CHAPTER 21

DLPs A400 to A499

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-A412 Install the DCU Shelf Assembly

Purpose	If you are installing dispersion compensation modules, use this task to install the dispersion compensation unit (DCU) chassis.
Tools/Equipment	#2 Phillips screwdriver Crimping tool #14 AWG wire and lug
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 The DCU chassis requires 1 rack unit (RU) in a standard 19-inch (482.6-mm) or 23-inch (584.2-mm) rack. Locate the RMU space specified in your site plan.

Step 2 Two sets of mounting brackets are included with the DCU mounting kit, one set each for 19-inch (482.6-mm) and 23-inch (584.2-mm) racks. Verify that your chassis is equipped with the correct set of brackets for your rack. Change the brackets as required.

Step 3 Align the chassis with the rack mounting screw holes; one at a time, insert and tighten the four screws.

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Step 4 Connect a frame ground to the ground terminal provided on either side of the chassis. Use minimum #14 AWG wire.

Step 5 Return to your originating procedure (NTP).

DLP-A416 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-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate Cisco Transport Controller (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 appear 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 shows the following information:

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—Circuit types are STS (STS circuit), VT (VT circuit), VTT (VT tunnel), VAP (VT aggregation point), OCHNC (dense wavelength division multiplexing [DWDM] optical channel network connection), STS-v (STS virtual concatenated [VCAT] circuit), and VT-v (VT VCAT circuit).
- Size—Circuit size. VT circuit size is 1.5. STS circuit sizes are 1, 3c, 6c, 9c, 12c,18c, 24c, 36c, 48c, and 192c. OCHNC circuit sizes are Equipped not specific, Multi-rate, 2.5 Gbps No FEC (forward error correction), 2.5 Gbps FEC, 10 Gbps No FEC, and 10 Gbps FEC (DWDM only; refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*). VCAT circuit sizes are VT1.5-*n*v, STS-1-*n*v, STS-3c-*n*v, and STS-12c-*n*v, where *n* is the number of members.
- OCHNC Wlen—For OCHNCs, the wavelength provisioned for the optical channel network connection. (DWDM only; refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)
- Direction—The circuit direction, either two-way or one-way.
- OCHNC Dir—The direction of the OCHNC, either East to West or West to East. (DWDM only; refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)
- Protection—The type of circuit protection. See Table 21-1 for a list of protection types.

Table 21-1 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 two-fiber bidirectional line switched ring (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 a both a two-fiber and a four-fiber BLSR.
DRI	The circuit is protected by a dual-ring interconnect (DRI). This is used for both path protection and BLSR DRIs.
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.
Splitter	The circuit is protected by the protect transponder (TXPP_MR_2.5G) splitter protection. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
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.
Y-Cable	The circuit is protected by a transponder or muxponder card Y-cable protection group. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

- Status—The circuit status. Table 21-2 lists the circuit statuses that can appear.

Table 21-2 Cisco ONS 15454 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 the circuit source to the circuit destination.
DELETING	CTC is deleting a circuit.

Table 21-2 Cisco ONS 15454 Circuit Status (continued)

Status	Definition/Activity
PARTIAL	A CTC-created circuit is missing a cross-connect or network span, a complete path from source to destination(s) does not exist, or an alarm interface panel (AIP) change occurred on one of the circuit nodes and the circuit is in need of repair. (AIPs store the node MAC address.) 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, an PARTIAL status does not necessarily mean a circuit traffic failure has occurred, because traffic might flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans are shown as green lines, and down spans are shown 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 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 will not appear on the network map. Subsequently, circuits routed on a network span that goes down will appear as DISCOVERED during the current CTC session, but they will appear as PARTIAL to users who log in after the span failure.
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, and a complete path from source to destination(s) does not exist.

- Source—The circuit source in the format: *node/slot/port “port name”/STS/VT.* (The port name will appear in quotes.) Node and slot will always appear; *port “port name”/STS/VT* might appear, depending on the source card, circuit type, and whether a name is assigned to the port. If the circuit is a concatenated size (3c, 6c, 12c, etc.), STSs used in the circuit are indicated by an ellipsis, for example, “S7..9,” (STSs 7, 8, and 9) or S10..12 (STS 10, 11, and 12).
- Destination—The circuit destination in same format (*node/slot/port “port name”/STS/VT*) as the circuit source.
- # of VLANS—The number of VLANs used by an Ethernet circuit.
- # of Spans—The number of internode links that constitute the circuit. Right-clicking the column shows a shortcut menu from which you can choose to show or hide circuit span detail.
- State—The circuit service state, IS, 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.

Step 3 Return to your originating procedure (NTP).

