



DLPs E200 to E299



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

DLP-E200 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task reinitializes the ONS 15600 using the CTC reinitialization (reinit) tool on a UNIX computer. Reinitialization uploads a new software package to the TSC cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	Cisco ONS 15600 SONET System Software CD, Version 6.0.x JRE 1.4.2 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitialization tool can run on JRE 1.3.1_02 or JRE 1.4.2.
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed to clear the existing database from a TSC card and restore the node default settings.
Onsite/Remote	Onsite or remote
Security Level	Superuser



Note

Restoring a node to the factory configuration deletes all cross-connects on the node.

- Step 1** Insert the Cisco ONS 15600 SONET System Software CD, Version 6.0.x, into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.
- Step 2** To find the recovery tool file, go to the CISCO15600 directory on the CD (usually /cdrom/cdrom0/CISCO15600).
- Step 3** If you are using a file explorer, double-click the RE-INIT.jar file. If you are working with a command line interface, run `java -jar RE-INIT.jar`. The NE Reinitialization window appears.

Step 4 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.
- Re-init Database—Check this box to send a new database to the node. (This is equivalent to the CTC database restore operation.) If unchecked, the node database is not modified.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Search Path—Enter the path to the CISCO15600 folder on the CD drive.

Step 5 Click **Go**.**Caution**

Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.


Step 6 Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the TSC cards, "Complete" appears in the status bar and the TSC cards will reboot. Wait a few minutes for the reboot to complete.

Step 7 After the reboot is complete, log into the node using the [“DLP-E26 Log into CTC” task on page 16-39](#).**Step 8** Complete the [“NTP-E22 Set Up Date, Time, and Contact Information” procedure on page 4-4](#).**Step 9** Return to your originating procedure (NTP).

DLP-E201 Provision ASAP Ethernet Ports

Purpose	This task provisions Any Service Any Port (ASAP) Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In the node view, double-click the ASAP card graphic to open the card.
- Step 2** Click the **Provisioning > Ethernet > Ports** tabs.
- Step 3** For each port, provision the following parameters:
- Port Name—If you want to label the port, type the port name.
 - Admin State—Choose **IS** to put the port in service.
 - Enable Flow Control—Check this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The ASAP attempts to negotiate symmetrical flow control with the attached device.
- Step 4** Click **Apply**.
- Step 5** Refresh the Ethernet statistics:
- a. Click the **Performance > Ethernet > Ether Ports > Statistics** tabs.
 - b. Click **Refresh**.
-  **Note** Reprovisioning an Ethernet port on the ASAP card does not reset the Ethernet statistics for that port.
-
- Step 6** Return to your originating procedure (NTP).
-

DLP-E202 Provision ASAP POS Ports

Purpose	This task provisions ASAP packet-over-SONET (POS) ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In the node view, double-click the ASAP card graphic to open the card.

Step 2 Click the **Provisioning > Ethernet > POS Ports** tabs.

Step 3 For each POS port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.
- Admin State—Choose **IS** 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 frame-mapped generic framing procedure (GFP-F) framing, the user can configure a **32-bit** cyclic redundancy check (CRC), the default, or **none** (no CRC). High-level data link control (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 The ASAP uses LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.



Note An Encapsulation Mismatch Path (ENCAP-MISMATCH-P) alarm appears when a point-to-point circuit is created between two Ethernet card ports with incompatible encapsulation payload types.

Step 4 Click **Apply**.

Step 5 Refresh the POS statistics:

- a. Click the **Performance > Ethernet > POS Ports > Statistics** tabs.
- b. Click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-E203 View ASAP OC-N PM Parameters

Purpose	This task enables you to view performance monitoring (PM) counts on an ASAP card to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Step 2 Click the **Performance > Optical** tabs ([Figure 18-1](#)).

Figure 18-1 Viewing OC-N Card Performance Monitoring Information

Card View

Performance tab

Optical tab

Directions radio button

Intervals radio button

Port drop-down list

Sub-signal STS drop-down list

Refresh button

Auto-refresh drop-down list

Baseline button

Clear button

Help button

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Pr
CV-L	0	0	0	0	0	0	0	0	0	0	
ES-L	0	0	0	0	0	0	0	0	0	0	
SES-L	0	0	0	0	0	0	0	0	0	0	
UAS-L	0	0	0	0	0	0	0	0	0	0	
FC-L	0	0	0	0	0	0	0	0	0	0	
CV-S	0	0	0	0	0	0	0	0	0	0	
ES-S	0	0	0	0	0	0	0	0	0	0	
SES-S	0	0	0	0	0	0	0	0	0	0	
SEFS-S	0	0	0	0	0	0	0	0	0	0	
PSC	0	0	0	0	0	0	0	0	0	0	

Step 3 In the Port drop-down list, click the port you want to monitor.

Step 4 Click **Refresh**.

Step 5 View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current), and Prev-*n* (previous) columns. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.

Step 6 To monitor another port on a multiport card, choose another port from the Port drop-down list and click **Refresh**.

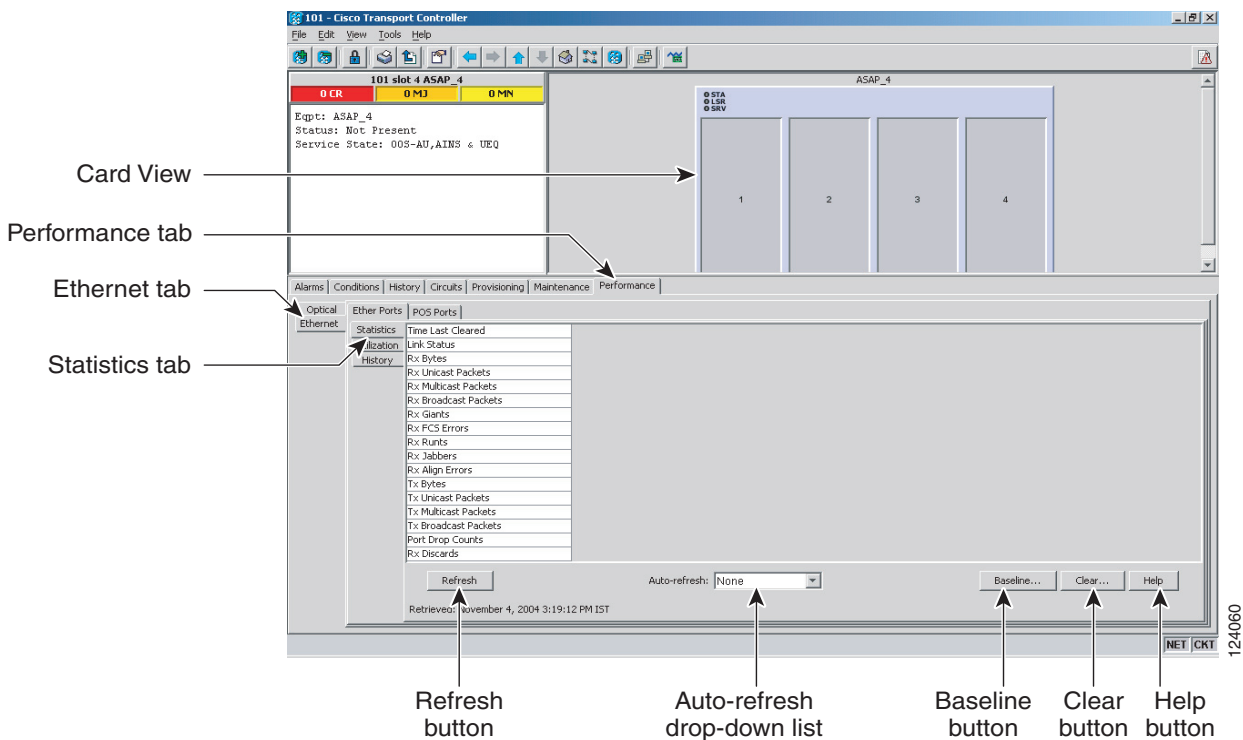
Step 7 Return to your originating procedure (NTP).

DLP-E204 View ASAP Ether Ports Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Figure 18-2 Ether Ports Statistics in the Card View Performance Window



- Step 3** Click **Refresh**. Performance monitoring statistics appear for each port on the card.
- Step 4** View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.



Note To refresh, reset, or clear PM counts, see the “NTP-E143 Change the PM Display” procedure on page 9-2.

Step 5 Return to your originating procedure (NTP).

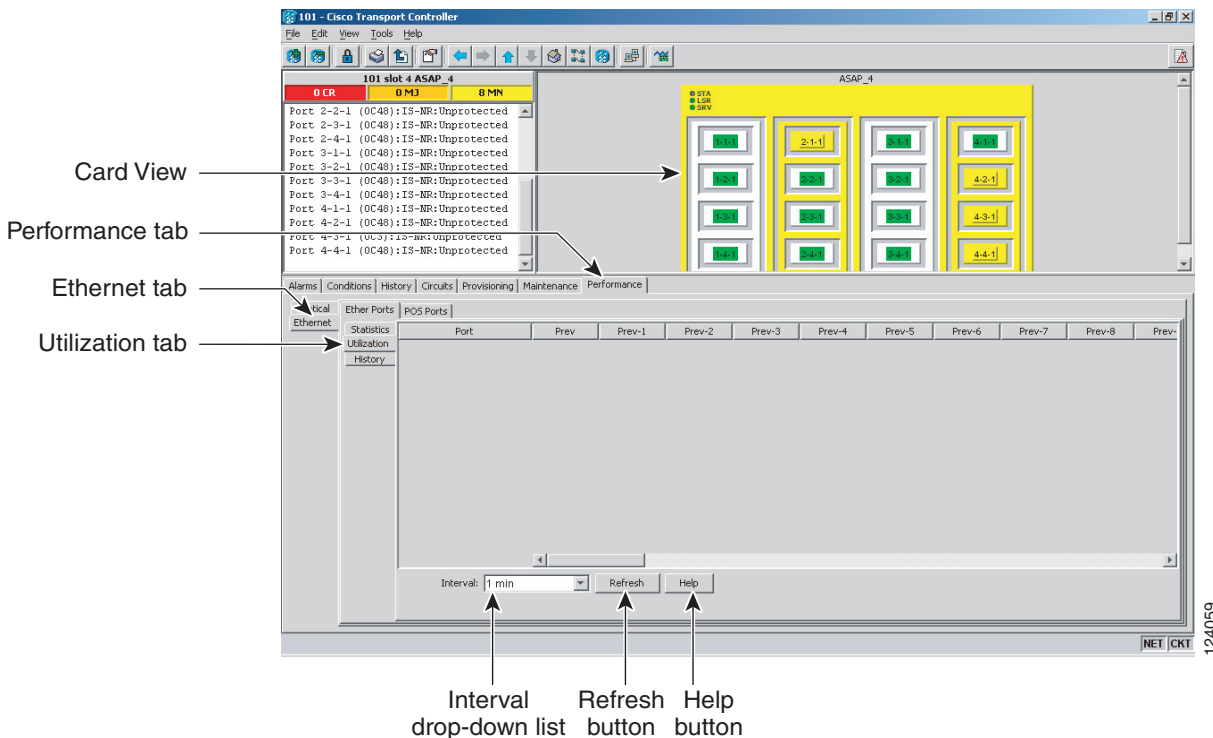
DLP-E205 View ASAP Ether Ports Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC , page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Step 2 Click the **Performance > Ethernet > Ether Ports > Utilization** tabs ([Figure 18-3](#)).

Figure 18-3 Ether Ports Utilization in the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring utilization values appear for each port on the card.

- Step 4** View the Port # column for the port that you want to monitor.
- Step 5** The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.



Note To refresh, reset, or clear PM counts, see the [“NTP-E143 Change the PM Display” procedure on page 9-2](#).

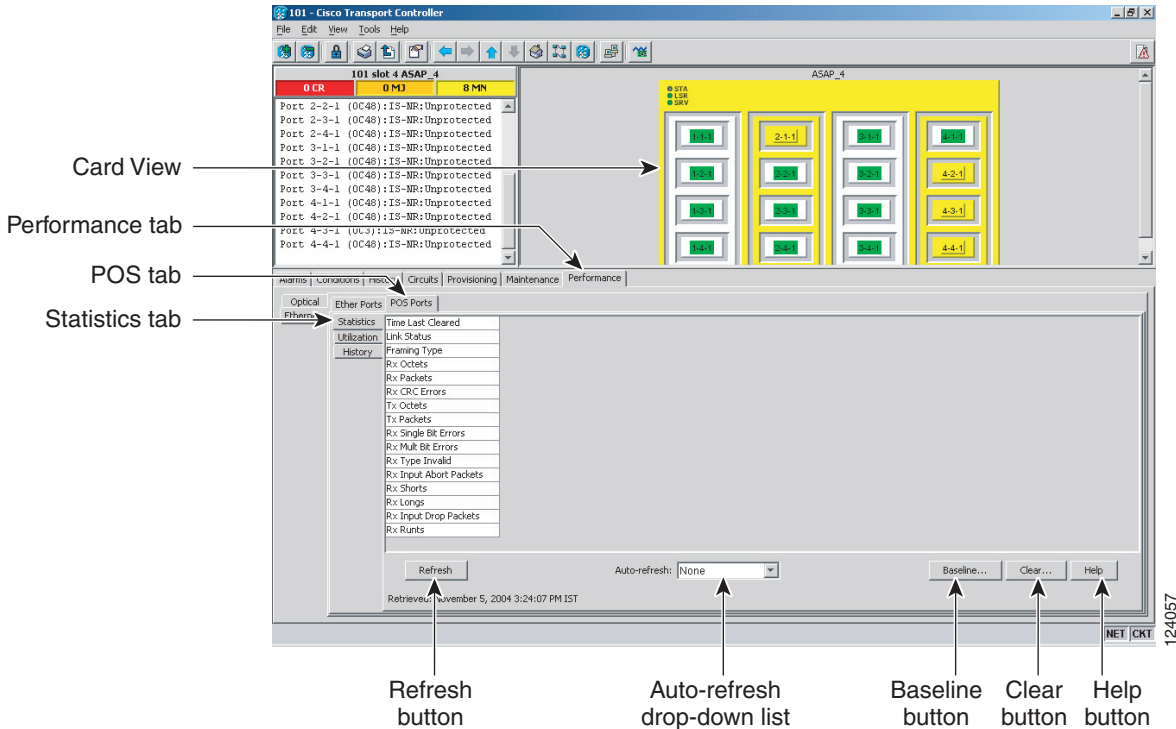
- Step 6** Return to your originating procedure (NTP).

DLP-E206 View ASAP POS Ports Statistics PM Parameters

Purpose	This task enables you to view POS port PM counts at selected time intervals on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

- Step 1** In node view, double-click the ASAP card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Ethernet > POS Ports > Statistics** tabs ([Figure 18-4](#)).

Figure 18-4 POS Ports Statistics in the Card View Performance Window



- Step 3** Click **Refresh**. Performance monitoring statistics appear for each port on the card.
- Step 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 *Cisco ONS 15600 Reference Manual*.



Note To refresh, reset, or clear PM counts, see the “[NTP-E143 Change the PM Display](#)” procedure on page 9-2.

- Step 5** Return to your originating procedure (NTP).

