



Manage the Node

This chapter explains how to modify node provisioning for the Cisco ONS 15454 and perform common management tasks such as monitoring the dense wavelength division multiplexing (DWDM) automatic power control (APC) and span loss values. To provision a new node, see [Chapter 3, “Turn Up a Node.”](#) To change default network element settings and to view a list of those settings, refer to the “Network Element Defaults” appendix.



Note

Unless otherwise specified, “ONS 15454” refers to both American National Standards Institute (ANSI) and European Telecommunications Standards Institute (ETSI) shelf assemblies.

Before You Begin

Before performing the following procedures, investigate all alarms and clear any trouble conditions. Refer to the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454 SDH Troubleshooting Guide* as necessary.

This section lists the chapter procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. [NTP-G76 Verify Span Loss, page 10-2](#)—Complete this procedure as needed to view or modify the DWDM span loss values.
2. [NTP-G77 Manage Automatic Power Control, page 10-3](#)—Complete this procedure as needed to manage the DWDM APC.
3. [NTP-G78 View ROADM Node Power Equalization, page 10-5](#)—Complete this procedure as needed to view and update a reconfigurable optical add/drop multiplexing (ROADM) node’s power equalization.
4. [NTP-G80 Change Node Management Information, page 10-6](#)—Complete this procedure as needed to change node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
5. [NTP-G81 Change CTC Network Access, page 10-9](#)—Complete this procedure as needed to change the IP address, default router, subnet mask, network configuration settings, and static routes.
6. [NTP-G82 Customize the CTC Network View, page 10-16](#)—Complete this procedure as needed to create domains and customize the appearance of the network map, including specifying a different default map, creating domains, selecting your own map or image, and changing the background color.
7. [NTP-G83 Modify or Delete Card Protection Settings, page 10-21](#)—Complete this procedure as needed.

8. [NTP-G84 Initiate and Clear Y-Cable and Splitter External Switching Commands, page 10-24](#)—Complete this procedure as needed.
9. [NTP-G85 Modify or Delete OSC Terminations, GCC Terminations, and Provisionable Patchcords, page 10-28](#)—Complete this procedure as needed to modify or delete generic communications channel (GCC) and optical service channel (OSC) terminations, and provisionable patchcords.
10. [NTP-G86 Convert a Pass-Through Connection to an Add/Drop Connection, page 10-32](#)—Complete this procedure as needed to convert a pass-through connection to an add/drop connection.
11. [NTP-G87 Change Node Timing Parameters, page 10-33](#)—Complete this procedure as needed.
12. [NTP-G88 Modify Users and Change Security, page 10-35](#)—Complete this procedure as needed to make changes to user settings, including security level and security policies, and to delete users.
13. [NTP-G131 Convert DWDM Nodes to Hybrid Nodes, page 10-43](#)—Complete this procedure as needed to convert a DWDM node to a hybrid node.
14. [NTP-G89 Change SNMP Settings, page 10-46](#)—Complete this procedure as needed.

NTP-G76 Verify Span Loss

Purpose	This procedure verifies the span loss between two DWDM nodes using Cisco Transport Controller (CTC). You perform this procedure after a node or network modification has occurred and you want to verify that the span loss between the nodes have not changed.
Tools/Equipment	None
Prerequisite Procedures	All procedures in Chapter 3, “Turn Up a Node” and Chapter 6, “Turn Up Network.”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the [“DLP-G155 Verify Optical Span Loss Using CTC” task on page 10-2](#) to check span loss using CTC. This task is faster than a span loss measurement using an optical time domain reflectometer (OTDR) and does not require fibers to be removed. However, the resolution is not as precise as an OTDR measurement.

Stop. You have completed this procedure.

DLP-G155 Verify Optical Span Loss Using CTC

Purpose	This task verifies span loss values between two DWDM nodes using CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24

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

-
- Step 1** In node view, click the **Provisioning > Comm Channels > OSC** tabs. Verify that two OSC terminations are provisioned and have an In-Service and Normal (IS-NR) (ANSI) or Unlocked-enabled (ETSI) service state.
- Step 2** Click the **Maintenance > DWDM > WDM Span Check** tabs.
- Step 3** Click **Retrieve Span Loss Values** to retrieve the latest span loss data.
- Step 4** View the following information:
- Side—Shows the side to which the span loss values apply, either east or west.
 - Min Expected Span Loss (dBm)—Shows the expected minimum span loss (in dBm). You can change the minimum by entering a new value in the field.
 - Meas Span Loss (dBm)—Shows the measured span loss (in dBm).
 - Max Expected Span Loss (dBm)—Shows the expected maximum span loss (in dBm). You can change the minimum by entering a new value in the field.
-  **Note** The minimum and maximum expected span loss values are calculated by Cisco MetroPlanner and imported to the node when you perform the [“NTP-G138 Import a Cisco MetroPlanner Configuration File” task on page 3-72](#).
-
- Resolution (dBm)—Shows the resolution of the span loss measurement (in dBm):
 - +/- 1.5 dB for measured span losses between 0 and 25 dB
 - +/- 2.5 dB for measured span losses between 25 and 38 dB
- If the measured span loss is not between the minimum and maximum expected span loss, contact your site planner for further instructions.
- Step 5** Return to your originating procedure (NTP).
-

NTP-G77 Manage Automatic Power Control

Purpose	This procedure manages the DWDM automatic power control (APC).
Tools/Equipment	None
Prerequisite Procedures	All procedures in the following chapters: Chapter 3, “Turn Up a Node” Chapter 6, “Turn Up Network”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** Complete the “[DLP-G46 Log into CTC](#)” task on page 2-24. If you are already logged in, continue with Step 2.
- Step 2** Complete the following tasks as necessary:
- [DLP-G157 Disable Automatic Power Control, page 10-4](#)
 - [DLP-G158 Enable Automatic Power Control, page 10-4](#)
 - [DLP-G159 Refresh Automatic Power Control Information, page 10-5](#)
- Stop.** You have completed this procedure.
-

DLP-G157 Disable Automatic Power Control

Purpose	This task disables the DWDM APC.
Tools/Equipment	None
Prerequisite Procedures	All procedures in the following chapters: • Chapter 3, “Turn Up a Node” • Chapter 6, “Turn Up Network”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser



Caution

Disable APC only to perform specific troubleshooting or node provisioning tasks. Always enable APC as soon as the tasks are completed. Leaving APC disabled can cause traffic loss.

-
- Step 1** In node view, click the **Maintenance > DWDM > APC** tabs.
- Step 2** Click **Disable APC**.
- Step 3** Verify that the APC State in the information window at the top left of the CTC window changes to Disable- user.
- Step 4** Return to your originating procedure (NTP).
-

DLP-G158 Enable Automatic Power Control

Purpose	This task enables the DWDM APC.
Tools/Equipment	None
Prerequisite Procedures	All procedures in the following chapters: Chapter 3, “Turn Up a Node” Chapter 6, “Turn Up Network”
Required/As Needed	As needed

	Onsite/Remote	Onsite or remote
	Security Level	Superuser
 Caution	Disable APC only to perform specific troubleshooting or node provisioning tasks. Always enable APC as soon as the tasks are completed. Leaving APC disabled can cause traffic loss.	
Step 1	In node view, click the Maintenance > DWDM > APC tabs.	
Step 2	Click Enable APC .	
Step 3	Verify that the APC State in the information window at the top left of the CTC window changes to Enable.	
Step 4	Return to your originating procedure (NTP).	

