

Managing the Shelf

Note Starting with Release 11.1.4, ONS 15454 M12 chassis and TCC3 card are not supported on the ONS 15454 DWDM and WSON software packages. You must not attempt to upgrade ONS 15454 M12 nodes from a previous release to Release 11.1.4.

This chapter explains how to provision a single Cisco ONS 15454 dense wavelength division multiplexing (DWDM) node and turn it up for service, including assigning the node name, date, and time; provisioning timing references; provisioning network attributes such as IP address and default router; setting up users and user security; and creating DWDM connections.

The procedures and tasks described in this chapter for the Cisco ONS 15454 platform is applicable to the Cisco ONS 15454 M2 and Cisco ONS 15454 M6 platforms, unless noted otherwise.

Procedures in this chapter require that you have a network plan calculated for your DWDM network with Cisco Transport Planner. Cisco Transport Planner is a DWDM planning tool that is available from your Cisco account representative. Cisco Transport Planner prepares a shelf plan for each network node and calculates the power and attenuation levels for the DWDM cards installed in the node. For information about Cisco Transport Planner, contact your Cisco account representative. For instructions on using Cisco Transport Planner, refer to the *Cisco Transport Planner DWDM Operations Guide*.

Note Unless otherwise specified, in this document “ONS 15454” refers to both ANSI (ONS 15454) and ETSI (ONS 15454 SDH) shelf assemblies.

Note During the conversion of single shelf to multishelf node controller shelf, it is recommended to delete all the existing circuits on the shelf once and then proceed with re-creating them to avoid any unnecessary results. For example, the TL1 retrievals will not return the right values if the circuits are not deleted before converting to multishelf node.

Note Due to memory limitations, TCC2/TCC2P cards are not supported from Release 10.5.2 onwards. As a result, in a multishelf configuration, the TCC2/TCC2P cards cannot be a node controller or a shelf controller. Upgrade the TCC2/TCC2P card to a TCC3 card.

Note Cisco Transport Controller (CTC) views referenced in these procedures depend on the mode. In single-shelf mode, the views are network, node, and card. In multishelf mode, the views are network, multishelf, shelf, and card. For more information about CTC views, refer to CTC Enhancements, Operations, and Shortcuts.

- NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2
- NTP-G22 Verifying Common Card Installation, on page 4
- NTP-G250 Verifying Digital Image Signing (DIS) Information, on page 6
- NTP-G144 Provisioning a Multishelf Node, on page 8
- Duplicate Node Controller, on page 11
- NTP-G23 Create Users and Assign Privileges, on page 12
- Setting Maximum Password Length Using CTC, on page 15
- NTP-G24 Setting Up Node Identification Information, on page 15
- NTP-G25 Setting Battery Power Monitor Thresholds, on page 18
- NTP-G26 Setting Up CTC Network Access, on page 19
- NTP-G194 Setting Up EMS Secure Access to the Node, on page 35
- NTP-G27 Setting Up the Node for Firewall Access, on page 35
- NTP-G28 Creating FTP Host, on page 37
- NTP-G132 Provisioning OSI, on page 39
- NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51
- NTP-G320 Configuring the Node as a Non-DWDM Network, on page 55
- NTP-G31 Installing the DWDM Dispersion Compensating Units, on page 57
- NTP-G239 Managing Passive Units and Passive Shelves, on page 58
- NTP-G152 Creating and Verifying Internal Patchcords, on page 64
- NTP-G242 Creating an Internal Patchcord Manually, on page 66
- NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option, on page 67
- NTP-G209 Creating, Editing, and Deleting Optical Sides, on page 77
- NTP-G38 Provisioning OSC Terminations, on page 80
- NTP-G37 Running Automatic Node Setup, on page 82
- NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode, on page 84
- NTP-G332 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode with TCC2P Cards as Subtending Shelf Controller, on page 86
- DLP-G730 Editing the Shelf ID of the Subtending Shelf in a Multishelf Configuration Using the LCD, on page 88

NTP-G139 Verifying Cisco Transport Planner Reports and Files

Purpose	This procedure verifies that you have the Cisco Transport Planner reports and files needed to turn up the node.

Tools/Equipment	None
Prerequisite Procedures	Chapter 1, "Install the Cisco ONS 15454, ONS 15454 M2, and ONS 15454 M6 Shelf" in the Cisco ONS 15454 Hardware Installation Guide
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Procedure

Step 1 Verify that you have the Cisco Transport Planner reports and files shown in the following table for the node that you will provision. The reports and files can be provided in one of the following ways:

- If you have Cisco Transport Planner, verify that you have the electronic network design plan from which you can generate the reports in Cisco Transport Planner. For information about generating the reports, refer to the *Cisco Transport Planner DWDM Operations Guide*.
- If you do not have Cisco Transport Planner, you must have printouts of all reports listed in the following table except the Assisted Configuration Setup file. Assisted Configuration Setup is an electronic file that will be imported into CTC. You must be able to access it from the CTC computer used to provision the node
- If you not do not have all the reports and files listed in the following table, do not continue. See your site planner or network planner for the required information and files.

Step 2 Print the following table for reference. You will need information from the reports during node turn-up.

Stop. You have completed this procedure.

Cisco Transport Planner Node Setup Information and Files

Table 1: Cisco Transport Planner Node Setup Information and Files

Source	Format	Description
Shelf layout	JPG file	Cisco Transport Planner provides a shelf layout showing the cards that should be installed in each slot. Cisco Transport Planner can export each of these cards as a JPG file with a user-defined name.
Installation Parameters	Table	Provides the target reference values for the variable optical attenuators (VOAs), output power, optical thresholds, and amplifier configuration parameters.
Internal Connections	Table	Identifies the patchcords that must be installed within the shelf.

Source	Format	Description
NE Update Configuration file	XML file	The Cisco Transport Planner NE Update configuration file is an electronic file with an XML extension and a name assigned by the network designer for the network you are provisioning. The file is imported into CTC where it preprovisions internal patchcords, optical sides and card parameters for optical cards, transponders, and passive units (DCUs and patch panels). It configures the ANS parameters based on the network calculated by Cisco Transport Planner.
Traffic Matrix	Table	Shows the traffic flow within the node. During node turn-up, this report is used to identify the location of Y-cable protection groups.
Cable list	Table or list	A list of cables needed to provision the node. The list can be derived from the Internal Connections Report or from the Bill of Materials report prepared by Cisco Transport Planner.

NTP-G22 Verifying Common Card Installation

Purpose	This procedure verifies the following: • Cisco ONS 15454 shelf has two TCC2/ TCC2P/TCC3 cards installed. • Cisco ONS 15454 M6 and the Cisco ONS 15454 M2 shelves have TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O cards installed. • Cisco ONS 15454 M6 and the NCS 2015 shelves have TNCS/TNCO cards installed. It also verifies the installation of the AIC-I and MS-ISC-100T cards, if they are installed.
Tools/Equipment	None
Prerequisite Procedures	Install the Shelf in the *Cisco 15454 Hardware Installation Guide*
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Retrieve or higher

Procedure

Step 1 Verify the following:

- TCC2/TCC2P/TCC3 cards are installed in Slots 7 and 11 on the ONS 15454 shelf.
- Two TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards are installed in Slots 1 and 8 on the ONS 15454 M6 shelf.

- A stand-alone TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O card is installed in Slot 1 on the ONS 15454 M2 shelf.
- Two TNCS/TNCS-O cards are installed in Slots 1and 17 on the NCS 2015 shelf.

Step 2 Verify that the FAIL LED is off on both the control cards.

Step 3 Verify that the green ACT (active) LED is illuminated on one control card and that the amber STBY (standby) LED is illuminated on the other control card.

Note
If the control cards are not installed, or if their LEDs are not operating as described, do not continue. Complete the "DLP-G33 Install the TCC2, TCC2P, or TCC3 Card" or " Installing and Configuring the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O or TNCS/TNCS-O Card" task in the Cisco ONS 15454 Hardware Installation Guide.

Step 4 (On 15454-DWDM shelf) If the AIC-I card is installed, verify that it is installed in Slot 9 and that its ACT (active) LED displays a solid green light.

Note
If the AIC-I card is not installed and the card is required by the Cisco Transport Planner shelf layout, or if it is installed and its LEDs are not operating as described, do not continue. Complete the "DLP-G34 Install the AIC-I Card" task in the Cisco ONS 15454 Hardware Installation Guide or refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide* to resolve installation problems before proceeding to the next step.

Step 5 Verify that the software release shown on the LCD matches the software release required for your network. On the LCD, the software release is shown under the platform (SONET or SDH) and date/temperature. If the release does not match, perform one of the following procedures:

- Perform a software upgrade using the software CD. Refer to the release-specific software upgrade document.
- On ONS 15454, replace the TCC2/TCC2P/TCC3 cards with cards containing the correct release.
- On ONS 15454 M6, replace the LCD and TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards with cards containing the correct release.
- On ONS 15454 M2, replace the power module and TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O cards with cards containing the correct release.
- On NCS 2015, replace the LCD and TNCS/TNCS-O cards with cards containing the correct release.

Step 6 (On ONS 15454 shelf) If the node will be configured as a multishelf node, verify that redundant MS-ISC-100T cards are installed (Slots 6 and 12 are recommended) and that the green ACT (active) LED is illuminated on both cards.

Note
If the MS-ISC-100T card is not installed and the card is required by the Cisco Transport Planner shelf layout, or if the card's LEDs are not operating as described, do not continue. Complete the "DLP-G309 Install the MS-ISC-100T Card" task in the Cisco ONS 15454 Hardware Installation Guide or refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide* to resolve installation problems before proceeding to the next procedure.

Stop. You have completed this procedure.

NTP-G250 Verifying Digital Image Signing (DIS) Information

Purpose	This procedure retrieves the following information for the TNC/TNCE/TSC/TSCE/TNCS-2/TNCS-2O/TNCS/TNCS-O cards: • Software signature information • Version of the digitally signed software • Public keys installed In a hybrid multi-shelf configuration involving ONS 15454 and ONS 15454 M6 shelf assemblies, DIS information is available for the ONS 15454 M6 shelf only.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As Needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve user

Procedure

Step 1 Do the following as applicable at the node where you want to verify the DIS information:

a) To retrieve the digitally signed software version, go to Step 2.

b) To retrieve the software signature information, go to Step 3.

c) To retrieve the public keys installed on the node, go to Step 4.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click **Maintenance** > **Software** tab to retrieve the digitally signed software version. The following columns appear in the pane:

- Node—Displays the node name or IP address.
- Type—Displays the node type.
- **Node Status**—Displays the node status, which is based on the highest alarm level at the node.
- **Working Version**—Displays the working node software version (the general software release number [n.n.n] followed by the specific software release identification number). For example, 9.2.0 (09.20-X10E-02.06).
- **Protect Version**—Displays the protect node software version (the general software release number [n.n.n] followed by the specific software release identification number). For example, 9.2.0 (09.20-X10E-02.06).
- **Download Status**—Displays the status of any in-progress network software downloads.

Step 3 In node view (single-shelf mode) or shelf view (multishelf view), click **Maintenance** > **DIS** > **Info** > **Retrieve Signature Information** tabs to retrieve signature information. The following information is displayed in the pane:

- Attribute**—**The following information is displayed:
  - Organization Name—Displays the owner of the software image.
  - Organization Unit—Displays the business unit within Cisco.
  - Serial Number—Displays the serial number of the certificate with the digital signature.
  - Common Name—Displays the name of the platform.
  - Hash Algorithm—Displays the hashing algorithm used.
  - Image Type—Shows the type of the image-Development or Production.
  - Key Version—Indicates the key version used to digitally sign the image. A key version is identified with an alphabetical character that ranges from A to Z.
  - Sign Algorithm—Refers to the RSA algorithm.
  - Working Software Information—Displays the signature information of the working software.
  - Protect Software Information—Displays the signature information of the protect software.

Note
To refresh the signature information, click **Refresh Signature Information.**

Step 4 In node view (single-shelf mode) or shelf view (multishelf mode), click **Maintenance** > **DIS** > **Available Keys** > **Retrieve All Keys** tabs to retrieve public key information. The following information is displayed in the pane:

- **Key Type—**Displays the public key available on the system for verification:
  - **Release Key—**Verifies release images.
  - **Development Key—**Verifies the development images.
- **Public Key Algorithm—**Displays the name of the algorithm used for public key cryptography.
- **Exponent—**Displays the exponent of the public key algorithm—release or development keys.
- **Key Version—**Displays the key version used for verification.
- **Modulus**—Displays the modulus of the public key algorithm with a size of 2048 bits.

Note
To refresh the public key information, click **Refresh All Keys.**

Stop. You have completed this procedure.

NTP-G144 Provisioning a Multishelf Node

Purpose	This procedure provisions a multishelf node from CTC. A multishelf node consists of a control node and subtending shelves that are configured to operate as a single node.
Tools/Equipment	None

Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4
	• Cisco ONS 15454 Hardware Installation Guide:
	  • "NTP-G301 Connect the ONS 15454 Multishelf Node and Subtending Shelves to an MS-ISC-100T Card"
	  • "NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950"
	  • "NTP-G295 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 3560"
	  • "NTP-G296 Upgrade the ONS 15454 Multishelf with MS-ISC Card Configuration Using the Catalyst 3560"
	  • "NTP-G297 Upgrade the ONS 15454 Multishelf with Catalyst 2950 Configuration Using the Catalyst 3560"
	  • "NTP-G308 Connect the ONS 15454 M6 Multishelf Node and the ONS 15454 M6 Subtending Shelves"
	  • "NTP-G309 Connect the ONS 15454 M6 and the ONS 15454 in a Mixed Multishelf Configuration"
	  • NTP-G310 Upgrade the ONS 15454 Multishelf Configuration using the ONS 15454 M6
	• DLP-G46 Log into CTC

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution An optical shelf in a multishelf configuration must be provisioned as the node controller shelf and not as a subtending shelf. Otherwise, traffic will be dropped. If there are no slots available on the optical shelf to install the MS-ISC-100T cards (needed for a node controller shelf), install and configure the Cisco Catalyst 2950 or Cisco Catalyst 3560. See the "NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950" procedure or the "NTP-G295 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 3560" procedure in the Cisco ONS 15454 Hardware Installation Guide. If you are using an ONS 15454 M6, then refer to the applicable procedure for connecting the ONS 15454 M6 as the node controller in the Cisco ONS 15454 Hardware Installation Guide.

Note If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

Note When a subtending shelf controller (SSC) having active and standby control cards is initially connected to the node controller, the Software Download In-progress alarm is not raised on the standby control card of SSC.

Procedure

Step 1 If you want to set up the login node as the node controller, complete the following steps. If not, continue with Step 2.

a) In node view (single-node mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **Multishelf Config** tabs.

b) Click **Enable as Node Controller**.

c) From the LAN Config drop-down list, complete one of the following:

- Choose **Ethernet Switch** if MS-ISC-100T cards or the Catalyst 2950 or the Catalyst 3560 switches are already installed and configured. Choose the public VLAN ID and private VLAN ID for the ONS 15454 multishelf node. In case of ONS 15454 M6, the public VLAN ID and private VLAN ID are static (1 and 2 respectively).

  Note
  Before a SSC is connected to a multishelf node controller shelf, ensure **Ethernet Switch** is selected from the LAN Config drop-down list.

  Note
  Public VLAN ID is used by the node controller to communicate with the external network. Private VLAN ID is used by the node controller to communicate with the subtending shelves.

  Note
  If the ONS 15454 M6 shelf is used as the node controller, then you can connect the subtending shelves directly to the MSM ports on the ECU. However, a Catalyst 3560 switch can also be used along with the ONS 15454 M6 node controller to extend the number of subtending shelves.

- Choose **Stand-Alone** if MS-ISC-100T cards are not installed yet but will be included in the final layout. This option will allow a safe migration of the control card database when the multishelf configuration is complete.

d) Click **Apply**.
e) In the confirmation dialog box, click **Yes** to allow the node to reboot. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)
f) After the node reboots, double-click the node. The multishelf view appears.

Note
The shelf ID of the node controller is automatically assigned as 1.

Step 2 If you want to add a node as a subtending shelf in the multishelf configuration, complete the following steps. If not, you have completed this procedure.

