Contents

DLP-D100 Delete a Proxy Tunnel

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

1. Click the **Provisioning > Network > Proxy** tabs.
2. Click the proxy tunnel that you want to delete.
3. Click **Delete**.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

1. Click the **Provisioning > Network > Firewall** tabs.
2. Click the firewall tunnel that you want to delete.
3. Click **Delete**.
4. Return to your originating procedure (NTP).

DLP-D102 Hard-Reset a CE-100T-8 Card Using CTC

Purpose	This task hard-resets the CE100T-8 Ethernet card.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution! Hard-resetting a CE100T-8 card causes a traffic hit.

Note: The hard-reset option is enabled only when the card is placed in the Locked-disabled,maintenance service state.

1. In node view, click the **Inventory** tab. Locate the appropriate card in the inventory pane.
2. Click the **Admin State** drop-down list and select Locked,maintenance. Click **Apply**.
3. Click **Yes** in the "Action may be service affecting. Are you sure?" dialog box.
4. The service state of the card becomes Locked enabled, loopback & maintenance. The card's faceplate appears blue in Cisco Transport Controller (CTC) and the SRV LED turns amber.

5. Right-click the card to reveal a shortcut menu.
6. Click **Hard-reset Card**.
7. Click **Yes** in the "Are you sure you want to hard-reset this card?" dialog box.
8. Return to your originating procedure (NTP).

DLP-D103 Soft-Reset a CE-100T-8 Card Using CTC

Purpose	This procedure soft-resets the CE-100T-8 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note: Soft-resetting the CE-100T-8 card is errorless in most cases. If there is a provisioning change during the soft reset, or if the firmware is replaced during the software upgrade process, the reset is not errorless.

1. In node view, right-click the CE-100T-8 card to reveal a shortcut menu.
2. Click **Soft-reset Card**.
3. Click **Yes** in the "Are you sure you want to soft-reset this card?" dialog box.
4. Return to your originating procedure (NTP).

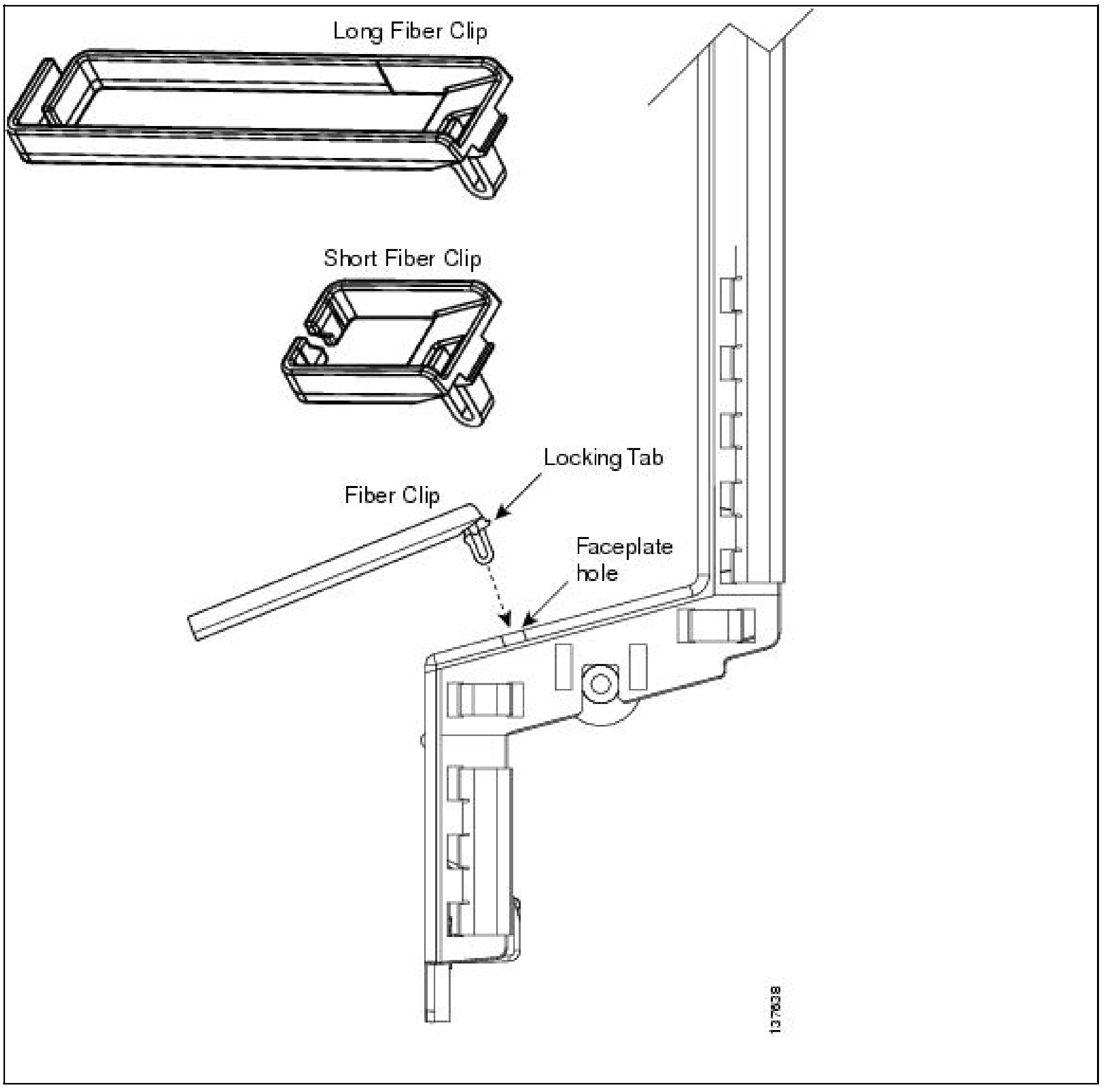
DLP-D104 Install the Fiber Clip on MRC Cards

Purpose	This task installs a fiber clip, which allows proper routing of the fiber. Required for 15454_MRC-12 and MRC-2.5G-12 cards. In CTC, the 15454_MRC-12 card appears as "MRC-12" only.
Tools/Equipment	Short or long fiber clip, as needed
Prerequisite Procedures	NTP-D16 Install STM-N Cards and Connectors
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note: You can install the fiber clip before or after the fibers are attached to the MRC card.

1. Determine the correct clip to use. Use the short clip with a standard cabinet door and a long clip with an extended door.
2. Insert the prong of the fiber clip into the rectangular cutout on the sloped face of the faceplate (Figure 18-1).

Figure 18-1: Installing the Fiber Clip



3. Push the clip into the hole until the locking tab snaps the clip securely into place. To remove a fiber clip, push on the locking tab to release the clip while rotating the clip forward and up.
4. Return to your originating procedure (NTP).

DLP-D105 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-D60 Log into CTC 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

Figure 18-1: Installing the Fiber Clip

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.

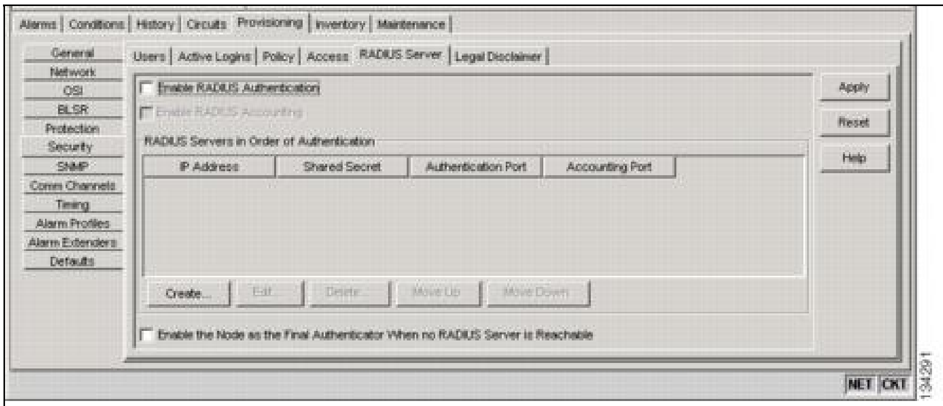
Note: The following Cisco vendor-specific attribute (VSA) needs to be specified when adding users to the RADIUS server:

shell:priv-lvl=*N*, where *N* is:

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

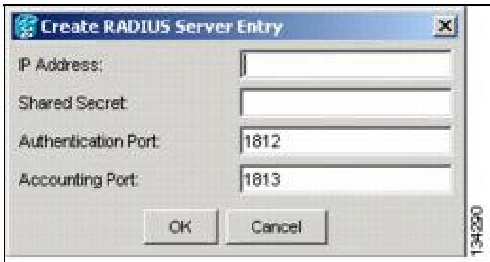
1. In node view, click the **Provisioning > Security > RADIUS Server** tabs (Figure 18-2).

Figure 18-2: RADIUS Server Tab



2. Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 18-3).

Figure 18-3: Create RADIUS Server Entry Window



Create RADIUS Server Entry

IP Address:

Shared Secret:

Authentication Port: 1812

Accounting Port: 1813

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.

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.
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.
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.
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.
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.
9. Click **Delete** to delete the selected RADIUS server.
10. Click **Move Up** or **Move Down** to reorder 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.
11. Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.
12. Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.
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.
14. Click **Apply** to save all changes or **Reset** to clear all changes.
15. Return to your originating procedure (NTP).

DLP-D106 View and Terminate Active Logins

Purpose	This procedure allows you to view active CTC logins, retrieve the last activity time, and terminate all current logins.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher for viewing; Superuser for session termination

1. In node view, click the **Provisioning > Security > Active Logins** tabs. The Active Logins subtab 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

2. Click **Logout** to end the session of every logged-in user. This will log out all current users, excluding the initiating Superuser.
3. Click **Retrieve Last Activity Time** to display the most recent activity date and time for users in the Last Activity Time field.
4. Return to your originating procedure (NTP).

DLP-D107 Preprovision an SFP or XFP Device

Purpose	This procedure preprovisions Small Form-factor Pluggables (SFPs/XFPs) on the MRC-12, MRC-2.5G-12, and STM64-XFP cards. The SFPs/XFPs are referred to as pluggable port modules (PPMs) in CTC. Cisco-approved STM-1, STM-4, STM-16, STM-64, and multirate PPMs are compatible with the ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note: Before you install SFPs on the MRC-12 or MRC-2.5G-12 card, refer to the card information in "Optical Cards" chapter of the *Cisco ONS 15454 SDH Reference Manual* for bandwidth restrictions based on the port where you install the SFP and the cross-connect card being used.

Note: If you preprovision a multirate SFP, you must next select the line rate using the "DLP-D132 Provision a Multirate PPM on the MRC-12 and MRC-2.5G-12 Cards" task.

1. In node view, click the **Alarms** tab:
    1. Verify that the alarm filter is not turned on. See the [[ONS 15454 SDH Procedure Guide R8.5.1 -- DLPs D200 to D299#"DLP-D227 Disable Alarm Filtering" task on page 19-26 as necessary.
    2. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.
    3. Complete the "DLP-D147 Export CTC Data" task to export alarm and condition information.
2. In node view, double-click the card where you want to provision PPM settings.
3. Click the **Provisioning > Pluggable Port Modules**tabs.
4. In the Pluggable Port Modules area, click **Create**. The Create PPM dialog box appears.
5. In the Create PPM dialog box, complete the following:
    - PPM-Choose the slot number where you want to preprovision the SFP/XFP from the drop-down list.
    - PPM Type-Choose the number of ports supported by your SFP/XFP from the drop-down list. If only one port is supported, PPM (1 port) is the only option.
6. Click **OK**. The newly created port appears in the Pluggable Port Modules area. The row in the Pluggable Port Modules area turns light blue and the Actual Equipment Type column lists the preprovisioned PPM as unknown until the actual SFP/XFP is installed. After the SFP/XFP is installed, the row turns white and the column lists the equipment name.
7. Verify that the PPM appears on the list in the Pluggable Port Modules area. If it does not, repeat Steps 4 through 6.
8. On the Provisioning tab, click the **Line** subtab. If applicable for the PPM you are preprovisioning, use the **Reach** and **Wavelength** columns to configure these parameters as needed.