DLP-G159 Refresh Automatic Power Control Information

Purpose	This task refreshes the DWDM APC information.
Tools/Equipment	None
Prerequisite Procedures	All procedures in the following chapters: Chapter 3, “Turn Up a Node” Chapter 6, “Turn Up Network”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser
Step 1	In node view, click the Maintenance > DWDM > APC tabs.
Step 2	Click Refresh .
Step 3	Return to your originating procedure (NTP).

NTP-G78 View ROADM Node Power Equalization

Purpose	This procedure allows you to view reconfigurable optical add/drop multiplexing (ROADM) node power equalization levels.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

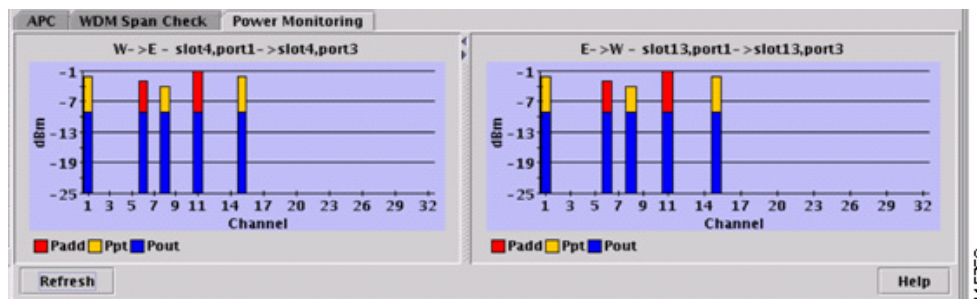
- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.
- Step 2** In node view, click the **Maintenance > DWDM > ROADM Power Monitoring** tabs.
- Step 3** On the Power Monitoring tab, view the following east-to-west (E > W) and west-to-east (W > E) power information:
- Padd—Add power. This power level is represented by the red bar.
 - Ppt—Pass-through power. This power level is represented by the yellow bar.
 - Pout—Output power. This power level is represented by the blue bar. It shows the per-channel (wavelength) power at the 32-WSS output (COM_TX) port.

**Note**

The 32-WSS is designed to handle minor differences in output power. The output power does not need to be exactly the same for all wavelengths.

Figure 10-1 shows an example of ROADM node with equalized output power.

Figure 10-1 Equalized ROADM Power Example



- Step 4** If needed, click **Refresh** to update the display.

Stop. You have completed this procedure.

NTP-G80 Change Node Management Information

Purpose	This procedure changes the node name, date, time, contact information, and login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-G24 Set Up Name, Date, Time, and Contact Information, page 3-8
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.

- Step 2** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 12-2.
- Step 3** Complete the “[DLP-G160 Change the Node Name, Date, Time, and Contact Information](#)” task on page 10-7, as needed.
- Step 4** Complete the “[DLP-G161 Change the Login Legal Disclaimer](#)” task on page 10-8, as needed.
- Step 5** After confirming the changes, complete the “[NTP-G103 Back Up the Database](#)” procedure on page 12-2.
- Stop. You have completed this procedure.**
-

DLP-G160 Change the Node Name, Date, Time, and Contact Information

Purpose	This task changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC , page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

Changing the date, time, or time zone might invalidate the node’s performance monitoring counters.

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

Step 2 Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude
- Location: Description



Note

To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click **Reset Node Position**.

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time
- AIS-V Insertion On STS-1 Signal Degradation - Path: Insert AIS-V on STS-1 SD-P
- AIS-V Insertion On STS-1 Signal Degradation - Path: SD-P BER

See the “[NTP-G24 Set Up Name, Date, Time, and Contact Information](#)” procedure on page 3-8 for detailed field descriptions.

- Step 3** Click **Apply**.
- Step 4** Return to your originating procedure (NTP).

DLP-G161 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

- Step 1** In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.
- Step 2** The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. Use the HTML commands in [Table 10-1](#) to format the text, as needed.

Table 10-1 *HTML Commands for the Legal Disclaimer*

Command	Description
	Begins boldface font
	Ends boldface font
<center>	Aligns type in the center of the window
</center>	Ends the center alignment
<font= <i>n</i> > (where <i>n</i> = font point size)	Changes the font to the new size
	Ends the font size command
<p>	Creates a line break
<sub>	Begins subscript
</sub>	Ends subscript
<sup>	Begins superscript
</sup>	Ends superscript
<u>	Begins underline
</u>	Ends underline

- Step 3** If you want to preview your changed statement and formatting, click the **Preview** subtab.
- Step 4** Click **Apply**.

Step 5 Return to your originating procedure (NTP).

NTP-G81 Change CTC Network Access

Purpose	This procedure changes or deletes network information, including IP settings, static routes, Open Shortest Path First (OSPF) options, proxy tunnels, and firewall tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-G26 Set Up CTC Network Access, page 3-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note

Additional ONS 15454 networking information and procedures, including IP addressing examples, static route scenarios, OSPF protocol, and routing information protocol options are provided in [Chapter 20, “CTC Connectivity Reference.”](#)

Step 1 Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.

Step 2 Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).

Step 3 Perform any of the following tasks as needed:

- [DLP-G162 Change IP Settings, page 10-10](#)
- [DLP-G265 Lock Node Security, page 10-11](#)
- [DLP-G266 Modify Backplane Port IP Settings, page 10-11](#)
- [DLP-G267 Disable Node Security Mode, page 10-12](#)
- [DLP-G163 Modify a Static Route, page 10-13](#)
- [DLP-G164 Delete a Static Route, page 10-14](#)
- [DLP-G165 Disable OSPF, page 10-14](#)
- [DLP-G59 Set Up or Change Open Shortest Path First Protocol, page 3-18](#)
- [DLP-G166 Delete a Proxy Tunnel, page 10-15](#)
- [DLP-G167 Delete a Firewall Tunnel, page 10-15](#)

Step 4 Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).

Stop. You have completed this procedure.

DLP-G162 Change IP Settings

Purpose	This task changes the IP address, subnet mask, default router, Dynamic Host Configuration Protocol (DHCP) access, firewall Internet Inter-Object Request Broker Protocol (IIOP) listener port, LCD IP display, and proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G56 Provision IP Settings, page 3-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser



Caution

Changing the node IP address, subnet mask, or IIOP listener port causes the TCC2/TCC2Ps to reboot. If Ethernet circuits using Spanning Tree Protocol (STP) originate or terminate on E-Series Ethernet cards installed in the node, circuit traffic will be lost for several minutes while the spanning trees reconverge. Other circuits are not affected by TCC2/TCC2P reboots.

Step 1 In node view, click the **Provisioning > Network > General** tabs.

Step 2 Change any of the following, as required:

- IP Address
- Net/Subnet Mask Length
- Default Router
- LCD IP Setting
- Suppress CTC IP Display
- Forward DHCP Request To
- TCC CORBA (IIOP) Listener Port
- Gateway Settings

See the “[DLP-G56 Provision IP Settings](#)” task on page 3-11 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed a network field that will cause the node to reboot, such as the IP address, subnet mask, or TCC Common Object Request Broker Architecture (CORBA) Listener Port, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS 15454 TCC2/TCC2P cards will reboot, one at a time. A TCC2/TCC2P card reboot causes a temporary loss of connectivity to the node, but traffic is unaffected.

Step 5 Confirm that the changes appear on the Provisioning > Network > General tab. If not, refer to the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454 SDH Troubleshooting Guide* as necessary.

Step 6 Return to your originating procedure (NTP).

DLP-G265 Lock Node Security

Purpose	This task locks the ONS 15454 security mode. When security mode is locked, two IP addresses must always be provisioned for the node, one for the TCC2P LAN (TCP/IP) port, and one for the backplane LAN port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G264 Enable Node Security Mode, page 3-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser



Caution

This task is irreversible. Do not proceed unless you want the node to permanently have two IP addresses.



