



## DLPs A300 to A399

---

### DLP-A300 Clear a BLSR Span Lockout

<b>Purpose</b>	This task clears a bidirectional line switched ring (BLSR) span lockout.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

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

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

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



**Tip** To move an icon to a new location, for example, to see BLSR channel (port) information more clearly, you can drag and drop icons on the Edit BLSR network graphic.

---

**Step 4** Right-click the BLSR node channel (port) where the lockout will be cleared and choose **Set West Protection Operation** or **Set East Protection Operation**.

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

**Step 6** In the Confirm BLSR Operation dialog box, click **Yes**. The “L” that indicated the lockout disappears from the network view map.

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

**Step 8** Return to your originating procedure (NTP).

---

## DLP-A301 Initiate a BLSR Manual Ring Switch

<b>Purpose</b>	This task performs a BLSR Manual ring switch. A Manual ring switch will switch traffic off a span if there is no higher priority switch (Force or lockout) and no signal degrade (SD) or signal failure (SF) conditions.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

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

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



**Tip**

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

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



**Note**

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

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

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

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

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

**Step 9** Return to your originating procedure (NTP).

## DLP-A303 Initiate a BLSR Force Ring Switch

<b>Purpose</b>	Use this task to perform a BLSR Force switch on a BLSR port. A Force ring switch will switch traffic off a span if there is no signal degrade (SD), signal failure (SF), or lockout switch present on the span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>

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

**Caution**

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

**Caution**

Traffic is not protected during a Force protection switch.

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

**Note**

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

**Note**

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

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

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

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

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

**Note**

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




---

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

---

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

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

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

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

**Step 7** Return to your originating procedure (NTP).

---

## DLP-A309 View the Ethernet MAC Address Table

<b>Purpose</b>	This task displays the Ethernet MAC address table for any node with one or more E-Series Ethernet cards installed.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

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

**Step 2** Select the appropriate E-Series Ethernet card in the Layer 2 Domain field.

**Step 3** Click **Retrieve**.

The MAC address table information appears.

**Step 4** Return to your originating procedure (NTP).

---

## DLP-A310 View Ethernet Trunk Utilization

<b>Purpose</b>	This task displays the Ethernet Trunk bandwidth usage on any node with one or more E-Series Ethernet cards installed.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- 
- Step 1** In node view, click the **Maintenance > Ether Bridge > Trunk Utilization** tabs.
- Step 2** Select the desired time interval in the Interval field.
- Step 3** Click **Refresh**.
- The trunk utilization information for the current and previous time intervals appears.
- Step 4** Return to your originating procedure (NTP).
- 

## DLP-A311 Provision a Half Circuit Source and Destination on a BLSR or 1+1 Configuration

<b>Purpose</b>	This task provisions a half circuit source and destination for BLSR and 1+1 configurations. A half circuit allows you to provision a partial path (one end of a circuit), for example, if you want to provision a circuit with the intent that the path will be completed at a later time or at a different location.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



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

- 
- Step 1** From the Node drop-down list, choose the node that will contain the half circuit.
- Step 2** From the Slot drop-down list, choose the slot containing the card where the circuit will originate.
- Step 3** From the Port drop-down list, choose the port where the circuit will originate. This field is not available if a DS-1 card is chosen in [Step 2](#).
- Step 4** If the circuit is a DS-1 circuit and you choose a DS-1 card as the source, choose the DS-1 where the traffic will originate from the DS1 drop-down list.

- Step 5** Click **Next**.
  - Step 6** From the Node drop-down list, select the node that you chose in [Step 1](#).
  - Step 7** From the Slot drop-down list, choose the OC-N card that you will use to map the DS-1 to a VT1.5 for OC-N transport or to map the DS-3 or OC-N synchronous transport signal (STS) circuit to an STS.
  - Step 8** Choose the destination STS or Virtual Tributary (VT) from the drop-down lists that appear.
  - Step 9** Return to your originating procedure (NTP).
- 

## DLP-A312 Provision a Half Circuit Source and Destination on a Path Protection

<b>Purpose</b>	This task provisions a half circuit source and destination on path protection configurations. A half circuit allows you to provision a partial path (one end of a circuit), for example, if you want to provision a circuit with the intent that the path will be completed at a later time or at a different location.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> The Circuit Creation wizard Circuit Source page must be open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the Node drop-down list, choose the node that will contain the half circuit.
  - Step 2** From the Slot drop-down list, choose the slot containing the card where the circuit will originate.
  - Step 3** From the Port drop-down list, choose the port where the circuit will originate. This field is not available if a DS-1 card is chosen in [Step 2](#).
  - Step 4** If the circuit is a DS-1 circuit and you choose a DS-1 card as the source, choose the DS-1 where the traffic will originate from the DS1 drop-down list.
  - Step 5** Click **Next**.
  - Step 6** From the Node drop-down list, choose the node that you selected in [Step 1](#).
  - Step 7** From the Slot drop-down list, choose the OC-N card that will be used to map the DS-1 to a VT1.5 for OC-N transport or to map the DS-3 or OC-N STS circuit to an STS.
  - Step 8** Choose the destination STS or VT from the drop-down lists that appear.
  - Step 9** Click **Use Secondary Destination** and repeat Steps [6](#) through [8](#).
  - Step 10** Return to your originating procedure (NTP).
-

## DLP-A313 Create a DCC Tunnel

<b>Purpose</b>	This task creates a data communications channel (DCC) tunnel to transport traffic from third-party SONET equipment across ONS 15454 networks. Tunnels can be created on the Section DCC channel (D1-D3) (if not used by the ONS 15454 as a terminated DCC), or any Line DCC channel (D4-D6, D7-D9, or D10-D12).
<b>Tools/Equipment</b>	OC-N cards must be installed
<b>Prerequisite Procedures</b>	<a href="#">NTP-A35 Verify Node Turn-Up, page 5-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

Cisco recommends a maximum of 84 DCC tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as a DCC tunnel endpoint, and a Section DCC that is used as a DCC tunnel endpoint cannot be terminated. All DCC tunnel connections are bidirectional.

- 
- Step 1** In network view, click the **Provisioning > Overhead Circuits** tabs.
- Step 2** Click **Create**.
- Step 3** In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:
- Name—Type the tunnel name.
  - Circuit Type—Choose one:
    - **DCC Tunnel-D1-D3**—Allows you to choose either the Section DCC (D1-D3) or a Line DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
    - **DCC Tunnel-D4-D12**—Provisions the full Line DCC as a tunnel.
- Step 4** Click **Next**.
- Step 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.
  - Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
    - **DCC1 (D1-D3)**—This is the Section DCC.
    - **DCC2 (D4-D6)**—This is Line DCC 1.
    - **DCC3 (D7-D9)**—This is Line DCC 2.
    - **DCC4 (D10-D12)**—This is Line DCC 3.
- DCC options do not appear if they are used by the ONS 15454 (DCC1) or other tunnels.
- Step 6** Click **Next**.
- Step 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.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—This is the Section DCC.
  - **DCC2 (D4-D6)**—This is Line DCC 1.
  - **DCC3 (D7-D9)**—This is Line DCC 2.
  - **DCC4 (D10-D12)**—This is Line DCC 3.

DCC options do not appear if they are used by the ONS 15454 (DCC1) or other tunnels.

- Step 8** Click **Finish**.
- Step 9** Put the ports that are hosting the DCC tunnel in service. See the “[DLP-A214 Change the Service State for a Port](#)” task on page 19-9 for instructions.
- Step 10** Return to your originating procedure (NTP).
- 

## DLP-A314 Assign a Name to a Port

<b>Purpose</b>	This task assigns a name to a port on any ONS 15454 card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A323 Verify Card Installation, page 4-2</a> <a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** Double-click the card that has the port you want to provision.
- Step 2** Click the **Provisioning** tab.
- Step 3** Click the **Port Name** column for the port number to which you are assigning a name.
- Step 4** Type the port name.  
The port name can be up to 32 alphanumeric/special characters. The field is blank by default.
- Step 5** Click **Apply**.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A315 Log Out a User on a Single Node

<b>Purpose</b>	This task logs out a user from a single node.
<b>Tools/Equipment</b>	None



<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** In node view, click the **Provisioning > Security > Active Logins** tabs.
- Step 2** Choose the user that you want to log out and click **Logout**.
- Step 3** In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out. This prevents the user from logging in after logout based on parameters provided in the user lockouts in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the “[DLP-A271 Change Security Policy on a Single Node](#)” task on page 19-52 for more information.
- Step 4** Click **OK**.
- Step 5** Click **Yes** to confirm the logout.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A316 Log Out a User on Multiple Nodes

<b>Purpose</b>	This task logs out a user from multiple nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** From the View menu, chose **Go to Network View**.
- Step 2** Click the **Provisioning > Security > Active Logins** tabs.
- Step 3** Choose the user you want to log out.
- Step 4** Click **Logout**.
- Step 5** In the Logout User dialog box, check the nodes where you want to log out the user.
- Step 6** Check **Lockout before Logout** if you want to lock the user out prior to logout. This prevents the user from logging in after logout based on user lockout parameters provisioned in the Policy tab. A manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the “[DLP-A271 Change Security Policy on a Single Node](#)” task on page 19-52 for more information.
- Step 7** In the Select Applicable Nodes area, uncheck any nodes where you do not want to change the user’s settings (all network nodes are selected by default).
- Step 8** Click **OK**.

**Step 9** Return to your originating procedure (NTP).

## DLP-A320 View ML-Series Ether Ports PM Parameters

<b>Purpose</b>	This task enables you to view ML-Series Ethernet port PM counts at selected time intervals to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher



### Note

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

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

**Step 2** Click the **Performance > Ether Ports** tabs (Figure 20-1).

**Figure 20-1 Ether Ports on the ML-Series Card View Performance Window**

The screenshot shows the CTC interface for a Cisco Transport Controller. The main window displays the configuration for a card (techdoc-454-822 slot 17 ML1000). The card view shows the card is in a mismatch state. The performance tab is selected, and the ether ports sub-tab is active. The ether ports tab displays a table of performance statistics for two ether ports (Port 0 and Port 1). The table includes columns for Link Status, Param, Port 0 (ETHER), and Port 1 (ETHER). The statistics include various counters such as rxTotalPkts, rxIncastPkts, rxMulticastPkts, rxBroadcastPkts, txTotalPkts, txIncastPkts, txMulticastPkts, txBroadcastPkts, dot3StatsAlignmentErrors, dot3StatsFCSErrors, etherStatsUndersizePkts, etherStatsOversizePkts, etherStatsJabbers, and etherStatsCollisions. The statistics are shown for both Port 0 and Port 1, with values of 0 for most parameters. The interface also includes a Refresh button, an Auto-refresh menu (set to None), a Baseline... button, and a Help button. The status bar at the bottom shows the date and time: Statistics at Sep 10, 2004 2:33:08 PM IST.

Param	Port 0 (ETHER)	Port 1 (ETHER)
Link Status	Down	Down
rxInOctets	0	0
rxTotalPkts	0	0
rxIncastPkts	0	0
rxMulticastPkts	0	0
rxBroadcastPkts	0	0
txTotalPkts	0	0
txIncastPkts	0	0
txMulticastPkts	0	0
txBroadcastPkts	0	0
dot3StatsAlignmentErrors	0	0
dot3StatsFCSErrors	0	0
etherStatsUndersizePkts	0	0
etherStatsOversizePkts	0	0
etherStatsJabbers	0	0
etherStatsCollisions	0	0

- Step 3** Click **Refresh**. Performance monitoring statistics for each port on the card appear.
- Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the 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](#)” procedure on page 8-2.

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

## DLP-A321 View ML-Series POS Ports PM Parameters

<b>Purpose</b>	This task enables you to view packet-over-SONET (POS) port PM counts at selected time intervals on an ML-Series Ethernet card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher



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

- Step 1** In node view, double-click the ML-Series Ethernet card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > POS Ports** tabs ([Figure 20-2](#)).

Figure 20-2 POS Ports on the ML-Series Card View Performance Window

The screenshot shows the Cisco Transport Controller interface for a card labeled 'techdoc-454-822 slot 17 ML1000'. The 'Performance' tab is active, displaying a table of performance monitoring (PM) parameters for two POS ports. The table has columns for 'Param', 'Port 0 (POS)', and 'Port 1 (POS)'. The status of both ports is 'Down'. Below the table are buttons for 'Refresh', 'Auto-refresh' (set to 'None'), 'Baseline...', and 'Help'. A status bar at the bottom shows 'Statistics at September 10, 2004 2:36:02 PM IST' and a 'NET CKT' indicator.

Param	Port 0 (POS)	Port 1 (POS)
Link Status	Down	Down
ifInOctets	0	0
rxTotalPkts	0	0
ifOutOctets	0	0
txTotalPkts	0	0
etherStatsDropEvents	0	0
rxFktsDroppedInternalCongestion	0	0
mediaIndStatsRxFramesTruncated	0	0
mediaIndStatsRxFramesTooLong	0	0
mediaIndStatsRxFramesBadCRC	0	0
mediaIndStatsRxShortPkts	0	0
hdlcInOctets	0	0
hdlcRxAboorts	0	0
hdlcOutOctets	0	0

- Step 3** Click **Refresh**. Performance monitoring statistics for each port on the card appear.
- Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the 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” procedure on page 8-2](#).

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

## DLP-A322 Manual or Force Switch the Node Timing Reference

<b>Purpose</b>	This task commands the node to switch to the timing reference you have selected if the synchronization status message (SSM) quality of the requested reference is not less than the current reference.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

- 
- Step 1** In node view, click the **Maintenance > Timing > Source** tabs.
- Step 2** From the Reference drop-down list for the desired Clock, choose the desired reference.
- Step 3** From the Operation drop-down list for the desired Clock, choose one of the following options:
- **Manual**—This operation commands the node to switch to the reference you have selected if the SSM quality of the reference is not lower than the current timing reference.
  - **Force**—This operation commands the node to switch to the reference you have selected, regardless of the SSM quality (if the reference is valid).
- For information about the Clear option, see the “[DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference](#)” task on page 20-13.
- Step 4** Click **Apply** next to the timing source.
- Step 5** Click **Yes** in the confirmation dialog box. If the selected timing reference is an acceptable valid reference, the node switches to the selected timing reference.
- Step 6** If the selected timing reference is invalid, a warning dialog box appears. Click **OK**; the node does not revert to the normal timing reference.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-A323 Clear a Manual or Force Switch on a Node Timing Reference

<b>Purpose</b>	This task clears a Manual or Force switch on a node timing reference and reverts the timing reference to its provisioned reference.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

---

- Step 1** In node view, click the **Maintenance > Timing > Source** tabs.
- Step 2** Find the Clock reference that is currently set to Manual or Force in the Operation menu.
- Step 3** From the Operation drop-down list choose **Clear**.
- Step 4** Click **Apply**.
- Step 5** Click **Yes** in the confirmation dialog box. If the normal timing reference is an acceptable valid reference, the node switches back to the normal timing reference as defined by the system configuration.
- Step 6** If the normal timing reference is invalid or has failed, a warning dialog box appears. Click **OK**; the timing reference does not revert.
- Step 7** Return to your originating procedure (NTP).
-

## DLP-A324 Provision a VCAT Circuit Source and Destination

<b>Purpose</b>	This task provisions a virtual concatenated (VCAT) circuit source and destination.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> The Circuit Creation wizard Circuit Source page must be open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

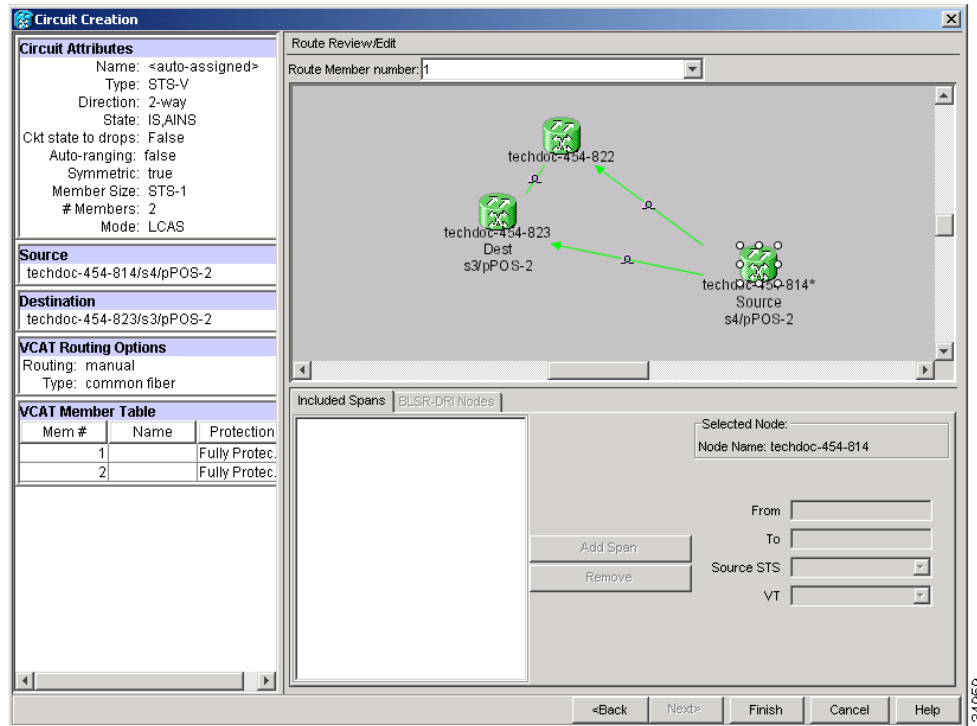
- 
- Step 1** From the Node drop-down list, choose the node where the circuit will originate.
- Step 2** From the Slot drop-down list, choose the slot containing the CE-Series, ML-Series, or FC\_MR-4 card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)
- Step 3** Depending on the circuit origination card, choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.
- Step 4** Click **Next**.
- Step 5** From the Node drop-down list, choose the destination node.
- Step 6** From the Slot drop-down list, choose the slot containing the CE-Series, ML-Series, or FC\_MR-4 card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)
- Step 7** Depending on the card selected in [Step 2](#), choose the source port and/or STS and, if applicable, VT from the Port and STS drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs and VTs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits.
- Step 8** Click **Next**.
- Step 9** Return to your originating procedure (NTP).
- 

## DLP-A325 Provision a VCAT Circuit Route

<b>Purpose</b>	This task provisions the circuit route for manually routed VCAT circuits.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> The Circuit Creation wizard Route Review and Edit page must be open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** In the Circuit Creation wizard in the Route Review and Edit area, choose the member number from the Route Member Number drop-down list.
- Step 2** Click the source node icon if it is not already selected.
- Step 3** Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns yellow. In the Selected Span area, the From and To fields provide span information. The source STS appears. [Figure 20-3](#) shows an example.

**Figure 20-3** Manually Routing a VCAT Circuit



- Step 4** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.
- Step 5** Repeat Steps 3 and 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes.
- Step 6** Repeat Steps 1 through 5 for each member.
- Step 7** Return to your originating procedure (NTP).

## DLP-A326 Change a BLSR Node ID

<b>Purpose</b>	This task changes a BLSR node ID.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed

<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

## DLP-A327 Configure the CTC Alerts Dialog Box for Automatic Popup

<b>Purpose</b>	This task sets up the CTC Alerts dialog box to open for all alerts, for circuit deletion errors only, or never. The CTC Alerts dialog box displays network disconnection, Send-PDIP inconsistency, circuit deletion status, condition retrieval errors, and software download failure.
<b>Tools</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher


- 
- Step 1** Click the **CTC Alerts** toolbar icon.
- Step 2** In the CTC Alerts dialog box, choose one of the following:
- **All alerts**—Sets the CTC Alerts dialog box to open automatically for all notifications.
  - **Error alerts only**—Sets the CTC Alerts dialog box to open automatically for circuit deletion errors only.
  - **Never**—Sets the CTC Alerts dialog box to never open automatically.
- Step 3** Click **Close**.
- Step 4** Return to your originating procedure (NTP).
- 

## DLP-A328 Create a Two-Fiber BLSR Using the BLSR Wizard

<b>Purpose</b>	This task creates a two-fiber BLSR at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at one time.
<b>Tools/Equipment</b>	None



<b>Prerequisite Procedures</b>	<a href="#">NTP-A40 Provision BLSR Nodes, page 5-10</a> <a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > BLSR** tabs.
- Step 3** Click **Create BLSR**.
- Step 4** In the BLSR Creation dialog box, set the BLSR properties:
- Ring Type—Choose two-fiber.
  - Speed—Choose the BLSR ring speed: OC-12, OC-48, or OC-192. The speed must match the OC-N speed of the BLSR trunk (span) cards.
-  **Note** If you are creating an OC-12 BLSR and will eventually upgrade it to OC-48 or OC-192, use the single-port OC-12 cards (OC12 IR/STM4 SH 1310, OC12 IR/STM4 SH 1310, or OC12 IR/STM4 SH 1310). You cannot upgrade a BLSR on a four-port OC-12 (OC12/STM4-4) because OC-48 and OC-192 cards are single-port.
- 
- Ring Name—Assign a ring name. The name can be from 1 to 6 characters in length. Any alphanumeric string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
  - Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path following a ring switch. The default is 5 minutes. Ring reversion can be set to Never.
- Step 5** Click **Next**. If the network graphic appears, go to Step 6.
- If CTC determines that a BLSR cannot be created, for example, not enough optical cards are installed or it finds circuits with path protection selectors, a “Cannot Create BLSR” message appears. If this occurs, complete the following steps:
- a. Click **OK**.
  - b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.
  - c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
  - d. Complete the “[NTP-A40 Provision BLSR Nodes](#)” procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.
- Step 6** In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to [Step 7](#).
- Step 7** Click **Finish**. If the BLSR window appears with the BLSR you created, go to [Step 8](#). If a “Cannot Create BLSR” or “Error While Creating BLSR” message appears:
- a. Click **OK**.
  - b. In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.

