



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 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 *Cisco ONS 15454 Release 4.7 Network Element Defaults* document.



Note

Unless otherwise specified, “ONS 15454” refers to both ANSI and 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 SONET and DWDM 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 9-2](#)—Complete this procedure as needed to view or modify the DWDM span loss values.
2. [NTP-G77 Manage Automatic Power Control, page 9-4](#)—Complete this procedure as needed to manage the DWDM automatic power control.
3. [NTP-G78 View ROADM Node Power Equalization, page 9-6](#)—Complete this procedure as needed to view and update a reconfigurable optical add/drop management node power equalization.
4. [NTP-G79 Modify Automatic Node Setup Parameters, page 9-7](#)—Complete as needed.
5. [NTP-G80 Change Node Management Information, page 9-8](#)—Complete this procedure as needed to change node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
6. [NTP-G81 Change CTC Network Access, page 9-10](#)—Complete this procedure as needed to change the IP address, default router, subnet mask, network configuration settings, and static routes.
7. [NTP-G82 Customize the CTC Network View, page 9-15](#)—As needed, complete this procedure 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.
8. [NTP-G83 Modify or Delete Card Protection Settings, page 9-20](#)—Complete as needed.
9. [NTP-G84 Initiate and Clear Y-Cable and Splitter External Switching Commands, page 9-23](#)—Complete as needed.

10. [NTP-G85 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 9-28](#)—Complete this procedure as needed to modify or delete generic communications channel (GCC) and optical service channel (OSC) terminations, and provisionable patchcords.
11. [NTP-G86 Convert a Pass-Through Connection to an Add/Drop Connection, page 9-31](#)—Complete this procedure as needed to convert a pass-through connection to an add/drop connection.
12. [NTP-G87 Change Node Timing Parameters, page 9-32](#)—Complete as needed.
13. [NTP-G88 Modify Users and Change Security, page 9-34](#)—Complete this procedure as needed to make changes to user settings, including security level and security policies, and to delete users.
14. [NTP-G89 Change SNMP Settings, page 9-42](#)—Complete as needed.

NTP-G76 Verify Span Loss

Purpose	This procedure verifies the span loss between two DWDM nodes using 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	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	All procedures in Chapter 3, “Turn Up a Node.”
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 2-25](#). If you are already logged in, continue with Step 2.
- Step 2** Perform the following span loss verification tasks as needed:
- Complete the [“DLP-G155 Verify Optical Span Loss Using CTC” task on page 9-3](#) 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.
 - Complete [“DLP-G156 Measure Span Insertion Loss Using an OTDR” task on page 9-4](#) to measure the span loss using an OTDR.

Stop. You have completed this procedure.

DLP-G155 Verify Optical Span Loss Using CTC

Purpose	This procedure verifies span loss values between two DWDM nodes using CTC.
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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 and modify 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 Expected 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 “[DLP-G74 Import a Cisco MetroPlanner Configuration File](#)” task on page 3-59.
- 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
- Step 5** If you modified the minimum or maximum expected span losses, click **Apply**. If not, continue with [Step 6](#).
- Step 6** Return to your originating procedure (NTP).
-

DLP-G156 Measure Span Insertion Loss Using an OTDR

Purpose	This task measures the span insertion loss using an optical time domain reflectometer (OTDR). You perform this task when OSC terminations fail to turn up properly and initial troubleshooting, including checks of the Optical Service Channel and Combiner/Splitter Module (OSC-CSM) or Optical Service Channel Module (OSCM) port states and physical fiber connections, do not solve the problem.
Tools/Equipment	OTDR test and measurement device.
Prerequisite Procedures	DLP-G75 Create OSC Terminations, page 3-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** Remove one of the fiber connections of the fiber span you will measure.
- Step 2** Following the instructions in the OTDR documentation, connect the OTDR to the end of the fiber.
- Step 3** Measure the insertion loss using the procedures in the OTDR documentation.
- Step 4** Display your site plan in MetroPlanner. Enter the insertion loss values calculated from the insertion loss measurement and recalculate the site plan. If the new insertion loss values are accepted, MetroPlanner will create a new configuration file. If so, continue with [Step 5](#). If the new insertion loss values require changes to the physical site, for example, additional cards or nodes, install the new nodes and cards following procedures in [Chapter 1, “Install the Shelf and Common Control Cards,”](#) and [Chapter 3, “Turn Up a Node.”](#)
- Step 5** If the span is out of range and the MetroPlanner design changed, complete the “[DLP-G74 Import a Cisco MetroPlanner Configuration File](#)” task on [page 3-59](#) at each node in the network.
- Step 6** Return to your originating procedure (NTP).
-