Note

The options in this task are available only when using TCC2P cards.

- Step 1** In node view, click the **Provisioning > Security > Data Comm** tabs.
- Step 2** Click **Lock**.
- Step 3** In the Confirm Lock Secure Mode dialog box, click **Yes**.
- Step 4** Return to your originating procedure (NTP).
-

DLP-G266 Modify Backplane Port IP Settings

Purpose	This task modifies the ONS 15454 backplane IP address, subnet mask, and default router. It also modifies settings that control backplane IP address visibility in CTC and the ONS 15454 LCD. To perform this task, secure mode must be enabled.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-G103 Back Up the Database, page 12-2 DLP-G46 Log into CTC, page 2-24 DLP-G264 Enable Node Security Mode, page 3-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

**Caution**

Provisioning an IP address that is incompatible with the ONS 15454 network might be service affecting.

**Note**

The options in this task are available only when using the TCC2P cards.

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

Step 2 Modify the following fields, as necessary:

- IP Address
- Subnet Mask
- Default Router
- LCD IP Setting—choose one of the following:
 - **Allow Configuration**—Displays the backplane IP address on the LCD and allows it to be changed using the LCD buttons.
 - **Display only**—Displays the backplane IP address on the LCD but does not allow it to be changed using the LCD buttons.
 - **Suppress Display**—Suppresses the display of the IP address on the LCD.
- Suppress CTC IP Address—If checked, suppresses the IP address from display on the Data Comm subtab, CTC node view information area, and other locations.

Step 3 Click **Apply**.

If you changed the IP address, subnet mask, or default router, the node will reboot. This will take 5 to 10 minutes.

Step 4 Return to your originating procedure (NTP).

DLP-G267 Disable Node Security Mode

Purpose	This task disables the ONS 15454 security mode and allows only one IP address to be provisioned for the backplane LAN port and the TCC2P LAN port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G264 Enable Node Security Mode, page 3-16
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

**Note**

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

**Note**

The options in this task are available only when using TCC2P cards.

-
- Step 1** Click the **Provisioning > Security > Data Comm** tabs.
- Step 2** Click **Change Mode**.
- Step 3** Review the information on the Change Secure Mode wizard page, then click **Next**.
- Step 4** On the Node IP Address page, choose the address you want to assign to the node:
- **Backplane Ethernet Port**—Assigns the backplane IP address as the node IP address.
 - **TCC Ethernet Port**—Assigns the TCC2P port IP address as the node IP address.
 - **New IP Address**—Allows you to define a new IP address. If you choose this option, enter the new IP address, subnet mask, and default router IP address.
- Step 5** Click **Next**.
- Step 6** On the SOCKS Proxy Server Settings page, choose one of the following:
- **External Network Element (ENE)**—If selected, the CTC computer is only visible to the ONS 15454 to which the CTC computer is connected. The computer is not visible to the data communications channel (DCC)-connected nodes. 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.
 - **Proxy-only**—If selected, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes for which the node serves as a proxy. The CTC computer is visible to other DCC-connected nodes. The node does not prevent traffic from being routed between the DCC and LAN port.
- Step 7** Click **Finish**.
- Within the next 30 to 40 seconds, the TCC2Ps reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to grey and a DISCONNECTED condition appears.
- Step 8** In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)
- Step 9** Return to your originating procedure (NTP).
-

DLP-G163 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G58 Create a Static Route, page 3-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, click the **Provisioning** > **Network** tabs.
- Step 2** Click the **Static Routing** tab.
- Step 3** Click the static route you want to edit.
- Step 4** Click **Edit**.
- Step 5** In the Edit Selected Static Route dialog box, enter the following:
- Mask
 - Next Hop
 - Cost
- See the “[DLP-G58 Create a Static Route](#)” task on page 3-17 for detailed field descriptions.
- Step 6** Click **OK**.
- Step 7** Return to your originating procedure (NTP).
-

DLP-G164 Delete a Static Route

Purpose	This task deletes an existing static route on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G58 Create a Static Route, page 3-17
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.
- Step 2** Click the static route that you want to delete.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Click **Yes**.
- Step 5** Return to your originating procedure (NTP).
-

DLP-G165 Disable OSPF

Purpose	This task disables the OSPF routing protocol process for an ONS 15454 LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G59 Set Up or Change Open Shortest Path First Protocol, page 3-18

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

-
- Step 1** In node view, click the **Provisioning** > **Network** > **OSPF** tabs. The OSPF subtab has several options.
- Step 2** In the OSPF on LAN area, uncheck the **OSPF active on LAN** check box.
- Step 3** Click **Apply**. Confirm that the changes appear.
- Step 4** Return to your originating procedure (NTP).
-

DLP-G166 Delete a Proxy Tunnel

Purpose	This task removes a proxy tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G97 Provision a Proxy Tunnel, page 7-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** Click the **Provisioning** > **Network** > **Proxy** subtabs.
- Step 2** Click the proxy tunnel that you want to delete.
- Step 3** Click **Delete**.
- Step 4** Continue with your originating procedure (NTP).
-

DLP-G167 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** Click the **Provisioning** > **Network** > **Firewall** subtabs.
- Step 2** Click the firewall tunnel that you want to delete.
- Step 3** Click **Delete**.

Step 4 Return to your originating procedure (NTP).

NTP-G82 Customize the CTC Network View

Purpose	This procedure modifies the CTC network view, including grouping nodes into domains for a less-cluttered display, changing the network view background color, and using a custom image for the network view background.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the “[DLP-G46 Log into CTC](#)” task on [page 2-24](#). If you are already logged in, continue with Step 2.

Step 2 Complete the following tasks, as needed:

- [DLP-G168 Change the Network View Background Color](#), page 10-16
- [DLP-G169 Change the Default Network View Background Map](#), page 10-17
- [DLP-G170 Apply a Custom Network View Background Map](#), page 10-18
- [DLP-G171 Create Domain Icons](#), page 10-18
- [DLP-G172 Manage Domain Icons](#), page 10-19
- [DLP-G173 Enable Dialog Box Do-Not-Display Option](#), page 10-20
- [DLP-G174 Switch Between TDM and DWDM Network Views](#), page 10-21

Stop. You have completed this procedure.

DLP-G168 Change the Network View Background Color

Purpose	This task changes the network view background color or the domain view background color (the area displayed when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC , page 2-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

**Note**

If you modify background colors, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

-
- Step 1** From the View menu in CTC, choose **Go to Network View**.
- Step 2** If you want to change a domain background, double-click the domain. If not, continue with [Step 3](#).
- Step 3** Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.
- Step 4** In the Choose Color dialog box, select a background color.
- Step 5** Click **OK**.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G169 Change the Default Network View Background Map

Purpose	This task changes the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC, page 2-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

**Note**

If you modify the background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

-
- Step 1** From the Edit menu, choose **Preferences > Map** and check the **Use Default Map** check box.
- Step 2** Click **Apply**.
- Step 3** Click **OK**. Verify that the United States map is displayed.
- Step 4** In the network view, double-click on any node on the map.
- Step 5** In the node view, click the **Provisioning > Defaults** tabs.
- Step 6** In the Defaults Selector area, choose **CTC** and then **network**. (You may have to scroll down on the list to find “network.”)
- Step 7** Click the **Default Value** field and choose a default map from the drop-down list. Map choices are Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States.
- Step 8** Click **Apply**.
- Step 9** Click **OK**.
- Step 10** From the View menu, select **Go to Network View**. Confirm that the new map is displayed.
- Step 11** If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the ONS 15454 icons are visible. (You can also choose **Fit Graph to Window**.)