- c. Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
- d. Complete the “[NTP-A40 Provision BLSR Nodes](#)” procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.



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

**Step 8** Verify the following:

- On the network view graphic, a green span line appears between all BLSR nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.



**Note** The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the “[DLP-A326 Change a BLSR Node ID](#)” task on page 20-15.

**Step 9** Return to your originating procedure (NTP).

## DLP-A329 Create a Two-Fiber BLSR Manually

<b>Purpose</b>	This task creates a BLSR at each BLSR-provisioned node without using the BLSR wizard.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A40 Provision BLSR Nodes, page 5-10</a> <a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

**Step 2** Click **Create**.

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

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

- Ring Type—Choose two-fiber.
- Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
- Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.

- Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
- West Line—Assign the west BLSR port for the node from the drop-down list.  
The east and west ports must match the fiber connections and DCC terminations set up in the [“NTP-A40 Provision BLSR Nodes” procedure on page 5-10](#).
- East Line—Assign the east BLSR port for the node from the drop-down list.

**Step 5** Click **OK**.




---

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

---

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

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

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

**Step 9** From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:

- A green span line appears between all BLSR nodes.
- All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared.

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

---

## DLP-A330 Preprovision a Card Slot

<b>Purpose</b>	This task preprovisions a card slot in CTC before you physically install the card in the ONS 15454.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** In node view, right-click the empty slot where you will later install a card.

**Step 2** From the Add Card shortcut menu, choose the card type that will be installed. Only cards that can be installed in the slot appear in the Add Card shortcut menu.

When you preprovision a slot, the card appears purple in the CTC shelf graphic, rather than white when a card is installed in the slot. NP (not present) on the card graphic indicates that the card is not physically installed.

**Step 3** Return to your originating procedure (NTP).

---

## DLP-A332 Change Tunnel Type

<b>Purpose</b>	This task converts a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional SDCC tunnel.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A313 Create a DCC Tunnel, page 20-7</a> <a href="#">DLP-A341 Create an IP-Encapsulated Tunnel, page 20-31</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

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

**Step 2** Click the **Provisioning > Overhead Circuits** tabs.

**Step 3** Click the circuit tunnel that you want to convert.

**Step 4** Click **Edit**.

**Step 5** In the Edit circuit window, click the **Tunnel** tab.

**Step 6** In the Attributes area, complete the following:

- If you are converting a traditional DCC tunnel to an IP-encapsulated tunnel, check the **Change to IP Tunnel** check box and type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).
- If you are converting an IP tunnel to a traditional DCC tunnel, check the **Change to SDCC Tunnel** check box.

**Step 7** Click **Apply**.

**Step 8** In the confirmation dialog box, click **Yes** to continue.

**Step 9** In the Circuit Changed status box, click **OK** to acknowledge that the circuit change was successful.

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

---

## DLP-A333 Delete Circuits

<b>Purpose</b>	This task deletes circuits.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Complete the “[NTP-A108 Back Up the Database](#)” procedure on page 15-4.
- Step 2** Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.
- Step 3** From the View menu, choose **Go to Network View**.
- Step 4** Click the **Alarms** tab.
- Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on page 19-18 as necessary.
  - 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.
- Step 5** Click the **Circuits** tab.
- Step 6** Choose the circuits you want to delete, then click **Delete**.
- Step 7** In the Delete Circuits confirmation dialog box, check one or both of the following, as needed:
- Change drop port admin state—Choose the administrative state for the drop ports:
    - IS—Puts the circuit cross-connects in the In-Service and Normal (IS-NR) service state.
    - OOS,DSBLD—Puts the circuit cross-connects in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. Traffic is not passed on the circuit. If the circuit is not the same size as the port or the only circuit using the port, CTC will not change the port service state.
    - IS,AINS—Puts the circuit cross-connects in the Out-of-Service and Autonomous, Automatic In-Service (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 Out-of-Service and Management, Maintenance (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.




---

**Note** CTC will not allow you to change a drop 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.

---

- Notify when completed—If checked, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are out of service (OOS) and the circuit is deleted. During this time, you cannot perform other CTC functions. If you are deleting many circuits, you might need to wait a few minutes for confirmation. Circuits are deleted whether or not this check box is checked.




---

**Note** The CTC Alerts dialog box will not automatically open to show a deletion error unless you checked All alerts or Error alerts only in the CTC Alerts check box. For more information, see the “[DLP-A327 Configure the CTC Alerts Dialog Box for Automatic Pop-up](#)” task on page 20-16. If the CTC Alerts dialog box is not set to open automatically with a notification, the red triangle inside the CTC Alerts toolbar icon indicates that a notification exists.

---

- Step 8** Complete one of the following:
- If you checked Notify when completed, the CTC Alerts dialog box appears. If you want to save the information, continue with [Step 9](#). If you do not want to save the information, continue with [Step 10](#).

- If you did not check Notify when completed, the Circuits window appears. Continue with [Step 11](#).
- Step 9** If you want to save the information in the CTC Alerts dialog box, complete the following steps. If you do not want to save, continue with the [Step 10](#).
- a. Click **Save**.
  - b. Click **Browse** and navigate to the directory where you want to save the file.
  - c. Type the file name using a .txt file extension, and click **OK**.
- Step 10** Click **Close** to close the CTC Alerts dialog box.
- Step 11** Complete the “[NTP-A108 Back Up the Database](#)” procedure on page 15-4.
- Step 12** Return to your originating procedure (NTP).
- 

## DLP-A334 Delete Overhead Circuits

<b>Purpose</b>	This task deletes overhead circuits. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, the AIC-I card orderwire, and the AIC-I card user data channel (UDC).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Caution

Deleting overhead circuits is service affecting if the circuits are in service (IS). To put circuits out of service (OOS), see the “[DLP-A214 Change the Service State for a Port](#)” task on page 19-9.

---

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Provisioning > Overhead Circuits** tabs.
- Step 3** Click the overhead circuit that you want to delete: local or express orderwire, user data, IP-encapsulated tunnel, or DCC tunnel.
- Step 4** Click **Delete**.
- Step 5** In the confirmation dialog box, click **Yes** to continue.
- Step 6** Return to your originating procedure (NTP).
-

## DLP-A335 Delete VLANs

<b>Purpose</b>	This task removes VLANs from a domain.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	See <a href="#">Chapter 6, “Create Circuits and VT Tunnels”</a> for circuit creation procedures.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** VLANs in use will not be deleted.

- 
- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** From the Tools menu, choose **Manage VLANs**.
- Step 3** In the All VLANs dialog box, click the VLAN that you want to remove.
- Step 4** Click **Delete**.
- Step 5** In the confirmation dialog box, click **Yes**.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A336 Repair an IP Tunnel

<b>Purpose</b>	This task repairs circuits that have a OOS-PARTIAL status as a result of node IP address changes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	See <a href="#">Chapter 6, “Create Circuits and VT Tunnels”</a> for circuit creation procedures.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Obtain the original IP address of the node in question.
- Step 2** From the View menu, choose **Go to Network View**.
- Step 3** From the Tools menu, choose **Overhead Circuits > Repair IP Circuits**.
- Step 4** Review the text in the IP Repair wizard and click **Next**.
- Step 5** In the Node IP address area, complete the following:
- Node—Choose the node that has an OOS-PARTIAL circuit.
  - Current IP Address—Type the current IP address.
  - Old IP Address—Type the node’s original IP address.

- Step 6** Click **Next**.
- Step 7** Click **Finish**.
- Step 8** Return to your originating procedure (NTP).
- 

## DLP-A337 Run the CTC Installation Wizard for Windows

<b>Purpose</b>	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 5.0, and the CTC JAR files on a Windows computer. JRE 5.0 is required to run Release 8.0. Pre-installing the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you login.
<b>Tools/Equipment</b>	Cisco ONS 15454 Release 8.0 software or documentation CD
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	This task is required if any one of the following is true: <ul style="list-style-type: none"> <li>• JRE 1.4.2 or JRE 5.0 is not installed.</li> <li>• CTC online user manuals are not installed and are needed.</li> <li>• CTC JAR files are not installed and are needed.</li> </ul>
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None



### Note

If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 1.4.2 or 5.0 and reinstall JRE 1.3.1\_2. To run Software R8.0, uninstall JRE 1.3.1\_2 and reinstall JRE 1.4.2 or 5.0. Software R8.0 supports JRE 1.4.2 or JRE 5.0; JRE 1.4.2 is provided on the software CD.

---



### Note

JRE 1.4.2 requires Netscape 7.x or Internet Explorer 6.x

---

- Step 1** Verify that your computer has the following:
- Processor—Pentium III, 700 Mhz or faster
  - RAM—384 MB recommended, 512 MB optimum
  - Hard drive—20 GB hard drive recommended with at least 50 MB of space available
  - Operating system—Windows 98 (1st and 2nd editions), Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), or Windows XP Home

If your operating system is Windows NT 4.0, verify that Service Pack 6a or later is installed. From the Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site.





**Note** Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

**Step 2** Insert the Cisco ONS 15454 Release 8.0 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to the CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 1.4.2
- Acrobat Reader 6.0.1
- Online User Manuals
- CTC JAR files

**Step 3** Click **Next**.

**Step 4** Complete one of the following:

- Click **Typical** to install all three components. If you already have JRE 1.4.2 or 5.0 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals. By default, the JRE and Acrobat Reader are selected.

**Step 5** Click **Next**.

**Step 6** Complete the following, as applicable:

- If you selected Typical in [Step 4](#), skip this step and continue with [Step 7](#).
- If you selected Custom, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with [Step 7](#).
  - If you did not select Online User Manuals, continue with [Step 9](#).

**Step 7** The directory where the installation wizard will install CTC online user manuals appears. The default is C:\Program Files\Cisco\CTC\Documentation.

- If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the directory, skip this step.

**Step 8** Click **Next**.

**Step 9** Review the components that will be installed. If you want to change the components, complete one of the following:

- If you selected Typical in [Step 4](#), click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 5 through 8.
- If you selected Custom in [Step 4](#), click **Back** once or twice (depending on the components selected) until the component selection page appears. Repeat Steps 6 through 8.

**Step 10** Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in [Step 4](#) and you need to install the JRE, continue with [Step 12](#).

**Step 11** To install the JRE, complete the following:

- a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:

- I accept the terms of the license agreement—Accepts the license agreement. Continue with Step [b](#).
- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with [Step 12](#).




---

**Note** If JRE 1.4.2 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step [e](#). If you choose Remove and click Next, continue with Step [i](#).

---

- b.** Click **Next**.
- c.** Choose one of the following:
  - Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
  - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.
- d.** Click **Next**.
- e.** If you selected Typical, continue with Step [i](#). If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:
  - Java 2 Runtime Environment—(Default) Installs JRE 1.4.2 with support for European languages.
  - Support for Additional Languages—Adds support for non-European languages.
  - Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

- f.** Click **Next**.
- g.** In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.




---

**Note** Setting the JRE as the default for these browsers might cause problems with these browsers.

---

- h.** Click **Next**.
- i.** Click **Finish**. If you are uninstalling the JRE, click **Remove**.

- Step 12** In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals install.
- Step 13** Click **Finish**.
- Step 14** Return to your originating procedure (NTP).

## DLP-A338 Run the CTC Installation Wizard for UNIX

<b>Purpose</b>	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 1.4.2, and the CTC JAR files on a Solaris workstation. JRE 1.4.2 or JRE 1.5 is required to run Release 8.0. Pre-installing the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TCC2/TCC2P card the first time you login.
<b>Tools/Equipment</b>	Cisco ONS 15454 Release 8.0 software or documentation CD
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required if any of the following are true: <ul style="list-style-type: none"> <li>• JRE 1.4.2 or 5.0 is not installed.</li> <li>• CTC online user manuals are not installed and are needed.</li> <li>• CTC JAR files are not installed are needed.</li> </ul>
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None



### Note

If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 1.4.2 or 5.0 and reinstall JRE 1.3.1\_2. To run Software R8.0, uninstall JRE 1.3.1\_2 and reinstall JRE 5.0. Software R8.0 supports JRE 5.0; JRE 5.0 is provided on the software CD.



### Note

JRE 5.0 requires Netscape 7.x or Internet Explorer 6.x

- Step 1** Verify that your computer has the following:
- RAM—384 MB recommended, 512 MB optimum
  - Hard drive—20 GB hard drive recommended with at least 50 MB of space available
  - Operating system—Solaris 8 or 9



### Note

These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

- Step 2** Change the directory, type:
- ```
cd /cdrom/cdrom0/
```
- Step 3** From the techdoc454 CD directory, type:
- ```
./setup.bat
```

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer:

- Java Runtime Environment 1.4.2
- Acrobat Reader 6.0.1
- Online User Manuals
- CTC JAR files

**Step 4** Click **Next**.

**Step 5** Complete one of the following:

- Click **Typical** to install both the Java Runtime Environment and online user manuals. If you already have JRE 5.0 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals.

**Step 6** Click **Next**.

**Step 7** Complete the following, as applicable:

- If you selected Typical in [Step 5](#), continue with [Step 8](#).
- If you selected Custom, check the CTC component that you want to install and click **Next**.
  - If you selected Online User Manuals, continue with [Step 8](#).
  - If you did not select Online User Manuals, continue with [Step 10](#).

**Step 8** The directory where the installation wizard will install CTC online user manuals appears. The default is `/usr/doc/ctc`.

- If you want to change the CTC online user manuals directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.
- If you do not want to change the CTC online user manuals directory, skip this step.

**Step 9** Click **Next**.

**Step 10** Review the components that will be installed.

- If you selected Typical in [Step 5](#), click **Back** twice to return to the installation setup type page. Choose **Custom** and repeat Steps 6 through 9.
- If you selected Custom in [Step 5](#), click **Back** once or twice (depending on the components selected) you reach the component selection page and check the desired components. Repeat Steps 7 through 9.

**Step 11** Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in [Step 4](#) and you need to install the JRE, continue with [Step 13](#).

**Step 12** To install the JRE, complete the following:

- a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:
  - I accept the terms of the license agreement—Accepts the license agreement. Continue with [Step b](#).
  - I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with [Step 13](#).

**Note**

If JRE 5.0 is already installed on your computer, the License Agreement page does not appear. You must click **Next** and then choose **Modify** to change the JRE installation or **Remove** to uninstall the JRE. If you choose **Modify** and click **Next**, continue with Step **e**. If you choose **Remove** and click **Next**, continue with Step **i**.

- b. Click **Next**.
- c. Choose one of the following:
  - Click **Typical** to install all JRE features. If you select **Typical**, the JRE version installed will automatically become the default JRE version for your browsers.
  - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.
- d. Click **Next**.
- e. If you selected **Typical**, continue with Step **i**. If you selected **Custom**, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:
  - Java 2 Runtime Environment—(Default) Installs JRE 5.0 with support for European languages.
  - Support for Additional Languages—Adds support for non-European languages.
  - Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

The drop-down list options for each program feature include:

- This feature will be installed on the local hard drive—Installs the selected feature.
- This feature and all subfeatures will be installed on the local hard drive—Installs the selected feature and all subfeatures.
- Don't install this feature now—Does not install the feature (not an option for Java 2 Runtime Environment).

To modify the directory where the JRE version is installed, click **Change**, navigate to the desired directory, and click **OK**.

- f. Click **Next**.
- g. In the Browser Registration dialog box, check the browsers that you want to register with the Java Plug-In. The JRE version will be the default for the selected browsers. It is acceptable to leave both browser check boxes unchecked.

**Note**

Setting the JRE version as the default for these browsers might cause problems with these browsers.

- h. Click **Next**.
- i. Click **Finish**. If you are uninstalling the JRE, click **Remove**.

**Step 13** In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals install.

**Step 14** Click **Finish**.

**Note**

Be sure to record the names of the directories you choose for JRE and the online user manuals.

**Step 15** Return to your originating procedure (NTP).

---

## DLP-A339 Delete a Node from the Current Session or Login Group

<b>Purpose</b>	This task removes a node from the current CTC session or login node group. To remove a node from a login node group that is not the current one, see the “ <a href="#">DLP-A372 Delete a Node from a Specified Login Node Group</a> ” task on page 20-55.
<b>Tools</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the node that you want to delete.
- Step 3** From the CTC File menu, click **Delete Selected Node**.  
After a few seconds, the node disappears from the network view map.
- Step 4** Return to your originating procedure (NTP).
- 

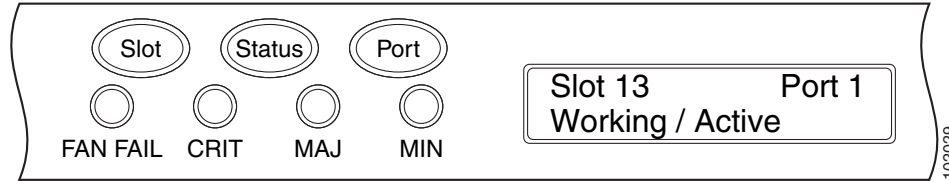
## DLP-A340 View Port Status on the LCD

<b>Purpose</b>	This task allows you to view OC-N port status without using CTC. The LCD shows the working/protection provisioning status and the active/standby line status for ports in 1+1 and BLSR configurations. For unprotected and path protection ports, the LCD always displays “Working/Active.”
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A16 Install Optical Cards and Connectors</a> , page 2-7
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

- Step 1** Press the **Slot** button on the LCD panel until the desired slot appears on the LCD.
- Step 2** Press the **Port** button until the desired port appears on the LCD. (Only Port 1 of single-port cards will display actual port status.)
- Step 3** Press the **Status** button. The LCD will display alarm information for approximately 10 seconds, and then will indicate if the port is in working or protect mode and is active or standby.

[Figure 20-4](#) shows an example of port status on the LCD panel.

**Figure 20-4** Port Status on the LCD Panel

**Note** A blank LCD results when the fuse on the AIP board has blown. If this occurs, contact Cisco Technical Assistance (TAC). See the [“Obtaining Documentation and Submitting a Service Request”](#) section on page lxiii for more information.

**Step 4** Return to your originating procedure (NTP).

## DLP-A341 Create an IP-Encapsulated Tunnel

<b>Purpose</b>	This task creates a an IP-encapsulated tunnel to transport traffic from third-party SONET equipment across ONS 15454 networks. IP-encapsulated tunnels are created on the Section DCC channel (D1-D3) (if not used by the ONS 15454 as a terminated DCC).
<b>Tools/Equipment</b>	OC-N cards must be installed.
<b>Prerequisite Procedures</b>	<a href="#">NTP-A35 Verify Node Turn-Up, page 5-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** Each ONS 15454 can have up to ten IP-encapsulated tunnel connections. Terminated Section DCCs used by the ONS 15454 cannot be used as tunnel endpoints, and a Section DCC that is used as a tunnel endpoint cannot be terminated. All tunnel connections are bidirectional.

- Step 1** Verify that IP addresses are provisioned at both the source and destination nodes of the planned tunnel. For more information, see the [“DLP-A249 Provision IP Settings”](#) task on page 19-30.
- Step 2** In network view, click the **Provisioning > Overhead Circuits** tabs.
- Step 3** Click **Create**.
- Step 4** In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:
- Name—Type the tunnel name.
  - Type—Choose **IP Tunnel-D1-D3**.
  - Maximum Bandwidth—Type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).
- Step 5** Click **Next**.
- Step 6** 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.
- Channel—Displays IPT (D1-D3).

