CHAPTER 18

DLPs D100 to D199

DLP-D100 Delete a Proxy Tunnel

Purpose	This task removes a proxy tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Click the **Provisioning > Network > Proxy** subtabs.

Step 2 Click the proxy tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Continue with your originating procedure (NTP).

DLP-D101 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Step 1 Click the **Provisioning > Network > Firewall** subtabs.

Step 2 Click the firewall tunnel that you want to delete.

Step 3 Click **Delete**.

Step 4 Return to your originating procedure (NTP).

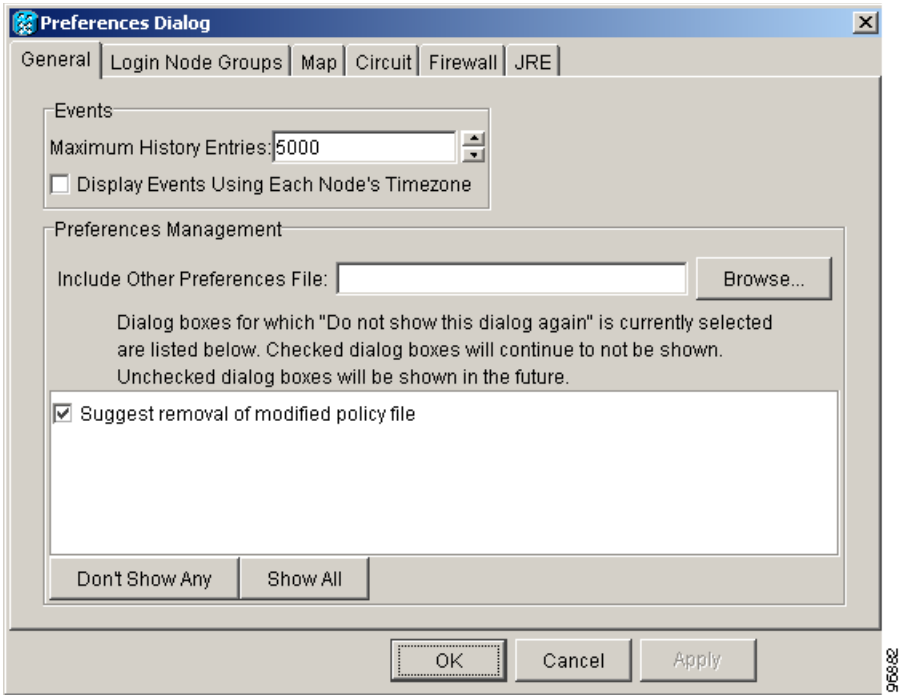
DLP-D111 Changing the Maximum Number of Session Entries for Alarm History

Purpose	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

The CTC Preferences dialog box appears (Figure 18-1).

Figure 18-1 CTC Preferences Dialog Box



Step 2 Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

Step 3 Click **Apply** and **OK**.

Note Setting the Maximum History Entries value to the high end of the range uses more Cisco Transport Controller (CTC) memory and could impair CTC performance.

Note This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

Step 4 Return to your originating procedure (NTP).

DLP-D112 Display Alarms and Conditions Using Time Zone

Purpose	This task changes the time stamp for events to the time zone of the ONS node reporting the alarm. By default, the events time stamp is set to the time zone for the CTC workstation.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

The CTC Preferences dialog box appears (Figure 18-1 on page 18-2).

Step 2 Check the **Display Events Using Each Node's Timezone** check box. The Apply button is enabled.

Step 3 Click **Apply** and **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-D113 Synchronize Alarms

Purpose	Use this task to view ONS 15454 SDH events at the card, node, or network level and to refresh the alarm listing so that you can check for new and cleared alarms and conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 At the card, node, or network view, click the **Alarms** tab.

Step 2 Click **Synchronize**.

This button causes CTC to retrieve a current alarm summary for the card, node, or network. This step is optional because CTC updates the Alarms window automatically as raise/clear messages arrive from the node.

Note Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

Step 3 Return to your originating procedure (NTP).

DLP-D114 View Conditions

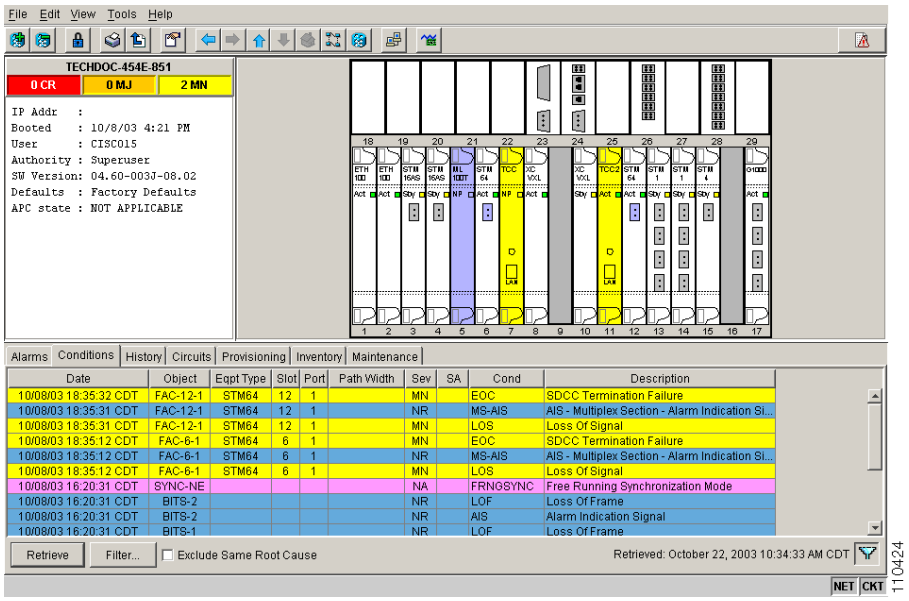
Purpose	Use this task to view conditions [events with a Not Reported (NR) severity] at the card, node, or network level. The Conditions tab gives you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From card, node, or network view, click the **Conditions** tab.

