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.

Contents

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

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

1. The DCU chassis requires 1 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.
2. Two sets of mounting brackets are included with the DCU mounting kit, one set each, for 19-inch (482.6-mm) or 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.
3. Align the chassis with the rack mounting screw holes; one at a time, insert and tighten the four screws.

4. Connect a frame ground to the ground terminal provided on either side of the chassis. Use minimum #14 AWG wire.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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.
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 [OCHNC]), STS-v (STS virtual concatenated [VCAT] circuit), and VT-v (VT VCAT circuit).
   - Size-Circuit size. VT circuit size is VT1.5 or VT2. 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 Procedure 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-(DWDM only) For OCHNCs, the provisioned wavelength. For more information, refer to the Cisco ONS 15454 DWDM Procedure Guide.
   - Direction-The circuit direction, either two-way or one-way.
   - OCHNC Dir-(DWDM only) For OCHNCs, the direction of the OCHNC, either East to West or West to East. For more information, refer to the Cisco ONS 15454 DWDM Procedure 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 (both path protection and BLSR).
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 configuration, or a path protection and 1+1 configuration.
Splitter	The circuit is protected by the protect transponder (TXPP_MR_2.5G) splitter protection. Refer to the Cisco ONS 15454 DWDM Procedure 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 configuration.
Y-Cable	The circuit is protected by a transponder or muxponder card Y-cable protection group. Refer to the Cisco ONS 15454 DWDM Procedure 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.
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.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this state. The circuit returns to the DISCOVERED state once the topology upgrade is complete. For more information about topology upgrades, refer to the "SONET Topologies and Upgrades" chapter in the *Cisco ONS 15454 Reference Manual*.
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 "SONET Topologies and Upgrades" chapter in the *Cisco ONS 15454 Reference Manual*.
DROP_PENDING	A circuit is set to this status when a new circuit drop is being added.
ROLL_PENDING	A circuit roll is awaiting completion or cancellation.

◊ Source-The circuit source in the format: *node/slot(card type)/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 port is on a MRC-12 or MRC-2.5G-4 card, the port format is *PPM-port_number*. If the circuit size is a concatenated size (3c, 6c, 12c, etc.), synchronous transport signals (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[card type]/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 Span Details to show or hide circuit span detail. For each node in the span, the span detail shows the *node/slot (card type)/port/STS/VT*.

◊ 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.

3. 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. You cannot perform it outside of this task.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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 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.
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 only if you will 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.

3. Return to your originating procedure (NTP).

DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks

Purpose	This task provisions the buffer memory levels for flow control on G-Series and CE-1000-4 Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the node view, double-click the G-Series or CE-1000-4 card graphic to open the card.
2. Click the **Provisioning > Port** tabs.
3. In the Water Marks column, click the cell in the row for the appropriate port.
4. To provision the Low Latency flow control watermark:
   1. Choose **Low Latency** from the drop-down list.
      The Flow Ctrl Lo and Flow Ctrl Hi values change.

2. Click Apply.

5. To provision a Custom flow control watermark:
    1. Choose **Custom** from the drop-down list.
    2. In the Flow Ctrl Lo column, click the cell in the row for the appropriate port.
    3. 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.
    4. In the Flow Ctrl Hi column, click the cell in the row for the appropriate port.
    5. 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.
    6. 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.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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.
2. Double-click one OC-48 AS BLSR trunk card.
3. Click the **Provisioning > Line** tabs.
4. Record on paper the byte in the BLSR Ext Byte column.
5. Repeat Steps 2 through 4 for the second OC-48 AS trunk card.
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.
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.
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
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-optic cable, available from many suppliers.

Note: Corning MetroCor fiber-optic cable is optimized for optical interfaces that transmit at 1550 nm or in the C and L DWDM windows. This fiber-optic cable 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-optic cable, OC-3 IR/STM-1 SH, OC-12 IR/STM-4 SH, and OC-48 IR/STM-16 SH interface optics 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/engineers should review the relative fiber type and optics specifications to determine attenuation, dispersion, and other characteristics to ensure appropriate deployment.

1. Plan your fiber connections. Use the same plan for all 1+1 nodes.
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-optic cable 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 fiber-optic cables are mismatched (one fiber-optic cable connects a receive port on one card to a receive port on another card, or the same situation with transmit ports). Figure 19-1 shows the cable location.
3. Repeat Steps 1 and 2 for the corresponding protect ports on the two nodes and for all other working/protect port pairs that you want to place in a 1+1 configuration.
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 *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. In node view, click the **Maintenance > Ether Bridge > Circuits** tabs.
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 Spanning Tree Protocol ID number.

- VLANS-Lists the VLANs associated with the circuit or port.

3. Return to your originating procedure (NTP).

DLP-A431 Change the JRE Version

Purpose	This task changes the JRE version, which is useful if you would like to upgrade to a later JRE version from earlier one without using the software 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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the Edit menu, choose **Preferences**.
2. Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.
3. Click the **Browse** button and navigate to the JRE directory on your computer.
4. Choose the JRE version.
5. Click **OK**.
6. From the File menu, choose **Exit**.
7. In the confirmation dialog box, click **Yes**.
8. Complete the "DLP-A60 Log into CTC" task.
9. Return to your originating procedure (NTP).

DLP-A433 Enable Node Secure Mode

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

Caution! The IP address assigned to the TCC2P TCP/IP (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 the ONS 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.

1. In node view, click the **Provisioning > Security > Data Comm** tabs.
2. Click **Change Mode**.
3. Review the information on the Change Secure Mode wizard page, then click **Next**.

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 or the ONS 15454 default router.
5. Click **Next**.
6. On the Backplane Ethernet Port page, modify the backplane IP address, subnet mask, and default router, if needed. (Normally, you do not need to modify these fields if no ONS 15454 network changes have occurred.)
7. Click **Next**.
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 where the CTC computer is connected. The computer is not visible to the data communications channel (DCC)-connected nodes. By default, SOCKS proxy is not enabled for an ENE. If SOCKS proxy is disabled, the NE cannot communicate with other secure mode NEs behind the firewall.
   - 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. By default, configuring the secure node as a GNE also enables SOCKS proxy for communication with other secure NEs.
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 changes to gray and a DISCONNECTED condition appears.
10. In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)
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.
    1. Display the node in node view.
    2. Click the **Provisioning > Security > Data Comm** tabs.
    3. If you do not want the IP address to appear on the LCD, in the LCD IP Setting field, choose **Suppress Display**.
    4. If you do not want the IP address to appear in CTC, 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.
    5. Click **Apply**.

       Note: After you turn on secure mode, the TCC2P IP (LAN) port address becomes the node's IP address. The backplane LAN port has a different IP address.
12. Return to your originating procedure (NTP).

DLP-A434 Lock Node Security

Purpose	This task locks the secure mode configuration on an ONS 15454. When secure mode is locked, two IP addresses must always be provisioned on the ONS 15454: one for the TCC2P TCP/IP (LAN) port and one for the backplane LAN port.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	DLP-A60 Log into CTC DLP-A433 Enable Node Secure Mode
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Superuser only

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

Note: For more information about secure mode, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*.

1. Click the **Provisioning > Security > Data Comm** tabs.
2. Click **Lock**.
3. In the Confirm Lock Secure Mode dialog box, click **Yes**.
4. Return to your originating procedure (NTP).

DLP-A435 Modify Backplane Port IP Settings in Secure Mode

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 DLP-A60 Log into CTC DLP-A433 Enable Node Secure Mode
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

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

1. Click the **Provisioning > Security > Data Comm** tabs.
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 the IP address to be changed using the LCD buttons.
        - **Display only-**Displays the backplane IP address on the LCD but does not allow the IP address 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, displays node IP information only to Superusers (that is, not to Provisioning, Maintenance, or Retrieve-level users) in the CTC Provisioning > General > Network tab; the Provisioning > Security > Data Comm tab, and the CTC node view information area.
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.

4. Return to your originating procedure (NTP).

DLP-A436 Disable Node Security Mode

Purpose	This task disables the ONS 15454 secure mode, meaning dual-IP addresses are no longer supported.With secure mode disabled, only one IP address can be provisioned for both the backplane LAN port and the TCC2P TCP/IP (LAN) port. If secure mode is disabled for a node, that node cannot identify other network nodes that are in secure mode.
Tools/Equipment	TCC2P cards must be installed.
Prerequisite Procedures	NTP-A108 Back Up the Database DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

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

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

1. Click the **Provisioning > Security > Data Comm** tabs.
2. Click **Change Mode**.
3. Review the information on the Change Secure Mode wizard page, then click **Next**.
4. On the Node IP Address page, choose the address you want to assign to the node:
   - Backplane Ethernet (LAN) Port-Assigns the backplane IP address as the node IP address.
   - TCC Ethernet (LAN) 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.
5. Click **Next**.
6. On the SOCKS Proxy Server Settings page, choose one of the following:
   - **External Network Element (ENE)**-If selected, SOCKS proxy is disabled by default, and the CTC computer is only visible to the ONS 15454 where the CTC computer is connected. The computer is not visible to the secure mode, DCC-connected nodes. Firewall is enabled, which means that the node prevents IP traffic from being routed between the DCC and the LAN port.
   - **Gateway Network Element (GNE)**-If selected, the CTC computer is visible to other DCC-connected nodes, and SOCKS proxy remains enabled. However, the node prevents IP traffic from being routed between the DCC and the LAN port.
   - **Proxy-only**-If selected, the ONS 15454 responds to CTC requests with a list of DCC-connected nodes within the firewall for which the node serves as a proxy. The CTC computer is visible to other DCC-connected nodes. The node does not prevent traffic from being routed between the DCC and LAN port.
7. Click **Finish**.