**Step 7** Click **Next**.

**Step 8** 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.
- Channel—Displays IPT (D1-D3).

**Step 9** Click **Finish**.

**Step 10** Put the ports that are hosting the IP-encapsulated tunnel in service. See the “[DLP-A214 Change the Service State for a Port](#)” task on page 19-9 for instructions.

**Step 11** Return to your originating procedure (NTP).

---

## DLP-A347 Refresh E-Series and G-Series Ethernet PM Counts

<b>Purpose</b>	This task changes the window view to display E-Series and G-Series Ethernet PM parameters intervals.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

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

**Step 2** Click the **Performance > History** tabs.

**Step 3** From the Interval drop-down list click one of the following:

- 1 min
- 15 min
- 1 hour
- 1 day

**Step 4** Click **Refresh**. Performance monitoring appears in the interval selected synchronized with the time of day.

**Step 5** View the Prev column to find PM counts for the latest selected interval.

Each monitored performance parameter has corresponding threshold values for the latest time period. If the value of the counter exceeds the threshold value for a particular selected interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.



- Step 6** View the Prev-*n* columns to find PM counts for the previous intervals.
- If a complete count over the selected interval is not possible, the value appears with a yellow background. For example, if you selected the 1-day interval, an incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port service states. When the problem is corrected, the subsequent 1-day interval appears with a white background.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-A348 Monitor PM Counts for a Selected Signal

<b>Purpose</b>	This task enables you to view near-end or far-end PM counts for a specific signal (STS <i>n</i> ), path (VT <i>n</i> ), and port (DS <i>n</i> ) on a selected card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

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

**Step 2** Click the **Performance** tab.

Different port and signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM cards list DS3, DS1, VT path, and STS path PM parameters as signal types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

**Step 3** In the signal type drop-down lists, click the following options as appropriate:

- DS: *n* or Port: *n* (card port number)
- VT: *n* (VT path number)
- STS: *n* (STS number within the VT path)

[Figure 20-5](#) shows the port and signal type drop-down lists on the Performance window for a DS3XM-6 card.

Figure 20-5 Signal Type Drop-Down Lists for a DS3XM-6 Card

The screenshot shows the Cisco Transport Controller interface for a DS3XM-6 card. The Performance tab is active, displaying a table of PM parameters. The control panel at the bottom includes several interactive elements:

- Directions radio buttons:** Near End (selected) and Far End.
- Intervals radio buttons:** 15 min (selected) and 1 day.
- Signal-type port drop-down list:** DS3:1
- Sub-signal drop-down list:** DS1:1
- Refresh button:** Refresh
- Auto-refresh drop-down list:** 15 Seconds
- Baseline button:** Baseline
- Clear button:** Clear...
- Help button:** Help

The table below shows the PM parameter values for the selected card and port:

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
DS3 CV-L	0	0	0	0	0	0	0	0	0	0
DS3 ES-L	0	0	0	0	0	0	0	0	0	0
DS3 LOSS-L	0	0	0	0	0	0	0	0	0	0
DS3 SES-L	0	0	0	0	0	0	0	0	0	0
DS3 MIS-P	0	0	0	0	0	0	0	0	0	0
DS3 CVP-P	0	0	0	0	0	0	0	0	0	0
DS3 ESP-P	0	0	0	0	0	0	0	0	0	0
DS3 SASP-P	0	0	0	0	0	0	0	0	0	0
DS3 SES-P	0	0	0	0	0	0	0	0	0	0
DS3 UASP-P	0	0	0	0	0	0	0	0	0	0
DS3 CVCP-P	0	0	0	0	0	0	0	0	0	0
DS3 ESCP-P	0	0	0	0	0	0	0	0	0	0

- Step 4** Click **Refresh**. All PM counts recorded by the near-end or far-end node for the specified outgoing signal type on the selected card and port appear. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.
- Step 5** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.
- Step 6** Return to your originating procedure (NTP).

## DLP-A349 Clear Selected PM Counts

<b>Purpose</b>	This task uses the Clear button to clear specified PM counts depending on the option selected.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

**Caution**

Pressing the Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes. After pressing this button the current bin is marked invalid. Also note that the UAS state is not cleared if you were counting UAS; therefore, this count could be unreliable when UAS is no longer counting.

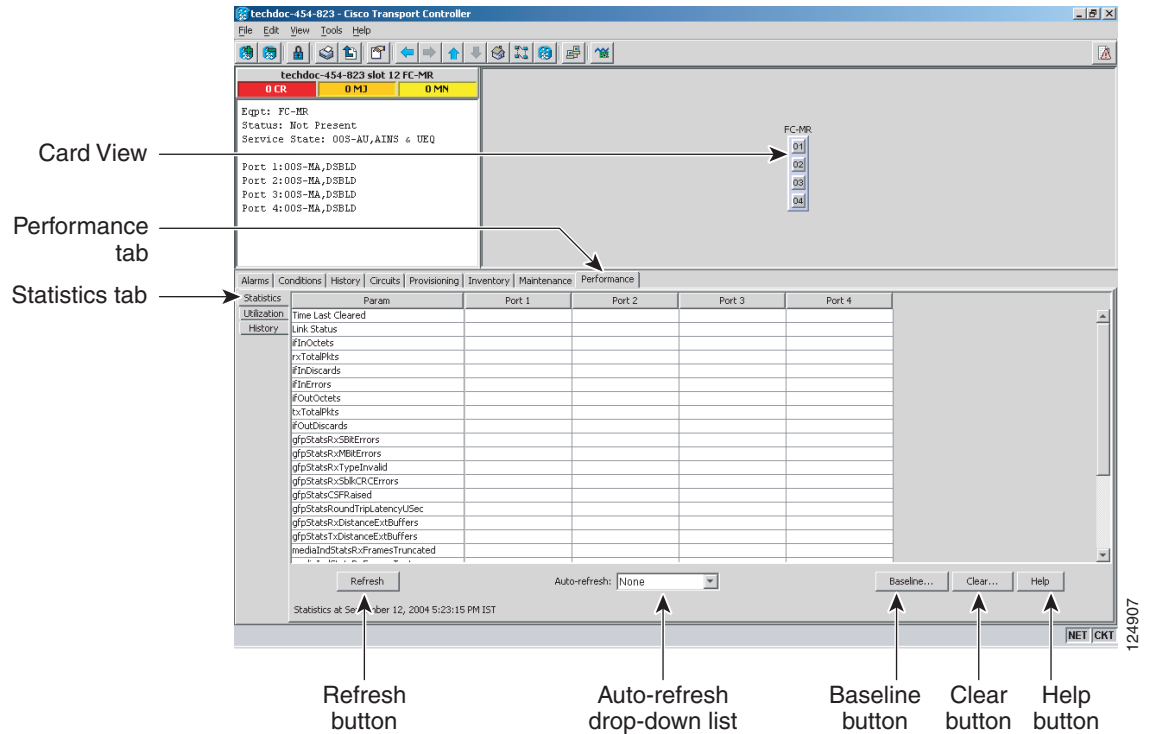
- 
- Step 1** In node view, double-click the card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** Click **Clear**.
- Step 4** From the Clear Statistics drop-down list, choose one of these three options:
- **Displayed statistics:** Clearing displayed statistics erases from the card and the window all PM counts associated with the current combination of statistics on the selected port. This means the selected time interval, direction, and signal type counts are erased from the card and the window.
  - **All statistics for port *x*:** Clearing all statistics for port *x* erases from the card and the window all PM counts associated with all combinations of the statistics on the selected port. This means all time intervals, directions, and signal type counts are erased from the card and the window.
  - **All statistics for card:** Clearing all statistics for card erases from the card and the window all PM counts for all ports.
- Step 5** From the Clear Statistics drop-down list, choose **OK** to clear the selected statistics.
- Step 6** Verify that the selected PM counts have been cleared.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-A350 View FC\_MR-4 Statistics PM Parameters

<b>Purpose</b>	This task enables you to view current statistical PM counts on an FC_MR-4 card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- 
- Step 1** In node view, double-click the FC\_MR-4 card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Statistics** tabs ([Figure 20-6](#)).

Figure 20-6 FC\_MR-4 Statistics on the Card View Performance Window



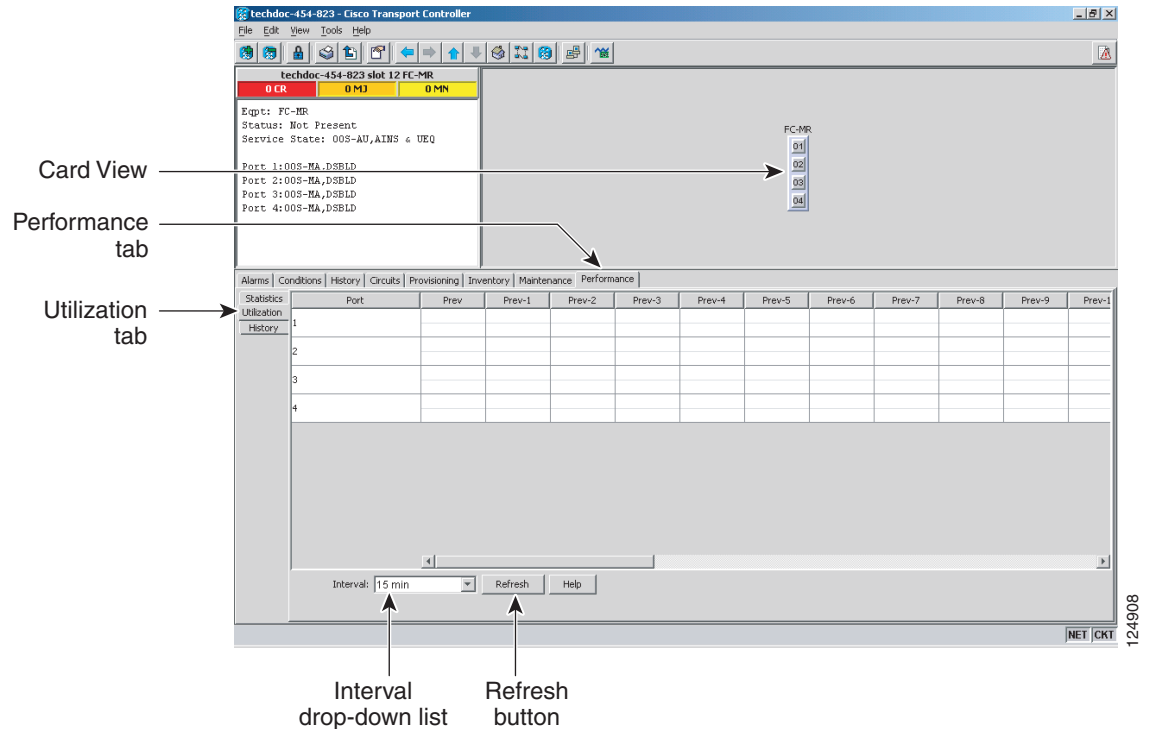
- Step 3** Click **Refresh**. Performance monitoring statistics for each port on the card appear.
- Step 4** View the PM parameter names appear in the Param column. The current PM parameter values appear in the Port # columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.
- Step 5** Return to your originating procedure (NTP).

## DLP-A351 View FC\_MR-4 Utilization PM Parameters

<b>Purpose</b>	This task enables you to view line utilization PM counts on an FC_MR-4 card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click the FC\_MR-4 card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Utilization** tabs (Figure 20-7).

Figure 20-7 FC\_MR-4 Utilization on the Card View Performance Window



- Step 3** Click **Refresh**. Performance monitoring utilization values for each port on the card appear.
- Step 4** View the Port # column to find the port you want to monitor.
- Step 5** The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.
- Step 6** Return to your originating procedure (NTP).

## DLP-A352 View FC\_MR-4 History PM Parameters

<b>Purpose</b>	This task enables you to view historical PM counts at selected time intervals on an FC_MR-4 card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click the FC\_MR-4 card where you want to view PM counts. The card view appears.

**Step 2** Click the **Performance > History** tabs (Figure 20-8).

**Figure 20-8** FC\_MR-4 History on the Card View Performance Window

Card View

Performance tab

History tab

Interval drop-down list

Port drop-down list

Refresh button

Param	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9
#InOctets										
#OutOctets										
#InDiscards										
#InErrors										
#OutErrors										
#OutDiscards										
gfpStatsRxSBBErrors										
gfpStatsRxMBRErrors										
gfpStatsRxTypeInvald										
gfpStatsRxSbKCRCErrors										
gfpStatsCSFRAssed										
mediaIndStatsRxFramesTruncated										
mediaIndStatsRxFramesTooLong										
mediaIndStatsRxFramesBadCRC										
mediaIndStatsTxFramesBadCRC										

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

**Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-*n* columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.

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

## DLP-A353 Refresh FC\_MR-4 PM Counts at a Different Time Interval

<b>Purpose</b>	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

**Step 1** In node view, double-click the FC\_MR-4 card where you want to view PM counts. The card view appears.

- Step 2** Click the **Performance** tab.
- Step 3** Click the **Utilization** or the **History** tab.
- Step 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.
- Step 5** Click **Refresh**. The PM counts refresh with values based on the selected time interval.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A356 TCC2/TCC2P Card Active/Standby Switch Test

<b>Purpose</b>	This task verifies that the TCC2/TCC2P cards can effectively switch from one to another.
<b>Tools/Equipment</b>	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Alarms** tab.
- a. Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on [page 19-18](#) as necessary.
  - b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 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.
- Step 4** On the network map, double-click the node containing the TCC2/TCC2P cards you are testing to open it in node view.
- Step 5** Make a note of which TCC2/TCC2P card is active and which is standby by examining the LEDs on the shelf graphic. TCC2/TCC2P cards are installed in Slot 7 and Slot 11. The active TCC2/TCC2P card has a green ACT LED, and the standby TCC2/TCC2P card has an amber SBY LED.
- Step 6** On the shelf graphic, right-click the active TCC2/TCC2P card and choose **Reset** from the shortcut menu.
- Step 7** In the Resetting Card dialog box, click **Yes**. After 20 to 40 seconds, a “lost node connection, changing to network view” message appears. On the network view map, the node where you reset the TCC2/TCC2P card will be gray.

- Step 8** After the node icon becomes available (within 1 to 2 minutes), double-click it. On the shelf graphic, observe the following:
- The previous standby TCC2/TCC2P card has a green ACT LED.
  - The previous active TCC2/TCC2P card LEDs go through the following LED sequence: NP (card not present), Ldg (software is loading), amber SBY LED (TCC2/TCC2P is in standby mode).
- Step 9** Verify that traffic on the test set connected to the node is still running. If a traffic interruption occurs, do not continue, refer to your next level of support.
- Step 10** Repeat Steps 2 through 9 to return the active/standby TCC2/TCC2P cards to their configuration at the start of the procedure.
- Step 11** Verify that the TCC2/TCC2P cards appear as noted in [Step 5](#).
- Step 12** Return to your originating procedure (NTP).
- 

## DLP-A357 Create FC\_MR-4 RMON Alarm Thresholds

<b>Purpose</b>	This task sets up remote monitoring (RMON) to allow network management systems to monitor FC_MR-4 ports.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60 at the node where you want to set up RMON
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



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

---

- Step 1** In node view, double-click the FC\_MR-4 card where you want to create the RMON alarm thresholds.
- Step 2** Click the **Provisioning > RMON Thresholds** tabs.
- Step 3** Click **Create**. The Create Threshold dialog box appears.
- Step 4** From the Slot drop-down list, choose the appropriate FC\_MR-4 card.
- Step 5** From the Port drop-down list, choose the applicable port on the FC\_MR-4 card you selected.
- Step 6** From the Variable drop-down list, choose the variable. See [Table 20-1](#) for a list of the FC\_MR-4 threshold variables available in this field.



**Table 20-1** *FC\_MR-4 Threshold Variables Fibre Channel/FICON Line Rate Mode (MIBs)*

<b>Variable</b>	<b>Definition</b>
ifInOctets	Total number of octets received on the interface, including framing octets.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
ifInErrors	Number of inbound packets discarded because they contain errors.
ifOutOctets	Total number of transmitted octets, including framing packets.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
txTotalPkts	Total number of transmit packets.
rxTotalPkts	Total number of receive packets.
fibresStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined Fibre Channel control words.
fibresStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.
fibresStatsRxFramesTooLong	Received oversize Fibre Channel frames > 2148 including cyclic redundancy check (CRC).
fibresStatsRxFramesBadCRC	Received Fibre Channel frames with bad CRC.
fibresStatsRxFrames	Received total Fibre Channel frames.
fibresStatsRxBits	Received total Fibre Channel data bytes within a frame.
fibresStatsTxFramesBadCRC	Transmitted Fibre Channel frames with bad CRC.
fibresStatsTxFrames	Transmitted total Fibre Channel frames.
fibresStatsTxBits	Transmitted total Fibre Channel data bytes within a frame.
fibresStatsLinkResets	Total number of link resets initiated by an FCMR port when the link recovery port setting is enabled.
gfpStatsRxBitsErrors	Received generic framing protocol (GFP) frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxBitsErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect Fibre Channel data.
gfpStatsRxBitsCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks which each contain Fibre Channel data.
gfpStatsCSFRaised	Number of Rx client management frames with Client Signal Fail indication.

**Table 20-1** *FC\_MR-4 Threshold Variables Fibre Channel/FICON Line Rate Mode (MIBs) (continued)*

Variable	Definition
mediaIndStatsTxFramesTooLong	Number of packets transmitted that are greater than 1548 bytes
mediaIndStatsRxFramesTruncated	Total number of frames received that are less than 5 bytes

Table 20-2 lists the enhanced mode MIBs available.

**Table 20-2** *FC\_MR-4 Threshold Variables Fiber Channel/FICON Enhanced Mode (MIBs)*

Variable	Definition
ifInOctets	Total number of octets received on the interface, including framing octets.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
ifInErrors	Number of inbound packets discarded because they contain errors.
ifOutOctets	Total number of transmitted octets, including framing packets.
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.
fcIngressRxDistanceExtBuffers	The maximum number of GFP buffers that are available at the GFP receiver.
fcEgressTxDistanceExtBuffers	The number of GFP buffers that the GFP transmitter is allowed to transmit. Remote GFP receiver tells the GFP transmitter how many buffers it has available.
fcStatsLinkRecoveries	The number of times a link reset was initiated due to a GFP out of frame condition. This is only valid when link recovery is enabled and is not valid when distance extension is enabled.
fcStatsRxCredits	The maximum number of Fibre Channel credits that the Fibre Channel/fiber connectivity (FICON) link partner will allow the FCMR Fibre Channel/FICON transmitter to transmit. (The maximum number of frames the link partner can receive.)
fcStatsTxCredits	The number of Fibre Channel credits that the FCMR Fibre Channel/FICON transmitter is left with. This is the number of frames that the Fibre Channel/FICON transmitter has available to send.  <b>Note</b> The Tx credits increment whenever a credit is received from the link partner, and decrement when a frame is sent.
fcStatsZeroTxCredits	This is a count that increments when the Fibre Channel/FICON Tx credits go from a non-zero value to zero.
fibreStatsInvalidOrderedSets	Received ordered sets that are not recognized as part of the defined Fibre Channel control words.
fibreStatsEncodingDispErrors	Received control words that cannot be decoded due to invalid disparity.

**Table 20-2** *FC\_MR-4 Threshold Variables Fiber Channel/FICON Enhanced Mode (MIBs) (continued)*

Variable	Definition
fibresStatsRxFramesTooLong	Received oversize Fibre Channel frames > 2148 including CRC.
fibresStatsRxFramesBadCRC	Received Fibre Channel frames with bad CRC.
fibresStatsRxFrames	Received total Fibre Channel frames.
fibresStatsRxOctets	Received total Fibre Channel data bytes within a frame.
fibresStatsTxFramesBadCRC	Transmitted Fibre Channel frames with bad CRC.
fibresStatsTxFrames	Transmitted total Fibre Channel frames.
fibresStatsTxOctets	Transmitted total Fibre Channel data bytes within a frame.
fibresStatsLinkResets	Total number of link resets initiated by FCMR port when link recovery port setting is enabled.
gfpStatsRxSBitErrors	Received GFP frames with single bit errors in the core header (these errors are correctable).
gfpStatsRxMBitErrors	Received GFP frames with multiple bit errors in the core header (these errors are not correctable).
gfpStatsRxTypeInvalid	Received GFP frames with invalid type (these are discarded). For example, receiving GFP frames that contain Ethernet data when we expect Fibre Channel data.
gfpStatsRxSblkCRCErrors	Total number of superblock CRC errors with the receive transparent GFP frame. A transparent GFP frame has multiple superblocks which each contain Fibre Channel data.
8b10bInvalidOrderedSets	Total number of ordered sets not complaint to GE/FC (Gigabit Ethernet/Fibre Channel) standard
8b10bStatsEncodingDispErrors	Total number of code groups that violate GE/FC disparity errors

**Step 7** From the Alarm Type drop-down list, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

**Step 8** From the Sample Type drop-down list, choose either **Relative** or **Absolute**. Relative restricts the threshold to use the number of occurrences in the user-set sample period. Absolute sets the threshold to use the total number of occurrences, regardless of time period.