Step 2 Click **Retrieve** (Figure 18-2).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when events change on the node. You must click Retrieve to see any changes.

Figure 18-2 Node View Conditions Window



Conditions include all fault conditions raised on the node, whether or not they are reported.

Note Alarms can be unreported when they are filtered out of the display. See the "DLP-D227 Disable Alarm Filtering" task on page 19-18 for information.

Events that are reported as Major (MJ), Minor (MN), or Critical (CR) severities are alarms. Events that are reported as Not Alarmed (NA) are conditions. Conditions that are not reported at all are marked NR in the Conditions window severity column.

Conditions that have a default severity of CR, MJ, MN, or NA but are not reported due to exclusion or suppression are shown as NR in the Conditions window.

Current conditions are shown with the severity chosen in the alarm profile, if used. For more information about alarm profiles, see the "NTP-D71 Create, Download, and Assign Alarm Severity Profiles" procedure on page 7-6.

Note When a port is placed in the Locked-enabled,maintenance service state, it raises an Alarms Suppressed for Maintenance (AS-MT) condition. For information about alarm and condition troubleshooting, refer to the *Cisco ONS 15454 SDH Troubleshooting Guide*.

Note When a port is placed in the Unlocked-disabled,automaticInService service state but is not connected to a valid signal, it generates a loss of signal (LOS) alarm.

Step 3 If you want to apply exclusion rules, check the **Exclude Same Root Cause** check box at the node or network view, but do not check the Exclude Same Root Cause check box in card view.

An exclusion rule eliminates all lower-level alarms or conditions that originate from the same cause. For example, a fiber break might cause an LOS alarm, an alarm indication signal (AIS) condition, and a signal failure (SF) condition. If you check the Exclude Same Root Cause check box, only the LOS alarm will appear. According to IEEE, exclusion rules apply to a query of "all conditions from a node."

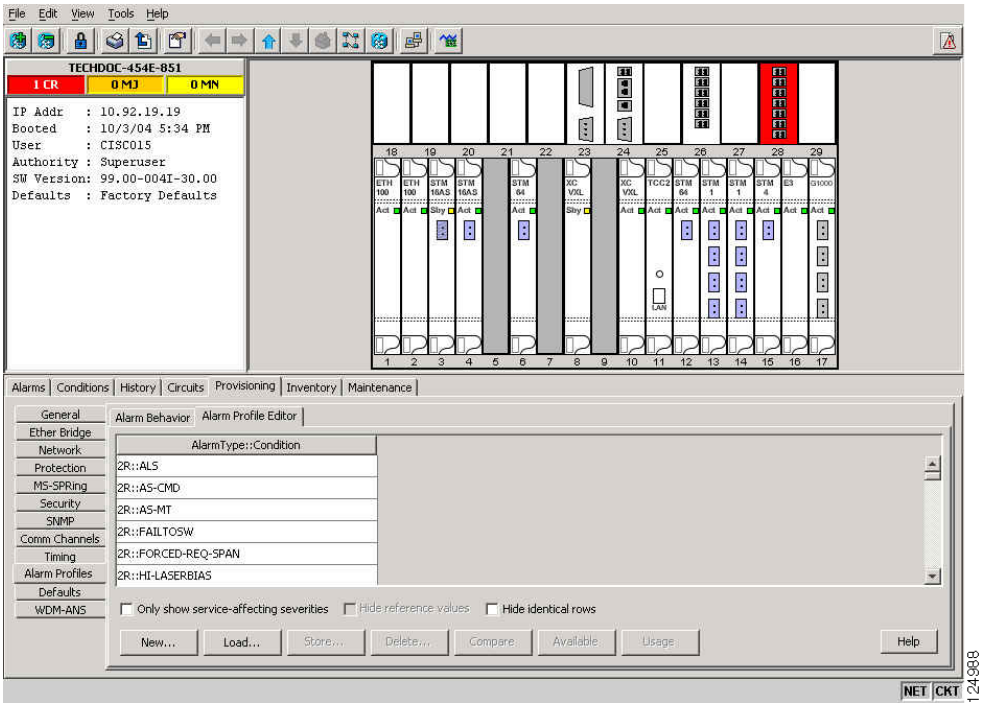
Step 4 Return to your originating procedure (NTP).

DLP-D117 Apply Alarm Profiles to Cards and Nodes

Purpose	This task applies a custom or default alarm profile to cards or nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D425 Create a New or Cloned Alarm Severity Profile, page 21-7 DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tab (Figure 18-3).

Figure 18-3 Node View Alarm Profile



Step 2 To apply profiles to a card:

a. Click the Profile row for the card.

b. Choose the new profile from the drop-down list.

c. Click **Apply**.

Step 3 To apply the profile to an entire node:

a. Click the **Node Profile** drop-down arrow at the bottom of the window (Figure 18-3).

b. Choose the new alarm profile from the drop-down list.

c. Click **Apply**.

Step 4 To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

Step 5 Return to your originating procedure (NTP).

DLP-D121 Enable Pointer Justification Count Performance Monitoring

Purpose	This task enables pointer justification counts, which provide a way to align the phase variations in VC4 payloads and to monitor the clock synchronization between nodes. A consistent, large, pointer justification count indicates clock synchronization problems between nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the STM-N card that you want to monitor. The card view appears.

See Table 18-1 for a list of STM-N line terminating equipment (LTE) cards.