- Step 12** If you need to reposition the node icons, hold down the Ctrl key while you drag and drop them one at a time to a new location on the map.
- Step 13** If you want to change the magnification of the network view map and icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.
- Step 14** Return to your originating procedure (NTP).

DLP-G170 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC, page 2-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher



Note

You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

- Step 1** From the Edit menu, choose **Preferences > Map** and uncheck the **Use Default Map** check box.
- Step 2** From the View menu, choose **Go to Network View**.
- Step 3** Right-click the network or domain map and choose **Set Background Image**.
- Step 4** Click **Browse**. Navigate to the graphic file you want to use as a background.
- Step 5** Select the file. Click **Open**.
- Step 6** Click **Apply** and then click **OK**.
- Step 7** If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15454 icons are visible.
- Step 8** If you need to reposition the node icons, hold down the Ctrl key while you drag and drop them one at a time to a new location on the map.
- Step 9** If you want to change the magnification of the network view map and icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.
- Step 10** Return to your originating procedure (NTP).

DLP-G171 Create Domain Icons

Purpose	This task creates a domain, which is an icon that groups ONS 15454 icons in CTC network view.
Tools/Equipment	None

Prerequisite procedures [DLP-G46 Log into CTC, page 2-24](#)

Required/As needed As needed

Onsite/Remote Onsite or remote

Security Level Provisioning or higher



Note

Domains created by one user are visible to all users who log into the network.

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Right-click the network map and choose **Create New Domain** from the shortcut menu.
- Step 3** When the domain icon appears on the map, click the map name and type the domain name.
- Step 4** Press **Enter**.
- Step 5** Return to your originating procedure (NTP).

DLP-G172 Manage Domain Icons

Purpose This task manages CTC network view domain icons.

Tools/Equipment None

Prerequisite procedures [DLP-G46 Log into CTC, page 2-24](#)

[DLP-G171 Create Domain Icons, page 10-18](#)

Required/As needed As needed

Onsite/Remote Onsite or remote

Security Level Provisioning or higher



Note

All domain changes, such as added or removed nodes, are visible to all users who log into the network.

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Locate the domain action that you want to perform in [Table 10-2](#) and complete the appropriate steps.

Table 10-2 Managing Domains

Domain Action	Steps
Move a domain	Press Ctrl and drag and drop the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose Rename Domain from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the node icon to the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Choose Move Node Back to Parent View .

Table 10-2 **Managing Domains (continued)**

Domain Action	Steps
Open a domain	• Double-click the domain icon, or • Right-click the domain and choose Open Domain.
Return to network view	Right-click the domain view area and choose Go to Parent View from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose Show Domain Overview . The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select Show Domain Overview .
Remove domain	Right-click the domain icon and choose Remove Domain . Any nodes in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-G173 Enable Dialog Box Do-Not-Display Option

Purpose	This task ensures that a user-selected do-not-display dialog box preference is enabled for subsequent sessions or to disable the do-not-display option.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC, page 2-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note

If any user who has rights to perform an operation (for example, creating a circuit) selects the “Do not show this message again” check box in a dialog box, the dialog box is not displayed for any other users who perform that operation on the network from the same computer unless the command is overridden using the following task. (The preference is stored on the computer, not in the node database.)

-
- Step 1** From the Edit menu, choose **Preferences**.
- Step 2** In the Preferences dialog box, click the **General** tab.
- The Preferences Management area field lists all dialog boxes where “Do not show this message again” is enabled.
- Step 3** Choose one of the following options, or uncheck the individual dialog boxes that you want to appear:
- **Don’t Show Any**—Hides all do-not-display check boxes.
 - **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.
- Step 4** Click **OK**.
- Step 5** Return to your originating procedure (NTP).
-

DLP-G174 Switch Between TDM and DWDM Network Views

Purpose	Use this task to switch between time division multiplexing (TDM) and DWDM network views.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC, page 2-24
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

-
- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** From the Network Scope drop-down list on the toolbar located in the upper right portion of the CTC window, choose one of the following:
- **All**—Displays both TDM and DWDM nodes.
 - **TDM**—Displays only ONS 15454s with SONET or SDH cards including the transponder and muxponder cards.
 - **DWDM**—Displays only ONS 15454s with DWDM cards, including the transponder and muxponder cards.
- Step 3** Return to your originating procedure (NTP).
-

NTP-G83 Modify or Delete Card Protection Settings

Purpose	This procedure modifies and deletes card protection settings.
Tools/Equipment	None
Prerequisite Procedures	NTP-G33 Create a Y-Cable Protection Group, page 3-36
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

Modifying and deleting protection groups can be service affecting.

-
- Step 1** Complete the “[DLP-G46 Log into CTC](#)” task on page 2-24. If you are already logged in, continue with Step 2.
- Step 2** Perform any of the following tasks as needed:
- [DLP-G175 Modify a Y-Cable Protection Group, page 10-22](#)
 - [DLP-G176 Modify a Splitter Protection Group, page 10-23](#)
 - [DLP-G177 Delete a Y-Cable Protection Group, page 10-23](#)
- Step 3** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 12-2.

Stop. You have completed this procedure.

DLP-G175 Modify a Y-Cable Protection Group

Purpose	This task modifies a Y-cable protection group for any client port on a MXP_2.5G_10G, TXP_MR_2.5G, or TXP_MR_10G card.
Tools/Equipment	None
Prerequisite Procedures	NTP-G33 Create a Y-Cable Protection Group, page 3-36 DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In node view, click the **Provisioning > Protection** tabs.
- Step 2** In the Protection Groups area, click the Y-cable protection group that you want to modify.
- Step 3** Click **Edit**.
- Step 4** In the Selected Group area, you can modify the following, as needed:
- **Name**—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
 - **Revertive**—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time list. Uncheck this box if you do not want traffic to revert.
 - **Reversion time**—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.
- Step 5** Click **OK**. Confirm that the changes appear.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G176 Modify a Splitter Protection Group

Purpose	This task modifies a splitter protection group for any client port on a TXPP_MR_2.5G or MXPP_MR_2.5G card. Splitter protection is automatically created when the TXPP or MXPP card is installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, click the **Provisioning** > **Protection** tabs.
- Step 2** In the Protection Groups area, click the splitter protection group that you want to modify.
- Step 3** Click **Edit**.
- Step 4** In the Selected Group area, you can modify the following, as needed:
- **Name**—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
 - **Revertive**—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time list. Uncheck this box if you do not want traffic to revert.
 - **Reversion time**—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.
- Step 5** Click **OK**. Confirm that the changes appear.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G177 Delete a Y-Cable Protection Group

Purpose	This task deletes a Y-cable protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, click the **Provisioning** > **Protection** tabs.
- Step 2** In the Protection Groups area, click the protection group you want to delete.
- Step 3** Click **Delete**.
- Step 4** Click **Yes** in the Delete Protection Group dialog box. Confirm that the changes appear.

Step 5 Return to your originating procedure (NTP).

NTP-G84 Initiate and Clear Y-Cable and Splitter External Switching Commands

Purpose	This procedure describes how to apply and remove Manual and Force protection switches on Y-cable and splitter protection groups. It also describes how to apply and remove a Lock On or Lock Out protection command to a Y-cable protection group.
Tools/Equipment	None
Prerequisite Procedures	NTP-G32 Install the Transponder and Muxponder Cards, page 3-31 NTP-G33 Create a Y-Cable Protection Group, page 3-36
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser



Note

Splitter protection groups are automatically created when you install a TXPP_MR_2.5G or MXPP_MR_2.5G card.

- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.
- Step 2** To perform a Manual protection switch, complete the [“DLP-G178 Apply a Manual Y-Cable or Splitter Protection Switch” task on page 10-25](#).
- Step 3** To perform a Force protection switch, complete the [“DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch” task on page 10-25](#).
- Step 4** To clear a Force or Manual protection switch, complete the [“DLP-G180 Clear a Manual or Force Y-Cable or Splitter Protection Switch” task on page 10-26](#).
- Step 5** To prevent traffic on a working or protect card from switching to the other card in the pair, complete the [“DLP-G181 Apply a Lock-On” task on page 10-26](#).
- Step 6** To prevent traffic from switching to the protect card, complete the [“DLP-G182 Apply a Lockout” task on page 10-27](#).
- Step 7** To remove a lock-on or lockout and return a protection group to its usual switching method, complete the [“DLP-G183 Clear a Lock-On or Lockout” task on page 10-28](#).

Stop. You have completed this procedure.

DLP-G178 Apply a Manual Y-Cable or Splitter Protection Switch

Purpose	This task performs a Manual protection switch on a Y-cable or splitter protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher



Caution

A Manual switch will move traffic from the active to the standby card only if network conditions permit it. If conditions change during the switch, CTC will attempt to place traffic back on the original active card.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the Y-cable or splitter protection group where you want to apply the Manual protection switch.
- Step 3** In the Selected Group area, click the active card or port.
- Step 4** In the Switch Commands area, click **Manual**.
- Step 5** In the Confirm Manual Operation dialog box, click **Yes**.
- If conditions permit, the Manual switch will be applied. To clear the Manual switch, see the “[DLP-G180 Clear a Manual or Force Y-Cable or Splitter Protection Switch](#)” task on page 10-26.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch

Purpose	This task performs a Force protection switch on a Y-cable or splitter protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher



Caution

A Force switch will move traffic from the active to the standby card or port immediately, regardless of network conditions. The switch will remain in effect until it is cleared.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the Y-cable or splitter protection group where you want to apply the Force protection switch.

- Step 3** In the Selected Group area, click the active card or port.
- Step 4** In the Switch Commands drop-down list, click **Force**.
- Step 5** In the Confirm Manual Operation dialog box, click **Yes**.
- The Force switch will be applied. To clear the Force switch, see the “[DLP-G180 Clear a Manual or Force Y-Cable or Splitter Protection Switch](#)” task on page 10-26.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G180 Clear a Manual or Force Y-Cable or Splitter Protection Switch

Purpose	This task clears a Manual or Force protection switch on a Y-Cable or splitter protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G178 Apply a Manual Y-Cable or Splitter Protection Switch, page 10-25 or DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch, page 10-25
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, click the protection group that contains the card you want to clear.
- Step 3** In the Selected Group area, click the card that you want to clear.
- Step 4** In the Switch Commands drop-down list, click **Clear**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The Manual or Force protection switch is cleared.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G181 Apply a Lock-On

Purpose	This task prevents traffic from being switched from the working/active card in a Y-cable protection group or port in a splitter protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

**Note**

You can apply the Lock On command only to the working/active card or port. If the working card or port is standby (traffic is switched), the Lock Out button is grayed.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, click the protection group that contains the card (Y-cable) or port (splitter) that you want to lock on.
- Step 3** In the Selected Group area, click the working/active card.
- Step 4** In the Inhibit Switching drop-down list, click **Lock On**.
- Step 5** Click **Yes** in the confirmation dialog box.

The lock on has been applied. Traffic cannot switch to the protect card. To clear the lock on, see the [“DLP-G183 Clear a Lock-On or Lockout” task on page 10-28](#).

**Note**

Provisioning a lock on raises a LOCKON-REQ or an FE-LOCKON condition in CTC. Clearing the lockout switch request clears these conditions.

- Step 6** Return to your originating procedure (NTP).

DLP-G182 Apply a Lockout

Purpose	This task keeps traffic from switching to the protect/standby card or port. The Lock Out command overrides the Force and Manual switching commands.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

**Note**

You can apply the lockout to the protect/standby card or port. If the protect card or port is active (traffic is switched), the lockout task cannot be performed.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, click the protection group that contains the card (Y-cable) or port (splitter) that you want to lock out.
- Step 3** In the Selected Group area, click the protect/standby card.
- Step 4** In the Inhibit Switching drop-down list, click **Lock Out**.
- Step 5** Click **Yes** in the confirmation dialog box.

The lockout has been applied. Traffic cannot switch to the protect card. To clear the lockout, see the [“DLP-G183 Clear a Lock-On or Lockout” task on page 10-28](#).



Note Provisioning a lockout raises a LOCKOUT-REQ or an FE-LOCKOUT condition in CTC. Clearing the lockout switch request clears these conditions.

Step 6 Return to your originating procedure (NTP).

DLP-G183 Clear a Lock-On or Lockout

Purpose	This task clears a lock-on or lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G181 Apply a Lock-On, page 10-26 or DLP-G182 Apply a Lockout, page 10-27
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, click the protection group that contains the card you want to clear.
- Step 3** In the Selected Group area, click the card you want to clear.
- Step 4** In the Inhibit Switching drop-down list, click **Unlock**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The lock on or lockout is cleared.
- Step 6** Return to your originating procedure (NTP).

NTP-G85 Modify or Delete OSC Terminations, GCC Terminations, and Provisionable Patchcords

Purpose	This procedure modifies GCC terminations, and deletes provisionable patchcords, OSC terminations, and GCC terminations.
Tools/Equipment	None
Prerequisite Procedures	DLP-G76 Provision GCC Terminations, page 7-13 or NTP-G38 Provision OSC Terminations and Ring ID, page 3-74 DLP-G99 Create a Provisionable Patchcord, page 6-10

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

**Caution**

Deleting an OSC termination can cause you to lose visibility of nodes that do not have other OSCs or network connections to the CTC computer.

- Step 1** Complete the “[DLP-G46 Log into CTC](#)” task on page 2-24. If you are already logged in, continue with Step 2.
- Step 2** In node view, complete the following tasks as needed:
- To modify a GCC termination, complete the “[DLP-G184 Change a GCC Termination](#)” task on page 10-29.
 - To delete a GCC termination, complete the “[DLP-G185 Delete a GCC Termination](#)” task on page 10-30.
 - To delete an OSC termination, complete the “[DLP-G186 Delete an OSC Termination](#)” task on page 10-30.
 - To delete a provisionable patchcord, complete the “[DLP-G187 Delete a Provisionable Patchcord](#)” task on page 10-31.

Stop. You have completed this procedure.

DLP-G184 Change a GCC Termination

Purpose	This task modifies a GCC termination. You can enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC , page 2-24
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

- Step 1** Click the **Provisioning > Comm Channels > GCC** tabs.
- Step 2** Click the GCC that you want to change.
- Step 3** Click **Edit**.
- Step 4** In the GCC Termination Editor dialog box, complete the following as necessary:
- **GCC Rate**—(Display only) Indicates the GCC rate.
 - **Disable OSPF on SDCC Link**—If checked, Open Shortest Path First is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.
 - **Far End is Foreign**—Check this box to specify that the GCC termination is a non-ONS node.

- Far end IP—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.

Step 5 Click **OK**.

Step 6 Return to your origination procedure (NTP).

DLP-G185 Delete a GCC Termination

Purpose	This task deletes the DWDM GCC terminations required for network setup when using the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note

Deleting the GCC termination on a port also deletes any provisionable patchcord links that might exist on the port.

