CHAPTER 10

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 (NE) settings and to view a list of those settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 DWDM Reference Manual*.

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 DWDM Troubleshooting Guide* as necessary.

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

1. NTP-G76 Verify Optical Span Loss Using CTC, 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 10-8—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 10-10—Complete this procedure as needed to change node name, contact information, latitude, longitude, date, time, and login legal disclaimer.
5. NTP-G134 Modify OSI Provisioning, page 10-12—Complete this procedure as needed to modify Open System Interconnection (OSI) parameters including the OSI routing mode, Target Identifier Address Resolution Protocol (TARP), routers, subnets, and IP-over-connectionless network service (CLNS) tunnels.
6. NTP-G81 Change CTC Network Access, page 10-21—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 10-29—Complete this procedure as needed to create domains and customize the appearance of the network map, including specifying a different default map, creating domains, consolidating links in the network view, selecting your own map or image, and changing the background color.

8. NTP-G83 Modify or Delete Card Protection Settings, page 10-37—Complete this procedure as needed.
9. NTP-G84 Initiate and Clear Y-Cable and Splitter External Switching Commands, page 10-40—Complete this procedure as needed.
10. NTP-G85 Modify or Delete OSC Terminations, DCC/GCC Terminations, and Provisionable Patchcords, page 10-45—Complete this procedure as needed to modify or delete generic communications channel (GCC) terminations, optical service channel (OSC) terminations, and provisionable patchcords.
11. NTP-G86 Convert a Pass-Through Connection to Add/Drop Connections, page 10-48—Complete this procedure as needed to convert a pass-through connection to an add/drop connection.
12. NTP-G87 Change Node Timing Parameters, page 10-50—Complete this procedure as needed.
13. NTP-G88 Modify Users and Change Security, page 10-51—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 10-64—Complete this procedure as needed.

NTP-G76 Verify Optical Span Loss Using CTC

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

Note Using CTC to verify span loss 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.

Step 1 Complete the “DLP-G46 Log into CTC” task on page 2-26. If you are already logged in, continue with Step 2.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 3 Click the **Maintenance > DWDM > WDM Span Check** tabs.

Step 4 Click **Retrieve Span Loss Values** to retrieve the latest span loss data.

Step 5 View the following information:

- Side—Shows the side to which the span loss values apply, from A through H.
- 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 TransportPlanner and imported to the node when you perform the "NTP-G143 Import the Cisco TransportPlanner NE Update Configuration File" task on page 3-42.

- 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 6 If the measured span loss is not between the minimum and maximum expected span loss, contact your site planner for further instructions.

Stop. **You have completed this procedure**.

NTP-G77 Manage Automatic Power Control

Purpose	This procedure manages APC. It displays APC information at the network-level and node-level APC domain level, and it enables and disables APC domains.
Tools/Equipment	None
Prerequisite Procedures	All procedures in the following chapters: Chapter 3, "Turn Up a Node" Chapter 6, "Turn Up a Network"
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note An APC domain is a set of nodes that are regulated by the same instance of APC at the network level. An APC domain optically identifies a network portion that can be independently regulated. Every domain is terminated by two node sides residing on a terminal node, ROADM node, hub node, line termination meshed node, or an XC termination meshed node. For more information about APC, refer to the "Automatic Power Control" section in the Network Reference chapter in the *ONS 15454 DWDM Reference Manual*.

Step 1 Complete the "DLP-G46 Log into CTC" task on page 2-26 at a node on the network where you want to manage APC. 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 10-5

- DLP-G430 Run Automatic Power Control, page 10-5
- DLP-G159 View Node-Level Automatic Power Control Information, page 10-6
- DLP-G431 View Network-Level Automatic Power Control Information, page 10-7

Stop. **You have completed this procedure**.

DLP-G157 Disable Automatic Power Control

Purpose	This task disables APC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

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

Step 2 Click the **Maintenance > APC** tabs.

Step 3 Click **Refresh**. The *APC Discovery dialog box appears with the discovered APC domains. It may take 10-15 seconds for all the domains to appear. Each discovered domain will be identified as "Discovered: Domain" followed by "node name side, node name side". If APC could not be discovered on a node, a triangle with an exclamation point appears next to the node. If this occurs, double-click the node to display the reason. If you want to save the APC discovery results to a text file, complete the following steps. Otherwise, continue with Step 4.*

a. Click **Save**.

b. In the Save Detailed Error Dialog to File dialog box, enter the path to a local or network server where you want to save the file, or click Browse to navigate to the directory.

c. Click **OK**.

Step 4 Click **Close** to close the APC Discovery dialog box.

Step 5 Choose the domain that you want to disable. *Only domains with a status, APC State: Enabled, can be disabled.*

Step 6 Click **Disable APC**.

Step 7 In the APC window, verify that the Check APC State status changes to Disable.

Step 8 Return to your originating procedure (NTP).

DLP-G158 Enable Automatic Power Control

Purpose	This task enables the DWDM APC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Click the **Maintenance > APC** tabs.

Step 3 Click **Refresh**. The APC Discovery dialog box appears with the discovered APC domains. It may take 10-15 seconds for all the domains to appear. Each discovered domain will be identified as “Discovered: Domain” followed by “node name side, node name side”. If APC could not be discovered on a node, a triangle with an exclamation point appears next to the node. If this occurs, double-click the node to display the reason. If you want to save the APC discovery results to a text file, complete the following steps. Otherwise, continue with Step 4.

a. Click **Save**.

b. In the Save Detailed Error Dialog to File dialog box, enter the path to a local or network server where you want to save the file, or click Browse to navigate to the directory.

c. Click **OK**.

Step 4 Click **Close** to close the APC Discovery dialog box.

Step 5 Choose the domain that you want to enable. (Only domains with a status, APC State: Disabled can be enabled.)

Step 6 Click **Enable APC**.

Step 7 In the APC window, verify that the Check APC State status changes to Enable.

Step 8 Return to your originating procedure (NTP).

DLP-G430 Run Automatic Power Control

Purpose	This task runs the DWDM APC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Click the **Maintenance > APC** tabs.

Step 3 Click **Refresh**. The APC Discovery dialog box appears with the discovered APC domains. It might take 10 to 15 seconds for all the domains to appear. Each discovered domain will be identified as "Discovered: Domain" followed by <node name side>, <node name side>. If APC could not be discovered on a node, a triangle with an exclamation point appears next to the node. If this occurs, double-click the node to display the reason. If you want to save the APC discovery results to a text file, complete the following steps. Otherwise, continue with Step 4.

a. Click **Save**.

b. In the Save Detailed Error Dialog to File dialog box, enter the path to a local or network server where you want to save the file, or click Browse to navigate to the directory.

c. Click **OK**.

Step 4 Click **Close** to close the APC Discovery dialog box.

Step 5 Choose the domain that you want to run. Only domains with the status, APC State: Enabled can be run.

Step 6 Click **Run APC**.

Step 7 Return to your originating procedure (NTP).

DLP-G159 View Node-Level Automatic Power Control Information

Purpose	This task displays the node-level APC information.
Tools/Equipment	A node provisioning plan prepared by Cisco TransportPlanner is required.
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 In the Side field, choose the side where you want to view the APC information. Options include A, B, C, D, E, F, G, and H (D through H do not appear if the sides are not provisioned). Choose **All** to choose all sides.