NTP-G77 Manage Automatic Power Control

Purpose	This procedure manages the DWDM automatic power control (APC).
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	All procedures in Chapter 3, “Turn Up a Node.”
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 2-25](#). 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 9-5](#)

- [DLP-G158 Enable Automatic Power Control](#), page 9-5
- [DLP-G159 Refresh Automatic Power Control Information](#), page 9-6

Stop. You have completed this procedure.

DLP-G157 Disable Automatic Power Control

Purpose	This task disables the DWDM automatic power control (APC).
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	All procedures in Chapter 3, “Turn Up a Node.”
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** Click the **Maintenance > DWDM > APC** tabs.
- Step 2** Click **Disable APC**,
- Step 3** On the confirmation dialog box, Click **Yes**.
- Step 4** Return to your originating procedure.
-

DLP-G158 Enable Automatic Power Control

Purpose	This procedure enables the DWDM automatic power control (APC).
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	All procedures in Chapter 3, “Turn Up a Node.”
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** Click the **Maintenance > DWDM > APC** tabs.
- Step 2** Click **Enable APC**.
- Step 3** On the confirmation dialog box, Click **Yes**.
-

Step 4 Return to your originating procedure.

DLP-G159 Refresh Automatic Power Control Information

Purpose	This procedure refreshes the DWDM automatic power control information.
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	All procedures in Chapter 3, “Turn Up a Node.”
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Click the **Maintenance > DWDM > APC** tabs.

Step 2 Click **Refresh**.

Step 3 Return to your originating procedure.

Stop. You have completed this procedure.

NTP-G78 View ROADM Node Power Equalization

Purpose	This task 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 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

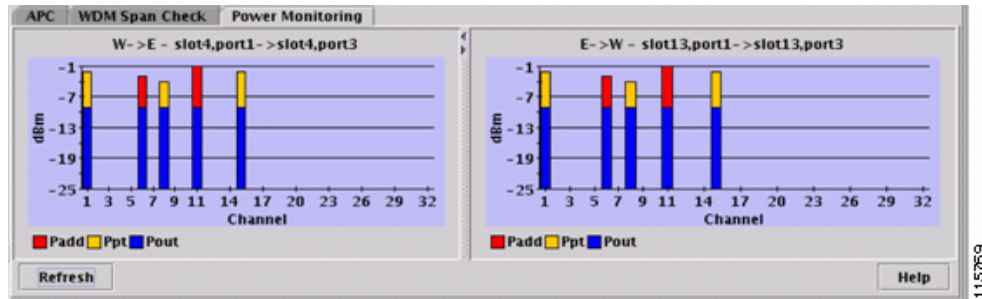
Step 1 Complete the “[DLP-G46 Log into CTC](#)” task on page 2-25. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Maintenance > DWDM > 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.
- Ppt—Pass-through power.
- Pout—Output power. The output power for all wavelengths does not need to be exactly the same for all wavelengths, but does need to be within the same range. [Figure 9-1](#) shows an example of ROADM node with equalized output power.

Figure 9-1 Equalized ROADM Power Example



- Step 4** If needed, click **Refresh** to update the display.
Stop. You have completed this procedure.