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

8. In the CTC Alerts dialog box, click **Close**. Wait for the reboot to finish. (This might take several minutes.)
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 VCAT circuits must exist on the network. See the NTP-A264 Create an Automatically Routed VCAT Circuit or the NTP-A265 Create a Manually Routed VCAT Circuit.
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 member that does not use the link capacity adjustment scheme (LCAS) if the new state matches the In Group VCAT state of the other members, or 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.

1. In node or network view, click the **Circuits** tab.
2. Click the VCAT circuit that you want to edit, then click **Edit**.
3. Click the **Members** tab.
4. Select the member that you want to change. To choose multiple members, press **Ctrl** and click each member.
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.
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 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.

Note the following behavior of the two VCAT members on ML-Series cards (both SW-LCAS and non-LCAS members):

- When changing a member from the IS-NR to the OOS-MT, MT or the OOS-MA,DSBLD service state, changing the service state of the first member causes both members to change service state autonomously.
- When changing a member from the OOS-MA,DSBLD to the OOS-MT, MT or the IS-NR service state, you must begin with the second VCAT member. For example, change the service state of the second member first, and then the first member. You cannot change the service state of the first member if the second member is in another service state.

7. Click **Apply**.
8. To close the Edit Circuit window, choose **Close** from the File menu.
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
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

1. In node view, double-click the FC_MR-4 card where you want to change the port settings.
2. Click the **Provisioning > Port > General** tabs.
3. Modify any of the settings described in Table 21-3 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.
4. Click **Apply**.

Table 21-3: FC_MR-4 Card General Port Settings

Parameter	Description	Options
Port	(Display only) 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. **Note:** If this port's Fibre Channel or FICON link will be discovered by the Cisco MDS Fabric Manager for use with a Cisco MDS 9000 switch, you must provision the Fiber Channel/FICON port name to the following string: FC: switch> interface> Where switch> is the DNS name or IPv4/v6 address of the Cisco MDS 9000 switch, and interface> is the card slot/port of the FC_MR-4 port you are assigning a name. Example: FC: 10.0.0.1 fc2/4
Admin State	Changes the port administrative service state unless network conditions prevent the change.	• IS-Puts the port in-service. The port service state changes to IS-NR.

		• IS,AINS-Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS. • 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. **Note:** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	• IS-NR-The port is fully operational and performing as provisioned. • OOS-MA,DSBLD-The port is out-of-service and unable to carry traffic. • OOS-MA,MT-The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.
Port Rate	Selects the fiber channel interface.	• 1 Gbps • 2 Gbps
Link Rate	(Display only) Shows the actual rate of the port.	-
Max GBIC Rate	(Display only) Shows 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.	• Yes • No
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

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

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

1. In node view, double-click the FC_MR-4 card where you want to change the port settings.
2. Click the **Provisioning > Port > Distance Extension** tabs.
3. Modify any of the settings described in Table 21-4 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.
4. Click **Apply**.

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

Parameter	Description	Options
Port	(Display only) 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 (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 Fibre Channel/FICON port.	Numeric. 2 through 256, multiples of 2 only
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

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

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

1. In node view, double-click the FC_MR-4 card where you want to change the port settings.
2. Click the **Provisioning > Port > Enhanced FC/FICON** tabs.
3. Modify any of the settings described in Table 21-5 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.
4. Click **Apply**.

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

Parameter	Description	Options
Port	(Display only) Port number.	1 through 4
Ingress Idle Filtering	If checked, prevents removal of excess Fibre Channel/FICON IDLE codes from SONET transport. IDLEs are 8b10b control words that are sent between frames or appear when there is no data to send. Ingress idle filtering applies only to SONET circuit bandwidth sizes that allow full line rate Fibre Channel/FICON transport. It can be used for interoperability with remote Fibre Channel/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

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 UBIC-H 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

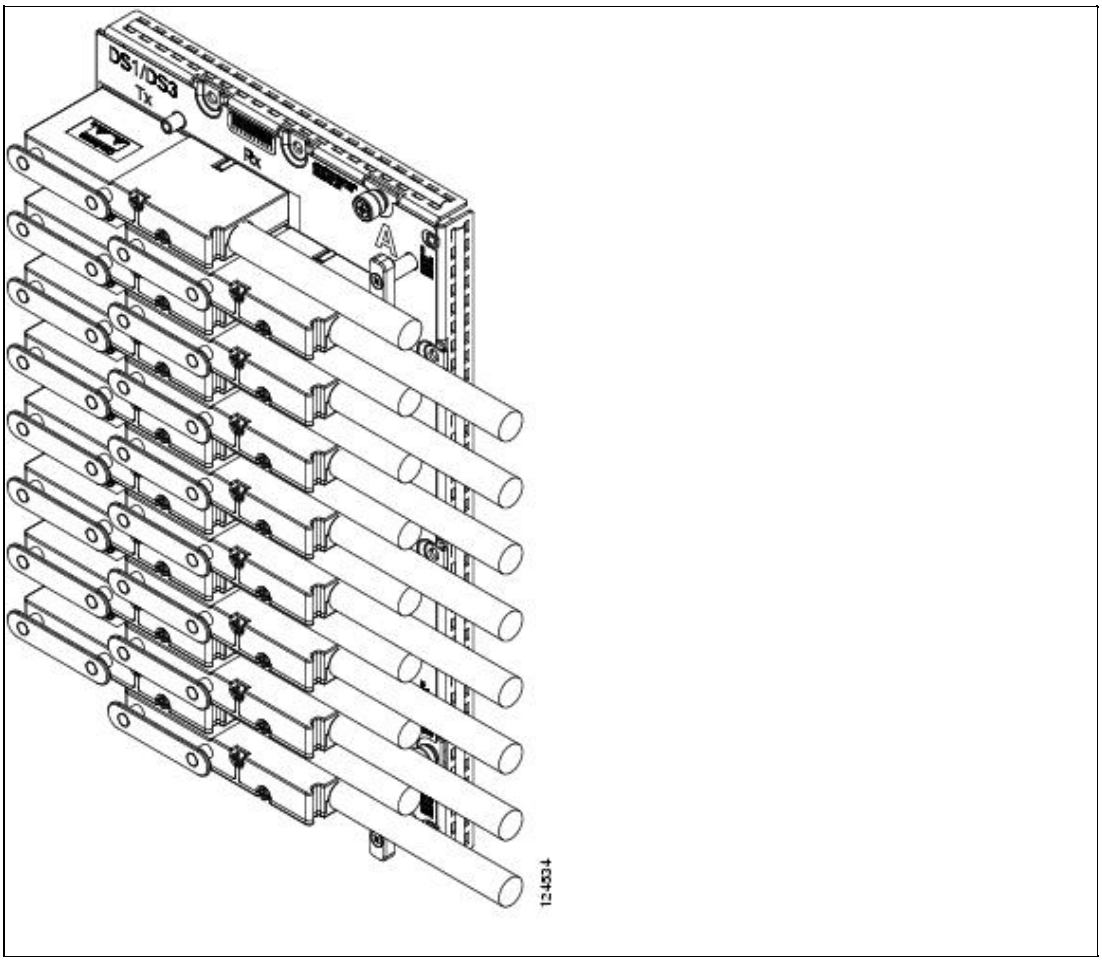
	• 15454-CADS1-H-250 • 15454-CADS1-H-350 • 15454-CADS1-H-450 • 15454-CADS1-H-550 • 15454-CADS1-H-655 • 15454-CADS3-SD • 15454-CADS3-ID • 15454-CADS3-LD
Prerequisite Procedures	DLP-A399 Install a UBIC-H EIA
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

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



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.
6. Return to your originating procedure (NTP).

DLP-A442 Verify Pass-Through Circuits

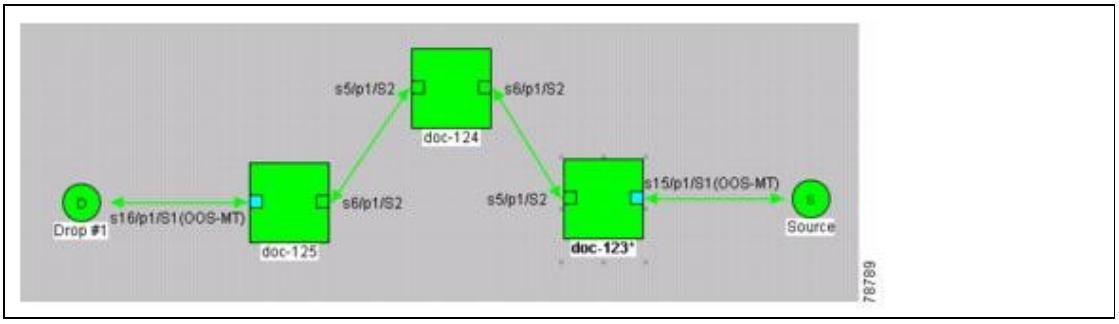
Purpose	This task verifies that circuits passing through a node enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the CTC Circuits window, choose a circuit that passes through the node that will be removed and click **Edit**.
2. In the Edit Circuits window, check **Show Detailed Map**.
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

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

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



4. Repeat Steps 1 to 3 for each circuit in the Circuits tab.
5. Delete and recreate each circuit recorded in Step 3. To delete the circuit, see the "DLP-A333 Delete Circuits" task. To create the circuit, see Create Circuits and VT Tunnels.
6. Return to your originating procedure (NTP).