Note
A Cisco ONS 15454 node configured with TCC2P and TCC3 cards must not be added to a multishelf configuration containing either of the following configurations:

- Cisco ONS 15454 node with TCC3 as the node controller
- Cisco ONS 15454 M6 node with TNC as the node controller

a. In multishelf view, right-click the white space in the rack and choose **Add Shelf** from the shortcut menu.

b. Select the type of subtending shelf.

c. In the Shelf ID Selection dialog box, choose a shelf ID (from 2 to 50) from the drop-down list.

d. Click **OK**. The shelf appears in multishelf view.

e. Disconnect the cross-over (CAT-5) LAN cable from the RJ-45 LAN (TCP/IP) port of the ONS 15454 subtending shelf TCC2/TCC2P/TCC3 card in Slot 11 or Slot 7, or from the EMS RJ-45 LAN (TCP/IP) on the ONS 15454 M6 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

f. Connect your Windows PC or Solaris workstation network interface card (NIC) to the RJ-45 LAN (TCP/IP) port on the TCC2/TCC2P/TCC3 card in Slot 11 or Slot 7, or to the EMS RJ-45 LAN (TCP/IP) on the ONS 15454 M6 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

g. Complete the DLP-G46 Log into CTC task at the subtending shelf.

h. Click the **Provisioning** > **General** > **Multishelf Config** tabs.

i. Click **Enable as Subtended Shelf**.

j. From the Shelf ID drop-down list, choose the shelf ID that you created in Step c.

k. Click **Apply**.

l. In the confirmation dialog box, click **Yes** to reboot the shelf. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)

m. Disconnect your Windows PC or Solaris workstation NIC from the RJ-45 LAN (TCP/IP) port of the ONS 15454 subtending shelf TCC2/TCC2P/TCC3 card in Slot 11 or Slot 7, or from the EMS RJ-45 LAN (TCP/IP) on the ONS 15454 M6 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

n. Reconnect the cross-over (CAT-5) LAN cable (disconnected in Step e) to the RJ-45 LAN (TCP/IP) port of the subtending shelf TCC2/TCC2P/TCC3 card in Slot 11 or Slot 7, or to the EMS RJ-45 LAN (TCP/IP) on the ONS 15454 M6 subtending shelf that correspond to the TNC/TNCE/TSC/TSCE card.

o. Repeat Steps a through n to set up additional subtending shelves.

Note
To connect the subtending shelves to the node controller, refer to the applicable procedures in the Cisco ONS 15454 Hardware Installation Guide.

Note
Non-LAN connected Multishelf nodes are not manageable from CTC unless SOCKS Proxy is enabled on the node.

Stop. You have completed this procedure.

Duplicate Node Controller

(Only on ONS 15454 M6 and NCS 2015) When a TNC/TNC-E/TSC/TSC-E/TNCS/TNCS-2/TNCS-2O/TNCS-O node controller connects to the same switch where an ONS 15454 M6 or NCS 2015 node controller exists, both the node controllers raise the critical Duplicate Node Controller (DUP-NC) alarm. The subtending shelves of both the node controllers raise the Shelf Communication Failure (SHELF-COMM-FAIL) alarm. Both the node controllers and their subtending shelves shut down their ports on ASIC towards the MSM ports in ECU. However, the traffic is not affected. This feature enables the original node to operate seamlessly in case of such misconfigurations, without the risk of its subtending shelves treating the new node controller as its primary.

The duplicate node controller can be any one of the following combinations.

- A node controller without any subtending shelf.
- A node controller with one or more subtending shelves connected through switch or daisy chain.

Recovering the Duplicate Node Controller

Note It is recommended to recover the nodes from the DUP-NC critical alarm in less than ten minutes.

Perform the following steps to recover the duplicate node controller.

- Disconnect the duplicate node controller's cable from switch.
- Perform soft reset of the active control card on both the node controllers. The DUP-NC alarm clears.
- Perform hard reset of the active control card on the subtending shelves to restore the multi-shelf.

NTP-G23 Create Users and Assign Privileges

Purpose	This procedure creates users and assigns their privilege levels.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verify Common Card Installation • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 Log into the node where you need to create users.

Note
You must log in as a Superuser to create additional users. The root user can be used to set up other users.

Step 2 Complete the "DLP-G54 Create a New User on a Single Node" task or the "DLP-G55 Create a New User on Multiple Nodes" task as needed.

Note
You must add the same user name and password to each node that a user will access.

Step 3 Complete the DLP-G282 Viewing and Terminating Active Logins as needed.

Step 4 If you want to modify the security policy settings, including password aging and idle user timeout policies, complete the NTP-G88 Modify Users and Change Security procedure.

Stop. You have completed this procedure.

DLP-G54 Create a Local User on a Single Node Using CTC

Purpose	This task creates a local user on a single node.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Superuser only

Procedure

Step 1 In node view or network view, click the **Provisioning** > **Security** > **Users** tabs.

Step 2 In the Users window, click **Create**.

Step 3 In the Create User dialog box, enter the following:

- Name—Type the user name. The user name must be a minimum of six and a maximum of 40 characters (only up to 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot). For TL1 compatibility, the user name must be of 6 to 10 characters.
- Password—Type the user password.

  Note
  The password change of root user is not supported from CTC.

  The minimum password length for CTC is six and maximum of 127 characters. To set the maximum length of a password, refer to . The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any character. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: **RETRIEVE**, **MAINTENANCE**, **PROVISIONING**, or **SUPERUSER**.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G55 Creating a New User on Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15454 nodes managed by CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note All nodes where you want to add users must be accessible in network view.

Procedure

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning** > **Security** > **Users** tabs.

Step 3 In the Users window, click **Create**.

Step 4 In the Create User dialog box, enter the following:

- Name—Type the user name. The user name must be a minimum of six and a maximum of 40 characters (only up to 39 characters for the TACACS and RADIUS authentication). It includes alphanumeric (a-z, A-Z, 0-9) characters and the allowed special characters are @, " - " (hyphen), and " . " (dot). For TL1 compatibility, the user name must be of 6 to 10 characters.
- Password—Type the user password.

  The password length, by default, is set to a minimum of six and a maximum of 127 characters. To set the maximum length of a password, refer to Setting Maximum Password Length Using CTC, on page 15. The minimum length can be set to two, four, eight, ten or twelve characters, and the maximum length to 127 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #,%) characters, where at least two characters are not alphabetic and at least one character is a special character; or the password can contain any character. The password must not contain the user name.
- Confirm Password—Type the password again to confirm it.
- Security Level—Choose a security level for the user: **RETRIEVE**, **MAINTENANCE**, **PROVISIONING**, or **SUPERUSER**.

  Note
  Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the NTP-G88 Modify Users and Change Security procedure.

  TACACS idle timeout considerations:

  - From release 11.1.2.3 onwards, the TACACS server sends the idle timeout value in the minute unit. Previously, the idle timeout value was measured in the second unit. After you upgrade to release 11.1.2.3, the idle timeout unit gets adjusted to minute unit from the second unit.

    Example: On the TACACS server, the idle timeout value of 900 seconds gets changed to 15 minutes after you upgrade to release 11.1.2.3.
  - The default idle timeout value on the TACACS server is 60 minutes. If you set an idle timeout value on the ISE/ACS TACACS server, the TACACS authenticated sessions expire once the idle timeout value is reached. However, the CTC sessions remain open if the CTC client is active after the idle timeout is expired.

Step 5 In the Select Applicable Nodes area, deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 6 Click **OK**.

Step 7 In the User Creation Results dialog box, verify that the user was added to all the nodes chosen in Step 5. If not, click **OK** and repeat Steps 2 through 6. If the user was added to all nodes, click **OK** and continue with the next step.

Step 8 Return to your originating procedure (NTP).

Setting Maximum Password Length Using CTC

Purpose	This task sets the maximum password length for a local user.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view, click the **Provisioning** > **Security** > **Policy** tabs.

Step 2 In the **Password Complexity** area, click **Maximum Length** drop-down list and choose the desired maximum length for password.

Note
The maximum password length for CTC is of 20, 80, or 127 characters.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

NTP-G24 Setting Up Node Identification Information

Purpose	This procedure provisions node identification information, including the node name, node alias, a contact name with phone number, the location of the node, and the date, time, and time zone.
Tools/Equipment	None

Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Log into the node that is to be turned up. If you are already logged in, go to Step 2.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

Step 3 In the Node Name/TID field, type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric (a-z, A-Z, 0-9) characters.

Note
To avoid errors when you import the Cisco Transport Planner configuration file using the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51, the CTC node name and the Cisco Transport Planner site name must either be the same or at least easy to identify.

Step 4 (Optional) In the Contact field, type the name of the node contact person and the phone number, using up to 255 characters.

Step 5 (Optional) In the Node Alias field, type the alias of the node, up to 128 characters. For TL1 compliance, the alias must not contain any commas, colons, or semi-colons. It does not support any international characters set.

Note
Node alias is displayed when the node is in the discovered state. It shows as a tool tip in the Network Map and Explorer Tree of the CTC. It also shows as a separate column in the Tab View pane of the Network view.

Step 6 (Optional) In the Latitude field, enter the node latitude: N (north) or S (south), degrees, and minutes.

Step 7 (Optional) In the Longitude field, enter the node longitude: E (east) or W (west), degrees, and minutes.

Note
The latitude and longitude values indicate only the geographical position of the nodes in the actual network and not the CTC node position.

Step 8 (Optional) In the Description field, type a description of the node. The description can be a maximum of 255 characters.

Step 9 (Optional) Check the Use NTP/SNTP Server check box if you want CTC to use a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node. Using an NTP or SNTP server ensures that all the network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

a) If you check the Use NTP/SNTP Server check box, complete the following fields:

- Use NTP/SNTP Server—Type the IP address of the primary NTP/SNTP server connected to the chassis or of another ONS 15454/15600/15310-CL/15310-MA as GNE with NTP/SNTP enabled that is connected to the ONS 15454 ENE.
- Backup NTP/SNTP Server—Type the IP address of the secondary NTP/SNTP server connected to the chassis or of another ONS 15454/15600/15310-CL/15310-MA as GNE with NTP/SNTP enabled that is connected to the ONS 15454 ENE.

  When the primary NTP/SNTP server fails or is not reachable, the node uses the secondary NTP/SNTP server to synchronize its date and time. If both the primary and secondary NTP/SNTP servers fail or are not reachable, an SNTP-FAIL alarm is raised. The node checks for the availability of the primary or secondary NTP/SNTP server at regular intervals until it can get the time from any one of the NTP/SNTP servers. After the node gets the time from any one server, it synchronizes its date and time with the server's date and time and the SNTP-FAIL alarm is cleared. For each retry and resynchronization, the node checks the availability of the primary NTP/SNTP server first, followed by the secondary NTP/SNTP server. The node synchronizes its date and time every hour.

  Note
  You will not be able to identify which NTP/SNTP server is being used for synchronization.

  Note
  If you plan to check gateway network element (GNE) for the SOCKS proxy server (see DLP-G56 Provisioning IP Settings, on page 20), external nodes must reference the gateway for NTP/SNTP timing. For more information about the gateway settings, refer to "Manage Network Connectivity" chapter.

  Caution
  If you reference another ONS 15454 for the NTP/SNTP server, make sure that the second ONS 15454 references an NTP/SNTP server and not the first ONS 15454 (that is, do not create an NTP/SNTP timing loop by having two ONS 15454 nodes reference each other).

b) If you do not check Use SNTP/NTP Server, complete the Date and Time fields. The node will use these fields for alarm dates and times. By default, CTC displays all alarms in the CTC computer time zone for consistency. To change the display to the node time zone, complete the DLP-G118 Display Alarms and Conditions Using Time Zone task.

- Date—Type the current date in the format m/d/yyyy, for example, September 24, 2002 is 9/24/2002.
- Time—Type the current time in the format hh:mm:ss, for example, 11:24:58. The node uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.

Step 10 Click the Time Zone field and choose a city within your time zone from the drop-down list. The list displays the 80 World Time Zones from –11 through 0 (GMT) to +14. Continental United States time zones are GMT-05:00 (Eastern), GMT-06:00 (Central), GMT-07:00 (Mountain), and GMT-08:00 (Pacific).

Step 11 Check the Use Daylight Savings Time check box if the time zone that you chose uses Daylight Savings Time.

Note
The Insert AIS-V on STS-1 SD-P and SD-P BER field are not used in DWDM networks.

Step 12 Click **Apply**.

Step 13 In the confirmation dialog box, click **Yes**.

Step 14 Review the node information. If you need to make corrections, repeat Steps 3 through 12 to enter corrections. If the information is correct, continue with the NTP-G25 Setting Battery Power Monitor Thresholds, on page 18.

Stop. You have completed this procedure.

NTP-G25 Setting Battery Power Monitor Thresholds

Purpose	This procedure provisions extreme high, low, and extreme low input battery power thresholds within a –48 VDC environment.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The default battery voltage thresholds are normally not changed. Threshold changes should only be performed at the direction of your site administrator.

Note When you change the battery voltage thresholds, alarms are raised twice with incorrect severity.

Note In Release 11.12, you can set the ECU voltage threshold for an ECU-48V to a maximum of 60V. However, it is recommended not to exceed 57.5V.

The voltage threshold range for each battery is -40.5 to -72.0.

Note When the thresholds are crossed, the control card generates warning alarms in CTC. For power specifications, see the Hardware Specifications.

Procedure

Step 1 Login to the node that you will set up. If you are already logged in, continue with Step 2.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning** > **General** > **Power Monitor** tabs.

Note
In multishelf mode, power monitor thresholds must be provisioned separately for each shelf within the multishelf including the node controller and all subtending shelves.

Step 3 To change the extreme low battery voltage threshold in 0.5 VDC increments, choose a voltage from the ELWBATVGVdc drop-down list. The default value is -40.5.

Step 4 To change the low battery voltage threshold in 0.5 VDC increments, choose a voltage from the LWBATVGVdc drop-down list. The default value is -44.

Step 5 To change the high battery voltage threshold in 0.5 VDC increments, choose a voltage from the HIBATVGVdc drop-down list. The default value is -54.

Step 6 To change the extreme high battery voltage threshold in 0.5 VDC increments, choose a voltage from the EHIBATVGVdc drop-down list. The default value is -56.5.

Step 7 Click **Apply**.

Stop. You have completed this procedure.

NTP-G26 Setting Up CTC Network Access

Purpose	This procedure provisions network access for a node, including its subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) server, Internet Inter-Orb Protocol (IIOP) listener port, gateway settings, static routes, Open Shortest Path First (OSPF) protocol, Routing Information Protocol (RIP), and designated SOCKS servers.
Tools/Equipment	None
Prerequisite Procedures	NTP-G22 Verifying Common Card Installation, on page 4
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 Complete the DLP-G46 Log into CTC task. If you are already logged in, continue with Step 2.

Step 2 Complete the DLP-G56 Provisioning IP Settings, on page 20 to provision the ONS 15454 IP address, subnet mask, default router, DHCP server, IIOP listener port, and SOCKS proxy server settings.

If you cannot log into the node, you can change its IP address, default router, and network mask by using the LCD on the ONS 15454 fan-tray assembly (unless LCD provisioning is suppressed). See the DLP-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD, on page 25 for instructions. However, you cannot use the LCD to provision any other network settings. In an ONS 15454 M2 shelf assembly, the LCD is on the fan-tray assembly. In a ONS 15454 M6 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU). In a ONS 15454 M15 shelf assembly, the LCD unit is integrated with the fan tray assembly

Note
When accessing CTC from a machine running Windows XP operating system, CTC may sometimes fail to reconnect to a GNE when the GNE proxies for several ENE nodes (approximately 15 ENE nodes). This can happen when there is a side switch or when the LAN is enabled/disabled. This is due to the Windows XP operating system limiting the number of simultaneous TCP/IP connection attempts. As a workaround, close the existing CTC session and relaunch CTC on the GNE node. You can configure a designated socks server list on the CTC to mitigate the problem.

Step 3 If the control cards are installed and you want to turn on the secure mode, which allows two IP addresses to be provisioned for the node, complete the DLP-G264 Enabling Node Security Mode, on page 28. Secure mode is not available if TCC2 cards are installed.

Step 4 If static routes are needed, complete the DLP-G58 Creating a Static Route, on page 30. For more information about static routes, see Managing Network Connectivity.