NTP-G79 Modify Automatic Node Setup Parameters

Purpose	Use this procedure to manually modify the DWDM automatic node setup (ANS) parameters.
Tools/Equipment	A node provisioning plan prepared by Cisco MetroPlanner is required.
Prerequisite Procedures	You must use Cisco MetroPlanner or another DWDM network calculation tool to prepare a configuration file for your network. NTP-G30 Install the DWDM Cards, page 3-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser



Caution

ANS parameters are normally not changed manually. Changes to the parameters at one node often require adjustments at other network nodes, and anticipating the changes is difficult. In general, you should always enter node or network changes in Cisco MetroPlanner, recalculate the parameters, then import them into the node and run ANS.

- Step 1** Complete the [“DLP-G46 Log into CTC” task on page 2-25](#). If you are already logged in, continue with Step 2.
- Step 2** Click the **WDM-ANS > Provisioning** tabs. ANS parameter groups are shown in tree view under the Selector area. Click a parameter group to view the individual parameters in it, for example, if you click the node name, all ANS parameters are shown. If you click West Side, only West Side parameters are shown, and if you click Amplifiers, only amplifier parameters are shown.
- For a list of ANS parameters by node type, refer to [Table 15-4 on page 15-26](#). For an ANS parameter summary including minimum, maximum, and default values, refer to [Table 15-5 on page 15-29](#).
- Step 3** To modify a parameter’s value, click the parameter under the Parameter column and modify its value in the Value column.
- Step 4** Click **Apply**.

Step 5 Click the **Port Status** tab. Click **Launch ANS**.

ANS (Automatic Node Setup) automatically calculates the variable optical attenuator (VOAs) setpoints to match the expected channel profile at the amplifier input port.

Stop. You have completed this procedure.

NTP-G80 Change Node Management Information

Purpose	This procedure changes the node name, date, time, contact information, and the login legal disclaimer.
Tools/Equipment	None
Prerequisite Procedures	NTP-G24 Set Up Name, Date, Time, and Contact Information, page 3-6
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 2-25. If you are already logged in, continue with Step 2.
- Step 2** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.
- Step 3** In node view, click the **Provisioning > General** tabs.
- Step 4** Complete the “[DLP-G160 Change the Node Name, Date, Time, and Contact Information](#)” task on page 9-8, as needed.
- Step 5** Complete the “[DLP-G161 Change the Login Legal Disclaimer](#)” task on page 9-9, as needed.
- Step 6** After confirming the changes, complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.
- Stop. You have completed this procedure.**

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

Purpose	This procedure changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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** 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 Degrade - Path: Insert AIS-V on STS-1 SD-P
- AIS-V Insertion On STS-1 Signal Degrade - Path: SD-P BER

See the “[NTP-G24 Set Up Name, Date, Time, and Contact Information](#)” procedure on page 3-6 for detailed field descriptions.

Step 3 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

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 2-25
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 9-1](#) to format the text, as needed.

Table 9-1 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> = 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 3-8
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 19, “CTC Connectivity Reference.”](#)

- Step 1** Complete the “[DLP-G46 Log into CTC](#)” task on page 2-25. If you are already logged in, continue with Step 2.
- Step 2** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.

- Step 3** Perform any of the following tasks as needed:
- [DLP-G162 Change IP Settings, page 9-11](#)
 - [DLP-G163 Modify a Static Route, page 9-12](#)
 - [DLP-G164 Delete a Static Route, page 9-13](#)
 - [DLP-G165 Disable OSPF, page 9-13](#)
 - [DLP-G59 Set Up or Change Open Shortest Path First Protocol, page 3-16](#)
 - [DLP-G166 Delete a Proxy Tunnel, page 9-14](#)
 - [DLP-G167 Delete a Firewall Tunnel, page 9-14](#)
- Step 4** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.
- Stop. You have completed this procedure.**
-

DLP-G162 Change IP Settings

Purpose	This task changes the IP address, subnet mask, default router, DHCP access, firewall IIOP listener port, LCD IP display, and proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25 DLP-G56 Provision IP Settings, page 3-9
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 TCC2s 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 reboots.