Table 18-1 Traffic Cards that Terminate the Line (LTEs)

Line Terminating Equipment
STM1E-12
OC3 IR 4/STM1 SH 1310
OC3 IR/STM1SH 1310-8
OC12 IR/STM4 SH 1310
OC12 LR/STM4 LH 1310
OC12 LR/STM4 LH 1550
OC12-4 IR/STM4 SH 1310-4
OC48 IR/STM16 SH AS 1310
OC48 LR/STM16 LH AS 1550
OC48 ELR/STM16 EH 100 GHz
OC192 SR/STM64 IO 1310

Table 18-1 Traffic Cards that Terminate the Line (LTEs) (continued)

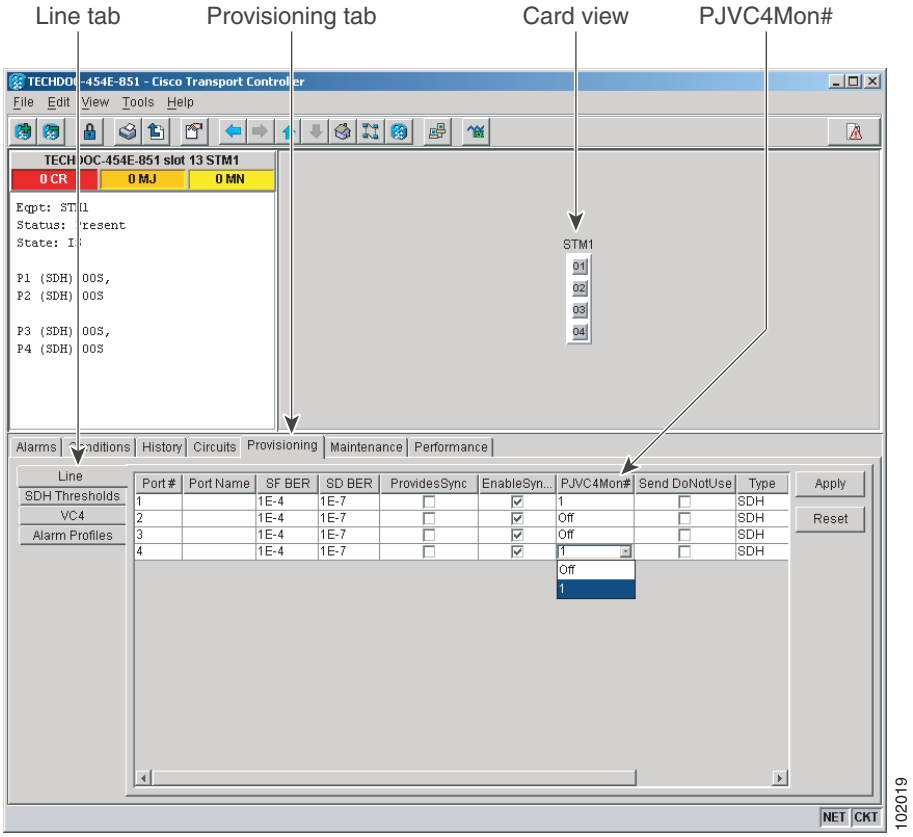
Line Terminating Equipment
OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550
OC192 ELR/STM64 LH ITU 15xx.xx

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Click the PJVC4Mon# drop-down list and make a selection based on the following rules (Figure 18-4):

- Off means pointer justification monitoring is disabled (default).
- Values 1 to *n* are the number of VC4s on the port. One VC4 per port can be enabled from the PJVC4Mon# card drop-down list.

Figure 18-4 Enabling or Disabling Pointer Justification Count Parameters



Step 4 In the Service State field, confirm that the port is in the Unlocked-enabled service state.

Step 5 If the port is Unlocked-enabled, click **Apply**. If the port is out of service (Locked-enabled,disabled; Locked-enabled,maintenance; Unlocked-disabled,automaticInService), choose **Unlocked** in the Admin State drop-down list and click **Apply**.

Step 6 Click the **Performance** tab to view performance monitoring (PM) parameters. Refer to the *Cisco ONS 15454 SDH Reference Manual* for more PM information, details, and definitions.

Note The fields for positive pointer justification count (PPJC) and negative pointer justification count (NPJC) PM parameters appear white and blank unless pointer justification count performance monitoring is enabled.

Step 7 Return to your originating procedure (NTP).

DLP-D122 Enable Intermediate Path Performance Monitoring

Purpose	This task enables intermediate path performance monitoring (IPPM), which allows you to monitor large amounts of VC4 traffic through intermediate nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

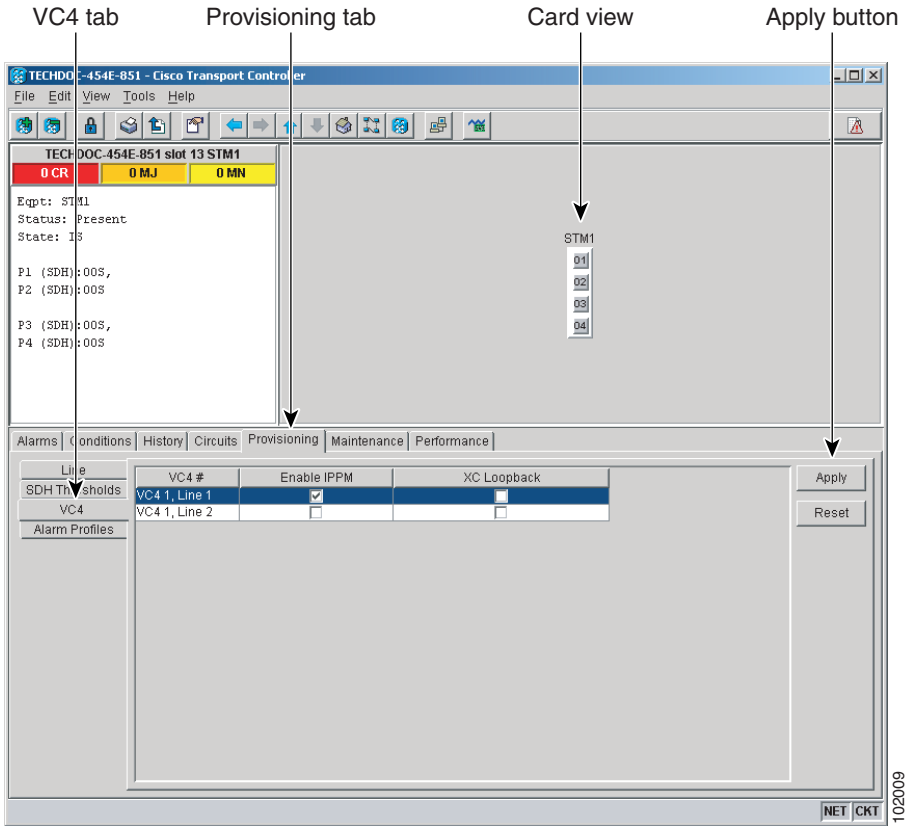
Note The monitored IPPM parameters are P-EB, P-BBE, P-ES, P-SES, and P-UAS. For more information about IPPM parameters, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

