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-A201 Apply a Lock-on

Purpose	This task prevents traffic from being switched from one card or port to another.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note: To apply a lock-on to a protect card in a 1:1 or 1:N protection group, the protect card must be active. If the protect card is in standby, the Lock On button is disabled. To make the protect card active, you must switch traffic from the working card to the protect card (Step 4). When the protect card is active, you can apply the lock on.

1. Use the following rules to determine if you can apply a lock on:
    - For a 1:1 electrical protection group, the working or protect cards can be placed in the Lock On state.
    - For a 1:N electrical protection group, the working or protect cards can be placed in the Lock On state.
    - For a 1+1 optical protection group, only the working port can be placed in the Lock On state.
2. In node view, click the **Maintenance > Protection** tabs.
3. In the Protection Groups list, click the protection group where you want to apply a lock on.
4. If you determine that the protect card is in standby mode and you want to apply the lock on to the protect card, make the protect card active:
    1. In the Selected Group list, click the protect card.
    2. In the Switch Commands area, click **Force**.
5. In the Selected Group list, click the active card where you want to lock traffic.

6. In the Inhibit Switching area, click **Lock On**.
7. Click **Yes** in the confirmation dialog box.
   The lock on has been applied and traffic cannot be switched to the working card. To clear the lock-on, see the "DLP-A203 Clear a Lock-on or Lockout" task.
8. Return to your originating procedure (NTP).

DLP-A202 Apply a Lockout

Purpose	This task switches traffic from one card to another using a lockout, which is a switching mechanism that overrides other external switching commands (Force, Manual, and Exercise).
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note: Multiple lockouts in the same protection group are not allowed.

1. Use the following rules to determine if you can put the intended card in a lockout state:
   - For a 1:1 electrical protection group, you can apply a lockout to the working or protect cards.
   - For a 1:N electrical protection group, you can apply a lockout to the working or protect cards.
   - For a 1+1 optical protection group, you can apply a lockout to the protect port.
2. In node view, click the **Maintenance > Protection** tabs.
3. In the Protection Groups list, click the protection group that contains the card you want to lock out.
4. In the Selected Group list, click the card where you want to lock out traffic.
5. In the Inhibit Switching area, click **Lock Out**.
6. Click **Yes** in the confirmation dialog box.
   The lock out has been applied and traffic is switched to the opposite card. To clear the lockout, see the "DLP-A203 Clear a Lock-on or Lockout" task.
   Note: Provisioning a lockout raises a LOCKOUT-REQ condition in Cisco Transport Controller (CTC). If applied to a span, the FE-LOCKOUTOFPR-SPAN condition is also raised. Clearing the lockout switch request clears these conditions.
7. Return to your originating procedure (NTP).

DLP-A203 Clear a Lock-on or Lockout

Purpose	This task clears a lock-on or lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC DLP-A201 Apply a Lock-on or DLP-A202 Apply a Lockout
Required/As Needed	As needed
Onsite/Remote	Both
Security Level	Maintenance or higher

1. In node view, click the **Maintenance > Protection** tabs.
2. In the Protection Groups list, click the protection group that contains the card you want to clear.
3. In the Selected Group list, click the card you want to clear.
4. In the Inhibit Switching area, click **Unlock**.
5. Click **Yes** in the confirmation dialog box.
   The lock-on or lockout is cleared.
6. Return to your originating procedure (NTP).

DLP-A204 Scope and Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes

Purpose	This task cleans the fiber connectors and adapters with alcohol and dry wipes.
Tools/Equipment	Compressed air/duster Isopropyl alcohol 70 percent or higher Optical swab Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
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. Remove the dust cap from the fiber connector.
2. Wipe the connector tip with the premoistened alcohol wipe.
3. Blow-dry using filtered air.
4. Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 to 3.
5. Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.
   Note: If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).
6. Return to your originating procedure (NTP).

DLP-A205 Clean Fiber Connectors with CLETOP

Purpose	This task cleans the fiber connectors with CLETOP.
Tools/Equipment	Type A Fiber Optic Connector Cleaner (CLETOP reel) Optical receiver cleaning stick
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

1. Remove the dust cap from the fiber connector.
2. Press the lever down to open the shutter door. Each time you press the lever, you expose a clean wiping surface.
3. Insert the connector into the CLETOP cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.
4. Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 to 3.
5. Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

   Note: If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).
6. Return to your originating procedure (NTP).

DLP-A206 Clean the Fiber Adapters

Purpose	This task cleans the fiber adapters.
Tools/Equipment	CLETOP stick swab
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

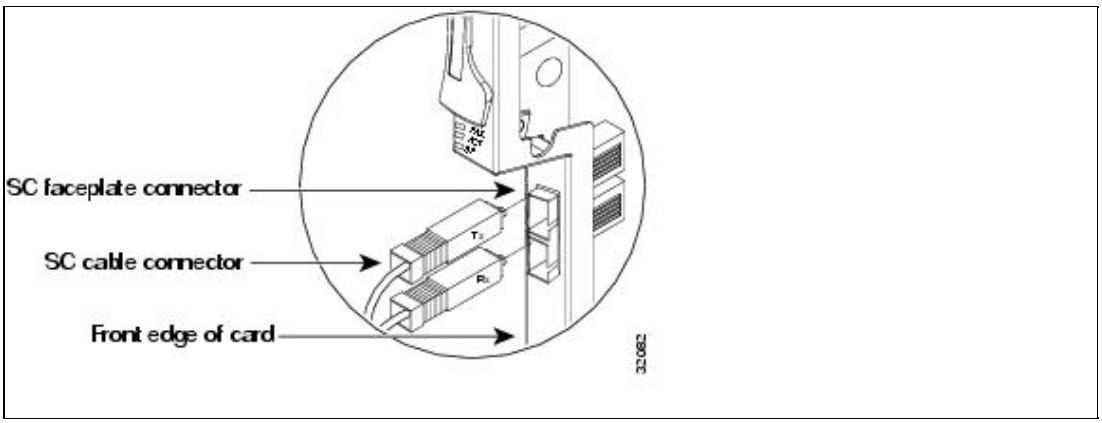
1. Remove the dust plug from the fiber adapter.
2. Insert a CLETOP stick swab (14100400) into the adapter opening and rotate the swab.
3. Place dust plugs on the fiber adapters when not in use.
4. Return to your originating procedure (NTP).

DLP-A207 Install Fiber-Optic Cables on the LGX Interface

Purpose	This task installs fiber-optic cables on the Lightguide Cross Connect (LGX) interface in the central office.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

1. Align the keyed ridge of the cable connector with the receiving SC connector on the LGX faceplate connection point. Each module supports at least one transmit and one receive connector to create an optical carrier port.
2. Gently insert the cable connector into the faceplate connection point until the connector snaps into place.
3. Connect the fiber-optic cable to the OC-N card. Figure 19-1 shows the cable location.

Figure 19-1: Installing Fiber-Optic Cables



4. Return to your originating procedure (NTP).

DLP-A208 Change External Alarms Using the AIC-I Card

Purpose	This task changes external alarm settings on the Alarm Interface Controller-International (AIC-I) card.
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: The procedure is the same if you are using the AEP. In this case, the number of contacts that are shown on the screen is changed accordingly.

1. Confirm that external-device relays are wired to the ENVIR ALARMS IN backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task for more information.
2. Double-click the AIC-I card to display it in card view.
3. Click the **Provisioning > External Alarms** tabs.
4. Modify any of the following fields for each external device wired to the ONS 15454 backplane. For definitions of these fields, see the NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International.
    - Enabled
    - Alarm Type
    - Severity
    - Virtual Wire
    - Raised When
    - Description
5. To provision additional devices, complete Step 4 for each additional device.
6. Click **Apply**.
7. Return to your originating procedure (NTP).

DLP-A209 Change External Controls Using the AIC-I Card

Purpose	This task changes external control settings on the AIC-I card.
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: The procedure is the same if you are using the alarm expansion panel (AEP). In this case, the number of contacts that are shown on the screen is changed accordingly.

1. Verify the external control relays to the ENVIR ALARMS OUT backplane pins. See the "DLP-A19 Install Alarm Wires on the Backplane" task for more information.
2. In node view, double-click the AIC-I card to display it in card view.
3. On the External Controls subtab, modify any of the following fields for each external control wired to the ONS 15454 backplane. For definitions of these fields, see the NTP-A258 Provision External Alarms and Controls on the Alarm Interface Controller-International.
    - Enabled
    - Trigger Type
    - Control Type
    - Description
4. To provision additional controls, complete Step 3 for each additional device.
5. Click **Apply**.
6. Return to your originating procedure (NTP).

DLP-A210 Change AIC-I Card Orderwire Settings

Purpose	This task changes orderwire settings on the AIC-I card.
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

Caution! When provisioning orderwire for ONS 15454s residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

Tip: Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

1. In node view, double-click the AIC-I card to display it in card view.
2. Click the **Provisioning > Local Orderwire** tabs or the **Provisioning > Express Orderwire** tabs, depending on the orderwire path that you want to create. Provisioning steps are the same for both types of orderwire.
3. If needed, adjust the transmit (Tx) and receive (Rx) decibels referred to one milliwatt (dBm) by moving the slider to the right or left for the headset type (four-wire or two-wire) that you will use. In general, you should not need to adjust the dBm.
4. If you want to turn on the audible alert (buzzer) for the orderwire, check the **Buzzer On** check box.
5. Click **Apply**.
6. Return to your originating procedure (NTP).

DLP-A212 Create a User Data Channel Circuit

Purpose	This task creates a user data channel (UDC) circuit on the ONS 15454. A UDC circuit allows you to create a dedicated data channel between nodes.

Tools/Equipment	OC-N cards must be installed.
Prerequisite Procedures	NTP-A323 Verify Card Installation DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In network view, click the Provisioning > Overhead **Circuits** tabs.
2. Click Create.
3. In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:
    - Name-Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
    - Type-Choose either **User Data-F1** or **User Data D-4-D-12** from the drop-down list. (User Data D-4-D-12 is not available if the ONS 15454 is provisioned for dense wavelength division multiplexing [DWDM].)
4. Click **Next**.
5. In the Circuit Source area, complete the following:
    - Node-Choose the source node.
    - Slot-Choose the source slot.
    - Port-If displayed, choose the source port.
6. Click **Next**.
7. In the Circuit Destination area, complete the following:
    - Node-Choose the destination node.
    - Slot-Choose the destination slot.
    - Port-If displayed, choose the destination port.
8. Click Finish.
9. Return to your originating procedure (NTP).

DLP-A214 Change the Service State for a Port

Purpose	This task changes the port service state.
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: To provision E-Series Ethernet ports, see the "DLP-A220 Provision E-Series Ethernet Ports" task.

1. In node view on the shelf graphic, double-click the card with the ports you want to put in or out of service. The card view appears.
2. Click the **Provisioning > Line** tabs for all cards except the G-Series cards. For the G-Series cards, choose the Provisioning > Port tabs.
3. In the Admin State column for the target port, choose one of the following from the drop-down list:
    - IS-Puts the port in the In-Service and Normal (IS-NR) service state.
    - OOS, DSBLD-Puts the port in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. In this service state, traffic is not passed on the port until the service state is changed to IS-NR; Out-of-Service and Management, Maintenance (OOS-MA,MT); or Out-of-Service and Autonomous, Automatic In-Service

(OOS-AU,AINS).