- Step 1** Determine if the port where you want to delete GCC is in-service (IS). (Click the **Provisioning** > **Line** tabs, and observe the Service State column for that port.) If it is IS, perform the “[DLP-G108 Change the Service State for a Port](#)” task on page 7-17 for that port. If not, go to [Step 2](#).
- Step 2** Click the **Provisioning** > **Comm Channels** > **GCC** tabs.
- Step 3** Click the GCC that you want to delete.
- Step 4** Click **Delete**.
- Step 5** Click **Yes**. GCC-EOC alarms appear until all network GCC terminations are deleted and the ports are out of service.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G186 Delete an OSC Termination

Purpose	This task deletes an OSC termination on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

**Caution**

Deleting a OSC termination might cause node isolation and loss of visibility to nodes that do not have other OSCs or network connections to the CTC computer.

-
- Step 1** Click the **Provisioning > Comm Channels > OSC** tab.
- Step 2** If a Ring ID is created, complete the following steps. Otherwise, continue with [Step 3](#).
- a. Select the DWDM Ring ID that you want to delete and click **Delete**.
 - b. In the Delete DWDM Ring ID confirmation box, click **Yes**. Confirm that the changes appear.
- Step 3** Click the OSC termination that you want to delete and click **Delete**.
- Step 4** In the Delete OSC Termination confirmation box, click **Yes**. Confirm that the changes appear.
- Until all network OSC terminations are deleted, loss of signal (LOS) or power failure alarms on the Optical Booster (OPT-BST) amplifier, OSCM card, and OSC-CSM card might appear.
- Step 5** Return to your originating procedure (NTP).
-

DLP-G187 Delete a Provisionable Patchcord

Purpose	This task deletes a provisionable patchcord.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24 DLP-G99 Create a Provisionable Patchcord, page 6-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

-
- Step 1** In node view, click the **Provisioning > Comm Channels > PPC** tabs. If you are in network view, click **Provisioning > Provisionable Patchcords** tabs.
- Step 2** Click the provisionable patchcord that you want to delete.
- Step 3** Click **Delete**.
- Step 4** In the confirmation dialog box, click **Yes**.
- Step 5** Return to your originating procedure (NTP).
-

NTP-G86 Convert a Pass-Through Connection to an Add/Drop Connection

Purpose	This procedure converts a pass-through connection into add/drop connections (one on the add side and the other on the drop side). Use this procedure during a network upgrade. Pass-through channel connections can be provided between channel input and output ports for the Channel OADM (AD-xC-xx.x), 4-Channel Multiplexer/Demultiplexer (4MD-xx.x), 32-Channel Multiplexer (32MUX-O), and 32-Channel Demultiplexer (32DMX-O and 32DMX) cards. You can set up pass-through connections in nodes that might require more add or drop channel capability or configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

-
- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#) at an ONS 15454 on the network.
- Step 2** In node view, click the **Circuits** tab. Delete the unidirectional or bidirectional pass-through optical channel network connection (OCHNC) that applies to the pass-through connection to be removed.
- Step 3** Remove the physical pass-through cabling. Click the **Provisioning > WDM-ANS > Connections** tabs to identify the card ports to be removed. The pass-through connection that you are removing can be connected in both OADM and hub nodes.
- For a hub node—Connect the 32DMX-O or 32DMX output port to the 32MUX-O input port.
 - For an OADM node—Connect the AD-xC-xx.x drop (TX) port to the AD-xC-xx.x add (RX) port.
- Step 4** Physically connect the proper client interface to the correct add and drop ports.
- Step 5** Delete the filter connections related to the pass-through connection that is being converted to an add/drop connection:
- a. In node view, click the **Provisioning > WDM-ANS > Port Status** tabs.
 - b. Highlight the pass-through connections between ITU channel add and drop ports filters.
 - c. Click **Delete**.
- Step 6** Create two new unidirectional OCHNCs (one heading east, the other heading west) to support the new add/drop channels. See the [“DLP-G105 Provision DWDM Optical Channel Network Connections” task on page 7-10](#).
- Step 7** As necessary, complete the [“DLP-G99 Create a Provisionable Patchcord” task on page 6-10](#).
- Step 8** As necessary, add an optical attenuator between the channel TX port of the OADM, 4MD-xx.x, or 32DMX-O card and the DWDM RX port on the TXP, MXP, or OC-N line card.



Note If the channel is coming from a 32DMX-O, the optical power can be adjusted in CTC by modifying the value of the internal per-channel VOA.

- Step 9** (Optional) The following verification steps might be needed for an intermediate node when a pass-through connection is converted:
- Verify that the received channels are at the specified power level. See the [“NTP-G76 Verify Span Loss” procedure on page 10-2](#) for instructions.
 - Verify that the added channels are equalized with the express channels within ± 1 dB.
 - If the channels are not equalized with the express channels within ± 1 dB, check the attenuation of the VOAs.
 - Check all the fiber adapters to minimize their insertion losses. See the [“NTP-G115 Clean Fiber Connectors” procedure on page 12-22](#) for instructions.
- Stop. You have completed this procedure.**
-

NTP-G87 Change Node Timing Parameters

Purpose	This procedure changes the timing parameters for the ONS 15454. To switch the timing reference, see the “NTP-G112 Change the Node Timing Reference” procedure on page 12-14 .
Tools/Equipment	None
Prerequisite Procedures	NTP-G53 Set Up Timing, page 6-3
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

The following procedure might be service affecting and should be performed during a scheduled maintenance window.

- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).
- Step 3** Click the **Provisioning** > **Timing** > **General** tabs.
- Step 4** In the General Timing section, change any of the following information:

- Timing Mode



Note

Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Revertive Time

See the [“NTP-G53 Set Up Timing” task on page 6-3](#) for field descriptions.

Step 5 In the Reference Lists area, you can change the following information:

**Note**

Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference
- BITS 1 Out
- BITS 2 Out

Step 6 In the BITS In area on the BITS Facilities tab, you can change the following information:

**Note**

The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- BITS In State
- Coding
- Framing
- Sync Messaging
- Admin SSM

Step 7 In the BITS Out area, you can change the following information.

**Note**

If Coding, Framing, or AIS Threshold is set in the BITS In area, it cannot be changed here.

- BITS Out State
- Coding
- Framing
- AIS Threshold
- LBO

Step 8 Click **Apply**. Confirm that the changes appear.

**Caution**

Internal timing is Stratum 3 and is not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 9 Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).

Stop. You have completed this procedure.

NTP-G88 Modify Users and Change Security

Purpose	This procedure modifies user and security properties for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-G23 Create Users and Assign Security, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).
- Step 3** Perform any of the following tasks as needed:
- [DLP-G188 Change Security Policy for a Single Node, page 10-35](#)
 - [DLP-G189 Change Security Policy for Multiple Nodes, page 10-37](#)
 - [DLP-G190 Change Node Access and PM Clearing Privilege, page 10-38](#)
 - [DLP-G191 Change User Password and Security Level on a Single Node, page 10-39](#)
 - [DLP-G192 Change User Password and Security Level for Multiple Nodes, page 10-40](#)
 - [DLP-G193 Delete a User From a Single Node, page 10-40](#)
 - [DLP-G194 Delete a User From Multiple Nodes, page 10-41](#)
 - [DLP-G195 Log Out a User on a Single Node, page 10-42](#)
 - [DLP-G196 Log Out a User on Multiple Nodes, page 10-42](#)
- Step 4** Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).
- Stop. You have completed this procedure.**
-

DLP-G188 Change Security Policy for a Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 2 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level that you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 3 In the User Lockout area, you can modify the following:

- **Failed Logins Before Lockout**—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- **Manual Unlock by Superuser**—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- **Lockout Duration**—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).



Note Manual Unlock by Superuser and Lockout Duration are mutually exclusive.