    Note: Only the parameters that are editable for the PPMs on a particular platform type are provisionable. For example, some platforms may not have PPMs with configurable wavelengths or reaches. In this case, wavelength and reach are not provisionable.

9. Repeat the task to create a second PPM.
10. Click **OK**.
11. When you are ready to install the SFP/XFP, complete the "DLP-D335 Install GBIC or SFP/XFP Devices" task.
12. Return to your originating procedure (NTP).

DLP-D108 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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: For the default values and domains of user-provisionable card settings, refer to the "Network Element Defaults" appendix in the *Cisco ONS 15454 SDH Reference Manual*.

1. In node view, double-click the STM-N card where you want to change the line settings.
2. Click the **Provisioning > Line** tabs.
3. Modify any of the settings listed in Table 18.
4. Click **Apply**.

Table 18-1: STM-N Card Line Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 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) • 1 to 12 (MRC-12, MRC-2.5G-12)
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.
Port Rate	(Display only) (MRC-12, MRC-2.5G-12, and STM64-XFP cards only) Displays the port rate set for the PPM.	• STM-1 • STM-4 • STM-16 • STM-64 (STM64-XFP only)
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	(Display only) If checked, the card is provisioned as a network element (NE) 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 (SSMs) (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
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 administrative 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. **Note:** CTC will not allow you to change a port service state from Unlocked-enabled to Locked-enabled,disabled. You must first change a port to the Locked-enabled,maintenance service state before putting it in the Locked-enabled,disabled service state.
Service State	(Display only) 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
ALS Mode	Sets the automatic laser shutdown function.	• Disabled • Auto Restart • Manual Restart • Manual Restart for Test
Reach	(Does not apply to all cards) Allows you to provision the reach value. You can also choose Auto Provision, which allows the system to automatically provision the reach from the PPM reach value on the hardware.	The options that appear in the drop-down list depend on the card: • SR (short reach, up to 2 km distance) • SR-1 (up to 2 km distance) • IR-1 (intermediate reach, up to 15 km distance) • IR-2 (up to 40 km distance) • LR-1 (long reach, up to 40 km distance) • LR-2 (up to 80 km distance) • LR-3 (up to 80 km distance)
Wavelength	(Does not apply to all cards) Allows you to provision the wavelength frequency.	• First Tunable Wavelength • 1310 nm • 1550 nm • 1470 nm • 1490 nm • 1510 nm • 1530 nm • 1570 nm • 1590 nm • 1610 nm

5. Return to your originating procedure (NTP).

DLP-D109 Change Optics Thresholds Settings for STM-64, MRC-12, and MRC-2.5G-12 Cards

Purpose	This task changes the optics thresholds settings for STM-64, MRC-12, and MRC-2.5G-12 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click the card where you want to change the optics settings.
2. Click the **Provisioning > Optics Thresholds** tabs.
3. Modify any of the settings described in Table 18-2 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

Table 18-2: Optics Thresholds Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 1 (STM-64, STM64-XFP) • 1-12 (MRC_12, MRC-2.5G-12)
LBC-LOW	Laser bias current-minimum.	Default (15 min/1 day): 50 percent
LBC-HIGH	Laser bias current-maximum.	Default (15 min/1 day): 150 percent
OPT-LOW	Optical power transmitted-minimum.	Default (15 min/1 day): 80 percent
OPT-HIGH	Optical power transmitted-maximum.	Default (15 min/1 day): 120 percent
OPR-LOW	Optical power received-minimum.	Default (15 min/1 day): 50 percent
OPR-HIGH	Optical power received-maximum.	Default (15 min/1 day): 200 percent
Set OPR	Setting the optical power received establishes the received power level as 100 percent. If the receiver power decreases, then the OPR percentage decreases to reflect the loss in receiver power. For example, if the receiver power decreases by 3 dBm, the OPR decreases 50 percent.	Click **SET**.
Types	Sets the type of alert that occurs when a threshold is crossed. To change the type of threshold, choose one and click **Refresh**.	• TCA (threshold cross alert) • Alarm
Intervals	Sets the time interval for collecting parameter counts. To change the time interval, choose the desired interval and click **Refresh**.	• 15 Min

		• 1 Day

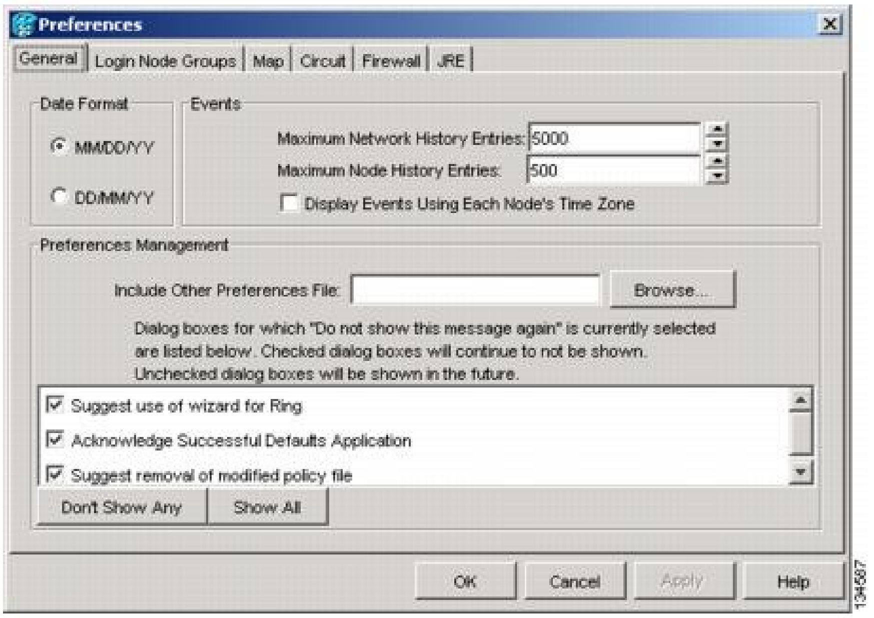
4. Click **Apply**.
5. Return to your originating procedure (NTP).

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

1. From the Edit menu, choose **Preferences**.
   The CTC Preferences dialog box appears (Figure 18-4).

Figure 18-4: CTC Preferences Dialog Box



● MM/DD/YY
○ DD/MM/YY

Maximum Network History Entries: 5000
Maximum Node History Entries: 500
□ Display Events Using Each Node's Time Zone

Include Other Preferences File:

Dialog boxes for which "Do not show this message again" is currently selected are listed below. Checked dialog boxes will continue to not be shown. Unchecked dialog boxes will be shown in the future.

☑ Suggest use of wizard for Ring
☑ Acknowledge Successful Defaults Application
☑ Suggest removal of modified policy file

2. Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.
3. Click **Apply** and **OK**.

   Note: Setting the Maximum History Entries value to the high end of the range uses more 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.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

   The CTC Preferences dialog box appears (Figure 18-4).
2. Check the **Display Events Using Each Node's Time Zone** check box. The Apply button is enabled.
3. Click **Apply** and **OK**.
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	D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. At the card, node, or network view, click the **Alarms** tab.
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.
3. Return to your originating procedure (NTP).

DLP-D114 View Conditions

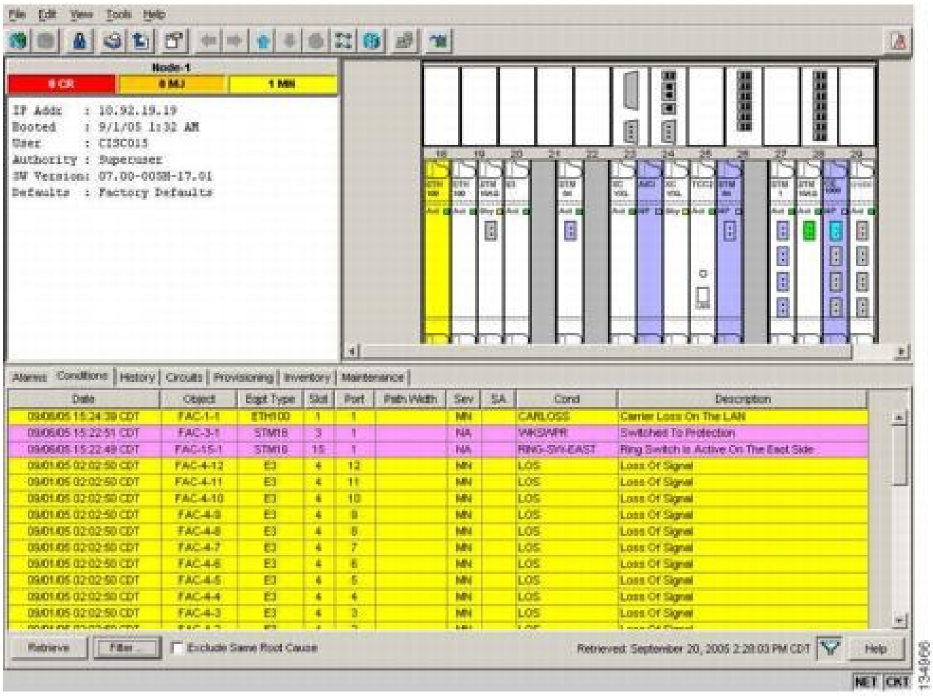
Purpose	Use this task to view conditions [events with a Not Reported (NR) severity] at the card, node, or network level. The Conditions tab gives you a clear record of changes or events that do not result in alarms.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed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

Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. From card, node, or network view, click the **Conditions** tab.
2. Click **Retrieve** (Figure 18-5).

   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 18-5: Node View Conditions Window



```
IP Addr   : 10.92.19.19
Booted    : 9/1/05 1:32 AM
User      : CISCO15
Authority : Superuser
SW Version: 07.00-00SH-17.01
Defaults  : Factory Defaults
```

Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	SA	Cond	Description
09/06/05 15:24:39 CDT	FAC-1-1	ETH100	1	1		MN		CARLOSS	Carrier Loss On The LAN
09/06/05 15:22:51 CDT	FAC-3-1	STM16	3	1		NA		WKSWPR	Switched To Protection
09/06/05 15:22:49 CDT	FAC-15-1	STM16	15	1		NA		RING-SW-EAST	Ring Switch Is Active On The East Side
09/01/05 02:02:50 CDT	FAC-4-12	E3	4	12		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-11	E3	4	11		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-10	E3	4	10		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-9	E3	4	9		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-8	E3	4	8		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-7	E3	4	7		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-6	E3	4	6		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-5	E3	4	5		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-4	E3	4	4		MN		LOS	Loss Of Signal
09/01/05 02:02:50 CDT	FAC-4-3	E3	4	3		MN		LOS	Loss Of Signal

□ Exclude Same Root Cause

Retrieved: September 20, 2005 2:28:03 PM CDT

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 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.

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.

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.

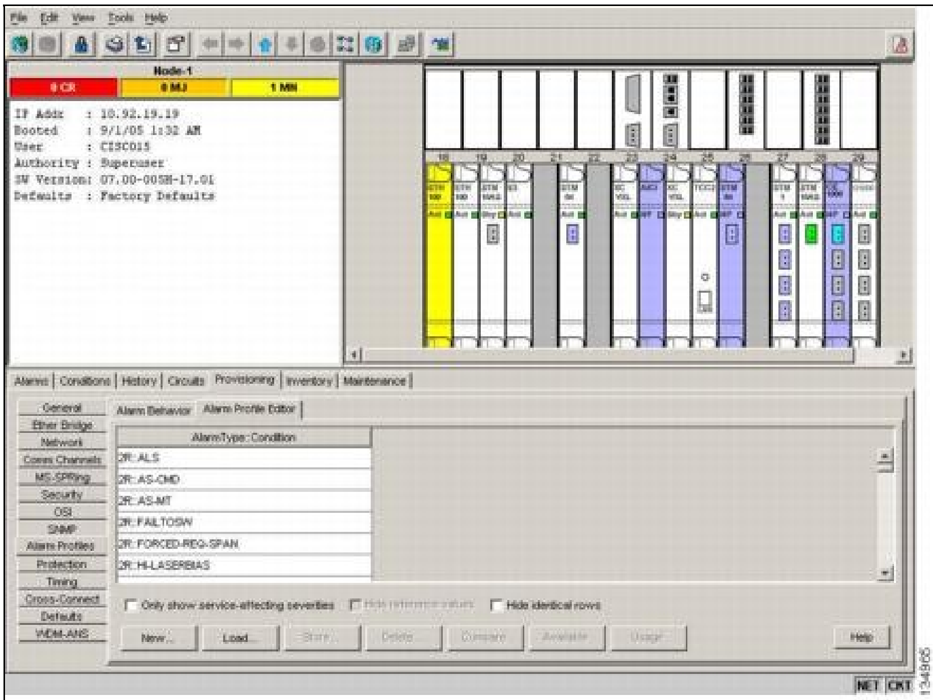
4. Return to your originating procedure (NTP).