Step 3 Click **Refresh.**

Step 4 View the APC information:

- Position—The node, side, and slot.
- Last Modification—The last time a modification to the APC parameters occurred, in Date-Hour-Time Zone format. APC parameters are reported only when their ports are in IS-NR/Unlocked-enabled service state.
- Parameter—The parameter that was last modified. Parameters can include
  - Gain and optical power setpoints on the LINE-TX ports of the OPT-BST, OPT-BST-L, OPT-BST-E, OPT-AMP-L, OPT-AMP-17-C, and OPT-AMP-C cards.
  - Gain and optical power setpoints on the COM_TX port of the OPT-PRE card.
  - VOA target attenuation on the COM-RX ports of 32DMX, 32DMX-O, 32DMX-L, and 40-DMX-C/40-DMX-CE cards.

  - VOA target attenuation on the EXP-TX and DROP-TX ports of the AD-1B-x.xx, AD-4B-x.xx, AD-1C-x.xx, AD-2C-x.xx, and AD-4C-x.xx cards.
- Last Check—The date and time the APC parameters were last monitored, in Date-Hour-Time Zone format. APC parameters are reported only when their ports are in IS-NR/Unlocked-enabled service state.
- Side—The letter of the side, A through H.
- APC State—Displays the APC state:
  - Enabled—APC is enabled
  - Disabled - User —APC was disabled by a user action.
  - Disabled Internal—APC was disabled by an internal action.
  - Not Applicable—APC parameters are not reported, for example, does not apply to the side, for example, no amplifiers are installed.

Step 5 Return to your originating procedure (NTP).

DLP-G431 View Network-Level Automatic Power Control Information

Purpose	This task displays the network-level APC information.
Tools/Equipment	A node provisioning plan prepared by Cisco TransportPlanner is required.
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Click the **Maintenance > APC** tabs.

Step 3 Click **Refresh**. The APC Discovery dialog box appears with the discovered APC domains. It may take 10-15 seconds for all the domains to appear. Each discovered domain will be identified as “Discovered: Domain” followed by “node name side, node name side”. If APC could not be discovered on a node, a triangle with an exclamation point appears next to the node. If this occurs, double-click the node to display the reason. If you want to save the APC discovery results to a text file, complete the following steps. Otherwise, continue with Step 4.

a. Click **Save**.

b. In the Save Detailed Error Dialog to File dialog box, enter the path to a local or network server where you want to save the file, or click Browse to navigate to the directory.

c. Click **OK**.

Step 4 Click **Close** to close the APC Discovery dialog box.

Step 5 Double-click the domain for which you want to view APC information.

Step 6 Right-click the APC span under the domain and choose the node and span.

Step 7 View the APC information:

- Position—Shows the shelf (multishelf nodes only) slot and port.

- Last Modification—Shows the last time a modification to the APC parameters occurred, in Date-Hour-Time Zone format. APC parameters are reported only when their ports are in IS-NR/Unlocked-enabled service state.
- Parameter—Shows the parameter that was last modified. Parameters can include
  - Gain and optical power setpoints on the LINE-TX ports of the OPT-BST, OPT-BST-L, OPT-BST-E, OPT-AMP-L, OPT-AMP-17-C, and OPT-AMP-C cards.
  - Gain and optical power setpoints on the COM_TX port of the OPT-PRE card.
  - VOA target attenuation on the COM-RX ports of 32DMX, 32DMX-O, 32DMX-L, and 40-DMX-C/40-DMX-CE cards.
  - VOA target attenuation on the EXP-TX and DROP-TX ports of the AD-1B-x.xx, AD-4B-x.xx, AD-1C-x.xx, AD-2C-x.xx, and AD-4C-x.xx cards.
- Last Check—Shows the date and time the APC parameters were last monitored, in Date-Hour-Time Zone format. APC parameters are reported only when their ports are in IS-NR/Unlocked-enabled service state.
- Side—Shows the letter of the side, A through H.
- APC State—Displays the APC state:
  - Enabled—APC is enabled
  - Disabled - User—APC was disabled by a user action.
  - Disabled - Internal—APC was disabled by an internal action.
  - Not Applicable—APC parameters are not normally reported, for example, a gain setpoint when working mode is set to Control Power.

Step 8 Return to your originating procedure (NTP).

NTP-G78 View ROADM Node Power Equalization

Purpose	This procedure allows you to view ROADM node power equalization levels.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note This procedure only applies to ROADM nodes or to terminal ROADM nodes (that is, terminal nodes with 32WSS, 32WSS-L, or 40-WSS-C/40-WSS-CE cards installed).

Step 1 Complete the "DLP-G46 Log into CTC" task on page 2-26. If you are already logged in, continue with Step 2.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Maintenance > DWDM > ROADM Power Monitoring > Optical Side** *n-n* tabs, where *n-n* = A-B, C-D, E-F, or G-H.

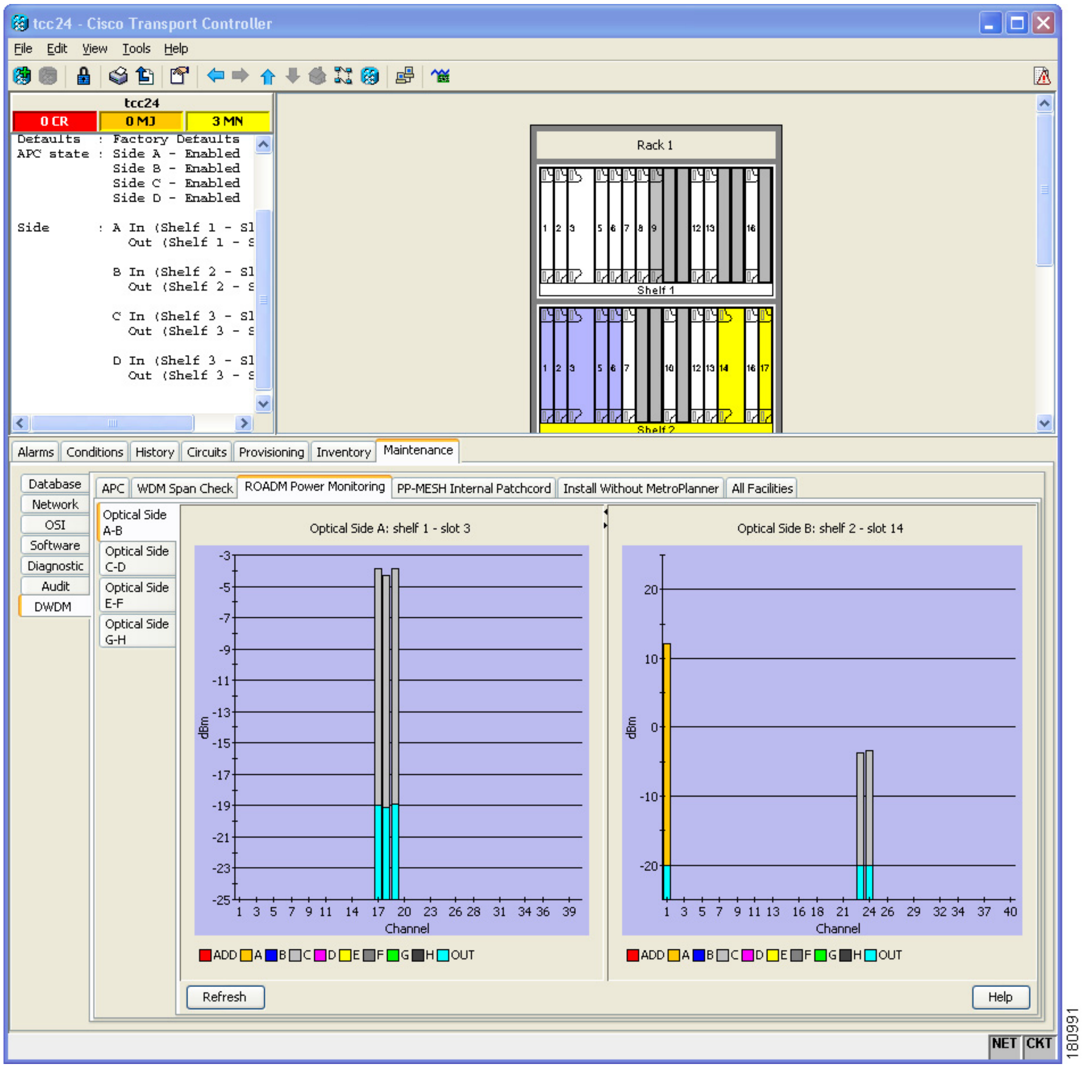
Step 3 On the Power Monitoring tab, view the power information:

- ADD—Add power. This power level is represented by the red bar.
- PT—Pass-through power. This power level is represented by the yellow bar.
- OUT—Output power. This power level is represented by the blue bar. It shows the per-channel (wavelength) power at the 32WSS, 32WSS-L, 40-WSS-C, 40-WSS-CE, or 40-WXC-C output (COM_TX) port.

Note The 32WSS, 32WSS-L, 40-WSS-C, 40-WSS-CE, and 40-WXC-C cards are 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



tcc24 - Cisco Transport Controller

tcc24
0 CR | 0 MJ | 3 MN

```
Defaults    : Factory Defaults
APC state : Side A - Enabled
            Side B - Enabled
            Side C - Enabled
            Side D - Enabled

Side        : A In (Shelf 1 - Sl
                Out (Shelf 1 - S

              B In (Shelf 2 - Sl
                Out (Shelf 2 - S

              C In (Shelf 3 - Sl
                Out (Shelf 3 - S

              D In (Shelf 3 - Sl
                Out (Shelf 3 - S
```

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 3-10
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 2-26. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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

Step 4 Complete the "DLP-G160 Change the Node Name, Date, Time, and Contact Information" task on page 10-10, as needed.

Step 5 Complete the "DLP-G161 Change the Login Legal Disclaimer" task on page 10-11, as needed.

Step 6 After confirming the changes, complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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 2-26
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 (single-shelf mode) or multishelf view (multishelf mode), 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: NTP/SNTP Server IP Address (if Use NTP/SNTP Server is checked)
- 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 3-10 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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
<b>	Begins boldface font
</b>	Ends boldface font
<center>	Aligns type in the center of the window
</center>	Ends the center alignment
<font=*n*> (where *n* = font point size)	Changes the font to the new size
</font>	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-G134 Modify OSI Provisioning

Purpose	This procedure modifies the ONS 15454 OSI parameters including the OSI routing mode, TARP, routers, subnets, and IP-over-CLNS tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-G132 Provision OSI, page 3-30
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional information about the ONS 15454 implementation of OSI is provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 DWDM Reference Manual*.

Step 1 Complete the "DLP-G46 Log into CTC" task on page 2-26. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

Step 3 Perform any of the following tasks as needed:

- DLP-G284 Modify the TARP Operating Parameters, page 10-13
- DLP-G285 Add a Static TID-to-NSAP Entry to the TARP Data Cache, page 3-34
- DLP-G286 Remove a Static TID to NSAP Entry from the TARP Data Cache, page 10-15
- DLP-G287 Add a TARP Manual Adjacency Table Entry, page 10-16
- DLP-G292 Remove a TARP Manual Adjacency Table Entry, page 10-16
- DLP-G293 Change the OSI Routing Mode, page 10-17
- DLP-G294 Edit the OSI Router Configuration, page 10-18
- DLP-G295 Edit the OSI Subnetwork Point of Attachment, page 10-19
- DLP-G296 Edit an IP-Over-CLNS Tunnel, page 10-20
- DLP-G297 Delete an IP-Over-CLNS Tunnel, page 10-21

Step 4 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

Stop. You have completed this procedure.

DLP-G284 Modify the TARP Operating Parameters

Purpose	This task modifies the TARP operating parameters including TARP protocol data unit (PDU) propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Provision the following parameters, as needed:

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

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

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

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

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

Note TARP Echo and NSAP to TID are not supported.

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

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

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

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

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

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

- LAN TARP Storm Suppression—If checked (default), enables TARP storm suppression. This function prevents redundant TARP PDUs from being unnecessarily propagated across the LAN network.
- Send Type 4 PDU on Startup—If checked, a TARP Type 4 PDU is originated during the initial ONS 15454 startup. Type 4 PDUs indicate that a TID or NSAP change has occurred at the NE. (The default setting is not enabled.)

- Type 4 PDU Delay—Sets the amount of time that will pass before the Type 4 PDU is generated when Send Type 4 PDU on Startup is enabled. 60 seconds is the default. The range is 0 to 255 seconds.

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

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

Note The T1, T2, and T4 timers are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-G286 Remove a Static TID to NSAP Entry from the TARP Data Cache

Purpose	This task removes a static TID to NSAP entry from the TDC.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the static entry that you want to delete.

Step 3 Click **Delete Static Entry**.

Step 4 In the Delete TDC Entry dialog box, click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-G287 Add a TARP Manual Adjacency Table Entry

Purpose	This task adds an entry to the TARP manual adjacency table (MAT). Entries are added to the MAT when the ONS 15454 must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click **Add**.

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

- Level—Sets the TARP Type Code that will be sent:
  - **Level 1**—Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
  - **Level 2**—Indicates that the adjacency is in a different area from the current node. The entry generates Type 2 PDUs.
- NSAP—Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.

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

Step 5 Return to your originating procedure (NTP).

DLP-G292 Remove a TARP Manual Adjacency Table Entry

Purpose	This task removes an entry from the TARP MAT.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution If TARP manual adjacency is the only means of communication to a group of nodes, loss of visibility will occur when the adjacency table entry is removed.

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

Step 2 Click the MAT entry that you want to delete.

Step 3 Click **Remove**.

Step 4 In the Delete TDC Entry dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G293 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Do not complete this procedure until you confirm the role of the node within the network. It will be either an ES, IS Level 1, or IS Level 1/Level 2. This decision must be carefully considered. For additional information about OSI provisioning, refer to the “Management Network Connectivity” chapter of the *Cisco ONS 15454 DWDM Reference Manual*.

Caution Link state PDU (LSP) buffers must be the same at all NEs within the network, or loss of visibility could occur. Do not modify the LSP buffers unless you are sure that all NEs within the OSI have the same buffer size.

Caution LSP buffer sizes cannot be greater than the LAP-D MTU size within the OSI area.