Step 4 In the Password Change area, you can modify the following:

- **Prevent Reusing Last [] Passwords**—Choose a value between 1 and 10 to set the number of different passwords that the user must create before they can reuse a password.
- **Cannot Change New Password for [] days**—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- **Require Password Change on First Login to New Account**—If checked, requires users to change their password the first time they log into their account.

Step 5 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- **Aging Period**—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
- **Warning Period**—Sets the number days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.

Step 6 In the Other area, you can provision the following:

- **Single Session Per User**—If checked, limits users to one login session at one time.
- **Disable Inactive User**—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 1 to 99 days.

Step 7 Click **Apply**. Confirm that the changes appear.

Step 8 Return to your originating procedure (NTP).

DLP-G189 Change Security Policy for Multiple Nodes

Purpose	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

-
- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > Security > Policy** tabs. A read-only table of nodes and their policies appears.
- Step 3** Click a node on the table that you want to modify, then click **Change**.
- Step 4** If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level that you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.
- Step 5** In the User Lockout area, you can modify the following:
- Failed Logins Before Lockout—The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
 - Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
 - Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).



Note Manual Unlock by Superuser and Lockout Duration are mutually exclusive.

- Step 6** In the Password Change area, you can modify the following:
- Prevent Reusing Last [] Passwords—Choose a value between 1 and 10 to set the number of different passwords that the user must create before they can reuse a password.
 - Cannot Change New Password for [] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
 - Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.
- Step 7** To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:
- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
 - Warning Period—Sets the number days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.
- Step 8** In the Other area, you can provision the following:

- **Single Session Per User**—If checked, limits users to one login session at one time.
 - **Disable Inactive User**—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 1 to 99 days.
- Step 9** In the Select Applicable Nodes area, uncheck any nodes where you do not want to apply the changes.
- Step 10** Click **OK**.
- Step 11** In the Security Policy Change Results dialog box, confirm that the changes are correct, then click **OK**.
- Step 12** Return to your originating procedure (NTP).
-

DLP-G190 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15454 and sets the user security level that can clear node performance monitoring (PM) data.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

- Step 1** In node view, click the **Provisioning > Security > Access** tabs.
- Step 2** In the Access area, provision the following:
- **LAN access**—Choose one of the following options to set the access paths to the node:
 - **No LAN Access**—Allows access to the node only through data communications channel (DCC) connections. Access through the TCC2/TCC2P RJ-45 port and backplane is not permitted.
 - **Backplane only**—Allows access through DCC connections and the backplane. Access through the TCC2/TCC2P RJ-45 port is not allowed.
 - **Front and Backplane**—Allows access through DCC, TCC2/TCC2P RJ-45, and backplane connections.
 - **Restore Timeout**—Sets a time delay for enabling of front and backplane access when DCC connections are lost and “DCC only” is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.
- Step 3** In the Shell Access area, set the shell program used to access the node:
- **Telnet**—If chosen, allows access to the node using Telnet. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). If chosen, choose the Telnet port. Port 23 is the default.
 - **SSH**—If chosen, allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links. If chosen, Port 22 is the default port. It cannot be changed.

- Enable Shell Password—If checked, enables the SSH password. To disable the password, you must uncheck the check box and click Apply. You must type the password in the confirmation dialog box and click OK to disable it.
- Step 4** In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.
- Step 5** Click **Apply**.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G191 Change User Password and Security Level on a Single Node

Purpose	This task changes settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 2 Click the user whose settings you want to modify, then click **Edit**.

Step 3 In the Change User dialog box, you can:

- Change a user password.
- Modify the user security level.
- Lock out the user.
- Disable the user.
- Force the user to change password on next login.

See the “[DLP-G54 Create a New User on a Single Node](#)” procedure on page 3-6 for field descriptions.

Step 4 Click **OK**.

Step 5 Click **OK** in the confirmation dialog box.



Note User settings that you changed during this task will not appear until that user logs off and logs back in.

Step 6 Return to your originating procedure (NTP).

DLP-G192 Change User Password and Security Level for Multiple Nodes

Purpose	This task changes settings for an existing user at multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser


Note

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

-
- Step 1** From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to change the users.
- Step 2** Click the **Provisioning > Security > Users** tabs. Highlight the user's name whose settings you want to change.
- Step 3** Click **Change**. The Change User dialog box appears.
- Step 4** In the Change User dialog box, you can:
- Change a user's password.
 - Modify the user's security level.
 - Lock out the user.
- See the “[DLP-G55 Create a New User on Multiple Nodes](#)” task on page 3-6 for field descriptions.
- Step 5** In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).
- Step 6** Click **OK**. A Change Results confirmation dialog box appears.
- Step 7** Click **OK** to acknowledge the changes.
- Step 8** Return to your originating procedure (NTP).
-

DLP-G193 Delete a User From a Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

**Note**

You cannot delete a user who is currently logged in. To log out a user, you can complete the “[DLP-G195 Log Out a User on a Single Node](#)” task on page 10-42, or you can choose the “Logout before delete” option in the Delete User dialog box.

**Note**

CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

-
- Step 1** In node view, click the **Provisioning > Security > Users** tabs.
- Step 2** Choose the user you want to delete.
- Step 3** Click **Delete**.
- Step 4** In the Delete User dialog box, verify that the user name displayed is the one you want to delete. Click **Logout before delete** if the user is currently logged in. (You cannot delete users if they are logged in.)
- Step 5** Click **OK**.
- Step 6** In the User Deletion Results box, click **OK**.
- Step 7** Return to your originating procedure (NTP).
-

DLP-G194 Delete a User From Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

**Note**

You cannot delete a user who is currently logged in. To log out a user, you can complete the “[DLP-G196 Log Out a User on Multiple Nodes](#)” task on page 10-42, or you can choose the “Logout before delete” option in the Delete User dialog box.

**Note**

CTC will allow you to delete other Superusers if one Superuser remains. For example, you can delete the CISCO15 user if you have created another Superuser. Use this option with caution.

-
- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > Security** tabs. Highlight the name of the user you want to delete.
- Step 3** Click **Delete**. The Delete User dialog box appears.
- Step 4** In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete this user.
- Step 5** Click **OK**. A User Deletion Results confirmation dialog box appears.

- Step 6** Click **OK** to acknowledge the changes. Confirm that the changes appear.
- Step 7** Return to your originating procedure (NTP).
-

DLP-G195 Log Out a User on a Single Node

Purpose	This task logs out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

- Step 1** In node view, click the **Provisioning > Security > Active Logins** tabs.
- Step 2** Choose the user that you want to log out and click **Logout**.
- Step 3** In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out. This prevents the user from logging in after logout based on user lockout parameters provisioned in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the “[DLP-G188 Change Security Policy for a Single Node](#)” task on [page 10-35](#) for more information.
- Step 4** Click **OK**.
- Step 5** Click **OK** to confirm the logout.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G196 Log Out a User on Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

- Step 1** From the View menu, chose **Go to Network View**.
- Step 2** Click the **Provisioning > Security > Active Logins** tabs.
- Step 3** Choose the user you want to log out.
- Step 4** Click **Logout**.
- Step 5** In the Logout User dialog box, check the nodes where you want to log out the user.

- Step 6** Check **Lockout before Logout** if you want to lock the user out prior to logout. This prevents the user from logging in after logout based on user lockout parameters provisioned in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the [“DLP-G189 Change Security Policy for Multiple Nodes” task on page 10-37](#) for more information.
- Step 7** In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user’s settings (all network nodes are selected by default).
- Step 8** Click **OK**.
- Step 9** Click **OK** in the confirmation dialog box.
- Step 10** Return to your originating procedure (NTP).