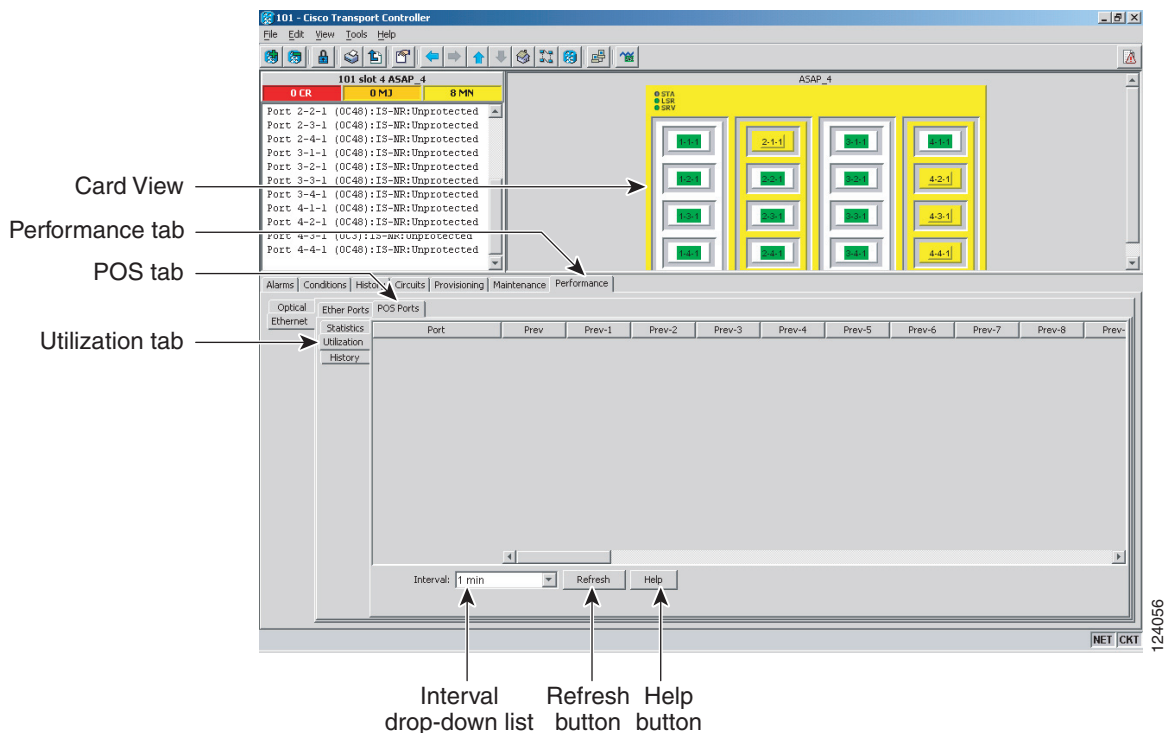
DLP-E207 View ASAP POS Ports Utilization PM Parameters

Purpose	This task enables you to view POS ports utilization PM counts on an ASAP card and ports to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Step 2 Click the **Performance > Ethernet > POS Ports > Utilization** tabs (Figure 18-5).

Figure 18-5 POS Ports Utilization in the Card View Performance Window



Step 3 Click **Refresh**. Performance monitoring utilization values for each port on the card appear.

Step 4 View the Port # column for the port you want to monitor.

Step 5 The Tx and Rx bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.



Note To refresh, reset, or clear PM counts, see the [“NTP-E143 Change the PM Display” procedure on page 9-2](#).

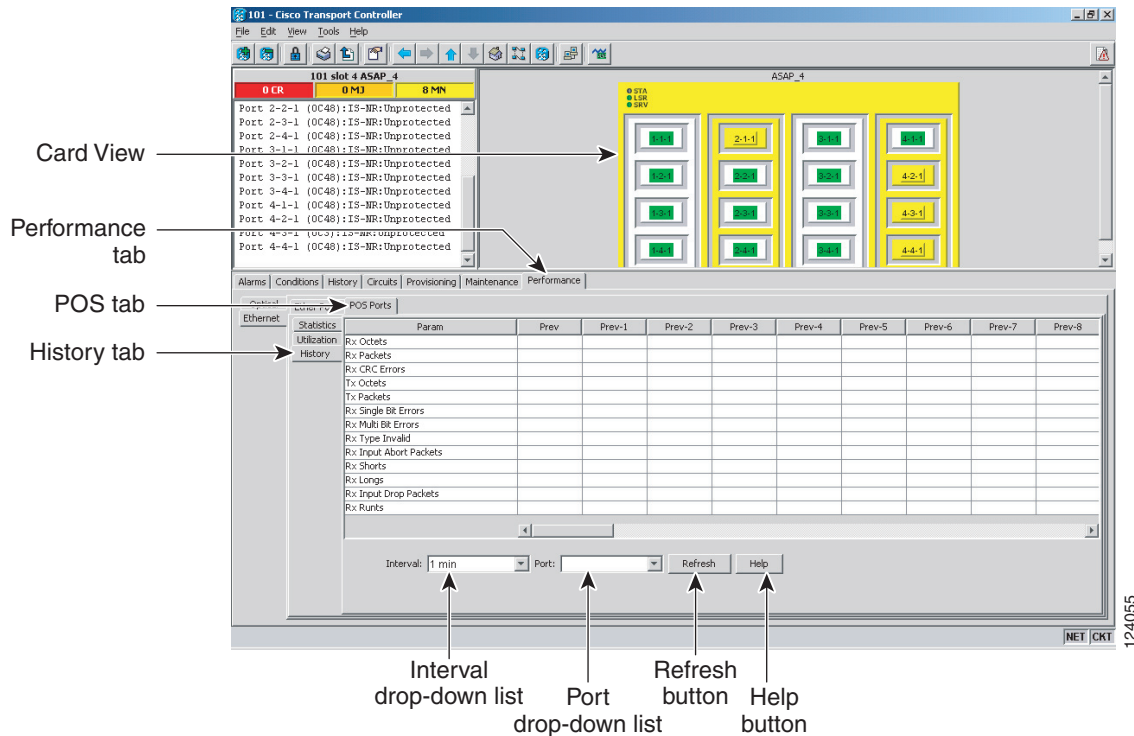
Step 6 Return to your originating procedure (NTP).

DLP-E208 View ASAP POS Ports History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC , page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

- Step 1** In node view, double-click the ASAP card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Ethernet > POS Ports > History** tabs (Figure 18-6).

Figure 18-6 Ethernet POS Ports History in the Card View Performance Window



- Step 3** Click **Refresh**. Performance monitoring statistics appear for each port on the card.
- Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.



Note To refresh, reset, or clear PM counts, see the [“NTP-E143 Change the PM Display” procedure on page 9-2](#).

Step 5 Return to your originating procedure (NTP).

DLP-E209 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15600 and sets the user security level that can clear node performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 2 In the Access area, provision the following:

- LAN access—Choose one of the following options to set the access paths to the node:
 - **No LAN Access**—Allows access to the node only through data communications channel (DCC) connections. Access through the TSC RJ-45 port and backplane is not permitted.
 - **Front only**—Allows access through the TSC RJ-45 port. Access through the DCC and the backplane is not permitted.
 - **Backplane only**—Allows access through DCC connections and the backplane. Access through the TSC RJ-45 port is not allowed.
 - **Front and Backplane**—Allows access through DCC, TSC RJ-45, and backplane connections.
- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and “DCC only” is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.

Step 3 In the Shell Access area, set the shell program used to access the node:

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

- Step 4** In the TL1 Access area, select the desired level of TL1 access. Disabled completely disables all TL1 access; Non-Secure, Secure allows access using SSH.
- Step 5** In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.
- Step 6** Select the Enable Craft Port check box to turn on the shelf controller serial ports.
- Step 7** Select the EMS access state from the list. Available states are Non-Secure and Secure (allows access using SSH).
- In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:
- **Default - TCC Fixed**—Uses Port 57790 to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 is open.
 - **Standard Constant**—Uses Port 683 (IIOP) or Port 684 (SSLIOP), the Common Object Request Broker Architecture (CORBA) default port number.
 - **Other Constant**—If the default port is not used, type the Internet Inter-ORB Protocol (IIOP) or SSLIOP port specified by your firewall administrator.
- Step 8** In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).
- Step 9** Click **Apply**.
- Step 10** Return to your originating procedure (NTP).

DLP-E210 Install the ASAP Carrier Modules

Purpose	This procedure explains how to install the carrier modules in the ONS 15600 shelf.
Tools/Equipment	ASAP carrier modules
Prerequisite Procedures	NTP-E10 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Warning

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the midplane with your hand or any metal tool, or you could shock yourself. Statement 181



Caution

Always use the supplied ESD wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.



Warning

Class 1 laser product. Statement 1008

**Warning**

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

**Note**

For information about the ASAP card, refer to the *Cisco ONS 15600 Reference Manual*.

Step 1

Remove the carrier module from the box and antistatic sleeve.

**Caution**

Setting an ASAP carrier module on its connectors can cause damage to the connectors.

Step 2

Slide the module along the top and bottom guide rails into the correct slot: Slots 1 to 4 and 11 to 14 are available for traffic cards. Insert the card until it contacts the backplane.

Step 3

Close the ejectors.

Step 4

Verify the LED activity on the card faceplate:

1. The STAT, SRV, and LASER ON LEDs turn on for 20 seconds.
2. The STAT LED blinks and the other LEDs turn on for 30 to 50 seconds.
3. All LEDs blink once and the SRV and LASER ON LEDs illuminate.

**Note**

If the LEDs do not turn on, check that the power breakers on the power distribution unit (PDU) are on. Refer to the *Cisco ONS 15600 Troubleshooting Guide*.

**Note**

If you insert a card into a slot provisioned for a different card, all red LEDs turn on and you will see a mismatched equipment (MEA) alarm for that slot when you open Cisco Transport Controller (CTC).

Step 5

After you have logged into CTC, verify that the card appears in the correct slot on the CTC node view. See [Chapter 3, “Connect the Computer and Log into the GUI”](#) for CTC information and setup instructions.

Step 6

Return to your originating procedure (NTP).

DLP-E211 Install the ASAP 4PIO (PIM) Modules

Purpose	This procedure explains how to install the 4-port I/O modules (4PIOs)/Pluggable Interface Modules (PIMs) in the carrier modules of the ASAP card.
Tools/Equipment	4PIO modules #2 Phillips screwdriver
Prerequisite Procedures	DLP-E210 Install the ASAP Carrier Modules, page 18-13
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Warning

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the midplane with your hand or any metal tool, or you could shock yourself. Statement 181



Caution

Always use the supplied ESD wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.



Warning

Class 1 laser product. Statement 1008



Warning

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

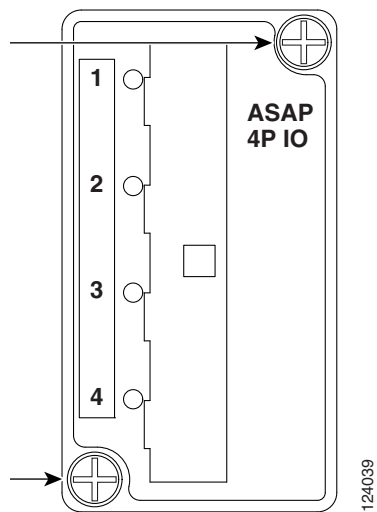


Note

For information about the ASAP card, refer to the *Cisco ONS 15600 Reference Manual*.

- Step 1** Remove the 4PIO module from the box and antistatic sleeve.
- Step 2** Determine in which slot on the ASAP card you want to install the 4PIO module.
- Step 3** Carefully slide the motherboard of the module along the top and bottom guide rails into the correct slot.
- Step 4** Use a Phillips screwdriver to tighten the screws at the top right and bottom left of the 4PIO module.
[Figure 18-7](#) shows the 4PIO module faceplate.

Figure 18-7 4PIO Module Faceplate



Note

The LEDs located on the 4PIO will not light until a fixed rate PIM is installed in the associated PIM slot or a multirate optical (MRO) PIM is installed and an optical rate is provisioned. If the port on the PIM is not in alarm, the associated LED will be green in color (which it will be if you left the port admin state as IS-AINS). If the port is in alarm, it will be amber in color (if you put admin state at IS and a valid signal is not present at its input).



Note

If you insert a card into a slot provisioned for a different card, all red LEDs turn on and you will see a MEA alarm for that slot when you open CTC.

Step 5 After you have logged into CTC, verify that the card appears in CTC card view. See [Chapter 3, “Connect the Computer and Log into the GUI”](#) for CTC information and setup instructions.

Step 6 Return to your originating procedure (NTP).

DLP-E212 Verify Pass-Through Circuits

Purpose	This task verifies that circuits passing through a node that will be removed enter and exit the node on the same synchronous transport signal (STS).
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In the Circuits window, choose a circuit that passes through the node that will be removed and click **Edit**.
- Step 2** In the Edit Circuits window, check **Show Detailed Map**.
- Step 3** Verify that the STS mapping on the node's east and west ports is the same. For example, if a circuit is mapping on the west port s2/p1/S1 (Slot 2, Port 1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit displays different STSs on the east and west ports, write down the name of the circuit.
- Step 4** Repeat Steps 1 to 3 for each circuit in the Circuits tab.
- Step 5** Delete and recreate each circuit recorded in Step 3 that entered/exited the node on different STSs. To delete the circuit, see the "[DLP-E163 Delete Circuits](#)" task on page 17-49. To create the circuit, see [Chapter 6, "Create Circuits."](#)
- Step 6** Return to your originating procedure (NTP).
-

DLP-E213 Preprovision an SFP

Purpose	This procedure preprovisions Small Form-factor Pluggables (SFPs), which are referred to as pluggable port modules (PPMs) in CTC. Cisco-approved OC-3, OC-12, OC-48, Ethernet, and multirate PPMs are compatible with the ONS 15600. See the <i>Cisco ONS 15600 Reference Manual</i> for a list of acceptable SFPs.
Tools/Equipment	None
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note If you preprovision a multirate SFP, you must next select the line rate using the "[DLP-E244 Provision an Optical Line Rate and Wavelength](#)" task on page 18-64.

- Step 1** Complete the "[DLP-E26 Log into CTC](#)" task on page 16-39 to log into an ONS 15600 on the network.