Step 1 Verify the following:

- All L1/L2 virtual routers on the NE must reside in the same area. This means that all neighboring virtual routers must have at least one common area address.
- For OSI L1/L2 to ES routing mode changes, only one L1/L2 virtual router and no more than one subnet can be configured.
- For OSI L1 to ES routing mode changes, only one L1 virtual router and no more than one subnet can be configured.

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

Step 3 Choose one of the following node routing modes:

- **End System**—The ONS 15454 performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.
- **Intermediate System Level 1**—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It does not communicate with IS nodes that reside in other OSI areas except through an IS L1/L2 node residing in its own area.
- **Intermediate System Level 1/Level 2**—The ONS 15454 performs IS functions. It communicates with IS and ES nodes that reside within its OSI area. It also communicates with IS L1/L2 nodes that reside in other OSI areas. Before choosing this option, verify the following:
  - The node is connected to another IS Level 1/Level 2 node that resides in a different OSI area.
  - The node is connected to all nodes within its area that are provisioned as IS L1/L2.

Note Changing a routing mode should be carefully considered. Additional information about OSI ESs and ISs and the ES-IS and IS-IS protocols are provided in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 DWDM Reference Manual*.

Step 4 Although Cisco does not recommend changing the LSP buffer sizes, you can adjust the buffers in the following fields:

- L1 LSP Buffer Size—Adjusts the Level 1 link state PDU buffer size.
- L2 LSP Buffer Size—Adjusts the Level 2 link state PDU buffer size.

Step 5 Return to your originating procedure (NTP).

DLP-G294 Edit the OSI Router Configuration

Purpose	This task allows you to edit the OSI router configuration, including enabling and disabling OSI routers, editing the primary area address, and creating or editing additional area addresses.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Choose the router you want provision and click **Edit**.

Step 3 In the OSI Router Editor dialog box:

a. Check or uncheck the Enabled box to enable or disable the router.

Note Router 1 must be enabled before you can enable Routers 2 and 3.

b. For enabled routers, edit the primary area address, if needed. The address can be between 8 and 24 alphanumeric characters in length.

c. If you want to add or edit an area address to the primary area, enter the address at the bottom of the Multiple Area Addresses area. The area address can be 2 to 26 numeric characters (0–9) in length. Click **Add**.

d. Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-G295 Edit the OSI Subnetwork Point of Attachment

Purpose	This task allows you to view and edit the OSI subnetwork point of attachment parameters. The parameters are initially provisioned when you create a section data communications channel (SDCC) (ANSI) or regeneration section (RS-DCC) (ETSI), Line data communications channel (LDCC) (ANSI) or multiplex section (MS-DCC) (ETSI), generic communications channel (GCC), or optical service channel (OSC), or when you enable the LAN subnet.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 If the subnet router is not enabled, complete "DLP-G294 Edit the OSI Router Configuration" task on page 10-18 to enable it. If it is enabled, continue with Step 2.

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

Step 3 Choose the subnet you want to edit, then click **Edit**.

Step 4 In the Edit <subnet type> Subnet <slot/port> dialog box, edit the following fields:

- ESH—The End System Hello (ESH) PDU propagation frequency. An end system NE transmits ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- ISH—The Intermediate System Hello (ISH) PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the NEs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—The Intermediate System to Intermediate System Hello (IIH) PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.

Note The IS-IS Cost and DIS Priority parameters are provisioned when you create or enable a subnet. You cannot change the parameters after the subnet is created. To change the DIS Priority and IS-IS Cost parameters, delete the subnet and create a new one.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-G296 Edit an IP-Over-CLNS Tunnel

Purpose	This task allows you to edit the parameters of an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-G291 Create an IP-Over-CLNS Tunnel, page 3-39 DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Changing the IP or NSAP addresses or an IP-over-CLNS tunnel can cause loss of NE visibility or NE isolation. Do not change network addresses until you verify the changes with your network administrator.

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

Step 2 Click **Edit**.

Step 3 In the Edit IP Over OSI Tunnel dialog box, complete the following fields:

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

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

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

- IP Address—Enter the IP address of the IP-over-CLNS tunnel destination.
- IP Mask—Enter the IP address subnet mask of the IP-over-CLNS destination.

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

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-G297 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

⚠ **Caution** Deleting an IP-over-CLNS tunnel might cause the nodes to lose visibility or cause node isolation. If node isolation occurs, onsite provisioning might be required to regain connectivity. Always confirm tunnel deletions with your network administrator.

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

Step 2 Choose the IP-over-CLNS tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK**.

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, OSPF options, proxy tunnels, and firewall tunnels.
Tools/Equipment	None
Prerequisite Procedures	NTP-G26 Set Up CTC Network Access, page 3-13
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Additional ONS 15454 networking information, including IP addressing examples, dual IP addressing (secure mode) information, static route scenarios, OSPF protocol information, and Routing Information Protocol (RIP) options are provided in the "Management Network Connectivity" chapter in the *Cisco ONS 15454 DWDM Reference Manual*.

Step 1 Complete the "DLP-G46 Log into CTC" task on page 2-26. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

Step 3 Perform any of the following tasks as needed:

- DLP-G162 Change IP Settings, page 10-22
- DLP-G265 Lock Node Security, page 10-24
- DLP-G266 Modify Backplane Port IP Settings in Security Mode, page 10-24
- DLP-G267 Disable Secure Mode, page 10-25
- DLP-G163 Modify a Static Route, page 10-27
- DLP-G164 Delete a Static Route, page 10-27
- DLP-G165 Disable OSPF, page 10-28
- DLP-G59 Set Up or Change Open Shortest Path First Protocol, page 3-23
- DLP-G167 Delete a Firewall Tunnel, page 10-28

Step 4 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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 2-26 DLP-G56 Provision IP Settings, page 3-14
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Changing the node IP address, subnet mask, or IIOP listener port causes the TCC2/TCC2P cards 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.

Note If the node contains TCC2P cards and is in default (repeater) mode, the node IP address refers to the TCC2P front-access TCP/IP (LAN) port as well as the backplane LAN port. If the node is in secure mode, this task only changes the front-access port IP address only. If the node is in secure mode and has been locked, the IP address cannot be changed unless the lock is removed by Cisco Technical Support.

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

Step 2 Change any of the following, as required:

- IP Address
- Net/Subnet Mask Length
- Default Router
- LCD Setting
- Suppress CTC IP Display
- Forward DHCP Request To

Gateway Settings

- Enable SOCKS proxy on Port. If enabled, one of the following:
  - External Network Element
  - Gateway Network Element
  - SOCK Proxy only

See the "DLP-G56 Provision IP Settings" task on page 3-14 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, or subnet mask, 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, both ONS 15454 TCC2/TCC2P cards 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 tabs. If not, refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

Step 6 Return to your originating procedure (NTP).

DLP-G265 Lock Node Security

Purpose	This task locks the ONS 15454 secure mode. When secure 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 2-26 DLP-G264 Enable Secure Mode, page 3-20
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution When a node is locked, it cannot be unlocked by any user or action. It can only be changed by Cisco Technical Support. Even if the node's database is deleted and another unlocked database is loaded, the node will remain locked. Do not proceed unless you want the node to permanently retain the current secure configuration including dual IP addresses.