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	NTP-D425 Create a New or Cloned Alarm Severity Profile DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tab (Figure 18-6).

Figure 18-6: Node View Alarm Profile



```
IP Addr    : 10.92.19.19
Booted     : 9/1/05 1:32 AM
User       : CISCO15
Authority  : Superuser
SW Version: 07.00-005H-17.01
Defaults   : Factory Defaults
```

AlarmType::Condition
2R: ALS
2R: AS-CMD
2R: AS-MT
2R: FAILTOSW
2R: FORCED-REQ-SPAN
2R: HI-LASERBIAS

□ Only show service-affecting severities □ Hide reference values □ Hide identical rows

2. To apply profiles to a card:
    1. Click the Profile row for the card.
    2. Choose the new profile from the drop-down list.
    3. Click **Apply**.
3. To apply the profile to an entire node:
    1. Click the **Node Profile** drop-down arrow at the bottom of the window (Figure 18-6).
    2. Choose the new alarm profile from the drop-down list.
    3. Click **Apply**.

4. To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. Enable Intermediate Path Performance Monitoring as specified in DLP-D122 Enable Intermediate Path Performance Monitoring
2. In node view, double-click the STM-N card that you want to monitor. The card view appears.
   See Table 18-3 for a list of STM-N line terminating equipment (LTE) cards.

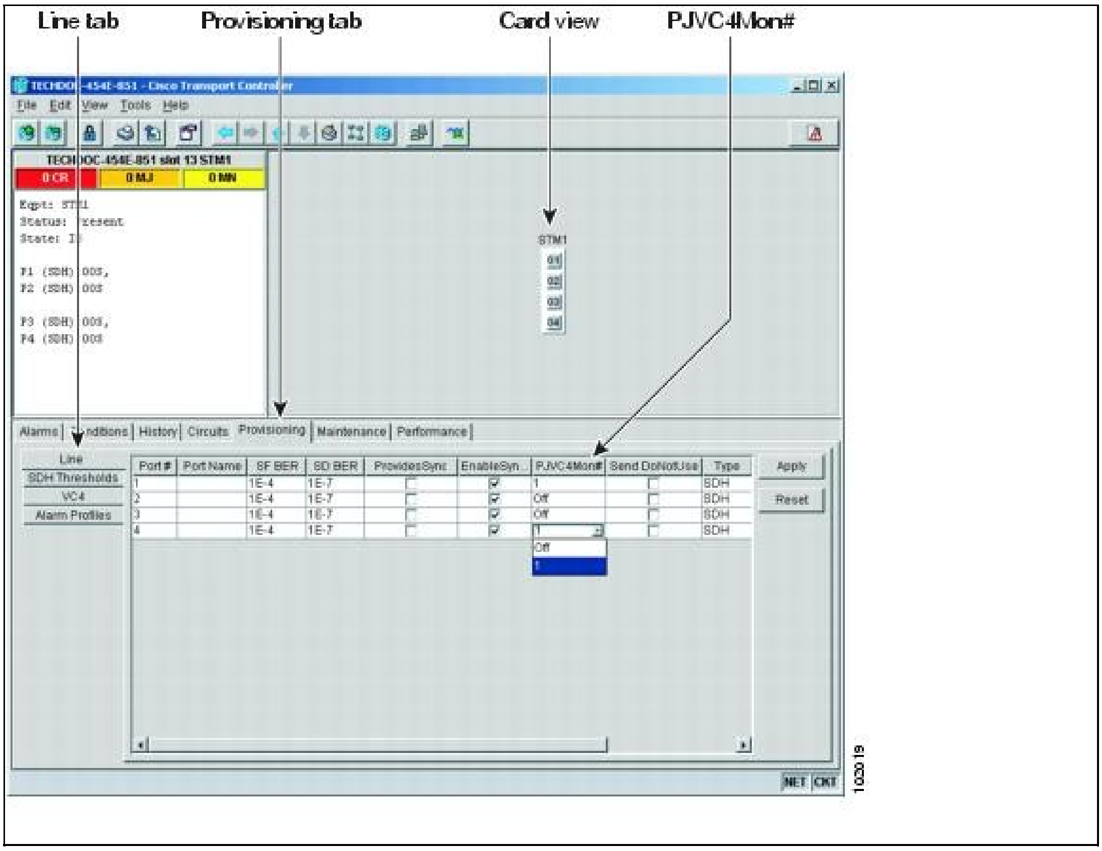
Table 18-3: Traffic Cards that Terminate the Line (LTEs)

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

3. Click the **Provisioning > Line** tabs.
4. Click the PJVC4Mon# drop-down list and make a selection based on the following rules (Figure 18-7):

   · 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 18-7: Enabling or Disabling Pointer Justification Count Parameters



Port #	Port Name	SF BER	SD BER	ProvidesSync	EnableSyn...	PJVC4Mon#	Send DoNotUse	Type
1		1E-4	1E-7	□	☑	1	□	SDH
2		1E-4	1E-7	□	☑	Off	□	SDH
3		1E-4	1E-7	□	☑	Off	□	SDH
4		1E-4	1E-7	□	☑	1	□	SDH

5. In the Service State field, confirm that the port is in the Unlocked-enabled service state.
6. 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**.
7. Click the **Performance** tab to view performance monitoring (PM) parameters. Refer to the "Performance Monitoring" chapter in 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.
8. Return to your originating procedure (NTP).

DLP-D122 Enable Intermediate Path Performance Monitoring

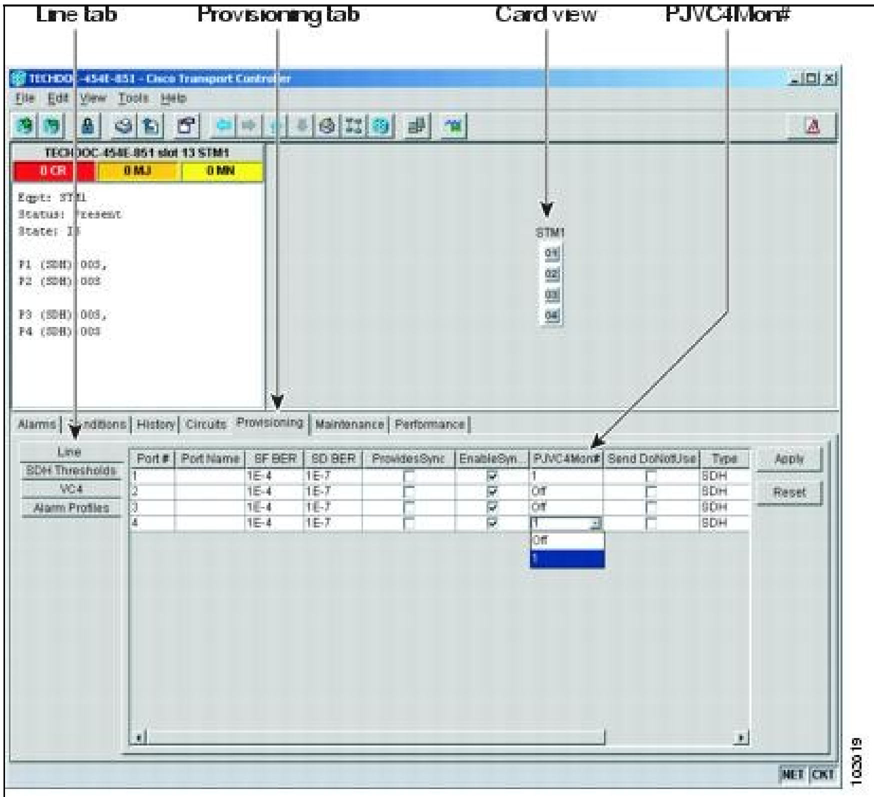
Purpose	This task enables intermediate path performance monitoring (IPPM), which allows you to monitor large amounts of VC4 traffic through intermediate nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level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

1. In node view, double-click the STM-N card you want to monitor. The card view appears.
   See Table 18-3 for a list of STM-N LTE cards.
2. Click the **Provisioning > VC4** tabs (Figure 18-8).

Figure 18-8: VC4 Tab for Enabling or Disabling IPPM



Eqpt: STM1
Status: Present
State: IS

P1 (SDH) 003,
P2 (SDH) 003

P3 (SDH) 003,
P4 (SDH) 003

Port #	Port Name	SF BER	SD BER	ProvidesSync	EnableSyn...	PJVC4Mon#	Send DoNotUse	Type
1		1E-4	1E-7	□	☑	1	□	SDH
2		1E-4	1E-7	□	☑	Off	□	SDH
3		1E-4	1E-7	□	☑	Off	□	SDH
4		1E-4	1E-7	□	☑	1	□	SDH

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.
4. Click **Apply**.
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*.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

2. Click the **Performance** tab.
3. Click the **15 min** radio button.
4. Click **Refresh**. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.
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.
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.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. Click the **1 day** radio button.
4. Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.
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.
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.
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

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

1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. Click the **Near End** radio button.
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*.
5. View the Curr column to find PM counts for the current time interval.
6. View the Prev-*n* columns to find PM counts for the previous time intervals.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. Click the **Far End** radio button.
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 "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.
5. View the Curr column to find PM counts for the current time interval.
6. View the Prev-*n* columns to find PM counts for the previous time intervals.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. Click **Baseline**.

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.

4. View the current statistics columns to observe changes to PM counts for the current time interval.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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.
2. Click the **Circuits** tab.
3. If you are in node or card view, choose the scope for the search (**Network** or **Node**) in the Scope drop-down list.
4. Click **Search**.
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.
6. Click **Find Next**. If a match is found, click **Find Next** again to find the next circuit.
7. Repeat Steps 5 and 6 until you are finished, then click **Cancel**.
8. Return to your originating procedure (NTP).

DLP-D132 Provision a Multirate PPM on the MRC-12 and MRC-2.5G-12 Cards

Purpose	This task provisions PPMs for the MRC-12 and MRC-2.5G-12 cards. Single-rate SFPs do not require provisioning.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Provisioning or higher

1. In node view, double-click the MRC-12 or MRC-2.5G-12 card where you want to provision PPM settings.
2. Click the **Provisioning** > Pluggable Port Modules **tabs.**
3. In the Pluggable Port Modules area, click **Create**. The Create PPM dialog box appears.
4. In the Create PPM dialog box, complete the following:
   - PPM-Choose the slot number where the SFP is installed from the drop-down list.
   - PPM Type-Choose the number of ports supported by your SFP from the drop-down list. If only one port is supported, PPM (1 port) is the only option.
5. Click **OK**. The newly created port appears in the Pluggable Port Modules are. The row in the Pluggable Port Modules are turns light blue and the Actual Equipment Type column lists the equipment name.
6. Verify that the PPM appears in the list in the Pluggable Port Modules area. If it does not, repeat Steps 4 through 5.
7. Repeat the task to provision a second PPM.
8. Click **OK**.
9. Continue with the "DLP-D133 Provision the Optical Line Rate on the MRC-12 and MRC-2.5G-12 Cards" task to provision the line rate.
10. Return to your originating procedure (NTP).