Step 1 In node view, double-click the STM-N card you want to monitor. The card view appears.

See Table 18-1 on page 18-7 for a list of STM-N LTE cards.

Step 2 Click the **Provisioning > VC4** tabs (Figure 18-5).

Figure 18-5 VC4 Tab for Enabling or Disabling IPPM



Step 3 Click the check box in the Enable IPPM column and make a selection based on the following rules:

- Unchecked means that IPPM is disabled for that VC4 (default).
- Checked means that IPPM is enabled for that VC4.

Step 4 Click **Apply**.

Step 5 Click the **Performance** tab to view PM parameters. For IPPM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

Step 6 Return to your originating procedure (NTP).

DLP-D124 Refresh PM Counts at 15-Minute Intervals

Purpose	This task changes the window view to display PM counts in 15-minute intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **15 min** radio button.

Step 4 Click **Refresh**. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-D125 Refresh PM Counts at One-Day Intervals

Purpose	This task changes the window view to display PM parameters in one-day intervals.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **1 day** radio button.

Step 4 Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.

Step 5 View the Curr column to find PM counts for the current 1-day interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 1-day interval, a TCA is raised. The number represents the counter value for each specific performance monitoring parameter.

Step 6 View the Prev-*n* columns to find PM counts for the previous 1-day intervals.

Note If a complete count over a 1-day interval is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

Step 7 Return to your originating procedure (NTP).

DLP-D126 View Near-End PM Counts

Purpose	This task enables you to view near-end PM counts for the selected card and port.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Near End** radio button.

Step 4 Click **Refresh**. All PM parameters occurring for the selected card on the incoming signal appear. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-D127 View Far-End PM Counts

Purpose	This task enables you to view far-end PM counts for the selected card and port. Only cards that allow far-end monitoring have the Far End radio button as an option.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click the **Far End** radio button.

Step 4 Click **Refresh**. All PM parameters recorded by the far-end node for the selected card on the outgoing signal appear. For PM parameter definitions, refer to the *Cisco ONS 15454 SDH Reference Manual*.

Step 5 View the Curr column to find PM counts for the current time interval.

Step 6 View the Prev-*n* columns to find PM counts for the previous time intervals.

Step 7 Return to your originating procedure (NTP).

DLP-D129 Reset Current PM Counts

Purpose	This task clears the current PM count, but it does not clear the cumulative PM count. This task allows you to see how quickly PM counts rise.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the card where you want to view PM counts. The card view appears.

Step 2 Click the **Performance** tab.

Step 3 Click **Baseline**.

Note The Baseline button clears the PM counts displayed in the current time interval, but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and on the window appear in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance Monitoring window.

Step 4 View the current statistics columns to observe changes to PM counts for the current time interval.

Step 5 Return to your originating procedure (NTP).

DLP-D131 Search for Circuits

Purpose	This task searches for ONS 15454 SDH circuits at the network, node, or card level.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To search the entire network, from the View menu, choose **Go to Network View**.
- To search for circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 If you are in node or card view, choose the scope for the search (**Network** or **Node**) in the Scope drop-down list.

Step 4 Click **Search**.

Step 5 In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the text of the circuit name you want to find.
- Match Whole Word Only—Check this check box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.
- Match Case—Check this check box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
- Direction—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.

Step 6 Click **Find Next**. If a match is found, click **Find Next** again to find the next circuit.

Step 7 Repeat Steps 5 and 6 until you are finished, then click **Cancel**.

Step 8 Return to your originating procedure (NTP).

DLP-D137 Provision a J1 Path Trace on STM-N Ports

Purpose	This task monitors a path trace on VC4 high-order ports within the circuit path.
Tools/Equipment	The STM-N ports you want to monitor must be on STM-N cards capable of receiving path trace. See Table 19-3 on page 19-47 for a list of applicable cards.
Prerequisite Procedures	DLP-D264 Provision a J1 Path Trace on Circuit Source and Destination Ports, page 19-46 DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note To monitor the J1 path on STM-N ports, the circuit endpoints must be transmitting VC4 J1 and not VC3 J1.

Step 1 From the View menu, choose **Go to Other Node**. In the Select Node dialog box, choose the node where path trace was provisioned on the circuit source and destination ports.

Step 2 Click **Circuits**.

Step 3 Choose the VC4 circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4 In the Edit Circuit window, click the Show Detailed Map check box at the bottom of the window. A detailed circuit graphic showing source and destination ports appears.

Step 5 On the detailed circuit map, right-click the circuit STM-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

Note The STM-N port must be on a receive-only card listed in Table 19-3 on page 19-47. If not, the Edit Path Trace menu item does not appear.