- OOS, MT-Puts the port in the OOS-MA,MT service state. This service state does not interrupt traffic flow and loopbacks are allowed, but alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use the OOS-MA,MT service state for testing or to suppress alarms temporarily. A port must be in the OOS-MA,MT service state before you can apply a loopback. Change to the IS-NR or OOS-AU,AINS service states when testing is complete.
- IS, AINS-Puts the port in the OOS-AU,AINS service state. In this service state, alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. After the soak period passes, the port changes to IS-NR. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.
  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.
  For more information about service states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15454 Reference Manual*.

4. If the port is in loopback (OOS-MA,LPBK & MT) and you set the Admin State to IS, a confirmation window displays indicating that the loopback will be released and that the action could be service affecting. To continue, click **Yes**.
5. If you set the Admin State to IS,AINS, set the soak period time in the AINS Soak field. This is the amount of time that the port will stay in the OOS-AU,AINS service state after a signal is continuously received. When the soak period elapses, the port changes to the IS-NR service state.
6. Click **Apply**. The new port service state appears in the Service State column.
7. As needed, repeat this task for each port.
8. Return to your originating procedure (NTP).

DLP-A217 BLSR Exercise Ring Test

Purpose	This task tests the bidirectional line switched ring (BLSR) functionality without switching traffic. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

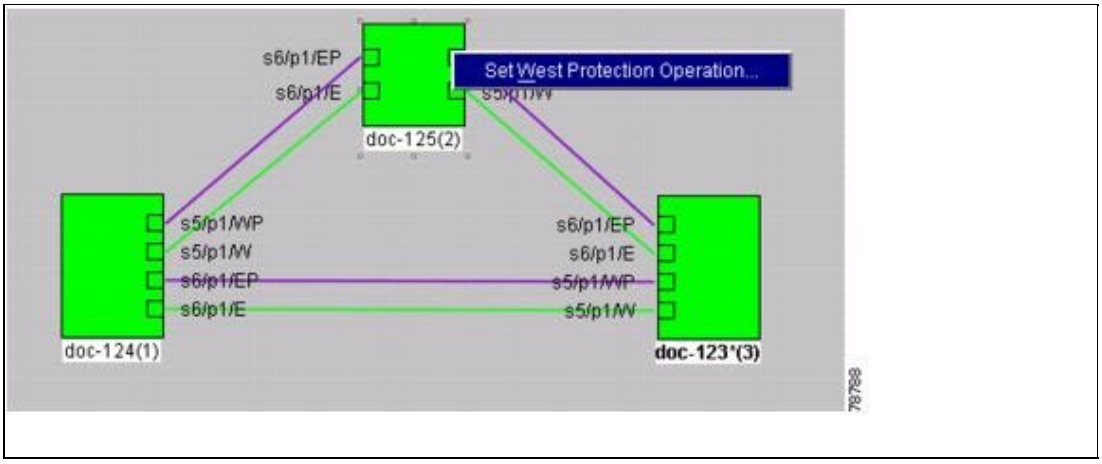
1. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > BLSR** tabs.
3. Click the row of the BLSR you will exercise, then click **Edit**.
4. Exercise the west port:

    1. Right-click the west port of any BLSR node and choose **Set West Protection Operation**. Figure 19-2 shows an example. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)

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

Right-click either working or protect ports.

Figure 19-2: Protection Operation on a Three-Node BLSR



2. In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

5. Click **OK**.
6. In the Confirm BLSR Operation dialog box, click **Yes**.

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

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

      Note: For two fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect ports.
   2. In the Set East Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.
   3. Click **OK**.
   4. In the Confirm BLSR Operation dialog box, click **Yes**.
      On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.
6. In the Cisco Transport Controller window, click the **History** tab.

   If you do not see any BLSR exercise conditions, click the **Filter** button and verify that filtering is not turned on. Also, check that alarms and conditions are not suppressed for a node or BLSR drop cards. See the NTP-A72 Suppress Alarms or Discontinue Alarm Suppression for more information.
7. Click the **Alarms** tab.
   1. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task as necessary.
   2. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the Cisco ONS 15454 Troubleshooting Guide if necessary.
8. From the File menu, choose **Close** to close the BLSR window.
9. Return to your originating procedure (NTP).

DLP-A218 Provision Path Protection Selectors

Purpose	This task provisions path protection selectors during circuit creation or during a topology upgrade conversion.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC The Circuit Attributes page of the Circuit Creation wizard must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: Provisioning path signal degrade (SD-P) or path signal fail (SF-P) thresholds in the Circuit Attributes page of the Circuit Creation wizard sets the values only for path protection-protected spans. The circuit source and destination use the node default values of 10E-4 for SD-P and 10E-6 for SF-P for unprotected circuits and for the source and drop of path protection circuits.

1. In the path protection area of the Circuit Attributes page of the Circuit Creation wizard, set the path protection selectors:
    - Provision working go and return on primary path-Check this box to route the working path on one fiber pair and the protect path on a separate fiber pair. This feature only applies to bidirectional path protection circuits.
    - Revertive-Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
    - Reversion time-If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
    - SF threshold-Set the path protection path-level signal failure bit error rate (BER) thresholds.
    - SD threshold-Set the path protection path-level signal degrade BER thresholds.
    - Switch on PDI-P-For synchronous transport signal (STS) circuits, check this box if you want traffic to switch when an STS payload defect indicator is received. Unavailable for Virtual Tributary (VT) circuits.
2. Return to your originating procedure (NTP).

DLP-A219 Provision a VT Tunnel Route

Purpose	This task provisions the route for a manually routed VT tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC The Circuit Creation wizard Route Review and Edit page must be open.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In the Circuit Creation wizard on the Route Review and Edit page, click the source node icon if it is not already selected. Arrows indicate the available spans for routing the tunnel from the source node.

2. Click the arrow of the span you want the VT tunnel to travel. The arrow turns yellow. In the Selected Span area, the From and To fields show the slot and port that will carry the tunnel. The source STS appears.
3. If you want to change the source STS, change it in the Source STS field; otherwise, continue with the next step.
4. Click Add Span. The span is added to the Included Spans list and the span arrow turns blue.
5. Repeat Steps 3 and 4 until the tunnel is provisioned from the source to the destination node through all intermediary nodes.
6. Return to your originating procedure (NTP).

DLP-A220 Provision E-Series Ethernet Ports

Purpose	This task enables the E100T-12, E100T-G, E1000-2, and E1000-2-G Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security	Provisioning or higher

1. In node view, double-click the Ethernet card that you want to provision.
2. Click the **Provisioning > Port** tabs.
3. For each Ethernet port, provision the following parameters:
    - Port Name-If you want to label the port, type a port name.
    - Mode-Choose the appropriate mode for the Ethernet port:
        - Valid choices for the E100T-12 and E100T-G cards are Auto, 10 Half, 10 Full, 100 Half, and 100 Full.
        - Valid choices for the E1000-2 and E1000-2-G cards are 1000 Full and Auto.

      Note: Both 1000 Full and Auto mode set the E1000-2 port to the 1000 Mbps and Full duplex operating mode; however, flow control is disabled when 1000 Full is selected. Choosing Auto mode enables the E1000-2 card to autonegotiate flow control. Flow control is a mechanism that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. The E1000-2 port handshakes with the connected network device to determine if that device supports flow control.
    - Enabled-Check this check box to activate the corresponding Ethernet port.
    - Priority-Choose a queuing priority for the port. Options range from 0 (Low) to 7 (High). Priority queuing (IEEE 802.1Q) reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. Refer to the priority queuing information in the *Cisco ONS 15454 Reference Manual*. This parameter does not apply to an E-Series card in port-mapped mode.
    - Stp Enabled-Check this check box to enable the Spanning Tree Protocol (STP) on the port. This parameter does not apply to an E-Series card in port-mapped mode. Refer to the spanning tree information in the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.
4. Click **Apply**.
5. Repeat Steps 1 through 4 for all other cards in the VLAN, or if the E-Series card is in port-mapped mode, repeat Steps 1 through 4 for the other card in the point-to-point circuit. Your Ethernet ports are provisioned and ready to be configured for VLAN membership.
6. Return to your originating procedure (NTP).

DLP-A221 Provision E-Series Ethernet Ports for VLAN Membership

Purpose	This task provisions E-Series ports for VLAN membership. It does not apply to E-Series cards in port-mapped mode.
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 node view, double-click the E-Series card graphic to open the card.
2. Click the **Provisioning > VLAN** tabs.
3. To put a port in a VLAN:
    1. Click the port and choose either **Tagged** or **Untag**.
    2. If a port is a member of only one VLAN, choose **Untag** from the Port column in the VLAN's row. Choose **--** for all of the other VLAN rows in that Port column.

        Note: The VLAN with Untag selected can connect to the port, but other VLANs cannot access that port.
    3. Choose **Tagged** at all VLAN rows that need to be trunked. Choose **Untag** at VLAN rows that do not need to be trunked, for example, the default VLAN.

        Note: Each Ethernet port must be attached to at least one untagged VLAN. A trunk port connects multiple VLANs to an external device, such as a switch, which also supports trunking. A trunk port must have tagging (IEEE 802.1Q) enabled for all of the VLANs that connect to that external device.
4. After each port is in the appropriate VLAN, click **Apply**. Table 19-1: VLAN Settings lists VLAN settings.

Table 19-1: VLAN Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15454 tags ingress frames and strips tags from egress frames.
Tagged	The ONS 15454 processes ingress frames according to the VLAN ID; egress frames do not have their tags removed.

Note: If Tagged is chosen, the attached external Ethernet devices must recognize IEEE 802.1Q VLANs.
Note: Both ports on an E1000-2 or E1000-2-G card cannot be members of the same VLAN.

5. Return to your originating procedure (NTP).

DLP-A222 Provision G-Series Ethernet Ports

Purpose	This task provisions G-Series Ethernet ports to carry traffic.
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: You can provision G-Series circuits before or after provisioning the card's ports. See the NTP-A343 Create an Automatically Routed Optical Circuit or the NTP-A344 Create a Manually Routed Optical Circuit, as needed.

1. In the node view, double-click the G-Series card graphic to open the card.
2. Click the **Provisioning > Port** tabs.
3. For each G-Series port, provision the following parameters:
   - Port Name-If you want to label the port, type the port name.
   - Admin State-Select the service state for the port. See the "DLP-A214 Change the Service State for a Port" task for more information.
     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.
   - Auto Negotiation-Click this check box to enable autonegotiation on the port (default). If you do not want to enable autonegotiation control, uncheck the box.
   - Flow Control-Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. To set custom flow control watermarks, see the "DLP-A421 Provision G-Series and CE-1000-4 Flow Control Watermarks" task.
   - Max Size-To permit the acceptance of jumbo size Ethernet frames, choose **Jumbo** (default). If you do not want to permit jumbo size Ethernet frames, choose **1548**.
     Note: The maximum frame size of 1548 bytes enables the port to accept valid Ethernet frames that use protocols such as Inter-Switch Link (ISL). ISL adds 30 bytes of overhead and might cause the frame size to exceed the traditional 1518 byte maximum.
   - Payload Type-Click in the Payload Type field and select a cyclic redundancy check (CRC) size to set the G-Series card's LEX encapsulation:
     - LEX-FCS-16 is 16-bit (2 byte) CRC.
     - LEX-FCS-32 is 32-bit (4 byte) CRC.
4. Click **Apply**.
5. Refresh the Ethernet statistics:
   1. Click the **Performance > Statistics** tabs.
   2. Click **Refresh**.
      Note: Reprovisioning an Ethernet port on the G-Series card does not reset the Ethernet statistics for that port.
6. Return to your originating procedure (NTP).

DLP-A224 Soft-Reset a CE-100T-8 Card Using CTC

Purpose	This procedure soft-resets the CE-100T-8 card.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note: A soft reset is errorless in most cases. If there is a provisioning change during the soft reset, or if the firmware is replaced during the software upgrade process, the reset is not errorless.