DLP-A417 View the BLSR Squelch Table

Purpose	This task allows you to view the BLSR squelch table for an ONS 15454 BLSR node. The table shows STSs that will be squelched for every isolated node. Squelching replaces traffic by the appropriate path alarm indication signal (AIS); it prevents traffic misconnections when a working channel service contends for access to a protection channel time slot carrying extra traffic. For more information about BLSR squelching, refer to Telcordia GR-1230.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Step 2 Click the BLSR whose squelch table you want to view.

Step 3 Click **Squelch Table**. In the BLSR Squelch Table window you can view the following information:

- STS Number—Shows the BLSR STS numbers. For two-fiber BLSRs, the number of STSs is half the BLSR OC-N, for example, an OC-48 BLSR squelch table will show 24 STSs. For four-fiber BLSRs, the number of STSs in the table is the same as the BLSR OC-N.
- West Source—If traffic is received by the node on its west span, the BLSR node ID of the source appears. (To view the BLSR node IDs for all nodes in the ring, click the **Ring Map** button.)
- West Dest—If traffic is sent on the node’s west span, the BLSR node ID of the destination appears.
- East Source—If traffic is received by the node on its east span, the BLSR node ID of the source appears.
- East Dest—If traffic is sent on the node’s east span, the BLSR node ID of the destination appears.

Note BLSR squelching is performed on STSs that carry STS circuits only. Squelch table entries will not appear for STSs carrying VT circuits or Ethernet circuits to or from E-Series Ethernet cards provisioned in a multicard Ethergroup.

Step 4 Return to your originating procedure (NTP).

DLP-A418 Install Public-Key Security Certificate

Purpose	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This task is performed during the "DLP-A60 Log into CTC" task on page 17-66. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- **Yes (Grant This Session)**—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15454.
- **No (Deny)**—Denies permission to install the certificate. If you choose this option, you cannot log into the ONS 15454.
- **Always (Grant Always)**—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- **More Details (View Certificate)**—Allows you to view the public-key security certificate.

Step 2 If the Login dialog box appears, continue with Step 3. If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if CTC finds a modified Java policy file (.java.policy) on your PC. In Software Release 4.0 and earlier, the Java policy file was modified to allow CTC software files to be downloaded to your PC. The modified Java policy file is not needed in Software R4.1 and later, so you can remove it unless you will log into ONS 15454s running software earlier than R4.1. Choose one of the following options:

- **Yes**—Removes the modified Java policy file from your PC. Choose this option if you will only log into ONS 15454s running Software R4.1 software or later.
- **No**—Does not remove the modified Java policy file from your PC. Choose this option if you will log into ONS 15454s running Software R4.0 or earlier. If you choose No, this dialog box will appear every time you log into the ONS 15454. If you do not want it to appear, check the **Do not show the message again** check box.

Caution If you delete the Java policy file, you cannot log into nodes running Software R4.0 and earlier. If you delete the file and want to log into an ONS 15454 running an earlier release, insert the software CD for the release into your PC CD-ROM and run the CTC setup wizard to reinstall the Java policy file.

Step 3 Return to your originating procedure (NTP).

DLP-A421 Provision G-Series Flow Control Watermarks

Purpose	This task provisions the buffer memory levels for flow control on G-Series Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the node view, double-click the G-Series card graphic to open the card.

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

Step 3 In the Water Marks column, click the cell in the row for the appropriate port.

Step 4 To provision the Low Latency flow control watermark:

a. Choose **Low Latency** from the drop-down list.

The Flow Ctrl Lo and Flow Ctrl Hi values change.

b. Click **Apply**.

Step 5 To provision a Custom flow control watermark:

a. Choose **Custom** from the drop-down list.

b. In the Flow Ctrl Lo column, click the cell in the row for the appropriate port.

c. Enter a value in the cell. The Flow Ctrl Lo value has a valid range from 1 to 510 and must be lower than the Flow Ctrl Hi value.

This value sets the flow control threshold for sending the signal to the attached Ethernet device to resume transmission.

d. In the Flow Ctrl Hi column, click the cell in the row for the appropriate port.

e. Enter a value in the cell. The Flow Ctrl Hi value has a valid range from 2 to 511 and must be higher than the Flow Ctrl Lo value.

This value sets the flow control threshold for sending the signal to the attached Ethernet device to pause transmission.

f. Click **Apply**.

Note Low watermarks are optimum for low latency subrate applications, such as voice-over-IP (VoIP) using an STS-1. High watermarks are optimum when the attached Ethernet device has insufficient buffering, best effort traffic, or long access line lengths.

Step 6 Return to your originating procedure (NTP).

DLP-A422 Verify BLSR Extension Byte Mapping

Purpose	This task verifies that the extension byte mapping is the same on BLSR trunk (span) cards that will be connected after a node is removed from a BLSR.
Tools/Equipment	OC-48 AS cards must be installed at one or both ends of the BLSR span that will be connected.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In network view, double-click a BLSR node with OC-48 AS trunk (span) cards that will be reconnected after a BLSR node removal.