Step 6 In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other path trace end as the current expected string. An alarm is raised when a string that differs from the baseline is received. For STM-N ports, Auto is recommended because Manual mode requires you to trace the circuit on the Edit Circuit window to determine whether the port is the source or destination path.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Note It is not necessary to set the format (16 or 64 bytes) for the expected string; the path trace process automatically determines the format.

Step 7 If you set the Path Trace Mode field to Manual, enter the string that the STM-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit window to determine whether the port is in the circuit source or destination path, then set the New Expected String to the string transmitted by the circuit source or destination. If you set the Path Trace Mode field to Auto, skip this step.

Step 8 Click **Apply**, then click **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-D140 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-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

Step 2 Change any of the following:

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

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

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time

See the "NTP-D316 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 for detailed field descriptions.

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

Step 4 Return to your originating procedure (NTP).

DLP-D142 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47 DLP-D65 Create a Static Route, page 17-54
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

Step 3 Click the static route you want to edit.

Step 4 Click **Edit.**

Step 5 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-D65 Create a Static Route" task on page 17-54 for detailed field descriptions.

Step 6 Click **OK**.

Step 7 Return to your originating procedure (NTP).

DLP-D143 Delete a Static Route

Purpose	This task deletes an existing static route on an ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47 DLP-D65 Create a Static Route, page 17-54
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-D144 Disable OSPF

Purpose	This task disables the Open Shortest Path First (OSPF) routing protocol process for an ONS 15454 SDH LAN.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Disabling OSPF can cause the TCC2/TCC2P card to reboot. A TCC2/TCC2P card reboot causes a temporary loss of connectivity to the node, but traffic is unaffected.

Step 1 In node view, click the **Provisioning > Network > OSPF** tabs. The OSPF subtab has several options.

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN?** check box.

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

Step 4 Return to your originating procedure (NTP).

DLP-D145 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-D60 Log into CTC, page 17-47
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

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

Step 2 If you want to change a domain background, double-click the domain. If not, continue with Step 3.

Step 3 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 4 In the Choose Color dialog box, select a background color.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-D148 Create Domain Icons

Purpose	This task creates a domain, which is an icon that groups ONS 15454 SDH icons in CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-D60 Log into CTC, page 17-47
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 To add nodes to the domain, continue with the "DLP-D149 Manage Domain Icons" task on page 18-19.

Step 6 Return to your originating procedure (NTP).

DLP-D149 Manage Domain Icons

Purpose	This task manages CTC network view domain icons.
Tools/Equipment	None
Prerequisite procedures	DLP-D60 Log into CTC, page 17-47 DLP-D148 Create Domain Icons, page 18-19
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Domain changes, such as added or removed node icons, are visible to all users who log into the network.

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

Step 2 Locate the domain action you want in Table 18-2 and complete the appropriate steps.

Table 18-2 Managing Domains

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

Step 3 Return to your originating procedure (NTP).

DLP-D150 Modify a 1:1 Protection Group

Purpose	This task modifies a 1:1 protection group for electrical cards (E1-N-14, E3-12, and DS3i-N-12) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D71 Create a 1:1 Protection Group, page 17-61 DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Protection Groups area, click the 1:1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Revertive—Check this box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time drop-down list. Uncheck if you do not want traffic to revert.
- Reversion time—If the Revertive check box is selected, choose the reversion time from the Reversion time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Note To convert 1:1 protection groups, see the "NTP-D91 Upgrade E1-N-14 and DS3 i-N-12 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 11-4.

Step 5 Return to your originating procedure (NTP).

DLP-D152 Modify a 1:N Protection Group

Purpose	This task modifies a 1:N protection group for E1-N-14 and DS3i-N-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D72 Create a 1:N Protection Group, page 17-62 DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the E1-N-14 and DS3i-N-12 cards are installed according to the 1:N specifications in the "DLP-D72 Create a 1:N Protection Group" task on page 17-62.

Step 2 In node view, click the **Provisioning** > **Protection** tabs.

Step 3 In the Protection Groups area, click the 1:N protection group you want to modify.

Step 4 In the Selected Group area, change any of the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Available Entities—If cards are available, they will appear here. Use the arrow buttons to move them into the Working Cards column.
- Working Entities—Use the arrow buttons to move cards out of the Working Cards column.
- Reversion Time—Choose a reversion time from the 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.

See the "DLP-D72 Create a 1:N Protection Group" task on page 17-62 for field descriptions.

Step 5 Click **Apply**. The changes are applied. Confirm that the changes appear; if not, repeat the task.

Note To convert 1:1 protection groups, see the "NTP-D91 Upgrade E1-N-14 and DS3 i-N-12 Protect Cards from 1:1 Protection to 1:N Protection" procedure on page 11-4.

Step 6 Return to your originating procedure (NTP).

DLP-D154 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port (STM-1, STM-4, STM-16, STM-64).
Tools/Equipment	None
Prerequisite Procedures	DLP-D73 Create a 1+1 Protection Group, page 17-63 DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Protection Groups area, click the 1+1 protection group you want to modify.

Step 3 In the Selected Group area, you can modify the following, as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—Check or uncheck.
- 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 drop-down list. Uncheck 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.

See the "DLP-D73 Create a 1+1 Protection Group" task on page 17-63 for field descriptions.

Step 4 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-D155 Delete a Protection Group

Purpose	This task deletes a 1:1, 1:N, 1+1, or Y Cable protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Protection Groups area, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box to confirm deletion. Confirm that the changes appear; if they do not, repeat Steps 1 through 3.

Step 5 Return to your originating procedure (NTP).

DLP-D156 Delete a Section DCC Termination

Purpose	This task deletes an SDH Section DCC (SDCC) termination on the ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Deleting a data communications channel (DCC) termination can cause you to lose visibility to nodes that do not have other DCCs or network connections to the CTC computer.

Step 1 Click the **SDCC** tab.