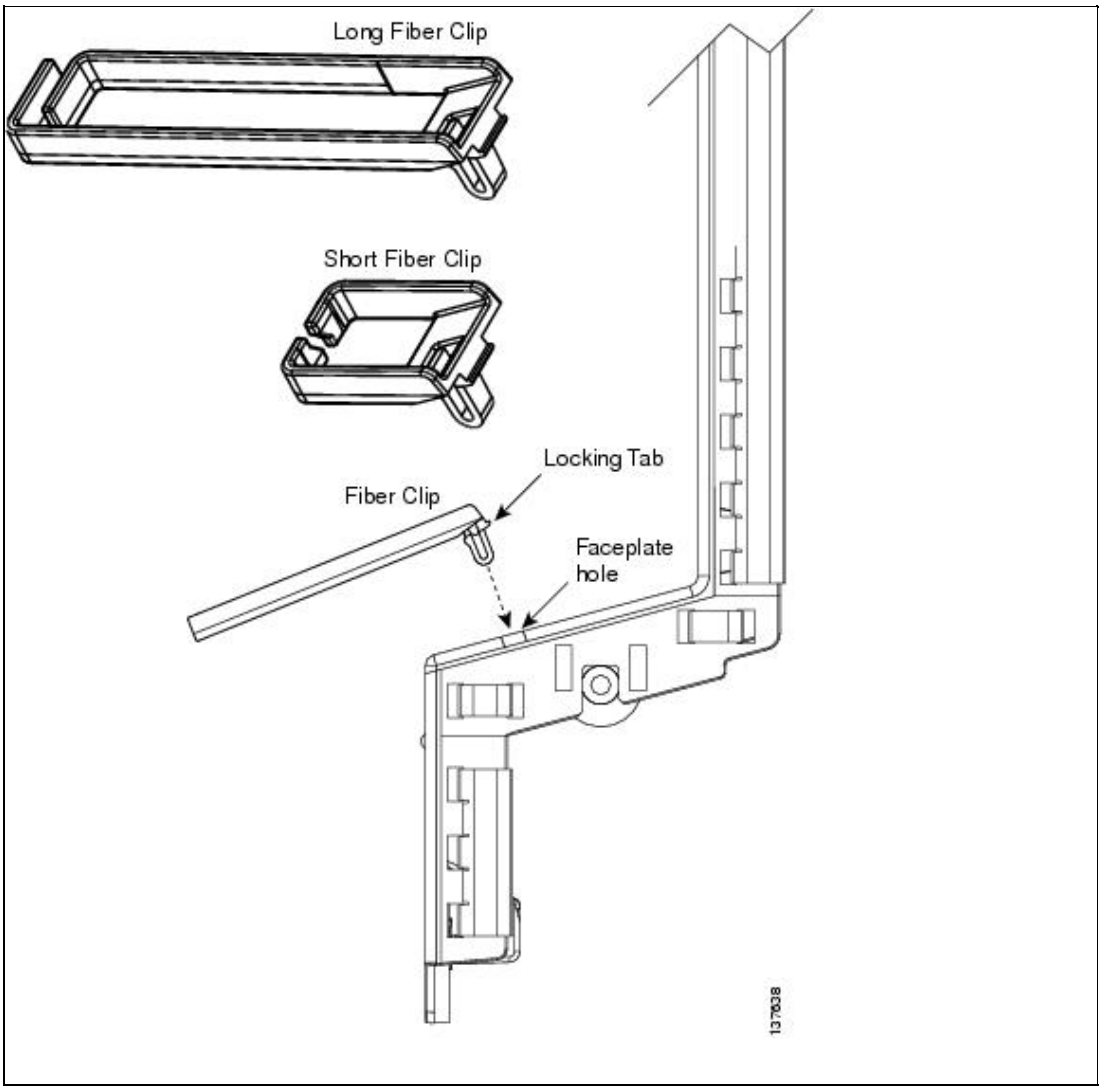
DLP-A443 Install the Fiber Clip on 15454_MRC-12 Cards

Purpose	This task installs a fiber clip, which allows proper routing of the fiber. Required for 15454_MRC-12 cards (known as the MRC-12 in CTC).
Tools/Equipment	Short or long fiber clip, as needed. Short clip: 52-0629-01 Long clip: 52-0628-01
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Note: You can install the fiber clip before or after the fibers are attached to the 15454_MRC-12 card.

1. Determine the correct clip to use. Use the short clip with a standard cabinet door and a long clip with an extended door.
2. Insert the prong of the fiber clip into the rectangular cutout on the sloped face of the faceplate (Figure 21-3).

Figure 21-3: Installing the Fiber Clip



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

DLP-A448 Convert DS3XM-6 or DS3XM-12 Cards From 1:1 to 1:N Protection

Purpose	This task converts DS3XM-6 or DS3XM-12 cards in 1:1 protection to 1:N protection. A 1:N protection group can protect a maximum of five working cards.
Tools/Equipment	DS3XM-12 card(s) Protection groups with either DS3XM-6 or DS3XM-12 cards
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Note: This procedure assumes that either DS3XM-6 or DS3XM-12 cards are installed in Slots 1 to 6 and/or Slots 12 to 17. If there are DS3XM-6 cards in Slots 3 or 15, which are the protection slots, they will be replaced with a DS3XM-12 cards.

Figure 21-3: Installing the Fiber Clip

1. In node view, click the **Maintenance > Protection** tabs.
2. Click the protection group containing Slot 3 or Slot 15. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-6 card, continue with Step 3. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-12 card, continue with Step 5.
3. Make sure the slot that you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby, and not Protect/Active. If the protect slot status is Protect/Active, switch traffic to the working card:
    1. Under Selected Group, click the protect card.
    2. Next to Switch Commands, click **Switch**.

        The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.
4. Repeat Steps 2 and 3 for each protection group that you need to convert.
5. Click the **Alarms** tab to verify that no standing alarms exist for any of the DS3-12 cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.
6. Click the **Provisioning > Protection** tabs.
7. Click the 1:1 protection group that contains the cards that you will move into the new protection group.
8. Click **Delete**.
9. When the confirmation dialog box appears, click **Yes**.

    Note: Deleting 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Therefore, complete this procedure as soon as possible.
10. If you are deleting more than one DS-3 1:1 protection group, repeat Steps 7 through 9 for each group that you want to include in a 1:N group.
11. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-6 card, physically remove the protect DS3-12 card from Slot 3 or Slot 15. This raises an improper removal (IMPROPRMVL) alarm. If the 1:1 protect card in Slot 3 or Slot 15 is a DS3XM-12 card, continue with Step 16.
12. In node view, right-click the slot that held the removed card and choose **Delete** from the shortcut menu. Wait for the card to disappear from the node view.
13. Physically insert a DS3XM-12 card into the same slot.
14. Verify that the card boots up properly.
15. Click the **Inventory** tab and verify that the new card appears as a DS3XM-12 card.
16. Click the **Provisioning > Protection** tabs.
17. Click **Create**.
18. Type a name for the protection group in the Name field (optional).
19. Click **Type** and choose **1:N (card)** from the drop-down list.
20. Verify that the DS3XM-12 card appears in the Protect Card field.
21. In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.
22. Click **OK**.

    The protection group should appear in the Protection Groups list on the Protection subtab.
23. Return to your originating procedure (NTP).

DLP-A449 Set Up SNMP for a GNE

Purpose	This procedure provisions simple network management protocol (SNMP) parameters so that you can use SNMP network management software with the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

   Note: The ONS firewall proxy feature only operates on nodes running releases 4.6 and later. Using this information effectively breaches the ONS firewall to exchange management information.
   For more information about the SNMP proxy feature, refer to the "SNMP" chapter of the *Cisco ONS 15454 Reference Manual*.

9. Click Apply.
10. Return to your originating procedure (NTP).

DLP-A450 Set Up SNMP for an ENE

Purpose	This procedure provisions the SNMP parameters for an ONS 15454 configured to be an ENE if you use SNMP proxy on the GNE.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

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

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

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

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

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

         The SNMP proxy directs SNMP traps in the following general order: ENE > RELAY A > RELAY B > RELAY C > NMS. The following parameters also apply:
       - If there is are 0 intermediate relays, the order is ENE > RELAY A (GNE) > NMS
       - If there is 1 intermediate relay, the order is ENE > RELAY A (NE 1) > RELAY B (GNE) > NMS
       - If there is are 0 intermediate relays, the order is ENE > RELAY A (NE 1) > RELAY B (NE 2) > RELAY C (GNE) > NMS
11. Click Apply.
12. Repeat Step 2 through Step 11 for all NEs between the GNE and ENE.
13. Return to your originating procedure (NTP).

DLP-A451 Format and Enter NMS Community String for SNMP Command or Operation

Purpose	This procedure describes how to format a network management system (NMS) community string to execute the following SNMP commands for GNEs and ENEs: Get, GetBulk, GetNext, and Set.

Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

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

   - Formatted community string input example 1:
   `allviews{192.168.7.4,,,net7node4}`
   If "allviews" is a valid community name value at the proxy-enabled SNMP agent (the GNE), the GNE is expected to forward the PDU to 192.168.7.4 at Port 161. The outgoing PDU will have "net7node4" as the community name. This is the valid community name for the ENE with address 192.168.7.4.
   - Formatted community string input example 2:
   `allviews{192.168.7.99,,,enter7{192.168.9.6,161,,net9node6}}`
   If "allviews" is a valid community name value at the proxy-enabled GNE, the GNE is expected to forward the PDU to 192.168.7.99 at the default port (Port 161) with a community name of "enter7{192.168.9.6,161,,net9node6}". The system with the address 192.168.7.99 (the NE between the GNE and ENE) forwards this PDU to 192.168.9.6 at Port 161 (at the ENE) with a community name of "net9node6". The community name "enter7" is valid for the NE between the GNE and the ENE and "net9node6" is a valid community name for the ENE.

3. Log into the NMS where the browser is installed to retrieve the network information from the ONS 15454.
4. On the same computer, go to Start and click the SNMP MIB browser application.
5. In the Host and Community areas, enter the IP address of the GNE through which the ONS 15454 with the information to be retrieved can be reached.
6. In the Community area, enter the community string as explained in Step 2.
7. Return to your originating procedure (NTP).

DLP-A452 Create a VLAN

Purpose	This task creates a new VLAN.
Tools/Equipment	None
Prerequisite Procedures	See Create Circuits and VT Tunnels for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the View menu, choose **Go to Network View**.
2. From the Tools menu, choose **Manage VLANS**.
3. In the All VLANs dialog box, click **Create**.
4. In the Define New VLAN dialog box, complete the following:
   - VLAN Name-Assign an easily identifiable name to your VLAN.
   - VLAN ID-Assign a VLAN ID. The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.
   - Topology Host-Choose the node to serve as the topology host from the drop-down list. The topology host is used to discover the VLAN topology. The login node is the default.
5. Click **OK**.
6. Click **Close**.
7. Return to your originating procedure (NTP).

DLP-A453 Delete a Server Trail

Purpose	This task deletes a server trail.
Tools/Equipment	None
Prerequisite Procedures	NTP-A326 Create a Server Trail DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > Server Trails** tabs.
3. Click the server trail that you want to delete.
4. Click **Delete**.
5. In the confirmation dialog box, click **Yes**.

Note: You can use the server trail audit log to recreate a server trail that you may have accidentally deleted. The server trail audit log includes the following parameters:

- Server trail ID
- Peer IP address
- Circuit size
- Protection type
- Number of trails
- Starting STS/VT
- SRLG value

You can look at the audit log of the source or destination node and find the entry for the delete call. This log entry has the STS/VT path definitions on the node, peer IP address, and server trail ID. You can then look at the audit log of the peer IP address, locate the delete call for the specific server trail ID, and find the STS/VT path definitions on the node. This would provide you with the required information to recreate the server trail.

6. Return to your originating procedure (NTP).

DLP-A454 View the BLSR STS Squelch Table

Purpose	This task allows you to view the BLSR STS squelch table for an ONS 15454 BLSR node. For example, if a fiber cut occurs, the BLSR STS squelch tables show STSs that will be squelched for every isolated node. Squelching replaces traffic by inserting the appropriate alarm indication signal path (AIS-P); it prevents traffic misconnections. For an STS with a VT-access check mark, the AIS-P will be removed after 100 ms. For more information about BLSR squelching, refer to Telcordia GR-1230.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. To open the squelch table in node view:
    1. In node view, click the **Provisioning > BLSR** tabs.
    2. Click the BLSR whose squelch table you want to view.
    3. Click Squelch Table.
2. To open the squelch table in network view:
    1. In network view, click the **Provisioning > BLSR** tabs.
    2. Click the BLSR whose squelch table you want to view.
    3. Click **Edit**.
    4. Right-click a node in the **Edit** window.
    5. Click Squelch Table from the drop-down list.
3. 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 VT (from the West Source)-A check mark indicates that the STS carries incoming VT traffic. The traffic source is coming from the west side.
    - West VT (from the West Destination)-A check mark indicates that the STS carries outgoing VT traffic. The traffic is dropped on the west side.
    - 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 VT (from the East Source)-A check mark indicates that the STS carries incoming VT traffic. The traffic source is coming from the east side.
    - East VT (from the East Destination)-A check mark indicates that the STS carries outgoing VT traffic. The traffic is dropped on the east side.
    - 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.
4. Return to your originating procedure (NTP).

DLP-A455 View the BLSR VT Squelch Table

Purpose	BLSR VT squelch tables only appear on the node dropping VTs from a BLSR and are used to perform VT-level squelching when a node is isolated. VT squelching is supported on the ONS 15454 and the ONS 15327 platforms. The ONS 15600 platform does not support VT squelching; however, when an ONS 15454 and an ONS 15600 are in the same network, the ONS 15600 node allows the ONS 15454 node to carry VT circuits in a VT tunnel. The ONS 15600 performs 100-ms STS-level squelching for each VT-access STS at the switching node in case of a node failure. For more information about BLSR squelching, refer to Telcordia GR-1230.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

1. To open the squelch table in node view:
    1. In node view, click the **Provisioning > BLSR** tabs.
    2. Click the BLSR whose squelch table you want to view.
    3. Click Squelch Table.
2. To open the squelch table in network view:
    1. In network view, click the **Provisioning > BLSR** tabs.
    2. Click the BLSR whose squelch table you want to view.
    3. Click **Edit**.
    4. Right-click a node in the **Edit** window.
    5. Choose Squelch Table from the drop-down list.
3. In the BLSR STS Squelch Table window, double-click the VT check mark. In the BLSR VT Squelch Table window you can view the following information:

    Note: The check mark appears on every VT-access STS; however, the VT squelch table appears only by double-clicking the check mark on the node dropping the VT. The intermediate node of the VT does not maintain the VT-squelch table.

    - VT Number-Shows the BLSR VT numbers. The VT number includes VT group and channel (VT group 2 and channel 1 are displayed as 2-1.)
    - 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.)
    - East Source-If traffic is received by the node on its east span, the BLSR node ID of the source appears.
4. Return to your originating procedure (NTP).

DLP-A456 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-A60 Log into CTC

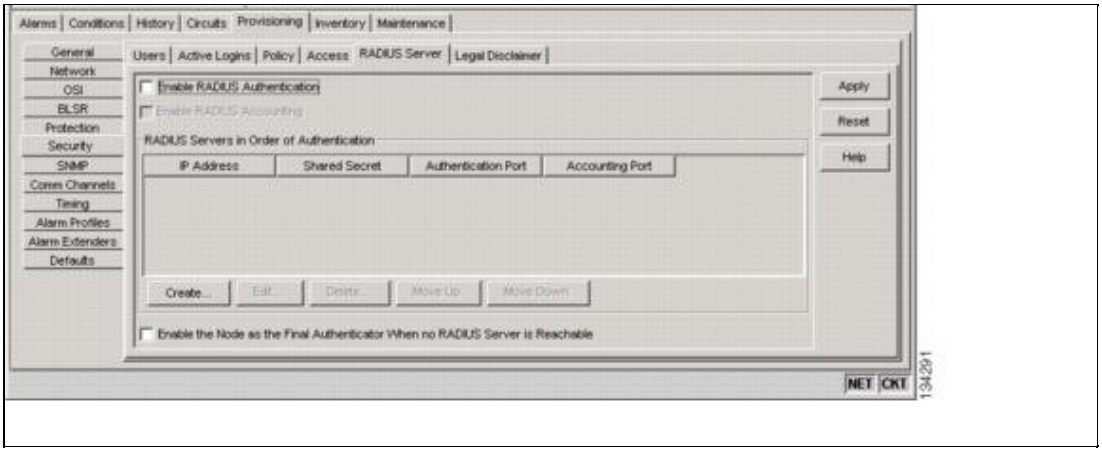
	Before configuring the node for RADIUS authentication, you must first add the node as a network device on the RADIUS server. Refer to the User Guide for Cisco Secure ACS for Windows Server for more information about configuring a RADIUS server.
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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.

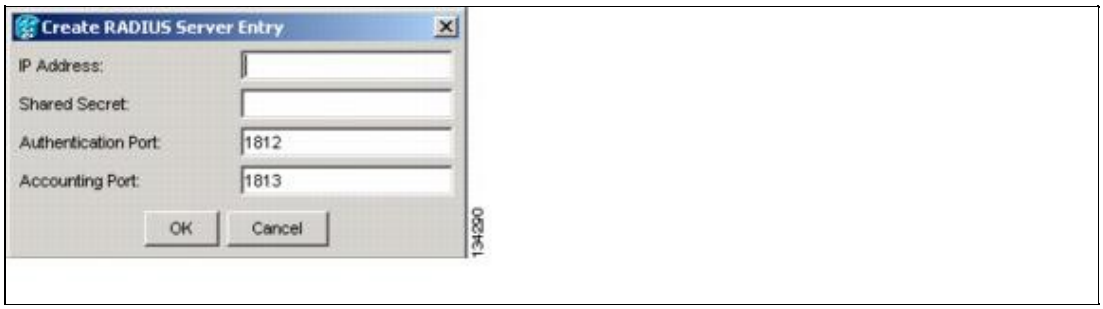
1. In node view, click the Provisioning > Security > RADIUS Server tabs (Figure 21-4).