Step 2 Double-click one OC-48 AS BLSR trunk card.

Step 3 Click the **Provisioning** > **Line** tabs.

Step 4 Record on paper the byte in the BLSR Ext Byte column.

Step 5 Repeat Steps 2 through 4 for the second OC-48 AS trunk card.

Step 6 If the node at the other end of the new span contains OC-48 AS trunk cards, repeat Steps 1 through 5 at the node. If it does not have OC-48 AS cards, their trunk cards are mapped to the K3 extension byte. Continue with Step 7.

Step 7 If the trunk cards on each end of the new span are mapped to the same BLSR extension byte, continue with Step 8. If they are not the same, remap the extension byte of the trunk cards at one of the nodes. See the "DLP-A89 Remap the K3 Byte" task on page 17-87.

Step 8 Return to your originating procedure (NTP).

DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration

Purpose	This task installs fiber-optic cables on optical (OC-N) cards in a 1+1 linear configuration.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 15-13
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Note The Cisco OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics, all working at 1310 nm, are optimized for the most widely used SMF-28 fiber, available from many suppliers.

Note Corning MetroCor fiber is optimized for optical interfaces that transmit at 1550 nm or in the C and L DWDM windows. This fiber targets interfaces with higher dispersion tolerances than those found in OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics. If you are using Corning MetroCor fiber, the interface optics for these cards will become dispersion limited before they will become attenuation limited. In this case, consider using OC-3 LR/STM-1 LH, OC-12 LR/STM-4 LH, and OC-48 LR/STM-16 LH cards instead of OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH cards.

Note With all fiber types, network planners and engineers should review the relative fiber type and optics specifications to determine attenuation, dispersion, and other characteristics to ensure appropriate deployment.

Step 1 Plan your fiber connections. Use the same plan for all 1+1 nodes.

Step 2 Align the keyed ridge of the cable connector with the transmit (Tx) connector of a working OC-N card at one node and plug the other end of the fiber into the receive (Rx) connector of a working OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports). Figure 19-1 on page 19-6 shows the cable location.

Step 3 Repeat Steps 1 and 2 for the corresponding protect ports on the two nodes and all other working/protect port pairs that you want to place in a 1+1 configuration.

Step 4 Return to your originating procedure (NTP).

DLP-A430 View Spanning Tree Information

Purpose	This task allows you to view E-Series Ethernet circuits and the Ethernet front ports operating with the Spanning Tree Protocol (STP). The E-Series card supports up to eight STPs per node. For more information about STP, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454 SDH, Cisco ONS 15454, and Cisco ONS 15327*.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, click the **Maintenance > Ether Bridge > Circuits** tabs.

Step 2 In the EtherBridge Circuits window, you can view the following information:

- Type—Identifies the type of Ethernet circuit mapped to the spanning tree, such as EtherSwitch point-to-point.
- Circuit Name/Port—Identifies the circuit name for the circuit in the spanning tree. This column also lists the Ethernet slots and ports mapped to the spanning tree for the node.

- STP ID—Shows the STP ID number.
- VLANS—Lists the VLANs associated with the circuit or port.

Step 3 Return to your originating procedure (NTP).

DLP-A431 Change the JRE Version

Purpose	This task changes the Java Runtime Environment (JRE) version, which is useful if you would like to upgrade to a later JRE version from earlier one without using the software or documentation CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used.
Tools	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task is not used in Software R5.0 because only one JRE version is supported. This task is used in CTC releases that support multiple JRE versions.

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

Step 2 Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.

Step 3 Click the **Browse** button and navigate to the JRE directory on your computer.

Step 4 Choose the JRE version.

Step 5 Click **OK**.

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

Step 7 In the confirmation dialog box, click **Yes**.

Step 8 Complete the "DLP-A60 Log into CTC" task on page 17-66.

Step 9 Return to your originating procedure (NTP).

DLP-A433 Enable Node Security Mode

Purpose	This task enables the ONS 15454 security mode. When security mode is enabled, two IP addresses are assigned to the node. One address is assigned to the backplane LAN port and the other to the TCC2P RJ-45 TCP/IP (LAN) port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-4 DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution The IP address assigned to the TCC2P LAN port must reside on a different subnet from the backplane LAN port and the ONS 15454 default router. Verify that the new TCC2P IP address meets this requirement and is compatible with ONE 15454 network IP addresses.

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

Step 1 Click the **Provisioning** > **Security** > **Data Comm** tabs.

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode wizard page, then click **Next**.

Step 4 On the TCC Ethernet Port page, enter the IP address and subnet mask for the TCC2P LAN (TCP/IP) port. The IP address cannot reside on the same subnet as the backplane LAN port, nor the ONS 15454 default router.

Step 5 Click **Next**.