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

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 in Security Mode

Purpose	This task modifies the ONS 15454 backplane IP address, subnet mask, and default router when security mode is enabled. It also modifies settings that control backplane IP address visibility in CTC and the ONS 15454 LCD.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-G103 Back Up the Database, page 13-2 DLP-G46 Log into CTC, page 2-26 DLP-G264 Enable Secure Mode, page 3-20
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Caution This task cannot be performed on a secure mode NE that has been locked.

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

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 or multishelf 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 Secure Mode

Purpose	This task disables the ONS 15454 secure 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 2-26 DLP-G264 Enable Secure Mode, page 3-20
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Note If you change an NE from secure mode to the default (repeater) mode, the backplane IP address becomes the node IP address.

Note This task cannot be performed if the NE's secure mode configuration is locked. If secure mode is locked, you must contact Cisco Technical Support to change the node configuration.

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

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, SOCKS proxy will be disabled by default, and the CTC computer is only visible to the ONS 15454 where the CTC computer is connected. The computer is not visible to the secure mode data communications channel (DCC)-connected nodes. 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 and SOCKS proxy remains enabled. However, 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 within the firewall 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 TCC2P cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node changes to gray and a DISCONNECTED condition appears.

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 2-26 DLP-G58 Create a Static Route, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

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 3-22 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 2-26 DLP-G58 Create a Static Route, page 3-22
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 2-26 DLP-G59 Set Up or Change Open Shortest Path First Protocol, page 3-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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-G167 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-G46 Log into CTC" task on page 2-26. 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 10-29
- DLP-G169 Change the Default Network View Background Map, page 10-30
- DLP-G170 Apply a Custom Network View Background Map, page 10-31
- DLP-G171 Create Domain Icons, page 10-31
- DLP-G172 Manage Domain Icons, page 10-32
- DLP-G173 Enable Dialog Box Do-Not-Display Option, page 10-33
- DLP-G174 Switch Between TDM and DWDM Network Views, page 10-34
- DLP-G330 Consolidate Links in Network View, page 10-34

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 2-26
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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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 network view, double-click any node on the map.

Step 5 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning > Defaults** tabs. Wait for the Defaults selector frame to load the defaults. This could take a few minutes.

Step 6 In the Defaults Selector area, choose **CTC** and then **network**. (You might 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, 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 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 2-26
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. By default, domains are visible to all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means any user can maintain the domain information in his or her

Preferences file, meaning domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only superusers can create a domain or put a node into a domain.) See the "NTP-G135 Edit Network Element Defaults" procedure on page 13-42 to change NE default values.

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. By default, domains are visible to all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26 DLP-G171 Create Domain Icons, page 10-31
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means any user can maintain the domain information in his or her Preferences file, meaning domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only superusers can create a domain or put a node into a domain.) See the "NTP-G135 Edit Network Element Defaults" procedure on page 13-42 to change NE default values.

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.

Table 10-2 Managing Domains (continued)

Domain Action	Steps
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	Complete one of the following: • Double-click the domain icon. • 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 disables the do-not-display option.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
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 2-26
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 (TXP) and muxponder (MSP) cards.
- **DWDM**—Displays only ONS 15454s with DWDM cards, including the TXP and MXP cards.

Step 3 Return to your originating procedure (NTP).

DLP-G330 Consolidate Links in Network View

Purpose	This task consolidates DCC, GCC, optical transport service (OTS) and provisionable patchcord (PPC) links in CTC network view.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note Global consolidation persists when CTC is re-launched but local consolidation does not persist.

Step 1 From the View menu, choose **Go to Network View**. CTC shows the link icons by default.

Step 2 Perform the following steps as needed:

- To toggle between the links, go to Step 3.
- To consolidate all the links on the network map, go to Step 4.

- To consolidate a link or links between two nodes, go to Step 5.
- To view information about a consolidated link, go to Step 6.
- To access an individual link within a consolidated link, go to Step 7.
- To expand consolidated links, go to Step 8.
- To filter the links by class, go to Step 9.

Step 3 Right-click on the network map and choose **Show Link Icons** to toggle the link icons on and off.

Step 4 To consolidate all the links on the network map (global consolidation):

a. Right-click anywhere on the network map.

b. Choose **Collapse/Expand Links** from the shortcut menu. The Collapse/Expand Links dialog window appears.

c. Select the check boxes for the link classes you want to consolidate.

d. Click **OK**. The selected link classes are consolidated throughout the network map.

Step 5 To consolidate a link or links between two nodes (local consolidation):

a. Right-click the link on the network map.

b. Choose **Collapse Link** from the shortcut menu. The selected link type consolidates to show only one link.

Note The links consolidate by class. For example, if you select a DCC link for consolidation only the DCC links will consolidate, leaving any other link classes expanded.

Figure 10-2 shows the network view with unconsolidated DCC and PPC links.

Figure 10-2 Unconsolidated Links in the Network View

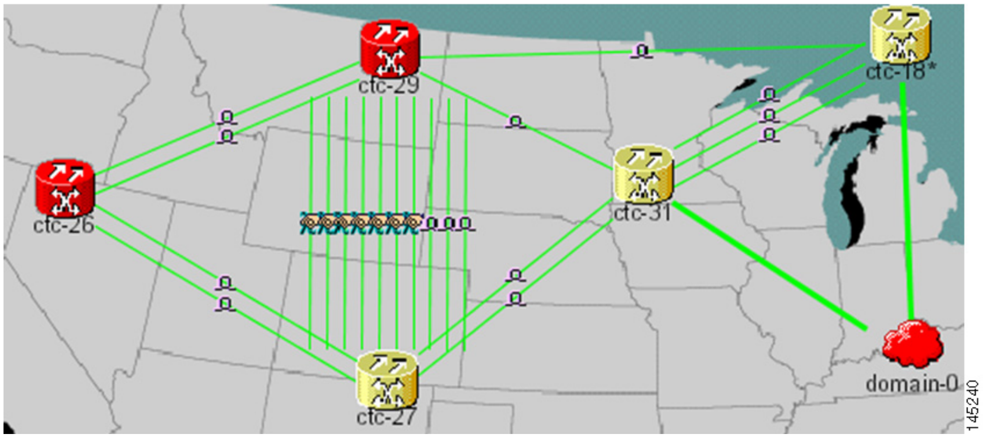


Figure 10-3 shows a network view with globally consolidated links.