- Step 2** Click the **Alarms** tab:
- Verify that the alarm filter is not turned on. See the “[DLP-E157 Disable Alarm Filtering](#)” task on [page 17-46](#) as necessary.
 - Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide*.
 - Complete the “[DLP-E265 Export CTC Data](#)” task on [page 18-84](#) to export alarm and condition information.
- Step 3** In node view, double-click the ASAP card where you want to provision PPM settings.
- Step 4** Click the **Provisioning > Pluggable Port Modules** tabs.
- Step 5** In the Pluggable Port Modules pane, click **Create**. The Create PPM dialog box appears.
- Step 6** In the Create PPM dialog box, complete the following:
- PPM—Click the slot number where you want to preprovision the SFP from the drop-down list.
 - PPM Type—Click 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 menu option.
- Step 7** Click **OK**. The newly created port appears on the Pluggable Port Modules pane. The row on the Pluggable Port Modules pane turns light blue and the Actual Equipment Type column lists the preprovisioned PPM as unknown until the actual SFP is installed. After the SFP is installed, the row on the pane turns white and the column lists the equipment name.
- Step 8** Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 5 through 8.
- Step 9** Repeat steps 1 to 9 create a second PPM.
- Step 10** Click **OK**.
- Step 11** When you are ready to install the SFP, complete the “[DLP-E215 Install an SFP](#)” task on [page 18-20](#).
- Step 12** Return to your originating procedure (NTP).
-

DLP-E214 Print CTC Data

Purpose	This task prints CTC windows and CTC table data such as alarms and inventory.
Equipment/Tools	A printer must be connected to the CTC computer
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

- Step 1** From the CTC File menu, click **Print**.
- Step 2** In the Print dialog box ([Figure 18-8](#)), choose an option:
- Entire Frame—Prints the entire CTC window including the graphical view of the card, node, or network.
 - Tabbed View—Prints the lower half of the CTC window.

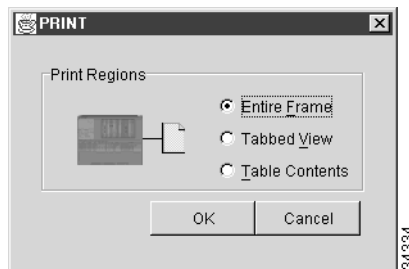
- Table Contents—Prints CTC data in table format; this option is only available for CTC table data (see the “Table Display Options” section on page A-9) so it does not apply to:
 - Provisioning > General, SNMP, and Timing windows
 - Provisioning > Network > General window
 - Provisioning > Security > Policy, Access, and Legal Disclaimer windows
 - Provisioning > OSI > Main Setup window
 - Maintenance > Database, Protection, and Diagnostic windows
 - Maintenance > Timing > Source 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 network view does not contain an Inventory or Performance tab.

Figure 18-8 **Selecting CTC Data for Print**



- Step 3** Click **OK**.
- Step 4** In the Windows Print dialog box, choose a printer and click **OK**.
- Step 5** Return to your originating procedure (NTP).

DLP-E215 Install an SFP

Purpose	This task installs SFPs into the 4PIO modules (PIMs) on the ASAP card.
Tools/Equipment	SFPs appropriate for your network
Prerequisite Procedures	DLP-E210 Install the ASAP Carrier Modules, page 18-13 DLP-E211 Install the ASAP 4PIO (PIM) Modules, page 18-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher


Note

SFPs are generically called PPMs in the CTC software interface.

-
- Step 1** Verify that the SFP is correct for your network and ASAP card. Refer to the *Cisco ONS 15600 Reference Manual* for more information.
- Step 2** Orient the SFP so that the Cisco serial number label is facing away from the shelf (to the right).
- Step 3** Unlatch (move to the left) the bail clasp before inserting it into the slot.
- Step 4** Slide the SFP into the slot and move the bail clasp to the right to secure the SFP.


Caution

Do not remove the protective caps until you are ready to attach the network fiber-optic cable.


Note

Multirate SFPs must be provisioned in CTC; single-rate PPMs do not need to be provisioned. As needed, complete the “[DLP-E243 Provision a Multirate PPM](#)” task on page 18-64 or the “[DLP-E244 Provision an Optical Line Rate and Wavelength](#)” task on page 18-64 as need to provision the line rate for an SFP.

- Step 5** Return to your originating procedure (NTP).
-

DLP-E216 Remove an SFP

Purpose	This task removes SFPs from 4PIO modules (PIMs) on the ASAP card.
Tools/Equipment	None
Prerequisite Procedures	DLP-E211 Install the ASAP 4PIO (PIM) Modules, page 18-15
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** Disconnect the network fiber cable from the SFP.
- Step 2** Release the SFP from the slot by unlatching the bail clasp and swinging it to the left.

- Step 3** Slide the SFP out of the slot.
- Step 4** As needed, complete the “[DLP-E246 Delete a PPM](#)” task on page 18-66 to delete an SFP (PPM) from CTC.
- Step 5** Return to your originating procedure (NTP).

DLP-E217 Remove a 4PIO (PIM) Module

Purpose	This procedure explains how to remove the 4PIO (PIM) in the carrier modules of the ASAP card.
Tools/Equipment	4PIO modules #2 Phillips screwdriver
Prerequisite Procedures	DLP-E211 Install the ASAP 4PIO (PIM) Modules, page 18-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Warning

During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the midplane with your hand or any metal tool, or you could shock yourself. Statement 181



Warning

Class 1 laser product.Statement 1008



Warning

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057



Caution

Always use the supplied ESD wristband when working with a powered ONS 15600. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf.



Note

For information about the ASAP card, refer to the *Cisco ONS 15600 Reference Manual*.

- Step 1** Determine in which slot on the ASAP card you want to remove the 4PIO module.
- Step 2** Use a Phillips screwdriver to loosen and remove the screws at the top right and bottom left of the 4PIO module.

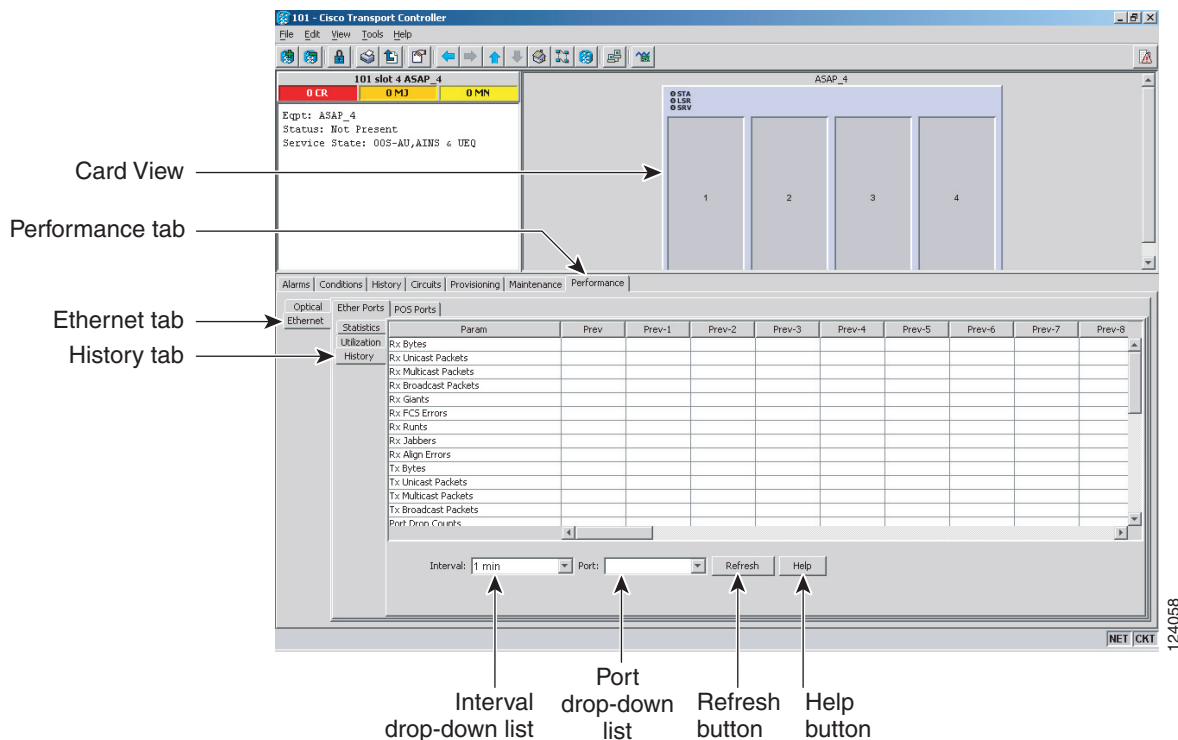
- Step 3** Carefully pull the motherboard of the module along the top and bottom guide rails out of the correct slot.
- Step 4** Log into CTC and verify that the card does not appear in CTC card view. See [Chapter 3, “Connect the Computer and Log into the GUI”](#) for CTC information and setup instructions.
- Step 5** Return to your originating procedure (NTP).

DLP-E218 View ASAP Ether Ports History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an ASAP card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

- Step 1** In node view, double-click the ASAP card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Ethernet > Ether Ports > History** tabs ([Figure 18-9](#)).

Figure 18-9 Ethernet Ether Ports History on the Card View Performance Window



- Step 3** Click **Refresh**. Performance monitoring statistics for each port on the card appear.

- Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.



Note To refresh, reset, or clear PM counts, see the “[NTP-E143 Change the PM Display](#)” procedure on [page 9-2](#).

- Step 5** Return to your originating procedure (NTP).

DLP-E219 Create a Two-Fiber BLSR Using the BLSR Wizard

Purpose	This task creates a two-fiber bidirectional line switched ring (BLSR) at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at one time.
Tools/Equipment	None
Prerequisite Procedures	E163 Provision BLSR Nodes, page 6 DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > BLSR** tabs.
- Step 3** Click **Create BLSR**.
- Step 4** In the BLSR Creation dialog box, set the BLSR properties:
- Ring Type—Choose **two-fiber**.
 - Speed—Choose the BLSR ring speed: **OC-12**, **OC-48**, or **OC-192**. The speed must match the OC-N speed of the BLSR trunk (span) ports.
 - Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string All in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
 - Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversion can be set to Never.
- Step 5** Click **Next**. If the network graphic appears, go to Step 6.
- If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with path protection selectors, a “Cannot Create BLSR” message appears. If this occurs, complete the following steps:
- a. Click **OK**.
 - b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

- c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
- d. Complete the “[NTP-E163 Provision BLSR Nodes](#)” procedure on page 5-6, making sure all steps are completed accurately, then start this procedure again.

Step 6 In the network graphic, double-click a BLSR span line. If the span line is DCC-connected to other BLSR ports that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click the span lines until a complete ring is formed. When the ring is DCC-connected, go to [Step 7](#).

Step 7 Click **Finish**. If the BLSR window appears with the BLSR you created, go to [Step 8](#). If a “Cannot Create BLSR” or “Error While Creating BLSR” message appears:

- a. Click **OK**.
- b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.
- c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
- d. Complete the “[NTP-E163 Provision BLSR Nodes](#)” procedure on page 5-6, making sure all steps are completed accurately, then start this procedure again.



Note Some or all of the following alarms might briefly appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC.

Step 8 Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15600 Troubleshooting Guide* for alarm troubleshooting.



Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15600 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the “[DLP-E223 Change a BLSR Node ID](#)” task on page 18-29.

Step 9 Return to your originating procedure (NTP).

DLP-E220 Create a Two-Fiber BLSR Manually

Purpose	This task creates a two-fiber BLSR at each BLSR-provisioned node without using the BLSR wizard.
Tools/Equipment	None
Prerequisite Procedures	NTP-E163 Provision BLSR Nodes, page 5-6 DLP-E26 Log into CTC, page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click **Create**.

Step 3 In the Suggestion dialog box, click **OK**.

Step 4 In the Create BLSR dialog box, set the BLSR properties:

- Ring Type—Choose **two-fiber**.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string All in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
- West Line—Assign the west BLSR port for the node from the drop-down list.



Note The east and west ports must match the fiber connections and DCC terminations set up in the [“NTP-E163 Provision BLSR Nodes” procedure on page 5-6](#).

- East Line—Assign the east BLSR port for the node from the drop-down list.

Step 5 Click **OK**.



Note Some or all of the following alarms will appear until all the BLSR nodes are provisioned: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

Step 6 From the View menu, choose **Go to Other Node**.

Step 7 In the Select Node dialog box, choose the next node that you want to add to the BLSR.

Step 8 Repeat Steps 1 through 7 at each node that you want to add to the BLSR. When all nodes have been added, continue with [Step 9](#).

- Step 9** From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:
- A green span line appears between all BLSR nodes.
 - All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared.
- Step 10** Return to your originating procedure (NTP).
-

DLP-E221 Create a Four-Fiber BLSR Using the BLSR Wizard

Purpose	This task creates a four-fiber BLSR at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all of the nodes at one time.
Tools/Equipment	None
Prerequisite Procedures	NTP-E163 Provision BLSR Nodes, page 5-6 DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > BLSR** tabs.
- Step 3** Click **Create BLSR**.
- Step 4** In the BLSR Creation dialog box, set the BLSR properties:
- Ring Type—Choose **four-fiber**.
 - Speed—Choose the BLSR ring speed: **OC-48** or **OC-192**. The speed must match the OC-N speed of the BLSR trunk (span) ports.
 - Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string All in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
 - Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversion can be set to Never.
 - Span Reversion—Set the amount of time that will pass before the traffic reverts to the original working path following a span switch. The default is 5 minutes. Span reversion can be set to Never.
- Step 5** Click **Next**. If the network graphic appears, go to Step 6.
- If CTC determines that a BLSR cannot be created, for example, not enough optical ports are available or it finds circuits with path protection selectors, a “Cannot Create BLSR” message appears. If this occurs, complete the following steps:
- a. Click **OK**.
 - b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

- c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
 - d. Complete the “[NTP-E163 Provision BLSR Nodes](#)” procedure on page 5-6, making sure all steps are completed accurately, then start this procedure again.
- Step 6** In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR ports that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click the span lines until a complete ring is formed. When the ring is DCC connected, go to [Step 7](#).
- Step 7** Click **Next**. In the Protect Port Selection area, choose the protect ports from the West Protect and East Protect columns.
- Step 8** Click **Finish**. If the BLSR window appears with the BLSR you created, go to [Step 9](#). If a “Cannot Create BLSR” or “Error While Creating BLSR” message appears:
- a. Click **OK**.
 - b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.
 - c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
 - d. Complete the “[NTP-E163 Provision BLSR Nodes](#)” procedure on page 5-6, making sure all steps are completed accurately, then start this procedure again.



Note Some or all of the following alarms might briefly appear during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC.

- Step 9** Verify the following:
- On the network view graphic, a green span line appears between all BLSR nodes.
 - All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15600 Troubleshooting Guide* for alarm troubleshooting.



Note The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15600 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the “[DLP-E223 Change a BLSR Node ID](#)” task on page 18-29.

- Step 10** Return to your originating procedure (NTP).
-

DLP-E222 Create a Four-Fiber BLSR Manually

Purpose	This task creates a four-fiber BLSR at each BLSR-provisioned node without using the BLSR wizard.
Tools/Equipment	None
Prerequisite Procedures	“NTP-E163 Provision BLSR Nodes” section on page 5-6 DLP-E26 Log into CTC, page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click **Create**.

Step 3 In the Suggestion dialog box, click **OK**.

Step 4 In the Create BLSR dialog box, set the BLSR properties:

- Ring Type—Choose **four-fiber**.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and uppercase and lowercase letters can be combined. Do not use the character string All in either uppercase or lowercase letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.
- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
- West Line—Assign the west BLSR port for the node from the drop-down list.



Note The east and west ports must match the fiber connections and DCC terminations set up in the [“NTP-E163 Provision BLSR Nodes” procedure on page 5-6](#).