Step 2 Click the SDCC termination and click **Delete**. The Delete SDCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-D157 Change the Node Timing Source

Purpose	This task changes the SDH timing source for the ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
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.

Note See the "DLP-D69 Set Up External or Line Timing" task on page 17-57 for descriptions of the fields mentioned in this task.

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

Step 2 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.

- Revertive
- Reversion Time

Step 3 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 pins on the MIC-C/T/P. 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 4 Click the **BITS Facilities** tab.

Step 5 In the BITS In and BITS Out areas, you can change the following information:

Note The BITS Facilities section sets the parameters for your BITS-1 and BITS-2 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.

- Facility Type: E1, 2 MHz
- BITS In State
- BITS Out State
- Coding
- Framing
- Sync Messaging
- Admin SSM
- AIS Threshold
- Sa Bit

Step 6 Click **Apply**. Confirm that the changes appear; if not, repeat the task.

Note Refer to the "Security and Timing" chapter in the *Cisco ONS 15454 SDH Reference Manual* for timing information.

Step 7 Return to your originating procedure (NTP).

DLP-D158 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-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 2 Click the user whose settings you want to modify.

Step 3 Click **Change**.

Step 4 In the Change User dialog box, you can:

- Change the existing user password
- Change the existing user security level
- Lock out the user

See the "NTP-D30 Create Users and Assign Security" procedure on page 4-3 for fields and descriptions.

Step 5 Click **OK**.

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-D159 Delete a User on a Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-D315 Log Out a User on a Single Node" task on page 20-10, or you can choose the "Logout before delete" option on the Delete User dialog box.

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

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

Step 2 Choose the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, verify that the user name displayed is the one you want to delete.

Step 5 Click **OK**. Confirm that the changes appear; if not, repeat the task.

Step 6 Return to your originating procedure (NTP).

DLP-D160 Change User Password and Security Level on Multiple Nodes

Purpose	This task modifies existing user settings for multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 1 From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to add users.

Step 2 Click the **Provisioning > Security > Users** tabs. Highlight the user's name whose settings you want to change.

Step 3 Click **Change**. The Change User dialog box appears.

Step 4 In the Change User dialog box, enter the following information:

- New Password
- Confirm New Password
- Security Level

See the "DLP-D75 Create a New User on Multiple Nodes" task on page 17-64 for field descriptions.

Step 5 Under "Select applicable nodes," uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).

Step 6 Click **OK**. A Change Results confirmation dialog box appears.

Step 7 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 8 Return to your originating procedure (NTP).

DLP-D161 Delete a User on Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note You cannot delete a user who is currently logged in. To log out a user, you can complete the "DLP-D316 Log Out a User on Multiple Nodes" task on page 20-10, or you can choose the "Logout before delete" option on the Delete User dialog box.

Note CTC will allow you to delete other Superuser only if at least one Superuser remains. For example, you can delete the CISCO15 user only 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 > Users** tabs. Highlight the name of the user you want to delete.

Step 3 Click **Delete**. The Delete User dialog box appears.

Step 4 Click **OK**. A Change Results confirmation dialog box appears.

Step 5 Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.

Step 6 Return to your originating procedure (NTP).

DLP-D163 Delete SNMP Trap Destination

Purpose	This task deletes SNMP trap destinations on an ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Trap Destinations area, click the trap you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**. Confirm that the changes appear; if not, repeat the task.

Step 5 Return to your originating procedure (NTP).

DLP-D170 Change Line Settings for STM-N Cards

Purpose	This task changes the line transmission settings for STM-N cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the STM-N card where you want to change the line settings.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 Modify any of the settings listed in Table 18-3.

Step 4 Click **Apply**.

Table 18-3 STM-N Card Line Settings

Parameter	Description	Options
Port	Displays the port number (read-only).	• 1 (STM-4, STM-16, STM-64) • 1 to 4 (OC3 IR 4/STM1 SH 1310, OC12 IR/STM4 SH 1310-4) • 1 to 8 (OC3IR/STM1SH 1310-8)
Port Name	Assign a name to the specified port.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-D314 Assign a Name to a Port" task on page 20-9.
SF BER	Sets the signal fail bit error rate.	• 1E-3 • 1E-4 • 1E-5
SD BER	Sets the signal degrade bit error rate.	• 1E-5 • 1E-6 • 1E-7 • 1E-8 • 1E-9
Provides Synch	(Read-only) If checked, the card is provisioned as a network element timing reference.	• Yes • No
Send Do Not Use	When checked, sends a do not use (DUS) message on the S1 byte.	• Yes • No
Synch Message In	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	• Yes • No
Send <FF> DoNotUse	When checked, sends a special DUS (0xff) message on the S1 byte.	• Yes • No
Admin SSM In	Overrides the synchronization traceability unknown (STU) value (default setting). You cannot select Admin SSM In if Sync Message In is enabled on the STM-N card.	• G811 • G812T • G812L • SETS • DUS
MS-SPRing Ext. Byte	Allows you to change the multiplex section-shared protection ring (MS-SPRing) extension byte.	• K3 • Z2 • E2 • F1

Table 18-3 STM-N Card Line Settings (continued)

Parameter	Description	Options
PJVC4Mon #	Sets the VC4 that will be used for pointer justification. If set to 0, no VC4 is monitored. Only one VC4 can be monitored on each STM-N port.	• 0 - 1 (STM-1, per port) • 0 - 4 (STM-4, per port) • 0 - 16 (STM-16) • 0 - 64 (STM-64)
Admin State	Sets the port service state unless network conditions prevent the change. For more information about administrative states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 SDH Reference Manual*.	• Unlocked—Puts the port in-service. The port service state changes to Unlocked-enabled. • Unlocked,automaticInService—Puts the port in automatic in-service. The port service state changes to Unlocked-disabled,automaticInService. • Locked,disabled—Removes the port from service and disables it. The port service state changes to Locked-enabled,disabled. • Locked,maintenance—Removes the port from service for maintenance. The port service state changes to Locked-enabled,maintenance.
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State. For more information about service states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 SDH Reference Manual*.	• Unlocked-enabled—The port is fully operational and performing as provisioned. • Unlocked-disabled,automaticInService—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in the Unlocked-disabled,automaticInService state for the duration of the soak period. After the soak period ends, the port service state changes to Unlocked-enabled. • Locked-enabled,disabled—The port is out-of-service and unable to carry traffic. • Locked-enabled,maintenance—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
AINS Soak	Sets the automatic in-service soak period.	• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically • 0 to 48 hours, 15-minute increments
Type	Displays the port as SDH.	• SDH

Step 5 Return to your originating procedure (NTP).