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

DLP-A225 Enable Alarm Filtering

Purpose	This task enables alarm filtering for alarms, conditions, or event history in all network nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

1. At the node, network, or card view, click the **Alarms** tab.
2. Click the **Filter** tool at the lower-right side of the bottom toolbar.
   Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).
   Alarm filtering will be enabled in the card, node, and network views of the Alarms tab at the node and for all other nodes in the network. If, for example, the Alarm Filter tool is enabled in the Alarms tab of the node view at one node, the Alarms tab in the network view and card view of that node will also show the tool enabled. All other nodes in the network will also have the tool enabled.
   If you filter an alarm in card view, the alarm will still be displayed in node view. In this view, the card will display the color of the highest-level alarm. The alarm is also shown for the node in the network view.
3. If you want alarm filtering enabled when you view conditions, repeat Steps 1 and 2 using the Conditions window.
4. If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History window.
5. Return to your originating procedure (NTP).

DLP-A227 Disable Alarm Filtering

Purpose	This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A225 Enable Alarm Filtering DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve

1. At node, network, or card view, click the **Alarms** tab.
2. Click the **Filter** tool at the lower-right side of the bottom toolbar.
   Alarm filtering is enabled if the tool is indented and disabled if the tool is raised (not selected).
3. If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and click the Filter tool.
4. If you want alarm filtering disabled when you view alarm history, click the **History** tab and click the Filter tool.
5. Return to your originating procedure (NTP).

DLP-A229 View Circuits on a Span

Purpose	This task allows you to view circuits on an ONS 15454 span as well as unused STSs and VTs on a span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span. See Create Circuits and VT Tunnels for circuit creation 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, choose **View > Go to Network View**. If you are already in network view, continue with Step 2.
2. Right-click the green line containing the circuits that you want to view and choose one of the following:
   - Circuits-To view BLSR, path protection, 1+1, virtual concatenated (VCAT), DWDM optical channel network connections (OCHNCs), or unprotected circuits on the span.
   - PCA Circuits-To view circuits routed on a BLSR protected channel. (This option does not appear if the span you right-clicked is not a BLSR span.)
     In the Circuits on Span dialog box, you can view the following information about the span. The information that appears depends on the circuit type.
   - STS-Lists the STSs.
   - VT-Lists the VTs.
   - Path Protection-(Path protection span only) If checked, path protection circuits are on the span.
   - Circuit-Displays the circuit name. If an STS or VT is not used by a circuit, "unused" appears in this column.
   - Switch State-(Path protection span only) Displays the switch state of the circuit, that is, whether any span switches are active. For path protection spans, switch types include: CLEAR (no spans are switched), MANUAL (a manual switch is active), FORCE (a force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).
     Note: You can perform other procedures from the Circuits on Span dialog box. If the span is in a path protection configuration, you can switch the span traffic. See the "DLP-A197 Initiate a Path Protection Force Switch" task for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-A231 Edit a Circuit Name" task or the "DLP-A233 Edit Path Protection Circuit Path Selectors" task for instructions.
3. Return to your originating procedure (NTP).

DLP-A230 Change a Circuit Service State

Purpose	This task changes the service state of a circuit.
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. From the View menu, choose **Go to Network View**.

2. Click the **Circuits** tab.
3. Click the circuit with the service state that you want to change.

   Note: You cannot edit the circuit service state if the circuit is routed to nodes with a CTC software release older than Release 3.4. These circuits will automatically be in service (IS).
4. From the Tools menu, choose **Circuits > Set Circuit State**.
5. In the Set Circuit State dialog box, choose the administrative state from the Target Circuit Admin State drop-down list:
   - IS-Puts the circuit cross-connects in the IS-NR service state.
   - OOS,DSBLD-Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
   - IS,AINS-Puts the circuit cross-connects in the OOS-AU,AINS service state. When the connections receive a valid signal, the cross-connect service states automatically change to IS-NR.
   - OOS,MT-Puts the circuit cross-connects in the OOS-MA,MT service state. This service state does not interrupt traffic flow and allows loopbacks to be performed on the circuit, but suppresses alarms and conditions. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; OOS; or IS,AINS when testing is complete.
   - OOS,OOG-(VCAT circuits only) Puts the member in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to place a member circuit out of the group and to stop sending traffic. OOS-MA,OOG only applies to the cross-connects on an end node where VCAT resides. The cross-connects on intermediate nodes are in the OOS-MA,MT service state.

     For additional information about circuit and VCAT service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.
6. If you want to apply the service state to the circuit source and destination ports, check the **Apply to Drop Ports** check box.
7. Click **Apply**.
8. If the Apply to Ports Results dialog box appears, view the results and click **OK**.

   CTC will not change the service state of the circuit source and destination port in certain circumstances. For example, if a port is in loopback (OOS-MA,LPBK & MT), CTC will not change the port to IS-NR. In another example, if the circuit size is smaller than the port, such as a VT1.5 circuit on an STS port, CTC will not change the port service state from IS-NR to OOS-MA,DSBLD. If CTC cannot change the port service state, you must change the port service state manually. For more information, see the "DLP-A214 Change the Service State for a Port" task.
9. Return to your originating procedure (NTP).

DLP-A231 Edit a Circuit Name

Purpose	This task edits the name of a circuit or VCAT member.
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. From the View menu, choose **Go to Network View**.
2. Click the **Circuits** tab.
3. Select the circuit you want to rename and click **Edit**.
4. If you want to edit a VCAT circuit member name, complete the following steps in the Edit Circuit

window. If not, continue with Step 5.
    1. Click the **Members** tab.
    2. Click the VCAT member that you want to edit, then click **Edit Member**. The Edit Member window appears.
5. In the General tab, click the **Name** field and edit or rename the circuit.
    Note: Names can be up to 48 alphanumeric and/or special characters. However, to ensure that a monitor circuit can be created on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.
6. Click **Apply**.
7. From the File menu, choose **Close**.
8. If you changed the name of a VCAT circuit member, repeat Step 7 for the Edit Circuit window.
9. In the Circuits window, verify that the circuit was correctly renamed.
10. Return to your originating procedure (NTP).

DLP-A232 Change Active and Standby Span Color

Purpose	This task changes the color of active (working) and standby (protect) circuit spans shown on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple.
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. From the Edit menu in any view, choose **Preferences**.
2. In the Preferences dialog box, click the **Circuit** tab.
3. Complete one or more of the following steps, as required:
    - To change the color of the active (working) span, go to Step 4.
    - To change the color of the standby (protect) span, go to Step 5.
    - To return active and standby spans to their default colors, go to Step 6.
4. As needed, change the color of the active span:
    1. In the Span Colors area, click the colored square to the right of the word Active.
    2. In the Pick a Color dialog box, click the color for the active span, or click the **Reset** button if you want the active span to display the last applied (saved) color.
    3. Click **OK** to close the Pick a Color dialog box. If you want to change the standby span color, go to Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.
5. As needed, change the color of the standby span:
    1. In the Span Colors area, click the colored square to the right of the word Standby.
    2. In the Pick a Color dialog box, click the color for the standby span, or click the **Reset** button if you want the standby span to display the last applied (saved) color.
    3. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.
6. As needed, return the active and standby spans to their default colors:
    1. Click **Reset to Defaults**.
    2. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.
7. Return to your originating procedure (NTP).

DLP-A233 Edit Path Protection Circuit Path Selectors

Purpose	This task changes the path protection SF and SD thresholds, the reversion and reversion time, and the path payload defect indication (PDI-P) settings for one or more path protection circuits.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes 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 **Circuits** tab.
3. In the Circuits tab, click the path protection circuit(s) that you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose nonadjoining circuits) and click each circuit that you want to change.
4. From the Tools menu, choose **Circuits > Set Path Selector Attributes**.
5. In the Path Selectors Attributes dialog box, edit the following path protection selectors, as needed:
    - Revertive-If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If the check box is not checked, traffic does not revert.
    - Reversion Time (Min)-If Revertive is checked, this value sets the amount of time that will elapse before traffic reverts to the working path. The range is 0.5 to 12 minutes in 0.5 minute increments.
    - In the STS Circuits Only area, set the following thresholds:
        - SF threshold-Sets the path protection signal failure BER threshold.
        - SD threshold-Sets the path protection signal degrade BER threshold.
        - Switch on PDI-P-When checked, traffic switches if an STS payload defect indication is received.
    - In the VT Circuits Only area, set the following thresholds:
        - SF threshold-Sets the path protection signal failure BER threshold.
        - SD threshold-Sets the path protection signal degrade BER threshold.
6. Click **OK** and verify that the changed values are correct in the Circuits window.
7. Return to your originating procedure (NTP).

DLP-A241 Clear a BLSR Manual Ring Switch

Purpose	This task clears a Manual ring switch.
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. From the View menu choose **Go to Network View**.
2. Click the **Provisioning > BLSR** tabs.
3. Choose the BLSR and click **Edit**.

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

4. Right-click the BLSR node channel (port) where the Manual ring switch was applied and choose **Set West Protection Operation** or **Set East Protection Operation**, as applicable.
5. In the dialog box, choose **CLEAR** from the drop-down list. Click **OK**.
6. Click **Yes** on the Confirm BLSR Operation dialog box. The letter "M" is removed from the channel (port) and the span turns green on the network view map.
7. From the File menu, choose **Close**.
8. Return to your originating procedure (NTP).

DLP-A242 Create a BLSR on a Single Node

Purpose	This task creates a BLSR on a single node. Use it to add a node to an existing BLSR or when you delete and then recreate a BLSR temporarily on one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > BLSR** tabs.
2. In the Suggestion dialog box, click **OK**.
3. In the Create BLSR dialog box, enter the BLSR information:
   - Ring Type-Enter the ring type (either 2 Fiber or 4 Fiber) of the BLSR.
   - Ring Name-Enter the BLSR ring name. If the node is being added to a BLSR, use the BLSR ring name.
   - Node ID-Enter the node ID. If the node is being added to a BLSR, use an ID that is not used by other BLSR nodes.
   - Ring Reversion-Enter the ring reversion time of the existing BLSR.
   - West Line-Enter the slot on the node that will connect to the existing BLSR via the node's west line (port).
   - East Line-Enter the slot on the node that will connect to the existing BLSR via the node's east line (port).

   If you are adding the node to a four-fiber BLSR, complete the following for the second set of fibers:
   - Span Reversion-Enter the span reversion time of the existing BLSR.
   - West Line-Enter the slot on the node that will connect to the existing BLSR via the node's west line.
   - East Line-Enter the slot on the node that will connect to the existing BLSR via the node's east line.
4. Click **OK**.

   Note: The BLSR is incomplete and alarms are present until the node is connected to other BLSR nodes.
5. Return to your originating procedure (NTP).