Step 6 On the Backplane Ethernet Port page, modify the backplane IP address, subnet mask, and default router, if needed. (You normally do not modify these fields if no ONS 15454 network changes have occurred.)

Step 7 Click **Next**.

Step 8 On the SOCKS Proxy Server Settings page, choose one of the following options:

- **External Network Element (ENE)**—If selected, the CTC computer is only visible to the ONS 15454 to which the CTC computer is connected. The computer is not visible to the DCC-connected nodes. In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
- **Gateway Network Element (GNE)—**If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port.

Note The SOCKS proxy server is automatically enabled when you enable secure mode.

Step 9 Click **Finish**.

Within the next 30 to 40 seconds, the TCC2P cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node color changes to grey and a DISCONNECTED condition appears.

Step 10 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish (this might take several minutes).

Step 11 After the DISCONNECTED condition clears, complete the following steps to suppress the backplane IP address from display in CTC and the LCD. If you do not want to suppress the backplane IP address display, continue with Step 12.

a. Display the node in node view.

b. Click the **Provisioning** > **Security** > **Data Comm** tabs.

c. In the LCD IP Setting field, choose **Suppress Display**. This removes the IP address from display on the ONS 15454 LCD.

d. Check the **Suppress CTC IP Address** check box. This removes the IP address from display in the CTC information area and from the Provisioning > Security > Data Comm tab.

e. Click **Apply**.

Note After you turn on secure mode, the TCC2P IP address becomes the node IP address.

Step 12 Return to your originating procedure (NTP).

DLP-A434 Lock Node Security

Purpose	This task locks the ONS 15454 security mode. When security mode is locked, two IP addresses must always be provisioned for the node, one for the TCC2P LAN (TCP/IP) port, and one for the backplane LAN port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66 DLP-A433 Enable Node Security Mode, page 21-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution This task is irreversible. Do not proceed unless you want the node to permanently have two IP addresses.

Step 1 Click the **Provisioning** > **Security** > **Data Comm** tabs.

Step 2 Click **Lock**.

Step 3 In the Confirm Lock Secure Mode dialog box, click **Yes**.

Step 4 Return to your originating procedure (NTP).

DLP-A435 Modify Backplane Port IP Settings

Purpose	This task modifies the ONS 15454 backplane IP address, subnet mask, and default router. It also modifies settings that control backplane IP address visibility in CTC and the ONS 15454 LCD. To perform this task, secure mode must be enabled.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-4 DLP-A60 Log into CTC, page 17-66 DLP-A433 Enable Node Security Mode, page 21-11
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 1 Click the **Provisioning** > **Security** > **Data Comm** tabs.

Step 2 Modify the following fields, as necessary:

- IP Address
- Subnet Mask
- Default Router
- LCD IP Setting—choose one of the following:
  - **Allow Configuration**—Displays the backplane IP address on the LCD and allows it to be changed using the LCD buttons.
  - **Display only—**Displays the backplane IP address on the LCD but does not allow it to be changed using the LCD buttons.
  - **Suppress Display**—Suppresses the display of the IP address on the LCD.
- Suppress CTC IP Address—If checked, suppresses the IP address from display on the Data Comm subtab, CTC node view information area, and other locations.

Step 3 Click **Apply**.

If you changed the IP address, subnet mask, or default router, the node will reboot. This will take 5 to 10 minutes.

Step 4 Return to your originating procedure (NTP).

DLP-A436 Disable Node Security Mode

Purpose	This task disables the ONS 15454 security mode and allows only one IP address to be provisioned for the backplane LAN port and the TCC2P LAN port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database, page 15-4 DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

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

Step 1 Click the **Provisioning** > **Security** > **Data Comm** tabs.

Step 2 Click **Change Mode**.

Step 3 Review the information on the Change Secure Mode wizard page, then click **Next**.

Step 4 On the Node IP Address page, choose the address you want to assign to the node:

- **Backplane Ethernet Port**—Assigns the backplane IP address as the node IP address.
- **TCC Ethernet Port**—Assigns the TCC2P port IP address as the node IP address
- **New IP Address**—Allows you to define a new IP address. If you choose this option, enter the new IP address, subnet mask, and default router IP address.

Step 5 Click **Next**.

Step 6 On the SOCKS Proxy Server Settings page, choose one of the following:

- **External Network Element (ENE)**—If selected, the CTC computer is only visible to the ONS 15454 to which the CTC computer is connected. The computer is not visible to the DCC-connected nodes. In addition, firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
- **Gateway Network Element (GNE)**—If selected, the CTC computer is visible to other DCC-connected nodes. The node prevents IP traffic from being routed between the DCC and the LAN port.
- **Proxy-only**—If selected, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes for which the node serves as a proxy. The CTC computer is visible to other DCC-connected nodes. The node does not prevent traffic from being routed between the DCC and LAN port.