DLP-D176 Convert E1-N-14 Cards From 1:1 to 1:N Protection

Purpose	This task converts E1-N-14 cards in a 1:1 protection scheme to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes E1-N-14 cards are installed in Slots 1 through 6 and/or Slots 12 through 17. The E1-N-14 cards in Slots 3 and 15 are the protect cards. Each protect card protects the other E1-N-14 cards in that half of the shelf. The ONS 15454 SDH must run CTC Software Release 4.0 or later.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains Slot 3 or Slot 15 (where you will install the protect E1-N-14 card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby and not Working/Active. If the protect slot status is Working/Active, use the following steps to switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click Switch.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they do not change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 1 through 3 for each protection group that you need to convert.

Step 5 Verify that no standing alarms exist for any of the E1-N-14 cards that you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection group does not disrupt service. However, no protection bandwidth exists for the working circuits until you complete the 1:N protection procedure. Therefore, complete this procedure as quickly as possible.

Step 10 If needed, repeat Steps 7 through 9 for other protection groups.

Step 11 Physically insert an E1-N-14 card into the protection slot (Slot 3 or Slot 15).

Step 12 Verify that the card boots up properly.

Step 13 Click the **Inventory** tab and verify that the new card appears as an E1-N-14.

Step 14 Click the **Provisioning > Protection** tabs.

Step 15 Click **Create**.

Step 16 Type a name for the protection group in the Name field (optional).

Step 17 From the Type drop-down list, choose **1:N (card)**.

Step 18 From the Protect Card drop-down list, choose the E1-N-14 card. Verify that the correct E1-N-14 card appears in the Protect Card field.

Step 19 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (**>>**) tab to move the cards to the Working Cards list.

Step 20 If necessary, set a new reversion time in the Reversion time drop-down list.

Note 1:N protection groups are always revertive.

Step 21 Click **OK**. The protection group appears in the Protection Groups list on the Protection subtab.

Step 22 Return to your originating procedure (NTP).

DLP-D177 Convert DS3i-N-12 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3i-N-12 cards from 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note This procedure assumes that DS3i-N-12 cards are installed in Slots 1 to 6 and/or Slots 12 to 17. The DS3i-N-12 cards in Slots 3 and 15 are the protect cards. Each protect card protects the other DS3i-N-12 cards in that half of the shelf. The ONS 15454 SDH must run CTC Software R4.0 or later.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains Slot 3 or Slot 15 (where you will install the DS3i-N-12 card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby and not Working/Active. If the protect slot status is Working/Active, use the following steps to switch traffic to the working card:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

Step 4 Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5 Verify that no standing alarms exist for any of the DS3i-N-12 cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning > Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog box appears, click **Yes**.

Note Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Therefore, complete this procedure as soon as possible.

Step 10 If you are deleting more than one protection group, repeat Steps 7 through 9 for each group.

Step 11 Physically insert a DS3i-N-12 card into the same slot.

Step 12 Verify that the card boots up properly.

Step 13 Click the **Inventory** tab and verify that the new card appears as a DS3i-N-12 card.

Step 14 Click the **Provisioning > Protection** tabs.

Step 15 Click **Create**.

Step 16 Type a name for the protection group in the Name field (optional).

Step 17 Click Type and choose **1:N (card)** from the drop-down list.

Step 18 Verify that the DS3i-N-12 card appears in the Protect Card field.

Step 19 In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 20 Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

Step 21 Return to your originating procedure (NTP).

DLP-D189 Verify that a 1+1 Working Slot is Active

Purpose	This task verifies that a working slot in a 1+1 protection scheme is active (and that the protect slot is in standby).
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Selected Group pane, verify that the working slot/port is shown as Working/Active. If so, this task is complete.

Step 3 If the working slot says Working/Standby, perform a Manual switch on the working slot:

a. In the Selected Group pane, choose the Protect/Active slot.

b. In the Switch Commands field, choose **Manual**.

c. Click **Yes** in the confirmation dialog box.

Step 4 Verify that the working slot is carrying traffic (Working/Active).

Note If the slot is not active, look for conditions or alarms that might be preventing the card from carrying working traffic. Refer to the *Cisco ONS 15454 SDH Troubleshooting Guide*.

Step 5 When the working slot is carrying traffic, clear the Manual switch:

a. In the Switch Commands field, choose **Clear**.

b. Click **Yes** in the confirmation dialog box.

Step 6 Verify that the working slot does not switch back to Standby, which might indicate a problem on the working span.

Step 7 Return to your originating procedure (NTP).

DLP-D191 Delete a Card

Purpose	This task deletes a card from CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Provisioning or higher

Step 1 On the shelf graphic, right-click the card that you want to remove and choose **Delete Card**.