Step 5 If the ONS 15454 is connected to a LAN or WAN that uses OSPF and you want to share routing information between the LAN or WAN and the ONS network, complete the DLP-G59 Setting Up or Changing Open Shortest Path First Protocol, on page 31.

Step 6 If the ONS 15454 is connected to a LAN or WAN that uses RIP, complete the DLP-G60 Setting Up or Changing Routing Information Protocol, on page 33.

Step 7 Complete the DLP-G439 Provisioning the Designated SOCKS Servers, on page 24 after the network is provisioned and one or more of the following conditions exist:

- SOCKS proxy is enabled.
- The ratio of ENEs to GNEs is greater than eight to one.
- Most ENEs do not have LAN connectivity.

Stop. You have completed this procedure.

DLP-G56 Provisioning IP Settings

Purpose	This task provisions IP settings, which includes the IP address, IP address version, default router, DHCP access, firewall access, and SOCKS proxy server settings for ONS 15454 node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC

Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution All network changes should be approved by your network (or LAN) administrator.

Caution Verify that the IPv4 or IPv6 addresses assigned to the node are unique in the network. Duplicate IP addresses in the same network cause loss of visibility.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **General** tabs.

Step 2 Complete the following information in the fields listed:

- IP Address—Type the IP address assigned to the ONS 15454 node.

  Note
  If the control cards are installed, dual IP addressing is available using the secure mode. When secure mode is off (sometimes called repeater mode), the IP address entered in the IP Address field applies to the backplane LAN port (ONS 15454), EMS RJ-45 port or Craft port on the ECU (ONS 15454 M6), EMS RJ-45 port on the power module (ONS 15454 M2), and the control card (LAN) port. When secure mode is on, the IP Address field shows the address assigned to the control card (LAN) port and the Superuser can enable or disable display of the backplane IP address. See the DLP-G264 Enabling Node Security Mode, on page 28 as needed. See Managing Network Connectivity chapter for more information about secure mode.

- Net/Subnet Mask Length—Type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length.
- MAC Address—(Display only) Displays the IEEE 802 MAC address.

  Note
  In secure mode, the front and back TCP/IP (LAN) ports are assigned different MAC addresses, and the backplane information can be hidden or revealed by a Superuser.

- Default Router—If the node is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the node cannot directly access. This field is ignored if any of the following are true:
  - The node is not connected to a LAN.
  - The SOCKS proxy server is enabled and the node is provisioned as an end network element (ENE).
  - OSPF is enabled on both the node and the LAN where the node is connected. (OSPF is provisioned in the DLP-G59 Setting Up or Changing Open Shortest Path First Protocol, on page 31.)

- LCD IP Setting—Choose one of the following:
  - **Allow Configuration**—Displays the node IP address on the LCD and allows users to change the IP settings using the LCD. This option enables the DLP-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD, on page 25.
  - **Display Only**—Displays the node IP address on the LCD but does not allow users to change the IP settings using the LCD.
  - **Suppress Display**—Suppresses the node IP address display on the LCD.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from appearing in CTC to users with Provisioning, Maintenance, or Retrieve security levels. (The IP address suppression is not applied to users with Superuser security level.)

  Note
  IP address suppression is not applied to users with Superuser security level. However, in secure mode the backplane IP address visibility can be restricted to only a locally connected Superuser viewing the routing table. In this case, the backplane IP address is not revealed to any user at any other NE, either on the routing table or in autonomous messages (such as the TL1 REPT DBCHG message, alarms, and performance monitoring [PM] reporting).
- IPv6 Configuration—Allows provisioning of IPv6 addresses. After you provision an IPv6 address, you can access the device using the IPv6 address. Configure these settings only if you want to enable IPv6 on the node. IPv6 cannot be configured using the LCD push buttons.
  - Enable IPv6—Select this check box to assign an IPv6 address to the node. The IPv6 Address, Prefix Length, and IPv6 Default Router fields are enabled only if this check box is selected. The check box is disabled by default.

    Note
    Enable SOCKS Proxy on Port check box is enabled when you enable IPv6 and can be disabled only when IPv6 is disabled.

    Note
    By default, when IPv6 is enabled, the node processes both IPv4 and IPv6 packets on the LAN interface. If you want the node to process only IPv6 packets, you need to disable IPv4 on the node. For more information, see DLP-G317 Change Node Access and PM Clearing Privilege.
  - IPv6 Address—Enter the IPv6 address that you want to assign to the node. This IP address is the global unicast IPv6 address. This field is disabled if the Enable IPv6 check box is not selected.
  - Prefix Length—Enter the prefix length of the IPv6 address. This field is disabled if the Enable IPv6 check box is not selected.
  - IPv6 Default Router—Enter the IPv6 address of the default router of the IPv6 NE. This is optional. This field is disabled if the Enable IPv6 check box is not selected.

    Note
    The DWDM node uses NAT-PT internally to support native IPv6. NAT-PT uses the IPv4 address range 128.0.0.0 to 128.0.1.254 for packet translation. Do not use this address range when you enable IPv6 feature.

    Note

You can provision IPv6 in secure or nonsecure mode. To enable secure mode, see DLP-G264 Enabling Node Security Mode, on page 28.

- Forward DHCP Request To—Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the SOCKS proxy server features, do not check this check box.

  Note
  If you enable DHCP, computers connected to the node can obtain temporary IP addresses from an external DHCP server. The node only forwards DHCP requests; it does not act as a DHCP server.

- Gateway Settings—Provisions the SOCKS proxy server features. (SOCKS is a standard proxy protocol for IP-based applications.) Do not change these options until you review Scenario 7 “Provisioning the ONS 15454 Proxy Server” in "Manage Network Connectivity" chapter. In SOCKS proxy server networks, the node is either an ENE, a GNE, or a proxy-only server. Provisioning must be consistent for each NE type.

- Enable SOCKS proxy server on port—If checked, the node serves as a proxy for connections between CTC clients and nodes that are connected by data communications channels (DCCs) to the proxy node. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes; it only requires IP connectivity to the proxy node. If the Enable SOCKS proxy server on port check box is unchecked, the node does not proxy for any CTC clients. When this box is checked, you can provision one of the following options:

  - **External Network Element (ENE)**—Choose this option when the node is not connected to a LAN but has DCC connections to other nodes. A CTC computer connected to the ENE through the control card TCP/IP (craft) port can manage nodes that have DCC connections to the ENE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN or WAN that those nodes might be connected to.

  - **Gateway Network Element (GNE)**—Choose this option when the node is connected to a LAN and has DCC connections to other nodes. A CTC computer connected to the LAN can manage all nodes that have DCC connections to the GNE, but the CTC computer does not have direct IP connectivity to them. The GNE option isolates the LAN from the DCC network so that IP traffic originating from the DCC-connected nodes and any CTC computers connected to them is prevented from reaching the LAN.

  - **SOCKS proxy only**—Choose this option when the node is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS proxy only option is the same as the GNE option, except that the SOCKS proxy only option does not isolate the DCC network from the LAN.

    Note
    If a node is provisioned in secure mode, it is automatically provisioned as a GNE with SOCKS proxy enabled. However, this provisioning can be overridden, and the secure node can be changed to an ENE. In secure mode, SOCKS cannot be disabled. For information about provisioning, including GNE and ENE status, see the DLP-G264 Enabling Node Security Mode, on page 28.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

The control cards reboot one at a time if changes were made to the IP address, subnet mask, or gateway settings. During this time (approximately 5 to 6 minutes), the active and standby control card LEDs will blink,

turn on, and turn off at different intervals. Eventually, a “Lost node connection, switching to network view” message appears.

Step 5 Click **OK**. The network view appears. The node icon appears in gray, during which time you cannot access the node.

Step 6 Double-click the node icon when it becomes green.

Step 7 Return to your originating procedure (NTP).

DLP-G439 Provisioning the Designated SOCKS Servers

Purpose	This task identifies the ONS 15454 SOCKS servers in SOCKS-proxy-enabled networks. Identifying the SOCKS servers reduces the amount of time required to log into a node and have all NEs appear in network view (NE discovery time). The task is recommended when the combined CTC login and NE discovery time is greater than five minutes in networks with SOCKS proxy enabled. Long (or failed) login and NE discovery times can occur in networks that have a high ENE-to-GNE ratio and a low number of ENEs with LAN connectivity.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To complete this task, you must have either the IP addresses or DNS names of all the nodes in the network with LAN access that have SOCKS proxy enabled.

Note SOCKS proxy servers can be any accessible ONS network nodes that have LAN access, including the ONS 15310-MA, ONS 15310-CL, ONS 15454, ONS 15454 SDH, ONS 15600, ONS 15600 SDH, ONS 15454 M6, and ONS 15454 M2 nodes.

Note You must repeat this task any time that changes to SOCKS proxy server nodes occur, for example, whenever LAN connectivity is added to or removed from a node, or when nodes are added or removed from the network.

Note If you cannot log into a network node, complete the DLP-G46 Log into CTC task choosing the Disable Network Discovery option. Complete this task, then login again with network discovery enabled.

Procedure

Step 1 From the CTC Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **SOCKS** tab.

Step 3 In the Designated SOCKS Server field, type the IP address or DNS node name of the first SOCKS server. The server that you enter must have SOCKS proxy server enabled, and it must have LAN access.

Step 4 Click **Add**. The node is added to the SOCKS server list. If you need to remove a node on the list, click **Remove**.

Step 5 Repeat Steps 3 and 4 to add all qualified nodes within the network. Add all the nodes that have SOCKS proxy enabled and are connected to the LAN.

Step 6 Click **Check All Servers**. CTC verifies that all nodes can perform as SOCKS servers. Once verified, a check is placed next to the node IP address or node name in the SOCKS server list. An X placed next to the node indicates one or more of the following:

- The entry does not correspond to a valid DNS name.
- The numeric IP address is invalid.
- The node cannot be reached.
- The node can be reached, but the SOCKS port cannot be accessed, for example, a firewall problem might exist.

Step 7 Click **Apply**. The list of nodes, including ones that received an X in Step 6, are added as SOCKS servers.

Step 8 Click **OK** to close the Preferences dialog box.

Step 9 Return to your originating procedure (NTP).

DLP-G57 Setting the IP Address, Default Router, and Network Mask Using the LCD

Purpose	This task changes the ONS 15454 IP address, default router, and network mask using the LCD on the fan-tray assembly. Use this task if you cannot log into CTC. In a ONS 15454 M2 shelf assembly, the LCD is on the fan-tray assembly. In a ONS 15454 M6 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU). In a ONS 15454 M15 shelf assembly, the LCD unit is integrated with the fan tray assembly.
Tools/Equipment	None
Prerequisite Procedures	DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card

Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note You cannot perform this task if the LCD IP Display field on the node view Provisioning > Network tab is set to Display Only or Suppress Display. See the DLP-G56 Provisioning IP Settings, on page 20 to view or change the LCD IP Display field. If the node is locked in secure mode with the LCD display disabled, you will not be able to change this provisioning unless the lock is disabled by Cisco Technical Support. See Managing Network Connectivity chapter for more information about secure mode.

Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

Procedure

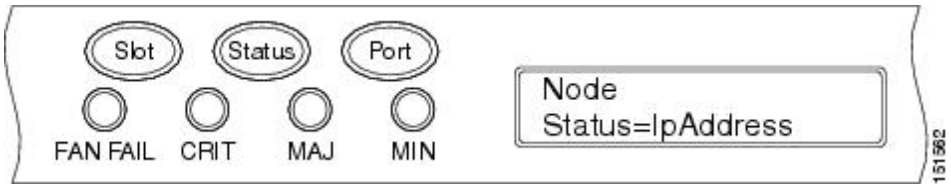
Step 1 On the ONS 15454 front panel, repeatedly press the **Slot** button until SHELF appears on the first line of the LCD. You are in the Shelf menu.

Note
In a ONS 15454 M2 shelf assembly, the LCD panel and the **Slot**, **Port**, and **Status** buttons are present on the fan-tray assembly. In a ONS 15454 M6 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU); the **Slot**, **Port**, and **Status** buttons are present on the LCD unit. In a ONS 15454 M15 shelf assembly, the **Slot**, **Port**, and **Status** buttons are present on the LCD unit that is integrated with the fan tray assembly.

Step 2 Repeatedly press the **Port** button until the following information appears:

- To change the node IP address, Node Status=IpAddress
- To change the node network mask, Node Status=Net Mask
- To change the default router IP address, Node Status=Default Rtr

Figure 1: Selecting the IP Address Option

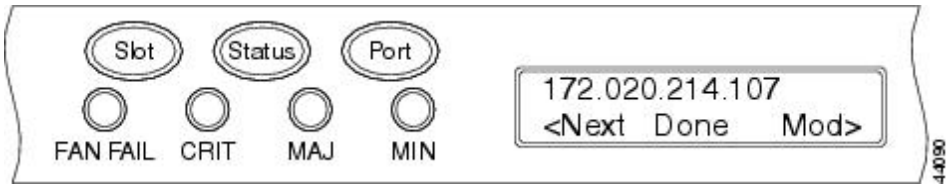


Step 3 Press the **Status** button to display the node IP address, the node subnet mask length, or the default router IP address.

The following IP addresses are displayed in the LCD one after the other:

- Regular IP—Node IP address that is used to access the node when the controller card is in nonsecure mode.
- Secure IP (15454 secure mode IP)—IP address that is assigned to the backplane LAN port. This port connects the node to an operations support system (OSS) through a central office LAN or private enterprise network. This IP address becomes a private address in the secure mode and prevents the front-access craft port user from accessing the LAN through the backplane port.

Figure 2: Changing the IP Address



Step 4 Push the **Slot** button to move to the digit of the IP address, subnet mask, or default router that you want to change. The selected digit flashes.

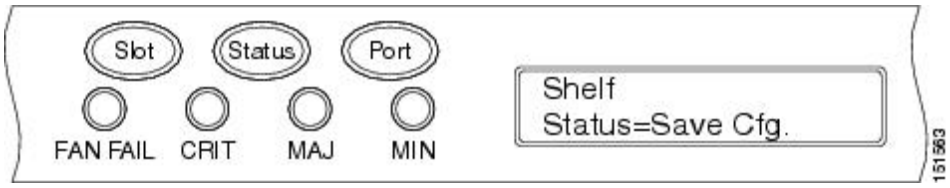
Tip The Slot, Status, and Port button positions correspond to the positions of the commands shown on the LCD. For example, you press the Slot button to invoke the Next command and the Status button to invoke the Done command.

Step 5 Press the **Port** button to cycle the IP address, subnet mask, or default router to the correct digit.

Step 6 When the change is complete, press the **Status** button to return to the relevant Node Status menu.

Step 7 Repeatedly press the **Port** button until the Shelf Save Configuration option appears.

Figure 3: Selecting the Save Configuration Option



Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears.

Figure 4: Saving and Rebooting the Control Card



Step 9 Press the **Slot** button to apply the new IP address, subnet mask, or default router configuration or press **Port** to cancel the configuration.

Note
The IP address and default router must be on the same subnet. If not, you cannot apply the configuration.

Step 10 Saving the new configuration causes the control cards to reboot. During the reboot, a message appears on the LCD. The LCD returns to the normal alternating display after both the control cards finish rebooting.

Step 11 Return to your originating procedure (NTP).

DLP-G264 Enabling Node Security Mode

Purpose	This task enables the security mode. When security mode is enabled, two IP addresses are assigned to the node. One address is assigned to the backplane LAN port (ONS 15454) or to the EMS port (ONS 15454 M2 and ONS 15454 M6). The other address is assigned to the RJ-45 TCP/IP (LAN) port of the control cards. The TCC2 card does not support security mode. The security mode options are not available in CTC if TCC2 cards or a mix of TCC2 and TCC2P cards are installed.
Tools/Equipment	The control cards must be installed.
Prerequisite Procedures	• NTP-G103 Backing Up the Database • DLP-G46 Log into CTC `
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution The IP address assigned to the control card TCP/IP (LAN) port must reside on a different subnet from the backplane LAN port (ONS 15454) and the EMS port (ONS 15454 M2 and ONS 15454 M6). Verify that the new control card IP address meets this requirement.

Note The node will reboot after you complete this task, causing a temporary disconnection between the CTC computer and the node.

Note If an OTS-to-OTS PPC is created between nodes, it will no longer function if the node Security Mode is enabled. The reason for this is that if the Secure mode is enabled, it is no longer possible for the DCN extension feature to use the LAN interface to extend the internal network (due to the network isolation in this configuration mode). The result is that the topology discovery on the OTS-to-OTS PPC no longer operates.