DLP-A244 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

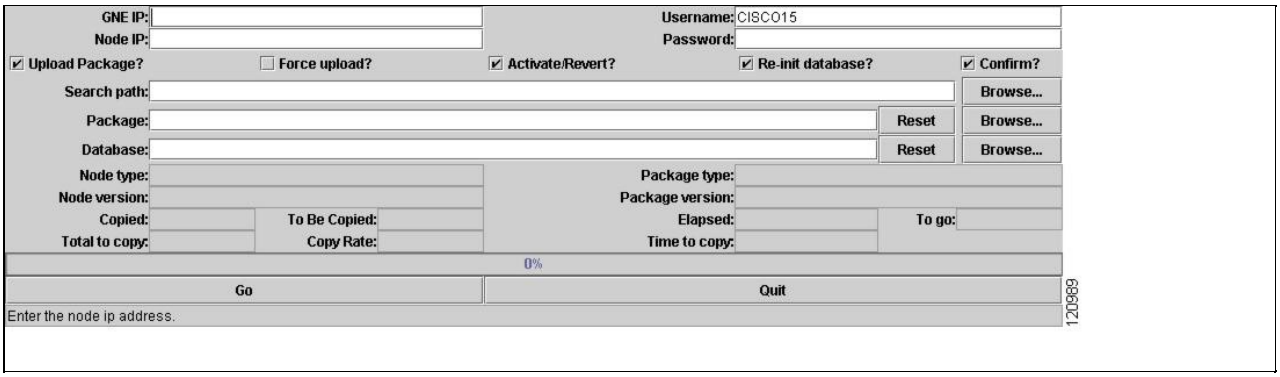
Purpose	

	This task reinitializes the ONS 15454 using the CTC reinitialization tool on a Windows computer. Reinitialization uploads a new software package to the TCC2/TCC2P cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 SONET System Software CD, Version 8.5 JRE 1.4.2 or JRE 5.0 must be installed on the computer to log into the node when the reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

1. Insert the system software CD into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.
2. From the Windows Start menu, choose **Run.** In the Run dialog box, click **Browse** and navigate to the CISCO15454 folder on the software CD.
3. In the Browse dialog box Files of Type field, choose **All Files**.
4. Choose the RE-INIT.jar file and click **Open**. The NE Re-Initialization window appears (Figure 19-3).

Figure 19-3: Reinitialization Tool



5. Complete the following fields:

   · GNE IP-If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
   · Node IP-Enter the node name or IP address of the node that you are reinitializing.
   · User ID-Enter the user ID needed to access the node.
   · Password-Enter the password for the user ID.
   · Upload Package-Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
   · Force Upload-Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
   · Activate/Revert-Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software

is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.

- Re-init Database-Check this box to send a new database to the node. (This is equivalent to the CTC database restore operation.) If unchecked, the node database is not modified.
- Confirm-Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Search Path-Enter the path to the CISCO15454 folder on the CD drive.

6. Click **Go**.
7. **Caution!** Before continuing with the next step, verify that the database to upload is correct. You cannot reverse the upload process after you click Yes.
8. Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

   The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the TCC2/TCC2P cards, "Complete" appears in the status bar and the TCC2/TCC2P cards will reboot. Wait a few minutes for the reboot to complete.
9. After the reboot is complete, log into the node using the "DLP-A60 Log into CTC" task.
10. Complete the NTP-A25 Set Up Name, Date, Time, and Contact Information and NTP-A169 Set Up CTC Network Access.
11. Return to your originating procedure (NTP).

DLP-A245 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task reinitializes the ONS 15454 using the CTC reinitialization tool on a UNIX computer. Reinitialization uploads a new software package to the TCC2/TCC2P cards, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15454 SONET System Software CD, Version 8.5 JRE 1.4.2 must be installed on the computer to log into the node when the reinitialization is complete. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

1. Insert the system software CD containing the reinit tool, software, and defaults database into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.
2. To find the recovery tool file, go to the CISCO15454 directory on the CD (usually /cdrom/cdrom0/CISCO15454).
3. If you are using a file explorer, double-click the **RE-INIT.jar** file. If you are working with a command line, run **java -jar RE-INIT.jar**. The NE Re-Initialization window appears (Figure 19-3).
4. Complete the following fields:
   - GNE IP-If the node you are reinitializing is accessed through another node configured as a GNE, enter the GNE IP address. If you have a direct connection to the node, leave this field

Figure 19-3: Reinitialization Tool

blank.

- Node IP-Enter the node name or IP address of the node that you are reinitializing.
- User ID-Enter the user ID needed to access the node.
- Password-Enter the password for the user ID.
- Upload Package-Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload-Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert-Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tabs.
- Re-init Database-Check this box to send a new database to the node. (This is equivalent to the CTC database restore operation.) If unchecked, the node database is not modified.
- Confirm-Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Search Path-Enter the path to the CISCO15454 folder on the CD drive.

5. Click **Go**.

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

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

   The reinitialization begins. After the software is downloaded and activated and the database is uploaded to the TCC2/TCC2P cards, "Complete" appears in the status bar and the TCC2/TCC2P cards will reboot. Wait a few minutes for the reboot to complete.
7. After the reboot is complete, log into the node using the "DLP-A60 Log into CTC" task.
8. Complete the NTP-A25 Set Up Name, Date, Time, and Contact Information and the NTP-A169 Set Up CTC Network Access.
9. Return to your originating procedure (NTP).

DLP-A246 Provision E-Series Ethernet Card Mode

Purpose	This task provisions an E-Series Ethernet card for multicard EtherSwitch Group, single-card EtherSwitch, or port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed.
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution! You cannot change the mode while the Ethernet card is carrying circuits. If you want to change the card mode, delete any circuits that it carries first. See the NTP-A278 Modify and Delete Overhead Circuits and Server Trails.

1. In the network view, double-click the node containing the E-Series Ethernet card you want to provision, then double-click the Ethernet card.
2. Click the **Provisioning > Card** tabs.
3. In the Card Mode area, choose one of the following:
   - For multicard EtherSwitch circuit groups, choose **Multicard EtherSwitch Group**.
   - For single-card EtherSwitch circuits, choose **Single-card EtherSwitch**.
   - For port-mapped circuits, choose Port-mapped.
4. Click Apply.
5. If you are using multicard EtherSwitch circuits, repeat Steps 2 through 4 for all other Ethernet cards in the node that will carry the multicard EtherSwitch circuits.
6. Repeat Steps 1 through 5 for other nodes as necessary.
7. Return to your originating procedure (NTP).

DLP-A247 Change an OC-N Card

Purpose	This task changes an OC-N card while maintaining existing provisioning, including data communications channels (DCCs), circuits, protection, timing, and rings. This task is intended to be used when you are replacing a card with a card of identical type and line rate; when a slot is preprovisioned and you want to change the optical speed of the card; or when you have backed out of an automatic span upgrade.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution! Physically removing an OC-N card can cause a loss of working traffic or a protection switch. See Upgrade Cards and Spans for information on upgrading traffic to a higher speed.

Note: You can change a multiport card to a card with a smaller number of ports only if the new card has the same line rate as the multiport card. (The MRC-12 card can be changed to either a single-port OC-12 card or a single-port OC-48 card.)

Note: You can upgrade only one-port OC-12 or one-port OC-48 cards to MRC-12 or MRC-2.5G-4 cards. The port in one-port OC-12 or one-port OC-48 card map to Port 1 on the MRC-12 or MRC-2.5G-4 card.

1. If the card the active card in a 1+1 protection group, switch traffic away from the card:
   1. Log into a node on the network. If you are already logged in, go to Substep 2.
   2. Display the CTC node (login) view.
   3. Click the **Maintenance > Protection** tabs.
   4. Double-click the protection group that contains the reporting card.
   5. Click the active card of the selected group.
   6. Click Switch and Yes in the Confirmation dialog box.
2. In CTC, right-click the card that you want to remove and choose Change Card.
3. In the Change Card drop-down list, choose the desired card type and click **OK**. A mismatched equipment alarm (MEA) appears until you replace the card.
4. Physically remove the card:
   1. Disconnect any fiber connections to the front of the card.
   2. Open the card latches/ejectors.
   3. Use the latches/ejectors to pull the card forward and away from the shelf.
5. Complete the NTP-A16 Install Optical Cards and Connectors.

6. Return to your originating procedure (NTP).

DLP-A249 Provision IP Settings

Purpose	This task provisions IP settings, which includes the IP address, default router, Dynamic Host Configuration Protocol (DHCP) access, firewall access, and SOCKS proxy server settings for an ONS 15454 node.
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! All ONS 15454 IP addresses and network parameters should be reviewed by your network (or LAN) administrator.

Caution! Verify that the IP address assigned to the node does not duplicate an address assigned to another ONS 15454 on the same subnet. If the same addresses are assigned to ONS 15454s on the same subnet, loss of visibility will occur.

1. In node view, click the **Provisioning > Network > General** tabs.
2. Complete the following information in the fields listed:
    - IP Address-Type the IP address assigned to the ONS 15454 node.
      Note: If TCC2P cards are installed, dual IP addressing via secure mode is available. When secure mode is off (sometimes called repeater mode), the IP address entered in the IP Address field applies to the backplane LAN port and the TCC2P TCP/IP (LAN) port. When secure mode is on, the IP Address field shows the address assigned to the TCC2P TCP/IP (LAN) port and the Superuser can enable or disable display of the backplane IP address. See the "DLP-A433 Enable Node Secure Mode" task as needed. Refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.
    - Net/Subnet Mask Length-Type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15454s in the same subnet.
    - MAC Address-(Display only) Displays the ONS 15454 IEEE 802 MAC address.
      Note: In secure mode, the front and back TCP/IP (LAN) ports are assigned different MAC addresses, and the backplane information can be hidden or revealed by a Superuser.
    - Default Router-If the ONS 15454 is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the ONS 15454 cannot directly access. This field is ignored if any of the following are true:
        - The ONS 15454 is not connected to a LAN.
        - The SOCKS proxy server is enabled and the ONS 15454 is provisioned as an end network element (ENE).
        - Open Shortest Path First (OSPF) is enabled on both the ONS 15454 and the LAN where the ONS 15454 is connected.
    - LCD IP Setting-Choose one of the following:
        - **Allow Configuration**-Displays the node IP address on the LCD and allows users to change the IP settings using the LCD. This option enables the "DLP-A64 Set the IP Address, Default Router, and Network Mask Using the LCD" task.
        - **Display Only**-Displays the node IP address on the LCD but does not allow users to

change the IP address using the LCD.

◊ **Suppress Display**-Suppresses the node IP address display on the LCD.

- Suppress CTC IP Display-Check this check box if you want to prevent the node IP address from being displayed in CTC (IP Address field, information area) to users with Provisioning, Maintenance, or Retrieve security levels. If the IP address is not suppressed, it is shown in the IP Address field.

  Note: IP address suppression is not applied to users with a Superuser security level. However, in secure mode the backplane IP address visibility can be restricted to only a locally connected Superuser viewing the routing table. In this case, the backplane IP address is not revealed to any user at any other NE on the routing table or in autonomous messages (such as the TL1 REPT^DBCHG command, alarms, and PM reporting).
- Forward DHCP Request To-Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the ONS 15454 SOCKS proxy server features, leave this field blank.

  Note: If you enable DHCP, computers connected to an ONS 15454 node can obtain temporary IP addresses from an external DHCP server. The ONS 15454 only forwards DHCP requests; it does not act as a DHCP server.
- Gateway Settings-Provisions the ONS 15454 SOCKS proxy server features. (SOCKS is a standard proxy protocol for IP-based applications.) Do not change any of these options until you review the SOCKS proxy server scenario in the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*. In SOCKS proxy server networks, the ONS 15454 is either an ENE, GNE, or proxy-only server. Provisioning must be consistent for each NE type.
- Enable SOCKS proxy server on port-If checked, the ONS 15454 serves as a proxy for connections between CTC clients and ONS 15454s that are DCC-connected to the proxy ONS 15454. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes, only to the proxy ONS 15454. If Enable SOCKS proxy server on port is off, the node does not proxy for any CTC clients. When this box is checked, you can set the node as an ENE or a GNE:
  - ◊ External Network Element (ENE)-Choose this option when the ONS 15454 is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE through the TCC2/TCC2P craft port can manage nodes that have DCC connections to the ENE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN/WAN that those nodes might be connected to.
  - ◊ Gateway Network Element (GNE)-Choose this option when the ONS 15454 is connected to a LAN and has DCC connections to other nodes. A CTC computer connected to the LAN can manage all nodes that have DCC connections to the GNE, but the CTC computer does not have direct IP connectivity to them. The GNE option isolates the LAN from the DCC network so that IP traffic originating from the DCC-connected nodes and any CTC computers connected to them is prevented from reaching the LAN.
  - ◊ SOCKS Proxy-Only-Choose this option when the ONS 15454 is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS Proxy Only is the same as the GNE option, except the SOCKS Proxy Only option does not isolate the DCC network from the LAN.