Figure 21-4: RADIUS Server Tab



2. Click Create to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 21-5).

Figure 21-5: Create RADIUS Server Entry Window



3. Enter the RADIUS server IP address in the IP Address field. If the node is an end network element (ENE), enter the IP address of the gateway network element (GNE) in this field. The GNE passes authentication requests from the ENEs in its network to the RADIUS server, which grants authentication if the GNE is listed as a client on the server. **Caution!** Because the ENE nodes use the

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

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

   Note: You can add up to 10 RADIUS servers to a node's list of authenticators.
8. Click Edit to make changes to an existing RADIUS server. You can change the IP address, the shared secret, the authentication port, and the accounting port.
9. Click Delete to delete the selected RADIUS server.
10. Click Move Up or Move Down to reorder the list of RADIUS authenticators. The node requests authentication from the servers sequentially from top to bottom. If one server is unreachable, the node will request authentication from the next RADIUS server on the list.
11. Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.
12. Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.
13. Click the **Enable the Node as the Final Authenticator** check box if you want the node to be the final autheticator. This means that if every RADIUS authenticator is unavailable, the node will authenticate the login rather than locking the user out.
14. Click Apply to save all changes or Reset to clear all changes.
15. Return to your originating procedure (NTP).

DLP-A457 Grant Superuser Privileges to a Provisioning User

Purpose	This task enables a provisioning user to perform tasks such as retrieve an audit log, restore a database, and activate and revert a software load.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

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

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

   Note: You must close your current CTC session and restart a new CTC session for the changes to take effect.

5. Return to your originating procedure (NTP).

DLP-A458 Clear All PM Thresholds

Purpose	This task clears and resets all PM thresholds to the default values.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution! Pressing the Reset button can mask problems if used incorrectly. This button is commonly used for testing purposes.

1. In node view, double-click the card where you want to view PM thresholds. The card view appears.
2. Click the **Provisioning > Threshold** tab. The subtab names vary depending on the card selected.
3. Click **Reset to Default**.
4. Click **Yes** in the Reset to Default dialog box.
5. Verify that the PM thresholds have been reset.
6. Return to your originating procedure (NTP).

DLP-A459 Change Optics Thresholds Settings for OC-192, MRC-12, and MRC-2.5G-4 Cards

Purpose	This task changes the optics thresholds settings for OC-192, MRC-12, and MRC-2.5G-4 cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

1. In node view, double-click the card where you want to change the optics settings.
2. Click the **Provisioning > Optics Thresholds** tabs.

   Note: If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.
3. Modify any of the settings described in Table 21-6 by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.
4. Click **Apply**.

Table 21-6: Optics Thresholds Settings

Parameter	Description	Options
Port	(Display only) Port number.	• 1 (OC-192,

		OC192-XFP) • 1-12 (MRC_12) • 1-4 (MRC-2.5G-4)
LBC-LOW	Laser bias current-minimum.	Default (15 min/1 day): 50 percent
LBC-HIGH	Laser bias current-maximum.	Default (15 min/1 day): 150 percent
OPT-LOW	Optical power transmitted-minimum.	Default (15 min/1 day): 80 percent
OPT-HIGH	Optical power transmitted-maximum.	Default (15 min/1 day): 120 percent
OPR-LOW	Optical power received-minimum.	Default (15 min/1 day): 50 percent
OPR-HIGH	Optical power received-maximum.	Default (15 min/1 day): 200 percent
Set OPR	Setting the optical power received establishes the received power level as 100 percent. If the receiver power decreases, then the OPR percentage decreases to reflect the loss in receiver power. For example, if the receiver power decreases by 3 dBm, the OPR decreases 50 percent.	Click **SET**.
Types	Sets the threshold values of alerts that trigger an alarm or TCA response. To view the provisionable thresholds that generate an Alarm or TCA, choose the type and click **Refresh**.	• TCA (threshold cross alert) • Alarm
Intervals	Sets the time interval for collecting parameter counts. To change the time interval, choose the desired interval and click **Refresh**.	• 15 Min • 1 Day

5. Return to your originating procedure (NTP).

DLP-A460 Reset a Traffic Card Using CTC

Purpose	This task resets an optical, electrical, E-Series Ethernet, G-Series Ethernet, ML-Series Ethernet, or CE-1000-4 Ethernet card in CTC. The CE100T-8 Ethernet card has unique reset tasks; see the "DLP-A54 Hard-Reset a CE-100T-8 Card Using CTC" task or the "DLP-A224 Soft-Reset a CE-100T-8 Card Using CTC" task for more information.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note: To reset transponder (TXP) or muxponder (MXP) cards, refer to the *Cisco ONS 15454 DWDM Procedure Guide*.

Caution! If you soft reset a working electrical card that is part of a protection group, while the card is rebooting do not unlock that card or the protect card that protects the reset working electrical card. If you do so, a traffic loss will result. Wait until the working electrical card fully reboots before reversing a lock-out on protect on the protect card or reversing a lock-on on the working card. This applies to all electrical cards except the E1-42 card.

1. In node view, position the cursor over the traffic card slot.
2. Right-click the card and choose **Reset Card** from the shortcut menu.
3. Click **Yes** in the Resetting Card dialog box.
4. Return to your originating procedure (NTP).

DLP-A461 Preprovision an SFP or XFP Device

Purpose	This task preprovisions SFPs/XFPs on the MRC-12, MRC-2.5G-4, and OC192-XFP cards. Cisco-approved OC-3, OC-12, OC-48, OC-192 and multirate SFPs/XFPs are compatible with the ONS 15454. Refer to the *Cisco ONS 15454 Reference Manual* for a list of card and SFP/XFP compatibility. The SFPs/XFPs are referred to as pluggable port modules (PPMs) in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	None

Note: Before you install SFPs on the MRC-12 or MRC-2.5G-4 card, refer to the MRC-12 or MRC-2.5G-4 section in the "Optical Cards" chapter of the *Cisco ONS 15454 Reference Manual* for bandwidth restrictions based on the port where you install the SFP and the cross-connect card being used.

Note: If you preprovision a multirate SFP, you must next select the line rate using the "DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card" task.

1. In node view, click the **Alarms** tab:
    1. Verify that the alarm filter is not turned on. See the "DLP-A227 Disable Alarm Filtering" task as necessary.
    2. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide*.
    3. Complete the "DLP-A532 Export CTC Data" task to export alarm and condition information.
2. In node view, double-click the card where you want to provision PPM settings.
3. Click the **Provisioning > Pluggable Port Modules** tabs.
4. In the Pluggable Port Modules pane, click Create. The Create PPM dialog box appears.
5. In the Create PPM dialog box, complete the following:
    - PPM-Choose the slot number where you want to preprovision the SFP/XFP from the drop-down list.

- ♦ PPM Type-Choose the number of ports supported by your SFP/XFP from the drop-down list. If only one port is supported, PPM (1 port) is the only option.

6. Click **OK**. The newly created port appears 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/XFP is installed. After the SFP/XFP is installed, the row on the pane turns white and the column lists the equipment name.
7. Verify that the PPM appears in the list on the Pluggable Port Modules pane. If it does not, repeat Steps 4 through 6.
8. On the Provisioning tab, click the **Line** subtab. If applicable for the PPM you are preprovisioning, use the Reach and Wavelength columns to configure these parameters as needed.

   Note: Only the parameters that are editable for the PPMs on a particular platform type are provisionable. For example, some platforms may not have PPMs with configurable wavelengths or reaches. In that case, wavelength md reach ares not provisionable.
9. Repeat the task to create a second PPM.
10. Click **OK**.
11. When you are ready to install the SFP/XFP, complete the "DLP-A469 Install a GBIC or SFP/XFP Device" task.
12. Return to your originating procedure (NTP).

DLP-A462 View and Terminate Active Logins

Purpose	This task allows you to view active CTC logins, retrieve the last activity time, and terminate all current logins.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher for viewing; Superuser for session termination

1. In node view, click the **Provisioning > Security > Active Logins** tab. The Active Logins tab displays the following information:

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

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

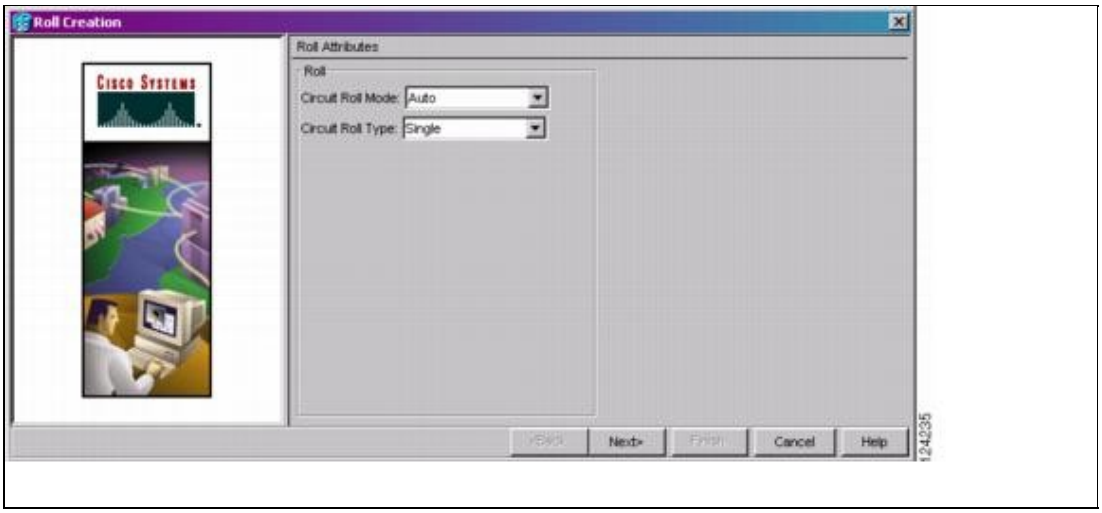
DLP-A463 Roll the Source or Destination of One Optical Circuit

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
	DLP-A60 Log into CTC

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

1. From the View menu, choose **Go To Network View**.
2. Click the **Circuits** tab.
3. Click the circuit that you want to roll. The circuit must have a DISCOVERED status for you to begin a roll.
4. From the Tools menu, choose **Circuits > Roll Circuit**.
5. In the Roll Attributes area, complete the following (Figure 21-6):
    1. 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).
    2. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll one cross-connect on the chosen circuit.