DLP-D133 Provision the Optical Line Rate on the MRC-12 and MRC-2.5G-12 Cards

Purpose	This task provisions the optical line rate on a multirate PPM. Single-rate SFPs do not require line rate provisioning.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click the MRC-12 or MRC-2.5G-12 card where you want to provision PPM settings.
2. Click the **Provisioning > Pluggable Port Modules** tabs.
3. In the Pluggable Ports area, click **Create**. The Create Port dialog box appears.
4. In the Create Port dialog box, complete the following:
   - Port-Click the PPM number and port number from the drop-down list. The first number indicates the PPM and the second number indicates the port number on the PPM. For example, the first PPM displays as 1-1 and the second PPM displays as 2-1.
   - Port Type-Click the type of port from the drop-down list. The port type list displays the supported port rates on your PPM. See Table 18-4 for definitions of the supported rates on the MRC-12 and MRC-2.5G-12 cards.

Table 18-4: PPM Port Types

Card	Port Type
MRC-12 MRC-2.5G-12	• STM-1-155 Mbps • STM-4-622 Mbps* STM-16-2.48 Gbps

5. Click **OK**.
6. Repeat Steps 3 through 5 to configure the port rates as needed.
7. Click **OK**. The row in the Pluggable Ports area turns light blue until the actual SFP is installed and then the row turns white.
8. Return to your originating procedure (NTP).

DLP-D134 Change the Optical Line Rate on the MRC-12 and MRC-2.5G-12 Cards

Purpose	This task changes the optical line rate on a multirate PPM. Perform this task if you want to change the port rate on a multirate SFP that is already provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, double-click the MRC-12 or MRC-2.5G-12 card where you want to provision PPM settings.
2. Click the **Provisioning** > Pluggable Port Modules **tabs.**
3. Click the port with the port rate you want to change in the Pluggable Ports area. The highlight changes to dark blue.
4. Click **Edit**. The Edit Port Rate dialog box appears.
5. In the Change To field, use the drop-down list to select the new port rate and click **OK**.
6. Click **Yes** in the Confirm Port Rate Change dialog box.
7. Return to your originating procedure (NTP).

DLP-D135 Delete a PPM from the MRC-12, MRC-2.5G-12, or STM64-XFP Card

Purpose	This task deletes PPM provisioning for SFPs on the MRC-12, MRC-2.5G-12, or STM64-XFP card.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. Determine if the PPM can be deleted.

   You cannot delete a port on a PPM if it is in service, part of a protection group, has a communications channel termination in use, is used as a timing source, has circuits, or has overhead circuits. As needed, complete the following procedures and tasks:

   - DLP-D150 Modify a 1:1 Protection Group
   - NTP-D85 Change Node Timing
   - NTP-D277 Modify or Delete Communications Channel Terminations
   - NTP-D287 Modify and Delete Circuits
   - NTP-D288 Modify and Delete Overhead Circuits and Server Trails
   - DLP-D214 Change the Service State for a Port

2. In node view, double-click the MRC-1,2, MRC-2.5G-12, or STM64-XFP card where you want to delete PPM settings.
3. Click the **Provisioning > Pluggable Port Modules** tabs.
4. To delete a PPM and the associated ports:
   1. Click the PPM line that appears in the Pluggable Port Modules area. The highlight changes to dark blue.
   2. Click **Delete**. The Delete PPM dialog box appears.
   3. Click **Yes**. The PPM provisioning is removed from the Pluggable Port Modules area and the Pluggable Ports area.
5. Verify that the PPM provisioning is deleted:

   · If the PPM was preprovisioned, CTC shows an empty slot in CTC after it is deleted.
   · If the SFP (PPM) is physically present when you delete the PPM provisioning, CTC transitions to the deleted state; the ports (if any) are deleted, and the PPM is represented as a gray graphic in CTC. The SFP can be provisioned again in CTC or the equipment can be removed, in which case the removal causes the graphic to disappear.
6. If you need to remove the SFP, see the "DLP-D336 Remove GBIC or SFP/XFP Device" task.
7. Return to your originating procedure (NTP).

DLP-D136 Provision CE-100T-8 and CE-MR-10 Ethernet Ports

Purpose	This task provisions CE-100T-8 and CE-MR-10 Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: You can provision SONET contiguous concatenated (CCAT) or VCAT circuits for the CE-100T-8 and CE-MR-10 cards before or after provisioning the card's Ethernet ports and/or packet-over-SDH (POS) ports. See the NTP-D323 Create an Automatically Routed High-Order Circuit or the NTP-D283 Create an Automatically Routed VCAT Circuit, as needed.

1. In node view, double-click the CE-100T-8 or CE-MR-10 card graphic to open the card.
2. Click the **Provisioning > Ether Ports** tabs.
3. For each CE-100T-8 or CE-MR-10 port, provision the following parameters:
   ♦ Port Name-If you want to label the port, enter the port name.
   Note: Circuit table displays port name of the POS port and not the Ethernet port.
   ♦ Admin State-Choose **Unlocked** to put the port in service.
   ♦ Expected Speed-Choose the expected speed of the device that is or will be attached to the Ethernet port. If you know the speed, choose 100 Mbps or 10 Mbps (for CE-100T-8), or 1000 Mbps, 100 Mbps, or 10 Mbps (for CE-MR-10) to match the attached device. If you do not know the speed, choosing **Auto** enables autonegotiation for the speed of the port, and the CE-100T-8 or CE-MR-10 port will attempt to negotiate a mutually acceptable speed with the attached device. If the expected speed is set to **Auto**, you cannot enable selective autonegotiation.
   ♦ Expected Duplex-Choose the expected duplex of the device that is or will be attached to the Ethernet port. If you know the duplex, choose **Full** or **Half** to match the attached device. If you do not know the duplex, choosing **Auto** enables autonegotiation for the duplex of the port, and the CE-100T-8 or CE-MR-10 port will attempt to negotiate a mutually acceptable

duplex with the attached device. If the expected duplex is set to **Auto**, you cannot enable selective autonegotiation.

- ♦ Enable Selective Auto Negotiation-Click this check box to enable selective autonegotiation on the Ethernet port. If you do not want to enable selective autonegotiation, uncheck the box. If checked, the CE-100T-8 or CE-MR-10 port attempts to autonegotiate only to the selected expected speed and duplex. The link will come up if both the expected speed and duplex of the attached autonegotiating device matches that of the port. You cannot enable selective autonegotiation if either the expected speed or expected duplex is set to **Auto**.
- ♦ Enable Flow Control-Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The CE-100T-8 or CE-MR-10 card attempts to negotiate symmetrical flow control with the attached device.
- ♦ 802.1Q VLAN CoS-For a class-of-service (CoS)-tagged frame, the CE-100T-8 or CE-MR-10 card can map the eight priorities specified in CoS for either priority or best effort treatment. Any CoS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the CoS is set to 7, which is the highest CoS value. The default results in all traffic being treated as best effort.
- ♦ IP ToS-The CE-100T-8 or CE-MR-10 card can also map any of the 256 priorities specified in IP type of service (ToS) to either priority or best effort treatment. Any ToS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the ToS is set to 255, which is the highest ToS value. This results in all traffic being sent to the best effort queue by default.
  Note: Untagged traffic is treated as best effort.
  Note: If traffic is tagged with both CoS and IP ToS, then the CoS value is used, unless the CoS value is 7.

4. Click **Apply**.
5. Refresh the Ethernet statistics:
   1. Click the **Performance > Ether Ports > Statistics** tabs.
   2. Click **Refresh**.
      Note: Reprovisioning an Ethernet port on the CE-100T-8 or CE-MR-10 card does not reset the Ethernet statistics for that port.
6. 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 that you want to monitor must be on STM-N cards capable of receiving path trace. See Table 19-5 for a list of applicable cards.
Prerequisite Procedures	DLP-D264 Provision a J1 Path Trace on Circuit Source and Destination Ports DLP-D60 Log into CTC
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.

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

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.
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 19-5. If not, the Edit Path Trace menu item does not appear.
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.
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.
8. Click **Apply**, then click **Close**.
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
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.

1. In node view, click the **Provisioning > General** tabs.
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 for detailed field descriptions.

3. Click **Apply**. Confirm that the changes appear; if not, repeat the task.
4. Return to your originating procedure (NTP).

DLP-D141 Provision CE-100T-8, CE-1000-4, and CE-MR-10 POS Ports

Purpose	This task provisions CE-100T-8, CE-1000-4, or CE-MR-10 POS ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: You can provision SONET CCAT or VCAT circuits for the CE-100T-8, CE-1000-4, or CE-MR-10 card before or after provisioning the card's Ethernet and/or POS ports. See the NTP-D323 Create an Automatically Routed High-Order Circuit or the NTP-D283 Create an Automatically Routed VCAT Circuit, as needed.

1. In node view, double-click the CE-100T-8, CE-1000-4, or CE-MR-10 card graphic to open the card.
2. Click the **Provisioning > POS Ports**tabs.
3. For each CE-100T-8, CE-1000-4, or CE-MR-10 port, provision the following parameters:
    - Port Name-If you want to label the port, enter the port name.
      Note: Circuit table displays port name of the POS port and not the Ethernet port.
    - Admin State-Choose **Unlocked** to put the port in service.
    - Framing Type-Choose **GPF-F POS** framing (the default) or **HDLC POS** framing. The framing type needs to match the framing type of the POS device at the end of the SONET circuit.
    - Encap CRC-With GFP-F framing, the user can configure a 32-bit cyclic redundancy check (CRC) (the default) or none (no CRC). HDLC framing provides a set 32-bit CRC. The CRC should be set to match the CRC of the POS device on the end of the SONET circuit.
      Note: For more details about the interoperability of ONS Ethernet cards, including information on encapsulation, framing, and CRC, refer to the "POS on ONS Ethernet Cards" chapter of the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
      Note: The CE-Series cards use LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.
4. Click **Apply**.
5. Refresh the POS statistics:
    1. Click the **Performance > POS Ports > Statistics** tabs.
    2. Click **Refresh**.
6. 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

	DLP-D65 Create a Static Route
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning** > **Network** tabs.
2. Click the **Static Routing** tab.
3. Click the static route you want to edit.
4. Click **Edit.**
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 for detailed field descriptions.
6. Click **OK**.
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 DLP-D65 Create a Static Route
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning** > **Network** > **Static Routing** tabs.
2. Click the static route you want to delete.
3. Click **Delete**. A confirmation dialog box appears.
4. Click **Yes**.
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
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.

1. In node view, click the **Provisioning** > **Network** > **OSPF** tabs. The OSPF subtab has several options.
2. In the OSPF on LAN area, uncheck the **OSPF active on LAN?** check box.
3. Click **Apply**.
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
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.

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

DLP-D146 Print CTC Data

Purpose	This task prints CTC card, node, or network data in graphical or tabular form on a Windows-provisioned printer.
Tools/Equipment	Printer connected to the CTC computer by a direct or network connection.
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. Click the tab (and subtab, if present) containing the information you want to print. For example, click the **Alarms** tab to print Alarms window data.

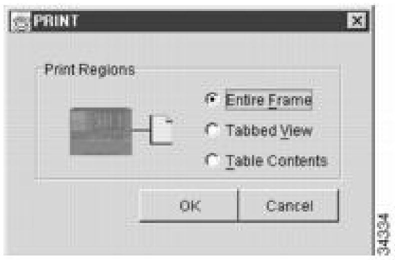
   The print operation is available for all network, node, and card view windows.
2. From the File menu choose **Print**.
3. In the Print dialog box, click a a printing option (Figure 18-9).
   - Entire Frame-Prints the entire CTC window including the graphical view of the card, node, or network. This option is available for all windows.
   - Tabbed View-Prints the lower half of the CTC window containing tabs and data. The printout includes the selected tab (on top) and the data shown in the tab window. For example, if you print the History window Tabbed View, you print only history items appearing in the window. This option is available for all windows.