  Note: If a node is provisioned in secure mode, it is automatically provisioned as a GNE with SOCKS proxy enabled. However, this provisioning can be overridden, and the secure node can be changed to an ENE. In secure mode, SOCKS cannot be disabled. See the "DLP-A433 Enable Node Secure Mode" task for provisioning instructions, including GNE or ENE status.

3. Click **Apply**.

4. Click **Yes** in the confirmation dialog box.
   Both TCC2/TCC2P cards reboot, one at a time. During this time (approximately 5 minutes), the active and standby TCC2/TCC2P card LEDs go through the cycle shown in Table 19-2. Eventually, a "Lost node connection, switching to network view" message appears.

Table 19-2: LED Behavior During TCC2/TCC2P Reboot

Reboot Activity	Active TCC2/TCC2P LEDs	Standby TCC2/TCC2P LEDs
Standby TCC2/TCC2P card updated with new network information. Memory test (1 to 2 minutes). If an AIC-I card is installed, the AIC FAIL and alarm LEDs light up briefly when the AIC is updated. The standby TCC2/TCC2P becomes the active TCC2/TCC2P.	ACT/STBY: Flashing green.	1. ACT/STBY: Flashing yellow. 2. FAIL LED: Solid red. 3. All LEDs on except ACT/STBY. 4. CRIT turns off. 5. MAJ and MIN turn off. 6. REM, SYNC, and ACO turn off. 7. All LEDs (except A&B PWR) turn off (1 to 2 minutes). 8. ACT/STBY: Solid yellow. 9. Alarm LEDs: Flash once. 10. ACT/STBY: Solid green.
Memory test (1 to 2 minutes). TCC2/TCC2P updated with new network information. The active TCC2/TCC2P becomes the standby TCC2/TCC2P.	1. All LEDs: Turn off (1 to 2 minutes). CTC displays "Lost node connection, switching to network view" message. 2. FAIL LED: Solid red. 3. FAIL LED: Flashing red. 4. All LEDs on except ACT/STBY. 5. CRIT turns off. 6. MAJ and MIN turn off. 7. REM, SYNC, and ACO turn off; all LEDs are off. 8. ACT/STBY: Solid yellow. 9. ACT/STBY: Flashing yellow. 10. ACT/STBY: Solid yellow.	ACT/STBY: Solid green.

5. Click **OK**. The network view appears. The node icon appears in gray, during which time you cannot access the node.
6. Double-click the node icon when it becomes green.
7. Return to your originating procedure (NTP).

DLP-A250 Set Up or Change Open Shortest Path First Protocol

Purpose	This task enables the OSPF routing protocol on the ONS 15454. Perform this task if you want to include the ONS 15454 in OSPF-enabled networks.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15454 is connected.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > Network > OSPF** tabs.
2. On the top left side of the OSPF pane, complete the following:
   - DCC/GCC OSPF Area ID Table-In dotted decimal format, enter the number that identifies the ONS 15454s as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.
   - SDCC Metric-This value is normally unchanged. It sets a cost for sending packets across the Section DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 100.
   - LDCC Metric-Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.
3. In the OSPF on LAN area, complete the following:
   - OSPF active on LAN-When checked, enables the ONS 15454 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454s that directly connect to OSPF routers.
   - LAN Port Area ID-Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15454 is connected. (This number is different from the DCC/generic communications channel [GCC] OSPF Area ID.)
4. By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with Step 5.
   1. Click the **No Authentication** button.
   2. In the Edit Authentication Key dialog box, complete the following:
      - Type-Choose **Simple Password**.
      - Enter Authentication Key-Enter the password.
      - Confirm Authentication Key-Enter the same password to confirm it.
   3. Click **OK**.
      The authentication button label changes to Simple Password.
5. Provision the OSPF priority and interval settings.
   The OSPF priority and interval defaults are ones most commonly used by OSPF routers. Verify that these defaults match the ones used by the OSPF router where the ONS 15454 is connected.
   - Router Priority-Selects the designated router for a subnet.
   - Hello Interval (sec)-Sets the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
   - Dead Interval-Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

- Transit Delay (sec)-Indicates the service speed. One second is the default.
- Retransmit Interval (sec)-Sets the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric-Sets a cost for sending packets across the *LAN*. This value should always be lower than the DCC metric. Ten is the default.

6. In the OSPF Area Range Table area, create an area range table if one is needed:
   Note: Area range tables consolidate the information that is outside an OSPF area border. One ONS 15454 in the ONS 15454 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 OSPF area.
   1. In the OSPF Area Range Table area, click **Create**.
   2. In the Create Area Range dialog box, enter the following:
      - Range Address-Enter the area IP address for the ONS 15454s that reside within the OSPF area. For example, if the ONS 15454 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
      - Range Area ID-Enter the OSPF area ID for the ONS 15454s. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
      - Mask Length-Enter the subnet mask length. In the Range Address example, this is 16.
      - Advertise-Check this box if you want to advertise the OSPF range table.
   3. Click **OK**.
7. All OSPF areas must be connected to area 0. If the ONS 15454 OSPF area is not physically connected to area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to area 0:
   1. In the OSPF Virtual Link Table area, click **Create**.
   2. In the Create Virtual Link dialog box, complete the following fields. OSPF settings must match OSPF settings for the ONS 15454 OSPF area:
      - Neighbor-The router ID of the area 0 router.
      - Transit Delay (sec)-The service speed. One second is the default.
      - Hello Int (sec)-The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
      - Auth Type-If the router where the ONS 15454 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
      - Retransmit Int (sec)-Sets the time that will elapse before a packet is resent. Five seconds is the default.
      - Dead Int (sec)-Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
   3. Click **OK**.
8. After entering ONS 15454 OSPF area data, click **Apply**.
   If you changed the Area ID, the TCC2/TCC2P cards reset, one at a time. The reset takes approximately 10 to 15 minutes. Table 19-2 shows the LED behavior during the TCC2/TCC2P reset.
9. Return to your originating procedure (NTP).

DLP-A251 Set Up or Change Routing Information Protocol

Purpose	This task enables Routing Information Protocol (RIP) on the ONS 15454. Perform this task if you want to include the ONS 15454 in RIP-enabled networks.
Tools/Equipment	None
	DLP-A60 Log into CTC

Prerequisite Procedures	You need to create a static route to the router adjacent to the ONS 15454 for the ONS 15454 to communicate its routing information to non-DCC-connected nodes.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

1. In node view, click the **Provisioning > Network > RIP** tabs.
2. Check the **RIP Active** check box if you are activating RIP.
3. Choose either RIP Version 1 or RIP Version 2 from the drop-down list, depending on which version is supported in your network.
4. Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.
5. By default, RIP is set to No Authentication. If the router that the ONS 15454 is connected to requires authentication, complete the following steps. If not, continue with Step 6.
    1. Click the **No Authentication** button.
    2. In the Edit Authentication Key dialog box, complete the following:
        - ◊ Type-Choose **Simple Password**.
        - ◊ Enter Authentication Key-Enter the password.
        - ◊ Confirm Authentication Key-Enter the same password to confirm it.
    3. Click **OK**.
       The authentication button label changes to Simple Password.
6. If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the ONS 15454 is a gateway NE with multiple external ONS 15454 NEs attached with IP addresses in different subnets.
    1. In the RIP Address Summary area, click **Create**.
    2. In the Create Address Summary dialog box, complete the following:
        - ◊ Summary Address-Enter the summary IP address.
        - ◊ Mask Length-Enter the subnet mask length using the up and down arrows.
        - ◊ Hops-Enter the number of hops. The smaller the number of hops, the higher the priority.
    3. Click **OK.**
7. Return to your originating procedure (NTP).

DLP-A255 Cross-Connect Card Side Switch Test

Purpose	This task verifies that the XCVT, XC10G, and XC-VXC-10G cards can effectively switch service (active to standby and standby to active).
Tools/Equipment	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Caution! Always wait 60 seconds between cross-connect card (side) switches to allow the system to stabilize. This is applicable to all the types of side switches (soft reset or manual switch using CTC or TL1). This condition is also applicable to all the cross-connect types (XC-10G, XC-VXC-10G, XC-VT).

1. From the View menu, choose **Go to Network View**.
2. Click the **Alarms** tab.

1. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task as necessary.
2. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the Cisco ONS 15454 Troubleshooting Guide if necessary.

3. Click the **Conditions** tab. 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 if necessary.
4. On the network map, double-click the node containing the cross-connect cards you are testing to open it in node view.
5. Click the **Maintenance > Cross-Connect** tabs.
6. In the Cross-Connect Cards area, make a note of the active and standby slots.
7. On the shelf graphic, verify that the active cross-connect card has a green ACT LED and the standby cross-connect card has an amber SBY LED. If these conditions are not present, review the "DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards" task or contact your next level of support.
8. Click **Switch**.
9. In the Confirm Switch dialog box, click **Yes**.

   Note: A cross-connect side-switch performed using XC-VXC-10G cards and TCC2/TCC2P cards is errorless.

10. Verify that the active slot noted in Step 6 becomes the standby slot, and that the standby slot becomes the active slot. The switch should appear within 1 to 2 seconds.
11. Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, do not continue. Refer to your next level of support.
12. Wait 60 seconds, then repeat Steps 7 through 9 to return the active/standby slots to their configuration at the start of the procedure.
13. Verify that the cross-connect card appears as you noted in Step 6.
14. Return to your originating procedure (NTP).

    Note: During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.

DLP-A256 View Ethernet Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on an Ethernet card and port to detect possible performance problems.
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, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance > Statistics** tabs.
3. Click **Refresh**. Performance monitoring statistics for each port on the card appear.
4. View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring"

chapter in the *Cisco ONS 15454 Reference Manual*.

Note: To refresh, reset, or clear PM counts, see the NTP-A253 Change the PM Display.

5. Return to your originating procedure (NTP).

DLP-A257 View Ethernet Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on an Ethernet card and port to detect possible performance problems.
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, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance > Utilization** tabs.
3. Click **Refresh**. Performance monitoring utilization values for each port on the card appear.
4. View the Port # column to find the port you want to monitor.
5. The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

   Note: To refresh, reset, or clear PM counts, see the NTP-A253 Change the PM Display.
6. Return to your originating procedure (NTP).

DLP-A258 View Ethernet History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on an Ethernet card and port to detect possible performance problems.
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, double-click the E-Series or G-Series Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance > History** tabs.
3. Click **Refresh**. Performance monitoring statistics for each port on the card appear.
4. View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15454 Reference Manual*.

   Note: To refresh, reset, or clear PM counts, see the NTP-A253 Change the PM Display.
5. Return to your originating procedure (NTP).

DLP-A259 Refresh Ethernet PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.