NTP-G131 Convert DWDM Nodes to Hybrid Nodes

Purpose	This procedure upgrades an OSCM card to an OSC-CSM card. OSCM cards use Slots 8 and 10, which are required for cross-connect cards in TDM and DWDM hybrid configurations. The OSC-CSM cards use Slots 1 to 6 and 12 to 17.
Tools/Equipment	Two OSC-CSM cards
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Maintenance or higher



Note You cannot perform this upgrade on software released prior to Software Release 4.6.



Note Downgrade procedures from OSC-CSM cards to OSCM cards are not supported. Contact the Cisco Technical Assistance Center (TAC) for more information. See the [“Obtaining Technical Assistance” section on page lxxiv](#).

- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#) at the node where you will perform the upgrade. If you are already logged in, continue with Step 2.
- Step 2** Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).
- Step 3** If you have timing set up on the OSCM card, delete the timing source:
- In node view, click the **Provisioning > Timing** tabs.
 - Scroll to the Reference Lists area.
 - In the NE Reference column, select **Internal Clock** from the drop-down list for all entries where the selected Clock Source is the OSCM that you are removing.
 - Click **Apply**.
- Step 4** If you have overhead circuits on the node, complete the [“DLP-G112 Delete Overhead Circuits” task on page 7-21](#).

- Step 5** Delete the DWDM ring ID:
- In node view, click the **Provisioning > Comm Channels > OSC** tabs.
 - Select the DWDM Ring ID that you want to delete and click **Delete**.
 - In the Delete DWDM Ring ID confirmation box, click **Yes**. Confirm that the changes appear.
- Step 6** If you have OSC terminations, refer to the [“DLP-G186 Delete an OSC Termination” task on page 10-30](#) to delete the OSC termination.
- Step 7** Delete the OSCM card wavelength division multiplexing-automatic node setup (WDM-ANS) connections:
- In node view, click the **Provisioning > WDM-ANS > Connections** tabs.
 - Select the connection to be deleted.
 - Click **Delete**.
 - In the Delete Optical Link dialog box, click **Yes**.
- Step 8** Delete the card from CTC:
- In node view, right-click the OSCM card.
 - Select **Delete Card** from the menu.
- The card name disappears and the slot turns gray.
- Step 9** Remove the cables from the OSCM OSC ports.
- Step 10** Physically replace the deleted OSCM card on the ONS 15454 with an OSC-CSM card:

**Note**

The OSCM card and OSC-CSM card do not have the same slot requirements.

- Open the OSCM card ejectors.
- Slide the card out of Slot 8 or 10.
- Open the ejectors on the OSC-CSM card.
- Slide the OSC-CSM card into the slot along the guide rails. Use ONS 15454 card Slots 1 to 6 or 12 to 17, according to your site plan.
- Close the ejectors.

**Note**

On the OSC-CSM card, the fail LED above the ACT/STBY LED becomes red, blinks for several seconds, and turns off. The ACT/STBY LED turns green and remains on. In node view, the OSC-CSM appears green.

- Step 11** If an OSCM card was removed from Slot 8 and an OSC-CSM card was installed in Slots 12 to 17, modify the OSC-CSM line direction from east-to-west to west-to-east.

**Note**

The Cisco MetroPlanner configuration file labels the OSC-CSM card as west even if it is installed in the east side of the node.

- To modify the OSC-CSM card line direction, double-click the OSC-CSM card in node view. The card view appears.
- Click the **Provisioning > Optical Line > Parameter** tabs.

- b. In the port number 2 line, click the Line Direction drop-down list and choose **West to East**.
- c. Click **Apply**.

Step 12 If an OSCM card was removed from Slot 10 and an OSC-CSM card was installed in Slots 1 to 6, modify the OSC-CSM line direction from west-to-east to east-to-west.



Note The Cisco MetroPlanner configuration file will label the OSC-CSM card as east even if it is installed in the west side of the node.

- a. To modify the OSC-CSM card line direction, double-click the OSC-CSM card in node view. The card view appears.
- b. Click the **Provisioning > Optical Line > Parameter** tabs.
- c. In the port number 2 line, click the Line Direction drop-down list and choose **East to West**.
- d. Click **Apply**.

Step 13 Calculate default connections using WDM-ANS:

- a. Click the CTC up arrow to get back to node view.
- a. In node view, click the **Provisioning > WDM-ANS > Connections** tabs.
- b. Click the **Calculate Connections** button.

Step 14 Connect the cables from the OSC-CSM LINE ports to the OPT-BST amplifier OSC ports. Follow the recommended connections that were automatically calculated in the **Connections** tab as described in Step 13.

Step 15 Launch ANS port regulation:

- a. In node view, click the **Provisioning > WDM-ANS > Port Status** tabs.
- b. Click the **Launch ANS** button.
- c. In the Link Status column, the ports change to Regulated.

Step 16 Create OSC terminations starting from the OSC-CSM card. See the [“NTP-G38 Provision OSC Terminations and Ring ID” procedure on page 3-74](#).

Step 17 (Optional) If you want to set up timing on the OSC-CSM card, create the timing source:

- a. In node view, click the **Provisioning > Timing** tabs.
- b. Scroll down to the Reference Lists area.
- c. In the NE Reference column, select **Internal Clock** from the drop-down list for all entries where the selected Clock Source is the OSC-CSM that you are adding.
- d. Click **Apply**.

Step 18 (Optional) Complete the [“NTP-G60 Create Overhead Circuits” procedure on page 7-13](#).

Step 19 Repeat Steps 3 through 18 for each OSCM card you are replacing in the node.

Step 20 If you are installing cross-connect cards, refer to the *Cisco ONS 15454 Procedure Guide* or the *Cisco ONS 15454 SDH Procedure Guide* for instructions.

Stop. You have completed this procedure.

NTP-G89 Change SNMP Settings

Purpose	This procedure modifies Simple Network Management Protocol (SNMP) settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-G28 Set Up SNMP, page 3-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-24](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).
- Step 3** Perform any of the following tasks as needed:
- [DLP-G197 Modify SNMP Trap Destinations, page 10-46](#)
 - [DLP-G198 Delete SNMP Trap Destinations, page 10-47](#)
- Step 4** Complete the [“NTP-G103 Back Up the Database” procedure on page 12-2](#).
- Stop. You have completed this procedure.**
-

DLP-G197 Modify SNMP Trap Destinations

Purpose	This task modifies the SNMP trap destinations on an ONS 15454 including community name, default User Datagram Protocol (UDP) port, SNMP trap version, and maximum traps per second.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, click the **Provisioning > SNMP** tabs.
- Step 2** Select a destination trap from the **Trap Destinations** area.
- For a description of SNMP traps, refer to the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454 SDH Troubleshooting Guide*.
- Step 3** Highlight the Destination row field entry in the Community column and change the entry to another valid community name.
- The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the network management system.

- Step 4** If needed, modify the UDP port in the UDP Port field. The default UDP port for SNMP is 162.
- Step 5** Set the Trap Version field for either SNMPv1 or SNMPv2.
Refer to your network management system (NMS) documentation to determine whether to use SNMPv1 or SNMPv2.
- Step 6** If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.
- Step 7** If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistics retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box located on the SNMP tab.
- Step 8** Click **Apply**.
- Step 9** SNMP settings are now modified. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations area. Confirm that the changes appear.
- Step 10** Return to your originating procedure (NTP).
-

DLP-G198 Delete SNMP Trap Destinations

Purpose	This task deletes SNMP trap destinations on an ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-24
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In node view, click the **Provisioning > SNMP** tabs.
- Step 2** In the Trap Destinations area, click the destination trap that you want to delete.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Click **Yes**. Confirm that the changes appear.
- Step 5** Return to your originating procedure (NTP).
-