**Step 9** Type in an appropriate number of seconds for the Sample Period field.

**Step 10** Type in the appropriate number of occurrences for the Rising Threshold field.

For a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a rising threshold of 1000 collisions every 15 minutes and a problem causes 1001 collisions in 15 minutes, the excess occurrences trigger an alarm.

**Step 11** Enter the appropriate number of occurrences in the Falling Threshold field. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15-minute period, an event again

triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise, a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

- Step 12** Click **OK**.
- Step 13** Return to your originating procedure (NTP).
- 

## DLP-A358 Delete FC\_MR-4 RMON Alarm Thresholds

<b>Purpose</b>	This task deletes RMON threshold crossing alarms for FC_MR-4 ports.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A357 Create FC_MR-4 RMON Alarm Thresholds, page 20-40</a> <a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** In node view, double-click the FC\_MR-4 card where you want to delete the RMON alarm thresholds.
- Step 2** Click the **Provisioning > RMON Thresholds** tabs.
- Step 3** Click the RMON alarm threshold that you want to delete.
- Step 4** Click **Delete**. The Delete Threshold dialog box appears.
- Step 5** Click **Yes** to delete the threshold.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A359 Delete a Line DCC Termination

<b>Purpose</b>	This task deletes a SONET LDCC termination on the ONS 15454.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Caution

Deleting a DCC termination can cause you to lose visibility of nodes that do not have other DCCs or network connections to the CTC computer.

---

- Step 1** Click the **Provisioning > Comm Channel > LDCC** tabs.
-

- Step 2** Click the LDCC termination to be deleted and click **Delete**. The Delete LDCC Termination dialog box appears.
- Step 3** Click **Yes** in the confirmation dialog box. Confirm that the changes appear; if not, repeat the task.
- Step 4** Return to your originating procedure (NTP).

## DLP-A362 Create a Four-Fiber BLSR Using the BLSR Wizard

<b>Purpose</b>	This task creates a four-fiber BLSR at each BLSR-provisioned node using the CTC BLSR wizard. The BLSR wizard checks to see that each node is ready for BLSR provisioning, then provisions all the nodes at one time.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-A40 Provision BLSR Nodes, page 5-10</a> <a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

- d. Complete the “[NTP-A40 Provision BLSR Nodes](#)” procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.
- Step 6** In the network graphic, double-click a BLSR span line. If the span line is DCC connected to other BLSR cards that constitute a complete ring, the lines turn blue. If the lines do not form a complete ring, double-click span lines until a complete ring is formed. When the ring is DCC connected, go to [Step 7](#).
- Step 7** Click **Next**. In the Protect Port Selection section, choose the protect ports from the West Protect and East Protect columns.
- Step 8** Click **Finish**. If the BLSR window appears with the BLSR you created, go to [Step 9](#). If a “Cannot Create BLSR” or “Error While Creating BLSR” message appears:
- Click **OK**.
  - In the Create BLSR window, click **Excluded Nodes**. Review the information explaining why the BLSR could not be created, then click **OK**.
  - Depending on the problem, click **Back** to start over or click **Cancel** to cancel the operation.
  - Complete the “[NTP-A40 Provision BLSR Nodes](#)” procedure on page 5-10, making sure all steps are completed accurately, then start this procedure again.




---

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

---

- Step 9** Verify the following:
- On the network view graphic, a green span line appears between all BLSR nodes.
  - All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared. See the *Cisco ONS 15454 Troubleshooting Guide* for alarm troubleshooting.




---

**Note** The numbers in parentheses after the node name are the BLSR node IDs assigned by CTC. Every ONS 15454 in a BLSR is given a unique node ID, 0 through 31. To change it, complete the “[DLP-A326 Change a BLSR Node ID](#)” task on page 20-15.

---


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

## DLP-A363 Create a Four-Fiber BLSR Manually

<b>Purpose</b>	This task creates a four-fiber BLSR at each BLSR-provisioned node without using the BLSR wizard.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

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

- Step 2** Click **Create**.
- Step 3** In the Suggestion dialog box, click **OK**.
- Step 4** In the Create BLSR dialog box, set the BLSR properties:
- Ring Type—Choose four-fiber.
  - Ring Name—Assign a ring name. You must use the same ring name for each node in the BLSR. Any alphanumeric character string is permissible, and upper and lower case letters can be combined. Do not use the character string “All” in either upper or lower case letters; this is a TL1 keyword and will be rejected. Do not choose a name that is already assigned to another BLSR.
  - Node ID—Choose a Node ID from the drop-down list (0 through 31). The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.
  - Reversion time—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR must have the same reversion time setting.
  - West Line—Assign the west BLSR port for the node from the drop-down list.  
The east and west ports must match the fiber connections and DCC terminations set up in the [“NTP-A40 Provision BLSR Nodes” procedure on page 5-10](#).
  - East Line—Assign the east BLSR port for the node from the drop-down list.
  - Span Reversion—Set the amount of time that will pass before the traffic reverts to the original working path following a span reversion. The default is 5 minutes. Span reversion can be set to Never. If you set a reversion time, the times must be the same for both ends of the span. That is, if Node A’s west fiber is connected to Node B’s east port, the Node A west span reversion time must be the same as the Node B east span reversion time. To avoid reversion time mismatches, Cisco recommends that you use the same span reversion time throughout the ring.
  - West Protect—Assign the west BLSR port that will connect to the west protect fiber from the drop-down list.
  - East Protect—Assign the east BLSR port that will connect to the east protect fiber from the drop-down list.
- Step 5** Click **OK**.
-  **Note** Some or all of the following alarms will appear until all the BLSR nodes are provisioned: E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.
- Step 6** From the View menu, choose **Go to Other Node**.
- Step 7** In the Select Node dialog box, choose the next node that you want to add to the BLSR.
- Step 8** Repeat Steps 1 through 7 at each node that you want to add to the BLSR. When all nodes have been added, continue with [Step 9](#).
- Step 9** From the View menu, choose **Go to Network View**. After 10 to 15 seconds, verify the following:
- A green span line appears between all BLSR nodes.
  - All E-W-MISMATCH, RING-MISMATCH, APSCIMP, APSCDFLTK, and BLSROSYNC alarms are cleared.
- Step 10** Return to your originating procedure (NTP).

## DLP-A364 Reset the TCC2/TCC2P Card Using CTC

<b>Purpose</b>	This task resets the TCC2/TCC2P card and switches the node to the redundant card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A36 Install the TCC2/TCC2P Cards, page 17-38</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only



### 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



### Note

Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.



### Note

When a software reset is performed on an active TCC2/TCC2P, the AIC-I card goes through an initialization process and also resets. The AIC-I card reset is normal and happens each time an active TCC2/TCC2P card goes through a software-initiated reset.

- Step 1** Complete the [“DLP-A60 Log into CTC” task on page 17-60](#) at the node where you want to reset the TCC2/TCC2P card. If you are already logged in, continue with [Step 2](#).
- Step 2** In node view, right-click the TCC2/TCC2P card to reveal a shortcut menu.
- Step 3** Click **Reset Card**.
- Step 4** Click **Yes** when the confirmation dialog box appears.
- Step 5** Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.



### Note

For LED behavior during a TCC2/TCC2P reboot, see [Table 19-2 on page 19-33](#).

- Step 6** Confirm that the TCC2/TCC2P card LED is amber (standby).
- Step 7** Return to your originating procedure (NTP).

## DLP-A365 Initiate an Optical Protection Switch

<b>Purpose</b>	This procedure explains how to initiate a Manual or Force switch on an optical port.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>



<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

- 
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group you want to switch.
- Step 3** In the Selected Group area, select the card and port you want to switch.
- Step 4** Click **Manual** or **Force**.
- If you choose a Manual switch, the command will switch traffic only if the path has an error rate less than the signal degrade bit error rate threshold. A Force switch will switch traffic even if the path has SD or SF conditions; however, a Force switch will not override an SF on a 1+1 protection channel A Force switch has a higher priority than a Manual switch.
- Step 5** In the confirmation dialog box, click **Yes**.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A366 Initiate an Electrical Protection Switch

<b>Purpose</b>	This task explains how to initiate a traffic witch on an electrical card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher



**Note** A user-initiated switch overrides the revertive delay, that is, when you clear a switch you clear the timer and traffic reverts immediately.

---

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group you want to switch.
- Step 3** In the Selected Group area, select the card you want to switch.
- Step 4** Click **Switch**.
- Step 5** In the confirmation dialog box, click **Yes**.
- Step 6** Return to your originating procedure (NTP).
-

## DLP-A367 Create a Provisionable Patchcord

<b>Purpose</b>	This task creates a provisionable patchcord, which is a user-provisioned link that is advertised by OSPF throughout the network. Provisionable patchcords appear as dashed lines in CTC network view.  For the specific situations in which a patchcord is necessary, refer to the <i>Cisco ONS 15454 Reference Manual</i> .
<b>Tools/Equipment</b>	OC-N, transponder/muxponder, optical add/drop multiplexer, and multiplexer/demultiplexer cards.  For the card combinations that support patchcords, refer to the <i>Cisco ONS 15454 Reference Manual</i> .
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning and higher



**Note** To set up a provisionable patchcord between an optical port and a transponder/muxponder, optical add/drop multiplexer, or multiplexer/demultiplexer port, the optical port must have an SDCC/LDCC termination provisioned. If the port is the protection port in a 1+1 group, the working port must have an SDCC/LDCC termination provisioned. As needed, complete the “[DLP-A377 Provision Section DCC Terminations](#)” task on page 20-68 or the “[DLP-A378 Provision Line DCC Terminations](#)” task on page 20-70.



**Note** An optical port requires two patchcords when the remote end is Y-cable protected or is an optical add/drop multiplexer or multiplexer/demultiplexer port.



**Note** An optical patchcord must be provisioned between an OCH filter and an OCH trunk port.



**Note** If a provisionable patchcord is created manually by CTC, it automatically tunes the TXP or MXP trunk as an OCH filter if the TXP or MXP is set to autoprovisioning at the first tunable wavelength. On the TL1 interface, this feature is supported for internal patchcords only (OPR-LNK).

- 
- Step 1** In node view, click the **Provisioning > Comm Channels > Provisionable Patchcords** tabs. If you are in network view, click the **Provisioning > Provisionable Patchcords** tabs.
- Step 2** Click **Create**. The Provisionable Patchcord dialog box appears.
- Step 3** In the Origination Node area, complete the following:
- If you are in node view, the Origination Node defaults to the current node. If you are in network view, click the desired origination node from the drop-down list.
  - Type a patchcord identifier (0 through 32767) in the TX/RX ID field.
  - Click the desired origination slot/port from the list of available slots/ports.

- Step 4** In the Termination Node area, complete the following:
- Click the desired termination node from the drop-down list. If the remote node has not previously been discovered by CTC but is accessible by CTC, type the name of the remote node.
  - Type a patchcord identifier (0 through 32767) in the TX/RX ID field. The origination and termination IDs must be different if the patchcord is set up between two cards on the same node.
  - Click the desired termination slot/port from the list of available slots/ports. The origination port and the termination port must be different.
- Step 5** If you need to provision Tx and Rx separately for multiplexer/demultiplexer cards, check the **Separate Tx/Rx** check box. If not, continue with [Step 6](#). The origination and termination TX ports are already provisioned. Complete the following to provision the RX ports:
- In the Origination Node area, type a patchcord identifier (0 through 32767) in the RX ID field. The origination Tx and Rx and termination Tx and Rx IDs must be different.
  - Click the desired origination slot/port from the list of available slots/ports.
  - In the Termination Node area, type a patchcord identifier (0 through 32767) in the RX ID field. The origination Tx and Rx and termination Tx and Rx IDs must be different.
  - Click the desired termination slot/port from the list of available slots/ports.
- Step 6** Click **OK**.
- Step 7** If you provisioned a patchcord on a port in a 1+1 protection group, a dialog box appears to ask if you would like to provision the peer patchcord. Click **Yes**. Repeat Steps [3](#) through [6](#).
- Step 8** Return to your originating procedure (NTP).

## DLP-A368 Delete a Provisionable Patchcord

<b>Purpose</b>	This task deletes a provisionable patchcord.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning and higher



**Note** Deleting the last DCC termination on an optical port automatically deletes all provisionable patchcords provisioned on the port. If the port is in a 1+1 protection group, CTC automatically deletes the patchcord link on the protection port.

- Step 1** In node view, click the **Provisioning > Comm Channels > Provisionable Patchcords** tabs. If you are in network view, click the **Provisioning > Provisionable Patchcords** tabs.
- Step 2** Click the provisionable patchcord that you want to delete.
- Step 3** Click **Delete**.
- Step 4** In the confirmation dialog box, click **Yes**.

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

## DLP-A369 Provision an OC-N Circuit Route

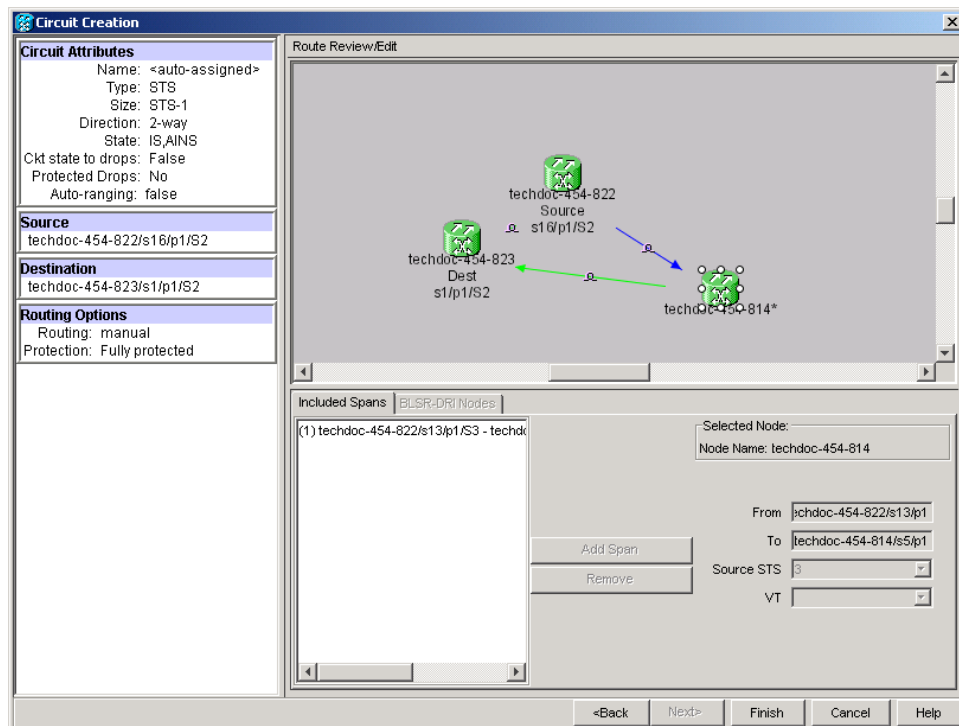
<b>Purpose</b>	This task provisions the circuit route for manually routed OC-N circuits.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
	The Circuit Creation wizard, Route Review/Edit area, must be open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Step 1** In the Circuit Creation wizard in the Route Review/Edit area, click the source node icon if it is not already selected.

**Step 2** Starting with a span on the source node, click the arrow of the span you want the circuit to travel. To reverse the direction of the arrow, click the arrow twice.

The arrow turns yellow. In the Selected Span area, the From and To fields provide span information. The source STS appears. [Figure 20-9](#) shows an example of a manually routed circuit.

**Figure 20-9** Manually Routing an OC-N Circuit



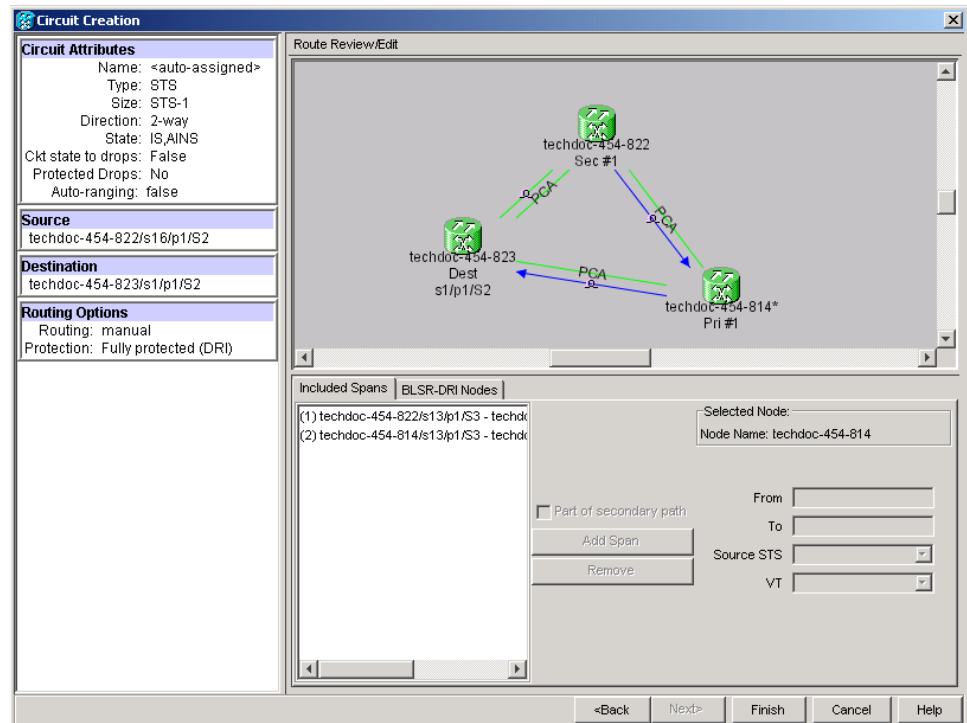
**Step 3** If you want to change the source STS, adjust the Source STS field; otherwise, continue with [Step 4](#).



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

- Step 4** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.
- Step 5** Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protected Path is checked in the Circuit Routing Preferences page, you must:
- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination.
  - Add one span for all BLSR or 1+1 portions of route from the source to the destination.
  - Add primary spans for BLSR-DRI from the source to the destination through the primary nodes, and then add spans through the secondary nodes as an alternative route. [Figure 20-10](#) shows an example of a manually routed BLSR DRI circuit. PCA spans can only be chosen as part of the secondary path.

**Figure 20-10** Manually Routing a BLSR DRI Circuit Route



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

## DLP-A371 Remove Pass-through Connections

<b>Purpose</b>	This task removes pass-through connections from a node deleted from a ring.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Log into the deleted node.
- Step 2** In the CTC Login dialog box, check the **Disable Network Discovery** check box.
- Step 3** Choose **None** from the Additional Nodes drop-down list.
- Step 4** Click the **Login** button.
- Step 5** Click the **Circuits** tab. All internode circuits are shown as PARTIAL.
- Step 6** Refer to the diagram or CTC print out you created in the “[NTP-A240 Remove a BLSR Node](#)” procedure on page 14-6 or the “[NTP-A294 Remove a Path Protection Node](#)” procedure on page 14-12. Find the circuits on the line cards of the removed node.
- Step 7** Click the **Filter** button.
- Step 8** Type the slot and port of a trunk card on the removed node.
- Step 9** Click **OK**.
- Step 10** In the Circuits tab, select all PARTIAL circuits that pass the filter and click the **Delete** button.




---

**Note** To select more than one circuit, press the **Shift** key and simultaneously click on all circuits to be deleted.