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, double-click the Ethernet card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
   Note: For CE-Series and ML-Series cards, click **Performance > Ether Ports** or **Performance > POS Ports** tabs
3. Click the **Utilization** tab or the **History** tab.
4. From the Interval drop-down list, choose one of four options:
   - **1 min**: This option appears the specified PM counts in one-minute time intervals.
   - **15 min**: This option appears the specified PM counts in 15-minute time intervals.
   - **1 hour**: This option appears the specified PM counts in one-hour time intervals.
   - **1 day**: This option appears the specified PM counts in one-day (24 hours) time intervals.
5. Click **Refresh**. The PM counts refresh with values based on the selected time interval.
6. Return to your originating procedure (NTP).

DLP-A260 Set Auto-Refresh Interval for Displayed PM Counts

Purpose	This task changes the window auto-refresh intervals for updating the displayed PM counts.
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, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. From the Auto-refresh drop-down list, choose one of six options:
   - **None**: This option disables the auto-refresh feature.
   - **15 Seconds**: This option sets the window auto-refresh to 15-second time intervals.
   - **30 Seconds**: This option sets the window auto-refresh to 30-second time intervals.
   - **1 Minute**: This option sets the window auto-refresh to 1-minute time intervals.
   - **3 Minutes**: This option sets the window auto-refresh to 3-minute time intervals.
   - **5 Minutes**: This option sets the window auto-refresh to 5-minute time intervals.
4. Click **Refresh**. The PM counts for the newly selected auto-refresh time interval appear.
   Depending on the selected auto-refresh interval, the displayed PM counts automatically update when each refresh interval completes. If the auto-refresh interval is set to None, the PM counts that appear are not updated unless you click Refresh.
5. Return to your originating procedure (NTP).

DLP-A261 Refresh PM Counts for a Different Port

Purpose	This task changes the window view to display PM counts for another port on a multiport card.
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, double-click the card where you want to view PM counts. The card view appears.
2. Click the **Performance** tab.
3. In the Port drop-down list, choose a port.
4. Click **Refresh**. The PM counts for the newly selected port appear.
5. Return to your originating procedure (NTP).

DLP-A262 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the Circuits window. You can filter the circuits in network, node, or card view based on circuit name, size, type, direction, and other attributes.
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 CTC view:
   - To filter network circuits, from the View menu, choose **Go to Network View**.
   - To filter 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 filter circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.
2. Click the **Circuits** tab.
3. Set the attributes for filtering the circuit display:
   1. Click the **Filter** button.
   2. In the General tab of the Circuit Filter dialog box, set the following filter attributes, as necessary:
      - Name-Enter a complete or partial circuit name to filter circuits based on the circuit name; otherwise leave the field blank.
      - Direction-Choose one: **Any** (direction not used to filter circuits), **1-way** (display only one-way circuits), or **2-way** (display only two-way circuits).
      - OCHNC Dir-(DWDM OCHNCs only) Choose one: **East to West** (displays only east-to-west circuits); **West to East** (displays only west-to-east circuits). For more information, refer to the Cisco ONS 15454 DWDM Procedure Guide.
      - OCHNC Wlen-(DWDM OCHNCs only) Choose an OCHNC wavelength to filter the circuits. For example, choosing 1530.33 displays channels provisioned on the

1530.33 nm wavelength. For more information, refer to the Cisco ONS 15454 DWDM Procedure Guide.

- ◊ Status-Choose a circuit status to filter the circuits. For more information about circuit statuses, see Table 21-2.
- ◊ State-Choose one: **OOS** (display only out-of-service circuits), **IS** (display only in-service circuits; OCHNCs have IS status only), or **OOS-PARTIAL** (display only circuits with cross-connects in mixed service states).
- ◊ Protection-Choose a protection type to filter the circuits. For more information about protection types, see Table 21-1.
- ◊ Slot-Enter a slot number to filter circuits based on the source or destination slot; otherwise leave the field blank.
- ◊ Port-Enter a port number to filter circuits based on the source or destination port; otherwise leave the field blank.
- ◊ Type-Choose one: **Any** (type not used to filter circuits), **STS** (displays only STS circuits), **VT** (displays only VT circuits), **VT Tunnel** (displays only VT tunnels), **STS-V** (displays STS VCAT circuits), **VT-V** (displays VT VCAT circuits), **VT Aggregation Point** (displays only VT aggregation points), or **OCHNC** (displays only OCHNCs; refer to the Cisco ONS 15454 DWDM Procedure Guide).
- ◊ Size-Click the appropriate check boxes to filter circuits based on size: VT1.5, VT2, STS-1, STS3c, STS-6c, STS-9c, STS-12c, STS-18c, STS-24c, STS-36c, STS-48c, STS-192c, Multi-rate, Equipment non specific, 2.5 Gbps FEC, 2.5 Gbps No FEC, 10 Gbps FEC, or 10 Gbps No FEC.

  The check boxes shown depend on the Type field selection. If you chose Any, all sizes are available. If you chose VT, VT1.5 or VT2 are available. If you chose VT-V, only VT1.5 is available. If you chose STS, only STS sizes are available, and if you chose VT Tunnel or VT Aggregation Point, only STS-1 is available. If you chose OCHNC as the circuit type, Multi-rate, Equipment non specific, 2.5 Gbps FEC, 2.5 Gbps No FEC, 10 Gbps FEC, and 10 Gbps No FEC appear (DWDM only; refer to the Cisco ONS 15454 DWDM Procedure Guide). If you chose STS-V, only STS-1, STS3c, and STS-12c are available.

4. To set the filter for ring, node, link, and source and drop type, click the **Advanced** tab and complete the following substeps. If you do not want to make advanced filter selections, continue with Step 5.
   1. If you made selections on the General tab, click **Yes** in the confirmation box to apply the settings.
   2. In the Advanced tab of the Circuit Filter dialog box, set the following filter attributes as necessary:
      - ◊ Ring-Choose the ring from the drop-down list.
      - ◊ Node-Click the check boxes by each node in the network to filter circuits based on node.
      - ◊ Link-Choose the desired link in the network.
      - ◊ Source/Drop-Choose one of the following to filter circuits based on whether they have one or multiple sources and drops: **One Source and One Drop Only** or **Multiple Sources or Multiple Drops**.
5. Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box appear in the Circuits window.
6. To turn filtering off, click the Filter icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on, and click the **Filter** button to change the filter attributes.
7. Return to your originating procedure (NTP).

DLP-A263 Edit Path Protection Dual-Ring Interconnect Circuit Hold-Off Timer

Purpose	This task changes the amount of time a path selector switch is delayed for circuits routed on a path protection dual-ring interconnect (DRI) topology. Setting a switch hold-off time (HOT) prevents unnecessary back and forth switching when a circuit is routed through multiple path protection selectors.
Tools/Equipment	None
Prerequisite Procedures	NTP-A44 Provision Path Protection Nodes DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note: Cisco recommends that you set the DRI port HOT value to zero and the circuit path selector HOT value to a number equal to or greater than zero.

1. From the View menu, choose **Go to Network View**.
2. Click the **Circuits** tab.
3. Click the path protection circuit you want to edit, then click **Edit**.
4. In the Edit Circuit window, click the **Path Protection Selectors** tab.
5. Create a hold-off time for the circuit source and destination ports:
    1. In the Holder Off Timer area, double-click the cell of the circuit source port (top row), then type the new hold-off time. The range is 0 to 10,000 ms in increments of 100.
    2. In the Hold-Off Timer area, double-click the cell of the circuit destination port (bottom row), then type the hold-off time entered in Substep 1.
6. Click **Apply**, then close the Edit Circuit window by choosing **Close** from the File menu.
7. Return to your originating procedure (NTP).

DLP-A264 Provision a J1 Path Trace on Circuit Source and Destination Ports

Purpose	This task creates a path trace on STS circuit source ports and destination ports or a VCAT circuit member.
Tools/Equipment	ONS 15454 cards capable of transmitting and receiving path trace must be installed at the circuit source and destination ports. See Table 19-3 for a list of cards.
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 assumes you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

1. From the View menu, choose **Go to Network View**.
2. Click the **Circuits** tab.
3. For the STS circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string. See Table 19-3 for a list of cards.

Table 19-3: Path-Trace-Capable ONS 15454 Cards

J1 Function	Cards
Transmit and Receive	CE-1000-4 CE-100T-8 DS1-14[1] DS1N-14 DS1/E1-56 DS3-12E DS3i-N-12 DS3/EC1-48 DS3N-12E DS3XM-6 DS3XM-12 G-Series ML-Series
Receive Only	EC1-12 OC3 IR 4/STM1 SH 1310 OC3 IR 4/STM1 SH 1310-8 OC12/STM4-4 OC48 IR/STM16 SH AS 1310 OC48 LR/STM16 LH AS 1550 OC192 SR/STM64 IO 1310 OC192 LR/STM64 LH 1550 OC192 IR/STM SH 1550 ML-Series FC_MR-4

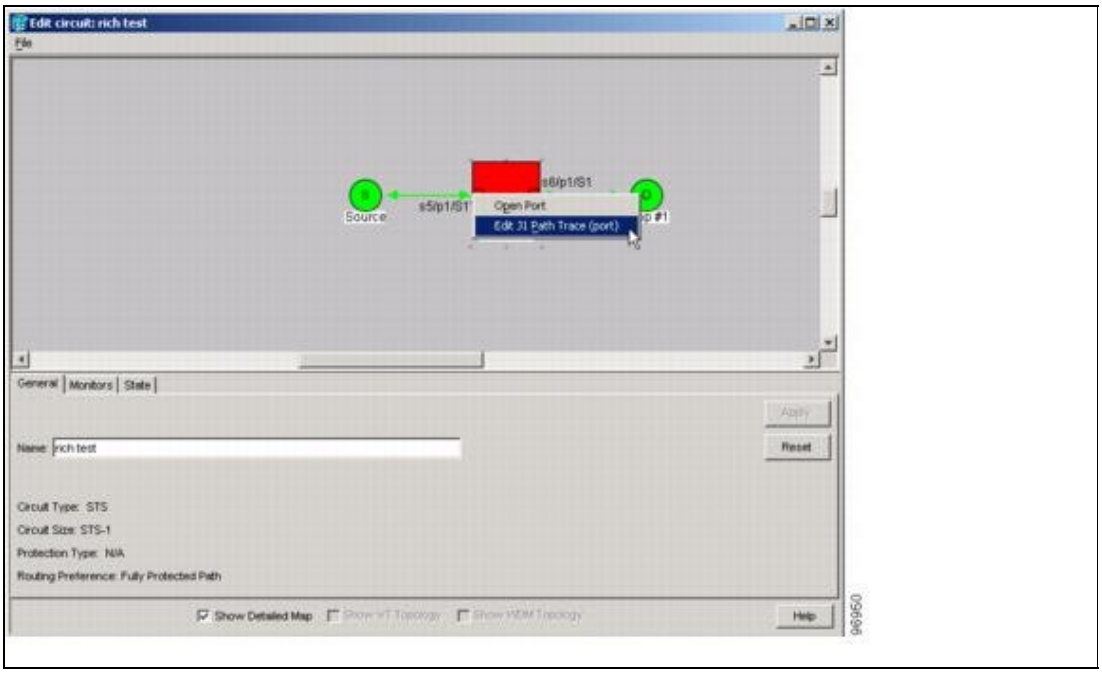
1. J1 path trace is not supported for DS-1s used in VT circuits.