- East Line—Assign the east BLSR port for the node from the drop-down list.
- Span Reversion—Set the amount of time that will pass before the traffic reverts to the original working path following a span reversion. The default is 5 minutes. Span reversion can be set to Never. If you set a reversion time, the times must be the same for both ends of the span. That is, if Node A’s west fiber is connected to Node B’s east port, the Node A west span reversion time must be the same as the Node B east span reversion time. To avoid reversion time mismatches, Cisco recommends that you use the same span reversion time throughout the ring.
- West Protect—Assign the west BLSR port that will connect to the west protect fiber from the drop-down list.
- East Protect—Assign the east BLSR port that will connect to the east protect fiber from the drop-down list.

Step 5 Click **OK**.



Note Some or all of the following alarms will appear until all the BLSR nodes are provisioned: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, and BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

- Step 6** From the View menu, choose **Go to Other Node**.
- Step 7** In the Select Node dialog box, choose the next node that you want to add to the BLSR.
- Step 8** Repeat Steps 1 through 7 at each node that you want to add to the BLSR. When all nodes have been added, continue with [Step 9](#).
- Step 9** From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:
- A green span line appears between all BLSR nodes.
 - All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared.
- Step 10** Return to your originating procedure (NTP).
-

DLP-E223 Change a BLSR Node ID

Purpose	This task changes a BLSR node ID.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** On the network map, double-click the node with the node ID you want to change.
- Step 3** Click the **Provisioning > BLSR** tabs.
- Step 4** Choose a Node ID number. Do not choose a number already assigned to another node in the same BLSR.
- Step 5** Click **Apply**.
- Step 6** Return to your originating procedure (NTP).
-

DLP-E224 Four-Fiber BLSR Exercise Span Test

Purpose	This task exercises a four-fiber BLSR span. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

Step 3 Click the BLSR you will exercise, then click **Edit**.

Step 4 Exercise the west span:

- a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)



Note The squares on the network map represent ports. Right-click a working port.

- b. In the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.
- c. Click **OK**. In the Confirm BLSR Operation dialog box, click **Yes**.
On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 5 Verify the conditions:

- a. Click the **Conditions** tab, then click **Retrieve**.
- b. Verify the following conditions:
 - EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
 - FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the east span of the node connected to the west side of the node where you exercised the span.
 - KB-PASSTHR—If applicable, a K Byte Pass Through Active condition is reported.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the [“DLP-E157 Disable Alarm Filtering” task on page 17-46](#) as necessary.

- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide* if necessary.

Step 7 Exercise the east span:

- a. Right-click the east port of the four-fiber BLSR node that you want to exercise and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.
- c. Click **OK**.
- d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 8 From the File menu, choose **Close**.

Step 9 Verify the conditions:

- a. Click the **Conditions** tab, then click **Retrieve**.
- b. Verify the following conditions:
 - EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
 - FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the east span of the node connected to the west side of the node where you exercised the span.
 - KB-PASSTHR—If applicable, a K Byte Pass Though Active condition is reported.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 10 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the “[DLP-E157 Disable Alarm Filtering](#)” task on [page 17-46](#) as necessary.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide* if necessary.

Step 11 From the File menu, choose **Close** to close the BLSR window.

Step 12 Return to your originating procedure (NTP).

DLP-E225 Four-Fiber BLSR Span Switching Test

Purpose	This task verifies that traffic will switch from working to protect fibers on a four-fiber BLSR span.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

Step 3 Click **Edit**. A BLSR window appears containing a graphic of the BLSR.



Note If the node icons are stacked on the BLSR graphic, press Ctrl while you drag and drop each one to a new location so you can see the BLSR port information clearly.

Step 4 Switch the west span:

- a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**.



Note The squares on the network map represent ports. Right-click a working port.

- b. In the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the protection switch. The BLSR span lines turn purple where the Force Span switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that a SPAN-SW-WEST (Span Switch West) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-EAST (Span Switch East) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the [“DLP-E157 Disable Alarm Filtering” task on page 17-46](#) as necessary.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide* if necessary.

Step 7 Display the BLSR window where you invoked the Force Span switch (the window might be hidden by the CTC window).

Step 8 Clear the west switch:

- a. Right-click the west port of the BLSR node where you invoked the Force Span switch and choose **Set West Protection Operation**.
- b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F disappears, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 9 Switch the east span:

- a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Span switch. The BLSR span lines are purple where the Force Span switch was invoked, and all span lines between other BLSR nodes are green. The span lines might take a few moments to change color.

Step 10 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that a Span Switch East (SPAN-SW-EAST) condition is reported on the node where you invoked the Force Span switch, and a Span Switch West (SPAN-SW-WEST) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off.

Step 11 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the [“DLP-E157 Disable Alarm Filtering” task on page 17-46](#) as necessary.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide* if necessary.

Step 12 Display the BLSR window where you invoked the Force Span switch (the window might be hidden by the CTC window).

Step 13 Clear the east switch:

- a. Right-click the east port of the BLSR node where you invoked the Force Span switch and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

- Step 14** From the File menu, choose **Close** to close the BLSR window.
- Step 15** Return to your originating procedure (NTP).

DLP-E226 BLSR Exercise Ring Test

Purpose	This task tests the BLSR ring functionality without switching traffic. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Provisioning > BLSR** tabs.
- Step 3** Click the row of the BLSR you will exercise, then click **Edit**.
- Step 4** Exercise the west port:
- Right-click the west port of any BLSR node and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)



Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect ports.

- In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.
 - Click **OK**.
 - In the Confirm BLSR Operation dialog box, click **Yes**.
- On the network view graphic, an E appears on the working BLSR channel where you invoked the protection switch. The E will appear for 10 to 15 seconds, then disappear.

- Step 5** Exercise the east port:
- Right-click the east port of any BLSR node and choose **Set East Protection Operation**.



Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect ports.

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


- d. In the Confirm BLSR Operation dialog box, click **Yes**.

On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

- Step 6** In the Cisco Transport Controller window, click the **History** tab. Verify that an Exercising Ring Successfully (EXERCISE-RING) condition appears for the node where you exercised the ring. Other conditions that appear include EXERCISE-RING-REQ, KB-PASSTHR, and FE-EXERCISING-RING. If you do not see any BLSR exercise conditions, click the **Filter** button and verify that filtering is not turned on. Also, check that alarms and conditions are not suppressed for a node or BLSR drop cards. See the “[NTP-E47 Suppress and Restore Alarm Reporting](#)” procedure on page 8-7 for more information.
- Step 7** Click the **Alarms** tab.
- a. Verify that the alarm filter is not on. See the “[DLP-E157 Disable Alarm Filtering](#)” task on page 17-46 for instructions.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide*.
- Step 8** From the File menu, choose **Close** to close the BLSR window.
- Step 9** Return to your originating procedure (NTP).

DLP-E227 BLSR Switch Test

Purpose	This task verifies that protection switching is working correctly in a BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC , page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > BLSR** tabs.
- Step 3** Click the row of the BLSR you will switch, then click **Edit**.
- Step 4** Initiate a Force Ring switch on the west port:
- a. Right-click any BLSR node west port and choose **Set West Protection Operation**. (To move a graphic icon, click it, then press **Ctrl** while you drag and drop it to a new location.)
-  **Note** For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect port.
- b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Ring switch. The BLSR span lines turn purple where the switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the west port:
 - **FORCE-REQ-RING**—A Force Switch Request On Ring condition is reported against the span's working slot on the west side of the node.
 - **RING-SW-EAST**—A Ring Switch Active on the east side condition is reported against the working span on the east side of the node.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

- d. Verify that the following conditions are reported on the node that is connected to the West line of the node where you performed the switch:
 - **FE-FRCDWKSWPR-RING**—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the east side of the node.
 - **RING-SW-WEST**—A Ring Switch Active on the west side condition is reported against the working span on the west side of the node.

Step 6 (Optional) If you remapped the K3 byte to run an ONS 15600 BLSR through third-party equipment, check the following condition. Verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 7 Verify the BLSR line status on each node:

- a. From the View menu, choose **Go to Node View**.
- b. Click the **Maintenance > BLSR** tabs.
- c. Verify the following:
 - The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node where you invoked the Force Ring switch.
 - The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node that is connected to the west line of the node where you invoked the Force Ring switch.
 - The line states are shown as Act/Act on both the east and west sides of the remaining nodes in the ring.

Step 8 From the View menu, choose **Go to Network View**.

Step 9 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the [“DLP-E157 Disable Alarm Filtering” task on page 17-46](#) for instructions.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide*.

Step 10 Display the BLSR window where you invoked the Force Ring switch (the window might be hidden by the CTC window).

Step 11 Clear the switch on the west port:

- a. Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set West Protection Operation**.
- b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 12 In network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.

Step 13 Verify the BLSR line status on each node:

- a. From the View menu, choose **Go to Node View**.
- a. Click the **Maintenance > BLSR** tabs.
- b. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

Step 14 Initiate a Force Ring switch on the east port:

- a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the working BLSR channel where you invoked the Force Ring switch. The BLSR span lines are purple where the Force Ring switch was invoked, and all span lines between other BLSR nodes are green. The span lines might take a few moments to change color.

Step 15 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the east port:
 - **FORCE-REQ-RING**—A Force Switch Request On Ring condition is reported against the span's working slot on the east side of the node.
 - **RING-SW-WEST**—A Ring Switch Active on the west side condition is reported against the working span on the east side of the node.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

- d. Verify that the following conditions are reported on the node that is connected to the East line of the node where you performed the switch:
 - FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the west side of the node.
 - RING-SW-EAST—A Ring Switch Active on the east side condition is reported against the working span on the west side of the node.
- Step 16** (Optional) If you remapped the K3 byte to run an ONS 15600 BLSR through third-party equipment, verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.
- Step 17** Verify the BLSR line status on each node:
- a. From the View menu, choose **Go to Node View**.
 - b. Click the **Maintenance > BLSR** tabs. Verify the following:
 - The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node where you invoked the Force Ring switch.
 - The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node that is connected to the east line of the node where you invoked the Force Ring switch.
 - The line states are shown as Act/Act on both east and west sides of the remaining nodes in the ring.
- Step 18** From the View menu, choose **Go To Network View**.
- Step 19** Click the **Alarms** tab.
- a. Verify that the alarm filter is not on. See the [“DLP-E157 Disable Alarm Filtering” task on page 17-46](#) for instructions.
 - b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide*.
- Step 20** Display the BLSR window where you invoked the Force Ring switch (the window might be hidden by the CTC window).
- Step 21** Clear the switch on the east port:
- a. Right-click the east port of the BLSR node where you invoked the Force Ring switch and choose **Set East Protection Operation**.
 - b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.
 - c. Click **OK**.
 - d. Click **Yes** in the Confirm BLSR Operation dialog box.
- On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.
- Step 22** From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.
- Step 23** Verify the BLSR line status on each node:
- a. From the View menu, choose **Go to Node View**.
 - b. Click the **Maintenance > BLSR** tabs.
 - c. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

- Step 24** From the File menu, choose **Close** to close the BLSR window.
- Step 25** Return to your originating procedure (NTP).

DLP-E228 Provision an OC-N Circuit Route

Purpose	This task provisions the circuit route for manually routed OC-N circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39 The Circuit Creation Wizard must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In the Circuit Creation wizard in the Route Review/Edit area, click the source node icon if it is not already selected.
- Step 2** Starting with a span on the source node, click the arrow of the span you want the circuit to travel. To reverse the direction of the arrow, click the arrow twice.
The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source STS appears.
- Step 3** If you want to change the source STS, adjust the Source STS field; otherwise, continue with [Step 4](#).



Note The VT option is disabled for OC-N circuits.

- Step 4** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.
- Step 5** Repeat Steps [2](#) through [4](#) until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protected Path is checked in the Circuit Routing Preferences area, you must:
- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination.
 - Add one span for all BLSR or 1+1 portions of route from the source to the destination.
 - Add primary spans for BLSR-DRI from the source to the destination through the primary nodes, and then add spans through the secondary nodes as an alternative route. The circuit map shows all span types: unprotected, BLSR, and PCA. PCA spans can only be chosen as part of the secondary path.
- Step 6** Return to your originating procedure (NTP).

DLP-E229 Initiate a BLSR Manual Ring Switch

Purpose	This task performs a BLSR Manual ring switch. A Manual ring switch will switch traffic off a span if there is no higher priority switch (Force or lock out) and no signal degrade (SD) or signal failure (SF) conditions.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher



Caution

Traffic is not protected during a manual ring protection switch.

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

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

Step 3 Choose the BLSR and click **Edit**.



Tip

To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon, and drag and drop it in a new location.

Step 4 Right-click any BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).



Note

The squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **MANUAL RING** from the drop-down list. Click **OK**.

Step 6 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Step 7 Verify that the channel (port) displays the letter “M” for Manual ring. Also verify that the span lines between the nodes where the Manual switch was invoked turn purple, and that the span lines between all other nodes turn green on the network view map. This confirms the Manual switch.

Step 8 From the File menu, choose **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-E230 Clear a BLSR Manual Ring Switch

Purpose	This task clears a manual ring switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

Step 3 Choose the BLSR and click **Edit**.



Tip To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, click an icon on the Edit BLSR network graphic and while pressing **Ctrl**, drag the icon to a new location.

Step 4 Right-click the BLSR node channel (port) where the manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.

Step 5 In the dialog box, choose **CLEAR** from the drop-down list. Click **OK**.

Step 6 Click **Yes** in the Confirm BLSR Operation dialog box. The letter “M” is removed from the channel (port) and the span turns green on the network view map.

Step 7 From the File menu, choose **Close**.

Step 8 Return to your originating procedure (NTP).

DLP-E231 Create a BLSR on a Single Node

Purpose	This task creates a BLSR on a single node. Use this task to add a node to an existing BLSR or when you delete and then recreate a BLSR temporarily on one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

Step 2 In the Suggestion dialog box, click **OK**.

Step 3 In the Create BLSR dialog box, enter the BLSR information:

- Ring Type—Enter the ring type (either 2 Fiber or 4 Fiber) of the BLSR.
- Ring Name—Enter the BLSR ring name. If the node is being added to a BLSR, use the BLSR ring name.
- Node ID—Enter the node ID. If the node is being added to a BLSR, use an ID that is not used by other BLSR nodes.
- Ring Reversion—Enter the ring reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR through the node's west line (port).
- East Line—Enter the slot on the node that will connect to the existing BLSR through the node's east line (port).

If you are adding the node to a four-fiber BLSR, complete the following for the second set of fibers:

- Span Reversion—Enter the span reversion time of the existing BLSR.
- West Line—Enter the slot on the node that will connect to the existing BLSR through the node's west line.
- East Line—Enter the slot on the node that will connect to the existing BLSR through the node's east line.

Step 4 Click **OK**.



Note The BLSR is incomplete and alarms are present until the node is connected to other BLSR nodes.

Step 5 Return to your originating procedure (NTP).

DLP-E232 Initiate a BLSR Force Ring Switch

Purpose	Use this task to perform a BLSR Force switch on a BLSR port. A Force ring switch will switch traffic off a span if there is no signal degrade (SD), signal failure (SF), or lockout switch present on the span.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher



Caution

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



Caution

Traffic is not protected during a Force protection switch.