Figure 10-3 Consolidated Links in the Network View

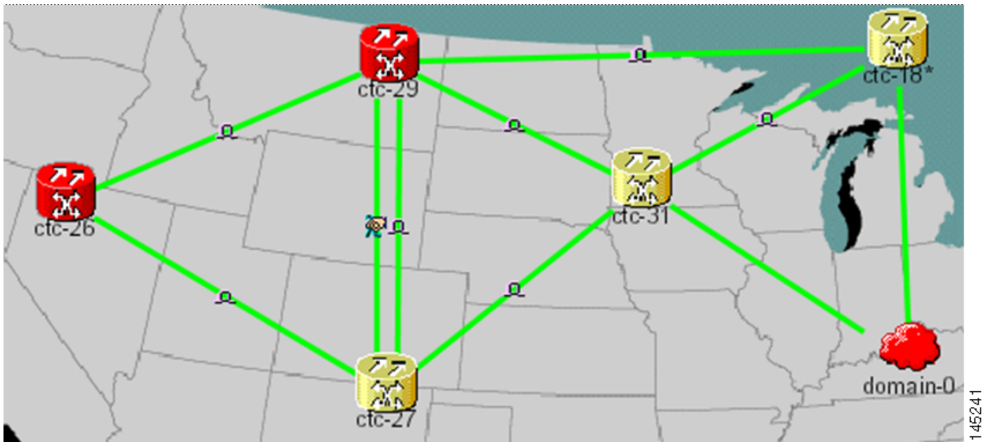
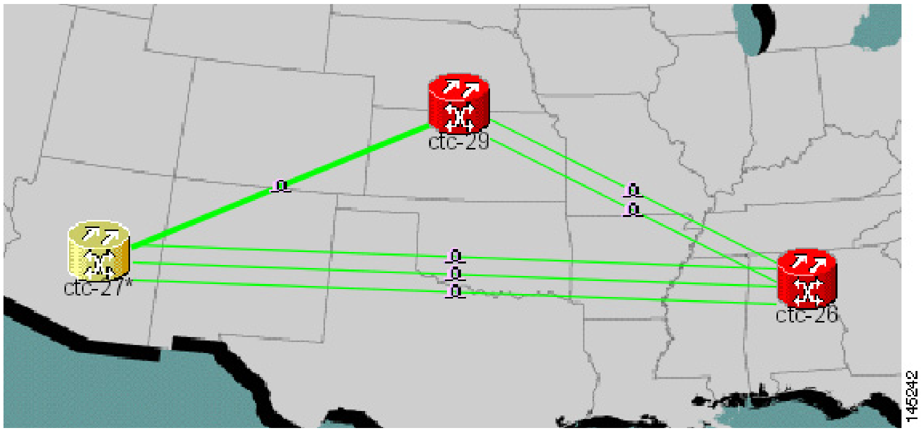


Figure 10-4 shows a network view with local DCC link consolidation between two nodes.

Figure 10-4 Network View with Local Link Consolidation



Step 6 To view information about a consolidated link, either move your mouse over the link (the tooltip displays the number of links and the link class) or single-click the link to display detailed information on the left side of the window.

Step 7 To access an individual link within a consolidated link (for example, if you need to perform a span upgrades):

a. Right-click the consolidated link. A shortcut menu appears with a list of the individual links.

b. Hover the mouse over the selected link. A cascading menu appears where you can select an action for the individual link or navigate to one of the nodes where the link is attached.

Step 8 To expand locally consolidated links, right-click the consolidated link and choose **Expand** [*link class*] **Links** from the shortcut menu, where “link class” is DCC, PPC, etc.

Step 9 To filter the links by class:

a. Click the **Link Filter** button in the upper right area of the window. The Link Filter dialog appears.

The link classes that appear in the Link Filter dialog are determined by the Network Scope you choose in the network view (Table 10-3).

Table 10-3 Link Classes By Network Scope

Network Scope	Displayed Link Classes
ALL	DCC, GCC, OTS, PPC, Server Trail
DWDM	GCC, OTS, PPC
TDM	DCC, PPC

b. Check the check boxes next to the links you want to display.

c. Click **OK**.

Step 10 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 5-16
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 2-26. 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 10-38
- DLP-G176 Modify a Splitter Protection Group, page 10-38
- DLP-G177 Delete a Y-Cable Protection Group, page 10-39

Step 3 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

Stop. You have completed this procedure.

DLP-G175 Modify a Y-Cable Protection Group

Purpose	This task modifies a Y-cable protection group that has been created for two TXP, MXP, GE_XP or 10GE_XP card client ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-G33 Create a Y-Cable Protection Group, page 5-16 DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the Near End Transponder Card to open it in the card view.

Step 2 In the card view mode, click the **Provisioning** tab. The Line tab view with the ports provisioned is displayed.

Step 3 Click the **Admin State** list box and select the **Out-of-Service (OOS)** option for the Near End Transponder Trunk and Client Ports (example:1-1(OC3), 2(OC48)).

Step 4 Click **Apply**. Repeat steps 1-4 for the Far End Transponder Card.

Step 5 Right-click the **Tranponder card** in card view mode and select **Go to Parent View**.

Step 6 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning->Protection** tabs.

Step 7 In the Protection Groups area, disconnect the Y-Cable fiber for the Protection Transponder ports in the protection group you want to delete.

Step 8 Select the protection group and click **Delete**.

Step 9 Click **Yes** in the Delete Protection Group dialog box. Confirm that the changes appear.

Step 10 Return to your originating procedure (NTP).

Note When you delete the protection group, traffic drops because both the Transponder TX ports will be in a Service state (Protect TX port gets turned on). The Transponder TX ports are connected through a Y-cable and as a result two signals will be passing through the same fiber. Hence, you should put the protect port OOS and remove the fibering for the protect port and then delete the protection group.

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-G179 Install the TXP, MXP, GE_XP, 10GE_XP, and ADM-10G Cards, page 3-58 NTP-G33 Create a Y-Cable Protection Group, page 5-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Superuser only

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 2-26. 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 10-41.

Step 3 To perform a Force protection switch, complete the "DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch" task on page 10-41.

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 10-42.

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 10-43.

Step 6 To prevent traffic from switching to the protect card, complete the "DLP-G182 Apply a Lockout" task on page 10-43.

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 10-44.

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 2-26
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 (single-shelf mode) or shelf view (multishelf mode), 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 drop-down list, 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 10-42.

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 2-26
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 (single-shelf mode) or shelf view (multishelf mode), 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 10-42.

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 2-26 One of the following tasks: • DLP-G178 Apply a Manual Y-Cable or Splitter Protection Switch, page 10-41 • DLP-G179 Apply a Force Y-Cable or Splitter Protection Switch, page 10-41
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 2-26
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 On button is not available.

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 10-44.

Note Provisioning a lock-on raises a LOCKON-REQ or an FE-LOCKON condition in CTC. Clearing the lock-on 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 2-26
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 (single-shelf mode) or shelf view (multishelf mode), 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 10-44.

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 2-26 One of the following tasks: • DLP-G181 Apply a Lock-On, page 10-43 • DLP-G182 Apply a Lockout, page 10-43
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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, DCC/GCC Terminations, and Provisionable Patchcords

Purpose	This procedure modifies DCC/GCC terminations, and deletes provisionable patchcords, OSC terminations, and DCC/GCC terminations.
Tools/Equipment	None
Prerequisite Procedures	One or more of the following tasks: • DLP-G76 Provision DCC/GCC Terminations, page 7-58 • NTP-G38 Provision OSC Terminations, page 3-104 • NTP-G184 Create a Provisionable Patchcord, page 7-50
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 2-26. If you are already logged in, continue with Step 2.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), complete the following tasks as needed:

- DLP-G184 Change a DCC/GCC Termination, page 10-46.
- DLP-G185 Delete a DCC/GCC Termination, page 10-46.
- DLP-G186 Delete an OSC Termination, page 10-47.
- DLP-G187 Delete a Provisionable Patchcord, page 10-48.

Stop. You have completed this procedure.

DLP-G184 Change a DCC/GCC Termination

Purpose	This task modifies a DCC/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 2-26
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

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

Step 2 Select the DCC or GCC tabs as necessary. Available tabs are:

- GCC (both ANSI and ETSI)
- DCC
  - SDCC and LDCC (for ANSI)
  - RS-DCC and MS-DCC (for ETSI)

Step 3 Select the DCC/GCC that you want to change.