- Table Contents-Prints CTC data in table format without graphical representations of shelves, cards, or tabs. This option does not apply to:
    - Provisioning > General > General, Multishelf Config, and Power Monitor windows
    - Provisioning > Network > General window
    - Provisioning > Security > Policy, Access, and Legal Disclaimer windows
    - Provisioning > SNMP window
    - Provisioning > Timing > General and BITS Facilities windows
    - Provisioning > OSI > Main Setup window
    - Provisioning > OSI > TARP > Config window
    - Provisioning > Cross-Connect window
    - Provisioning > Comm Channels > LMP > General window
    - Provisioning > WDM-ANS > Node Setup window
    - Maintenance > Cross-Connect > Cards window
    - Maintenance > Database window
    - Maintenance > Diagnostic window
    - Maintenance > Protection window
    - Maintenance > Timing > Source window
    - Maintenance > DWDM > ROADM Power Monitoring window

      The Table Contents option prints all the data contained in a table and the table column headings. For example, if you print the History window Table Contents view, you print all data included in the table whether or not items appear in the window.

  Tip: When you print using the Tabbed View option, it can be difficult to distinguish whether the printout applies to the network, node, or card view. To determine the view, compare the tabs on the printout. The network, node, and card views are identical except that the network view does not contain an Inventory tab or a Performance tab.

Figure 18-9: Selecting CTC Data For Print



4. Click **OK**.
5. In the Windows Print dialog box, click a printer and click **OK**.
6. Repeat this task for each window that you want to print.
7. Return to your originating procedure (NTP).

DLP-D147 Export CTC Data

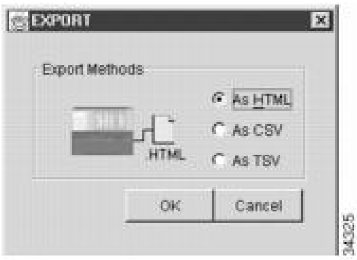
Purpose	This task exports CTC table data as delineated text to view or edit the data in text editor, word processing, spreadsheet, database management, or web browser applications. You can also export data from the Edit Circuits window.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
	As needed

Required/As Needed	
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. Click the tab containing the information you want to export (for example, the Alarms tab or the Circuits tab).
2. If you want to export detailed circuit information, complete the following:
    1. In the Circuits window, choose a circuit and click **Edit** to open it in the Edit Circuits window.
    2. In the Edit Circuits window, choose the desired tab: **Drops**, **SNCP Selectors**, **SNCP Switch Counts**, **State**, or **Merge**.

        Note: Depending upon your configuration, you may or may not see all of the above tabs when you click Edit.
3. Choose **Export** from the File menu.
4. In the Export dialog box, click a data format (Figure 18-10):
    - **As HTML**-Saves data as a simple HTML table file without graphics. The file must be viewed or edited with applications such as Netscape Navigator, Microsoft Internet Explorer, or another application capable of opening HTML files.
    - **As CSV**-Saves the CTC table as comma-separated values (CSV). This option does not apply to the Maintenance > Timing > Report window.
    - **As TSV**-Saves the CTC table as tab-separated values (TSV).

Figure 18-10: Selecting CTC Data For Export



Export Methods

● As HTML
○ As CSV
○ As TSV

OK
Cancel

5. If you want to open a file in a text editor or word processor application, procedures vary. Typically, you can use the File > Open command to view the CTC data, or you can double-click the file name and choose an application such as Notepad.

    Text editor and word processor applications format the data exactly as it is exported, including comma or tab separators. All applications that open the data files allow you to format the data.
6. If you want to open the file in spreadsheet and database management applications, procedures vary. Typically, you need to open the application, choose File > Import, and then choose a delimited file to format the data in cells.

    Spreadsheet and database management programs also allow you to manage the exported data.
    Note: An exported file cannot be opened in CTC.
    The export operation does not to apply to:

    · Provisioning > General > General, Multishelf Config, and Power Monitor windows
    · Provisioning > Network > General window
    · Provisioning > Security > Policy, Access, and Legal Disclaimer windows

· Provisioning > SNMP window
· Provisioning > Timing > General and BITS Facilities windows
· Provisioning > OSI > Main Setup window
· Provisioning > OSI > TARP > Config window
· Provisioning > Cross-Connect window
· Provisioning > Comm Channels > LMP > General window
· Provisioning > WDM-ANS > Node Setup window
· Maintenance > Cross-Connect > Cards window
· Maintenance > Database window
· Maintenance > Diagnostic window
· Maintenance > Protection window
· Maintenance > Timing > Source window
· Maintenance > DWDM > ROADM Power Monitoring window

7. Click **OK**.
8. In the Save dialog box, enter a name in the File name field using one of the following formats:

   · *Filename*.html for HTML files
   · *Filename*.csv for CSV files
   · *Filename*.tsv for TSV files
9. Navigate to a directory where you want to store the file.
10. Click **OK**.
11. Repeat the task for each window that you want to export.
12. 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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

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-D345 Edit Network Element Defaults to change NE default values.

1. From the View menu, choose **Go to Network View**.
2. Right-click the network map and choose **Create New Domain** from the shortcut menu.
3. When the domain icon appears on the map, click the map name and type the domain name.
4. Press **Enter**.
5. To add nodes to the domain, continue with the "DLP-D149 Manage Domain Icons" task.
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 DLP-D148 Create Domain Icons
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.

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-D345 Edit Network Element Defaults to change NE default values.

1. From the View menu, choose **Go to Network View**.
2. Locate the domain action you want in Table 18-5 and complete the appropriate steps.

Table 18-5: 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.

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 (E3-12 and DS3i-N-12) cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-D71 Create a 1:1 Protection Group DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning** > **Protection** tabs.
2. In the Protection Groups area, click the 1:1 protection group you want to modify.
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.
4. Click **Apply**. Confirm that the changes appear; if not, repeat the task.

    Note: To convert 1:1 protection groups, see the NTP-D91 DS3 i-N-12 Protect Cards from 1:1 Protection to 1:N Protection.
5. Return to your originating procedure (NTP).

DLP-D151 Set Up SNMP for a GNE

Purpose	This procedure provisions Simple Network Management Protocol (SNMP) parameters so that you can use SNMP network management software with the ONS 15454 SDH.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

1. In node view, click the Provisioning > SNMP tabs.
2. In the Trap Destinations area, click Create.
3. In the Create SNMP Trap Destination dialog box, complete the following fields:
    - Destination IP Address-Enter the IP address of your network management system (NMS).
    - Community-Enter the SNMP community name. (For more information about SNMP, refer to the "SNMP" chapter in the *Cisco ONS 15454 SDH Reference Manual.*)

      Note: The community name is a form of authentication and access control. The community name assigned to the ONS 15454 SDH is case-sensitive and must match the community name of the NMS.

- UDP Port-The default User Datagram Protocol (UDP) port for SNMP traps is 162.
- Trap Version-Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

4. Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.
5. Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.
6. If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.
7. If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the '*Enable SNMP Proxy* check box on the SNMP tab.
8. If you want to allow using generic SNMP MIBs, check the **Use Generic MIB** check box.

   Note: The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.

   For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15454 SDH Reference Manual*.
9. Click **Apply**.
10. Return to your originating procedure (NTP).

DLP-D152 Modify a 1:N Protection Group

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

1. Verify that the DS3i-N-12 cards are installed according to the 1:N specifications in the "DLP-D72 Create a 1:N Protection Group" task.
2. In node view, click the **Provisioning** > **Protection** tabs.
3. In the Protection Groups area, click the 1:N protection group you want to modify.
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 for field descriptions.
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 DS3 i-N-12 Protect Cards from 1:1 Protection to 1:N Protection.
6. Return to your originating procedure (NTP).

DLP-D153 Set Up SNMP for an ENE

Purpose	This procedure provisions the SNMP parameters for an ONS 15454 SDH configured to be an ENE if you use SNMP proxy on the GNE.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > SNMP** tabs.
2. In the Trap Destinations area, click **Create**.
3. In the Create SNMP Trap Destination dialog box, complete the following fields:
    - Destination IP Address-Enter the IP address of your NMS.
    - Community-Enter the SNMP community name. (For more information about SNMP, refer to the "SNMP" chapter in the *Cisco ONS 15454 SDH Reference Manual*.)
      Note: The community name is a form of authentication and access control. The community name assigned to the ONS 15454 SDH is case-sensitive and must match the community name of the NMS.
    - UDP Port-The default UDP port for SNMP traps is 162.
    - Trap Version-Choose either SNMPv1 or SNMPv2. Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.
4. Click **OK**. The node IP address of the node where you provisioned the new trap destination appears in the Trap Destinations area.
5. Click the node IP address in the Trap Destinations area. Verify the SNMP information that appears in the Selected Destination list.
6. If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.
7. If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across ONS firewalls, click the **Enable SNMP Proxy** check box on the SNMP tab.

    Note: The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.
    For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15454 SDH Reference Manual*.
8. Click **Apply**.
9. If you are setting up SNMP proxies, you can set up to three relays for each trap address to convey SNMP traps from the NE to the NMS. To do this, complete the following substeps:
    1. Click the first trap destination IP address. The address and its community name appear in the Destination fields.
    2. If the node you are logged into is an ENE, set the Relay A address to the GNE and type its community name in the community field. If there are NEs between the GNE and ENE, you can enter up to two SNMP proxy relay addresses and community names in the fields for Relay and Relay C. When doing this, consult the following guidelines:
        - ◊ If the NE is directly connected to the GNE, enter the address and community name of the GNE for Relay A.
        - ◊ If this NE is connected to the GNE through other NEs, enter the address and community name of the GNE for Relay A and the address and community name of NE 1 for Relay B and NE 2 for Relay C.
          The SNMP proxy directs SNMP traps in the following general order:

ENE > RELAY A > RELAY B > RELAY C > NMS

For example:

◊ If there is are 0 intermediate relays, the order is ENE > RELAY A (GNE) > NMS

◊ If there is 1 intermediate relay, the order is ENE > RELAY A (NE 1) > RELAY B (GNE) > NMS

◊ If there is are 0 intermediate relays, the order is ENE > RELAY A (NE 1) > RELAY B (NE 2) > RELAY C (GNE) > NMS

10. Click **Apply**.
11. Repeat Step 2 through Step 10 for all NEs between the GNE and ENE.
12. 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 DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning** > **Protection** tabs.
2. In the Protection Groups area, click the 1+1 protection group you want to modify.
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 for field descriptions.
4. Click **Apply**. Confirm that the changes appear; if not, repeat the task.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

2. In the Protection Groups area, click the protection group you want to delete.
3. Click **Delete**.
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.
5. 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
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 for descriptions of the fields mentioned in this task.

1. In node view, click the **Provisioning > Timing > General** tabs.
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
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
4. Click the **BITS Facilities** tab.
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

6. Click **Apply**.

   Note: Refer to the "Timing" chapter in the *Cisco ONS 15454 SDH Reference Manual* for timing information.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

1. In node view, click the **Provisioning** > **Security > Users** tabs.
2. Click the user whose settings you want to modify.
3. Click **Change**.
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 for fields and descriptions.
5. Click **OK**.

   Note: User settings that you changed during this task will not appear until that user logs off and logs back in.
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
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-D315 Log Out a User on a Single Node" task, 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.

1. In node view, select the **Provisioning** > **Security > Users** tabs.
2. Choose the user you want to delete.
3. Click **Delete**.
4. In the Delete User dialog box, verify that the user name displayed is the one you want to delete.
5. Click **OK**. Confirm that the changes appear; if not, repeat the task.
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
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 the user will access.

1. From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to add users.
2. Click the **Provisioning** > **Security > Users** tabs. Highlight the user's name whose settings you want to change.
3. Click **Change**. The Change User dialog box appears.
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 for field descriptions.
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).
6. Click **OK.** A Change Results confirmation dialog box appears.
7. Click **OK** to acknowledge the changes.
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
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-D316 Log Out a User on Multiple Nodes" task, 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.

1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning** > **Security > Users** tabs. Highlight the name of the user you want to delete.
3. Click **Delete**. The Delete User dialog box appears.
4. Click **OK**. A Change Results confirmation dialog box appears.
5. Click **OK** to acknowledge the changes. Confirm that the changes appear; if not, repeat the task.
6. Return to your originating procedure (NTP).