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > BLSR** tabs. Select the BLSR.
- Step 3** Click **Edit**.
- Step 4** To apply a Force switch to the west line:
- a. Right-click the west BLSR port where you want to switch the BLSR traffic and choose **Set West Protection Operation**.



Note If node icons overlap, drag and drop the icons to a new location. You can also return to network view and change the positions of the network node icons, because BLSR node icons are based on the network view node icon positions.



Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

- b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list. Click **OK**.
- c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

- Step 5** To apply a Force switch to the east line:
- a. Right-click the east BLSR port and choose **Set East Protection Operation**.



Note If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons. BLSR node icons are based on the network view node icon positions.



Note For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working port.

- b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list. Click **OK**.
- c. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network graphic, an F appears on the working BLSR channel where you invoked the protection switch. The span lines change color to reflect the forced traffic. Green span lines indicate the new BLSR path, and the lines between the protection switch are purple.

Performing a Force switch generates several conditions including FORCED-REQ-RING and WKSWPR.

- Step 6** From the File menu, choose **Close**.
- Step 7** Return to your originating procedure (NTP).
-

DLP-E233 View Circuit Information

Purpose	This task enables you to view information about circuits, such as name, type, size, and direction.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To view circuits for an entire network, from the View menu, choose **Go To Network View**.
- To view 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 view circuits that originate, terminate, or pass through a specific card, in node view, double-click the card containing the circuits you want to view.



Note In node or card view, you can change the scope of the circuits that are displayed by choosing Card (in card view), Node, or Network from the Scope drop-down list in the bottom right corner of the Circuits window.

Step 2 Click the **Circuits** tab. The Circuits tab has the following information:

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—For the ONS 15600, the circuit type is STS (STS circuit).
- Size—VT circuit size is 1.5. STS circuit sizes can be 1, 3c, 6c, 9c, 12c, 24c, 48c, or 192c.
- OCHNC Wlen—(ONS 15454 dense wavelength division multiplexing [DWDM] only) For OCHNCs, the wavelength provisioned for the optical channel network connection. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Direction—The circuit direction, either two-way or one-way.
- OCHNC Dir—(ONS 15454 DWDM only) For OCHNCs, the direction of the optical channel network connection, either East to West or West to East. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Protection—The protection type; see [Table 18-1](#).

Table 18-1 *Circuit Protection Types*

Protection Type	Description
1+1	The circuit is protected by a 1+1 protection group.
2F BLSR	The circuit is protected by a 2-fiber BLSR.
4F BLSR	The circuit is protected by a four-fiber BLSR.
2F-PCA	The circuit is routed on a protection channel access (PCA) path on a two-fiber BLSR. PCA circuits are unprotected.
4F-PCA	The circuit is routed on a PCA path on a four-fiber BLSR. PCA circuits are unprotected.
BLSR	The circuit is protected by both a two-fiber and a four-fiber BLSR.
DRI	The circuit is protected by dual-ring interconnect (DRI).
N/A	A circuit with connections on the same node is not protected.
PCA	The circuit is routed on a PCA path on both two-fiber and four-fiber BLSRs. PCA circuits are unprotected.
Protected	The circuit is protected by diverse SONET topologies, for example a BLSR and a path protection, or a path protection and 1+1.
Unknown	A circuit has a source and destination on different nodes and communication is down between the nodes. This protection type appears if not all circuit components are known.
Unprot (black)	A circuit with a source and destination on different nodes is not protected.
Unprot (red)	A circuit created as a fully protected circuit is no longer protected due to a system change, such as removal of a BLSR or 1+1 protection group.
Path Protection	The circuit is protected by a path protection.

- Status—The circuit status. [Table 18-2](#) lists the circuit statuses that can appear.

Table 18-2 *ONS 15600 Circuit Status*

Status	Definition/Activity
CREATING	CTC is creating a circuit.
DISCOVERED	CTC created a circuit. All components are in place and a complete path exists from circuit source to destination.
DELETING	CTC is deleting a circuit.

Table 18-2 ONS 15600 Circuit Status (continued)

Status	Definition/Activity
PARTIAL	<p>A CTC-created circuit is missing a connection or circuit span (network link), a complete path from source to destination(s) does not exist, or a MAC address change occurred on one of the circuit nodes and the circuit is in need of repair (in the ONS 15454, the MAC address resides on the alarm interface panel (AIP); in the ONS 15600, the MAC address resides on the backplane EEPROM).</p> <p>In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is PARTIAL. However, a PARTIAL status does not necessarily mean a circuit traffic failure has occurred, because traffic might flow on a protect path.</p> <p>Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans appear as green lines, and down spans appear as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray to indicate that the span is down. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line does not appear on the network map.</p> <p>Subsequently, circuits routed on a network span that goes down appear as DISCOVERED during the current CTC session, but appear as PARTIAL to users who log in after the span failure.</p>
DISCOVERED_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is complete. A complete path from source to destination(s) exists.
PARTIAL_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is missing a cross-connect or circuit span (network link), and a complete path from source to destination(s) does not exist.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this status. The circuit returns to the DISCOVERED status when the topology upgrade is complete. For more information about topology upgrades, refer to the <i>Cisco ONS 15600 Reference Manual</i> .
PENDING_MERGE	Any new circuits created to represent an alternate path in a topology upgrade are set to this status to indicate that it is a temporary circuit. These circuits can be deleted if a topology upgrade fails. For more information about topology upgrades, refer to the <i>Cisco ONS 15600 Reference Manual</i> .
ROLL_PENDING	Roll is awaiting completion or cancellation. When a roll is in the ROLL PENDING state, you can complete a manual roll and cancel an automatic or manual roll.

- **Source**—The circuit source in the format: *node/slot/port/STS*. If an ASAP PPM port is the circuit source, the port format is *PIM-PPM-port*, where PIM and PPM values are 1 through 4 (for example, p1-1-1). PPMs have only one port.
- **Destination**—The circuit destination in the format: *node/slot/port/STS*. If an ASAP PPM port is the circuit destination, the port format is *PIM-PPM-port*, where PIM and PPM values are 1 through 4 (for example, p1-1-1). PPMs have only one port.
- **# of VLANs**—(Future use) The number of VLANs used by an Ethernet circuit.
- **# of Spans**—The number of internode links that compose the circuit.
- **State**—The circuit service state, In-Service (IS), Out-of-Service (OOS), or OOS-PARTIAL. The circuit service state is an aggregate of the service states of its cross-connects:
 - **IS**—All cross-connects are in the In-Service and Normal (IS-NR) service state.
 - **OOS**—All cross-connects are in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) and/or Out-of-Service and Management, Maintenance (OOS-MA,MT) service state.
 - **OOS-PARTIAL**—At least one cross-connect is IS-NR and others are OOS-MA,DSBLD and/or OOS-MA,MT. The OOS-PARTIAL state can occur during automatic or manual transitions between states. OOS-PARTIAL can appear during a manual transition caused by an abnormal event such as a CTC crash or communication error, or if one of the cross-connects could not be changed. Refer to the *Cisco ONS 15600 Troubleshooting Guide* for troubleshooting procedures.

Step 3 Return to your originating procedure (NTP).

DLP-E234 Install Fiber-Optic Cables for BLSR Configurations

Purpose	This task installs the fiber-optics to the east and west BLSR ports at each node. See Chapter 5, “Turn Up Network” to provision and test BLSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-E11 Install the OC-N Cards, page 2-4 NTP-E77 Clean Fiber Connectors and Adapters, page 14-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Caution

Do not provision the BLSR east and west ports on the same OC-N card.



Note

To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.



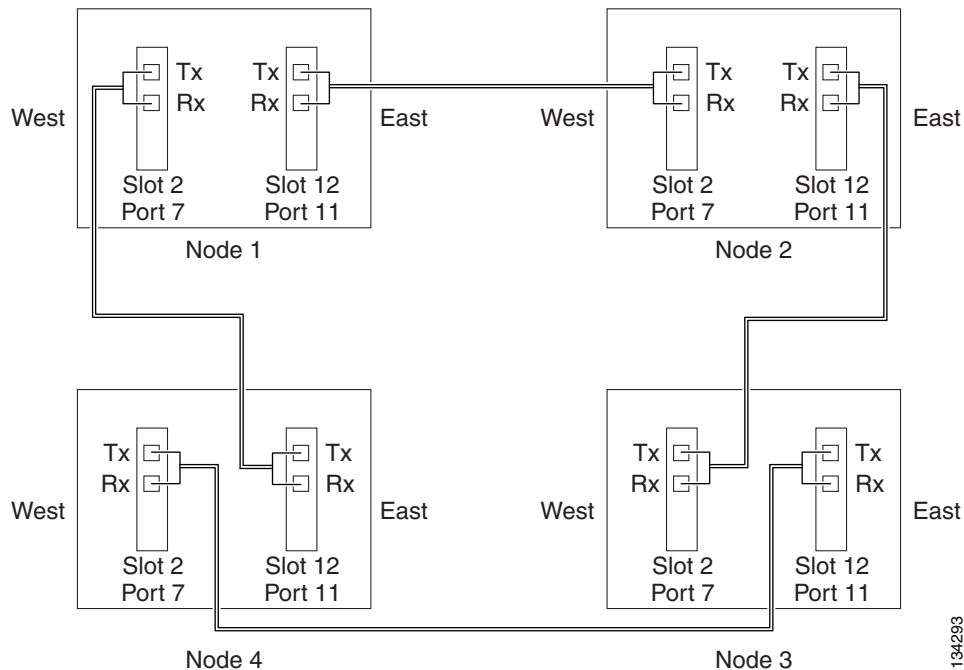
Note

See [Table 16-1 on page 16-23](#) and [Table 16-2 on page 16-24](#) for OGI connector pinouts of OC-N cards.

- Step 1** Plan your fiber connections. Use the same plan for all BLSR nodes. BLSR configuration is achieved by correctly cabling the transmit and receive fibers of each node to the others.
- Step 2** Plug the fiber into the Tx connector of an OC-N port at one node and plug the other end into the Rx connector of an OC-N port at the adjacent node. The card displays a SF LED if the transmit and receive fibers are mismatched.
- Step 3** Repeat [Step 2](#) until you have configured the ring.

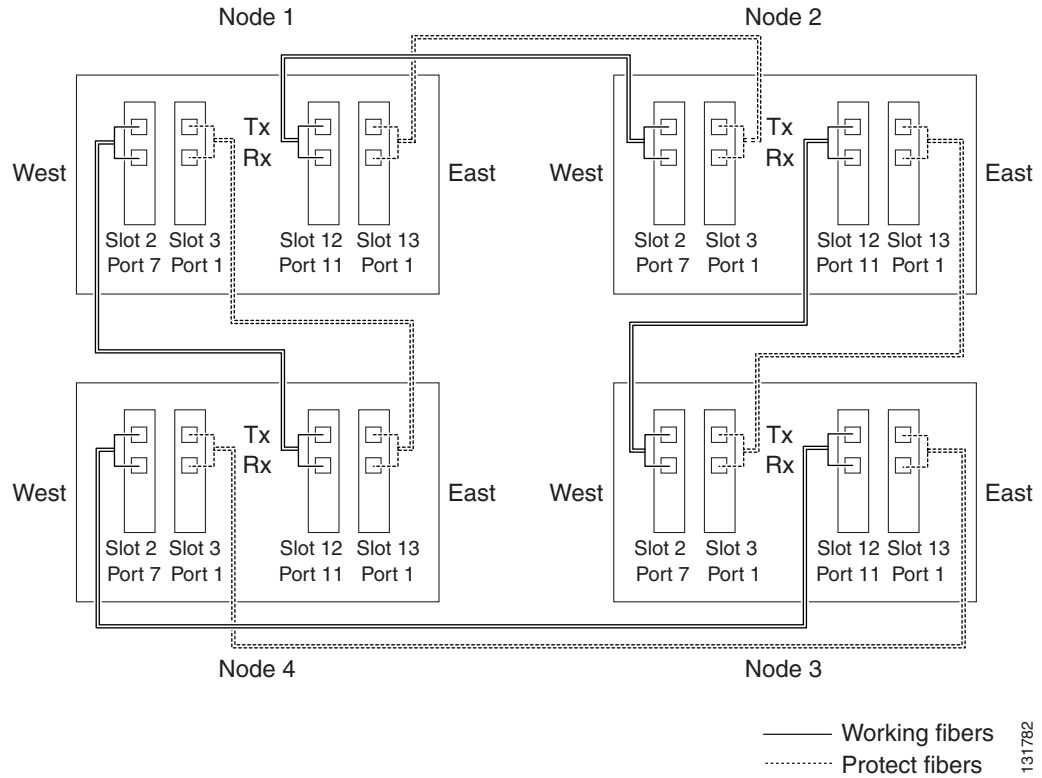
[Figure 18-10](#) shows fiber connections for a two-fiber BLSR with trunk ports in Slot 2, Port 7 (west) and Slot 12, Port 11 (east).

Figure 18-10 Connecting Fiber to a Four-Node, Two-Fiber BLSR



[Figure 18-11](#) shows fiber connections for a four-fiber BLSR. Slot 2, Port 7 (west) and Slot 12, Port 11 (east) carry the working traffic. Slot 3, Port 1 (west) and Slot 13, Port 1 (east) carry the protect traffic.

Figure 18-11 Connecting Fiber to a Four-Node, Four-Fiber BLSR



Note To provision a BLSR, see [Chapter 5, “Turn Up Network.”](#)

Step 4 Return to your originating procedure (NTP).

DLP-E235 Delete a BLSR from a Single Node

Purpose	This task deletes a BLSR from a node after you remove the node from the BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, display the node that was removed from the BLSR:

- If the node that was removed is connected to the same LAN as your computer, from the File menu, choose **Add Node**, then enter the node name or IP address.

- If the node that was removed is not connected to the same LAN as your computer, you must connect to the node using a direct connection. See [Chapter 3, “Connect the Computer and Log into the GUI”](#) for procedures.

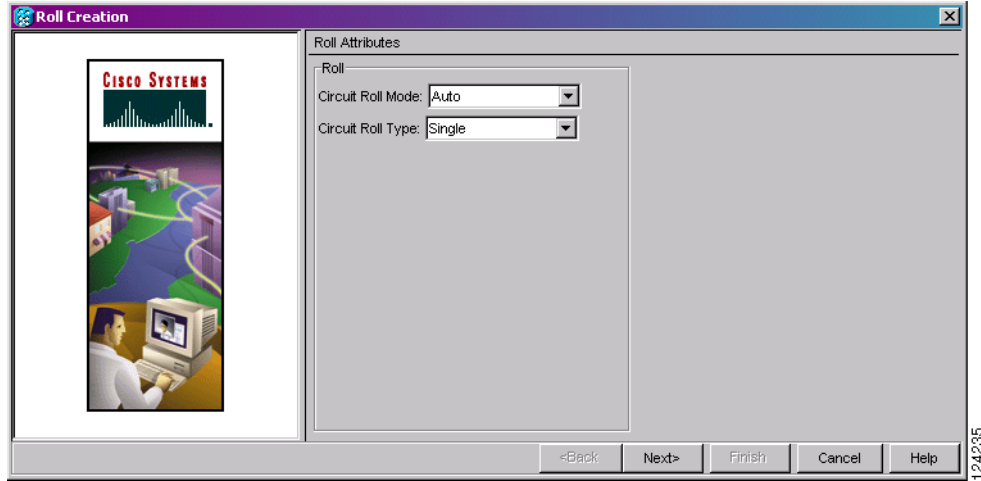
- Step 2** Click the **Provisioning > BLSR** tabs.
- Step 3** Highlight the ring and click **Delete**.
- Step 4** In the Suggestion dialog box, click **OK**.
- Step 5** In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.
- Step 6** Return to your originating procedure (NTP).
-

DLP-E236 Roll the Source or Destination of One Optical Circuit

Purpose	This task reroutes traffic from one source or destination to another on the same circuit, thus changing the original source or destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Circuits** tab.
- Step 3** Click the circuit that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.
- Step 4** From the Tools menu, choose **Circuits > Roll Circuit**.
- Step 5** In the Roll Attributes area, complete the following ([Figure 18-12](#)):
- From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for a 1-way destination roll).
 - From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll one cross-connect on the chosen circuit.

