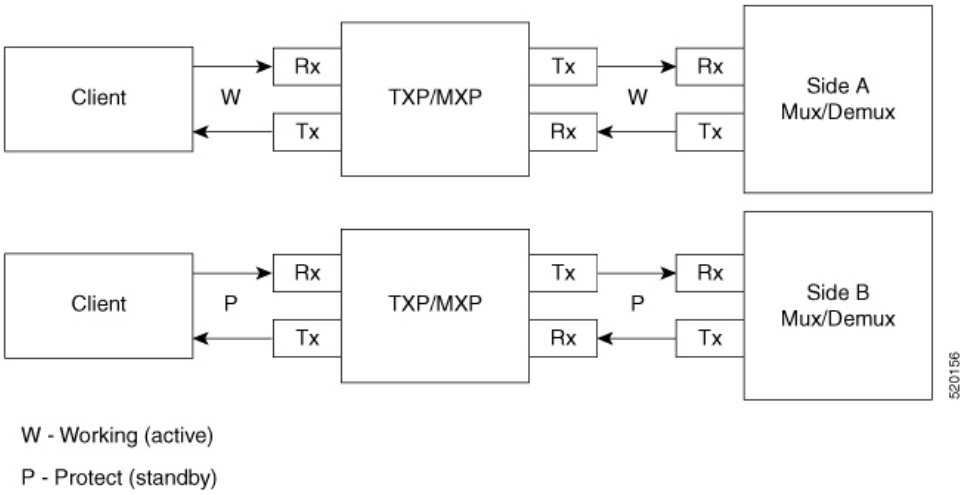
Unprotected

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 and 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. Users 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. 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, with the option for users to define additional restoration paths.

S+NS

Supported on both SSON and non-SSON NCS 4000-NCS 2000 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 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 demands:

- ODU-1,ODU-2,ODU-3,ODU-4
- GE – Gigabit Ethernet
- 10GE – 10-Gigabit Ethernet
- 100GE –100-Gigabit Ethernet
- 400GE –400-Gigabit Ethernet

  The 400GE service is supported on the NCS 1010 networks.
- STS-3
- STS-12
- STS-48
- STS-192
- VC-4-4
- VC-4-16
- VC-4-64
- STM-64

Supported DWDM channel interfaces

For detailed information on the DWDM channel interfaces supported by Cisco ONP, refer toSupported Cards and Pluggables and Supported Optical Sources.

Supported fiber types

Cisco ONP supports these 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 a new user

Use this task to register yourself as a user.

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 generated password is autopopulated in the **Password**, and **Confirm Password** fields.

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 7, for more information.

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

After logging 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 various menus such as File, Network, Export, Import, Manage, Logs, Job Monitor, Control Panel, and Help. [Additional information or reference needed here]

Last login details

- **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 information

- **User name**: Displays the name of the currently logged-in user, for example, ADMIN.

Reports tabs

The home page includes various report tabs that provide access to different reports. The availability of reports depends on whether a network has been analyzed. Reports can also be accessed in site properties after network analysis.

Network tree

The network tree displays the network name and its elements, such as Sites, Fibers, Waves or Media Channels, SRLGs, and Subnet. [Additional information or reference needed here]

Expanding the workable area

To expand the Cisco ONP workable area, click the horizontal and vertical arrows on the home page. If an empty grey window appears, ensure you are using the latest version of your browser. For detailed hardware and software requirements, refer to theCisco ONP Installation Guide.

Change Password

use this task to change your existing password.

Before you begin

Log in to Cisco ONP web interface, on page 7.

Procedure

Step 1 Click the Login icon in the top-right corner of the home page, and choose **Change Password**.

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

Reset your password

The following procedure shows how to reset the password.

Procedure

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, and click **Continue**.

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

Step 4 Enter the verification code, new password and confirm password, and click **Continue**.

Sign out from Cisco ONP

Use this task 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.

Cisco Secure Development Lifecycle compliance

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.

Cisco ONP incorporates several CSDL compliances to enhance security and user management:

Passphrase security

- **Dictionary check**: Ensures new passphrases do not exist in a dictionary of common passwords.
- **Expiration warning**: You receive pop-up messages alerting them about impending passphrase expiration.
- **Configurable lifetime and grace period**: Admin users or those with CONFIGURATION_MANAGEMENT permission can set the lifetime of a passphrase and a grace period for changing it via the system configuration tab.
- **Passphrase requirements**: Passphrases must be between 8 and 127 characters, including at least one lowercase letter, one uppercase letter, one number, and one special character.

Passphrase management

- **Initial admin login**: Prompts the admin to change the passphrase upon first login.
- **Installation encryption**: Allows setting a passphrase or key for encrypting credentials during the installation of the Live Network Import (LNI) application. If unspecified, a default key is used.
- **Installation passphrase length**: During Cisco ONP and LNI database installation, users can set a passphrase between 8 and 64 characters.

User login information

- **Last login details**: Displays the last login date, time, and IP address in the Cisco ONP user interface.

Additional security features

- **Password generation**: Users have the option to generate a password using the Generate Password feature.
- **Password strength display**: The strength of the password set by the user is displayed.