Procedure

Step 1 Click the **Provisioning** > **Security** > **Data Comm** tabs.

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode page, then click **Next**.

Step 4 On the Ethernet Port page, enter the IP address and subnet mask for the the control card LAN port.

Step 5 Click **Next**.

Step 6 If needed, on the Backplane Ethernet Port page, modify the backplane IP address, subnet mask, and default router. You normally do not modify these fields if no network changes have occurred.

Step 7 Click **Next**.

Step 8 On the SOCKS Proxy Server Settings page, choose one of the following options:

- **External Network Element (ENE)**—If selected, the CTC computer is only visible to the ONS 15454 where the CTC computer is connected. The CTC computer is not visible to the nodes connected to the DCC. In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
- **Gateway Network Element (GNE)**—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port.

Note
The SOCKS proxy server is automatically enabled when you enable secure mode.

Step 9 Click **Finish**.

Within the next 30 to 40 seconds, the control cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and a DISCONNECTED condition appears in the Alarms tab.

Step 10 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)

Step 11 After the DISCONNECTED condition clears, complete the following steps to suppress the backplane IP address from appearing in CTC and the LCD. If you do not want to suppress the backplane IP address display, continue with Step 12.

a) Display the node in node view (single-shelf mode) or multishelf view (multishelf mode).
b) Click the **Provisioning** > **Security** > **Data Comm** tabs.
c) In the LCD IP Setting field, choose **Suppress Display**. The IP address will not appear on the LCD.
d) Check the **Suppress CTC IP Address** check box. The IP address will not appear in the CTC information area or the Provisioning > Security > Data Comm tabs.
e) Click **Apply**.

Note
After you turn on secure mode, the control card IP address becomes the node IP address.

Step 12 Return to your originating procedure (NTP).

DLP-G58 Creating a Static Route

Purpose	This task creates a static route to establish CTC connectivity to a computer on another network. This task is performed when one of the following conditions exists: • CTC computers on one subnet need to connect to ONS 15454 nodes that are connected by a router to ONS 15454 nodes residing on another subnet. • OSPF is not enabled (the OSPF Active on LAN check box is not checked on the Provisioning > Network > OSPF tab) and the External Network Element (ENE) gateway setting is not checked. • You need to enable multiple CTC sessions among ONS 15454 nodes residing on the same subnet and the External Network Element (ENE) gateway setting is not checked.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** tabs.

Step 2 Click the **Static Routing** tab. Click **Create**.

Step 3 In the Create Static Route dialog box, enter the following:

- Destination—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- Mask—Enter a subnet mask. If the destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.
- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the node and the computer.

Step 4 Click **OK**. Verify that the static route appears in the Static Route window.

Note

Static route networking examples are provided in the Managing Network Connectivity chapter.

Step 5 Return to your originating procedure (NTP).

DLP-G59 Setting Up or Changing Open Shortest Path First Protocol

Purpose	This task enables the OSPF routing protocol on the ONS 15454. Perform this task if you want to include the ONS 15454 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15454 is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **OSPF** tabs.

Step 2 On the top left side of the OSPF area, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15454 nodes as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.

  ANSI Nodes

- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the Section DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 100.

- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

  ETSI Nodes

- RS-DCC Metric—This value is normally unchanged. It sets a cost for sending packets across the regenerator section DCC (RS-DCC), which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default RS-DCC metric is 100.

- MS-DCC Metric—Sets a cost for sending packets across the multiplex section DCC (MS-DCC). This value should always be lower than the SDCC metric. The default MS-DCC metric is 33. It is usually not changed.

Step 3 In the OSPF on LAN area, complete the following:

- OSPF active on LAN—When checked, enables the ONS 15454 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454 nodes that directly connect to OSPF routers.
- LAN Port Area ID—Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15454 is connected. (This number is different from the DCC/GCC OSPF Area ID.)

Step 4 By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.

a) Click the **No Authentication** button.
b) In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.
- Confirm Authentication Key—Enter the same password to confirm it.

c) Click **OK**.

The authentication button label changes to Simple Password.

Step 5 Provision the OSPF priority and interval settings. The OSPF priority and interval defaults are the defaults most commonly used by OSPF routers. Verify that these defaults match the ones used by the OSPF router where the ONS 15454 is connected.

- Router Priority—Provision the router priority, which determines the designated router for a subnet.
- Hello Interval (sec)—Provision the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Provision the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- Transit Delay (sec)—Provision the service speed. One second is the default.
- Retransmit Interval (sec)—Provision the number of seconds that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Provision the cost for sending packets across the LAN. This value should always be lower than the SDCC or RS-DCC metric. Ten is the default.

Step 6 Under OSPF Area Range Table, create an area range table if one is needed:

Note
Area range tables consolidate the information that is outside an OSPF area border. One node in the ONS 15454 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 OSPF area.

a) Click **Create**.
b) In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the ONS 15454 nodes that reside within the OSPF area. For example, if the ONS 15454 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.

- Range Area ID—Enter the OSPF area ID for the ONS 15454 nodes. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
- Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
- Advertise—Check this box if you want to advertise the OSPF range table.

c) Click **OK**.

Step 7 All OSPF areas must be connected to Area 0. If the ONS 15454 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

a) Under the OSPF Virtual Link Table, click **Create**.

b) In the Create Virtual Link dialog box, complete the following fields. OSPF settings must match OSPF settings for the ONS 15454 OSPF area:

- Neighbor—Enter the router ID of the Area 0 router.
- Transit Delay (sec)—Enter the service speed. One second is the default.
- Hello Int (sec)—Provision the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Auth Type—If the router where the ONS 15454 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Retransmit Int (sec)—Provision the time that will elapse, in seconds, before a packet is resent. Five seconds is the default.
- Dead Int (sec)—Provision the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c) Click **OK**.

Step 8 After entering the ONS 15454 OSPF area data, click **Apply**.

If you changed the Area ID, the control cards reset, one at a time. The reset takes approximately 10 to 15 minutes.

Step 9 Return to your originating procedure (NTP).

DLP-G60 Setting Up or Changing Routing Information Protocol

Purpose	This task enables RIP on the ONS 15454. Perform this task if you want to include the ONS 15454 in RIP-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC You need to create a static route to the router adjacent to the ONS 15454 for the ONS 15454 to communicate its routing information to non-DCC-connected nodes.

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Network** > **RIP** tabs.

Step 2 Check the **RIP Active** check box if you are activating RIP.

Step 3 Choose either RIP Version 1 or RIP Version 2 from the drop-down list, depending on which version is supported in your network.

Step 4 Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 5 By default, RIP is set to No Authentication. If the router that the ONS 15454 is connected to requires authentication, complete the following steps. If not, continue with Step 6.

a) Click the **No Authentication** button.

b) In the Edit Authentication Key dialog box, complete the following:

- Type—Choose **Simple Password**.
- Enter Authentication Key—Enter the password.
- Confirm Authentication Key—Enter the same password to confirm it.

c) Click **OK**.

The authentication button label changes to Simple Password.

Step 6 If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the ONS 15454 is a gateway NE with multiple external ONS 15454 NEs attached with IP addresses in different subnets.

a) In the RIP Address Summary area, click **Create**.

b) In the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.
- Mask Length—Enter the subnet mask length using the up and down arrows.
- Hops—Enter the number of hops. The smaller the number of hops, the higher the priority.

c) Click **OK**.

Step 7 Return to your originating procedure (NTP).

NTP-G194 Setting Up EMS Secure Access to the Node

Purpose	This procedure provisions nodes and CTC computers for secure access.
Tools/Equipment	None
Prerequisite Procedures	NTP-G26 Setting Up CTC Network Access, on page 19
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 In node view, click the **Provisioning** > **Security** > **Access** pane.

Step 2 Under the **EMS Access** area, change the **Access State** to **Secure**.

Step 3 Click **Apply**. The CTC disconnects and reconnects through a secure socket connection.

Step 4 To create a secure connection, enter **https://node-address**.

Note
After setting up a CTC connection in secure mode, http requests are automatically redirected to https mode.

Step 5 A first time connection is authenticated by the **Website Certification is Not Known** dialog box. Accept the certificate and click **OK**. The **Security Error: Domain Name Mismatch** dialog box appears. Click **OK** to continue.

Stop. You have completed this procedure.

NTP-G27 Setting Up the Node for Firewall Access

Purpose	This procedure provisions ONS 15454 nodes and CTC computers for access through firewalls.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

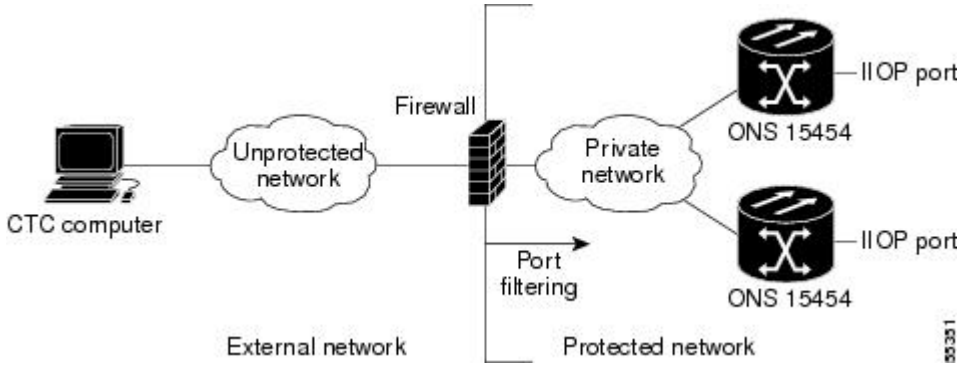
Procedure

Step 1 Log into a node that is behind the firewall. If you are already logged in, continue with Step 2.

Step 2 If the node is in a protected network and the CTC computer is in an external network, complete the DLP-G61 Provisioning the IIOP Listener Port on the ONS 15454, on page 38.

The following figure shows nodes in a protected network and the CTC computer in an external network. For the computer to access the nodes, you must provision the IIOP listener port specified by your firewall administrator on the node.

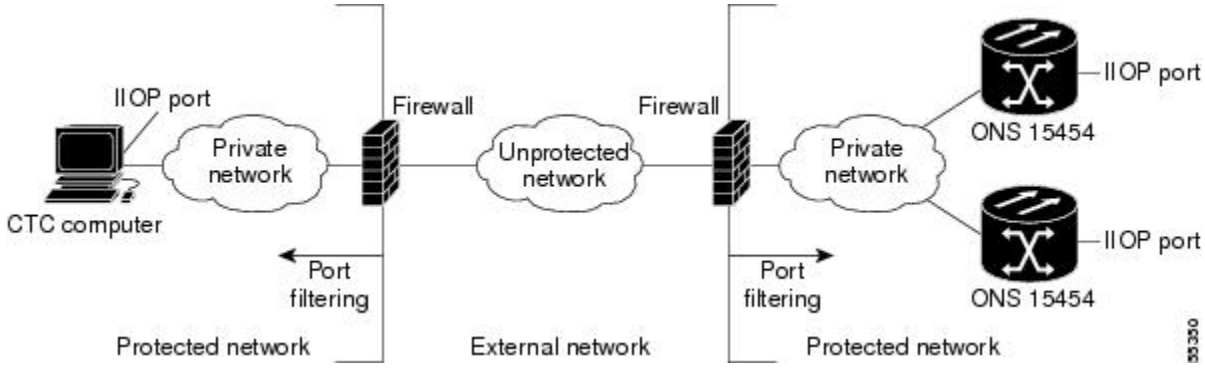
Figure 5: Nodes Behind a Firewall



Step 3 If the CTC computer resides behind a firewall, complete the DLP-G62 Provisioning the IIOP Listener Port on the CTC Computer, on page 39.

The following figure shows a CTC computer and node behind firewalls. For the computer to access the node, you must provision the IIOP port on the CTC computer and on the node.

Figure 6: CTC Computer and Nodes Residing Behind Firewalls



Stop. You have completed this procedure.

NTP-G28 Creating FTP Host

Purpose	This procedure provisions an FTP Host that you can use to perform database backup and restore or software download to an End Network Element (ENE) when proxy or firewall is enabled.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G26 Setting Up CTC Network Access, on page 19 • NTP-G27 Setting Up the Node for Firewall Access, on page 35 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 If you want to turn on the ONS 15454 secure mode, which allows two IPv4 addresses to be provisioned for the node if the control cards are installed, complete the DLP-G264 Enabling Node Security Mode, on page 28. Refer to the Managing Network Connectivity chapter for information about secure mode.

Step 2 In Node view, click the **Provisioning** > **Network** > **FTP Hosts** tabs.

Step 3 Click **Create**.

Step 4 Enter a valid IP address in the FTP Host Address field. A maximum of 12 host can be entered.

Note
In Software Release 9.1 and later, you can configure an IPv6 address for an FTP server, in addition to an IPv4 address.

Step 5 The Mask is automatically set according to the Net/Subnet Mask length specified in DLP-G56 Provisioning IP Settings, on page 20. To change the Mask, click the Up/Down arrows on the Length menu.

Step 6 Check the **FTP Relay Enable** radio button to allow FTP commands at the GNE relay. If you will enable the relay at a later time, go to Step 8. Certain TL1 commands executed on an ENE require FTP access into the Data Communication Network (DCN), the FTP relay on the GNE provides this access. The FTP hosts that you have configured in CTC can be used with the TL1 COPY-RFILE (for database backup and restore or software download) or COPY-IOSCFG (for Cisco IOS Configuration File backup and restore) commands.

Step 7 Enter the time, in minutes, that FTP Relay will be enabled. A valid entry is a number between 0 and 60. The number 0 disallows FTP command relay. After the specified time has elapsed the FTP Relay Enable flag is unset and FTP command relay is disallowed.

Step 8 Click **OK**.

Step 9 Repeat Step 3 through Step 8 to provision additional FTP Hosts.

Stop. You have completed this procedure.

DLP-G61 Provisioning the IIOP Listener Port on the ONS 15454

Purpose	This task sets the IIOP listener port on the ONS 15454shelf which enables you to access nodes that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If the Enable SOCKS proxy on port 1080 check box is checked, CTC will use Port 1080 and ignore the configured IIOP port setting. If the check box is later unchecked, the configured IIOP listener port will be used.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Security** > **Access** tabs.

Step 2 In the TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 to connect to the nodes on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is available.
- **Standard Constant**—Uses Port 683, the Common Object Request Broker Architecture (CORBA) default port number.
- **Other Constant**—If Port 683 is not used, type the IIOP port specified by your firewall administrator.

Step 3 Click **Apply**.

Step 4 When the Change Network Configuration message appears, click **Yes**.

The control cards reboot, one at a time. The reboot takes approximately 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-G62 Provisioning the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port for CTC and must be completed if the computer running CTC resides behind a firewall.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 From the Edit menu, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Firewall** tab.

Step 3 In the CTC CORBA (IIOP) Listener Port area, choose a listener port option:

- **Default - Variable**—Use to connect to ONS 15454 nodes from within a firewall or if no firewall is used (default).
- **Standard Constant**—Use Port 683, the CORBA default port number.
- **Other Constant**—If Port 683 is not used, enter the IIOP port defined by your administrator.

Step 4 Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.

Step 5 Click **OK**.

Step 6 In the Preferences dialog box, click **OK**.

Step 7 To access the ONS 15454 using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit** from the File menu).

Step 8 Return to your originating procedure (NTP).

NTP-G132 Provisioning OSI

Purpose	This procedure provisions the ONS 15454 so it can be installed in networks with other vendor NEs that use the OSI protocol stack for data communications network (DCN) communications. This procedure provisions the Target Identifier Address Resolution Protocol (TARP), OSI routers, manual area addresses, subnetwork points of attachment, and IP-over-Connectionless Network Service (CLNS) tunnels.

Tools/Equipment	None
Prerequisite Procedures	• DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution This procedure requires an understanding of OSI protocols, parameters, and functions. Before you begin, review the OSI reference sections in the Managing Network Connectivity chapter and ensure that you know the role of the ONS 15454 within the OSI and IP network.

Note This procedure requires provisioning of non-ONS equipment including routers and third party NEs. Do not begin until you have the capability to complete that provisioning.