DLP-D162 Format and Enter NMS Community String for SNMP Command or Operation

Purpose	This procedure describes how to format a network management system (NMS) community string to execute the following SNMP commands for GNEs and ENEs: Get, GetBulk, GetNext, and Set.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

1. If the SNMP **Get** command (or other operation) is enabled on the ONS 15454 SDH configured as a GNE, enter the community name assigned to the GNE in community name field on the MIB browser.

   Note: The community name is a form of authentication and access control. The community name of the NMS must match the community name assigned to the ONS 15454 SDH.
2. If the SNMP **Get** command (or other operation) is enabled for the ENE through a SOCKS proxy-enabled GNE, create a formatted string to enter in the MIB browser community name field. Refer to the following examples when constructing this string for your browser:

   ◊ Formatted community string input example 1:
   `allviews{192.168.7.4,,,net7node4}`
   If "allviews" is a valid community name value at the proxy-enabled SNMP agent (the GNE), the GNE is expected to forward the PDU to 192.168.7.4 at Port 161. The outgoing PDU will have "net7node4" as the community name. This is the valid community name for the ENE with address 192.168.7.4.

   ◊ Formatted community string input example 2:
   `allviews{192.168.7.99,,,enter7{192.168.9.6,161,,net9node6}}`
   If "allviews" is a valid community name value at the proxy-enabled GNE, the GNE is expected to forward the PDU to 192.168.7.99 at the default port (Port 161) with a community name of "enter7{192.168.9.6,161,,net9node6}". The system with the address 192.168.7.99 (the NE between the GNE and the ENE) forwards this PDU to 192.168.9.6 at Port 161 (at the ENE) with a community name of "net9node6". The community name "enter7" is valid for the NE between the GNE and the ENE and "net9node6" is a valid community name for the ENE.
3. Log into the NMS where the browser is installed to retrieve the network information from the ONS 15454 SDH.
4. On this computer, go to Start and click the SNMP MIB browser application.
5. In the Host and Community areas, enter the IP address of the GNE through which the ONS 15454 SDH with the information to be retrieved can be reached.
6. In the Community area, enter the community string as explained in Step 2.
7. 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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning** > **SNMP** tabs.
2. In the Trap Destinations area, click the trap you want to delete.
3. Click **Delete**. A confirmation dialog box appears.
4. Click **Yes**. Confirm that the changes appear; if not, repeat the task.
5. Return to your originating procedure (NTP).

DLP-D165 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15454 SDH is connected to networks with third party network elements (NEs) that use the OSI protocol stack for data communications network (DCN) communication.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution! Do not complete this task until you confirm the role of the node within the network. It will be either an 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 SDH Reference Manual.*

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

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

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

1. In node view, click the **Provisioning** > **OSI > Main Setup** tabs.
2. Choose a routing mode:
   - ♦ **End System**-The ONS 15454 SDH performs OSI end system (ES) functions and relies upon an intermediate system (IS) for communication with nodes that reside within its OSI area.
     Note: The End System routing mode is not available if more than one virtual router is enabled.
   - ♦ **Intermediate System Level 1**-The ONS 15454 SDH performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS

L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.

- **Intermediate System Level 1/Level 2**-The ONS 15454 SDH 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.

3. If needed, change the LSP data buffers:
    - ♦ L1 LSP Buffer Size-Adjusts the Level 1 link state protocol data unit (PDU) buffer size. The default is 512. It should not be changed.
    - ♦ L2 LSP Buffer Size-Adjusts the Level 2 link state PDU buffer size. The default is 512. It should not be changed.
4. Return to your originating procedure (NTP).

DLP-D166 Provision or Modify TARP Operating Parameters

Purpose	This task provisions or modifies the Target Identifier Address Resolution Protocol (TARP) operating parameters including TARP PDU propagation, timers, and loop detection buffer (LDB).
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

1. In node view, click the **Provisioning > OSI > TARP > Config** tabs.
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 network element (NE) is the target of the Type 1 PDU, and PDUs are not propagated to the NE from which the PDU was received.

      Note: TARP PDUs L1 Propagation 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 occurs if the NE is not the target of the Type 2 PDU, and PDUs are not propagated to the NE from which the PDU was received.

      Note: TARP PDUs L2 Propagation is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.
    - ♦ TARP PDUs Origination-If checked (default), the node performs all TARP origination functions including:
        - ◊ TID-to-NSAP resolution requests (originate TARP Type 1 and Type 2 PDUs)
        - ◊ NSAP-to-TID requests (originate Type 5 PDUs)
        - ◊ TARP address changes (originate Type 4 PDUs)

      Note: TARP Echo and NSAP to TID is not supported.
    - ♦ TARP Data Cache-If checked (default), the node maintains a TARP data cache (TDC). The TDC is a database of TID-to-NSAP pairs created from TARP Type 3 PDUs received by the

node and modified by TARP Type 4 PDUs (TID-to-NSAP updates or corrections). TARP 3 PDUs are responses to Type 1 and Type 2 PDUs. The TDC can also be populated with static entries entered on the TARP > Static TDC tab.
Note: TARP Data Cache is only used when the TARP PDUs Origination parameter is enabled.

- L2 TARP Data Cache-If checked (default), the TIDs and NSAPs of NEs originating Type 2 requests are added to the TDC before the node propagates the requests to other NEs.
  Note: L2 TARP Data Cache 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 LDP 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 TARP PDUs Origination 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 the TARP PDUs Origination check box is not checked.

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

DLP-D167 Add a Static TID-to-NSAP Entry to the TARP Data Cache

Purpose	This task adds a static TID-to-NSAP entry to the TDC. The static entries are required for NEs that do not support TARP and are similar to static routes. For a specific TID, you must force a specific NSAP.

Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

1. In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.
2. Click **Add Static Entry**.
3. In the Add Static Entry dialog box, enter the following:
   - TID-Enter the TID of the NE. (For ONS nodes, the TID is the Node Name parameter on the node view Provisioning > General tab.)
   - NSAP-Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.
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.
5. Return to your originating procedure (NTP).

DLP-D168 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-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

1. In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.
2. Click the static entry that you want to delete.
3. Click **Delete Static Entry**.
4. In the Delete TDC Entry dialog box, click **Yes**.
5. Return to your originating procedure (NTP).

DLP-D169 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 SDH must communicate across routers or non-SDH NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > OSI > TARP > MAT** tabs.
2. Click **Add**.

3. In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:
    - ♦ Level-Sets the TARP Type Code that will be sent:
        - ◊ **Level 1**-Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
        - ◊ **Level 2**-Indicates that the adjacency is in a different area than the current node. The entry generates Type 2 PDUs.
    - ♦ NSAP-Enter the OSI NSAP address in the NSAP field or, if preferred, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box.
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.
5. Return to your originating procedure (NTP).

DLP-D171 Provision OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Note: The Router 1 manual area address, System ID, and Selector "00" create the node NSAP address. Changing the Router 1 manual area address changes the node's NSAP address.

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

1. In node view, click the **Provisioning > OSI > Routers > Setup** tabs.
2. Chose the router you want provision and click **Edit**. The OSI Router Editor dialog box appears.
3. In the OSI Router Editor dialog box:
    1. Check **Enable Router** to enable the router and make its primary area address available for editing.
    2. Click the manual area address, then click **Edit**.
    3. In the Edit Manual Area Address dialog box, edit the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the edits in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 8 to 24 alphanumeric characters (0-9, a-f) in length.
    4. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.
4. Return to your originating procedure (NTP).

DLP-D172 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. Three additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	NTP-D24 Verify Card Installation

	NTP-D171 Provision OSI Routers
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. Click the **Provisioning > OSI > Routers > Setup** tabs.
2. Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box appears.
3. In the OSI Router Editor dialog box:
    1. Check **Enable Router** to enable the router and make its primary area address available for editing.
    2. Click the manual area address, then click **Add**.
    3. In the Add Manual Area Address dialog box, enter the primary area address in the Area Address field. If you prefer, click **Use Mask** and enter the address in the Masked NSAP Entry dialog box. The address (hexadecimal format) can be 2to 24 alphanumeric characters (0-9, a-f) in length.
    4. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.
4. Return to your originating procedure (NTP).

DLP-D173 Enable the OSI Subnet on the LAN Interface

Purpose	This task enables the OSI subnetwork point of attachment on the LAN interface.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: OSI subnetwork points of attachment are enabled on data communications channels (DCCs) when you create DCCs. See the "DLP-D363 Provision Regenerator-Section DCC Terminations" task and the "DLP-D364 Provision Multiplex-Section DCC Terminations" task.

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

Note: If Secure Mode is on, the OSI subnet is enabled on the backplane LAN port, not the front TCC2P port.

1. In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.
2. Click **Enable LAN Subnet**.
3. In the Enable LAN Subnet dialog box, complete the following fields:
    - ESH-Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
    - ISH-Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
    - IIH-Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
    - IS-IS Cost-Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default IS-IS cost for LAN subnets is 20. It

normally should not be changed.

- ♦ DIS Priority-Sets the designated intermediate system (DIS) priority. In IS-IS networks, one router is elected to serve as the DIS (LAN subnets only). Cisco router DIS priority is 64. For the ONS 15454 LAN subnet, the default DIS priority is 63. It normally should not be changed.

4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-D174 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-ConnectionLess Network Service (CLNS) tunnel to allow ONS 15454 SDH nodes to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

1. In node view, click the **Provisioning > OSI > Tunnels** tabs.
2. Click **Create**.
3. In the Create IP Over OSI Tunnel dialog box, complete the following fields:

- Tunnel Type-Choose a tunnel type:
  - ◊ **Cisco**-Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
  - ◊ **GRE**-Creates a Generic Routing Encapsulation tunnel. 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 OSPF metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- NSAP Address-Enter the destination NE or OSI router NSAP address.

4. Click **OK**.
5. Provision the other tunnel endpoint using the documentation.
6. Return to your originating procedure (NTP).

DLP-D175 Remove a TARP Manual Adjacency Table Entry

Purpose	This task removes an entry from the TARP manual adjacency table.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
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.

1. In node view, click the **Provisioning > OSI > TARP > MAT** tabs.
2. Click the MAT entry that you want to delete.
3. Click **Remove**.
4. In the Delete TDC Entry dialog box, click **OK**.
5. Return to your originating procedure (NTP).

DLP-D178 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
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 SDH Reference Manual*.

Caution! 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.

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.
2. In node view, click the **Provisioning** > **OSI** tabs.
3. Choose one of the following routing modes:

- ♦ **End System**-The ONS 15454 SDH performs OSI IS functions. It communicates with IS and ES nodes that reside within its OSI area. It depends upon an IS L1/L2 node to communicate with IS and ES nodes that reside outside its OSI area.
- ♦ **Intermediate System Level 1/Level 2**-The ONS 15454 SDH 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 SDH Reference Manual.

4. Although Cisco does not recommend changing the LSP (Link State Protocol Data Unit) 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.
5. Return to your originating procedure (NTP).

DLP-D179 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-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > OSI > Routers > Setup** tabs.
2. Chose the router you want provision and click **Edit**.
3. In the OSI Router Editor dialog box:
   1. 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.
   2. For enabled routers, edit the primary area address, if needed. The address can be between 8 and 24 alphanumeric characters in length.
   3. 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**.
   4. Click **OK**.
4. Return to your originating procedure (NTP).

DLP-D180 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 DCC (SDCC), Line DCC (LDCC), generic communications channel (GCC), or optical service channel (OSC), or when you enable the LAN subnet.
Tools/Equipment	None
	DLP-D60 Log into CTC

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

1. In node view, click the **Provisioning > OSI > Routers > Subnet** tabs.
2. Choose the subnet you want to edit, then click **Edit**.
3. In the Edit <*subnet type*> Subnet <*slot/port*> dialog box, edit the following fields:
   - ESH-The End System Hello 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 PDU propagation frequency. An intermediate system NE sends ISHs to other ESs and ISs to inform them about the NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
   - IIH-The Intermediate System to Intermediate System Hello 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.
4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-D181 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-D174 Create an IP-Over-CLNS Tunnel DLP-D60 Log into CTC
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.