Note: For FC_MR-4 cards, the path trace string must be identical for all members of the VCAT circuit. You cannot mix path trace strings across members of a VCAT group. When retrieving the

path trace string on the FC_MR-4 card view Maintenance > Path Trace subtab, only the member assigned a path trace string displays the path trace information.
Note: If neither port is on a transmit/receive card, you will not be able to complete this procedure. If one port is on a transmit/receive card and the other is on a receive-only card, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

4. Choose the STS circuit you want to trace, then click **Edit**.
5. If you chose a VCAT circuit, complete the following. If not, continue with Step 6.
    1. In the Edit Circuit window, click the **Members** tab.
    2. Click **Edit Member** and continue with Step 6.
6. In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports appears.
7. Provision the circuit source transmit string:
    1. On the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J1 Path Trace (port)** from the shortcut menu. Figure 19-4 shows an example.

Figure 19-4: Selecting the Edit Path Trace Option



    2. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.
    3. Click **Apply**, then click **Close**.
8. Provision the circuit destination transmit string:
    1. On the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu (Figure 19-4).
    2. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.
    3. Click **Apply**.
9. Provision the circuit destination expected string:

1. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:
   - Auto-The first string received from the source port is automatically provisioned as the current expected string. An alarm is raised when a string that differs from the baseline is received.
   - Manual-The string entered in the Current Expected String field is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.
2. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.
3. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and remote defect indication (RDI) when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.
4. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.
5. Click **Apply**, then click **Close**.
   Note: It is not necessary to set the format (16 or 64 bytes) for the circuit destination expected string; the path trace process automatically determines the format.

10. Provision the circuit source expected string:
    1. In the Edit Circuit window (with Show Detailed Map chosen, see Figure 19-4) right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.
    2. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:
       - Auto-Uses the first string received from the port at the other path trace end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
       - Manual-Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.
    3. If you set the Path Trace Mode field to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.
    4. Click the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the AIS and RDI when the TIM-P alarm appears. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for descriptions of alarms and conditions.
    5. (Check box visibility depends on card selection) Click the **Disable AIS on C2 Mis-Match** check box if you want to suppress the AIS when a C2 mismatch occurs.
    6. Click **Apply**.
       Note: It is not necessary to set the format (16 or 64 bytes) for the circuit source expected string; the path trace process automatically determines the format.
11. After you set up the path trace, the received string appears in the Received field on the path trace setup window. The following options are available:
    - Click **Hex Mode** to display path trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the path trace to ASCII format.
    - Click the **Reset** button to reread values from the port.
    - Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

    Caution! Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

    The expect and receive strings are updated every few seconds if the Path Trace Mode field is set to Auto or Manual.

Figure 19-4: Selecting the Edit Path Trace Option

12. Click **Close**.
    The detailed circuit map indicates path trace with an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.
13. Return to your originating procedure (NTP).

DLP-A265 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
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 > Security > Legal Disclaimer > HTML** tabs.
2. The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. Use the following HTML commands to format the text, as needed:
    - Begins boldface font
    - Ends boldface font
    - Aligns type in the center of the window
    - Ends the center alignment
    - <font=n, where n = point size> Changes the font to the new size
    - Ends the font size command
    - <p> Creates a line break
    - <sub>Begins subscript
    - </sub> Ends subscript
    - <sup> Begins superscript
    - </sup>Ends superscript
    - <u>Starts underline
    - </u> Ends underline
3. If you want to preview your changed statement and formatting, click the **Preview** subtab.
4. Click **Apply**.
5. Return to your originating procedure (NTP).

DLP-A266 Change IP Settings

Purpose	This task changes the IP address, subnet mask, default router, DHCP access, firewall Internet Inter-ORB Protocol (IIOP) listener port, LCD IP display, and SOCKS proxy server settings.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC DLP-A249 Provision IP Settings
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Security Level	Superuser only

Caution! Changing the node IP address, subnet mask, or IIOP listener port causes the TCC2/TCC2P cards to reboot. If Ethernet circuits using Spanning Tree Protocol (STP) originate or terminate on E-Series Ethernet cards installed in the node, circuit traffic will be lost for several minutes while the spanning trees reconverge. Other circuits are not affected by TCC2/TCC2P reboots.

Note: If the node contains TCC2P cards and is in default (repeater) mode, the node IP address refers to the TCC2P front-access TCP/IP (LAN) port as well as the backplane LAN port. If the node is in secure mode, this task will only change the front-access port IP address. If the node is in secure mode and has been locked, the IP address cannot be changed unless the lock is removed by Cisco Technical Support.

1. In node view, click the **Provisioning > Network > General** tabs.
2. Change any of the following:
   - IP Address
   - Suppress CTC IP Display
   - LCD IP Setting
   - Default Router
   - Forward DHCP Request To
   - Net/Subnet Mask Length
   - TCC CORBA (IIOP) Listener Port
   - Gateway Settings

   See the "DLP-A249 Provision IP Settings" task for detailed field descriptions. For more information about secure mode, refer to the "Management Network Connectivity" chapter of the *Cisco ONS 15454 Reference Manual*
3. Click **Apply**.

   If you changed a network field that will cause the node to reboot, such as the IP address, subnet mask, or TCC Common Object Request Broker Architecture (CORBA) Listener Port, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears.
4. If a confirmation dialog box appears, click **Yes**.

   If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS 15454 TCC2/TCC2P cards reboot, one at a time. A TCC2/TCC2P card reboot causes a temporary loss of connectivity to the node, but traffic is unaffected. See Table 19-2 for TCC2/TCC2P reboot behavior.
5. Confirm that the changes appear on the **Provisioning > Network > General** tab. If the changes do not appear, repeat the task. Refer to the *Cisco ONS 15454 Troubleshooting Guide* as necessary.
6. Return to your originating procedure (NTP).

DLP-A268 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map of 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: You can replace the network view background image with any JPEG or GIF image that is accessible on a local or network drive. If you apply a custom background image, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

1. From the Edit menu, choose **Preferences > Map** and uncheck the **Use Default Map** check box.

2. From the View menu, choose **Go to Network View**.
3. Right-click the network or domain map and choose **Set Background Image**.
4. Click **Browse**. Navigate to the graphic file you want to use as a background.
5. Select the file. Click **Open**.
6. Click **Apply** and then click **OK**.
7. If the ONS 15454 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15454 icons are visible.
8. If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.
9. If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15454 icons are displayed at the magnification you want.
10. Return to your originating procedure (NTP).

DLP-A269 Enable Dialog Box Do-Not-Display Option

Purpose	This task ensures that a user-selected do-not-display dialog box preference is enabled for subsequent sessions or it disables the do-not-display option.
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: If any user who has rights to perform an operation (for example, creating a circuit) selects the "Do not show this dialog again" check box in a dialog box, the dialog box is not displayed for any other users who perform that operation on the network from the same computer unless the command is overridden using the following task. (The preference is stored on the computer, not in the node database.)

1. From the Edit menu, choose **Preferences**.
2. In the Preferences dialog box, click the **General** tab.
   The Preferences Management area field lists all dialog boxes where "Do not show this dialog again" is enabled.
3. Choose one of the following options, or uncheck the individual dialog boxes that you want to appear:
   - **Don't Show Any**-Hides all do-not-display check boxes.
   - **Show All**-Overrides do-not-display check box selections and displays all dialog boxes.
4. Click **OK**.
5. Return to your originating procedure (NTP).

DLP-A271 Change Security Policy on a Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuseronly

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

2. If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.
3. In the User Lockout area, you can modify the following:
    - Failed Logins Allowed Before Lockout-The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
    - Manual Unlock by Superuser-If checked, allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
    - Lockout Duration-Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).
4. In the Password Change area, you can modify the following:
    - Prevent Reusing Last [ ] Passwords-Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
    - New Password must Differ from the Old Password by [ ] Characters-Choose the number of characters that must differ between the old and new password. The default number is 1.
    - Cannot Change New Password for [ ] days-If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
    - Require Password Change on First Login to New Account-If checked, requires users to change their password the first time they log into their account.
5. To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:
    - Aging Period-Sets the amount of time that must pass before the user must change their password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
    - Warning-Sets the number of days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.
6. In the Other area, you can provision the following:
    - Single Session Per User**-**If checked, limits users to one login session at one time.
    - Prevent Superuser Disable-If checked, the super user is NOT disabled after the period of time specified in the Inactive Duration box expires.
    - Disable Inactive User-If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 0 to 99 days. **Note:** If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.
7. Click **Apply**.
8. Return to your originating procedure (NTP).

DLP-A272 Change Security Policy on Multiple Nodes

Purpose	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
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. From the View menu, choose **Go to Network View**.
2. Click the **Provisioning > Security > Policy** tabs. A read-only table of nodes and their policies appears.
3. Click a node on the table that you want to modify, then click **Change**.
4. If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.
5. In the User Lockout area, you can modify the following:
    - Failed Logins Allowed Before Lockout-The number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
    - Manual Unlock by Superuser-Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
    - Lockout Duration-Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals).
6. In the Password Change area, you can modify the following:
    - Prevent Reusing Last [ ] Passwords-Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
    - New Password must Differ from the Old Password by [ ] Characters-Choose the number of characters that must differ between the old and new password. The default number is 1.
    - Cannot Change New Password for [ ] days-If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
    - Require Password Change on First Login to New Account-If checked, requires users to change their password the first time they log into their account.
7. To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:
    - Aging Period-Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
    - Warning-Sets the number of days the user will be warned to change their password for each security level. The range is 2 to 20 days.
8. In the Other area, you can provision the following:
    - Single Session Per User**-**If checked, limits users to one login session at one time.
    - Prevent Superuser Disable-If checked, the superuser is NOT disabled after the period of time specified in the Inactive Duration box expires.
    - Disable Inactive User-If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 0 to 99 days. **Note:** If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.
9. In the Select Applicable Nodes area, uncheck any nodes where you do not want to apply the changes.
10. Click **OK**.
11. In the Security Policy Change Results dialog box, confirm that the changes are correct, then click **OK**.
12. Return to your originating procedure (NTP).

DLP-A273 Modify SNMP Trap Destinations

Purpose	This task modifies the Simple Network Management Protocol (SNMP) trap destinations on an ONS 15454 including community name, default User Datagram Protocol (UDP) port, SNMP trap version, and maximum traps per second.

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 node view, click the **Provisioning > SNMP** tabs.
2. Select a trap from the **Trap Destinations** area.
   For a description of SNMP traps, refer to the "SNMP" chapter in the *Cisco ONS 15454 Reference Manual*.
3. Highlight the Destination row field entry under the Community column and change the entry to another valid community name.
   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 network management system.
   Note: The default UDP port for SNMP is 162.
4. Set the Trap Version field for either SNMPv1 or SNMPv2.
   Refer to your NMS documentation to determine whether to use SNMP v1 or v2.
5. If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.
6. 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 Allow SNMP Proxy check box located on the SNMP tab.
7. If you want to enable using generic SNMP MIBs, click the Use Generic MIBs checkbox.
8. Click **Apply**.
9. SNMP settings are now modified. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen.
10. Return to your originating procedure (NTP).

DLP-A293 Perform a Manual Span Upgrade on a Two-Fiber BLSR

Purpose	This task upgrades a two-fiber BLSR span to a higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade Attenuators might be needed for some applications
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning! Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard. Statement 206

Caution! Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note: All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Note: BLSR protection channel access (PCA) circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48), which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the NTP-A278 Modify and Delete Overhead Circuits and Server Trails. To create circuits, see Create Circuits and VT Tunnels.

1. Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See the "DLP-A303 Initiate a BLSR Force Ring Switch" task.
2. Remove the fiber from both endpoints and ensure that traffic is still running.
3. Remove the OC-N cards from both endpoints.
4. From both endpoints, in node view right-click each OC-N slot and choose **Change Card**.
5. In the Change Card dialog box, choose the new OC-N card type.
6. Click **OK**.
7. Complete the NTP-A16 Install Optical Cards and Connectors to install the new OC-N cards in both endpoints.
8. Verify that the transmit and receive signals fall within the acceptable range. See Table 2-5 for OC-N card transmit and receive levels. If the receive level falls outside the acceptable range for that card, attenuate accordingly.
9. Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
10. When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (loss of signal [LOS], SD, and SF) are cleared, remove the forced switch from both endpoints on the upgraded span. See the "DLP-A194 Clear a BLSR Force Ring Switch" task.
11. Perform an exercise ring test to check the BLSR ring functionality without switching traffic. See the "DLP-A217 BLSR Exercise Ring Test" task.
12. Repeat this task for each span in the BLSR. When you are done with each span, the upgrade is complete.
13. Return to your originating procedure (NTP).

DLP-A294 Perform a Manual Span Upgrade on a Four-Fiber BLSR

Purpose	This task upgrades a four-fiber BLSR span to a higher OC-N rate. Repeat the task to upgrade each span to the higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade Attenuators might be needed for some applications
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning! Do not reach into a vacant slot or chassis while you install or remove a module or a fan.

Exposed circuitry could constitute an energy hazard. Statement 206

Caution! Do not perform any other maintenance operations or add any circuits during a span upgrade.

Note: All spans connecting the nodes in a BLSR must be upgraded before the bandwidth is available.

Note: BLSR PCA circuits, if present, will remain in their existing STSs. Therefore, they will be located on the working path of the upgraded span and will have full BLSR protection. To route PCA circuits on protection channels in the upgraded span, delete and recreate the circuits after the span upgrade. For example, if you upgrade an OC-48 span to an OC-192, PCA circuits on the protection STSs (STSs 25 to 48) in the OC-48 BLSR will remain in their existing STSs (STSs 25 to 48), which are working, protected STSs in the OC-192 BLSR. Deleting and recreating the OC-48 PCA circuits moves the circuits to STSs 96 to 192 in the OC-192 BLSR. To delete circuits, see the NTP-A278 Modify and Delete Overhead Circuits and Server Trails. To create circuits, see Create Circuits and VT Tunnels.

1. Apply a Force switch to both span endpoints (nodes) on the span that you will upgrade first. See the "DLP-A303 Initiate a BLSR Force Ring Switch" task.
2. Remove the fiber from both working and protect cards at both span endpoints (nodes) and ensure that traffic is still running.
3. Remove the OC-N cards from both end points.
4. For both ends of the span endpoints, in node view right-click each OC-N slot and choose **Change Card**.
5. In the Change Card dialog box, choose the new OC-N card type.
6. Click **OK**.
7. Complete the NTP-A16 Install Optical Cards and Connectors to install the new OC-N cards in both endpoints.
8. Verify that the transmit signal falls within the acceptable range. See Table 2-5 for OC-N card transmit and receive levels.
9. Complete the "DLP-A44 Install Fiber-Optic Cables for BLSR Configurations" task to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
10. When cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD, and SF) are cleared, remove the forced switch from both endpoints (nodes) on the upgraded span. See "DLP-A194 Clear a BLSR Force Ring Switch" task.
11. Perform an exercise ring test to check the BLSR ring functionality without switching traffic. See the "DLP-A217 BLSR Exercise Ring Test" task.
12. Repeat these steps for each span in the BLSR. When all spans in the BLSR have been upgraded, the ring is upgraded.
13. Return to your originating procedure (NTP).

DLP-A295 Perform a Manual Span Upgrade on a Path Protection Configuration

Purpose	This task upgrades path protection spans to a higher OC-N speed. Repeat the task for each span to upgrade the entire ring to the higher OC-N rate. To downgrade a span, repeat this task but choose a lower-rate card in Step 5.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning! Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard. Statement 206

Caution! Do not perform any other maintenance operations or add any circuits during a span upgrade.

1. Complete the "DLP-A197 Initiate a Path Protection Force Switch" task to apply a Force switch on the span that you will upgrade.
2. Remove the fiber from both endpoint nodes in the span and ensure that traffic is still running.
3. Remove the OC-N cards from both span endpoints.
4. For both ends of the span, in node view right-click each OC-N slot and choose **Change Card**.
5. In the Change Card dialog box, choose the new OC-N card type.
6. Click **OK**.
7. Complete the NTP-A16 Install Optical Cards and Connectors to install the new OC-N cards in both endpoints.
8. Verify that the transmit signal falls within the acceptable range. See Table 2-5 for OC-N card transmit and receive levels.
9. Complete the "DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations" task to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
10. Complete the "DLP-A198 Clear a Path Protection Force Switch" task when cards in both endpoint nodes have been successfully upgraded and all the facility alarms (LOS, SD, and SF) are cleared.
11. Return to your originating procedure (NTP).

DLP-A296 Perform a Manual Span Upgrade on a 1+1 Protection Group

Purpose	This task upgrades a linear span to a higher OC-N rate. To downgrade a span, follow this task but choose a lower-rate card in Step 6.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning! Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard. Statement 206

Caution! Do not perform any other maintenance operations or add any circuits during a span upgrade.

1. Initiate a Force switch on the ports you will upgrade, beginning with the protect port:
    1. In node view, click the **Maintenance > Protection** tabs.
    2. Choose the protection group from the Protection Groups area. In the Selected Group area, the working and protect spans appear.
    3. In the Selected Group area, click the protect OC-N port.
    4. In Switch Commands, choose Force.
    5. Click Yes in the confirmation dialog box.

        FORCE-SWITCH-TO-WORKING appears next to the forced span.
2. If you are upgrading a multiport card, repeat Step 1 for each port.
3. Remove the fiber from both ends of the span and ensure that traffic is still running.
4. Remove the OC-N cards from both span endpoints.
5. At both ends of the span, in node view, right-click the OC-N slot and choose Change Card.

6. In the Change Card dialog box, choose the new OC-N card type.
7. Click **OK**.
8. Complete the NTP-A16 Install Optical Cards and Connectors to install the new OC-N cards in both endpoints.
9. Verify that the transmit signal falls within the acceptable range. See Table 2-3 for OC-N card transmit and receive levels.
10. Complete the "DLP-A428 Install Fiber-Optic Cables in a 1+1 Configuration" task to attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
11. When cards on each end of the span have been successfully upgraded and all the facility alarms (LOS, SD, and SF) are cleared, remove the Force switch:
    1. In node view, click the **Maintenance > Protection** tabs.
    2. In the Protection Groups area, click the protection group that contains the card/port you want to clear.
    3. In the Selected Group area, click the card you want to clear.
    4. In Switch Commands, choose Clear.
    5. Click Yes in the confirmation dialog box.
12. Repeat this task for any other spans in the 1+1 linear configuration.
13. Return to your originating procedure (NTP).

DLP-A297 Perform a Manual Span Upgrade on an Unprotected Span

Purpose	This task manually upgrades unprotected spans to a higher OC-N rate.
Tools/Equipment	Higher-rate cards Compatible hardware necessary for the upgrade
Prerequisite Procedures	DLP-A60 Log into CTC
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	Provisioning or higher

Warning! Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard. Statement 206

Caution! Upgrading unprotected spans will cause all traffic running on those spans to be lost.

Caution! Do not perform any other maintenance operations or add any circuits during a span upgrade.

Caution! Removing the fiber will cause all traffic on the unprotected span to be lost.

1. Remove the fiber from both endpoint nodes in the span.
2. Remove the OC-N cards from both span endpoints.
3. For both ends of the span, in node view, right-click each OC-N slot and choose **Change Card**.
4. In the Change Card dialog box, choose the new OC-N type.
5. Click **OK**.
6. When you have finished Steps 2 through 5 for both nodes, install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
7. Return to your originating procedure (NTP).

DLP-A298 Check the Network for Alarms and Conditions

Purpose	This task verifies that no alarms or conditions exist on the network.
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. From the View menu, choose **Go to Network View**. Verify that all affected spans on the network map are green.
2. Verify that the affected spans do not have active switches on the network map. Span ring switches are represented by the letters "L" for lockout ring, "F" for Force ring, "M" for Manual ring, and "E" for Exercise ring.
3. A second verification method can be performed from the Conditions tab. Click **Retrieve Conditions** and verify that no switches are active. Make sure the Filter button is not selected.
4. Click the **Alarms** tab.
    1. Verify that the alarm filter is not on. See the "DLP-A227 Disable Alarm Filtering" task as necessary.
    2. Verify that no unexplained alarms appear on the network. If alarms appear, investigate and resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* for procedures.
5. Return to your originating procedure (NTP).

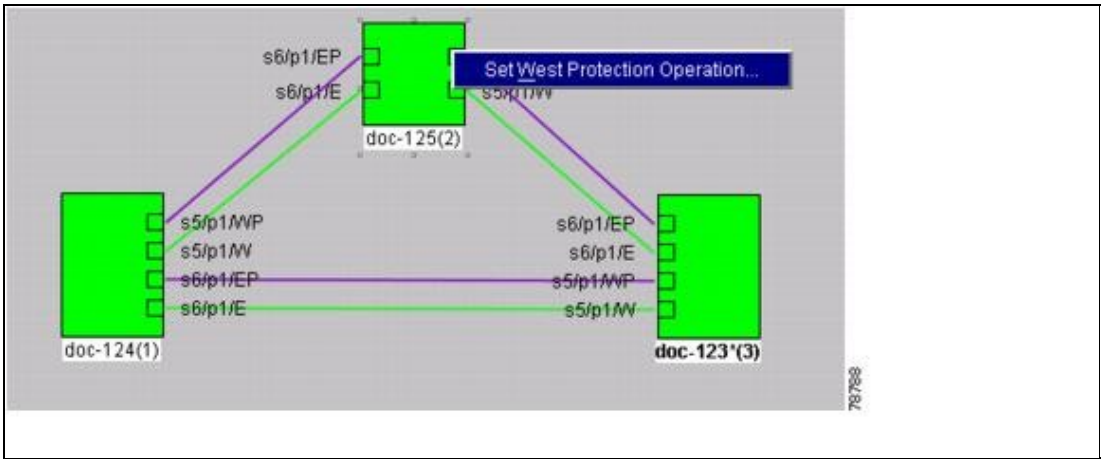
DLP-A299 Initiate a BLSR Span Lockout

Purpose	This task allows you to perform a BLSR span lockout, which prevents traffic from switching to the locked out span.
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

Caution! Traffic is not protected during a span lockout.

1. Click the **Provisioning > BLSR** tabs.
2. Choose the BLSR and click **Edit**.
    Tip: To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.
3. To lock out a west span:
    1. Right-click any BLSR node west channel (port) and choose **Set West Protection Operation**. Figure 19-5 shows an example.
    Note: For two-fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. You can right-click either working port.

Figure 19-5: Protection Operation on a Three-Node BLSR



2. In the Set West Protection Operation dialog box, choose **LOCKOUT PROTECT SPAN** from the drop-down list. Click **OK**.

4. In the Confirm BLSR Operation dialog box, click **Yes**. An "L" appears on the selected channel (port) where you created the lock out.

   Lockouts generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.

4. To lock out an east span:
   1. Right-click the node's east channel (port) and choose **Set East Protection Operation**.
   2. In the Set East Protection Operation dialog box, choose **LOCKOUT PROTECT SPAN** from the drop-down list. Click **OK**.
   3. In the Confirm BLSR Operation dialog box, click **Yes**. An "L" indicating the lockout appears on the selected channel (port) where you invoked the protection switch. Lockouts generate LKOUTPR-S and FE-LOCKOUTOFPR-SPAN conditions.
5. From the File menu, choose **Close**.
6. Return to your originating procedure (NTP).