Procedure

As needed, complete the following tasks:

- DLP-G283 Provisioning OSI Routing Mode, on page 41—Complete this task first.
- DLP-G284 Provisioning the TARP Operating Parameters, on page 42—Complete this task second.
- DLP-G285 Adding a Static TID-to-NSAP Entry to the TARP Data Cache, on page 44—Complete this task as needed.
- DLP-G287 Adding a TARP Manual Adjacency Table Entry, on page 45—Complete this task as needed.
- DLP-G288 Provisioning OSI Routers, on page 46—Complete this task as needed.
- DLP-G289 Provisioning Additional Manual Area Addresses, on page 47—Complete this task as needed.
- DLP-G290 Enabling the OSI Subnet on the LAN Interface, on page 48—Complete this task as needed.
- DLP-G291 Creating an IP-Over-CLNS Tunnel, on page 49—Complete this task as needed.

Stop. You have completed this procedure.

DLP-G283 Provisioning OSI Routing Mode

Purpose	This task provisions the OSI routing mode. Complete this task when the ONS 15454 is connected to networks with third party NEs that use the OSI protocol stack for DCN communication.
Tools/Equipment	None
Prerequisite Procedures	• DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution Do not complete this task until you confirm the role of the node within the network. It will be either an End System, Intermediate System Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to Managing Network Connectivity chapter.

Caution Link State Protocol (LSP) buffers must be the same at all NEs within the network, or loss of visibility might occur. Do not modify the LSP buffers unless you confirm that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D maximum transmission unit (MTU) size within the OSI area.

Note For ONS 15454 nodes, three virtual routers can be provisioned. The node primary Network Service Access Point (NSAP) address is also the Router 1 primary manual area address. To edit the primary NSAP, you must edit the Router 1 primary manual area address. After you enable Router 1 on the Routers subtab, the Change Primary Area Address button is available to edit the address.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **OSI** tabs.

Step 2 Choose a routing mode:

- **End System**—The ONS 15454 performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.

  Note
  The End System routing mode is not available if more than one virtual router is enabled.

- I**ntermediate System Level 1**—The ONS 15454 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.
- **Intermediate System Level 1/Level 2**—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Step 3 If needed, change the LSP data buffers:

- L1 LSP Buffer Size—Adjusts the Level 1 link state protocol data unit (PDU) buffer size. The default is 512. It should not be changed.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size. The default is 512. It should not be changed.

Step 4 Return to your originating procedure (NTP).

DLP-G284 Provisioning the TARP Operating Parameters

Purpose	This task provisions the TARP operating parameters including TARP PDU propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **OSI** > **TARP** > **Config** tabs.

Step 2 Provision the following parameters, as needed:

- TARP PDUs L1 Propagation—If checked (default), TARP Type 1 PDUs that are received by the node and are not excluded by the LDB are propagated to other NEs within the Level 1 OSI area. (Type 1 PDUs request a protocol address that matches a target identifier [TID] within a Level 1 routing area.) The propagation does not occur if the NE is the target of the Type 1 PDU, and PDUs are not propagated to the NE from which the PDU was received.

  Note
  The TARP PDUs L1 Propagation parameter is not used when the Node Routing Area (on the Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation—If checked (default), TARP Type 2 PDUs that are received by the node and are not excluded by the LDB are propagated to other NEs within the Level 2 OSI areas. (Type 2 PDUs request a protocol address that matches a TID within a Level 2 routing area.) The propagation occurs if the NE is not the target of the Type 2 PDU, and PDUs are not propagated to the NE from which the PDU was received.

  Note
  The TARP PDUs L2 Propagation parameter is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.

- TARP PDUs Origination—If checked (default), the node performs all TARP origination functions including:
  - TID-to-NSAP resolution requests (originate TARP Type 1 and Type 2 PDUs)
  - NSAP-to-TID requests (originate Type 5 PDUs)
  - TARP address changes (originate Type 4 PDUs)

  Note
  TARP Echo and NSAP to TID are not supported.

- TARP Data Cache—If checked (default), the node maintains a TARP data cache (TDC). The TDC is a database of TID-to-NSAP pairs created from TARP Type 3 PDUs received by the node and modified by TARP Type 4 PDUs (TID-to-NSAP updates or corrections). TARP 3 PDUs are responses to Type 1 and Type 2 PDUs. The TDC can also be populated with static entries entered on the TARP > Static TDC tab.

  Note
  TARP Data Cache is only used when the TARP PDUs Origination parameter is enabled.

- L2 TARP Data Cache—If checked (default), the TIDs and NSAPs of NEs originating Type 2 requests are added to the TDC before the node propagates the requests to other NEs.

  Note
  The L2 TARP Data Cache parameter is designed for Intermediate System Level 1/Level 2 nodes that are connected to other Intermediate System Level 1/Level 2 nodes. Enabling the parameter for Intermediate System Level 1 nodes is not recommended.

- LDB—If checked (default), enables the TARP loop detection buffer. The LDB prevents TARP PDUs from being sent more than once on the same subnet.

  Note
  The LDB parameter is not used if the Node Routing Mode is provisioned to End System or if the TARP PDUs L1 Propagation parameter is not enabled.

- LAN TARP Storm Suppression—If checked (default), enables TARP storm suppression. This function prevents redundant TARP PDUs from being unnecessarily propagated across the LAN network.
- Send Type 4 PDU on Startup—If checked, a TARP Type 4 PDU is originated during the initial startup. Type 4 PDUs indicate that a TID or NSAP change has occurred at the NE. (The default setting is not enabled.)
- Type 4 PDU Delay—Sets the amount of time that will pass before the Type 4 PDU is generated when Send Type 4 PDU on Startup is enabled. 60 seconds is the default. The range is 0 to 255 seconds.

Note
The Send Type 4 PDU on Startup and Type 4 PDU Delay parameters are not used if TARP PDUs Origination is not enabled.

- LDB Entry—Sets the TARP loop detection buffer timer. The loop detection buffer time is assigned to each LDB entry for which the TARP sequence number (tar-seq) is zero. The default is 5 minutes. The range is 1 to 10 minutes.
- LDB Flush—Sets the frequency period for flushing the LDB. The default is 5 minutes. The range is 0 to 1440 minutes.
- T1—Sets the amount of time to wait for a response to a Type 1 PDU. Type 1 PDUs seek a specific NE TID within an OSI Level 1 area. The default is 15 seconds. The range is 0 to 3600 seconds.
- T2—Sets the amount of time to wait for a response to a Type 2 PDU. TARP Type 2 PDUs seek a specific NE TID value within OSI Level 1 and Level 2 areas. The default is 25 seconds. The range is 0 to 3600 seconds.
- T3—Sets the amount of time to wait for an address resolution request. The default is 40 seconds. The range is 0 to 3600 seconds.
- T4—Sets the amount of time to wait for an error recovery. This timer begins after the T2 timer expires without finding the requested NE TID. The default is 20 seconds. The range is 0 to 3600 seconds.

Note
The T1, T2, and T4 timers are not used if the TARP PDUs Origination check box is not checked.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-G285 Adding a Static TID-to-NSAP Entry to the TARP Data Cache

Purpose	This task adds a static TID-to-NSAP entry to the TDC. The static entries are required for NEs that do not support TARP and are similar to static routes. For a specific TID, you must force a specific NSAP.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC
Required/As needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **OSI** > **TARP** > **Static TDC** tabs.

Step 2 Click **Add Static Entry**.

Step 3 In the Add Static Entry dialog box, enter the following:

- TID—Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node or multishelf view Provisioning > General tab.)
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-G287 Adding a TARP Manual Adjacency Table Entry

Purpose	This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the ONS 15454 must communicate across routers or NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **OSI** > **TARP** > **MAT** tabs.

Step 2 Click **Add**.

Step 3 In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:

- Level—Sets the TARP Type Code that will be sent:

- **Level 1**—Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
- **Level 2**—Indicates that the adjacency is in a different area than the current node. The entry generates Type 2 PDUs.

- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

Step 4 Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.

Step 5 Return to your originating procedure (NTP).

DLP-G288 Provisioning OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Router 1 must be enabled before you can enable and edit the primary manual area addresses for Routers 2 and 3.

Note The Router 1 manual area address, System ID, and Selector “00” create the node NSAP address. Changing the Router 1 manual area address changes the node NSAP address.

Note The System ID for Router 1 is the node MAC address. The System IDs for Routers 2 and 3 are created by adding 1 and 2 respectively to the Router 1 System ID. You cannot edit the System IDs.

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.

Step 2 Chose the router you want provision and click **Edit**. The OSI Router Editor dialog box appears.

Step 3 In the OSI Router Editor dialog box:

a) Check **Enable Router** to enable the router and make its primary area address available for editing.

b) Click the manual area address, then click **Edit**.

c) In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0–9, a–f) in length.

d) Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-G289 Provisioning Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary area and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G288 Provisioning OSI Routers, on page 46 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.

Step 2 Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box appears.

Step 3 In the OSI Router Editor dialog box:

a) Check **Enable Router** to enable the router and make its primary area address available for editing.

b) Click the manual area address, then click **Add**.

c) In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2 to 24 alphanumeric characters (0–9, a–f) in length.

d) Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-G290 Enabling the OSI Subnet on the LAN Interface

Purpose	This task enables the OSI subnetwork point of attachment on the LAN interface.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note When you create communication channels (optical service channel [OSC] or generic communications channel [GCC]), OSI subnetwork points of attachment are enabled on the communication channels. See the NTP-G38 Provisioning OSC Terminations, on page 80 and the DLP-G76 Provisioning DCC/GCC Terminations task.

Note The OSI subnetwork point of attachment cannot be enabled for the LAN interface if the OSI routing mode is set to ES.

Note If secure mode is on, the OSI subnet is enabled on the backplane LAN port, not the front control card TCP/IP (LAN) port.

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Routers** > **Subnet** tabs.

Step 2 Click **Enable LAN Subnet**.

Step 3 In the Enable LAN Subnet dialog box, complete the following fields:

- ESH—Sets the End System Hello (ESH) propagation frequency. An ES NE transmits ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the Intermediate System Hello (ISH) PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the IS NEs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello (IIH) PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default IS-IS cost for LAN subnets is 20. It normally should not be changed.
- DIS Priority—Sets the designated intermediate system (DIS) priority. In IS-IS networks, one router is elected to serve as the DIS (LAN subnets only). Cisco router DIS priority is 64. For the LAN subnet, the default DIS priority is 63. It normally should not be changed.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G291 Creating an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15454nodes to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution IP-over-CLNS tunnels require two endpoints. You will create one point on a ONS 15454. The other endpoint is generally provisioned on non-ONS equipment including routers and other vendor NEs. Before you begin, verify that you have the capability to create an OSI-over-CLNS tunnel on the other equipment location.

Note The Cisco proprietary tunnel is slightly more efficient than the GRE tunnel because it does not add the GRE header to each IP packet. The two tunnel types are not compatible. Most Cisco routers support the Cisco IP tunnel, while only a few support both GRE and Cisco IP tunnels. You generally should create Cisco IP tunnels if you are tunneling between two Cisco routers or between a Cisco router and the node.

Procedure

Step 1 Click the **Provisioning** > **OSI** > **Tunnels** tabs.

Step 2 Click **Create**.

Step 3 In the Create IP Over CLNS Tunnel dialog box, complete the following fields:

- Tunnel Type—Choose a tunnel type:
  - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - **GRE**—Creates a generic routing encapsulation (GRE) tunnel. GRE tunnels add the CLNS header and a GRE header to the IP packets.

    Caution
    Always verify that the IP-over-CLNS tunnel type that you choose is supported by the equipment at the other end of the tunnel.

- IP Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- IP Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.
- OSPF Metric—Enter the OSPF metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address—Enter the destination NE or OSI router NSAP address.

Step 4 Click **OK**.

Step 5 Provision the other tunnel endpoint using the documentation provided by the manufacturer of the third party vendor NE.

Step 6 Return to your originating procedure (NTP).

NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File

Purpose	This procedure imports the Cisco Transport Planner NE Update configuration file and creates a log file.
Tools/Equipment	A Cisco Transport Planner NE Update file for the network where the node is installed must be accessible to the CTC computer.
Prerequisite Procedures	• NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Verify that you have the correct Cisco Transport Planner network file before you begin this procedure. The file will have an XML extension and a name assigned by your network planner. Check with your network planner or administrator if you have any questions.

Note The import operation of Cisco Transport Planner NE Update configuration file is based on the number of configurations. The import operation takes more time for a very large configuration that includes several pluggable modules and ports. When the configuration file is imported in non-interactive mode, CTC can be used for other operations.

Note The configuration file, which is provided in XML format, provisions internal patchcords, optical sides and card parameters for optical units, transponders, and passive units (DCUs and patch panels). Finally, the NE Update file installs the ANS parameters calculated by Cisco Transport Planner. The log file, which is a text document records the results of the NE update.

Note The Cisco Transport Planner configuration file contains parameters for the node, shelf, card type, port (including the card's wavelength), pluggable port module (PPM), as well as OTN and FEC parameters. Only the values present in XML format appear in the configuration file parameters; if the values are not in XML format, a column appears blank. The XML file values are independently reported and do not affect any configuration changes that you apply.

Note Common control cards are not provisioned by Cisco Transport Planner.

Procedure

Step 1 If you choose the Provision Node Layout option to preprovision the cards in the shelf, complete the following steps. If not, continue with Step 2.

a) Display the node in node view (single-shelf mode) or multishelf view (multishelf mode).

b) Verify that the common control cards are the only cards installed. If in single or multishelf mode, verify that each shelf in the multishelf has two control cards.

- If common control cards are the only cards installed, continue with Step 2.
- If other cards appear, continue with Step c.

c) If a physical card other than the common control cards is installed, remove it from the shelf.

d) If preprovisioned DWDM cards are present, delete them using the DLP-G351 Deleting a Card in CTC, then repeat Steps a and b.

Step 2 If you have not created a log file to record the results of the NE update, complete the following steps. If a log file has been created, continue with Step 3.

a) Open a text editor or word processing application.

b) Create a new text (TXT) document with a file name of your choosing.

c) Save the text document in a directory that is easy to navigate to from CTC.

Step 3 In CTC node view (single-shelf mode) or multishelf view, click the **Provisioning** > **WDM-ANS** > **Node Setup** tabs.

Step 4 Choose **Load latest installation file from node** to reload the latest XML file that was applied and stored in the node. Continue with Step 7.

Step 5 Choose **Load installation file from network repository** and navigate to the Cisco Transport Planner node setup file containing the parameters for the network where the node resides. This option downloads the XML file from the remote server. Continue with Step 7.

Step 6 In the field under Select XML file, type the path to the Cisco Transport Planner node setup file containing the parameters for the network where your node resides, or click **Browse** and navigate to the file on your computer. Click the file, then click **Open**. The file will have an XML extension. Continue with Step 7.

Step 7 In the field under Select Log file, type the path to the text file that you created in Step 2, or click **Browse** and navigate to the file on your computer or a network server where you want the node setup results recorded.

Note
The log file records the parameters that were updated successfully and provides an explanation of why an update could not be completed. Each node setup session overwrites the log file contents. If you want to save the results from a previous NE update, save the log file with new name.

Step 8 Click **Apply**.

Step 9 When **Load installation file from network repository** option is chosen, the FTP Remote Installation File *Node-Name* page appears.

a) When the node is configured as a Gateway Network Element (GNE) node, enter the parameters (host name, port, user name, password, remote directory, and XML file name of the remote server) and click **Next**.
b) When the node is configured as a Elementary Network Element (ENE) node, an additional parameter called GNE Selector appear. From the **GNE Selector** drop-down list, select the appropriate GNE in the network. The FTP relay must be configured on the selected GNE to the remote server where the XML file is stored. See NTP-G28 Creating FTP Host, on page 37 to configure the FTP relay on the selected GNE.

Step 10 When the Node Setup Selection for *Node-Name* page appears, complete the following steps. If not, continue with Step 11.

a) Choose the node profile that you want to apply to the node. The Cisco Transport Planner XML file contains profiles for all nodes in the network. Choose the profile that applies to the node you are provisioning.
b) Click **Next**.