---

- Step 11** Repeat Steps 6 through 10 for the other trunk card.
- Step 12** Log out of CTC.
- Step 13** Return to your originating procedure (NTP).
-

## DLP-A372 Delete a Node from a Specified Login Node Group

<b>Purpose</b>	This task removes a node from a specified login node group. To remove a node from the current login node group, see the “ <a href="#">DLP-A339 Delete a Node from the Current Session or Login Group</a> ” task on page 20-30.
<b>Tools</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From the CTC Edit menu, choose **Preferences**.
- Step 2** In the Preferences dialog box, click the **Login Node Groups** tab.
- Step 3** Click the login node group tab containing the node you want to remove.
- Step 4** Click the node you want to remove, then click **Remove**.
- Step 5** Click **OK**.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-A373 Install a MiniBNC EIA

<b>Purpose</b>	This task installs a MiniBNC EIA. You can use MiniBNC EIAs with DS-1, DS-3, or DS3XM cards.
<b>Tools/Equipment</b>	#2 Phillips screwdriver Small slot-head screwdriver 6 perimeter screws, 6-32 x 0.375-inch Phillips head (P/N 48-0422-01) MiniBNC, A side (15454-xxxx) EIA panel and/or MiniBNC, B side (15454-xxx) EIA panel
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



### Caution

Always use an electrostatic discharge (ESD) wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



### Note

MiniBNC EIAs can only be installed on shelf assembly 15454-SA-HD. 15454-SA-HD shelf assemblies are differentiated from other shelf assemblies by the blue hexagon symbol, which indicates the available high-density slots, found under Slots 1 through 3 and 15 through 17.

**Note**

MiniBNC or UBIC EIAs are required when using high-density (48-port DS-3 and DS3XM-12) electrical cards.

- 
- Step 1** Locate the correct MiniBNC EIA for the side you want to install, and remove the MiniBNC EIA from the packaging.
- Step 2** Verify that none of the pins on the MiniBNC EIA are bent.
- Step 3** If present, remove the yellow connector protectors.
- Step 4** Line up the connectors on the card with the mating connectors on the backplane, making sure the keys on the back of the card line up properly with the backplane. Push the card with consistent pressure until the connectors fit together firmly.

**Caution**

Do not force the MiniBNC EIA onto the backplane if you feel strong resistance. Make sure that the MiniBNC EIA lines up properly on the backplane and that no backplane pins are bent.

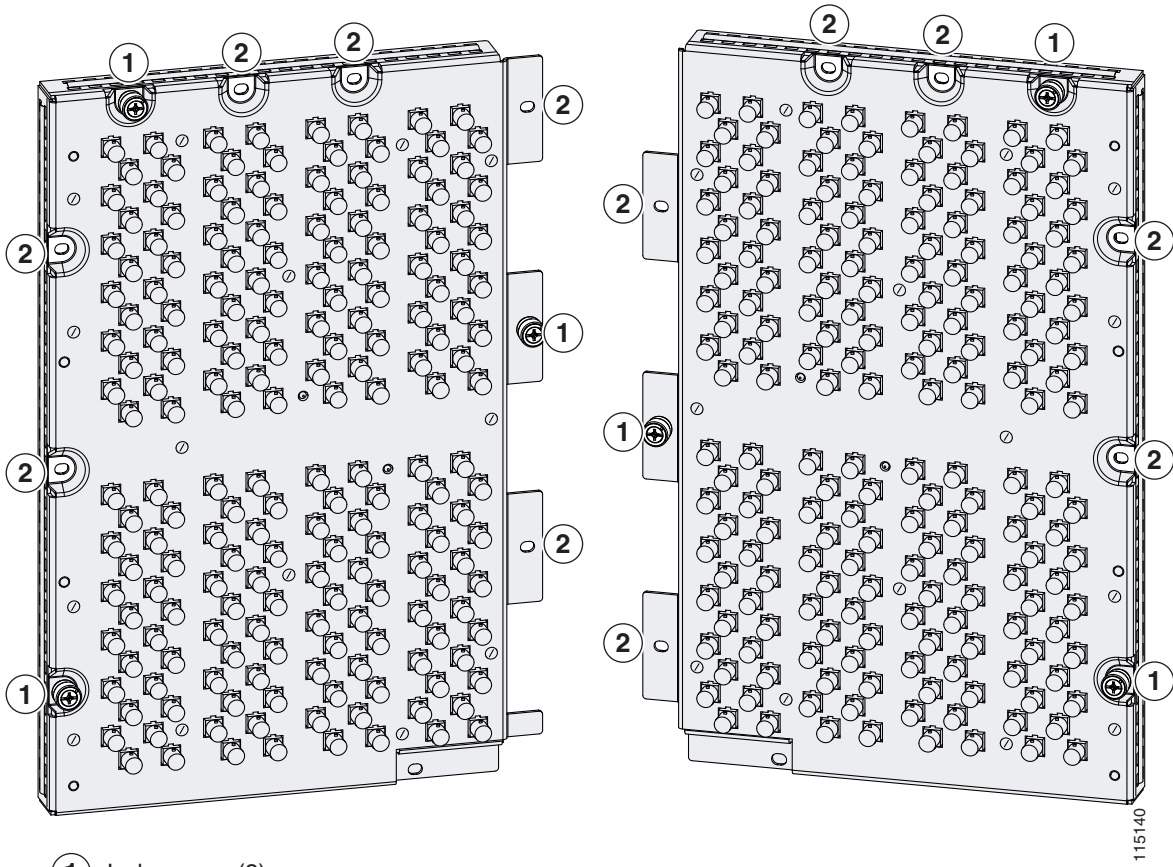
- Step 5** Locate the three jack screws on the MiniBNC ([Figure 20-11](#)). Starting with any thumbscrew, tighten it a few turns and move to the next one, turning each thumbscrew a few turns at a time until all three screws are hand tight ([Figure 20-12](#)).

**Caution**

Tightening the jack screws unevenly could cause damage to the MiniBNC connectors.

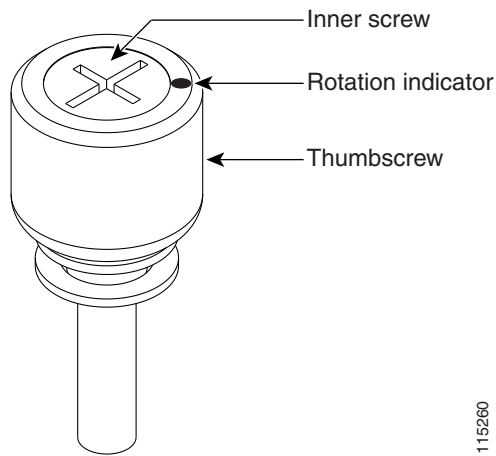


Figure 20-11 MiniBNC EIA Screw Locations



- 1 Jack screws (3)
- 2 Perimeter screws, 6-32 x 0.375-inch Phillips head (6)

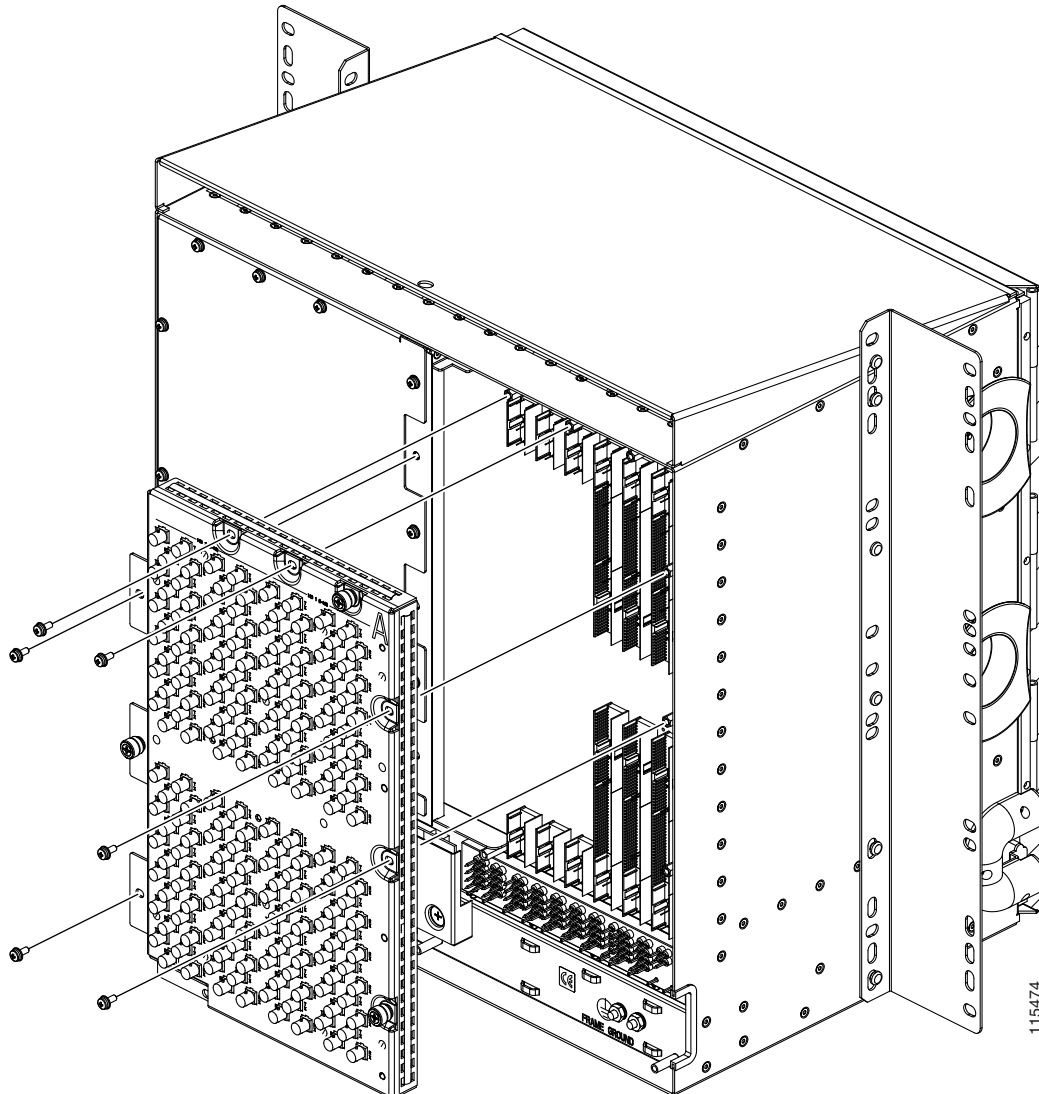
Figure 20-12 MiniBNC EIA Jack Screw



115260

- Step 6** Use a Phillips screwdriver to install the six perimeter screws and bracket screws (P/N 48-0422-01) at 8 to 10 lbf-inch (9.2 to 11.5 kgf-cm) to secure the cover panel to the backplane (Figure 20-11 on page 20-57). Install the alarm and timing panel cover and then insert and tighten the last perimeter screw. Figure 20-13 shows a MiniBNC EIA installation.

**Figure 20-13** Installing the MiniBNC EIA



- Step 7** Return to your originating procedure (NTP).

## DLP-A374 Change a Section DCC Termination

<b>Purpose</b>	This task modifies an SDCC. You can enable or disable Open Shortest Path First (OSPF) and enable or disable the foreign node setting.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Click the **Provisioning > Comm Channels > SDCC** tabs.
- Step 2** Click the SDCC that you want to change.
- Step 3** Click **Edit**.
- Step 4** In the SDCC Termination Editor dialog box, complete the following as necessary:
- **Disable OSPF on SDCC Link**—If checked, OSPF is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.
  - **Far End is Foreign**—Check this box to specify that the SDCC termination is a non-ONS node.
  - **Far End IP**—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.
- Step 5** Click **OK**.
- Step 6** Return to your origination procedure (NTP).
- 

## DLP-A375 Change a Line DCC Termination

<b>Purpose</b>	This task modifies an LDCC. You can enable or disable OSPF and enable or disable the foreign node setting.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Click the **Provisioning > Comm Channels > LDCC** tabs.
- Step 2** Click the LDCC that you want to change.
- Step 3** Click **Edit**.
- Step 4** In the LDCC Termination Editor dialog box, complete the following as necessary:
- **Disable OSPF on LDCC Link**—If checked, OSPF is disabled on the link. OSPF should be disabled only when the slot and port connect to third-party equipment that does not support OSPF.

- Far End is Foreign—Check this box to specify that the LDCC termination is a non-ONS node.
- Far end IP—If you checked the Far End is Foreign check box, type the IP address of the far-end node or leave the 0.0.0.0 default. An IP address of 0.0.0.0 means that any address can be used by the far end.

**Step 5** Click **OK**.

**Step 6** Return to your origination procedure (NTP).

## DLP-A376 Change Line and Threshold Settings for the DS1/E1-56 Cards

<b>Purpose</b>	This task changes the line and threshold settings for the DS1/E1-56 cards.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



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

**Step 1** Double-click the DS1/E1-56 card where you want to change the line or threshold settings.

**Step 2** Click the **Provisioning** tab.

**Step 3** Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **SONET Thresholds**, or **Cards** tab.



**Note** See [Chapter 9, “Manage Alarms”](#) for information about the Alarm Profiles tab.



**Note** If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

**Step 4** Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

**Step 5** Click **Apply**.

**Step 6** Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see [Table 20-3](#). For definitions of the line threshold settings, see [Table 20-4 on page 20-64](#). For definitions of the electrical path threshold settings, see [Table 20-5 on page 20-65](#). For definitions of the SONET threshold settings, see [Table 20-6 on page 20-65](#). For definitions of the card settings, see [Table 20-7 on page 20-66](#).

[Table 20-3](#) describes the values on the Provisioning > Line tabs for the DS1/E1-56 cards.

**Table 20-3** Line Options for the DS1/E1-56 Card

Parameter	Description	Options
Port	(Display only) Port number.	1 to 56
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the “DLP-A314 Assign a Name to a Port” task on page 20-8.
Admin State	Sets the port service state unless network conditions prevent the change.	<ul style="list-style-type: none"> <li>IS—Puts the port in-service. The port service state changes to IS-NR.</li> <li>IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS.</li> <li>OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD.</li> <li>OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT.</li> </ul> <p><b>Note</b> 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.</p>

Table 20-3 Line Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	<ul style="list-style-type: none"> <li>IS-NR—The port is fully operational and performing as provisioned.</li> <li>OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR.</li> <li>OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic.</li> <li>OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.</li> </ul>
SF BER	Sets the signal fail bit error rate.	<ul style="list-style-type: none"> <li>1E-3</li> <li>1E-4</li> <li>1E-5</li> </ul>
SD BER	Sets the signal degrade bit error rate.	<ul style="list-style-type: none"> <li>1E-5</li> <li>1E-6</li> <li>1E-7</li> <li>1E-8</li> <li>1E-9</li> </ul>
Line Type	Defines the line framing type.	<p>For DS1 mode</p> <ul style="list-style-type: none"> <li>Unframed - default</li> <li>J_ESF</li> <li>ESF</li> <li>D4</li> <li>Auto Frame</li> </ul> <p>For E1 mode</p> <ul style="list-style-type: none"> <li>Auto Frame</li> <li>Unframed</li> <li>E1_MF</li> <li>E1_CRCMF</li> </ul>

**Table 20-3** *Line Options for the DS1/E1-56 Card (continued)*

Parameter	Description	Options
Line Coding	Defines the transmission coding type that is used.	For DS1 mode <ul style="list-style-type: none"> <li>• B8ZS</li> <li>• AMI</li> </ul> For E1 mode <ul style="list-style-type: none"> <li>• HDB3</li> </ul>
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	<ul style="list-style-type: none"> <li>• 0 - 131 (default)</li> <li>• 132 - 262</li> <li>• 263 - 393</li> <li>• 394 - 524</li> <li>• 525 - 655</li> </ul>
AINS Soak	Sets the automatic in-service soak period.	Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically. Value ranges from 0 to 48 hours in 15-minute increments.
FDL Mode	Sets the mode for far-end loopbacks and far-end performance monitoring.	<ul style="list-style-type: none"> <li>• T1.403</li> <li>• Bidirectional fiber data link (BFDL)</li> </ul>
Send AIS-V for Ds1 AIS	Sends an Alarm Indication Signal VT (AIS-V) instead of DS1 AIS (from line side towards backplane/system side) when a line side trigger occurs.	<ul style="list-style-type: none"> <li>• Off (unchecked, default)</li> <li>• On (checked)</li> </ul>
Raise AIS for LOF	Sends AIS when a Loss of Frame (LOF) occurs.	<ul style="list-style-type: none"> <li>• Off (unchecked, default)</li> <li>• On (checked)</li> </ul>
ProvidesSync	The port is provisioned as a near-end timing reference.	<ul style="list-style-type: none"> <li>• Off (unchecked, default)</li> <li>• On (checked)</li> </ul>
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	<ul style="list-style-type: none"> <li>• Off (unchecked, default)</li> <li>• On (checked)</li> </ul>
SendDoNotUse	Sends a DUS (do not use) message on the S1 byte.	<ul style="list-style-type: none"> <li>• Off (unchecked, default)</li> <li>• On (checked)</li> </ul>
Enable Retiming	<p>When checked, retimes the transmit clock to the clock reference of the NE, removing the asynchronous relationship between electrical line and SONET transport time domains for the electrical path.</p> <p>When not checked, leaves the port as “through-timed,” which means that the transmit clock is extracted from the DS1/E1 data from the SONET payload coming from the backplane.</p>	<ul style="list-style-type: none"> <li>• Off (unchecked, default)</li> <li>• On (checked)</li> </ul>

**Table 20-3** Line Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Ds1 Mapping	Sets the mapping mode.	<ul style="list-style-type: none"> <li>Asynchronous: DS1 transport over SONET uses asynchronous mapping into VT1.5 (within a VT-structured STS-1 synchronous payload envelope [SPE]).</li> <li>Byte Synchronous: DS1 transport over SONET uses byte-synchronous mapping into VT1.5 (within a VT-structured STS-1 SPE).</li> <li>Japan Byte Synchronous: E1 transport over SONET uses asynchronous mapping into VT2 (within a VT-structured STS-1 SPE).</li> </ul>
Admin SSM	Overrides the synchronization status message (SSM) synchronization traceability unknown (STU) value. If the node does not receive an SSM signal, it defaults to STU.	<ul style="list-style-type: none"> <li>PRS—Primary Reference Source (Stratum 1)</li> <li>ST2—Stratum 2</li> <li>TNC—Transit node clock</li> <li>ST3E—Stratum 3E</li> <li>ST3—Stratum 3</li> <li>SMC—SONET minimum clock</li> <li>ST4—Stratum 4</li> <li>DUS—Do not use for timing synchronization</li> <li>RES—Reserved; quality level set by user</li> </ul>

Table 20-4 describes the values on the Provisioning > Line Thresholds tabs for the DS1/E1-56 card.

**Table 20-4** Line Threshold Options for DS1/E1-56 Card

Parameter	Description
Port	(Display only) Port number; 1 to 56.
CV	Coding violations. Available for Near End only.
ES	Errored seconds. Available for Near End only.
SES	Severely errored seconds. Available for Near End only.
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects. Available for Near End only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.



Table 20-5 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS1/E1-56 card.

**Table 20-5 Electrical Path Threshold Options for the DS1/E1-56 Card**

Parameter	Description
Port	(Display only) Port number; 1 to 56.
CV	Coding violations. Available for Near End and Far End.
ES	Errored seconds. Available for Near End and Far End.
SES	Severely errored seconds. Available for Near End and Far End.
SAS	Severely errored frame/alarm indication signal. Available for Near End only.
AISS	Alarm indication signal seconds. Available for Near End only.
UAS	Unavailable seconds. Available for Near End and Far End.
FC	Failure Count. Available for Near End only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-6 describes the values on the Provisioning > SONET Thresholds tabs for the DS1/E1-56 card.

**Table 20-6 SONET Threshold Options for the DS1/E1-56 Card**

Parameter	Description
Port	(Display only) DS-1 ports partitioned for STS Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations. Available for Near End and Far End, STS termination only.
ES	Errored seconds. Available for Near End and Far End, STS termination only.
FC	Failure count. Available for Near End and Far End, STS termination only.
SES	Severely errored seconds. Available for Near End and Far End, STS termination only.
UAS	Unavailable seconds. Available for Near End and Far End, STS termination only.
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-7 describes the values on the Provisioning > Card tabs for the DS1/E1-56 card.