Figure 18-12 Selecting Single Roll Attributes

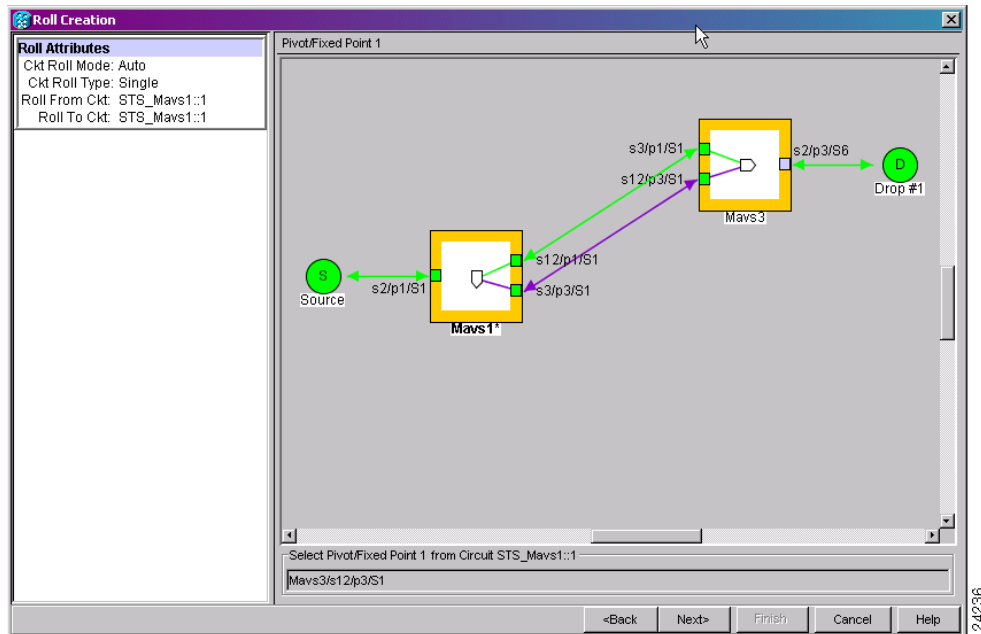


Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square in the graphic image that represents the facility that you want to keep (Figure 18-13).

This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

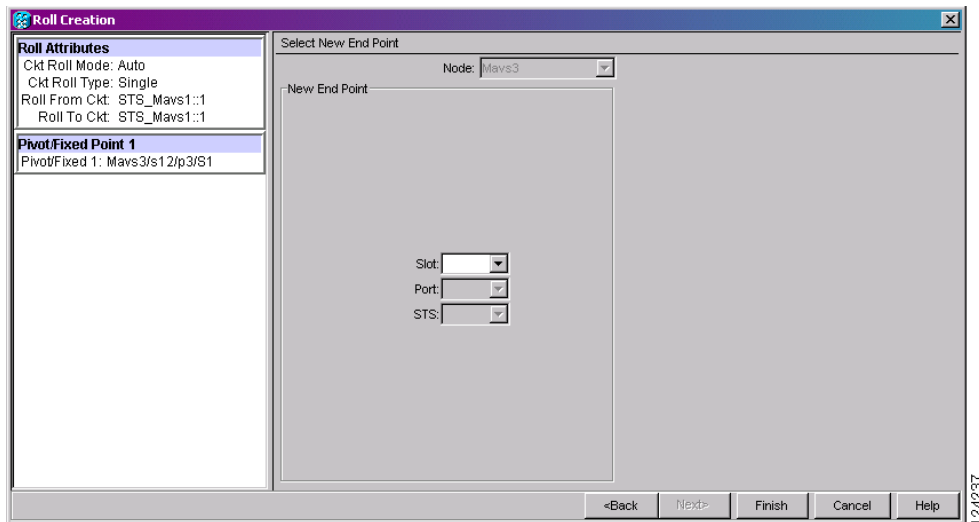
Figure 18-13 Selecting a Path



Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **STS** from the drop-down lists to select the Roll To facility (Figure 18-14).

Figure 18-14 Selecting a New Endpoint



Step 10 Click **Finish**. On the Circuits tab, the circuit status for the Roll From port changes from DISCOVERED to ROLL_PENDING.

Step 11 Click the **Rolls** tab (Figure 18-15). For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the “Circuits and Timing” section in the General Troubleshooting chapter of the *Cisco ONS 15600 Troubleshooting Guide*. To cancel the roll, see the “DLP-E242 Cancel a Roll” task on page 18-63.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.



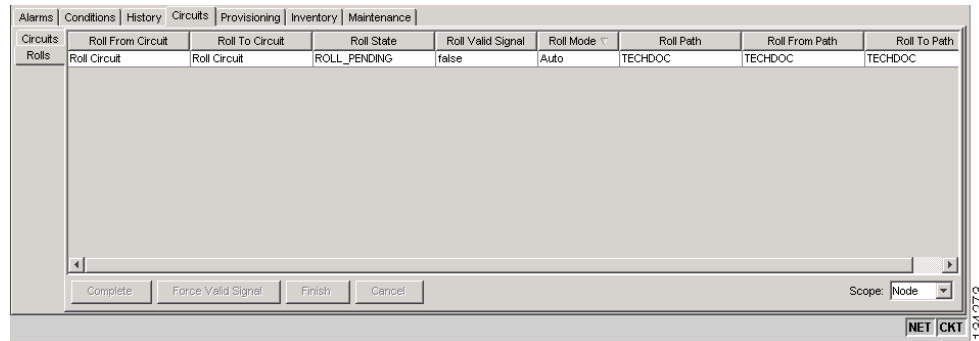
Note You cannot cancel an automatic roll after a valid signal is found.

- You can force a signal onto the Roll To circuit by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll might drop depending on conditions at the other end of the circuit when the roll is completed. You must force a signal if the circuits do not have a signal or have a bad signal and you want to complete the roll.



Note For a one-way destination roll in manual mode, you do not need to force the valid signal.

Figure 18-15 Viewing the Rolls Tab



- Step 12** If you selected Manual in [Step 5](#), click the rolled facility on the Rolls tab and then click **Complete**. If you selected Auto, continue with [Step 13](#).
- Step 13** For both Manual and Auto rolls, click **Finish** to complete the circuit roll process. The roll clears from the Rolls tab and the rolled circuit now appears on the Circuits tab in the DISCOVERED status.
- Step 14** Return to your originating procedure (NTP).

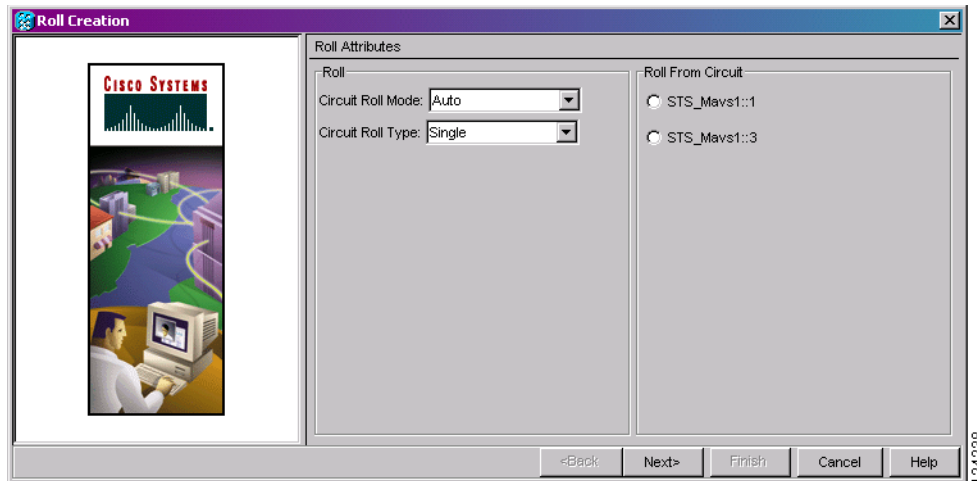
DLP-E237 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a cross-connect on one circuit onto another circuit resulting in a new destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39 DLP-E114 Provision Section DCC Terminations, page 17-14 for the ports involved in the roll
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Circuits** tab.
- Step 3** Press **Ctrl** and click the two circuits that you want to use in the roll process.
The circuits must have a DISCOVERED status; in addition, they must be the same size and direction for you to start a roll. The planned Roll To circuit must not carry traffic. The Roll To facility should be DCC connected to the source node of the Roll To circuit.
- Step 4** From the Tools menu, choose **Circuits > Roll Circuit**.
- Step 5** In the Roll Attributes area, complete the following ([Figure 18-16](#)):
- From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

- b. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll a single connection from the Roll From circuit to the Roll To circuit.
- c. In the Roll From Circuit area, click the circuit that contains the Roll From connection.

Figure 18-16 Selecting Roll Attributes for a Single Roll onto a Second Circuit



Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the facility that you want to keep ([Figure 18-13](#) on [page 18-51](#)).

This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **STS** from the drop-down lists to identify the Roll To facility on the connection being rolled.

Step 10 Click **Finish**.

The statuses of the Roll From and Roll To circuits change from DISCOVERED to ROLL_PENDING in the Circuits tab.

Step 11 Click the **Rolls** tab. For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with [Step 12](#).

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the “Circuits and Timing” section in the General Troubleshooting chapter of the *Cisco ONS 15600 Troubleshooting Guide*. To cancel the roll, see the “[DLP-E242 Cancel a Roll](#)” task on [page 18-63](#).
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a “true” Roll Valid Signal status for a one-way destination roll.



Note You cannot cancel an automatic roll after a valid signal is found.

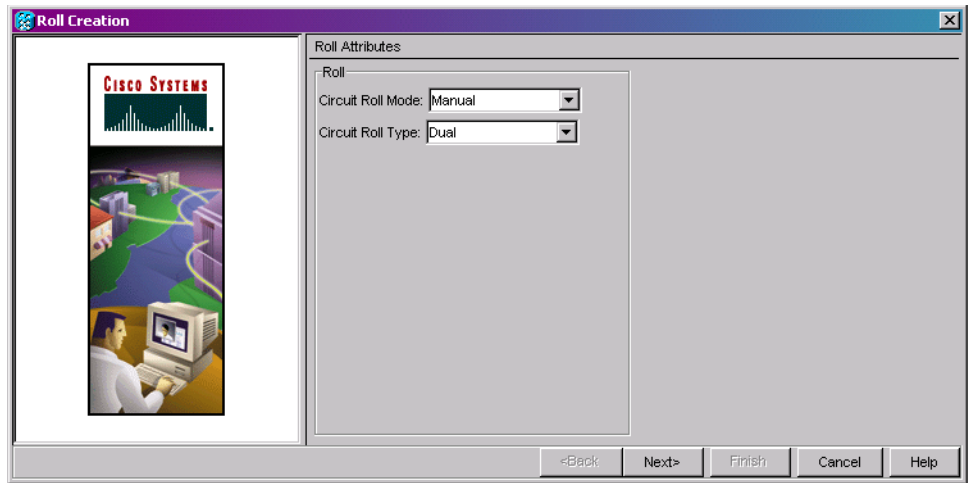
- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped once the roll is completed.
- Step 12** If you selected Manual in [Step 5](#), click the roll on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with [Step 13](#).
- Step 13** For both manual and automatic rolls, click **Finish** to complete the circuit roll process. The roll is cleared from the Rolls tab and the new rolled circuit on Circuits tab returns to the DISCOVERED status.
- Step 14** Return to your originating procedure (NTP).
-

DLP-E238 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing

Purpose	This task reroutes the network path while maintaining the same source and destination. This task allows CTC to automatically select a Roll To path.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Circuits tab**.
- Step 3** Click the circuit that has the connections that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.
- Step 4** From the Tools menu, choose **Circuits > Roll Circuit**.
- Step 5** In the Roll Attributes area, complete the following ([Figure 18-17](#)):
- a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.
 - b. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Figure 18-17 Selecting Dual Roll Attributes



Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first connection to be rolled (Figure 18-13 on page 18-51).

This path is a fixed point in the cross connection involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**.
- If multiple Roll From paths do not exist, continue with [Step 10](#). The circuit status for the Roll To path changes states from DISCOVERED to ROLL_PENDING.

Step 10 In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.

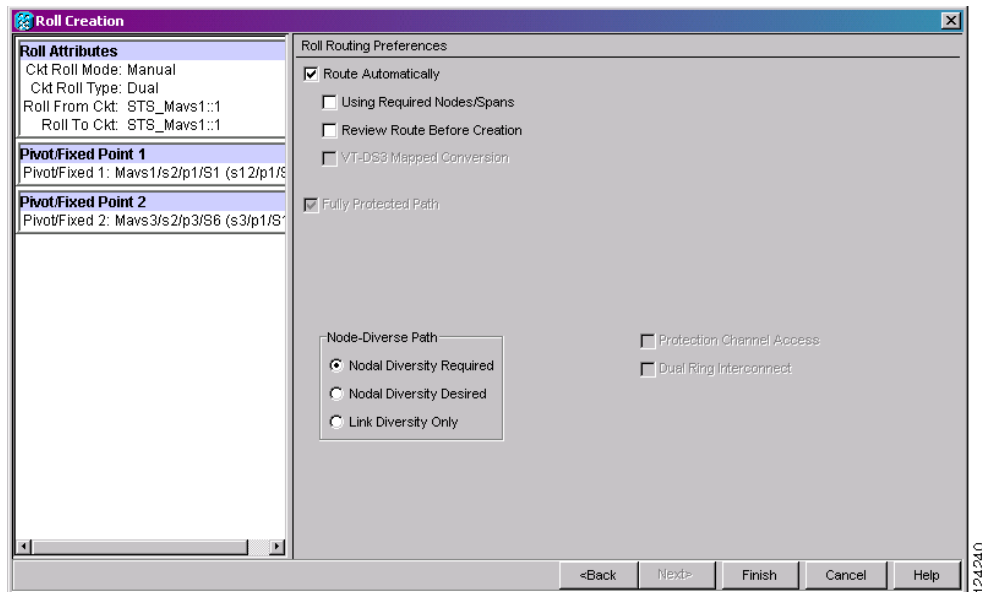
The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, check **Route Automatically** to allow CTC to find the route (Figure 18-18). If you check Route Automatically, the following options are available:

- Using Required Nodes/Spans—If checked, you can specify nodes and spans to include or exclude in the CTC-generated circuit route in [Step 15](#).
- Review Route Before Creation—If checked, you can review and edit the circuit route before the circuit is created.