Step 7 Click **Finish**.

Within the next 30 to 40 seconds, the TCC2P cards reboot. CTC switches to network view, and the CTC Alerts dialog box appears. In network view, the node color changes to grey and a DISCONNECTED condition appears.

Step 8 In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)

Step 9 Return to your originating procedure (NTP).

DLP-A437 Change a VCAT Member Service State

Purpose	This task displays the Edit Circuit window for VCAT members, where you can change the service state.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66 VCAT circuits must exist on the network. See the "NTP-A264 Create an Automatically Routed VCAT Circuit" procedure on page 6-86 or the "NTP-A265 Create a Manually Routed VCAT Circuit" procedure on page 6-90.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note CTC only permits you to change the state of a non-Link Capacity Adjustment Scheme (LCAS) member if the new state matches the In Group VCAT state of the other members, or if the new state is an Out of Group VCAT state. The In Group VCAT state indicates that a member has cross-connects in the IS-NR; OOS-MA,AINS; or OOS-AU,MT service states. For non-LCAS VCAT members, the Out of Group VCAT state is the OOS-MA,DSBLD service state.

Step 1 In node or network view, click the **Circuits** tab.

Step 2 Click the VCAT circuit that you want to edit, then click **Edit**.

Step 3 Click the **Members** tab.

Step 4 Select the member that you want to change. To choose multiple members, press **Ctrl** and click each member.

Step 5 From the Tools menu, choose **Set Circuit State**.

Note You can also change the state for all members listed in the Edit Circuit window using the State tab. Another alternative is to click the Edit Member button to access the Edit Member Circuit window for the selected member, and click the State tab.

Step 6 From the Target Circuit Admin State drop-down list, choose the administrative state:

- **IS**—Puts the member cross-connects in the IS-NR service state.
- **OOS,DSBLD**—Puts the member cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- **IS,AINS**—Puts the member cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.

- **OOS,MT**—Puts the member cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete.
- **OOS,OOG**—(LCAS and Software–Link Capacity Adjustment Scheme [Sw-LCAS] VCAT only.) Puts VCAT member cross-connects in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to put a member circuit out of the group and to stop sending traffic.

Step 7 Click **Apply**.

Step 8 To close the Edit Circuit window, choose **Close** from the File menu.

Step 9 Return to your originating procedure (NTP).

DLP-A438 Change General Port Settings for the FC_MR-4 Card

Purpose	This task changes the general port settings for FC_MR-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning > Port > General** tabs.

Step 3 Modify any of the settings described in Table 21-3.

Table 21-3 FC_MR-4 Card General Port Settings

Parameter	Description	Options
Port	(Display only.) Displays the port number.	1 through 4
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the "DLP-A314 Assign a Name to a Port" task on page 20-8.

Table 21-3 FC_MR-4 Card General Port Settings (continued)

Parameter	Description	Options
Admin State	Changes the port service state unless network conditions prevent the change.	• IS—Puts the port in-service. The port service state changes to IS-NR. • OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD. • OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT.
Service State	Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR—(In-Service and Normal) The port is fully operational and performing as provisioned. • OOS-MA,DSBLD—(Out-of-Service and Management,Disabled) The port is out-of-service and unable to carry traffic. • OOS-MA,MT—(Out-of-Service and Management,Maintenance) The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
Port Rate	Selects the Fibre Channel interface.	• 1 Gbps • 2 Gbps
Link Rate	Displays the actual rate of the port.	—
Max GBIC Rate	Displays the maximum Gigabit Interface Converter (GBIC) rate. Cisco supports two GBICs for the FC_MR-4 card (ONS-GX-2FC-SML and ONS-GX-2FC-MMI). If used with another GBIC, “Contact GBIC vendor” is displayed.	—
Link Recovery	Enables or disables link recovery if a local port is inoperable. If enabled, a link reset occurs when there is a loss of transport from a cross-connect switch, protection switch, or an upgrade.	—
Media Type	Sets the proper payload value for the Transparent Generic Framing Protocol (GFP-T) frames.	• Fibre Channel - 1 Gbps • Fibre Channel - 2 Gbps • FICON 1 Gbps • FICON 2 Gbps • Unknown

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A439 Change Distance Extension Port Settings for the FC_MR-4 Card

Purpose	This task changes the distance extension parameters for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning** > **Port** > **Distance Extension** tabs.

Step 3 Modify any of the settings described in Table 21-4.