Step 11 On the Node Setup for *node name* page, choose one or more of the following:

- Node Layout—Preprovisions the slots in each shelf in CTC for the cards defined in the network plan. Choose this option when no DWDM cards are installed. (Errors will occur if cards are installed or the slots are preprovisioned.) Preprovisioning the slots before the physical cards are installed ensures that card installers place the cards in the correct slots. Preprovisioning the slots is also useful if you want to set up the network prior to card installation. The node layout also preprovisions the chassis and passive units.
- Card Parameters—If checked, provisions the following parameters, if the cards are installed.
  - TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, and OTU2_XP cards—Provisions the OTN and FEC parameters.
  - OPT-AMP-L, OPT-AMP-17-C, OPT-AMP-C, OPT-EDFA-17, OPT-EDFA-24, OPT-EDFA-35, GE_XP, 10GE_XP, GE_XPE, and 10GE_XPE cards—Provisions the card mode.
- Pluggable Port Modules— If checked, allows the provisioning of PPMs on TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, and OTU2_XP cards, including PPM payloads.
- Internal Patchcords—If checked, allows creation of internal patchcords among cards provisioned in the node.
- Optical Sides—If checked, allows the provisioning of optical sides.
- ANS Parameters—If checked, installs the ANS parameters. ANS parameters provision the values required for the node to function within the specified network design. ANS parameters include span losses, optical power, optics thresholds, amplifier working mode, gain, tilt, and many others. Refer to Node Reference chapter for a list of ANS parameters.

  Note
  If you are importing the Cisco Transport Planner configuration file for the first time, you normally choose all the available options.

- Skip Interactive Mode—If checked, CTC provisions all the chosen setup components automatically without allowing you to view the results after each one.
- Save Installation Files (XML and log) On Node—If checked, CTC saves the XML and log files on the node.

Step 12 Click **Next.** If you chose Skip Interactive Mode, continue with Step 13. If not, the wizard page that appears depends on the options chosen in Step 11. Complete the steps shown in the following table for each option.

Table 2: NE Update Wizard Options

NE Update Function	
Node/Shelves Layout	View the cards and slots on the left side of the page and verify that they are the same as the la Cisco Transport Planner Shelf Layout (see Cisco Transport Planner Node Setup Information page 3). If the cards and slots match, click **Apply**. If not, click **Cancel**. and contact your nex support to verify that you have the correct node setup file. If the site has a multishelf configu **Next** and repeat this step for each shelf at the site. CTC preprovisions the slots. This might take a few seconds. The results appear in the Log wi that are successfully provisioned display an "Applied" status. A "Slot not empty" status appe cannot be provisioned because a card is physically installed or the slot is already provisioned. complete the following steps. Otherwise, continue with the next NE Update function. **a.** Click **Cancel**, then click **Yes** in the confirmation dialog box. The slot preprovisioning do when you click Cancel. **b.** If a physical card is installed, remove it from the shelf. **c.** Perform one of the following steps: • Delete all the preprovisioned slots using the DLP-G351 Deleting a Card in CTC tas Steps 1 through Step 12 . • Delete the slot where the Slot Not Empty error occurred using the DLP-G351 Deleti CTC task. Complete the DLP-G353 Preprovisioning a Slot task to provision the slot r repeat Steps 1 through 12 making sure to uncheck the Provision Node Layout optio **Note** When you preprovision a slot, the card is purple in the CTC shelf graphic and "NP" appears on the card. After the physical card is installed, the card changes to white ar removed from the CTC shelf graphic.
Passive Units Layout	**a.** Review the passive unit settings. **b.** Click **Apply**. **c.** Click **Next.**
Pluggable Port Modules	**a.** Review the PPM settings for each TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, a card. **b.** Click **Apply**. **c.** Click **Next.**

NE Update Function	
Card Parameters	**a.** Review the OTN, FEC, and card mode settings for each TXP, MXP, GE_XP, 10GE_X 10GE_XPE, and OTU2_XP card. **b.** Click **Apply**. **c.** Click **Next.**
Internal Patchcords	**a.** Review the internal patchcords. **b.** Click **Apply**. **c.** Click **Next.**
Optical Sides	**a.** Review the optical side assignments. **b.** Click **Apply**. **c.** Click **Next.**
ANS Parameters	**a.** Review the ANS parameters on the left half of the page. **b.** Click **Apply**. The log file displays the results. At the end, a Done status will appear. If a not be applied, a Setting Refused status appears. If this occurs, contact your next leve
Select All	If checked, selects all the options.
Skip Interactive Mode	If checked, CTC provisions all the chosen setup components automatically without allow the results after each one.
Save Installation Files (XML and log) On Node	If checked, CTC saves the XML and log files on the node.

Step 13 Click **Finish**, then click **OK** in the Wizard Complete confirmation dialog box. The confirmation box indicates whether the xml import process was completed successfully.

Stop. You have completed this procedure.

NTP-G320 Configuring the Node as a Non-DWDM Network

Purpose	This tasks configures a node as a Non-DWDM network.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Provisioning** tabs.

Step 2 From the Selector area, select Network Type.

Step 3 Choose **Not-DWDM**, from the Value drop-down list. Click **Apply**.

Step 4 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Port Status** tabs.

Step 5 Click the **Launch ANS** button. The relevant ports in the node will be in IS state.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-G348 Using the Cisco Transport Planner Shelf Layout Report

Purpose	This task describes how to use the Cisco Transport Planner shelf layout report to install cards in a DWDM node.
Tools/Equipment	None
Prerequisite Procedures	NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Procedure

Step 1 Display the Cisco Transport Planner shelf layout report for your site. The report can be viewed in Cisco Transport Planner. It can also be viewed as a JPEG graphic. Refer to the *Cisco Transport Planner DWDM Operations Guide* for information about generating shelf layout reports.

Step 2 Review the following installation information:

- Rack—Indicates the rack in the node where the cards must be installed.
- Shelf—Indicates the shelf in the rack where the cards must be installed. Shelf options include:
  - Flex Shelf—The ONS 15216 FlexLayer mechanical shelf houses Y-cable modules. Flex shelf positions are numbered 1 to 4 from left to right.
  - DCU Shelf—The Cisco ONS 15216 dispersion compensation shelf assembly houses DCUs. DCU positions are numbered 1 to 2 from left to right.

- Shelf-ANSI-*n* or Shelf-ETSI-*n*—The ONS 15454 shelf assembly houses ONS 15454 common, DWDM, and client cards. Positions in this type of shelf are numbered 1 to 17 from left to right. Multiple shelves might appear.

- Slot—Indicates the slot in the specific shelf where the cards must be installed:
  - Unit Name (Product ID)— Identifies the card by its Product ID.
  - Unit Description—Identifies the card by its name.
- Unit Side—Identifies the side of the node that the specific card is serving: A, B, C, D, E, F, G, or H.
- Unit Plug-in Modules—Identifies the type and number of PPMs that will be used with specific TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, or OTU2_XP cards.

Step 3 Return to your originating procedure (NTP).

NTP-G31 Installing the DWDM Dispersion Compensating Units

Purpose	This procedure describes how to install the DCUs for DWDM shelves.
Tools/Equipment	DCUs
Prerequisite Procedures	• DLP-G604 Installing the TNC, TNCE, TSC, TSCE, TNCS-2, TNCS-2O, TNCS-O, or TNCS Card • NTP-G30 Installing the DWDM Cards • NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning Class I (CDRH) and Class 1M (IEC) laser products. Statement 1055

Warning Warning Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Statement 1056

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. For detailed instructions on how to wear the ESD wristband, refer to the Electrostatic Discharge and Grounding Guide for Cisco CPT and Cisco ONS Platforms.

Note For US installations, complies with the US Federal Drug Administration Code of Federal Regulations Title 21, Sections 1040.10 and 1040.11, except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.

Procedure

Step 1 Remove the DCU from its packaging, then remove the protective caps from the connectors. (Safety caps are typically yellow.)

Step 2 Use both hands to push the DCU all the way into the chassis until the connector spring lock on the right side of the module clicks into place.

Step 3 Open the cover with the laser warning on the connector adapter and then connect the cable connector.

Note
The Side A DCU is commonly installed on the left side and the Side B DCU is commonly installed on the right side.

Note
Double-check the placement of the DCU card(s) with your Cisco Transport Planner shelf layout. If you install the wrong DCU in a slot, remove the DCU and install the correct one.

Stop. You have completed this procedure.

NTP-G239 Managing Passive Units and Passive Shelves

Purpose	This procedure explains how to add or delete passive units or passive shelves.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Complete the DLP-G46 Log into CTC task to log in to a ONS 15454 node on the network.

Step 2 As needed, complete the following tasks:

- Complete the DLP-G543 Adding Passive Units or Passive Shelves Manually, on page 59 to manually preprovision a passive unit or passive shelf.

- Complete the DLP-G544 Deleting a Passive Unit or Passive Shelf, on page 60 to delete a passive unit or passive shelf.
- Upgrade the firmware of the passive shelves.
- Complete the #unique_114 to associate a passive unit or passive shelf with the USB port, perform a Blink LED operation, or a Power Refresh on the passive units or passive shelves.

Stop. You have completed this procedure.

DLP-G543 Adding Passive Units or Passive Shelves Manually

Purpose	This task preprovisions passive units (passive shelves, patch panels, and DCUs) in CTC. Preprovisioning of the passive units is normally performed when you complete the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51 . Use this task if you need to manually preprovision a passive unit or passive shelf. All slot preprovisioning must be based upon the Cisco Transport Planner shelf layout prepared for your site.
Tools/Equipment	Cisco Transport Planner shelf layout table or JPG file.
Prerequisite Procedures	• DLP-G46 Log into CTC • NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Click **Create**. The Create Passive Card dialog box appears.

Step 3 Choose the unit from the Card Type drop-down list and click **OK**.

If PASSIVE SHELF MF or PASSIVE SHELF MF10 is selected, go to the next step, otherwise go to Step 5.

Note
You can also add a passive unit in the multishelf view by right-clicking the slot inside the rack. Refer to the NTP-G146 Add a Rack, Passive Unit, or Shelf to a Multishelf Node procedure.

Note
If you need to view the details of the passive units that have been installed on a node, click the Inventory tab.

Step 4 Enter a shelf ID in the PShelf ID field.

The range is from 1 to 126. The next available ID is automatically assigned if a value is not specified.

Step 5 Choose the shelf where the passive unit is to be provisioned from the Passive Shelf drop-down list.

The drop-down list contains all provisioned passive shelves. If you want to provision a passive unit outside the passive shelf, choose the N/A option.

Step 6 Choose the slot from the Slot drop-down list if you have selected a passive shelf in Step 5.

Step 7 Choose the DCU type from the DCU Type drop-down list. The available values are SMF and ELEAF.

Step 8 Choose the DCU compensation from the DCU Compensation drop-down list.

After successfully adding the passive shelf, the shelf might not appear in the CTC. In this scenario, we recommend you to relaunch the CTC to display the newly added passive shelf.

Step 9 Return to your originating procedure (NTP).

DLP-G544 Deleting a Passive Unit or Passive Shelf

Purpose	This task deletes a passive unit or passive shelf.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Click the passive unit or passive shelf you want to delete.

Step 3 Click **Delete**, then click **Yes**.

Note
All slots in a shelf have to be empty to delete a passive shelf.

You can also delete a passive unit or passive shelf in the multi-shelf view. Refer to NTP-G147 Delete a Passive Unit, Shelf, or Rack from a Multishelf Node procedure.

Step 4 Return to your originating procedure (NTP).

DLP-G792 Performing a Firmware Upgrade on Passive Shelves

Purpose	This task upgrades the firmware of the fiber shuffle or MPO fan out unit.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The firmware upgrade is non-service-affecting. However, there is a temporary loss of connectivity. It is recommended to upgrade only one fiber shuffle or MPO fan out unit per node at a time.

Note During the firmware upgrade, do not reset the TNCS or TNCS-O card nor remove the cable from USB 3.0 port of the fiber shuffle or the MPO fan out unit.

Note Firmware upgrade is allowed only when the ports are in OOS (out-of-service) or Maintenance service state.

Note Event notifications are triggered at every stage of the firmware upgrade process. These event notifications are reported as transient conditions in the multishelf view > Alarms tab in CTC. The notifications are also displayed in the multishelf view > History > Session tab in CTC. The following event notifications are displayed:

- FIRMWARE_DOWNLOAD —When the firmware download is in progress. The firmware upgrade is initiated after the download is complete.
- FIRMWARE_UPG — When the firmware upgrade is progress.
- FIRMWARE_UPG_FAIL— When the firmware download or the firmware upgrade fails.
- FIRMWARE_UPG_COMPLETE —When the firmware upgrade is completed successfully.

Procedure

Step 1 In the multishelf view, double-click the MF-6RU or MF10-6RU shelf to open shelf mode or right-click the passive shelf and choose **Open Shelf.**

Step 2 Click the **Maintenance** > **Firmware** tab.

The revision number of the bootrom and kernel are displayed. If the bootrom revision is lower than the current revision, continue with the next step. If the bootroom revision is current and the kernel revision is lower than the current revision, go to Step 5.

Note
The Upgrade OS KERNEL button is disabled when the bootrom revision is lower than the current revision and is enabled only after the bootrom upgrade.

Step 3 Click the **Upgrade BOOTROM** button.

The upgrade process takes about 45 minutes.

Step 4 Verify the bootrom revision in the Maintenance > Firmware tab after the upgrade is complete.

The bootrom revision is also updated in the Inventory tab.

Step 5 Click the **Upgrade OS KERNEL** button.

The upgrade process takes about 30 minutes.

Step 6 Verify the kernel version in the Maintenance > Firmware tab after the upgrade is complete.

Step 7 Return to your originating procedure (NTP).

DLP-G793 Performing Upgrade on Fiber Shuffle

Table 3: Feature History

Feature Name	Release Information	Feature Description
Fiber Shuffle Upgrade	Cisco NCS 2000 Release 11.12	This feature allows you to upgrade the Boot ROM version, OS Kernel, and Uboot version of the fiber shuffle through CTC.

Purpose	This task upgrades the firmware of the passive fiber shuffle (NCS2K-MF10-6RU, and NCS2K-MF-6RU).
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Choose the passive card and click **Upgrade Firmware**.

The **Upgrade Passive Software** dialog box appears.

Step 3 Click **Upgrade BOOTROM** to upgrade the Boot ROM version necessary for the new software release.

Note
The upgrade process may take up to 80 minutes. Do not plug-out the device nor start other firmware upgrade operation until the Boot ROM upgrade operation is completed.

Step 4 Click **Upgrade OS KERNEL**.

Note
The upgrade process may take up to 40 minutes. Do not plug-out the device nor start other firmware upgrade operation until the kernel upgrade operation is completed.

Step 5 Click **Upgrade UBOOT** to update the Uboot version.

Note
You must upgrade the Boot ROM before proceeding with Uboot upgrade.

The upgrade process may take up to 15 minutes. Do not plug-out the device nor start other firmware upgrade operation until the Uboot upgrade operation is completed.

Step 6 Click **Yes** in the **Warning: Upgrade Firmware** dialog box.

Note
CTC confirms whether the device firmware is up to date. If the firmware is not the latest version, CTC triggers upgrade process with the help of USB commands to fiber shuffle. After successful upgrade you can see the upgraded version of Boot ROM / OS Kernel / Uboot in the **Upgrade Passive Software** dialog box.

DLP-G762 Associating Passive Units or Passive Shelves to USB Ports

Purpose	This task associates passive units (passive shelves, patch panels, and DCUs) to the USB ports in CTC. This task is also used to perform a power refresh on the passive units or passive shelves.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

Procedure

Step 1 In the node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Passive Cards** tabs.

Step 2 Select the passive unit or passive shelf to associate with the USB port.

Step 3 Click **Associate to USB Port**. The Associate USB port dialog box appears.

Step 4 Choose the shelf from the Shelf drop-down list.

Note
If the passive unit selected in Step 2 is provisioned in a passive shelf, check the Associate within Passive Shelf checkbox so that the Shelf drop-down lists the passive shelves.

Step 5 Choose the USB port from the USB port drop-down list.

The USB port drop-down list contains the USB ports that are physically connected to the equipment type selected in Step 2.

Step 6 Click **OK**.

The passive unit is associated with the selected USB port and shelf.

Step 7 To perform a LED blink function of the device connected to the selected USB port, click **Blink LED**.

The LED Blink dialog box appears indicating that the LED blink has been performed.

The LED blinks in blue color helping the operator to identify a specific passive module. Click **Blink LED** again to stop the blinking.