Figure 18-18 Setting Roll Routing Preferences



- Step 13** To route the circuit over a protected path, check **Fully Protected Path**. (If you do not want to route the circuit on a protected path, continue with [Step 14](#).) CTC creates a primary and alternate circuit route (virtual path protection) based on the following nodal diversity options. Select one of the following choices and follow subsequent window prompts to complete the routing:
- **Nodal Diversity Required**—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse.
 - **Nodal Diversity Desired**—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.
 - **Link Diversity Only**—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.
- Step 14** If you checked Route Automatically in [Step 12](#):
- If you checked Using Required Nodes/Spans, continue with [Step 15](#).
 - If you checked only Review Route Before Creation, continue with [Step 16](#).
 - If you did not check Using Required Nodes/Spans or Review Route Before Creation, continue with [Step 17](#).
- Step 15** If you checked Using Required Nodes/Spans in [Step 12](#):
- a. In the Roll Route Constraints area, click a node or span on the circuit map.
 - b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node/span from the circuit. The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction.
 - c. Repeat [Step b](#) for each node or span you wish to include or exclude.
 - d. Review the circuit route. To change the circuit routing order, select a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 If you checked Review Route Before Creation in [Step 12](#):

- a. In the Roll Route Review and Edit area, review the circuit route. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.
- b. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

Step 17 Click **Finish**.

In the Circuits tab, verify that a new circuit appears. This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.

Step 18 Click the **Rolls** tab. Two new rolls now appear. For each pending roll, view the Roll Valid Signal status. When one of the following requirements is met, continue with [Step 19](#).

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If a valid signal is not found, refer to the *Cisco ONS 15600 Troubleshooting Guide*. To cancel the roll, see the “[DLP-E242 Cancel a Roll](#)” task on page 18-63.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.



Note If you have completed a roll, you cannot cancel the sibling roll. You must cancel the two rolls together.



Note You cannot cancel an automatic roll after a valid signal is found.

- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped once the roll is completed.

Step 19 If you selected Manual in [Step 5](#), click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with [Step 20](#).



Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.



Step 20 For both manual and automatic rolls, click **Finish** to complete circuit roll process.

Step 21 Return to your originating procedure (NTP).

DLP-E239 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing

Purpose	This task reroutes a network path of an optical circuit using manual routing.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

-
- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Circuits** tab.
- Step 3** Click the circuit that you want to roll to a new path. The circuit must have a DISCOVERED status for you to start a roll.
- Step 4** From the Tools menu, choose **Circuits > Roll Circuit**.
- Step 5** In the Roll Attributes area, complete the following ([Figure 18-17 on page 18-56](#)):
- From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.
 - From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.
- Step 6** Click **Next**.
- Step 7** In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled ([Figure 18-13 on page 18-51](#)).
- This path is a fixed point in the cross-connect involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.
- Step 8** Click **Next**.
- Step 9** Complete one of the following:
- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**, then click **Next** ([Figure 18-18 on page 18-57](#)).
 - If multiple Roll From paths do not exist, click **Next** and continue with [Step 10](#). The circuit status for the Roll From path changes from DISCOVERED to ROLL_PENDING.
- Step 10** In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.
- The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is complete. The path identifier appears in the text box below the graphic image.
- Step 11** Click **Next**.
- Step 12** In the Circuit Routing Preferences area, uncheck **Route Automatically**.

- Step 13** Set the circuit path protection:
- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with [Step 14](#).
 - To create an unprotected circuit, uncheck **Fully Protected Path** and continue with [Step 15](#).
- Step 14** If you checked Fully Protected Path, choose one of the following:
- **Nodal Diversity Required**—Ensures that the primary and alternate paths within the path protection portions of the complete circuit path are nodally diverse.
 - **Nodal Diversity Desired**—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
 - **Link Diversity Only**—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.
- Step 15** Click **Next**. Beneath Route Review and Edit, node icons appear for you to route the circuit manually. The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.
- Step 16** Complete the “[DLP-E228 Provision an OC-N Circuit Route](#)” task on page 18-39.
- Step 17** Click **Finish**. In the Circuits tab, verify that a new circuit appears.
- This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.
- Step 18** Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with [Step 19](#).
- If the Roll Valid Signal status is true, a valid signal was found on the new port.
 - If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the “Circuits and Timing” section in the General Troubleshooting chapter of the *Cisco ONS 15600 Troubleshooting Guide*. To cancel the roll, see the “[DLP-E242 Cancel a Roll](#)” task on page 18-63.
 - The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.
-  **Note** You cannot cancel an automatic roll after a valid signal is found.
- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped once the roll is completed.
- Step 19** If you selected Manual in [Step 5](#), click each roll and click **Complete** to route the traffic to the new port. If you selected Auto, continue with [Step 20](#).
-  **Note** You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.
- Step 20** For both manual and automatic rolls, click **Finish** to complete the circuit roll process.
- Step 21** Return to your originating procedure (NTP).

DLP-E240 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a network path using two optical circuits by allowing CTC to select the Roll To path on the second circuit automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

-
- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Circuits** tab.
- Step 3** Press **Ctrl** and click the two circuits that you want to use in the roll process.
- The Roll From path will be on one circuit and the Roll To path will be on the other circuit. The circuits must have a DISCOVERED status and must be the same size and direction for you to start a roll. The planned Roll To circuit must not carry traffic. The first Roll To path must be DCC connected to the source node of the Roll To circuit, and the second Roll To path must be DCC connected to the destination node of the Roll To circuit.
- Step 4** From the Tools menu, choose **Circuits > Roll Circuit**.
- Step 5** In the Roll Attributes area, complete the following:
- From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).
 - From the Circuit Roll Type drop-down list, choose **Dual**.
 - In the Roll From Circuit area, click the circuit that contains the Roll From path.
- Step 6** Click **Next**.
- Step 7** In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled ([Figure 18-13 on page 18-51](#)).
- This path is a fixed point in the cross-connect involved in the roll process. The path identifier appears in the text box below the graphic image. The path that is not selected contains the Roll From path. The Roll From path is deleted after the roll is completed.
- Step 8** Click **Next**.
- Step 9** Complete one of the following:
- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK** ([Figure 18-18 on page 18-57](#)).
 - If multiple Roll From paths do not exist, continue with [Step 10](#).
- The circuit status for the Roll From path changes from DISCOVERED to ROLL PENDING.
- Step 10** In the Pivot/Fixed Point 2 window, click the square that represents the fixed path of the second connection to be rolled.
- The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

- Step 11** Click **Next**.
- Step 12** Click **Finish**. In the Circuits tab, the Roll From and Roll To circuits change from the DISCOVERED status to ROLL RENDING.
- Step 13** Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with [Step 14](#).
- If the Roll Valid Signal status is true, a valid signal was found on the new port.
 - If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If the signal is not found, refer to the “Circuits and Timing” section in the General Troubleshooting chapter of the *Cisco ONS 15600 Troubleshooting Guide*. To cancel the roll, see the “[DLP-E242 Cancel a Roll](#)” task on page 18-63.
 - The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.



Note You cannot cancel an automatic roll after a valid signal is found.

- A roll can be forced onto the Roll To Circuit destination without a valid signal by using the Force Valid Signal button. If you choose Force Valid Signal, traffic on the circuit that is involved in the roll will be dropped once the roll is completed.
- Step 14** If you selected Manual in [Step 5](#), click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with [Step 15](#).



Note You cannot complete a roll if you cancelled the sibling roll. You must complete the two rolls together.

- Step 15** For both manual and automatic rolls, click **Finish** to complete the circuit roll process.
- Step 16** Return to your originating procedure (NTP).
-

DLP-E241 Delete a Roll

Purpose	This task deletes a roll. Use caution when selecting this option, traffic may be affected. Delete a roll only if it cannot be completed or cancelled in normal ways. Circuits may have a PARTIAL status when this option is selected. See Table 18-2 on page 18-45 for a description of circuit statuses.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC , page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Circuits > Rolls** tabs.

- Step 3** Click the rolled circuit that you want to delete.
- Step 4** From the Tools menu, choose **Circuits > Delete Rolls**.
- Step 5** In the confirmation dialog box, click **Yes**.
- Step 6** Return to your originating procedure (NTP).
-

DLP-E242 Cancel a Roll

Purpose	This task cancels a roll. When the roll mode is Manual, you can only cancel a roll before you click the Complete button. When the roll mode is Auto, cancel roll is only allowed before a good signal is detected by the node or before clicking the Force Valid Signal button. A dual or single roll can be cancelled before the roll state changes to ROLL_COMPLETED.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39 NTP-E55 Bridge and Roll Traffic, page 7-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

If you click cancel while performing a Dual roll in Manual mode and have a valid signal detected on both rolls, you will see a dialog box stating that this can cause a traffic hit and asking if you want to continue with the cancellation. Cisco does not recommend cancelling a dual roll once a valid signal has been detected. To return the circuit to the original state, Cisco recommends completing the roll, then using bridge and roll again to roll the circuit back.

- Step 1** From the node or network view, click the **Circuits > Rolls** tabs.
- Step 2** Click the rolled circuit that you want to cancel.
- Step 3** Click **Cancel**.
- Step 4** Return to your originating procedure (NTP).
-

DLP-E243 Provision a Multirate PPM

Purpose	This task provisions multirate PPMs in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, double-click the ASAP card where you want to provision PPM settings.
- Step 2** Click the **Provisioning > Pluggable Port Modules** tabs.
- Step 3** In the Pluggable Port Modules area, click **Create**. The Create PPM dialog box appears.
- Step 4** In the Create PPM dialog box, complete the following:
- PPM—Click the slot number where the SFP is installed from the drop-down list.
 - PPM Type—Click 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.
- Step 5** Click **OK**. The newly created port appears in the Pluggable Port Modules area. The row on the Pluggable Port Modules area turns light blue if the PPM is provisioned strictly as an optical PPM, or green if it is provisioned as a DWDM PPM. The Actual Equipment Type column lists the equipment name.
- Step 6** Verify that the PPM appears in the list in the Pluggable Port Modules area. If it does not, repeat Steps 3 through 5.
- Step 7** Repeat the task to provision a second PPM.
- Step 8** Click **OK**.
- Step 9** Continue with the “[DLP-E244 Provision an Optical Line Rate and Wavelength](#)” task on page 18-64 to provision the line rate.
- Step 10** Return to your originating procedure (NTP).
-

DLP-E244 Provision an Optical Line Rate and Wavelength

Purpose	This task provisions the line rate and wavelength of a multirate PPM. Single-rate SFPs or 4PIOs/PIMs do not need line rate provisioning.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In node view, double-click the ASAP card where you want to provision the line rate.
- Step 2** Click the **Provisioning > Pluggable Port Modules** tabs.

Step 3 In the Pluggable Ports area, click **Create**. The Create Port dialog box appears.

Step 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 with one port displays as 1-1 and the second PPM with one port displays as 2-1. When a 4PIO (PIM) is present on an ASAP card, the port is identified as *PIM#-PPM#-Port#* (for example 4-4-1). The PIM number can be 1 to 4, the PPM number can be 1 to 4, but the port number is always 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 18-3](#) for definitions of the supported rates on the ASAP card.

Table 18-3 PPM Port Types

Card	Port Type
ASAP	<ul style="list-style-type: none"> • OC-3—155 Mbps • OC-12—622 Mbps • OC-48—2.48 Gbps • ETHER—10 Gbps Ethernet

Step 5 Click **OK**.

Step 6 Click the **Provisioning > Optical > Line** tabs.

Step 7 Find the port where you want to set the wavelength frequency of the PPM.

Step 8 In the Wavelength drop-down box, select the desired frequency. See [Table 10-1 on page 10-3](#) for definitions of the supported wavelengths on the ASAP card. The supported wavelengths depend on whether the PPM is used for dense wavelength division multiplexing (DWDM).

Step 9 Click **OK**.

Step 10 Repeat Steps 3 through 9 to configure the PPM port rates and wavelengths as needed.

Step 11 Click **OK**. The row on the Pluggable Ports area turns light blue until the actual SFP is installed and then the row turns white.

Step 12 Return to your originating procedure (NTP).

DLP-E245 Change the Optical Line Rate

Purpose	This task changes PPM port rates for the ASAP card. Perform this procedure if you want to change the port rate on a multirate SFP that is already provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

DLP-E246 Delete a PPM

Purpose	This task deletes PPM provisioning for SFPs on the ASAP card.
Tools/Equipment	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** Determine if you can delete the PPM. 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 task:
- [NTP-E61 Modify or Delete Optical 1+1 Port Protection Settings, page 11-4](#)
 - [NTP-E62 Change Node Timing, page 11-5](#)
 - [NTP-E128 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 11-8](#)
 - [NTP-E52 Modify and Delete Circuits, page 7-2](#)
 - [NTP-E134 Modify and Delete Overhead Circuits, page 7-3](#)
 - [DLP-E115 Change the Service State for a Port, page 17-16](#)

- Step 2** In node view, double-click the ASAP card where you want to delete PPM settings.
- Step 3** Click the **Provisioning > Pluggable Port Modules** tabs.
- Step 4** To delete a PPM and the associated ports:
- Click the PPM line that appears in the Pluggable Port Modules area. The highlight changes to dark blue.
 - Click **Delete**. The Delete PPM dialog box appears.
 - Click **Yes**. The PPM provisioning is removed from the Pluggable Port Modules area and the Pluggable Ports area.
- Step 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 or 4PIO (PIM) 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 or PIM can be provisioned again in CTC, or the equipment can be removed, in which case the removal causes the graphic to disappear.
- Step 6** If you need to remove the SFP, see the [“DLP-E216 Remove an SFP” procedure on page 18-20](#). If you need to remove the 4PIO, see the [“DLP-E217 Remove a 4PIO \(PIM\) Module” procedure on page 18-21](#).
- Step 7** Return to your originating procedure (NTP).

DLP-E247 Provision OSI Routing Mode

Purpose	This task provisions the Open System Interconnection (OSI) routing mode. Complete this task when the ONS 15600 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	NTP-E21 Verify Card Installation, page 4-2
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 IS Level 1 or an Intermediate System (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 *ONS 15600 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 15600s, twelve 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.

- Step 1** Complete the “[DLP-E26 Log into CTC](#)” task on page 16-39 at the node where you want to provision the OSI routing mode. If you are already logged in, continue with Step 2.
- Step 2** In node view, click the **Provisioning > OSI** tabs.
- Step 3** Choose a routing mode:
- **Intermediate System Level 1**—The ONS 15600 performs OSI IS functions. It communicates with IS and End System (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 15600 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.
- Step 4** If needed, change the LSP data buffers:
- **L1 LSP Buffer Size**—Adjusts the Level 1 link state 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.
- Step 5** Return to your originating procedure (NTP).

DLP-E248 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-E26 Log into CTC , page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

- Step 1** In node view, click the **Provisioning > OSI > TARP > Config** tabs.