You cannot delete a card if any of the following conditions apply:

- The card is a TCC2/TCC2P card. To replace a TCC2/TCC2P card, refer to the *Cisco ONS 15454 SDH Troubleshooting Guide*.
- The card is part of a protection group; see the "DLP-D155 Delete a Protection Group" task on page 18-23.
- The card has circuits; see the "DLP-D27 Delete Circuits" task on page 17-21.
- The card is part of an MS-SPRing; see the "NTP-D213 Remove an MS-SPRing Node" procedure on page 14-6.
- The card is being used for timing; see the "DLP-D157 Change the Node Timing Source" task on page 18-24.
- The card has a DCC termination; see the "DLP-D156 Delete a Section DCC Termination" task on page 18-23.

Note If you delete a card in CTC but do not remove the card from shelf, it will reboot and reappear in CTC.

Step 2 Return to your originating procedure (NTP).

DLP-D194 Clear an MS-SPRing Force Ring Switch

Purpose	This task removes a Force switch from an MS-SPRing port.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Click **Edit**.

Step 4 To clear a Force switch on the west line:

a. Right-click the MS-SPRing west port where you want to clear the protection switch and choose **Set West Protection Operation**. Ports with a force switch applied are marked with an F.

b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

c. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

Step 5 To clear a Force switch on the east line:

a. Right-click the MS-SPRing east port where you want to clear the protection switch and choose **Set East Protection Operation**. Ports with a Force switch applied are marked with an F.

b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

c. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

On the MS-SPRing network graphic, a green and a purple span line connects each node. This is the normal display for MS-SPRings when protection operations are not invoked.

Step 6 From the File menu, choose **Close**.

Step 7 Return to your originating procedure (NTP).

DLP-D195 Verify Timing in a Reduced Ring

Purpose	This task verifies timing in the ring where you removed a node.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite/remote
Security Level	Provisioning or higher

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

Step 2 Observe the Timing Mode field to see the type of timing (Line, External, Mixed) that has been set for that node.

Step 3 Scroll down to the Reference List and observe the NE Reference fields to see the timing references provisioned for that node.

Step 4 If the removed node was the only building integrated timing supply (BITS) timing source, perform the following:

a. Contact your synchronization coordinator or appropriate personnel before continuing with this procedure.

b. Look for another node on the ring that can be used as a BITS source and set that node's Timing Mode to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-D157 Change the Node Timing Source" task on page 18-24.

c. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set that node's Timing Mode to **External**, set the BITS-1 and BITS-2 BITS In State to **OOS**, and set the NE Reference to **Internal**. Then, choose line timing for all other nodes in the ring. This forces the first node to be their primary timing source. (See the "DLP-D157 Change the Node Timing Source" task on page 18-24.)

Note This type of timing conforms to SETS requirements and is not considered optimal.

Step 5 If the removed node was not the only BITS timing source, provision the adjacent nodes to line timing using SDH links (east and west) as timing sources, traceable to the node with external BITS timing. See the "NTP-D28 Set Up Timing" procedure on page 4-9.

Step 6 Return to your originating procedure (NTP).

DLP-D196 Delete an MS-SPRing from a Single Node

Purpose	This task deletes an MS-SPRing from a node after you remove the node from an MS-SPRing.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, display the node that was removed from the MS-SPRing:

- If the node that was removed is connected to the same LAN as your computer, from the File menu, choose **Add Node**, then enter the node name or IP address.
- If the node that was removed is not connected to the same LAN as your computer, you must connect to the node using a direct connection. See Chapter 3, "Connect the PC and Log into the GUI," for procedures.

Step 2 From node view, click the **Provisioning > MS-SPRing** tabs.

Step 3 Highlight the ring and click **Delete**.

Step 4 In the Suggestion dialog box, click **OK**.

Step 5 In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-D197 Initiate an SNCP Force Switch

Purpose	This task switches all circuits on an subnetwork connection protection (SNCP) span.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The Force Switch Away command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

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

Step 2 Right-click the span where you want to switch SNCP traffic away. Choose **Circuits** from the shortcut menu.

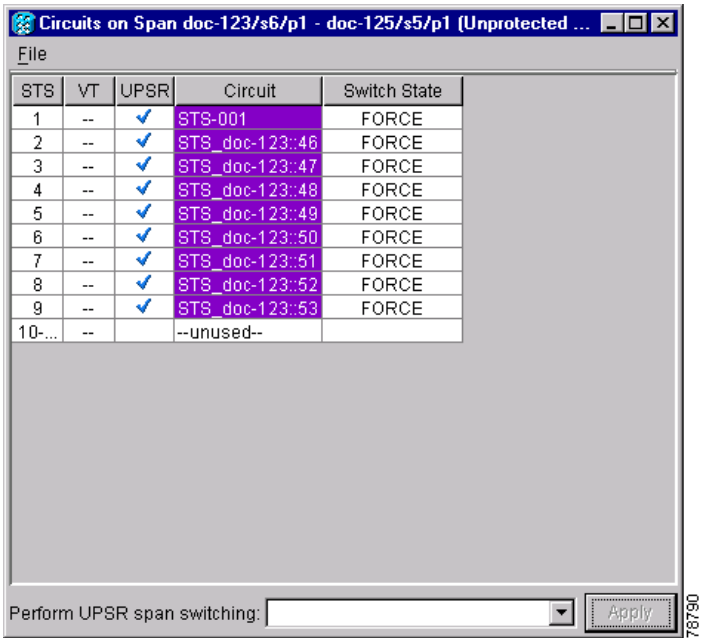
Step 3 In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

Step 4 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all circuits is FORCE. Figure 18-6 shows an example.

Figure 18-6 Circuits on Span Dialog Box with a Force Switch



Note A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition clears when you clear the force switch; it is informational only.

Step 6 Return to your originating procedure (NTP).

DLP-D198 Clear an SNCP Force Switch

Purpose	This task clears an SNCP Force switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC, page 17-47
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

Step 3 In the Circuits on Span dialog box, choose **CLEAR** to remove the Force switch. Click **Apply**.

Step 4 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all SNCP circuits is CLEAR.

Step 6 Return to your originating procedure (NTP).