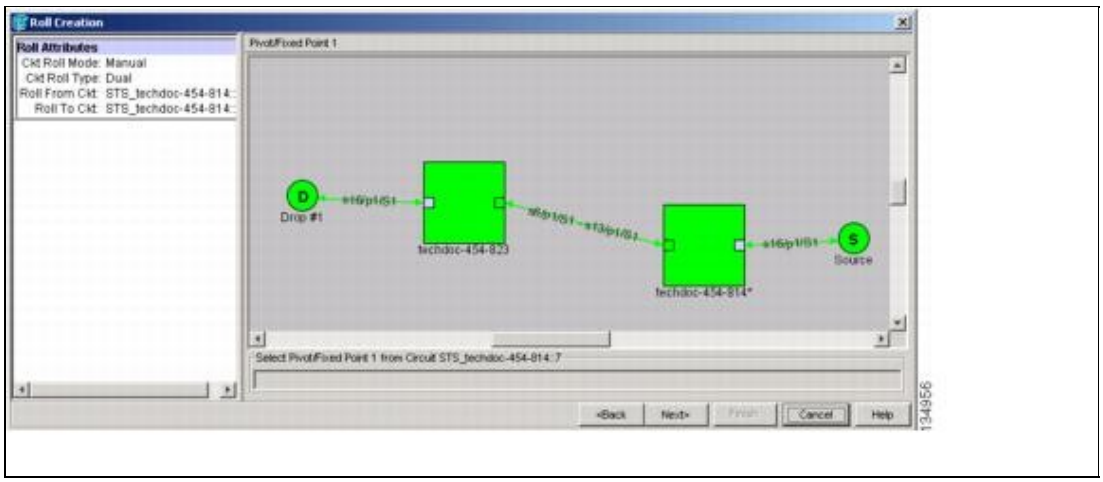
Figure 21-6: Selecting Single Roll Attributes



6. Click **Next**.
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 21-7).

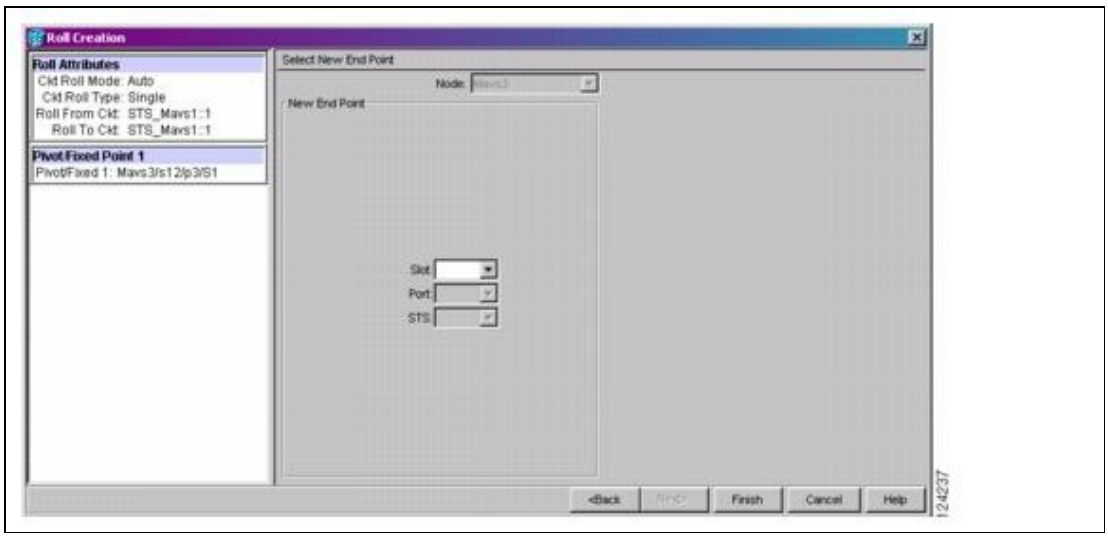
    This facility is the fixed location in the cross-connect involved in the roll process. The identifier appears in the text box below the graphic image. The facility that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed.

Figure 21-7: Selecting a Path



8. Click **Next**.
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 21-8).

Figure 21-8: Selecting a New Endpoint



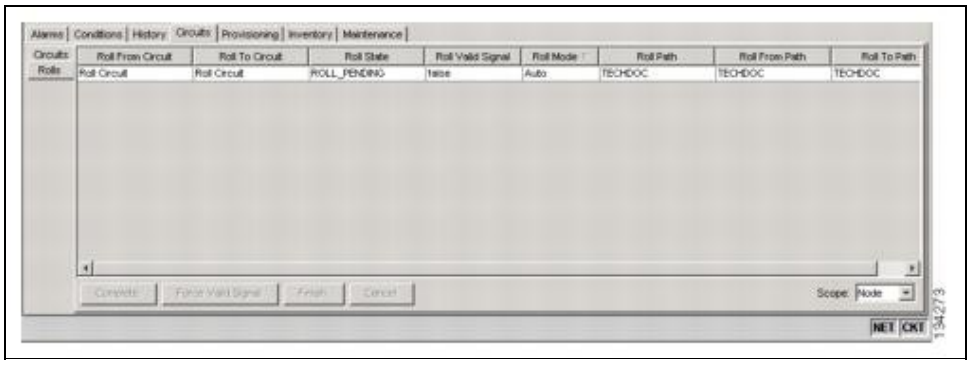
10. Click **Finish**. On the Circuits tab, the circuit status for the Roll From port changes from DISCOVERED to ROLL_PENDING.
11. Click the **Rolls** tab (Figure 21-9). For the pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 12.

    - 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 of the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task.
    - 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 21-9: Viewing the Rolls Tab



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.
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.
14. Return to your originating procedure (NTP).

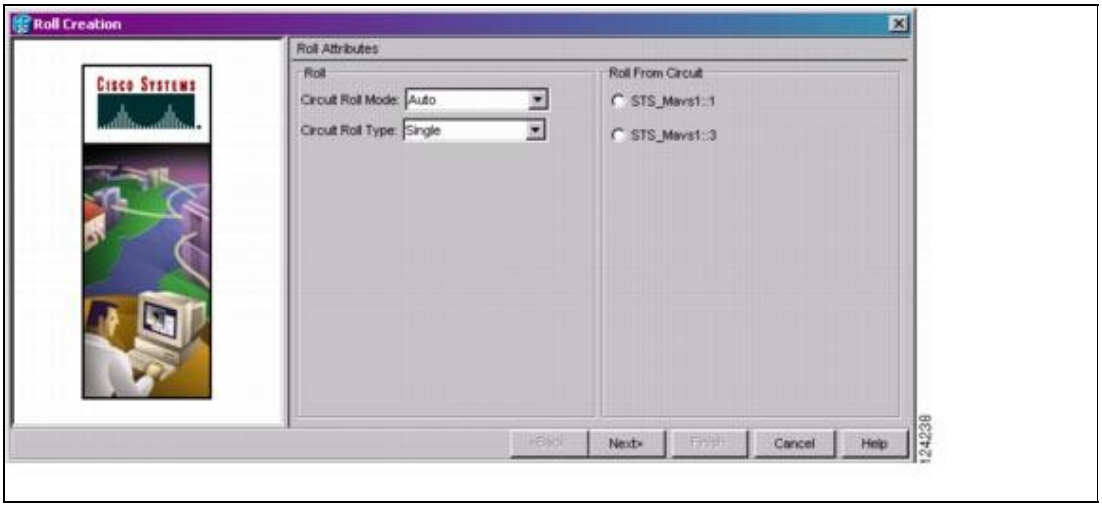
DLP-A464 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a cross-connect on one circuit onto another circuit, resulting in a new destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC DLP-A156 Delete a Section DCC Termination for the ports involved in the roll
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. From the View menu, choose **Go To Network View**.
2. Click the **Circuits** tab.
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 begin 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.
4. From the Tools menu, choose **Circuits > Roll Circuit**.
5. In the Roll Attributes area, complete the following (Figure 21-10):
   1. 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).
   2. 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.
   3. In the Roll From Circuit area, click the circuit that contains the Roll From connection.

Figure 21-10: Selecting Roll Attributes for a Single Roll onto a Second Circuit



6. Click **Next**.
7. In the Pivot/Fixed Point 1 window, click the square representing the facility that you want to keep (Figure 21-10).

   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.
8. Click **Next**.
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.
10. Click **Finish.**

    The statuses of the Roll From and Roll To circuits change from DISCOVERED to ROLL_PENDING in the Circuits tab.
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 of the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task.
    · 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 when the roll is completed.
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.
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.
14. Return to your originating procedure (NTP).