Step 8 To retrieve the power values on the selected passive unit or passive shelf, click **Power Refresh**.

Note
The Power Refresh and Blink LED functions can be performed only after associating the passive units or passive shelves to USB ports.

Step 9 Return to your originating procedure (NTP).

NTP-G152 Creating and Verifying Internal Patchcords

Purpose	This procedure imports the internal patchcords using the CTP XML file. Internal patchcords can also be manually provisioned.
Tools/Equipment	• Cisco Transport Planner shelf layout • Cisco Transport Planner Internal Connections Report

Prerequisite Procedures	• NTP-G22 Verifying Common Card Installation, on page 4 • NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 Login to the node where you want to provision the DWDM cable connections. If you are already logged in, continue with Step 2.

Step 2 Complete the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51 to import the Cisco Transport Planner NE update file.

Step 3 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcords** tabs.

Note
The Internal Patchcords tab does not show OPT-PRE DCU connections or span connections.

Note
The number of rows in the Provisioning > WDM-ANS > Internal Patchcords tab are created dynamically, as per the number of sides present in a node.

Note
On the ONS 15454 M2 and the ONS 15454 M6 shelves, you can create internal patchcords between the TNC and TNCE cards and the optical amplifier cards.

Step 4 Verify that the connections in the Internal Patchcords tab match the connections in the Cisco Transport Planner Internal Connections Report for the DWDM cards (see the DLP-G349 Using the Cisco Transport Planner Internal Connections Report task). The Internal Patchcords tab will not show OPT-PRE DCU connections or span connections.

Step 5 Complete the NTP-G242 Creating an Internal Patchcord Manually, on page 66 for any connections that require manual provisioning, for example, to create patchcords between TXP and MXP trunk ports and OCH filter ports. If you need to delete a connection, complete the DLP-G355 Deleting an Internal Patchcord, on page 76.

Note
Connections related to optical bypass circuits must be manually provisioned.

Step 6 To view patchcords that are directly connected to TXP cards only, check the TXP Only checkbox.

Stop. You have completed this procedure.

NTP-G242 Creating an Internal Patchcord Manually

Purpose	This procedure creates an internal patchcord manually.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Use only one management interface to complete the creation of internal patchcords. For example, do not begin the internal patchcord creation using the TL1 interface or CTP XML file and end the internal patchcord creation using CTC.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 Choose one of the following link types for the internal patchcord:

- Trunk to Trunk (L2)—Creates a bidirectional patchcord between the trunk ports of GE_XP and 10GE_XP cards. If you choose this option, complete NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option, on page 67.
- OCH-Trunk to OCH-Filter—Creates an internal patchcord between an optical channel trunk port on a TXP/MXP stage card (which includes GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line cards) and an optical channel filter port on an add/drop stage card (which includes 32MUX, 40-MUX-C, 32WSS, 40-WSS-C/40-WSS-CE, 32DMX, 32DMX-O, 40DMX, 40-SMR1-C, or 40-SMR2-C cards).

  You can use this option to also create an internal patchcord between an optical channel trunk port on a TXP/MXP stage card (which includes TXP, MXP, GE_XP, 10GE_XP, GE_XPE, 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line cards) and the COM port on a PSM card in channel protection configuration (where, PSM card is equipped between one TXP/MXP stage and two add/drop stages). In this case, the Internal Patchcord Creation wizard will prompt you to create patchcords between the working and protect ports on the PSM card and the ports on the two different add/drop stage cards (which includes 32MUX, 40-MUX-C, 32WSS, 40-WSS-C/40-WSS-CE, 32DMX, 32DMX-O, 40DMX, 40-SMR1-C, 40-SMR2-C, 80-WXC-C, or 16-WXC-FS cards). If you choose this option, complete DLP-G547 Creating an Internal Patchcord Manually Using the OCH-Trunk to OCH-Filter Option, on page 68.

- OCH-Filter to OCH-Filter—Creates an unidirectional or bidirectional internal patchcord between a MUX input port and a DMX output port. If you choose this option, complete DLP-G548 Creating an Internal Patchcord Manually Using the OCH-Filter to OCH-Filter Option, on page 70.
- OTS to OTS—Creates a unidirectional or bidirectional internal patchcord between two optical transport section (OTS) ports, between two optical cards, between an optical card and a passive card, between two passive cards, or between the TNC or TNCE cards and an optical amplifier card. This option also includes OSC ports. If you choose this option, complete DLP-G549 Creating an Internal Patchcord Manually Using the OTS to OTS Option, on page 72.
- Optical Path—Creates an internal patchcord between two optical cards, or between an optical card and a passive card. If you choose this option, complete DLP-G531 Creating an Internal Patchcord Manually Using the Optical Path Option, on page 75.

Note
Manual creation of OTS/OCH to OTS/OCH internal patchcords is not required for standard DWDM nodes. However, manual creation might be required for non-standard nodes, for example, a hub node that has wavelength selective switches installed. In such cases, manual creation is recommended by Cisco Transport Planner.

Note
To successfully create an internal patchcord between WSS/DMX channel port and TXP trunk port, choose the TXP as the source endpoint and WSS/DMX as the destination endpoint.

Stop. You have completed this procedure.

NTP-G354 Creating an Internal Patchcord Manually Using the Trunk to Trunk (L2) Option

Purpose	This task creates a bidirectional internal patchcord between the trunk ports of two GE_XP or 10GE_XP cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as Trunk to Trunk (L2) and click **Next**.

Step 4 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Slot—Choose the slot containing the card where the internal patchcord originates.
- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 5 Click **Next**.

Step 6 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Slot—Choose the slot containing the card where the internal patchcord terminates.
- Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 7 Click **Next**.

Step 8 Review the display-only information on the Internal Patchcord Origination Reverse page. This page shows the slot, and port that CTC will use for the opposite internal patchcord origination route.

Step 9 Click **Next**.

Step 10 Review the information displayed on the Internal Patchcord Termination Reverse page. This display-only page shows the slot, and port that CTC will use for the reverse internal patchcord termination route.

Step 11 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 12 Return to your originating procedure (NTP).

DLP-G547 Creating an Internal Patchcord Manually Using the OCH-Trunk to OCH-Filter Option

Purpose	This task creates a bidirectional internal patchcord between a TXP, MXP, or XP trunk and a DWDM add and drop channel port.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as OCH-Trunk to OCH-Filter option and click **Next**.

Step 4 On the Internal PatchcordOCH Attributes page, provision the following parameters:

- OCHNC Wavelength—Sets the OCHNC wavelength for the OCH trunk to OCH filter internal patchcord. Use the unnamed band selection box below to display C-band or L-band wavelengths in the OCHNC Wavelength field. Provision the OCHNC wavelength to the wavelength provisioned for the GE_XP, 10GE_XP, GE_XPE, or 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line card trunk port.
- PSM Protection—Select this check box if you have provisioned a PSM card in channel protection configuration.
- Colorless—Select this check box if you want to create a colorless patchcord.

Step 5 Click **Next**.

Step 6 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Slot—Choose the slot containing the card where the internal patchcord originates.
- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 7 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 8 Click **Next**.

Step 9 In the Internal Patchcord Origination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord origination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
- Side—Choose the side where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.

- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 7.

- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 10 Click **Next**.

Step 11 In the internal Patchcord Termination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord termination route:

- Slot—Choose the slot containing the card where the internal patchcord originates.
- Rx Port—Choose the RX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 12 Click **Next**.

Step 13 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 14 Return to your originating procedure (NTP).

DLP-G548 Creating an Internal Patchcord Manually Using the OCH-Filter to OCH-Filter Option

Purpose	This task creates a unidirectional or bidirectional internal patchcord between two DWDM add and drop channel ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as OCH-Filter to OCH-Filter option and click **Next**.

Step 4 On the Internal Patchcord OCH Attributes page, provision the following parameters:

- OCHNC Wavelength—Sets the OCHNC wavelength for the OCH trunk to OCH filter internal patchcord. Use the unnamed band selection box below to display C-band or L-band wavelengths in the OCHNC Wavelength field. Provision the OCHNC wavelength to the wavelength provisioned for the GE_XP, 10GE_XP, GE_XPE, or 10GE_XPE, ADM-10G, OTU2_XP, 100G-LC-C, 10x10G-LC, CFP-LC, 100G-CK-C, AR_MXP, AR_XP, AR_XPE or ITU-T line card trunk port.
- Bidirectional—If checked, creates a bidirectional internal patchcord.
- PSM Protection—Select this check box if you have provisioned a PSM card in channel protection configuration.

Step 5 Click **Next**.

Step 6 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Tx Port—Choose the TX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 7 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 8 If you did not choose bidirectional in Step 4, continue with Step 13. Otherwise, continue with the next step.

Step 9 Click **Next**.

Step 10 In the Internal Patchcord Origination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord origination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.

- Side—Choose the side where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 7.

- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 11 Click **Next**.

Step 12 In the internal Patchcord Termination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord termination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 6.

- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 13 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 14 Return to your originating procedure (NTP).

DLP-G549 Creating an Internal Patchcord Manually Using the OTS to OTS Option

Purpose	This task creates a unidirectional or bidirectional internal patchcord between two optical transport section (OTS) ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note When the creation of patchcords between two passive cards fails after deleting the previous internal patchcords, delete the passive cards and re-provision them.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as OTS to OTS and click **Next**.

Step 4 On the Internal Patchcords OTS Attributes page, provision the following parameters:

- Bidirectional—If checked, creates a bidirectional internal patchcord.
- MPO Connection—Creates all the patchcords between two MPO connectors. If this option is checked, the bidirectional option is disabled.
- Exclude Used Port—If checked, excludes the used ports for patchcord creation. If unchecked, more than one patchcord can be created starting from the same port.
- Grid Filter—Select the grid option from the drop-down list.
- Port Type—Select the port type from the drop-down list. The options are:
  - OSC only—Cards with OSC ports and OSCM cards are available for patchcord creation. The MPO Connection and Exclude Used Ports checkboxes are disabled and the Bidirectional option is checked.
  - DC only—Cards with DC ports and passive DCUs are available for patchcord creation. The MPO Connection and Exclude Used Ports checkboxes are disabled and the Bidirectional option is checked. Allows to create an internal patchcord between an optical card and a passive card.

Step 5 Click **Next.**

Step 6 On the Internal Patchcord Origination page, provision the internal patchcord origination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.
- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

- MPO—Choose the port where the internal patchcord originates.CTC automatically displays the list of ports that are available depending on the link type you choose. This field is visible only if you have chosen MPO connection in Step 4.

Step 7 Click **Next.**

Step 8 In the Internal Patchcord Termination page, provision the internal patchcord termination parameters:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.
- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.
- MPO—Choose the port where the internal patchcord originates.CTC automatically displays the list of ports that are available depending on the link type you choose. This field is visible only if you have chosen MPO connection in Step 4.

Step 9 If you did not choose bidirectional in Step 4, continue with Step 14. Otherwise, continue with the next step.

Step 10 Click **Next.**

Step 11 In the Internal Patchcord Origination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord origination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
- Side—Choose the side where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord originates. This field is visible only if you have chosen the type as Optical Card.
- Unit—Choose the passive card where the internal patchcord originates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 8.

- Tx Port—Choose the TX port where the internal patchcord originates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 12 Click **Next.**

Step 13 In the Internal Patchcord Termination Reverse page, provision the internal patchcord parameters for the reverse internal patchcord termination route:

- Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
- Side—Choose the side where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.
- Slot—Choose the slot containing the card where the internal patchcord terminates. This field is visible only if you have chosen the type as Optical Card.

- Unit—Choose the passive card where the internal patchcord terminates. This field is visible only if you have chosen the type as Passive Card.

  Note
  Choose the same passive card that you chose in Step 6.

- Rx Port—Choose the RX port where the internal patchcord terminates. CTC automatically displays the list of ports that are available depending on the link type you choose.

Step 14 Click **Finish**. The new internal patchcord appears in the Internal Patchcord table.

Step 15 Return to your originating procedure (NTP).

DLP-G531 Creating an Internal Patchcord Manually Using the Optical Path Option

Purpose	This task creates an internal patchcord manually between two optical cards or between an optical card and a passive card.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note When the creation of patchcords between two passive cards fails after deleting the previous internal patchcords, delete the passive cards and re-provision them.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click **Create**.

Step 3 On the Internal Patchcord Type Selection page, choose the patchcord type as Optical Path and click **Next**.

Step 4 On the Internal Patchcord Card List page, provision the following parameters:

- Card From Selection area:
  - Type—Choose the type of card (optical or passive card) where the internal patchcord originates.
  - Shelf—(Multishelf nodes only) Choose the shelf where the internal patchcord originates.

- Slot—Choose the slot containing the card where the internal patchcord originates.

- Card To Selection area:
  - Type—Choose the type of card (optical or passive card) where the internal patchcord terminates.
  - Shelf—(Multishelf nodes only) Choose the shelf where the internal patchcord terminates.
  - Slot—Choose the slot containing the card where the internal patchcord terminates.
- Choose the required patchcord from the list that CTC generates.

Step 5 Click **Next** to continue creating internal patchcords between cards and repeat Step 4. In the Internal Patchcord Card List page that follows, CTC automatically populates the Card From Selection fields with the values you entered in the Card To Selection fields in the previous page.

Note
After an internal patchcord is created, the selected optical card appears in the **Unit** drop-down list under *Passive Card Type*. To remove the optical card from the *Passive Card Type*, you must choose *Optical Card* and then *Passive Card* in the **Type** drop-down list. You must do this for every internal patchcord creation to correct the misplacement of the optical card.

Step 6 After creating all the internal patchcords between cards, click **Finish**. The new internal patchcords appear on the Internal Patchcord table.

Step 7 Return to your originating procedure (NTP).

DLP-G355 Deleting an Internal Patchcord

Purpose	This task deletes an internal patchcord.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Internal Patchcord** tabs.

Step 2 Click the connection you want to delete.

Step 3 Click **Delete**, then click **Yes**.

Step 4 Return to your originating procedure (NTP).

NTP-G209 Creating, Editing, and Deleting Optical Sides

Purpose	This procedure allows you to create, edit, and delete optical sides on a DWDM node.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note For any node type including mesh nodes, the association between the shelf, line card and side is reported in the left top window of CTC (Vital Status Pane) in the mode view.

Note For mesh nodes, the association between sides and the 40-WXC-C cards can be found in the **Provisioning** > **WDM-ANS** > **Internal Patchcords** screen. For example: PP-MESH, LC (A): Shelf 1, Slot 3 (40 WXC), port EXP-TX PP-MESH, MPO (A): Shelf 1, Slot 3 (40 WXC), port EXP-RX The above rows indicate that the: WXC port located in Shelf 1, Slot 3 is connected to the LC connector A (Side A) on PP-MESH. WXC port located in Shelf 1, Slot 3 is connected to the MPO connector A (Side A) on PP-MESH.

Procedure

As needed, complete the following tasks:

- Complete the DLP-G491 Creating an Optical Side, on page 78.
- Complete the DLP-G492 Editing an Optical Side, on page 78.
- Complete the DLP-G480 Deleting an Optical Side, on page 79.

Stop. You have completed this procedure.

DLP-G491 Creating an Optical Side

Purpose	This task creates an optical side.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Optical Sides** tabs.

Step 2 Click **Create**.

Step 3 In the Create Side dialog box, enter the following:

- Side ID—Choose a side ID (A, B,C, D, E, F, G, or H) from the drop-down list.
- Line In—Choose an RX port from the drop-down list.
- Line Out—Choose a TX port from the drop-down list.

Note
For a terminal node equipped with a PSM card in line or multiplex section protection configuration, you can only choose the W-RX and W-TX ports while creating an optical side. After you create the working (w) optical side, the control card automatically creates the protected (p) optical side involving the P-RX and P-TX ports of the PSM card. CTC refreshes the Optical Sides tab with both the working and protected optical sides.

Step 4 Return to your originating procedure (NTP).

DLP-G492 Editing an Optical Side

Purpose	This task edits the side ID of an optical side.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Optical Sides** tabs.

Step 2 Click the optical side that you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit Side ID dialog box, enter the following information:

- Side ID—Choose a side ID from the drop-down list.
- Side Description—Specify a description to identify the side.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-G480 Deleting an Optical Side

Purpose	This task deletes an optical side.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **WDM-ANS** > **Optical Sides** tabs.