**Table 20-7** Card Options for the DS1/E1-56 Card

Parameter	Description	Options
Transport Mode	Sets the encapsulation mode.	<ul style="list-style-type: none"> <li>SONET: (Default for DS1) Transports DS1s in VT1.5s and E1s in VT2s. In AU4 mode, only one STS-3c circuit shall be allowed.</li> <li>AU4: (Default for E1) Transports DS1s and E1s in a structured VC4 payload (STS-3c).</li> </ul> <p><b>Note</b> Switching from one transport mode to another is not allowed if a port is in a circuit, in service, or selected as a timing reference for the NE.</p>
Operating Mode	Sets the port usage. The restrictions on switching between these selections is based on existing circuits, ports being in service, and port usage as an NE reference source.	<ul style="list-style-type: none"> <li>All DS1: (Default) All 56 ports are used as DS1 ports. Ports 1 to 28 have retiming capability. Any of the 56 ports can be selected to provide timing reference to the NE.</li> <li>All E1: All 56 ports are used as E1 ports. Ports 1 to 21 have retiming capability. Any of the 56 ports can be selected to provide a timing reference to the NE.</li> </ul>

**Table 20-7** Card Options for the DS1/E1-56 Card (continued)

Parameter	Description	Options
Retiming Enabled	<p>When checked, retimes the transmit clock to the clock reference of the NE, removing the asynchronous relationship between electrical line and SONET transport time domains for the electrical path. If the Operating Mode is All DS1, Retiming Enabled is checked and cannot be changed.</p> <p>When not checked for E1 mode, leaves the port as “through-timed,” which means that the transmit clock is extracted from the DS1/E1 data from the SONET payload coming from the backplane.</p>	<ul style="list-style-type: none"> <li>• On (checked, default)</li> <li>• Off (unchecked)</li> </ul>
Port to VT Mapping	Selects the sequence in which DS1 ports are mapped into the VT1.5s within an STS-1. This setting applies to a group of DS1 ports associated with the same STS-1.	<ul style="list-style-type: none"> <li>• GR 253 interleaves the DS1 ports into the VT1.5 (DS1-14 compatible). In this mapping, sequential DS1 port numbers are mapped to interleave the 7 VT groups of VT1.5s. Interleaving by VT group essentially means that the DS1 ports follow the order of transmission of the VT1.5s, as indicated in Telcordia GR-253.</li> <li>• INDUSTRY maps sequential DS1 port numbers to fill each VT group in order. In this mapping, ports in sequential progression are packed into VTs filling an entire VT group before moving on to the next VT group.</li> </ul>



**Note** The threshold value appears after the circuit is created.

**Step 7** Return to your originating procedure (NTP).

## DLP-A377 Provision Section DCC Terminations

<b>Purpose</b>	This task creates the SONET data communications channel (DCC) terminations required for alarms, administration data, signal control information, and messages. In this task, you can also set up the node so that it has direct IP access to a far-end non-ONS node over the DCC network. In addition, this task can create an OSI subnetwork point of attachment on the DCC to allow the node to be networked with third-party NEs that are based on the OSI protocol stack.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Caution

If the ONS 15454 is configured as an OSI IS Level 1 or IS Level 1/Level 2 node and you are provisioning an OSI-only (LAP-D) SDCC to a third party NE, verify that the maximum area routing parameter on the vender NE is set to 3 before you start this task.



### Note

The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the “[DLP-A313 Create a DCC Tunnel](#)” task on page 20-7 to create a DCC tunnel.



### Note

When SDCC is provisioned, an LDCC termination is allowed on the same port, but is not recommended. Using SDCC and LDCC on the same port is only needed during a software upgrade if the software version does not support LDCC. You can provision SDCCs and LDCCs on different ports in the same node.

- Step 1** In node view, click the **Provisioning > Comm Channels > SDCC** tabs.
- Step 2** Click **Create**.
- Step 3** In the Create SDCC Terminations dialog box, click the ports where you want to create the SDCC termination. To select more than one port, press the Shift key or the Ctrl key.



### Note

SDCC refers to the Section DCC, which is used for ONS 15454 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15454) can be provisioned as DCC tunnels. See the “[DLP-A313 Create a DCC Tunnel](#)” task on page 20-7.

- Step 4** In the Port Admin State area, click **Set to IS** to put the port in service.
- Step 5** Verify that the Disable OSPF on SDCC Link is unchecked.

**Step 6** If the SDCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific IP address, see the “[DLP-A374 Change a Section DCC Termination](#)” task on page 20-59.

**Step 7** In the Layer 3 box, perform one of the following:

- Check the IP box only—if the SDCC is between the ONS 15454 and another ONS node and only ONS nodes reside on the network. The SDCC will use PPP (point-to-point protocol).
- Check the IP and OSI boxes—if the SDCC is between the ONS 15454 and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The SDCC will use PPP.
- Check OSI box only—if the SDCC is between an ONS node and a third party NE that uses the OSI protocol stack. The SDCC will use the LAP-D protocol.




---

**Note** If OSI is checked and IP is not checked (LAP-D), no network connections will appear in network view.

---

**Step 8** If you checked OSI, complete the following steps. If you checked IP only, continue with [Step 9](#).

- a. Click **Next**.
- b. Provision the following fields:
  - Router—Choose the OSI router.
  - ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
  - ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
  - IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
  - IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.
- c. If the OSI and IP boxes are checked, continue with [Step 9](#). If only the OSI is checked, click **Next** and provision the following fields:
  - Mode
    - AITS—(Default) Acknowledged Information Transfer Service. Does not exchange data until a logical connection between two LAP-D users is established. This service provides reliable data transfer, flow control, and error control mechanisms.
    - UITS—Unacknowledged Information Transfer Service. Transfers frames containing user data with no acknowledgement. The service does not guarantee that the data presented by one user will be delivered to another user, nor does it inform the user if the delivery attempt fails. It does not provide any flow control or error control mechanisms.
  - Role—Set to the opposite of the mode of the NE at the other end of the SDCC.
  - MTU—Maximum transmission unit. Sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets. The default is 512. You normally should not change it.

- T200—Sets the time between Set Asynchronous Balanced Mode (SABME) frame retransmissions. The default is 0.2 seconds. The range is 0.2 to 20 seconds.
- T203—Provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D “keep-alive” Receive Ready (RR) frames. The default is 10 seconds. The range is 4 to 120 seconds.

**Step 9** Click **Finish**.



**Note** EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms appear until you create all network DCC terminations and put the DCC termination OC-N ports in service.

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

## DLP-A378 Provision Line DCC Terminations

<b>Purpose</b>	This task creates the line data communications channel (LDCC) terminations required for alarms, administration data, signal control information, and messages. LDCCs are three-times larger than SDCCs. In this task, you can also set up the node so that it has direct IP access to a far-end non-ONS node over the DCC network. In addition, this task can create an OSI subnetwork point of attachment on the DCC to allow the node to be networked with third party NEs that are based on the OSI protocol stack.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the “[DLP-A313 Create a DCC Tunnel](#)” task on page 20-7 to create a DCC tunnel.



**Note** When LDCC is provisioned, an SDCC termination is allowed on the same port, but is not recommended. Using SDCC and LDCC on the same port is only needed during a software upgrade if the software version does not support LDCC. You can provision SDCCs and LDCCs on different ports in the same node.

**Step 1** In node view, click the **Provisioning > Comm Channels > LDCC** tabs.

**Step 2** Click **Create**.

**Step 3** In the Create LDCC Terminations dialog box, click the ports where you want to create the LDCC termination. To select more than one port, press the Shift key or the Ctrl key.



**Note** LDCC refers to the Line DCC, which is used for ONS 15454 DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15454) can be provisioned as DCC tunnels. See the [“DLP-A313 Create a DCC Tunnel” task on page 20-7](#).

**Step 4** In the Port Admin State area, click **Set to IS** to put the port in service.

**Step 5** Verify that the Disable OSPF on DCC Link check box is unchecked.

**Step 6** If the SDCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the [“DLP-A375 Change a Line DCC Termination” task on page 20-59](#).

**Step 7** In the Layer 3 box, perform one of the following:

- Check the IP box only—if the LDCC is between the ONS 15454 and another ONS node and only ONS nodes reside on the network. The LDCC will use PPP (point-to-point protocol).
- Check the IP and OSI boxes—if the LDCC is between the ONS 15454 and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The LDCC will use PPP.



**Note** OSI-only (LAP-D) is not available for LDCCs.

**Step 8** If you checked OSI, complete the following steps. If you checked IP only, continue with [Step 9](#).

- a. Click **Next**.
- b. Provision the following fields:
  - Router—Choose the OSI router
  - ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
  - ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
  - IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
  - IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

**Step 9** Click **Finish**.



**Note** EOC-L (Line DCC Termination Failure) and LOS (Loss of Signal) alarms appear until you create all network DCC terminations and put the DCC termination OC-N ports in service.

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

## DLP-A379 Change Line Transmission Settings for OC-N Cards

<b>Purpose</b>	This task changes the line transmission settings for OC-N cards.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher


**Note**

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

**Step 1** In node view, double-click the OC-N card where you want to change the line settings.

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


**Note**

If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

**Step 3** Modify the settings described in [Table 20-8](#) by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value or select or deselect a check box.

**Step 4** Click **Apply**.

**Table 20-8 OC-N Card Line Settings**

Parameter	Description	Options
Port	(Display only) Port number.	<ul style="list-style-type: none"> <li>1 (OC-12, OC-48, OC-192)</li> <li>1 – 4 (OC-3, OC12-4)</li> <li>1 – 8 (OC3-8)</li> <li>1 – 12 (MRC_12)</li> </ul>
Port Name	Provides the ability to assign the specified port a name.	User-defined. Name can be up to 32 alphanumeric/special characters. Blank by default. See the “ <a href="#">DLP-A314 Assign a Name to a Port</a> ” task on page 20-8.
Port Rate	(Display only; MRC-12 and OC192-XFP cards only) Displays the port rate set for the pluggable port module (PPM).	<ul style="list-style-type: none"> <li>OC-3</li> <li>OC-12</li> <li>OC-48</li> <li>OC-192 (OC192-XFP only)</li> </ul>



**Table 20-8** OC-N Card Line Settings (continued)

Parameter	Description	Options
SF BER	Sets the signal fail bit error rate.	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	Sets the signal degrade bit error rate.	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
BLSR Ext. Byte	Allows you to remap the extended byte that carries information governing BLSR protection switches. The K3 byte should not be changed unless specifically required to run an ONS BLSR through third-party equipment.	<ul style="list-style-type: none"> <li>• N/A</li> <li>• K3</li> </ul>
Provides Synch	(Display only) If checked, the card is provisioned as a network element timing reference.	—
SyncMsgIn	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte.	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Send <FF> DoNotUse	When checked, sends a special DUS (0xff) message on the S1 byte.	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Admin SSM In	If the node does not receive a sync status message (SSM) signal, it defaults to STU. Admin SSM In allows you to override the STU value.	<ul style="list-style-type: none"> <li>• PRS: Primary Reference Source (Stratum 1)</li> <li>• ST2: Stratum 2</li> <li>• TNC: Transit node clock</li> <li>• ST3E: Stratum 3E</li> <li>• ST3: Stratum 3</li> <li>• SMC: SONET minimum clock</li> <li>• ST4: Stratum 4</li> </ul>
PJSTSMon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port.	<ul style="list-style-type: none"> <li>• 0 - 3 (OC-3, per port)</li> <li>• 0 - 12 (OC-12)</li> <li>• 0 - 48 (OC-48)</li> <li>• 0 - 192 (OC-192)</li> </ul>

Table 20-8 OC-N Card Line Settings (continued)

Parameter	Description	Options
Admin State	Sets the port administrative service state unless network conditions prevent the change.	<ul style="list-style-type: none"> <li>IS—Puts the port in-service. The port service state changes to IS-NR.</li> <li>IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS.</li> <li>OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD.</li> <li>OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT.</li> </ul> <p><b>Note</b> 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.</p>
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	<ul style="list-style-type: none"> <li>IS-NR—The port is fully operational and performing as provisioned.</li> <li>OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR.</li> <li>OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic.</li> <li>OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.</li> </ul>
AINS Soak	Sets the automatic in-service soak period.	<ul style="list-style-type: none"> <li>Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically</li> <li>0 to 48 hours, 15-minute increments</li> </ul>

**Table 20-8** OC-N Card Line Settings (continued)

Parameter	Description	Options
Type	Defines the port as SONET or SDH. The Enable Sync Msg field and the Send Do Not Use field must be disabled before the port can be set to SDH.	<ul style="list-style-type: none"> <li>• Sonet</li> <li>• SDH</li> </ul>
ALS Mode	Sets the automatic laser shutdown function.	<ul style="list-style-type: none"> <li>• Disabled</li> <li>• Auto Restart</li> <li>• Manual Restart</li> <li>• Manual Restart for Test</li> </ul>
Reach	(Does not apply to all cards) Allows you to provision the reach value. You can also choose Auto Provision, which allows the system to automatically provision the reach from the PPM reach value on the hardware.	<p>The options that appear in the drop-down list depend on the card:</p> <ul style="list-style-type: none"> <li>• SR (short reach, up to 2 km distance)</li> <li>• SR-1 (up to 2 km distance)</li> <li>• IR-1 (intermediate reach, up to 15 km distance)</li> <li>• IR-2 (up to 40 km distance)</li> <li>• LR-1 (long reach, up to 40 km distance)</li> <li>• LR-2 (up to 80 km distance)</li> <li>• LR-3 (up to 80 km distance)</li> </ul>
Wavelength	(Does not apply to all cards) Allows you to provision the wavelength frequency.	<ul style="list-style-type: none"> <li>• First Tunable Wavelength</li> <li>• 1310 nm</li> <li>• 1550 nm</li> <li>• 1470 nm</li> <li>• 1490 nm</li> <li>• 1510 nm</li> <li>• 1530 nm</li> <li>• 1570 nm</li> <li>• 1590 nm</li> <li>• 1610 nm</li> </ul>

**Step 5** Click **Apply**.

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

## DLP-A380 Provision a Proxy Tunnel

<b>Purpose</b>	This task sets up a proxy tunnel to communicate with a non-ONS far-end node. Proxy tunnels are only necessary when the proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 proxy server tunnels.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> <a href="#">DLP-A377 Provision Section DCC Terminations, page 20-68</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only


**Note**

If the proxy server is disabled, you cannot set up a proxy tunnel.

- 
- Step 1** Click the **Provisioning > Network > Proxy** subtabs.
- Step 2** Click **Create**.
- Step 3** In the Create Tunnel dialog box, complete the following:
- Source Address—Type the IP address of the source node (32 bit length) or source subnet (any other length).
  - Length—Choose the length of the source subnet mask.
  - Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
  - Length—Choose the length of the destination subnet mask.
- Step 4** Click **OK**.
- Step 5** Return to your originating procedure (NTP).
-

## DLP-A381 Provision a Firewall Tunnel

<b>Purpose</b>	This task provisions destinations that will not be blocked by the firewall. Firewall tunnels are only necessary when the proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 firewall tunnels.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> <a href="#">DLP-A377 Provision Section DCC Terminations, page 20-68</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only



**Note** If the proxy server is configured as proxy-only or is disabled, you cannot set up a firewall tunnel.

- 
- Step 1** Click the **Provisioning > Network > Firewall** subtabs.
- Step 2** Click **Create**.
- Step 3** In the Create Tunnel dialog box, complete the following:
- **Source Address**—Type the IP address of the source node (32 bit length) or source subnet (any other length).
  - **Length**—Choose the length of the source subnet mask.
  - **Destination Address**—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
  - **Length**—Choose the length of the destination subnet mask.
- Step 4** Click **OK**.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-A382 Delete a Proxy Tunnel

<b>Purpose</b>	This task removes a proxy tunnel.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** Click the **Provisioning > Network > Proxy** subtabs.
- Step 2** Click the proxy tunnel that you want to delete.

- Step 3** Click **Delete**.
- Step 4** Return to your originating procedure (NTP).
- 

## DLP-A383 Delete a Firewall Tunnel

<b>Purpose</b>	This task removes a firewall tunnel.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

---

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

## DLP-A384 Add a Member to a VCAT Circuit

<b>Purpose</b>	<p>This task adds a member to one of the following VCAT circuits:</p> <ul style="list-style-type: none"> <li>• Software link capacity adjustment scheme (SW-LCAS) VCAT circuits on FC_MR-4 (enhanced mode) or CE-1000-4 cards</li> <li>• Non-LCAS and LCAS circuits on CE-100T-8 cards</li> </ul> <p>Adding a member to a VCAT circuit changes the size of the circuit. The new members use the VCAT member source, destination, and routing preference (common fiber or split routing) specified during the VCAT circuit creation procedure.</p>
<b>Tools/Equipment</b>	FC_MR-4 card (enhanced mode) or CE-Series card.
<b>Prerequisite Procedures</b>	<p><a href="#">DLP-A60 Log into CTC, page 17-60</a></p> <p>VCAT circuits must exist on the network. See the “<a href="#">NTP-A264 Create an Automatically Routed VCAT Circuit</a>” procedure on page 6-82 or the “<a href="#">NTP-A265 Create a Manually Routed VCAT Circuit</a>” procedure on page 6-87.</p>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Note**

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

**Note**

Adding a member to a non-LCAS VCAT circuit can be service affecting.

**Note**

Adding a member to SW-LCAS or LCAS VCAT circuits in the IS-NR, OOS-AU, AINS, or OOS-MA, MT service state could be service affecting. Cisco recommends using the OOS-MA, OOG service state when adding new members. You can put the member in the desired state after adding the member.

**Note**

You cannot add members to VCAT circuits that have a source or destination on an ML-Series or FC\_MR-4 (line rate mode) card.

- Step 1** In node or network view, click the **Circuits** tab.
- Step 2** Click the VCAT circuit that you want to edit, then click **Edit**.
- Step 3** Click the **Members** tab.
- Step 4** If you want to add a member to a non-LCAS VCAT circuit, complete the following substeps. If you want to add a member to a SW-LCAS or LCAS VCAT circuit, skip this step and continue with [Step 5](#).
- a. Select a member with a VCAT State of In Group. The In Group state indicates that a member has cross-connects in the IS-NR; OOS-MA, AINS; or OOS-MA, MT service states.
  - b. Click **Edit Member**.
  - c. In the Edit Member Circuit window, click the **State** tab.
  - d. View the cross-connect service state in the CRS Service State column. You will need this information when choosing the new member state.  
  
Cross-connects of all In Group non-LCAS members must be in the same service state. If all existing members are in the Out of Group VCAT state, which for non-LCAS members is the OOS-MA, DSBLD service state, you can choose any service state for the new member.
  - e. From the File menu, choose **Close** to return to the Edit Circuit window.
- Step 5** Click **Add Member**. The Add Member button is enabled if the VCAT circuit has sufficient bandwidth for an added member.
- Step 6** Define the number of members and member attributes:
- Number of members to add—Choose the number of members to add from the drop-down list. If the drop-down list does not show a number, the VCAT circuit has the maximum number of members allowed. The number of members allowed depends on the source and destination card and the existing size of the circuit. For more information on the number of members allowed for a card, refer to the “Circuits and Tunnels” chapter of the *Cisco ONS 15454 Reference Manual*.
  - New Circuit Size—(Display only) Automatically updates based on the number of added members.

- Create cross-connects only (TL1-like)—Check this box if you want to create one or more cross-connects to complete a signal path for TL1-generated circuits. If this box is checked, you cannot assign a name to the circuit.
- State—To add a non-LCAS member to a VCAT with In Group members, choose the state you viewed in [Step 4](#). To add a non-LCAS member to a VCAT with only Out of Group members, choose any of the following states. To add SW-LCAS or LCAS members, Cisco recommends the OOS,OOG state.
  - IS—Puts the member cross-connects in the IS-NR service state.
  - OOS,DSBLD—Puts the member cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
  - IS,AINS—Puts the member cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
  - OOS,MT—Puts the member cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete. See the [“DLP-A437 Change a VCAT Member Service State”](#) task on page 21-15.
  - OOS,OOG—(LCAS and SW-LCAS VCAT circuits only) Puts VCAT member cross-connects in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to put a member circuit out of the group and to stop sending traffic.

For additional information about circuit service states, refer to the “Circuits and Tunnels” chapter in the *Cisco ONS 15454 Reference Manual*.

**Step 7** Click **Next**.

**Step 8** To route the member(s) automatically, check **Route Automatically**. To manually route the members, leave Route Automatically unchecked.

**Step 9** If you want to set preferences for individual members, complete the following in the Member Preferences area. To set identical preferences for all added members, skip this step and continue with [Step 10](#).




---

**Note** Common fiber or split routing cannot be changed.

---

- Number—Choose a number (between 1 and 256) from the drop-down list to identify the member.
- Name—Type a unique name to identify the member. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available for each member when Fully Protected is chosen.

**Step 10** To set preferences for all members, complete the following in the Set Preferences for All Members area:



- Protection—Choose the member protection type:
  - Fully Protected—Routes the circuit on a protected path.
  - Unprotected—Creates an unprotected circuit.
  - PCA—Routes the member on a BLSR protection channel.
  - DRI—(Split routing only) Routes the member on a dual-ring interconnect circuit.
- Node-Diverse Path—(Split routing only) Available when Fully Protected is chosen.