Step 4 Click **Edit**. The Edit Termination dialog box appears.

Step 5 Complete the following as necessary:

- GCC Rate—(Display only) Indicates the communication channel rate.
- Disable OSPF on Link—If checked, OSPF 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 DCC/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 6 Click **OK**.

Step 7 Return to your origination procedure (NTP).

DLP-G185 Delete a DCC/GCC Termination

Purpose	This task deletes the DWDM DCC/GCC terminations required for network setup when using TXP, MXP, or ADM-10G cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

Step 2 Select the DCC or GCC tabs as necessary. Available tabs are:

- GCC (both ANSI and ETSI)
- DCC
  - SDCC and LDCC (for ANSI)
  - RS-DCC and MS-DCC (for ETSI)

Step 3 Select the DCC/GCC that you want to delete.

Step 4 Click **Delete**.

Step 5 In the Delete Terminations dialog box, check the **Set port OOS** check box if you want to place ports out of service.

Step 6 Click **Yes**. The following alarms will appear until all network terminations are deleted and the ports are out of service:

- GCC-EOC for GCC termination
- EOC for SDCC termination
- EOC-L for LDCC termination

Step 7 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 2-26
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 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning > Comm Channel > OSC** tabs.

Step 2 Click the OSC termination that you want to delete and click **Delete**.

Step 3 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 might appear on the OPT-BST amplifier, OSCM card, and OSC-CSM card.

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 2-26 NTP-G184 Create a Provisionable Patchcord, page 7-50
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 Add/Drop Connections

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 AD-xC-xx.x, 4MD-xx.x, 32MUX-O, 32DMX-O, 32DMX, 32DMX-L, 40-MUX-C, and 40-DMX-C/40-DMX-CE 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	None
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 2-26 at an ONS 15454 on the network.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 > Internal Patchcords** 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, 32DMX, or 32DMX-L output port to the 32MUX-O input port. Alternatively, connect the 40-DMX-C/40-DMX-CE output port to the 40-MUX-C 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 (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning > WDM-ANS > Internal Patchcords** tabs.

b. Highlight the pass-through connections between ITU-T channel add and drop port filters.

c. Click **Delete**.

Step 6 Create two new unidirectional OCHNCs (one heading Side B, the other heading Side A) to support the new add/drop channels. See the "DLP-G105 Provision Optical Channel Network Connections" task on page 7-21.

Step 7 As necessary, complete the "NTP-G184 Create a Provisionable Patchcord" procedure on page 7-50.

Step 8 As necessary, add an optical attenuator between the channel TX port of the AD-xC-xx.x, 4MD-xx.x, 32DMX-O, 32DMX, 32-DMX-L, or 40-DMX-C/40-DMX-CE card and the DWDM RX port on the TXP, MXP, or OC-N/STM-N ITU-T 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 variable optical attenuator (VOA).

Step 9 (Optional) The following verification steps might be needed for an intermediate node when a pass-through connection is converted:

a. Verify that the received channels are at the specified power level. See the "NTP-G76 Verify Optical Span Loss Using CTC" procedure on page 10-2 for instructions.

b. Verify that the added channels are equalized with the express channels within +/–1 dB.

c. If the channels are not equalized with the express channels within +/–1 dB, check the attenuation of the VOAs.

d. Check all the fiber adapters to minimize their insertion losses. See the "NTP-G115 Clean Fiber Connectors" procedure on page 13-26 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 13-18.
Tools/Equipment	None
Prerequisite Procedures	NTP-G53 Set Up Timing, page 6-4
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 2-26. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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 6-4 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 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Provisioning > Timing > BITS** Facilities 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 Out section, you can change the following information:

- Coding
- Framing
- AIS Threshold
- LBO

Step 9 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 10 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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 3-7
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 Complete the "DLP-G46 Log into CTC" task on page 2-26. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

Step 3 Perform any of the following tasks as needed:

- DLP-G188 Change Security Policy for a Single Node, page 10-52
- DLP-G189 Change Security Policy for Multiple Nodes, page 10-53
- DLP-G317 Change Node Access and PM Clearing Privilege, page 10-55
- DLP-G328 Grant Superuser Privileges to a Provisioning User, page 10-56
- DLP-G191 Change User Password and Security Level on a Single Node, page 10-57
- DLP-G192 Change User Password and Security Level for Multiple Nodes, page 10-58
- DLP-G193 Delete a User From a Single Node, page 10-59
- DLP-G194 Delete a User From Multiple Nodes, page 10-59
- DLP-G195 Log Out a User on a Single Node, page 10-60
- DLP-G196 Log Out a User on Multiple Nodes, page 10-61
- DLP-G281 Configure the Node for RADIUS Authentication, page 10-61
- DLP-G282 View and Terminate Active Logins, page 10-64

Step 4 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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.
- New Password must Differ from the Old Password—Choose the number of characters that must differ between the old and new password. The default number is 1. The range is 1 to 5.
- 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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.
- New Password must Differ from the Old Password—Choose the number of characters that must differ between the old and new password. The default number is 1. The range is 1 to 5.
- 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-G317 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 DCC connections. Access through the TCC2/TCC2P RJ-45 port and backplane is not permitted.
  - **Front only**—Allows access through the TCC2/TCC2P RJ-45 port. Access through the DCC and the 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 port, 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:

- Access State—Allows you to set the shell program access mode to Disable (disables shell access), Non-Secure, or Secure. Secure mode allows access to the node using the Secure Shell (SSH) program. SSH is a terminal-remote host Internet protocol that uses encrypted links.
- Telnet Port—Allows access to the node using the Telnet port. Telnet is the terminal-remote host Internet protocol developed for the Advanced Agency Research Project Network (ARPANET). Port 23 is the default.
- Enable Shell Password—If checked, enables the SSH password. To enable the shell password, check the box and click **Apply**. To disable the password, uncheck the check box, click **Apply**, type the current password in the Disable Shell Password dialog box, then click **OK**.

Step 4 In the TL1 Access area, select the desired level of TL1 access. Disabled completely disables all TL1 access; Non-Secure and Secure allow access using SSH.

Step 5 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.

Step 6 Select the Enable Craft Port check box to turn on the shelf controller serial ports.

Step 7 Select the EMS access state from the list. Available states are Non-Secure and Secure (allows access using SSH).

Step 8 In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
- **Standard Constant**—Uses Port 683 (IIOP) or Port 684 (SSLIOP), the CORBA default port number.
- **Other Constant**—If the default port is not used, type the IIOP or SSLIOP (Secure Socket Layer Inter-ORB Protocol) port specified by your firewall administrator.

Step 9 In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).

Step 10 Click **Apply**.

Step 11 Return to your originating procedure (NTP).

DLP-G328 Grant Superuser Privileges to a Provisioning User

Purpose	This task enables a provisioning user to retrieve audit logs, restore databases, clear PMs, and activate and revert software loads.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 In the Defaults Selector area, choose **NODE**.

Step 3 In the Default Name area, choose one of the following parameters:

- NODE.security.grantPermission.RetrieveAuditLog
- NODE.security.grantPermission.RestoreDB
- NODE.security.grantPermission.PMClearingPrivilege
- NODE.security.grantPermission.ActivateRevertSoftware

Step 4 Click the Default Value column and choose **Provisioning** from the drop-down list for each property in Step 3 that you want to change.