Step 2 Click the optical side that you want to delete.

Step 3 Click **Delete**.

Step 4 In the confirmation dialog box, click **Yes** to continue.

Step 5 Return to your originating procedure (NTP).

NTP-G38 Provisioning OSC Terminations

Purpose	This procedure provisions the OSC terminations.
Tools/Equipment	None
Prerequisite Procedures	• NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note The OSC provides a bidirectional channel that connects all nodes within a DWDM ring. The OSC carries a supervisory data channel and synchronizes clocking at network nodes. The OSC also carries a user data channel.

Note Before provisioning OSC terminations on TNC ports carrying Fast Ethernet (FE) payloads, ensure to set the ALS mode on these ports to Disabled.

Note This procedure automatically turns on any OPT-RAMP-C, OPT-RAMP-CE, or RAMAN-CTP cards installed in the DWDM ring.

Note The DCCs, GCCs, and OSCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH.

Note In a pure ONS 15454 M6 network configuration, provision the OSC in GE or FE SFP mode. If an OC3 OSC is mandatory, then the network must be timing-synchronized as SONET. Identify the primary node and provide external timing signal to the BITS input pins of the primary node and provision line timing to the remaining nodes in the network. In a mixed ONS 15454 and ONS 15454 M6 network configuration, provision the OSC only in OC3 SFP mode. Identify the primary node and provide external timing signal to the BITS input pins of the primary node and provision line timing to the remaining nodes in the network.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Comm Channels** > **OSC** tabs.

Step 2 In the OSC Terminations area, click **Create**.

Step 3 In the Create OSC Terminations dialog box, choose the ports where you want to create the OSC termination. To select more than one port, press the **Shift** key (to select a range of ports) or the Ctrl key (to select multiple individual ports).

Note
The number of OSC terminations that you create depends on the node type defined by Cisco Transport Planner. Terminal nodes require one OSC termination. Hub, OADM, and ROADM nodes require two OSC terminations.

Step 4 In the Layer 3 area, check the OSI box if the following conditions are met:

- The OSC termination is between two nodes.
- Third party NEs that use the OSI protocol stack are on the same network.

If you checked OSI, complete the following steps. If not, continue with Step 5.

a) Click **Next**.
b) Provision the following fields:

- Router—Choose the OSI router.
- ESH—Set the ESH propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs they serve. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—Sets the ISH PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the IIH PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- Metric—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

Step 5 Click **Finish**. Ports are automatically placed in service. The following alarms might appear in the node view (single-shelf mode) or multishelf view (multishelf mode) Alarms tab Description field. They will remain until all the network OSC connections between the adjacent nodes are created:

- SDCC Termination Failure (ANSI) or RS-DCC Termination Failure (ETSI) on the OSCM or OSC-CSM card
- LOS on the OC-3 port (Port 1) on the OSCM, OSC-CSM, or OPT-BST card
- OPWR-LFAIL on the OPT-BST or OSC-CSM card

Note

After the OSC termination is created, the line ports are placed in service and span power levels are checked.

Stop. You have completed this procedure.

NTP-G37 Running Automatic Node Setup

Purpose	This procedure runs the Launch ANS function.
Tools/Equipment	The Cisco Transport Planner Installation Parameters file
Prerequisite Procedures	• NTP-G139 Verifying Cisco Transport Planner Reports and Files, on page 2 • NTP-G30 Installing the DWDM Cards • NTP-G152 Creating and Verifying Internal Patchcords, on page 64 • NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51 • DLP-G46 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Launch ANS applies the ANS parameters (calculated in the NTP-G143 Importing the Cisco Transport Planner NE Update Configuration File, on page 51) to the node and to the ports for cards installed in the node. The applied ANS parameters include span loss values, threshold values, power references, and others. Launch ANS also sets the VOA references based on the calculated power references.

Note ANS provisioning parameters must be calculated by Cisco Transport Planner. ANS provisioning parameters must be manually changed only by Cisco qualified personnel. Setting wrong ANS provisioning (either as preamplifier or booster input power thresholds) may impact traffic.

Procedure

Step 1 Referring to the "Cisco Transport Planner Installation Parameters" table, identify the parameters that have a Yes in the Manually Set column. If there are no parameters that have a Yes in the Manually Set column, continue with Step 5.

Step 2 In CTC, display the card where the parameter is to be manually provisioned in card view.

Step 3 Enter the specified Calibration parameter from the Cisco Transport Planner Installation Parameters table. Click **Apply**.

Step 4 Repeat Steps 1 through 3 for each parameter in the Cisco Transport Planner Installation Parameters table that displays Yes in the Manually Set field.

Step 5 Change to node view (single-shelf mode) or multishelf view (multishelf mode).

Step 6 Click the **Provisioning** > **WDM-ANS** > **Port Status** tabs.

Step 7 Click **Launch ANS**.

Step 8 In the Apply Launch ANS dialog box, click **Yes**.

Step 9 In the Launch ANS confirmation dialog box, click **OK**.

Step 10 Verify that one of the following status appears in the Result column for all the ports:

- Success - Changed—The parameter setpoint was recalculated successfully.
- Success - Unchanged—The parameter setpoint did not need recalculation.
- Not applicable—When ports are not in use.

If one of the following statuses is shown, complete the provided instructions:

- Fail - Out of Range—The calculated setpoint is outside the expected range. If this status appears, do not continue until you have investigated and cleared the cause. This status might appear because of an error in the Cisco Transport Planner file. It could also appear because the insertion loss of the installed cards is greater than the estimated insertion loss calculated by Cisco Transport Planner. If so, the Cisco Transport Planner file will need to be recalculated. All of these possible causes should be investigated. Contact your next level of support if you are unable to clear this status.
- Fail - Missing Input Parameter—The parameter could not be calculated because the required provisioning data is unknown or unavailable. If this status appears, check if the correct Cisco Transport Planner file was imported.
- Unchanged - Port in IS—The parameter could not be calculated because the port is in service. This status should normally not appear at this point in node turn-up. If it does, display the card in card view, change the port administrative state to OOS,DSLB (ANSI) or Locked,disabled (ETSI), and repeat Steps 5 through 10.

Note
If the ports that are in service carry circuits, you must delete the circuits before you can place the ports out of service. See the Creating Optical Channel Circuits and Provisionable Patchcords chapter for information on circuit deletion.

Stop. You have completed this procedure.

NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode

Purpose	This procedure upgrades nodes in single-shelf mode to multishelf mode.
Tools/Equipment	The node you plan to use as the node controller must be equipped with optical units and cannot have a cross-connect card installed. Any nodes that you plan to add to the multishelf configuration as subtending shelves can be equipped with transponder and muxponder units.
Prerequisite Procedures	NTP-G22 Verifying Common Card Installation, on page 4 One of the following procedures in the Cisco ONS 15454 Hardware Installation Guide: • "NTP-G301 Connect the ONS 15454 Multishelf Node and Subtending Shelves to an MS-ISC-100T Card" • "NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950" • "NTP-G308 Connect the ONS 15454 M6 Multishelf Node and the ONS 15454 M6 Subtending Shelves" • "DLP-G682 Connect the ONS 15454 M6 as the Node Controller in a Mixed Multishelf Configuration" DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

Caution An optical shelf in a multishelf configuration must be provisioned as the node controller shelf and not a subtending shelf, otherwise traffic will be dropped. If no slots are available on an optical shelf to install the MS-ISC-100T cards needed for a node controller shelf, install and configure the Cisco Catalyst 2950. See the "NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950" procedure in the Cisco ONS 15454 Hardware Installation Guide.

Note If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

Procedure

Step 1 If you want to configure a shelf as the node controller, continue with Step 2. If you want to configure a shelf as a subtending shelf, continue with Step 3.

Step 2 To set up the login node as the node controller, complete the following steps:

a) In node view (single-node mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **Multishelf Config** tabs.

b) Click **Enable as Node Controller**.

c) From the LAN Config drop-down list, complete one of the following:

- Choose **Ethernet Switch** if MS-ISC-100T cards or the Catalyst 2950 switches are already installed and configured.
- Choose **Stand-Alone** if MS-ISC-100T cards are not installed yet but will be in the final layout or if this is a line amplifier or an OSC-only site. This option will allow a safe migration of the control card database when the multishelf configuration is complete.

d) Click **Apply**.

e) In the confirmation dialog box, click **Yes** to allow the node to reboot. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)

f) After the node reboots, double-click the node. The multishelf view appears.

Note
The shelf ID of the node controller is automatically assigned as 1.

Step 3 To add a node as a subtending shelf in the multishelf configuration, complete the following:

a) In multishelf view, right-click in the white space in the rack and choose **Add Shelf**.

b) Select the type of subtending shelf.

c) In the Shelf ID Selection dialog box, choose a shelf ID (from 2 to 50 if the controller card is TNC, TNCE, TSC, TSCE, or TCC3 card, from 2 to 12 if the controller card is TCC2P card) from the drop-down list.

Note
If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

d) Click **OK**. The shelf appears in the multishelf view.

e) Preprovision the new shelf so that it has the same provisioning as the actual shelf that you will add as the subtending shelf:

Caution
If the subtending shelf is not preprovisioned, traffic will be lost.

- Cards, PPMs, administrative states, client and trunk port configuration—For more information on card and port settings, see the Provisioning Transponder and Muxponder Cards chapter.
- Timing—For more information, see the NTP-G53 Set Up Timing procedure.
- GCC—For more information, see the DLP-G76 Provisioning DCC/GCC Terminations.

f) Disconnect the cross-over (CAT-5) LAN cable from the RJ-45 (LAN) port of the ONS 15454 subtending shelf TCC2/TCC2P/TCC3 card in Slot 7 or Slot 11, or from the EMS port of ONS 15454 M6 subtending shelf.

g) Connect your Windows PC or Solaris workstation NIC to the RJ-45 (LAN) port on the subtending shelf ONS 15454 TCC2/TCC2P/TCC3 card in Slot 7 or Slot 11, or to the EMS port of the ONS 15454 M6 subtending shelf.

h) Complete the DLP-G46 Log into CTC task at the subtending shelf.

i) Click the **Provisioning** > **General** > **Multishelf Config** tabs.

j) Click **Enable as Subtended Shelf**.

k) Select the appropriate subtending shelf.

l) From the Shelf ID drop-down list, choose the shelf ID that you created in Step c.

m) Click **Apply**.

n) In the confirmation dialog box, click **Yes** to reboot the shelf. The CTC view changes to network view and the node icon changes to gray. Wait for the reboot to finish. (This might take several minutes.)

o) Disconnect your Windows PC or Solaris workstation network interface card (NIC) from the RJ-45 (LAN) port of the subtending shelf TCC2/TCC2P/TCC3 card in Slot 7 or Slot 11, or from the EMS port of the ONS 15454 M6 subtending shelf.

p) Reconnect the cross-over (CAT-5) LAN cable (disconnected in Step f) to the RJ-45 (LAN) port of the subtending shelf TCC2/TCC2P/TCC3 card in Slot 7 or Slot 11, or to the EMS port of the ONS 15454 M6 subtending shelf.

Note
The Ethernet cable must be connected to the subtended shelf of the control card soon after the control card completes its boot phase (when it becomes active and its peer control card starts rebooting). Connecting it before the control card completes its boot phase is a risk in the conversion process. Connecting it long time after completion of the boot phase might affect traffic due to missing provisioning.

q) Repeat Steps a through p to set up additional subtending shelves.

Note
Cisco Transport Manager (CTM) users can use the CTM NE Explorer to monitor and configure single-shelf and multishelf nodes. When the upgrade is complete, the original individual subtending shelves will remain the CTM network view and must be manually deleted.

Stop. You have completed this procedure.

NTP-G332 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode with TCC2P Cards as Subtending Shelf Controller

Purpose	This procedure upgrades nodes in single-shelf mode to multishelf mode subtending shelf with ONS 15454 nodes with TCC2P cards in R9.60 or later releases.

Tools/Equipment	The node you plan to use as the node controller must be equipped with optical units and cannot have a cross-connect card installed. Any nodes that you plan to add to the multishelf configuration as subtending shelves can be equipped with transponder and muxponder units. For more information on multishelf configurations, see "Node Reference" chapter.
Prerequisite Procedures	NTP-G22 Verifying Common Card Installation, on page 4 One of the following procedures in the Cisco ONS 15454 Hardware Installation Guide: • "NTP-G301 Connect the ONS 15454 Multishelf Node and Subtending Shelves to an MS-ISC-100T Card" • "NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950" • "NTP-G308 Connect the ONS 15454 M6 Multishelf Node and the ONS 15454 M6 Subtending Shelves" • "DLP-G682 Connect the ONS 15454 M6 as the Node Controller in a Mixed Multishelf Configuration" DLP-G46 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

Caution An optical shelf in a multishelf configuration must be provisioned as the node controller shelf and not a subtending shelf, otherwise traffic will be dropped. If no slots are available on an optical shelf to install the MS-ISC-100T cards needed for a node controller shelf, install and configure the Cisco Catalyst 2950. See the "NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950" procedure in the Cisco ONS 15454 Hardware Installation Guide.

Note If a standalone node has unsupported cards, the node cannot be converted to a node controller or a subtended shelf controller.

Procedure

Step 1 Complete the NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode, on page 84 to configure a single-shelf as a subtending shelf in the multishelf configuration.

Step 2 Connect the subtending shelf to the multishelf node controller. Complete the following tasks in the Cisco ONS 15454 Hardware Installation Guide as appropriate:

- NTP-G301 Connect the ONS 15454 Multishelf Node and Subtending Shelves to an MS-ISC-100T Card.
- NTP-G302 Connect the ONS 15454 Multishelf Node and Subtending Shelves to a Catalyst 2950.
- NTP-G308 Connect the ONS 15454 M6 Multishelf Node and the ONS 15454 M6 Subtending Shelves.
- DLP-G682 Connect the ONS 15454 M6 as the Node Controller in a Mixed Multishelf Configuration.

Step 3 Complete the DLP-G730 Editing the Shelf ID of the Subtending Shelf in a Multishelf Configuration Using the LCD, on page 88 to change the Shelf ID of the subtended shelf in the range between 2 and 50.

Caution
The traffic is lost when you change the Shelf ID of the subtending shelf in a multishelf configuration.

Stop. You have completed this procedure.

DLP-G730 Editing the Shelf ID of the Subtending Shelf in a Multishelf Configuration Using the LCD

Purpose	This task edits the Shelf ID of a subtending shelf using LCD on the fan try assembly. In an ONS 15454 M6 shelf assembly, the LCD panel is a separate unit installed above the external connection unit (ECU).
Tools/Equipment	None
Prerequisite Procedures	NTP-G163 Upgrading Nodes in Single-Shelf Mode to Multishelf Mode, on page 84
Required/As Needed	As needed.
Onsite/Remote	Onsite
Security Level	Superuser only

Caution The traffic is lost when you change the Shelf ID of the subtending shelf in a multishelf configuration.

Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

Procedure

Step 1 On the ONS 15454 front panel, repeatedly press the **Slot** button until SHELF appears on the first line of the LCD. You are in the Shelf menu.

Note
In a ONS 15454 M6 shelf assembly, the LCD is a separate unit installed above the external connection unit (ECU); the **Slot**, **Port**, and **Status** buttons are present on the LCD unit.

Step 2 Repeatedly press the **Port** button until the "Controller Status = MS Configuration" appears on the LCD.

Step 3 Press the **Status** button to display the current multishelf configuration settings.

Step 4 Push the **Slot** button to move to the ID field that you want to change. The selected digit flashes.

Note
The Slot, Status, and Port button positions correspond to the positions of the commands shown on the LCD. For example, you press the Slot button to invoke the Next command and the Status button to invoke the Done command.

Step 5 Press the **Port** button to change the Shelf ID to the desired number.

Step 6 When the change is complete, press the **Status** button to return to the relevant Controller Status menu.

Step 7 Repeatedly press the **Port** button until the Shelf Save Configuration option appears.

Step 8 Press the **Status** button to choose the Save Configuration option.

A Save and REBOOT message appears.

Step 9 Press the **Slot** button to apply the new Shelf ID or press **Port** to cancel the configuration.

Step 10 Saving the new configuration causes the control cards to reboot. During the reboot, a message appears on the LCD. The LCD returns to the normal alternating display after both the control cards finish rebooting.

Step 11 Return to your originating procedure (NTP).