Step 2 Provision the following parameters, as needed:

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



Note This parameter is not used when the Node Routing Area (Provisioning > OSI > Main Setup tab) is set to End System.

- TARP PDUs L2 Propagation—If checked (default), TARP Type 2 PDUs received by the node that are not excluded by the LDB are propagated to other NEs within the Level 2 OSI areas. (Type 2 PDUs request a protocol address that matches a TID within a Level 2 routing area.) The propagation 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 This parameter is only used when the Node Routing Area is provisioned to Intermediate System Level 1/Level 2.

- TARP PDUs Origination—If checked (default), the node performs all TARP origination functions including:
 - TID to 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 This parameter is only used when the TARP PDUs Origination parameter is enabled.

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



Note This parameter is designed for Intermediate System Level 1/Level 2 nodes that are connected to other Intermediate System Level 1/Level 2 nodes. Enabling the parameter for Intermediate System Level 1 nodes is not recommended.

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



Note The 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 15600 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 Timers T1, T2, and T4 are not used if TARP PDUs Origination is not enabled.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-E249 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-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

-
- Step 1** In node view, click the **Provisioning > OSI > TARP > Static TDC** tabs.
- Step 2** Click **Add Static Entry**.
- Step 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.
- Step 4** Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.
- Step 5** Return to your originating procedure (NTP).
-

DLP-E250 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-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioner or higher

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

DLP-E251 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 15600 must communicate across routers or non-SONET NEs that lack TARP capability.
Tools/Equipment	None
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In the node view, click the **Provisioning > OSI > TARP > MAT** tabs.
- Step 2** Click **Add**.
- Step 3** In the Add TARP Manual Adjacency Table Entry dialog box, enter the following:
- **Level**—Sets the TARP Type Code that will be sent:
 - **Level 1**—Indicates that the adjacency is within the same area as the current node. The entry generates Type 1 PDUs.
 - **Level 2**—Indicates that the adjacency is in a different area 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.
- Step 4** Click **OK** to close the Masked NSAP Entry dialog box, if used, and then click **OK** to close the Add Static Entry dialog box.
- Step 5** Return to your originating procedure (NTP).
-

DLP-E252 Provision OSI Routers

Purpose	This task enables an OSI router and edits its primary manual area address.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
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 through 12.



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 through 12 are created by adding 1 through 12 respectively to the Router 1 System ID. You cannot edit the System IDs.

-
- Step 1** Complete the “[DLP-E26 Log into CTC](#)” task on page 16-39 at the node of the OSI routers that you want to provision.
- Step 2** Click the **Provisioning > OSI > Routers > Setup** tabs.
- Step 3** Chose the router you want provision and click **Edit**. The OSI Router Editor dialog box appears.
- Step 4** In the OSI Router Editor dialog box:
- a. Check **Enable Router** to enable the router and make its primary area address available for editing.
 - b. Click the manual area address, then click **Edit**.
 - c. 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.
 - d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Edit Manual Area Address, and OSI Router Editor.
- Step 5** Return to your originating procedure (NTP).
-

DLP-E253 Provision Additional Manual Area Addresses

Purpose	This task provisions the OSI manual area addresses. One primary and two additional manual areas can be created for each virtual router.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2 DLP-E252 Provision OSI Routers, page 18-72
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** Click the **Provisioning > OSI > Routers > Setup** tabs.
- Step 2** Chose the router where you want provision an additional manual area address and click **Edit**. The OSI Router Editor dialog box appears.
- Step 3** In the OSI Router Editor dialog box:
- a. Check **Enable Router** to enable the router and make its primary area address available for editing.
 - b. Click the manual area address, then click **Add**.
 - c. 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 2 to 24 alphanumeric characters (0–9, a–f) in length.

- d. Click **OK** successively to close the following dialog boxes: Masked NSAP Entry (if used), Add Manual Area Address, and OSI Router Editor.

Step 4 Return to your originating procedure (NTP).

DLP-E254 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	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note OSI subnetwork points of attachment are enabled on DCCs when you create DCCs. See the “[DLP-E114 Provision Section DCC Terminations](#)” task on page 17-14 and the “[DLP-E189 Provision Line DCC Terminations](#)” task on page 17-68.



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

- Step 1** Complete the “[DLP-E26 Log into CTC](#)” task on page 16-39 at the node whose OSI routers you want to provision.
- Step 2** Click the **Provisioning > OSI > Routers > Subnet** tabs.
- Step 3** Click **Enable LAN Subnet**.
- Step 4** In the Enable LAN Subnet dialog box, complete the following fields:
- **ESH**—Sets the End System Hello (ESH) propagation frequency on ONS nodes that can be provisioned as end system NEs. The field is not used by the ONS 15600.
 - **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.

- Step 5** Click **OK**.
- Step 6** Return to your originating procedure (NTP).

DLP-E255 Create an IP-Over-CLNS Tunnel

Purpose	This task creates an IP-over-CLNS tunnel to allow ONS 15600s to communicate across equipment and networks that use the OSI protocol stack.
Tools/Equipment	None
Prerequisite Procedures	NTP-E21 Verify Card Installation, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

IP-over-CLNS tunnels require two end points. You will create one point on an ONS 15600. The other end point 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.

- Step 1** Complete the “[DLP-E26 Log into CTC](#)” task on page 16-39 at the node of the OSI routers that you want to provision.
- Step 2** Click the **Provisioning > OSI > Tunnels** tabs.
- Step 3** Click **Create**.
- Step 4** 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 Open Shortest Path First (OSPF) metric for sending packets across the IP-over-CLNS tunnel. The OSPF metric, or cost, is used by OSPF routers to calculate the shortest path. The default is 110. Normally, it is not 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.

Step 5 Click **OK**.

Step 6 Provision the other tunnel end point using the documentation for the other equipment.

Step 7 Return to your originating procedure (NTP).

DLP-E256 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-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

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

Step 1 In node view, click the **Provisioning > OSI > TARP > MAT** tabs.

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

Step 3 Click **Remove**.

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

Step 5 Return to your originating procedure (NTP).

DLP-E257 Change the OSI Routing Mode

Purpose	This task changes the OSI routing mode.
Tools/Equipment	None
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
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 IS Level 1 or an 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 *ONS 15600 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.

Step 1 Verify that 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.

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

Step 3 Choose one of the following routing modes:

- **Intermediate System Level 1**—The ONS 15600 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 15600 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 systems and protocols are provided in the “Network Connectivity” chapter of the *ONS 15600 Reference Manual*.

Step 4 Although Cisco does not recommend changing the Link State Protocol Data Unit (LSP) buffer sizes, you can adjust the buffers in the following fields:

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

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

Step 5 Return to your originating procedure (NTP).

DLP-E258 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-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

Step 3 In the OSI Router Editor dialog box:

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



Note Router 1 must be enabled before you can enable Routers 2 through 12.

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

Step 4 Return to your originating procedure (NTP).

DLP-E259 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) or Line DCC (LDCC), or when you enable the LAN subnet.
Tools/Equipment	None
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, click the **Provisioning > OSI > Routers > Subnet** tabs.

Step 2 Choose the subnet you want to edit, then click **Edit**.

Step 3 In the Edit *subnet type* Subnet *slot/port* dialog box, edit the following fields:

- ESH—The End System Hello PDU propagation frequency. The field is not used by the ONS 15600.
- 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.
- IIS—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.

Click **OK**.

Step 4 Return to your originating procedure (NTP).

DLP-E260 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-E255 Create an IP-Over-CLNS Tunnel, page 18-75 DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

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

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

Step 2 Click **Edit**.

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

- Tunnel Type—Edit the tunnel type:
 - **Cisco**—Creates the proprietary Cisco IP tunnel. Cisco IP tunnels add the CLNS header to the IP packets.
 - **GRE**—Creates a Generic Routing Encapsulation 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.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-E261 Delete an IP-Over-CLNS Tunnel

Purpose	This task allows you to delete an IP-over-CLNS tunnel.
Tools/Equipment	None
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

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

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

DLP-E262 View IS-IS Routing Information Base

Purpose	This task allows you to view the 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-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In the node view, click the **Maintenance > OSI > IS-IS RIB** tabs.
- Step 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 MAC address.

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

DLP-E263 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 IS used to access the OSI network. For ISs, the only OSI level that can be provisioned on the ONS 15600, the ES-IS RIB shows the ESs connected to the IS node.
Tools/Equipment	None
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In the node view, click the **Maintenance > OSI > ES-IS RIB** tabs.
- Step 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 MAC address.
- Step 3** If additional routers are enabled, you can view their RIBs by choosing the router number in the Router field and clicking **Refresh**.
- Step 4** Return to your originating procedure (NTP).
-

DLP-E264 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 TID to NSAP mappings.
Tools/Equipment	None
Prerequisite procedures	DLP-E26 Log into CTC, page 16-39
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 View the following TDC information:

- **TID**—The target identifier of the originating NE. For ONS 15600s, 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.

Step 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 TDC is not enabled on the Provisioning > OSI > TARP subtab.

- a. Click the **TID to NSAP** button.
- b. In the TID to NSAP dialog box, enter the TID you want to map to an NSAP.
- c. Click **OK**, then click **OK** on the information message.
- d. 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 is displayed.

Step 4 If you want to delete all the dynamically generated TDC entries, click the **Flush Dynamic Entries** button. If not, continue with [Step 5](#).

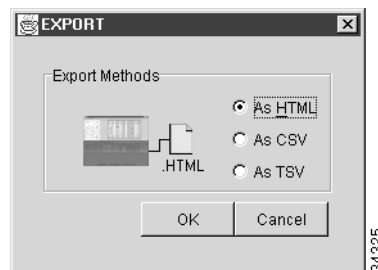
Step 5 Return to your originating procedure (NTP).

DLP-E265 Export CTC Data

Purpose	This task exports CTC table data for use by other applications such as spreadsheets, word processors, and database management applications.
Equipment/Tools	None
Prerequisite Procedures	DLP-E26 Log into CTC, page 16-39
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

-
- Step 1** Click the CTC tab containing the information you want to export (for example, the Alarms or Circuits tab).
- Step 2** From the CTC File menu, click **Export**.
- Step 3** In the Export dialog box choose a format for the data ([Figure 18-19](#)):
- **As HTML**—Saves the data as an HTML file. The file can be viewed with a web browser without running CTC.
 - **As CSV**—Saves the CTC table values as text, separated by commas. You can import CSV data into spreadsheets and database management programs.
 - **As TSV**—Saves the CTC table values as text, separated by tabs. You can import TSV data into spreadsheets and database management programs.

Figure 18-19 *Selecting CTC Data for Export*



- Step 4** 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 display the CTC data, or you can double-click the file name and choose an application such as Notepad.

Text editor and word processor applications display 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.

- Step 5** If you want to open the file in spreadsheet and database management applications, procedures vary; typically you need to open the application and choose File > Import, then choose a delimited file to display 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 applies to tabular data only, so it is not available for the following CTC tabs and subtabs:

- Provisioning > General, Protection, SNMP, and Timing windows
- Provisioning > Network > General window
- Provisioning > Security > Policy, Access, and Legal Disclaimer windows
- Provisioning > OSI > Main Setup
- Provisioning > OSI > TARP > Config
- Maintenance > Database, Protection, Diagnostic, and Timing windows

Step 6 Click **OK**.

Step 7 In the Save dialog box, enter a file name in one of the following formats:

- *filename.htm* for HTML files
- *filename.csv* for CSV files
- *filename.tsv* for TSV files

Step 8 Navigate to a directory where you want to store the file.

Step 9 Click **OK**.

Step 10 Return to your originating procedure (NTP).

DLP-E266 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-E26 Log into CTC, page 16-39
	Before configuring the node for RADIUS authentication, you must first add the node as a network device on the RADIUS server. Refer to the <i>User Guide for Cisco Secure ACS for Windows Server</i> for more information about configuring a RADIUS server.
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser



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

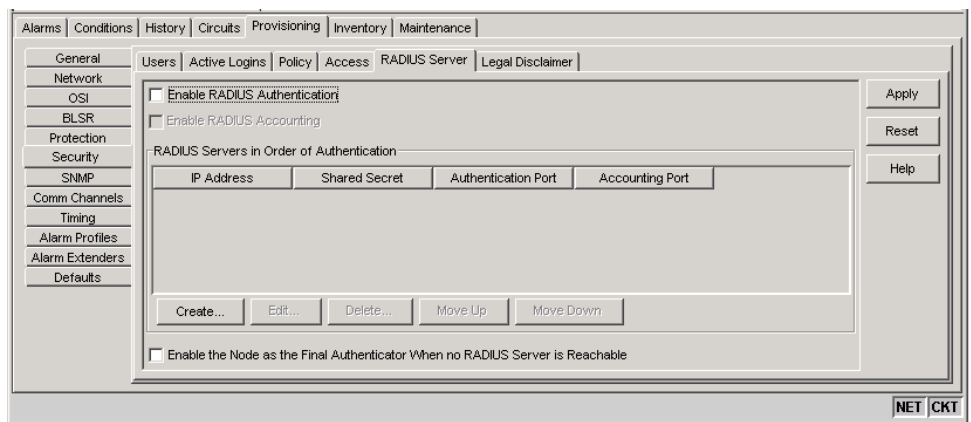
1 for Maintenance User

2 for Provisioning User

3 for Super User.

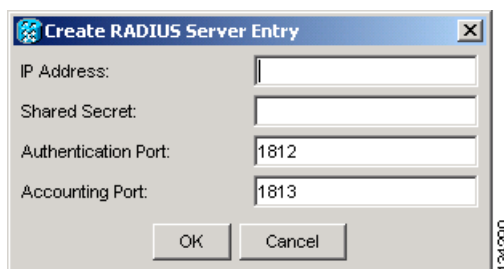
Step 1 In node view, click the **Provisioning > Security > RADIUS Server** tabs (Figure 18-20).

Figure 18-20 RADIUS Server Tab



Step 2 Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 18-21).

Figure 18-21 Create RADIUS Server Entry Window



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

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

**Caution**

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

- Step 4** Enter the shared secret in the Shared Secret field. A shared secret is a text string that serves as a password between a RADIUS client and RADIUS server.
- Step 5** Enter the RADIUS authentication port number in the Authentication Port field. The default port is 1812. If the node is an ENE, set the authentication port to a number within the range of 1860 to 1869.
- Step 6** Enter the RADIUS accounting port in the Accounting Port field. The default port is 1813. If the node is an ENE, set the accounting port to a number within the range of 1870 to 1879.
- Step 7** Click **OK**. The RADIUS server is added to the list of RADIUS authenticators.

**Note**

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

- Step 8** Click **Edit** to make changes to an existing RADIUS server. You can change the IP address, the shared secret, the authentication port, and the accounting port.
- Step 9** Click **Delete** to delete the selected RADIUS server.
- Step 10** 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.
- Step 11** Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.
- Step 12** Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.
- Step 13** Click the **Enable the Node as the Final Authenticator** check box if you want the node to be the final authenticator. This means that if every RADIUS authenticator is unavailable, the node will authenticate the login rather than locking the user out.
- Step 14** Click **Apply** to save all changes or **Reset** to clear all changes.
- Step 15** Return to your originating procedure (NTP).