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

- Step 2** Change any of the following:
- IP Address
 - Suppress CTC IP Display
 - LCD IP Setting
 - Default Router
 - Forward DHCP Request To
 - MAC Address
 - Net/Subnet Mask Length
 - TCC CORBA (IIOP) Listener Port

- Gateway Settings

See the “[DLP-G56 Provision IP Settings](#)” task on page 3-9 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 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 cards will reboot, one at a time. A TCC2 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 the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 SONET and DWDM Troubleshooting Guide* as necessary.

Step 6 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 2-25 DLP-G58 Create a Static Route , page 3-15
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 3-15 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 2-25 DLP-G58 Create a Static Route, page 3-15
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 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 Open Shortest Path First (OSPF) routing protocol process for an ONS 15454 LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25 DLP-G59 Set Up or Change Open Shortest Path First Protocol, page 3-16
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; if not, repeat the task.
- 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 2-25
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 2-25
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 2-25. 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 9-15
- [DLP-G169 Change the Default Network View Background Map](#), page 9-16
- [DLP-G170 Apply a Custom Network View Background Map](#), page 9-17
- [DLP-G171 Create Domain Icons](#), page 9-17
- [DLP-G172 Manage Domain Icons](#), page 9-18
- [DLP-G173 Enable Dialog Box Do-Not-Display Option](#), page 9-19
- [DLP-G174 Switch Between TDM and DWDM Network Views](#), page 9-20

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 2-25
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, 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 2-25
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** In the node view, click the **Provisioning > Defaults** tabs.
- Step 3** In the Defaults Selector area, choose **CTC** and then **network**.
- Step 4** 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 (default).
- Step 5** Click **Apply**. The new network map appears.
- Step 6** Click **OK**.
- Step 7** 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 8** If you need to reposition the node icons, 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 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-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 2-25
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, 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 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 2-25
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 2-25 DLP-G171 Create Domain Icons, page 9-17
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 9-2](#) and complete the appropriate steps.

Table 9-2 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 .
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	Use this task to ensure 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 2-25
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 dialog 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 dialog 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 TDM (time division multiplexing) and DWDM (dense wavelength division multiplexing) network views.
Tools/Equipment	None
Prerequisite procedures	DLP-G46 Log into CTC, page 2-25
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, 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 3-33
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 2-25](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the “[NTP-G103 Back Up the Database](#)” procedure on [page 11-2](#).
- Step 3** Perform any of the following tasks as needed:
- [DLP-G175 Modify a Y-Cable Protection Group, page 9-21](#)
 - [DLP-G176 Modify a Splitter Protection Group, page 9-22](#)
 - [DLP-G177 Delete a Y-Cable Protection Group, page 9-22](#)

- Step 4** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.
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 3-33 DLP-G46 Log into CTC , page 2-25
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** 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 4** Click **Apply**. Confirm that the changes appear; if not, repeat the task.
- Step 5** 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 card or MXPP_MR_2.5G. Splitter protection is automatically created when the TXPP transponder or MXPP muxponder card is installed.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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** 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 4** Click **Apply**. Confirm that the changes appear; if not, repeat the task.
- Step 5** 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 2-25
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; if they do not, repeat Steps 1 through 3.
- 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 a 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 3-30 NTP-G33 Create a Y-Cable Protection Group, page 3-33
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 2-25](#). 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 9-24](#).
- Step 3** To perform a Force protection switch, complete the [“DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch” task on page 9-24](#).
- 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 9-25](#).
- 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 9-26](#).
- Step 6** To prevent traffic from switching to the protect card, complete the [“DLP-G182 Apply a Lock Out” task on page 9-26](#).
- 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 Lock Out” task on page 9-27](#).

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 2-25
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** From Switch Commands, 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 9-25](#).
- 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 2-25
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** From Switch Commands, click **Force**.
- Step 5** In the Confirm Manual Operation dialog box, click **Yes**.
The Manual 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 9-25.
- 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 2-25 DLP-G178 Apply a Manual Y-Cable or Splitter Protection Switch, page 9-24 or DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch, page 9-24
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** From Switch Commands, 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 2-25
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 greyed.

-
- 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) you want to lock on.
- Step 3** In the Selected Group area, click the working/active card.
- Step 4** From Inhibit Switching, 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 Lock Out](#)” task on page 9-27.