Note If you click **Reset** before you click **Apply**, all values will return to their original settings.

Step 5 Click **Apply**.

A pencil icon will appear next to the default name that will be changed as a result of editing the defaults file.

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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note Each ONS 15454 must have one user with a Superuser security level. The default CISCO15 user name and security level cannot be changed unless you create another user with Superuser security.

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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" task on page 3-8 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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.
- Disable the user.
- Force the user to change password on next login.

See the "DLP-G55 Create a New User on Multiple Nodes" task on page 3-9 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).

Note The Select Applicable Nodes area does not appear for users who are provisioned for only one node.

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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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 10-60, 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 (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Security** > **Users** tabs.

Step 2 Choose the user that 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 that 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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 10-61, 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.

Note The Select Applicable Nodes area does not appear for users who are provisioned for only one node.

Step 5 Click **OK**. A User Deletion Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes.

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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 else 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 10-52 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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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 that 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 else 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 10-53 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).

DLP-G281 Configure the Node for RADIUS Authentication

Purpose	This task allows you to configure a node for Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS validates remote users who are attempting to connect to the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26 Before configuring the node for RADIUS authentication, you must first add the node as a network device on the RADIUS server. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about configuring a RADIUS server.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Do not configure a node for RADIUS authentication until after you have added that node to the RADIUS server and added the RADIUS server to the list of authenticators. If you do not add the node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Note The following Cisco vendor-specific attribute (VSA) needs to be specified when adding users to the RADIUS server:

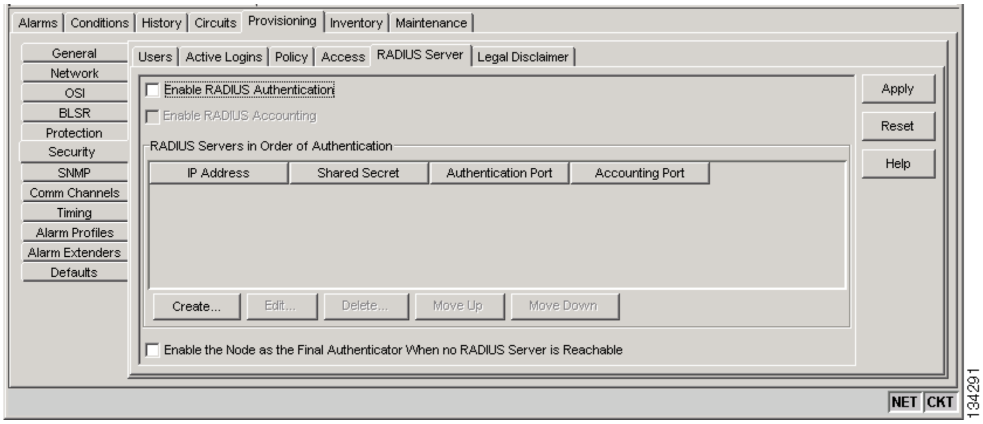
shell:priv-lvl=*N*

where *N* is equal to:

- 0 for Retrieve user
- 1 for Maintenance user
- 2 for Provisioning user
- 3 for Superuser

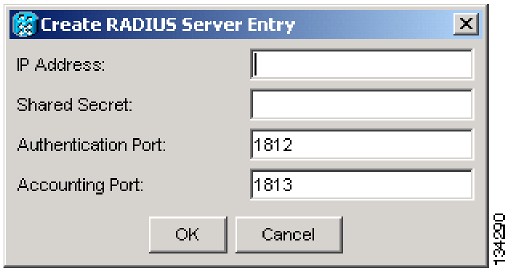
Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning > Security > RADIUS Server** tabs (Figure 10-5).

Figure 10-5 RADIUS Server Tab



Step 2 Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry dialog box appears (Figure 10-6).

Figure 10-6 Create RADIUS Server Entry Window



Create RADIUS Server Entry

IP Address:

Shared Secret:

Authentication Port: 1812

Accounting Port: 1813

Step 3 Enter the RADIUS server IP address in the IP Address field. If the node is an end network element (ENE), enter the IP address of the gateway network element (GNE) in this field.

The GNE passes authentication requests from the ENEs in its network to the RADIUS server, which grants authentication if the GNE is listed as a client on the server.

Caution Because the ENE nodes use the GNE to pass authentication requests to the RADIUS server, you must add the ENEs to the RADIUS server individually for authentication. If you do not add the ENE node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Step 4 Enter the shared secret in the Shared Secret field. A shared secret is a text string that serves as a password between a RADIUS client and RADIUS server.

Step 5 Enter the RADIUS authentication port number in the Authentication Port field. The default port is 1812. If the node is an ENE, set the authentication port to a number within the range of 1860 to 1869.

Step 6 Enter the RADIUS accounting port in the Accounting Port field. The default port is 1813. If the node is an ENE, set the accounting port to a number within the range of 1870 to 1879.

Step 7 Click **OK**. The RADIUS server is added to the list of RADIUS authenticators.

Note You can add up to 10 RADIUS servers to a node's list of authenticators.

Step 8 Click **Edit** to make changes to an existing RADIUS server. You can change the IP address, the shared secret, the authentication port, and the accounting port.

Step 9 Click **Delete** to delete the selected RADIUS server.

Step 10 Select a server and click **Move Up** or **Move Down** to reorder that server in the list of RADIUS authenticators. The node requests authentication from the servers sequentially from top to bottom. If one server is unreachable, the node will request authentication from the next RADIUS server on the list.

Step 11 Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.

Step 12 Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.

Step 13 Click the **Enable the Node as the Final Authenticator** check box if you want the node to be the final autheticator. This means that if every RADIUS authenticator is unavailable, the node will authenticate the login rather than locking the user out.

Step 14 Click **Apply** to save all changes or **Reset** to clear all changes.

Step 15 Return to your originating procedure (NTP).

DLP-G282 View and Terminate Active Logins

Purpose	This task allows you to view active CTC logins, retrieve the last activity time, and terminate all current logins.
Tools/Equipment	None
Prerequisite Procedures	DLP-G46 Log into CTC, page 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher for viewing; Superuser for session termination

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning > Security > Active Logins** tabs. The Active Logins tab displays the following information:

- User ID
- User IP address
- Current node the user is logged into
- Session Type (EMS, TL1, FTP, Telnet, or SSH)
- Login time
- Last activity time

Step 2 Click **Logout** to end the session of every logged-in user. This will log out all current users, excluding the initiating Superuser.

Step 3 Click **Retrieve Last Activity Time** to display the most recent activity date and time for users in the Last Activity Time field.

Step 4 Return to your originating procedure (NTP).

NTP-G89 Change SNMP Settings

Purpose	This procedure modifies the SNMP settings for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	NTP-G28 Set Up SNMP, page 3-40
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 2-26. If you are already logged in, continue with Step 2.

Step 2 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

Step 3 Perform any of the following tasks as needed:

- DLP-G197 Modify SNMP Trap Destinations, page 10-65
- DLP-G198 Delete SNMP Trap Destinations, page 10-66

Step 4 Complete the "NTP-G103 Back Up the Database" procedure on page 13-2.

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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 DWDM Reference Manual*.

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 (NMS).

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 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; if not, repeat the task.

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 2-26
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Trap Destinations area, click the trap that 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).