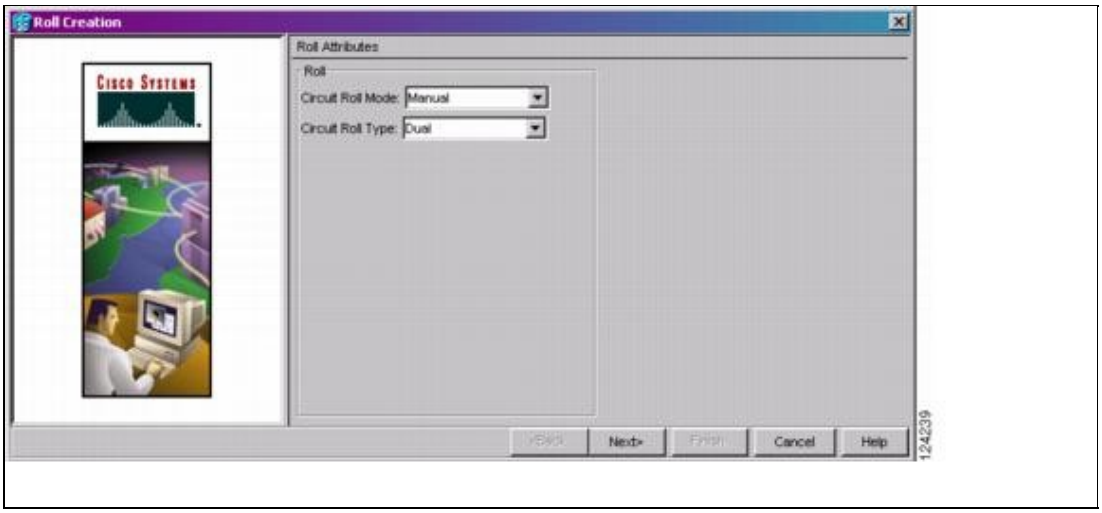
DLP-A465 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing

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-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: This task optionally uses automatic routing. Automatic routing is not available if both the Automatic Circuit Routing NE default and the Network Circuit Automatic Routing Overridable NE default are set to FALSE. For a full description of these defaults see the "Network Element Defaults" appendix in the *Cisco ONS 15454 Reference Manual*.

1. From the View menu, choose **Go To Network View**.
2. Click the **Circuits tab**.
3. Click the circuit that has the connections that you want to roll. The circuit must have a DISCOVERED status for you to begin a roll.
4. From the Tools menu, choose **Circuits > Roll Circuit**.
5. In the Roll Attributes area, complete the following (Figure 21-11):
    1. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.
    2. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Figure 21-11: Selecting Dual Roll Attributes



6. Click **Next**.
7. In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first connection to be rolled (Figure 21-11).

    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.

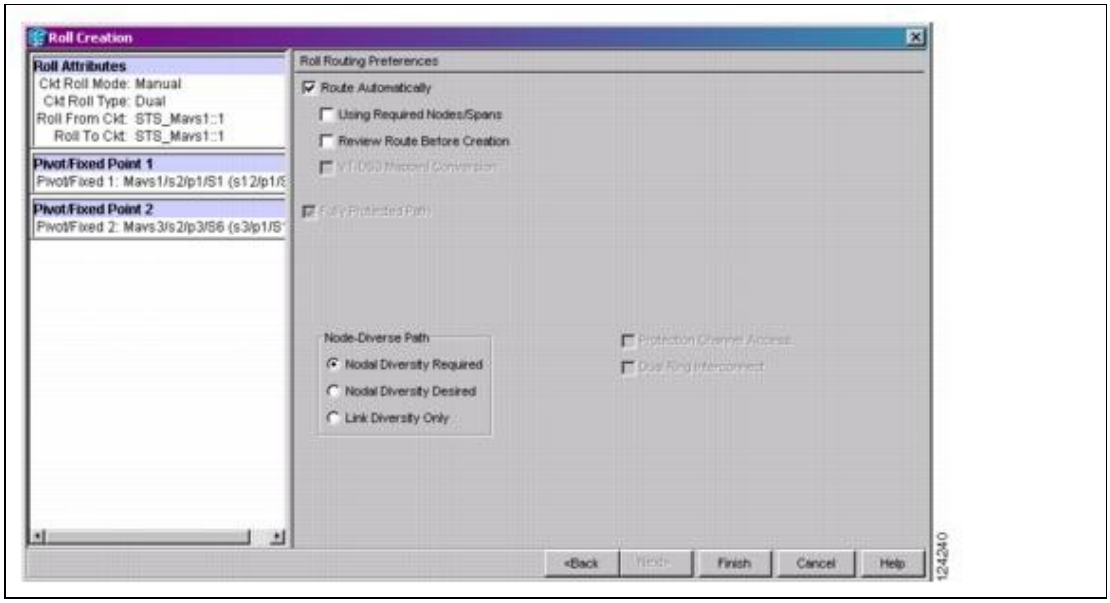
8. Click **Next**.
9. Complete one of the following:

   · 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.
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.
11. Click **Next**.
12. In the Circuit Routing Preferences area, check **Route Automatically** to allow CTC to find the route (Figure 21-12). 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 21-12: Setting Roll Routing Preferences



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.

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.

15. If you checked Using Required Nodes/Spans in Step 12:
    1. In the Roll Route Constraints area, click a node or span on the circuit map.
    2. 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.
    3. Repeat Substep 2 for each node or span you wish to include or exclude.
    4. 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.

16. If you checked Review Route Before Creation in Step 12:
    1. 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.
    2. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

    Caution! The following is only seen with DUAL roll mode when both ends of the circuit use the card(s) mentioned in this statement. If the termination card is a DS1/E1-56, DS1-14, DS1-N-14, DS3XM-6, or DS3XM-12 card, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of path payload defect indication (PDI-P) downstream for loss of signal (LOS), loss of frame alignment (LOF), and AIS line defects causes the roll to continue without a valid signal. On the DS1/E1-56, DS1-14, and DS1-N-14 cards, it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view Provisioning > Line tab. On the DS1-14 and DS1-N-14 cards, Send AIS-V for Ds1 AIS only works for VT circuits. On DS1/E1-56 cards, Send AIS-V for Ds1 AIS works for both STS and VT circuits.

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**.

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 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task.
    · 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 when the roll is completed.

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.
20. For both manual and automatic rolls, click **Finish** to complete circuit roll process.
21. Return to your originating procedure (NTP).

DLP-A466 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-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

1. From the View menu, choose **Go To Network View**.
2. Click the **Circuits tab.**
3. Click the circuit that you want to roll to a new path. The circuit must have a DISCOVERED status for you to begin a roll.
4. From the Tools menu, choose **Circuits > Roll Circuit**.
5. In the Roll Attributes area, complete the following (Figure 21-7):
    1. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.
    2. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.
6. Click **Next**.
7. In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 21-11: Selecting a Path).

    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.
8. Click **Next**.
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 21-12).
    - 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.
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.
11. Click **Next**.
12. In the Circuit Routing Preferences area, uncheck **Route Automatically**.
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.

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.
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.
16. Complete the "DLP-A369 Provision an OC-N Circuit Route" task.

Caution! The following is only seen with DUAL roll mode when both ends of the circuit use the card(s) mentioned in this statement. If the termination card is a DS1/E1-56, DS1-14, DS1-N-14, DS3XM-6, or DS3XM-12 card, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS1/E1-56, DS1-14, and DS1-N-14 cards, it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view Provisioning > Line tab. On the DS1-14 and DS1-N-14 cards, Send AIS-V for Ds1 AIS only works for VT circuits. On DS1/E1-56 cards, Send AIS-V for Ds1 AIS works for both STS and VT circuits.

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**.
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 of the *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task.
    · 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 when the roll is completed.
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.
20. For both manual and automatic rolls, click **Finish** to complete the circuit roll process.
21. Return to your originating procedure (NTP).

DLP-A467 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-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

1. From the View menu, choose **Go To Network View**.
2. Click the **Circuits** tab.
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 begin 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.
4. From the Tools menu, choose **Circuits > Roll Circuit**.
5. In the Roll Attributes area, complete the following:
   1. 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).
   2. From the Circuit Roll Type drop-down list, choose **Dual.**
   3. In the Roll From Circuit area, click the circuit that contains the Roll From path.
6. Click **Next**.
7. In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 21-7).
   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.
8. Click **Next**.
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 21-12).
   - 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.
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.
11. Click **Next**.

Caution! The following is only seen with DUAL roll mode when both ends of the circuit use the card(s) mentioned in this statement. If the termination card is a DS1/E1-56, DS1-14, DS1-N-14, DS3XM-6, or DS3XM-12 card, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS1/E1-56, DS1-14, and DS1-N-14 cards, it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected

from the card view Provisioning > Line tab. On the DS1-14 and DS1-N-14 cards, Send AIS-V for Ds1 AIS only works for VT circuits. On DS1/E1-56 cards, Send AIS-V for Ds1 AIS works for both STS and VT circuits.

12. Click **Finish**. In the Circuits tab, the Roll From and Roll To circuits change from the DISCOVERED status to ROLL PENDING.
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 *Cisco ONS 15454 Troubleshooting Guide*. To cancel the roll, see the "DLP-A489 Cancel a Roll" task.
    - 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 when the roll is completed.
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.
15. For both manual and automatic rolls, click **Finish** to complete the circuit roll process.
16. Return to your originating procedure (NTP).