Table 21-4 FC_MR-4 Card Distance Extension Port Settings

Parameter	Description	Options
Port	(Display only.) The card port number.	1 through 4
Enable Distance Extension	If checked, allows additional distance by providing a GFP-T based flow control scheme. It enables the node to be a part of a Storage Area Network (SAN) with long-distance, remote nodes. If left unchecked, the remaining options are not available for editing. If Distance Extension is enabled, set the connected Fibre Channel switches to Interop or Open Fabric mode, depending on the Fibre Channel switch. By default, the FC_MR card will interoperate with the Cisco MDS storage products.	—
Auto Detect Credits	If checked, enables the node to detect the transmit credits from a remote node. Credits are used for link flow control and for Extended Link Protocol (ELP) login frames between Fibre Channel/fiber connectivity (FC/FICON) Switch E ports.	—
Credits Available	Sets the number of credits if an ELP login frame setting is missing or if the ELP login frame cannot be detected. Credits Available is editable only if Auto Detect Credits is unchecked. **Note** Longer distances between connected devices need more credits to compensate for the latency introduced by the long-distance link. The value should never be greater than the number of credits supported by the FC/FICON port.	Numeric. 2 through 256, multiples of 2 only

Table 21-4 FC_MR-4 Card Distance Extension Port Settings (continued)

Parameter	Description	Options
Autoadjust GFP Buffer Threshold	If checked, guarantees the best utilization of the SONET/SDH transport in terms of bandwidth and latency.	—
GFP Buffers Available	Sets the GFP buffer depth. GFP Buffers Available is editable if Autoadjust GFP Buffer Threshold is unchecked. For shorter SONET transport distances, Cisco recommends lower values to decrease latency. For longer SONET transport distances, Cisco recommends higher values to provide higher bandwidth.	Numeric. 16 through 1200, multiples of 16 only

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A440 Change Enhanced FC/FICON Port Settings for the FC_MR-4 Card

Purpose	This task changes the enhanced FC/FICON parameters for FC_MR-4 ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the FC_MR-4 card where you want to change the port settings.

Step 2 Click the **Provisioning** > **Port** > **Enhanced FC/FICON** tabs.

Step 3 Modify any of the settings described in Table 21-5.

Table 21-5 FC_MR-4 Card Distance Extension Port Settings

Parameter	Description	Options
Port	(Display only.) The card port number.	1 through 4

Table 21-5 FC_MR-4 Card Distance Extension Port Settings (continued)

Parameter	Description	Options
Ingress Idle Filtering	If checked, prevents removal of excess FC/FICON IDLE codes from SONET transport. IDLEs are 8b10b control words that are sent between frames or when there is no data to send. Ingress idle filtering applies only to SONET circuit bandwidth sizes that allow full line rate FC/FICON transport. It can be used for interoperability with remote FC/FICON over third-party SONET equipment.	—
Maximum Frame Size	Sets the maximum size of a valid frame. This setting prevents oversized performance monitoring accumulation for frame sizes that are above the Fibre Channel maximum. This can occur for Fibre Channel frames with added virtual SAN (VSAN) tags that are generated by the Cisco MDS 9000 switches.	Numeric, 2148 through 2172

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-A441 Install Electrical Cables on the UBIC-H EIAs

Purpose	This task installs DS-1 and DS-3/EC-1 cables on the Universal Backplane Interface Connector–Horizontal (UBIC-H) electrical interface assemblies (EIAs).
Tools/Equipment	3/16-inch flat-head screwdriver DS-1 and DS-3/EC-1 cables, as needed: • 15454-CADS1-H-25 • 15454-CADS1-H-50 • 15454-CADS1-H-75 • 15454-CADS1-H-100 • 15454-CADS1-H-150 • 15454-CADS1-H-200 • 15454-CADS1-H-250 • 15454-CADS1-H-350 • 15454-CADS1-H-450 • 15454-CADS1-H-550 • 15454-CADS1-H-655 • 15454-CADS3-SD • 15454-CADS3-ID • 15454-CADS3-LD
Prerequisite Procedures	DLP-A399 Install a UBIC-H EIA, page 20-97
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note Cisco recommends that you plan for future slot utilization and fully cable all SCSI connectors that you will use later.

Step 1 Place a cable connector over the desired connection point on the backplane, making sure the cable runs toward the outside of the shelf.