Note

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

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

DLP-G182 Apply a Lock Out

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 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher


Note

You can apply the Lock Out to the protect/standby card or port. If the protect card or port is active (traffic is switched), the Lock Out 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) you want to lock out.
- Step 3** In the Selected Group area, click the protect/standby card.
- Step 4** From Inhibit Switching, click **Lock Out**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The lock out has been applied. Traffic cannot switch to the protect card. To clear the lock out, see the [“DLP-G183 Clear a Lock On or Lock Out” task on page 9-27](#).



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

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

DLP-G183 Clear a Lock On or Lock Out

Purpose	This task clears a lock on or lock out.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25 DLP-G181 Apply a Lock On, page 9-26 or DLP-G182 Apply a Lock Out, page 9-26
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** From Inhibit Switching, click **Unlock**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The Lock On or Lock Out is cleared.
- Step 6** Return to your originating procedure (NTP).
-

NTP-G85 Modify or Delete Communications Channel Terminations and Provisionable Patchcords

Purpose	This procedure modifies and deletes GCC and OSC terminations, as well as deletes provisionable patchcords on the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-G76 Provision GCC Terminations, page 3-62 or DLP-G75 Create OSC Terminations, page 3-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

Deleting a 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 2-25. 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 9-28.
 - To delete a GCC termination, complete the “[DLP-G185 Delete a GCC Termination](#)” task on page 9-29.
 - To delete an OSC termination, complete the “[DLP-G186 Delete an OSC Termination](#)” task on page 9-30.
 - To delete a provisioning patchcord, complete the “[DLP-G187 Delete a Provisionable Patchcord](#)” task on page 9-30.

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 2-25
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 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** Click the **Provisioning > Comm Channel > GCC** tabs.
- Step 2** In the GCC Terminations pane, click **Delete**.
- Step 3** In the Delete GCC Terminations dialog box, check **Set port OOS** check box if you want to place ports out of service.
- Step 4** Click **Yes**. GCC-EOC alarms appear until all network GCC terminations are deleted and the ports are out of service.
- Step 5** 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 2-25
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 **OSC** tab.
- Step 2** Click the OSC termination you want to delete and click **Delete**.
- Step 3** In the Delete OSC Termination confirmation box, click **Yes**. Confirm that the changes appear; if not, repeat the task.
- 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 4** 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 2-25
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher



Note

Deleting the GCC termination on a port also deletes the provisionable patchcord link on the port.

-
- Step 1** In node view, click the **Provisioning > Comm Channels > Provisionable Patchcords** 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 2-25
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 2-25](#) 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 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 6-9](#).
- Step 7** As necessary, complete the [“DLP-G99 Create a Provisionable Patchcord” task on page 5-12](#).
- 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 9-2](#) 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 11-32](#) 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 11-24 .
Tools/Equipment	None
Prerequisite Procedures	NTP-G53 Set Up Timing, page 5-4
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 2-25](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the [“NTP-G103 Back Up the Database” procedure on page 11-2](#).
- 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 5-4](#) 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 Click the **Provisioning > Timing > General** tabs.

Step 7 In the BITS In section, 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
- State
- Framing
- Sync Messaging
- Admin SSM

Step 8 In the BITS In section, you can change the following information:

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

Step 9 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

**Caution**

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

Step 10 Complete the [“NTP-G103 Back Up the Database” procedure on page 11-2](#).

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 3-3
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 2-25. If you are already logged in, continue with Step 2.
- Step 2** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.
- Step 3** Perform any of the following tasks as needed:
- [DLP-G188 Change Security Policy—Single Node, page 9-34](#)
 - [DLP-G189 Change Security Policy—Multiple Nodes, page 9-36](#)
 - [DLP-G190 Change Node Access and PM Clearing Privilege, page 9-37](#)
 - [DLP-G191 Change User Password and Security Level—Single Node, page 9-38](#)
 - [DLP-G192 Change User Password and Security Level—Multiple Nodes, page 9-38](#)
 - [DLP-G193 Delete User—Single Node, page 9-39](#)
 - [DLP-G194 Delete User—Multiple Nodes, page 9-40](#)
 - [DLP-G195 Log Out a User—Single Node, page 9-40](#)
 - [DLP-G196 Log Out a User—Multiple Nodes, page 9-41](#)
- Step 4** Complete the “[NTP-G103 Back Up the Database](#)” procedure on page 11-2.
- Stop. You have completed this procedure.**
-