1. In node view, click the **Provisioning > OSI > Tunnels** tabs.
2. Click **Edit**.
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 tunnel. 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 OSPF metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not be changed unless you are creating multiple tunnel routes and want to prioritize routing by assigning different metrics.
- ◊ NSAP Address-Enter the destination NE or OSI router NSAP address.

4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-D182 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
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 loose 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.

1. In node view, click the **Provisioning > OSI > Tunnels** tabs.
2. Choose the IP-over-CLNS tunnel that you want to delete.
3. Click **Delete**.
4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-D183 View IS-IS Routing Information Base

Purpose	This task allows you to view the Intermediate System to Intermediate System (IS-IS) protocol routing information base (RIB). IS-IS is an OSI routing protocol that floods the network with information about NEs on the network. Each NE uses the information to build a complete and consistent picture of a network topology. The IS-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Maintenance > OSI > IS-IS RIB** tabs.
2. View the following RIB information for Router 1:

- Subnet Type-Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
- Location-Indicates the OSI subnetwork point of attachment. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
- Destination Address-The destination NSAP of the IS.
- MAC Address-For destination NEs that are accessed by LAN subnets, the NE's MAC address.

3. If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.
4. Return to your originating procedure (NTP).

DLP-D184 View ES-IS Routing Information Base

Purpose	This task allows you to view the End System to Intermediate System (ES-IS) protocol RIB. ES-IS is an OSI protocol that defines how end systems (hosts) and intermediate systems (routers) learn about each other. For ESs, the ES-IS RIB shows the network view from the perspective of the ES node. For ISs, the ES-IS RIB shows the network view from the perspective of the IS node.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Maintenance > OSI > ES-IS RIB** tabs.
2. View the following RIB information for Router 1:
    - Subnet Type-Indicates the OSI subnetwork point of attachment type used to access the destination address. Subnet types include SDCC, LDCC, GCC, OSC, and LAN.
    - Location-Indicates the subnet interface. For DCC subnets, the slot and port are displayed. LAN subnets are shown as LAN.
    - Destination Address-The destination IS NSAP.
    - MAC Address-For destination NEs that are accessed by LAN subnets, the NE's MAC address.
3. If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.
4. Return to your originating procedure (NTP).

DLP-D185 Manage the TARP Data Cache

Purpose	This task allows you to view and manage the TDC. The TDC facilitates TARP processing by storing a list of TI-to-NSAP mappings.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Maintenance > OSI > TDC** tabs.
2. View the following TARP data cache information:
    - ♦ TID-The target identifier of the originating NE. For ONS 15454 SDH nodes, the TID is the name entered in the Node Name/TID field on the Provisioning > General tab.
    - ♦ NSAP/NET-The Network Service Access Point or Network Element Title of the originating NE.
    - ♦ Type-Indicates how the TDC entry was created:
        - ◊ Dynamic-The entry was created through the TARP propagation process.
        - ◊ Static-The entry was manually created and is a static entry.
3. If you want to query the network for an NSAP that matches a TID, complete the following steps. Otherwise, continue with Step 4.

    Note: The TID to NSAP function is not available if the TARP data cache is not enabled on the Provisioning > OSI > TARP tab.

    1. Click the **TID to NSAP** button.
    2. In the TID to NSAP dialog box, enter the TID you want to map to an NSAP.
    3. Click **OK**, then click **OK** in the information message box.
    4. On the TDC tab, click **Refresh**.
       If TARP finds the TID in its TDC, it returns the matching NSAP. If not, TARP sends PDUs across the network. Replies will return to the TDC later, and a "check TDC later" message appears.
4. If you want to delete all the dynamically generated TDC entries, click the **Flush Dynamic Entries** button. If not, continue with Step 5.
5. Return to your originating procedure (NTP).

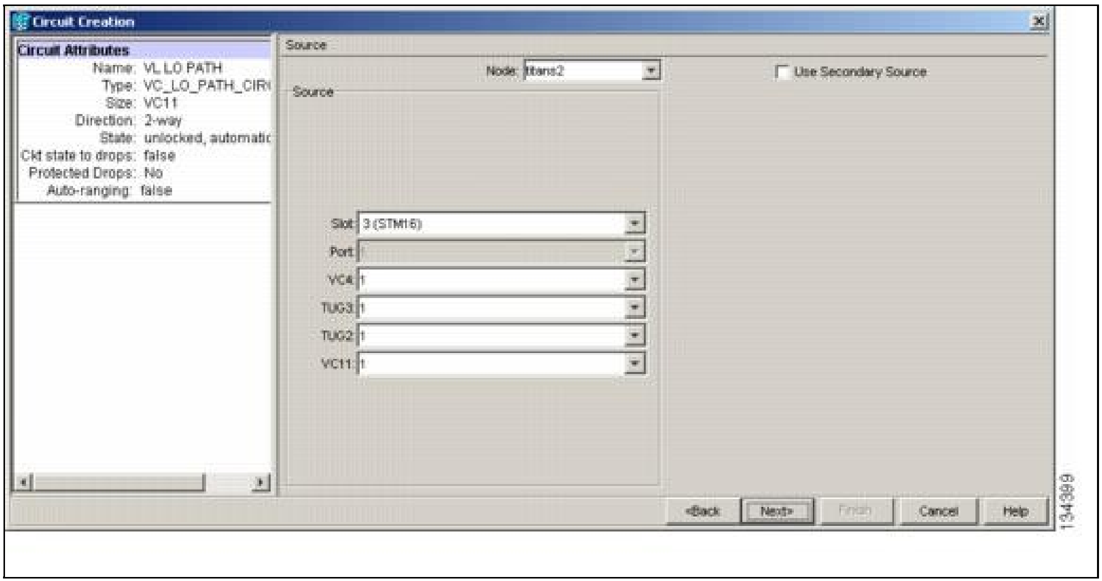
DLP-D186 Provision a Low-Order VC11 Circuit Source and Destination

Purpose	This task provisions an optical circuit source and destination for a low-order VC11 circuit.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC NTP-D334 Create an Automatically Routed Low-Order VC11 Circuit, or NTP-D335 Create a Manually Routed Low-Order VC11 Circuit, or NTP-D336 Create a Unidirectional Low-Order VC11 Circuit with Multiple Drops You must have the Source page of the Circuit Creation wizard open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: After you have selected the circuit properties in the Circuit Source dialog box according to the specific circuit creation procedure, you are ready to provision the circuit source.

1. From the Node drop-down list, choose the node where the source will originate.
2. From the Slot drop-down list, choose the slot containing the STM-N, MRC-12, or MRC-2.5G-12 card where the circuit will originate (Figure 18-11). If you choose an STM-N card, you can map the VC11 to VC4 for optical transport.

Figure 18-11: Defining the Circuit Source on an STM-16 Card



Circuit Creation

Circuit Attributes
Name: VL LO PATH
Type: VC_LO_PATH_CIR
Size: VC11
Direction: 2-way
State: unlocked, automatic
Ckt state to drops: false
Protected Drops: No
Auto-ranging: false

Source
Node: ttans2
□ Use Secondary Source
Source
Slot: 3 (STM16)
Port: 1
VC4: 1
TUG3: 1
TUG2: 1
VC11: 1

3. Choose the port from the Port drop-down list.
4. From the VC4 drop-down list, choose the source VC4.
5. From the TUG3 drop-down list, choose the source TUG3.
6. From the TUG2 drop-down list, choose the source TUG2.
7. From the VC11 drop-down list, choose the source VC11.
8. If you need to create a secondary source, for example, a subnetwork connection protection (SNCP) ring bridge/selector circuit entry point in a multivendor SNCP ring, click **Use Secondary Source** and repeat Steps 1 through 7 to define the secondary source. If you do not need to create a secondary source, continue with Step 9.
9. Click **Next**.
10. From the Node drop-down list, choose the destination (termination) node.
11. From the Slot drop-down list, choose the slot containing the destination card. You can choose a MRC-12, MRC-2.5G-12, or STM-N card to map the VC11 to a VC4 for optical transport.
12. Depending on the destination card, choose the destination port from the drop-down lists that appear based on the card selected in Step 11. See Table 6-2 for a list of valid options. CTC does not show ports, VC4s, TUG3s, TUG2s, or VC11s already used by other circuits.

    Note: If you and a user working on the same network choose the same VC4, TUG3, TUG2, or VC11 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.
13. If you need to create a secondary destination, for example, an SNCP ring bridge/selector circuit exit point in a multivendor SNCP ring, click **Use Secondary Destination** and repeat Steps 10 through 12 to define the secondary destination.
14. Click **Next**.
15. Return to your originating procedure (NTP).

DLP-D187 Provision a Low-Order VC11 Circuit Route

Purpose	This task provisions the circuit route for low-order VC11 manually routed circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC

	NTP-D335 Create a Manually Routed Low-Order VC11 Circuit You must have the Route Review and Edit page of the Circuit Creation wizard open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected.
2. Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source VC11 appears.
3. If you want to change the source VC11, adjust the Source VC11 field; otherwise, continue with Step 4.
4. If you want to change the source TUG2, TUG3, VC3, or VC4, adjust the TUG2, TUG3, VC3, or VC4 fields; otherwise, continue with Step 5.
5. Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.
6. Repeat Steps 2 through 5 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protect Path is checked in the Circuit Routing Preferences area, you must complete the following steps:
    - ♦ Add two spans for all SNCP ring or unprotected portions of the circuit route from the source to the destination.
    - ♦ Add one span for all MS-SPRing or 1+1 portions of the route from the source to the destination.
7. Return to your originating procedure (NTP).

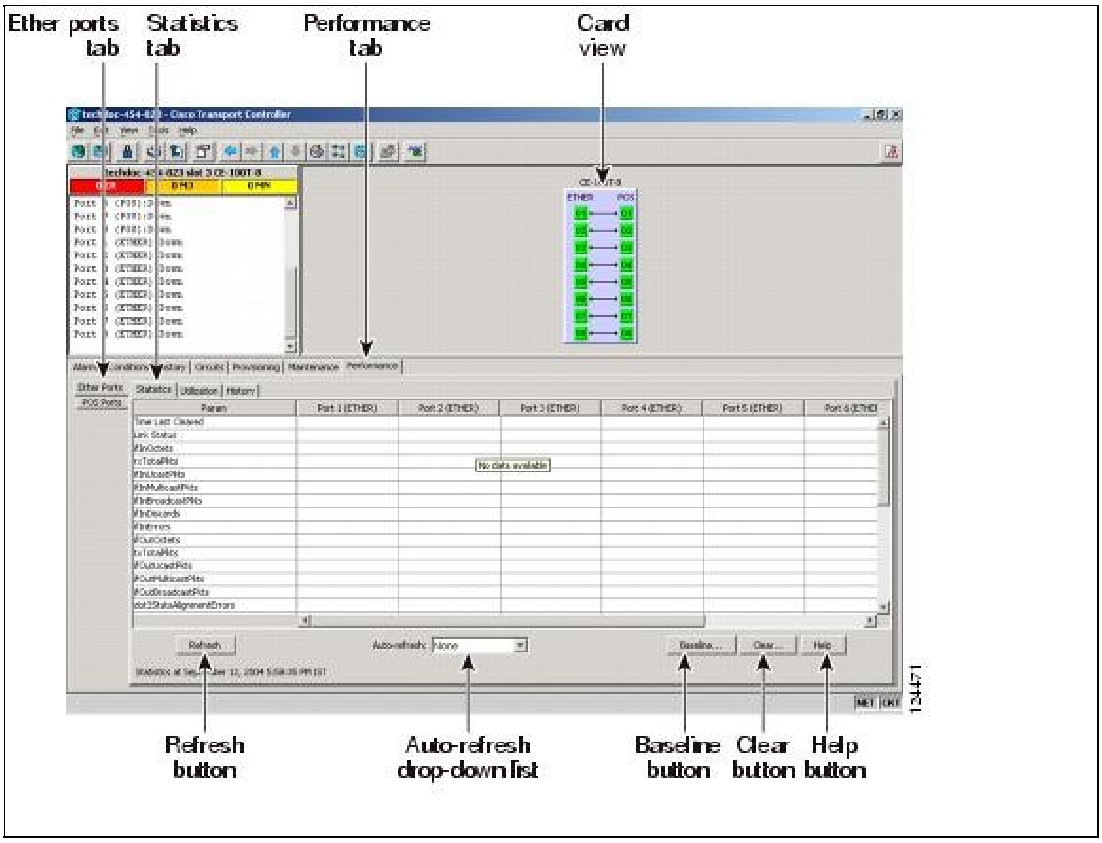
DLP-D188 View CE-Series Ethernet and POS Ports Statistics PM Parameters

Purpose	This task enables you to view CE-Series card Ethernet and POS port Statistics PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note: For CE-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*

1. In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance** > **Ether Ports > Statistics** (Figure 18-12) or **Performance > POS Ports** > **Statistics** tabs.