**Step 11** If you left Route Automatically unchecked in [Step 8](#), click **Next** and complete the following substeps. If you checked Route Automatically in [Step 8](#), continue with [Step 12](#).

- a. In the Route Review/Edit area of the Circuit Creation wizard, choose the member to route from the Route Member number drop-down list.
- b. Click the source node icon if it is not already selected.
- c. Starting with a span on the source node, click the arrow of the span you want the member to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information.
- d. If you want to change the source, adjust the Source STS field; otherwise, continue with [Step e](#).
- e. Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.
- f. Repeat [Steps c](#) through [e](#) until the member is provisioned from the source to the destination node through all intermediary nodes. If you selected Fully Protect Path, you must:
  - Add two spans for all path protection ring or unprotected portions of the member route from the source to the destination
  - Add one span for all BLSR or 1+1 portions of route from the source to the destination
  - For members routed on path protection dual-ring interconnect topologies, provision the working and protect paths as well as spans between the DRI nodes
- g. Repeat [Steps a](#) through [f](#) for each member.

**Step 12** If you checked Route Automatically in [Step 8](#) and checked Review Route Before Creation, complete the following substeps. If not, continue with [Step 13](#).

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

**Step 13** Click **Finish**.



**Note** Adding members to a VCAT circuit may take several minutes depending on the complexity of the network and the number of members to be added.

**Step 14** If you added an LCAS member, complete the following substeps:

- a. Click the Alarms tab and see if the VCAT Group Degraded (VCG-DEG) alarm appears. If it does appear, refer to the *Cisco ONS 15454 Troubleshooting Guide* for the procedure to clear the alarm. If it does not, continue with [Step b](#).
- b. Complete the “[DLP-A437 Change a VCAT Member Service State](#)” task on [page 21-15](#) to put the member in the IS service state.

**Step 15** Return to your originating procedure (NTP).

---

## DLP-A385 Delete a Member from a VCAT Circuit

<b>Purpose</b>	This task removes a member from a VCAT circuit that was created with one of the following criteria: <ul style="list-style-type: none"> <li>SW-LCAS VCAT circuits on FC_MR-4 (enhanced mode) or CE-1000-4 cards</li> <li>Non-LCAS and LCAS circuits on CE-100T-8 cards</li> </ul> This task reduces the size of the VCAT circuit.
<b>Tools/Equipment</b>	FC_MR-4 card (enhanced mode) or CE-Series card.
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> VCAT circuits must exist on the network. See the “ <a href="#">NTP-A264 Create an Automatically Routed VCAT Circuit</a> ” procedure on page 6-82 or the “ <a href="#">NTP-A265 Create a Manually Routed VCAT Circuit</a> ” procedure on page 6-87. As necessary, complete the “ <a href="#">DLP-A437 Change a VCAT Member Service State</a> ” task on page 21-15 to change a SW-LCAS or LCAS member state to OOS-MA,OOG.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note**

Whenever circuits are deleted in a VCAT group, make sure that the TL1 parameter, txcount in a VCAT group is updated with the number of existing circuits. TL1 and CTC will now show the correct number of VCAT circuits present.

---



**Note**

Deleting a member from a non-LCAS circuit can be service-affecting.

---



**Note**

Deleting SW-LCAS or LCAS members in the IS-NR or OOS-AU,AINS service state can be service affecting. Cisco recommends putting the member to be deleted in the OOS-MA,OOG service state before deleting. Non-LCAS members do not support the OOS-MA,OOG service state.

---



**Note**

You cannot delete members that have a source or destination on an ML-Series or FC\_MR-4 (line rate mode) card.

---

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

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

**Step 3** Click the **Members** tab.

- Step 4** Select the member that you want to delete. To select multiple members, press **Ctrl** and click the desired members.
- Step 5** Click **Delete Member**.
- Step 6** In the confirmation dialog box, click **Yes**.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-A386 Install Electrical Cables on the UBIC-V EIAs

<b>Purpose</b>	This task installs DS-1 and DS-3/EC-1 cables on the UBIC-V EIAs.
<b>Tools/Equipment</b>	3/16-inch flat-head screwdriver DS-1 and DS-3/EC-1 cables, as needed: <ul style="list-style-type: none"> <li>• DS-1 cable, 150 feet: 15454-CADS1-V-SD</li> <li>• DS-1 cable, 250 feet: 15454-CADS1-V-ID</li> <li>• DS-1 cable, 655 feet: 15454-CADS1-V-LD</li> <li>• DS-3/EC-1 cable, 75 feet: 15454-CADS3-V-SD</li> <li>• DS-3/EC-1 cable, 225 feet: 15454-CADS3-V-ID</li> <li>• DS-3/EC-1 cable, 450 feet: 15454-CADS3-V-LD</li> </ul>
<b>Prerequisite Procedures</b>	<a href="#">DLP-A190 Install a UBIC-V EIA, page 18-58</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



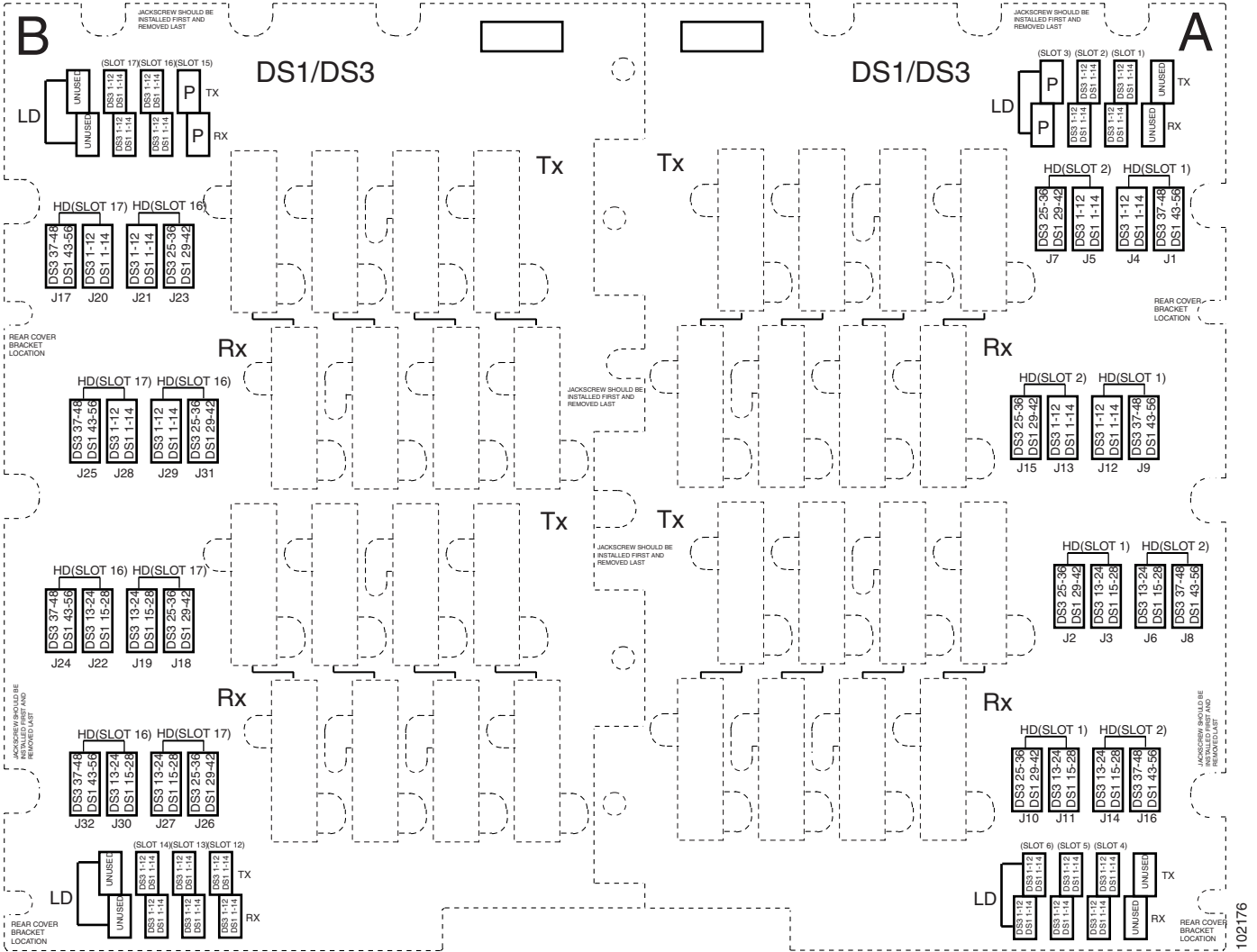
**Note** Cisco recommends that you plan for future slot utilization and fully cable all SCSI connectors you will use later.

---

- Step 1** Starting at the lowest row where you want to install cables on the UBIC-V place a cable connector over the desired connection point on the UBIC-V EIA.

[Figure 20-14](#) shows the UBIC-V slot designations.

Figure 20-14 UBIC-V Slot Designations



- Step 2** With the alignment slots of the cable connector aligned with the alignment standoffs of the UBIC connector, carefully install the cable.
- Step 3** Use the flat-head screwdriver to tighten the screw at the top left of the cable connector to 8 to 10 lbf-inch (9.2 to 11.5kgf-cm). Repeat this for the screw at the bottom right of the connector. Alternate between the two screws until both are tight.
- Step 4** Repeat Steps 1 through 3 for each cable you want to install, moving from the bottom row to the top row. If you are installing a cable near cables that are already installed, you might need to gently hold back the surrounding cables. Make sure you install cables in pairs, Tx and Rx, each time.

Figure 20-15 shows a UBIC-V with cables installed in all connectors.

Figure 20-15 Fully Cabled UBIC-V; Front- and Side-View

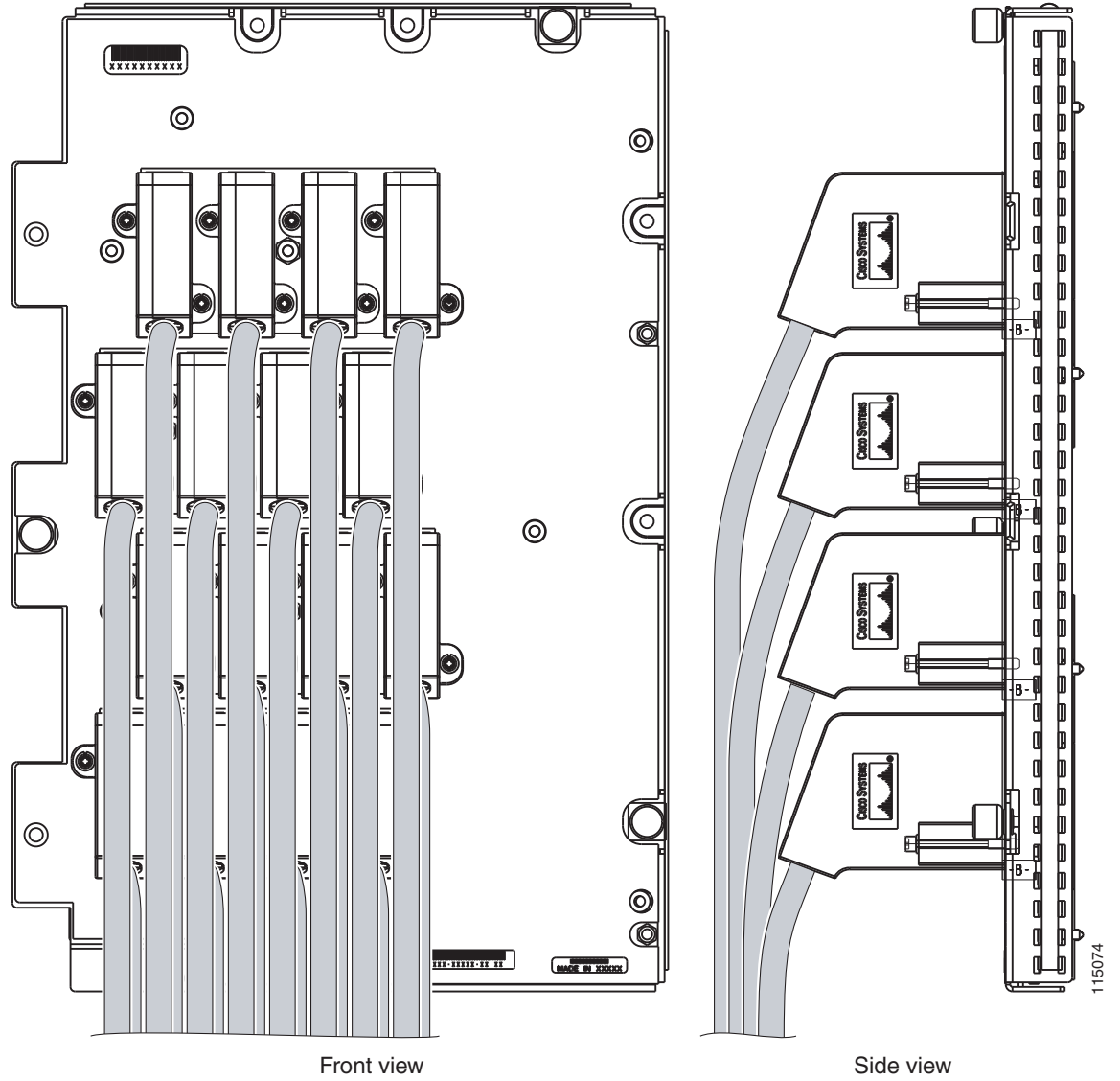
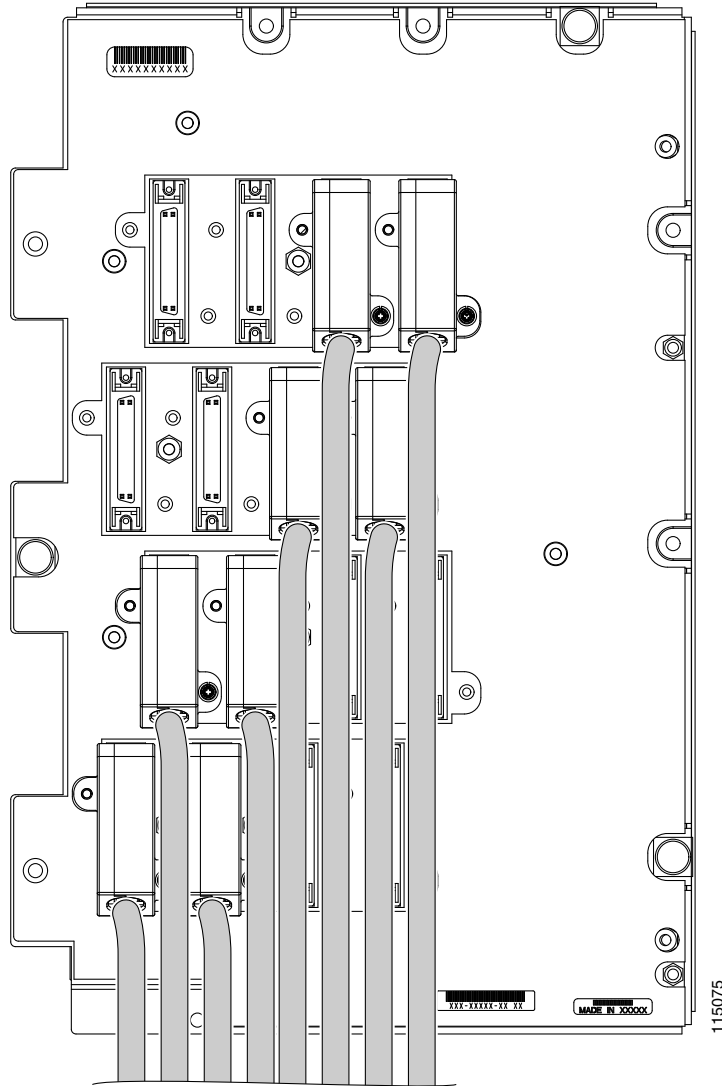


Figure 20-16 shows a partially populated UBIC-V.

Figure 20-16 Partially Cabled UBIC-V



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



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

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

## DLP-A387 Change Line and Threshold Settings for the DS3XM-12 Card

<b>Purpose</b>	This task changes the line and threshold settings for the DS3XM-12 card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher


**Note**

The DS3XM-12 (transmux) card can accept up to 12 channelized DS-3 signals and convert each signal to 28 VT1.5 signals for a total of 336 VT1.5 conversions. Conversely, the card can take 28 VT1.5s and multiplex them into a channeled C-bit or M13 framed DS-3 signal for each of the 12 DS-3 ports.


**Note**

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

**Step 1** In node view, double-click the DS3XM-12 card where you want to change the line or threshold settings.

**Step 2** Click the **Provisioning** tab.

**Step 3** Depending on the setting you need to modify, click the **Line**, **DS1**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** tab.


**Note**

See [Chapter 9, “Manage Alarms”](#) for information about the Alarm Profiles tab.


**Note**

If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

**Step 4** Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

**Step 5** Click **Apply**.

**Step 6** Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

**Step 7** For definitions of the line settings, see [Table 20-9](#). For definitions of the DS1 settings, see [Table 20-10 on page 20-89](#). For definitions of the line threshold settings, see [Table 20-11 on page 20-90](#). For definitions of the electrical path threshold settings, see [Table 20-12 on page 20-91](#). For definitions of the SONET threshold settings, see [Table 20-13 on page 20-91](#).

[Table 20-9](#) describes the values on the Provisioning > Line tabs for the DS3XM-12 cards.

**Table 20-9** Line Options for the DS3XM-12 Parameters

Parameter	Description	Options
Port #	(Display only) Port number.	1 to 36
Port Name	Displays the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default. See the “DLP-A314 Assign a Name to a Port” task on page 20-8.
SF BER	Sets the signal fail bit error rate.	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	<ul style="list-style-type: none"> <li>• IS-NR—The port is fully operational and performing as provisioned.</li> <li>• OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR.</li> <li>• OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic.</li> <li>• OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.</li> </ul>
AINS Soak	Sets the automatic in-service soak period.	<ul style="list-style-type: none"> <li>• Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically</li> <li>• 0 to 48 hours, 15-minute increments</li> </ul>
SD BER	Sets the signal degrade bit error rate.	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	Defines the line framing type.	<ul style="list-style-type: none"> <li>• M13 - default</li> <li>• C BIT</li> </ul>



**Table 20-9** Line Options for the DS3XM-12 Parameters (continued)

Parameter	Description	Options
Line Coding	Defines the DS-1 transmission coding type that is used.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	<ul style="list-style-type: none"> <li>0 - 225 (default)</li> <li>226 - 450</li> </ul>
Admin State	Sets the port service state unless network conditions prevent the change.	<ul style="list-style-type: none"> <li>IS—Puts the port in-service. The port service state changes to IS-NR.</li> <li>IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS.</li> <li>OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD.</li> <li>OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT.</li> </ul> <p><b>Note</b> 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.</p>

Table 20-10 describes the values on the Provisioning > DS1 tabs for the DS3XM-12 cards. Refer to the *Cisco ONS 15454 Reference Manual* for more information about “portless” protection on DS3XM-12 cards.

**Table 20-10** DS1 Options for the DS3XM-12 Card

Parameter	Description	Options
Port	(Display only) Displays the port number by DS-3 and corresponding DS-1.	DS-3: 1–35 DS-1: 1–28
Port Name	Displays the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default.  See the “DLP-A314 Assign a Name to a Port” task on page 20-8.

**Table 20-10** DS1 Options for the DS3XM-12 Card (continued)

Parameter	Description	Options
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	<ul style="list-style-type: none"> <li>IS-NR—The port is fully operational and performing as provisioned.</li> <li>OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR.</li> <li>OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic.</li> <li>OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.</li> </ul>
Line Type	Defines the line framing type.	<ul style="list-style-type: none"> <li>AUTO FRAME</li> <li>ESF - Extended Super Frame</li> <li>D4</li> <li>UNFRAMED</li> </ul>
FDL Mode	Defines the fiber data link (FDL) mode for the port.	<ul style="list-style-type: none"> <li>T1.403</li> <li>BFDL - Bidirectional FDL</li> </ul>

Table 20-11 lists the line thresholds options for DS3XM-12 cards.

**Table 20-11** Line Thresholds Options for the DS3XM-12 Card

Parameter	Description
Port	(Display only) Display the port number by DS-3 and corresponding DS-1. DS-3: 1 – 35 DS-1: 1 – 28
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
LOSS	Loss of signal seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-12 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3XM-12 cards.