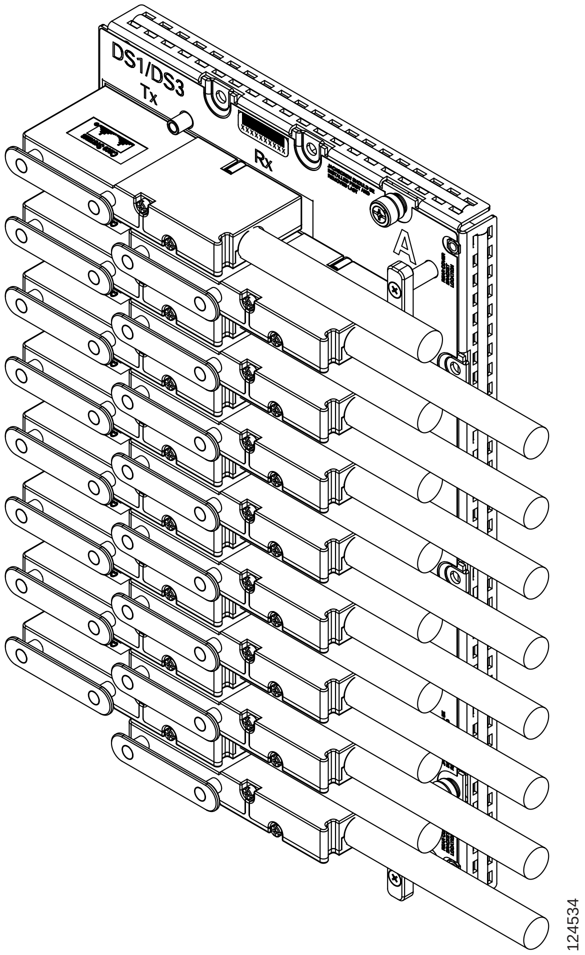
Step 2 Carefully push the connector into the backplane until the pin on the cable connector slides into the notch on the UBIC-H. Make sure the standoffs on the UBIC-H align properly with the notches on the cable.

Step 3 Use the flathead screwdriver to tighten the screws at the top and bottom of the end of cable connector two to three turns at 8 to 10 lbf-inch (9.2 to 11.5kgf-cm). Alternate between the two screws until both are tight.

Step 4 Repeat Steps 1 through 3 for each cable you want to install.

Figure 21-1 shows a UBIC-H with cables installed in all connectors.

Figure 21-1 Fully Cabled UBIC-H (A-Side)



Step 5 If available, tie wrap or lace the cables according to Telcordia standards (GR-1275-CORE) or local site practice.

Note When routing the electrical cables be sure to leave enough room in front of the alarm and timing panel so that it is accessible for maintenance activity.

Step 6 Return to your originating procedure (NTP).

DLP-A442 Verify Pass-Through Circuits

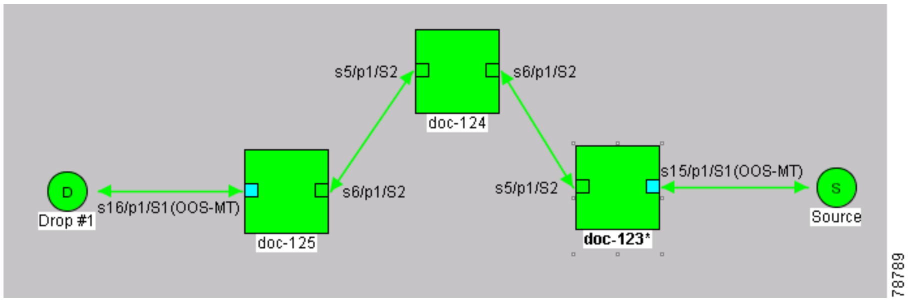
Purpose	This task verifies that circuits passing through a node enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-66
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the CTC 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 and VT mapping on the node's east and west ports are the same. For example, if the circuit mapping on the west port is s5/p1/S1 (Slot 5, Port 1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit displays different STSs and/or VTs on the east and west ports, record the name of the circuit. Figure 21-2 shows a circuit passing through a node (doc-124) on the same STS (STS 2).

Figure 21-2 Verifying Pass-Through STSs



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. To delete the circuit, see the "DLP-A333 Delete Circuits" task on page 20-21. To create the circuit, see Chapter 6, "Create Circuits and VT Tunnels."

Step 6 Return to your originating procedure (NTP).

DLP-A469 Install GBIC or SFP Connectors

Purpose	This task installs GBICs (required for E-Series Ethernet, G-Series Ethernet, and FC_MR-4 cards) and Small Form-factor Pluggables (SFPs) (required for ML1000-2 and MXP cards). SFPs are hot-swappable input/output devices that plug into a line card port to link the port with the fiber-optic network. For a description of SFP connectors on transponder or muxponder cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
Tools/Equipment	For the E1000-2-G use: • SX GBIC= for short-reach applications • LX GBIC= for long-reach applications For the G1000-4 or G1K-4 card use: • SX GBIC= for short-reach applications • LX GBIC= for long-reach applications • ZX GBIC= for extra long-reach applications • DWDM GBIC= for DWDM applications For the ML1000-2 card use: • SX SFP= for short-reach applications • LX SFP= for long-reach applications For the FC_MR-4 card use: • ONS-GX-2FC-SML= for 2-Gb FC 1310-nm single-mode with SC connectors • ONS-GX-2FC-MMI= for 2-Gb FC 850-nm multimode with SC connectors
Prerequisite Procedures	DLP-A39 Install Ethernet Cards, page 17-48 NTP-A274 Install the FC_MR-4 Cards, page 2-11
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note G-Series cards manufactured before August 2003 do not support DWDM GBICs. G1000-4 cards compatible with DWDM GBICs have a Common Language Equipment Identification (CLEI) code of SNP8KW0KAB. Compatible G1K-4 cards have a CLEI code of WM5IRWPCAA.