Figure 18-12: Ether Ports Statistics on the Card View Performance Window



3. Click **Refresh**. PM statistics for each port on the card appear.
4. View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

   Note: To refresh, reset, or clear PM counts, see the NTP-D257 Change the PM Display.
5. 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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Selected Group pane, verify that the working slot/port is shown as Working/Active. If so, this task is complete.
3. If the working slot says Working/Standby, perform a Manual switch on the working slot:
   1. In the Selected Group pane, choose the Protect/Active slot.
   2. In the Switch Commands field, choose **Manual**.
   3. Click **Yes** in the confirmation dialog box.
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*.

5. When the working slot is carrying traffic, clear the Manual switch:
    1. In the Switch Commands field, choose **Clear**.
    2. Click **Yes** in the confirmation dialog box.
6. Verify that the working slot does not switch back to Standby, which might indicate a problem on the working span.
7. Return to your originating procedure (NTP).

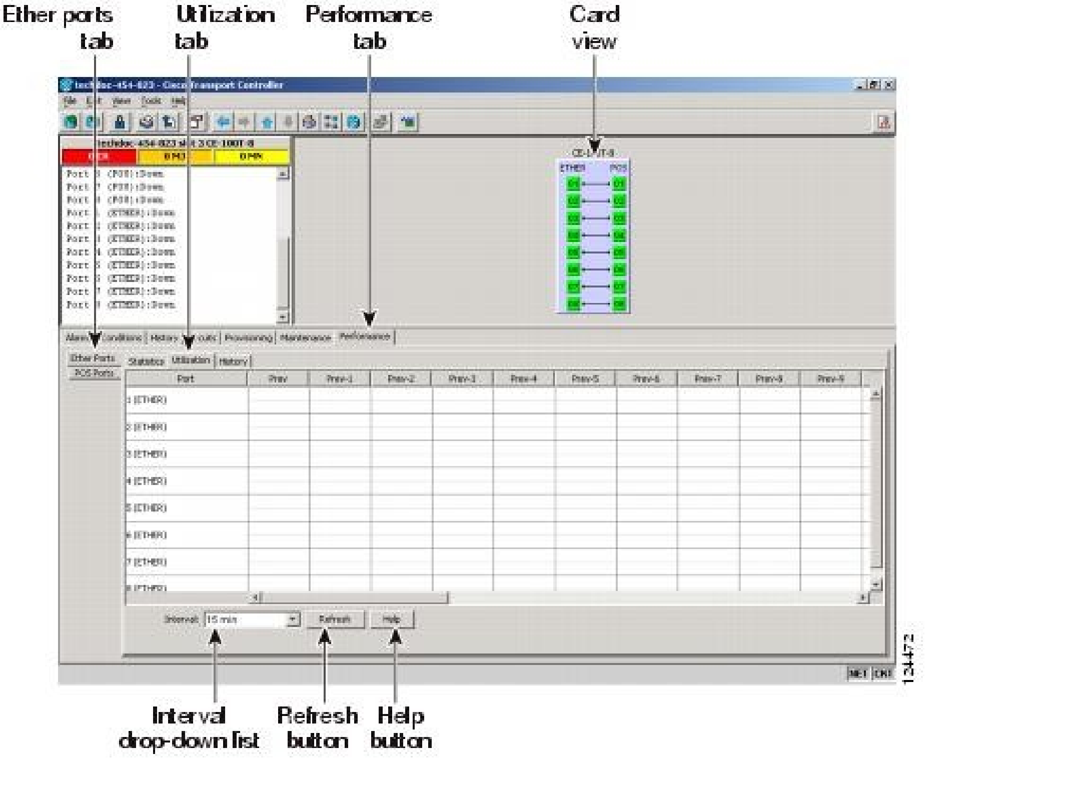
DLP-D190 View CE-Series Ethernet and POS Ports Utilization PM Parameters

Purpose	This task enables you to view CE-Series card Ethernet and POS port Utilization PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note: For CE-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*

1. In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance > Ether Ports > Utilization** (Figure 18-13) or **Performance > POS Ports > Utilization** tabs.

Figure 18-13: Ether Ports Utilization on the CE-Series Card View Performance Window



Port	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
1 (ETHER)										
2 (ETHER)										
3 (ETHER)										
4 (ETHER)										
5 (ETHER)										
6 (ETHER)										
7 (ETHER)										
8 (ETHER)										

Interval: 15 min

3. Click **Refresh**. Performance monitoring statistics for each port on the card appear.
4. View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual.*

   Note: To refresh, reset, or clear PM counts, see the NTP-D257 Change the PM Display.
5. 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
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Provisioning or higher

1. On the shelf graphic, right-click the card that you want to remove and choose **Delete Card**.
2. Ensure that none 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.
   - The card has circuits; see the "DLP-D27 Delete Circuits" task.
   - The card is part of an MS-SPRing; see the NTP-D213 Remove an MS-SPRing Node.
   - The card is being used for timing; see the "DLP-D157 Change the Node Timing Source" task.
   - The card has a DCC termination; see the "DLP-D360 Delete a Regenerator-Section DCC Termination" task or "DLP-D362 Delete a Multiplex-Section DCC Termination" task.
     Note: If you delete a card in CTC but do not remove the card from shelf, it will reboot and reappear in CTC.
3. Return to your originating procedure (NTP).

DLP-D192 View CE-Series Ethernet and POS Ports History PM Parameters

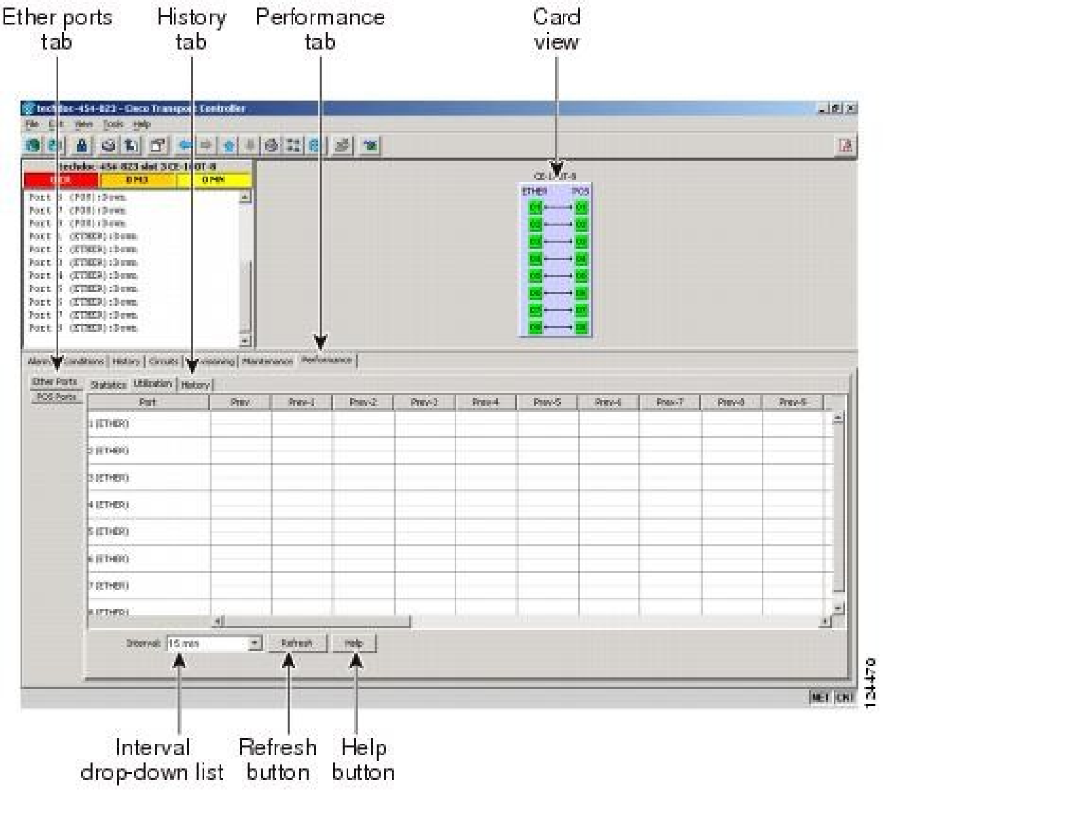
Purpose	This task enables you to view CE-Series card Ethernet and POS port History PM counts at selected time intervals to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note: For CE-Series card provisioning, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide.*

1. In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance** > **Ether Ports** > **History** (Figure 18-14) or **Performance** > **POS Ports > History** tabs.

Figure 18-13: Ether Ports Utilization on the CE-Series Card View Performance Window

Figure 18-14: Ether Ports History on the CE-Series Card View Performance Window



3. Click **Refresh**. Performance monitoring statistics for each port on the card appear.
4. View the PM parameter names that appear in the Param column. The PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

   Note: To refresh, reset, or clear PM counts, see the NTP-D257 Change the PM Display.
5. Return to your originating procedure (NTP).

DLP-D193 Grant Superuser Privileges to a Provisioning User

Purpose	This task enables Provisioning users to perform tasks such as retrieving audit logs, restoring databases, and activating and reverting software loads.
Tools/Equipment	None
Prerequisite Procedures	DLP-D60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

1. In node view, click the **Provisioning** > **Defaults** tabs.
2. In the Defaults Selector area, choose **NODE > security > grantPermission**.
3. Click in the Default Value column for the default property you are changing and choose **Provisioning** from the drop-down list.

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

4. Click **Apply**.

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

   Note: You must close your current CTC session and restart a new CTC session for the changes to take effect.
5. 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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > MS-SPRing** tabs.
3. Click **Edit**.
4. To clear a Force switch on the west line:
   1. 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.
   2. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.
   3. In the Confirm MS-SPRing Operation dialog box, click **Yes**.
5. To clear a Force switch on the east line:
   1. 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.
   2. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.
   3. 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.
6. From the File menu, choose **Close**.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

2. Observe the Timing Mode field to see the type of timing (Line, External, Mixed) that has been set for that node.
3. Scroll down to the Reference List and observe the NE Reference fields to see the timing references provisioned for that node.
4. If the removed node was the only building integrated timing supply (BITS) timing source, perform the following:
    1. Contact your synchronization coordinator or appropriate personnel before continuing with this procedure.
    2. 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.
    3. 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.)

        Note: This type of timing conforms to SETS requirements and is not considered optimal.
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.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 Connect the PC and Log into the GUI, for procedures.
2. From node view, click the **Provisioning > MS-SPRing** tabs.
3. Highlight the ring and click **Delete**.
4. In the Suggestion dialog box, click **OK**.
5. In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.
6. Return to your originating procedure (NTP).

DLP-D197 Initiate an SNCP Force Switch

Purpose	This task switches all circuits on an SNCP span.
Tools/Equipment	None
Prerequisite Procedures	D60 Log into CTC

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.

1. From the View menu in node view, choose **Go to Network View**.
2. Right-click the span where you want to switch SNCP traffic away. Choose **Circuits** from the shortcut menu.
3. In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.
4. In the Confirm SNCP Switch dialog box, click **Yes**.
5. In the Protection Switch Result dialog box, click **OK**.

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

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

1. From the View menu in node view, choose **Go to Network View**.
2. Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.
3. In the Circuits on Span dialog box, choose **CLEAR** to remove the Force switch. Click **Apply**.
4. In the Confirm SNCP Switch dialog box, click **Yes**.
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.
6. Return to your originating procedure (NTP).