DLP-G188 Change Security Policy—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 2-25
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 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).
- 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 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 their password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
 - **Warning**—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 45 to 90 days.
- Step 7** Click **Apply**. Confirm that the changes appear; if not, repeat the task.
- Step 8** Return to your originating procedure (NTP).
-

DLP-G189 Change Security Policy—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 2-25
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 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).
- 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 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—Sets the number days the user will be warned to change their 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 45 to 90 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 2-25
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—Sets the access paths to the node:
 - No LAN Access—Allows access to the node only through DCC connections. Access through the TCC2 RJ-45 port and backplane is not permitted.
 - Backplane only—Allows access through DCC connections and the backplane. Access through the TCC2 RJ-45 port is not allowed.
 - Front and Backplane—Allows access through DCC, TCC2 RJ-45, and backplane connections.
 - Restore Timeout—Sets a time delay for the 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.
- Step 4** In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: RETRIEVE, PROVISIONING, MAINTENANCE, or SUPERUSER.
- Step 5** Click **Apply**.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G191 Change User Password and Security Level—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 2-25
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 **Change**.

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

- Change a user password.
- Modify the user security level.
- Lock out the user.

See the “[DLP-G54 Create a New User—Single Node](#)” procedure on page 3-4 for field descriptions.

Step 4 Click **OK**.



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

Step 5 Return to your originating procedure (NTP).

DLP-G192 Change User Password and Security Level—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 2-25
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 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 add 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—Multiple Nodes](#)” task on page 3-4 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. Confirm that the changes appear; if not, repeat the task.
- Step 8** Return to your originating procedure (NTP).

DLP-G193 Delete User—Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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—Single Node](#)” task on page 9-40, 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**. Confirm that the changes appear; if not, repeat the task.
- Step 6** Return to your originating procedure (NTP).

DLP-G194 Delete User—Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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—Multiple Nodes” task on page 9-41](#), 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; if not, repeat the task.
 - Step 7** Return to your originating procedure (NTP).
-

DLP-G195 Log Out a User—Single Node

Purpose	This task logs out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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 parameters provided in the user lockouts 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—Single Node](#)” task on [page 9-34](#) for more information.
- Step 4** Click **OK**.
- Step 5** Click **Yes** to confirm the logout.
- Step 6** Return to your originating procedure (NTP).
-

DLP-G196 Log Out a User—Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-25
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—Multiple Nodes](#)” task on [page 9-36](#) 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** Return to your originating procedure (NTP).
-

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 3-22
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 2-25](#). If you are already logged in, continue with Step 2.
- Step 2** Complete the [“NTP-G103 Back Up the Database” procedure on page 11-2](#).
- Step 3** Perform any of the following tasks as needed:
- [DLP-G197 Modify SNMP Trap Destinations, page 9-42](#)
 - [DLP-G198 Delete SNMP Trap Destinations, page 9-43](#)
- Step 4** Complete the [“NTP-G103 Back Up the Database” procedure on page 11-2](#).
- 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 2-25
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 trap from the **Trap Destinations** area.
- For a description of SNMP traps, refer to the *Cisco ONS 15454 SONET and DWDM Troubleshooting Guide*.
- Step 3** Highlight the Destination row field entry under the Community column and change the entry to another valid community name.

**Note**

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.

**Note**

The default UDP port for SNMP is 162.

- Step 4** 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 5** 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 6** 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 7** Click **Apply**.
- Step 8** 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; if not, repeat the task.
- Step 9** 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 2-25
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 trap you want to delete.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Click **Yes**. Confirm that the changes appear; if not, repeat the task.
- Step 5** Return to your originating procedure (NTP).