Note All versions of G1000-4 and G1K-4 cards support coarse wavelength division multiplexing (CWDM) GBICs.

Note GBICs and SFPs are hot-swappable and can therefore be installed/removed while the card/shelf assembly is powered and running.

Step 1 Remove the GBIC or SFP from its protective packaging.

Step 2 Check the label to verify that the GBIC or SFP is the correct type for your network.

Table 21-6 shows the available GBICs.

Note The GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Table 21-6 Available GBICs

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseSX	E1000-2-G G1000-4 G1K-4	Short reach	Multimode fiber up to 550 m long	15454E-GBIC-SX=
1000BaseLX	E1000-2-G G1000-4 G1K-4	Long reach	Single-mode fiber up to 5 km long	15454E-GBIC-LX=
1000BaseZX	G1000-4 G1K-4	Extra long reach	Single-mode fiber up to 70 km long	15454E-GBIC-ZX=
	FC_MR-4	Long reach	Single-mode fiber, 1310 nm	ONS-GX-2FC-SML=
	FC_MR-4	Intermediate reach	Multimode fiber, 850 nm	ONS-GX-2FC-MMI=

Table 21-7 shows the available SFPs.

Table 21-7 Available SFPs

SFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	ML1000-2	Short reach	Multimode fiber up to 550 m long	15454E-SFP-LC-SX=
1000BaseLX	ML1000-2	Long reach	Single-mode fiber up to 5 km long	15454E-SFP-LC-LX=

Step 3 Verify the type of GBIC or SFP you are using:

- If you are using a GBIC with clips, go to Step 4.
- If you are using a GBIC with a handle, go to Step 5.
- If you are using an SFP, go to Step 6.

Step 4 For GBICs with clips:

a. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

Note GBICs are keyed to prevent incorrect installation.

b. Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

- **c.** When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.
- **d.** Continue with Step 7.

Step 5 For GBICs with a handle:

- **a.** Remove the protective plug from the SC-type connector.
- **b.** Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.
- **c.** Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to an SC-type connector.
- **d.** Slide the GBIC through the cover flap until you hear a click.

  The click indicates that the GBIC is locked into the slot.
- **e.** Continue with Step 7.

Warning **Class 1 laser product.** Statement 1008

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam 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 could pose an eye hazard.** Statement 1056

Step 6 For SFPs:

- **a.** Plug the LC duplex connector of the fiber into a Cisco-supported SFP connector.
- **b.** If the new SFP connector has a latch, close the latch over the cable to secure it.
- **c.** Plug the cabled SFP connector into the card port until it clicks.

Step 7 Return to your originating procedure (NTP).

DLP-A470 Remove GBIC or SFP Connectors

Purpose	This task disconnects fiber attached to GBICs or SFPs and removes the GBICs or SFPs.
Tools/Equipment	None
Prerequisite Procedures	DLP-A469 Install GBIC or SFP Connectors, page 21-24
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam 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 could pose an eye hazard.** Statement 1056

Step 1 Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector. If the SFP connector has a latch securing the fiber cable, pull it upward to release the cable.

Step 2 If you are using a GBIC with clips:

a. Release the GBIC from the slot by squeezing the two plastic tabs on each side of the GBIC.

b. Slide the GBIC out of the slot. A flap closes over the slot to protect the connector on the Gigabit Ethernet card.

Step 3 If you are using a GBIC with a handle:

a. Release the GBIC by opening the handle.

b. Pull the handle of the GBIC.

c. Slide the GBIC out of the slot. A flap closes over the slot to protect the connector on the Gigabit Ethernet card.

Step 4 If you are using an SFP:

a. If the SFP connector has a latch securing the fiber cable, pull it upward to release the cable.

b. Pull the fiber cable straight out of the connector.

c. Unplug the SFP connector and fiber from the card.

d. Slide the SFP out of the slot.

Step 5 Return to your originating procedure (NTP).

DLP-A498 Switch Between TDM and DWDM Network Views

Purpose	Use this task to switch between time division multiplexing (TDM) and DWDM network views.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC, page 17-66
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

Step 2 From the Network Scope drop-down list on the toolbar, choose one of the following:

- **All**—Displays both TDM and DWDM nodes.
- **TDM**—Displays only ONS 15454s with SONET or SDH cards including the transponder (TXP) and muxponder (MXP) cards.
- **DWDM**—Displays only ONS 15454s with DWDM cards, including the transponder and muxponder cards.

Note For information about DWDM, TXP, and MXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 3 Return to your originating procedure (NTP).