DLP-A468 Delete a Roll

Purpose	This task deletes a roll. Use caution when selecting this option, traffic might be affected. Delete a roll only if it cannot be completed or cancelled in normal ways. Circuits might have a PARTIAL status when this option is selected. See Table 21-2 for a description of circuit statuses.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC NTP-A334 Bridge and Roll Traffic
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

DLP-A469 Install a GBIC or SFP/XFP Device

Purpose	This task installs GBICs (required for E-Series Ethernet, G-Series Ethernet, CE-1000-4, E1000-4, and FC_MR-4 cards) and SFPs/XFPs (required for CE-MR-10, ML1000-2, ML100X-8, ML-MR-10, MXP, MRC-12, MRC-2.5G-4, and OC192-XFP cards) and attaches fiber to the devices. GBICs, SFPs, and XFPs are hot-swappable input/output devices that plug into a traffic card port to link the port with the fiber-optic network. For a description of SFP/XFP devices on transponder or muxponder cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
Tools/Equipment	To determine which cards are compatible with which GBICs, SFPs, and XFPs, refer to the "Optical Cards" or "Ethernet Cards" chapters in the *Cisco ONS 15454 Reference Manual*.
Prerequisite Procedures	One or more of the following, depending on the card where you will install the GBIC or SFP/XFP device: • NTP-A16 Install Optical Cards and Connectors • DLP-A39 Install Ethernet Cards • NTP-A274 Install the FC_MR-4 Card
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

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

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

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

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

1. Remove the GBIC, SFP, or XFP from its protective packaging.
2. Check the label to verify that the GBIC, SFP, or XFP is the correct type for your network. Refer to the "Optical Cards" chapter in the *Cisco ONS 15454 Reference Manual* for a list of card and SFP/XFP compatibility.

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

   Note: Before you install SFPs on the MRC-12 or MRC-2.5G-4 card, refer to the MRC-12 or MRC-2.5G-4 card information in the *Cisco ONS 15454 Reference Manual* for bandwidth restrictions based on the port where you install the SFP and the cross-connect card being used.
3. Verify the type of GBIC, SFP, or XFP 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 or XFP, go to Step 6.

4. For GBICs with clips:
    1. 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.
    2. 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.
    3. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC, save the plug for future use, then plug the fiber connector into the GBIC.
    4. Continue with Step 7.
5. For GBICs with a handle:
    1. Remove the protective plug from the SC-type connector.
    2. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.
    3. 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.
    4. Slide the GBIC through the cover flap until you hear a click.
        The click indicates that the GBIC is locked into the slot.
    5. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC, save the plug for future use, then plug the fiber connector into the GBIC.
    6. Continue with Step 7.
6. For SFPs and XFPs:
    1. Plug the LC duplex connector of the fiber into a Cisco-supported SFP or XFP.
    2. If the new SFP or XFP has a latch, close the latch over the cable to secure it.
    3. Plug the cabled SFP or XFP into the card port until it clicks.

SFPs and XFPs must be provisioned in CTC. If you installed a multirate PPM, complete the "DLP-A574 Provision a PPM on the MRC-12 or MRC-2.5G-4 Card" task. (Single-rate XFPs do not need to be provisioned in CTC.)

7. Return to your originating procedure (NTP).

DLP-A470 Remove GBIC or SFP/XFP Devices

Purpose	This task disconnects fiber attached to GBICs, SFPs, or XFPs and removes the GBICs, SFPs, or XFPs from their cards.
Tools/Equipment	None
Prerequisite Procedures	DLP-A469 Install a GBIC or SFP/XFP Device
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

1. Disconnect the network fiber cable from the GBIC SC connector or the SFP/XFP LC duplex connector. If the SFP/XFP connector has a latch securing the fiber cable, pull it upward to release the cable.
2. If you are using a GBIC with clips:

   1. Release the GBIC from the slot by squeezing the two plastic tabs on each side of the GBIC.
   2. Slide the GBIC out of the slot. A flap closes over the slot to protect the connector on the Gigabit Ethernet card.
3. If you are using a GBIC with a handle:
   1. Release the GBIC by opening the handle.
   2. Pull the handle of the GBIC.
   3. Slide the GBIC out of the slot. A flap closes over the slot to protect the connector on the Gigabit Ethernet card.
4. If you are using an SFP/XFP:
   1. If the SFP/XFP connector has a latch securing the fiber cable, pull it upward to release the cable.
   2. Pull the fiber cable straight out of the connector.
   3. Unplug the SFP/XFP connector and fiber from the card.
   4. Slide the SFP/XFP out of the slot.
5. Return to your originating procedure (NTP).

DLP-A489 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, cancelling a 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-A60 Log into CTC NTP-A334 Bridge and Roll Traffic
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 after 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.

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

DLP-A495 Consolidate Links in Network View

Purpose	This task consolidates data communications channel (DCC), GCC, optical transport section (OTS), provisionable patchcord (PPC), and server trail links in the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed

Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

1. From the View menu, choose **Go to Network View**. CTC shows the link icons by default.
2. Perform the following steps as needed:

   - To toggle between the links, go to Step 3.
   - To consolidate all the links on the network map, go to Step 4.
   - To consolidate a link or links between two nodes, go to Step 5.
   - To view information about a consolidated link, go to Step 6.
   - To access an individual link within a consolidated link, go to Step 7.
   - To expand consolidated links, go to Step 8.
   - To filter the links by class, go to Step 9.

3. Right-click on the network map and choose **Show Link Icons** to toggle the link icons on and off.
4. To consolidate all the links on the network map (global consolidation):
   1. Right-click anywhere on the network map.
   2. Choose **Collapse/Expand Links** from the shortcut menu. The Collapse/Expand Links dialog window appears.
   3. Select the check boxes for the link classes you want to consolidate.
   4. Click OK. The selected link classes are consolidated throughout the network map.
5. To consolidate a link or links between two nodes (local consolidation):
   1. Right-click the link on the network map.
   2. Choose **Collapse Link** from the shortcut menu. The selected link type consolidates to show only one link.
      Note: The links consolidate by class. For example, if you select a DCC link for consolidation only the DCC links will consolidate, leaving any other link classes expanded.

Figure 21-13 shows the network view with unconsolidated DCC and PPC links.

Figure 21-13: Unconsolidated Links in the Network View

Output/145240.jpg

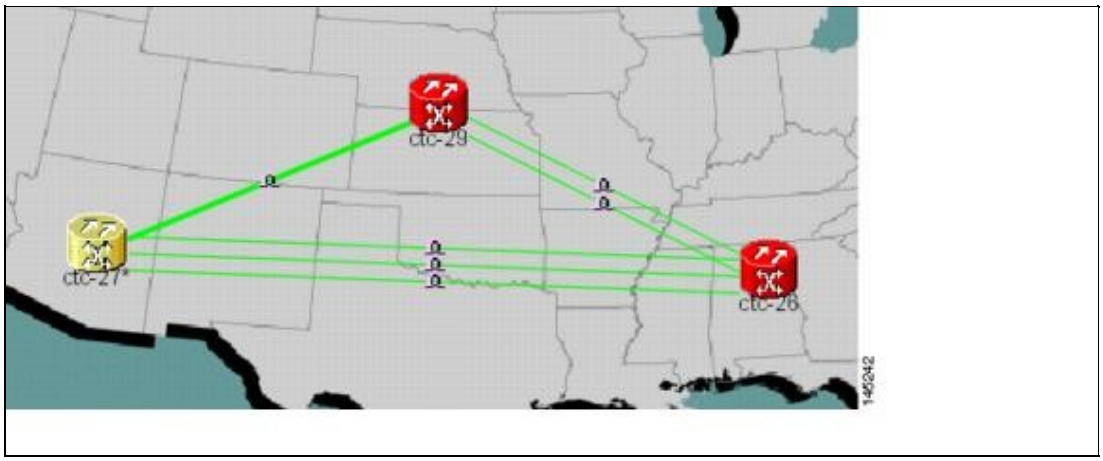
Figure 21-14 shows a network view with globally consolidated links.

Figure 21-14: Consolidated Links in the Network View

Output/145241.jpg

Figure 21-15 shows a network view with local DCC link consolidation between two nodes.

Figure 21-15: Network View with Local Link Consolidation



6. To view information about a consolidated link, either move your mouse over the link (the tooltip displays the number of links and the link class) or single-click the link to display detailed information on the left side of the window.
7. To access an individual link within a consolidated link (for example, if you need to perform a span upgrades):
    1. Right-click the consolidated link. A shortcut menu appears with a list of the individual links.
    2. Hover the mouse over the selected link. A cascading menu appears where you can select an action for the individual link or navigate to one of the nodes where the link is attached.
8. To expand locally consolidated links, right-click the consolidated link and choose **Expand [***link class***] Links** from the shortcut menu, where "link class" is DCC, GCC, OTS, PPC, or Server Trail.
9. To filter the links by class:
    1. Click the **Link Filter** button in the upper right area of the window. The Link Filter dialog appears.

        The link classes that appear in the Link Filter dialog are determined by the Network Scope you choose in the network view (Table 21-7).

        Table 21-7: Link Classes By Network Scope

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

    2. Check the check boxes next to the links you want to display.
    3. Click OK.
10. Return to your originating procedure (NTP).

DLP-A498 Switch Between TDM and DWDM Network Views

Purpose	This task switches between time division multiplexing (TDM) and dense wavelength division multiplexing (DWDM) network views.
Tools/Equipment	None
Prerequisite procedures	DLP-A60 Log into CTC
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Figure 21-15: Network View with Local Link Consolidation

1. From the View menu, choose **Go to Network View**.
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 TXP and MXP cards. **Note:** For information about DWDM, TXP, and MXP cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.
3. Return to your originating procedure (NTP).