**Table 20-12 Electrical Path Threshold Options for the DS3XM-12 Card**

Parameter	Description
Port	(Display only) Port number; 1 to 36
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
SAS	Severely errored frame/alarm indication signal
AISS	Alarm indication signal seconds
UAS	Unavailable seconds
FC	Failure Count (available for STS only)
CSS	Controlled Slip Seconds
ESA	Errored Seconds (Type A)
ESB	Errored Seconds (Type B)
SEFS	Severely Errored Frame Seconds
ESNE	Errored seconds (Near End)
ESFE	Errored seconds (Far End)
SESNE	Severely errored seconds (Near End)
SESFE	Severely errored seconds (Far End)
UASNE	Unavailable seconds (Near End)
UASFE	Unavailable seconds (Far End)
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-13 describes the values on the Provisioning > SONET Thresholds tabs for the DS3XM-12 cards.

**Table 20-13 SONET Threshold Options for the DS3XM-12 Card**

Parameter	Description
CV	Coding violations
ES	Errored seconds
FC	Failure count
SES	Severely errored seconds
UAS	Unavailable seconds

**Table 20-13** SONET Threshold Options for the DS3XM-12 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.



**Note** The threshold value appears after the circuit is created.

**Step 8** Return to your originating procedure (NTP).

## DLP-A388 Change Line and Threshold Settings for the DS3/EC1-48 Cards

<b>Purpose</b>	This task changes the line and threshold settings for the DS3/EC1-48 cards.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



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

**Step 1** Double-click the DS3/EC1-48 card where you want to change the line or threshold settings.

**Step 2** Click the **Provisioning** tab.

**Step 3** Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, or **SONET Thresholds** tab.



**Note** See [Chapter 9, “Manage Alarms”](#) for information about the Alarm Profiles tab.



**Note** If you want to modify a threshold setting, it might be necessary to click on the available directional, type, and interval (15 Min, 1 Day) radio buttons and then click **Refresh**. This will display the desired threshold setting.

**Step 4** Modify the settings found under these subtabs by clicking in the field you want to modify. In some fields you can choose an option from a drop-down list; in others you can type a value.

**Step 5** Click **Apply**.

**Step 6** Repeat Steps 3 through 5 for each subtab that has parameters you want to provision.

For definitions of the line settings, see [Table 20-14](#). For definitions of the line threshold settings, see [Table 20-15 on page 20-94](#). For definitions of the electrical path threshold settings, see [Table 20-16 on page 20-95](#). For definitions of the SONET threshold settings, see [Table 20-17 on page 20-95](#).

**Table 20-14** Line Options for the DS3/EC1-48 Card

Parameter	Description	Options
Port	(Display only) Port number.	1 to 48
Port Name	Sets the port name.	User-defined, up to 32 alphanumeric/special characters. Blank by default.  See the “ <a href="#">DLP-A314 Assign a Name to a Port</a> ” task on page 20-8.
Admin State	Sets the port service state unless network conditions prevent the change.	<ul style="list-style-type: none"> <li>IS—Puts the port in-service. The port service state changes to IS-NR.</li> <li>IS,AINS—Puts the port in automatic in-service. The port service state changes to OOS-AU,AINS.</li> <li>OOS,DSBLD—Removes the port from service and disables it. The port service state changes to OOS-MA,DSBLD.</li> <li>OOS,MT—Removes the port from service for maintenance. The port service state changes to OOS-MA,MT.</li> </ul> <p><b>Note</b> 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.</p>
Service State	(Display only) Identifies the autonomously generated state that gives the overall condition of the port. Service states appear in the format: Primary State-Primary State Qualifier, Secondary State.	<ul style="list-style-type: none"> <li>IS-NR—The port is fully operational and performing as provisioned.</li> <li>OOS-AU,AINS—The port is out-of-service, but traffic is carried. Alarm reporting is suppressed. The ONS node monitors the ports for an error-free signal. After an error-free signal is detected, the port stays in OOS-AU,AINS state for the duration of the soak period. After the soak period ends, the port service state changes to IS-NR.</li> <li>OOS-MA,DSBLD—The port is out-of-service and unable to carry traffic.</li> <li>OOS-MA,MT—The port is out-of-service for maintenance. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed.</li> </ul>

**Table 20-14** Line Options for the DS3/EC1-48 Card (continued)

Parameter	Description	Options
SF BER	Sets the signal fail bit error rate.	<ul style="list-style-type: none"> <li>• 1E-3</li> <li>• 1E-4</li> <li>• 1E-5</li> </ul>
SD BER	Sets the signal degrade bit error rate.	<ul style="list-style-type: none"> <li>• 1E-5</li> <li>• 1E-6</li> <li>• 1E-7</li> <li>• 1E-8</li> <li>• 1E-9</li> </ul>
Line Type	Defines the line framing type.	<ul style="list-style-type: none"> <li>• Unframed - default</li> <li>• M13</li> <li>• C BIT</li> <li>• Auto Provision Fmt</li> </ul>
Detected Line Type	(Display only) Displays the detected line type.	<ul style="list-style-type: none"> <li>• M13</li> <li>• C Bit</li> <li>• Unframed</li> <li>• Unknown</li> </ul>
Line Coding	Defines the DS-3 transmission coding type that is used.	B3ZS
Line Length	Defines the distance (in feet) from backplane connection to the next termination point.	<ul style="list-style-type: none"> <li>• 0 - 225 (default)</li> <li>• 226 - 450</li> </ul>
AINS Soak	Sets the automatic in-service soak period.	Duration of valid input signal, in hh.mm format, after which the card becomes in service (IS) automatically. Value is between 0 and 48 hours, in 15-minute increments.

[Table 20-15](#) describes the values on the Provisioning > Line Thresholds tabs for the DS3/EC1-48 card.

**Table 20-15** Line Threshold Options for DS3/EC1-48 Card

Parameter	Description
Port	(Display only) Port number; 1 to 48.
CV	Coding violations.
ES	Errored seconds.
SES	Severely errored seconds.
LOSS	Loss of signal seconds; number of one-second intervals containing one or more LOS defects.

**Table 20-15** Line Threshold Options for DS3/EC1-48 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-16 describes the values on the Provisioning > Elect Path Thresholds tabs for the DS3/EC1-48 card.

**Table 20-16** Electrical Path Threshold Options for the DS3/EC1-48 Card

Parameter	Description
Port	(Display only) Port number; 1 to 48.
CV	Coding violations
ES	Errored seconds
SES	Severely errored seconds
SAS	Severely errored frame/alarm indication signal
AISS	Alarm indication signal seconds
UAS	Unavailable seconds
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.

Table 20-17 describes the values on the Provisioning > SONET Thresholds tabs for the DS3/EC1-48 card.

**Table 20-17** SONET Threshold Options for the DS3/EC1-48 Card

Parameter	Description
Port	(Display only) DS-3 ports partitioned for STS Line 1, STS 1, Line 2, STS 1 Line 3, STS 1, Line 4 STS 1
CV	Coding violations. Available for Near and Far End, STS termination only.
ES	Errored seconds. Available for Near and Far End, STS termination only.
FC	Failure count. Available for Near and Far End, STS termination only.
SES	Severely errored seconds. Available for Near and Far End, STS termination only.
UAS	Unavailable seconds. Available for Near and Far End, STS termination only.

**Table 20-17** SONET Threshold Options for the DS3/EC1-48 Card (continued)

Parameter	Description
15 Min radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 15-minute intervals.
1 Day radio button	Clicking this radio button and then clicking Refresh will cause the threshold values on this tab to display for 1-day intervals.



**Note** The threshold value appears after the circuit is created.

**Step 7** Return to your originating procedure (NTP).

## DLP-A390 View Alarms

<b>Purpose</b>	Use this task to view current alarms on a card, node, or network.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Step 1** In the card, node, or network view, click the **Alarms** tab to view the alarms for that card, node, or network.

**Table 20-18** Alarm Column Descriptions

Column	Information Recorded
Num	Sequence number of the original alarm
Ref	Reference number of the original alarm
New	Indicates a new alarm; to change this status, click either the Synchronize button or the Delete Cleared Alarms button.
Date	Date and time of the alarm.
Node	The name of the node where the alarm is located. (In dense wavelength-division multiplexing [DWDM] configurations, one node can contain multiple shelves.) Visible in network view.
Object	TL1 access identifier (AID) for the alarmed object; for an STSmon or VTmon, this is the monitored STS or VT.
Eqpt Type	If an alarm is raised on a card, the card type in this slot.
Slot	If an alarm is raised on a card, the slot where the alarm occurred (appears only in network and node view).



**Table 20-18 Alarm Column Descriptions (continued)**

Column	Information Recorded
Port	If an alarm is raised on a card, the port where the alarm is raised; for STSTerm and VTTerm, the port refers to the upstream card it is partnered with.
Path Width	Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is described in the <i>Cisco ONS 15454 Troubleshooting Guide</i> .
Sev	Severity level: CR (Critical), MJ (Major), MN (minor), NA (Not Alarmed), NR (Not Reported).
ST	Status: R (raised), C (clear), or T (transient).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name; these names are alphabetically defined in the <i>Cisco ONS 15454 Troubleshooting Guide</i> .
Description	Description of the alarm.
Shelf	For DWDM configurations, the shelf where the alarmed object is located. Visible in network view.

Table 20-19 lists the color codes for alarm and condition severities.

**Table 20-19 Color Codes for Alarms and Condition Severities**

Color	Description
Red	Raised Critical (CR) alarm
Orange	Raised Major (MJ) alarm
Yellow	Raised Minor (MN) alarm
Magenta (pink)	Raised Not Alarmed (NA) condition
Blue	Raised Not Reported (NR) condition
White	Cleared (C) alarm or condition

- Step 2** If alarms are present, refer to the *Cisco ONS 15454 Troubleshooting Guide* for information and troubleshooting procedures.
- Step 3** Return to your originating procedure (NTP).

## DLP-A391 View CE-Series Ether Ports and POS Ports Statistics PM Parameters

<b>Purpose</b>	This task enables you to view CE-Series Ethernet port Statistics PM counts at selected time intervals to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Ether Ports > Statistics** (Figure 20-17) or **Performance > POS Ports > Statistics** tabs.

**Figure 20-17 Ether Ports Statistics on the CE-Series Card View Performance Window**

The screenshot shows the CTC Performance window with the following components labeled:

- Ether ports tab**: Located at the top left, showing a list of ports and their status (e.g., Down).
- Statistics tab**: The active tab, showing the performance monitoring table.
- Performance tab**: Located at the top center, currently inactive.
- Card view**: Located at the top right, showing a visual representation of the CE-Series card (CE-1U-VF-8) with port indicators.
- Refresh button**: A button at the bottom left of the table area.
- Auto-refresh drop-down list**: A dropdown menu at the bottom center, currently set to 'None'.
- Baseline button**: A button at the bottom right of the table area.
- Clear button**: A button at the bottom right of the table area.
- Help button**: A button at the bottom right of the table area.

- Step 3** Click **Refresh**. Performance monitoring statistics for each port on the card appear.
- Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the 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](#)” procedure on page 8-2.

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

## DLP-A392 View CE-Series Ether Ports and POS Ports Utilization PM Parameters

<b>Purpose</b>	This task enables you to view CE-Series Ethernet port Utilization PM counts at selected time intervals to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

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

**Step 2** Click the **Performance > Ether Ports > Utilization** ([Figure 20-18](#)) or **Performance > POS Ports > Utilization** tabs.

Figure 20-18 Ether Ports Utilization on the CE-Series Card View Performance Window

The screenshot shows the Performance Monitoring window for a CE-Series Card. The window is divided into four tabs: Ether ports tab, Utilization tab, Performance tab, and Card view. The Card view shows a card with 8 ports, each with Ether and POS status indicators. Below the card is a table with columns for Port, Prev, Prev-1, Prev-2, Prev-3, Prev-4, Prev-5, Prev-6, Prev-7, Prev-8, and Prev-9. The table is currently empty. At the bottom of the table are controls for Interval (15 min), Refresh, and Help buttons.

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

Interval: 15 min Refresh Help

Interval drop-down list Refresh button Help button

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

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

**Step 5** The transmit (Tx) and receive (Rx) bandwidth utilization values for the previous time intervals appear in the Prev-*n* columns. For PM parameter definitions, refer to the “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](#)” procedure on page 8-2.

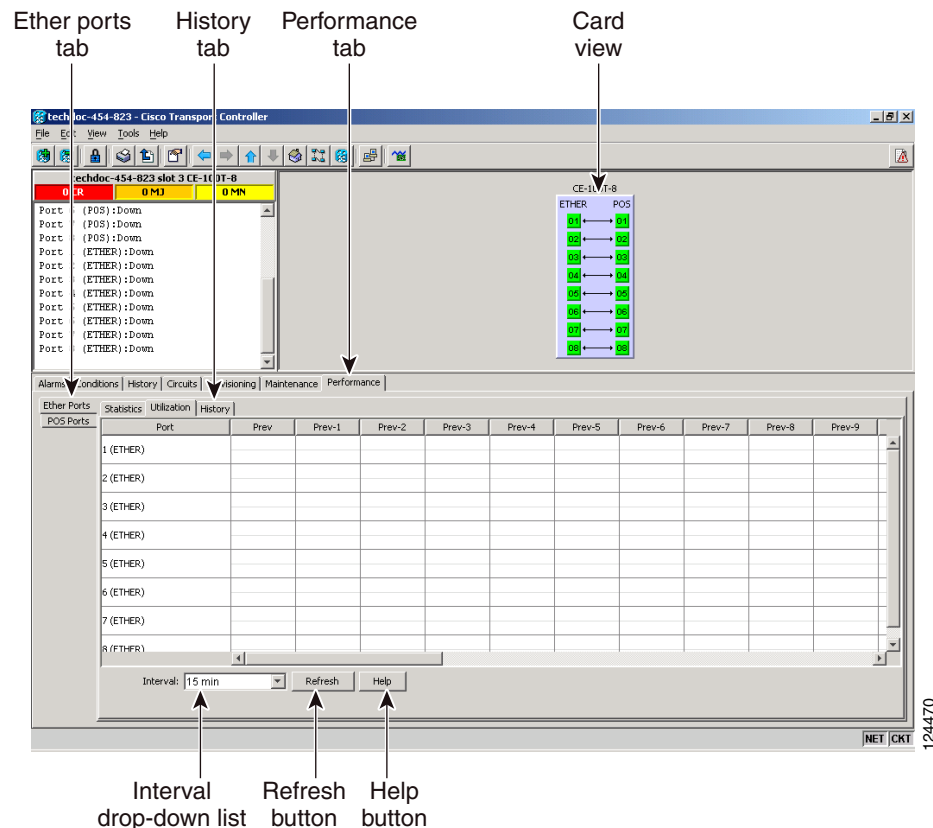
**Step 6** Return to your originating procedure (NTP).

## DLP-A393 View CE-Series Ether Ports and POS Ports History PM Parameters

<b>Purpose</b>	This task enables you to view CE-Series Ethernet port History PM counts at selected time intervals to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click the CE-Series Ethernet card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > Ether Ports > History** tabs ([Figure 20-19](#)) **Performance > POS Ports > History** tabs.

**Figure 20-19** Ether Ports History on the CE-Series Card View Performance Window



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

- Step 4** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Prev-n columns. For PM parameter definitions, refer to the “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” procedure on page 8-2.

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

## DLP-A394 View DS-N/SONET PM Parameters for the DS3XM-12 Card

<b>Purpose</b>	This task enables you to view DS-N/SONET PM parameters for near-end or far-end performance during selected time intervals on an DS3XM-12 electrical card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see <a href="#">Chapter 6, “Create Circuits and VT Tunnels”</a> and <a href="#">Chapter 10, “Change Card Settings.”</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click the DS3XM-12 electric card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > DSn/SONET PM** tabs to view the DS-N/SONET Performance parameters ([Figure 20-20](#)).

Figure 20-20 Viewing DS3XM-12 Card DSn/SONET Performance Monitoring Information

The screenshot shows the Cisco Transport Controller interface for a DS3XM-12 card. The interface is divided into three main sections: 'DSn/Sonet tab', 'Performance tab', and 'Card view'. The 'Performance tab' is active, displaying a table of performance monitoring parameters. The table has columns for 'Param', 'Curr', 'Prev', 'Prev-1', 'Prev-2', 'Prev-3', 'Prev-4', 'Prev-5', 'Prev-6', 'Prev-7', and 'Prev-8'. The 'Param' column lists various DS3XM-12 parameters such as DS3 CV-L, DS3 ES-L, DS3 LOSS-L, DS3 SES-L, DS3 AIS-S-P, DS3 CVP-P, DS3 ESP-P, DS3 SASP-P, DS3 SESP-P, DS3 UASP-P, DS3 CVCP-P, DS3 ESCP-P, DS3 SASCP-P, DS3 SESCP-P, and DS3 UASCP-P. The 'Curr' and 'Prev' columns are currently empty, and a 'No data available' message is displayed in the table area. Below the table, there are several controls: a 'Directions' section with radio buttons for 'Near End' and 'Far End'; an 'Intervals' section with radio buttons for '15 min' and '1 day'; a 'Signal-type drop-down list' showing 'DS3:1'; a 'Sub-signal STS drop-down list' showing 'DS1:1'; a 'Refresh' button; an 'Auto-refresh' drop-down list set to 'None'; a 'Baseline' button; a 'Clear...' button; and a 'Help' button. The interface also shows a 'NET' and 'CKT' indicator in the bottom right corner.



**Note** Different port and signal-type drop-down lists appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM cards list DS3, DS1, VT path, and STS path PM parameters as signal types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

- Step 3** In the signal type drop-down lists, choose the DS-3 port and the DS-1 port within the specified DS-3.
- Step 4** Click **Refresh**.
- Step 5** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the “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” procedure on page 8-2.

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

## DLP-A395 View BFDL PM Parameters for the DS3XM-12 Card

<b>Purpose</b>	This task enables you to view bidirectional fiber data link (BFDL) PM parameters for near-end or far-end performance during selected time intervals on an DS3XM-12 electrical card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	Before you monitor performance, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For more information, see <a href="#">Chapter 6, “Create Circuits and VT Tunnels”</a> and <a href="#">Chapter 10, “Change Card Settings.”</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click the DS3XM-12 card where you want to view PM counts. The card view appears.
- Step 2** Click the **Performance > BFDL PM** tabs to view the BFDL performance parameters ([Figure 20-21](#)).

**Figure 20-21 Viewing DS3XM-12 Card BFDL Performance Monitoring Information**

BFDL tab      Performance tab      Card view

The screenshot shows the Cisco Transport Controller interface. The top navigation bar includes 'Alarms', 'Conditions', 'History', 'Circuits', 'Provisioning', 'Maintenance', and 'Performance'. The 'Performance' tab is active, showing a table of BFDL PM parameters. The table has columns for 'Param', 'Curr', 'Curr 1Day', 'Prev', 'Prev-1', 'Prev-2', 'Prev-3', 'Prev-4', 'Prev-5', 'Prev-6', and 'Prev-7'. The parameters listed are CSS, ES, SES, BES, UAS, and LOFC. Below the table, there is a 'Request' drop-down list set to 'Enhanced UAS One Day', a 'DS3' drop-down list set to '1', a 'DS1' drop-down list, and a 'Refresh' button. The status bar at the bottom shows 'BFDL Far End Registers accessed: 9, 2004 5:00:36 PM IST' and the card identifier 'NET CKT 124469'.

Request drop-down list      Signal-type drop-down list      Sub-signal STS drop-down list      Refresh button





**Note** Different port and signal-type drop-down lists appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path) appear based on the card. For example, the DS3XM cards list DS3, DS1, VT path, and STS path PM parameters as signal types. This enables you to select both the DS-3 port and the DS-1 within the specified DS-3.

- Step 3** From the Request drop-down list choose one of the following:
- Enhanced ES One Day
  - Enhanced BES One day
  - Enhanced SES One Day
  - Enhanced UAS One Day
  - Enhanced CSS/LOFC One day
- Step 4** In the signal type drop-down lists, choose the DS-3 port and the DS-1 port within the specified DS-3.
- Step 5** Click **Refresh**.
- Step 6** View the PM parameter names that appear in the Param column. The PM parameter values appear in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15454 Reference Manual*.
- To refresh, reset, or clear PM counts, see the “[NTP-A253 Change the PM Display](#)” procedure on [page 8-2](#).
- Step 7** Return to your originating procedure (NTP).

## DLP-A397 Manually Route a Path Protection Circuit for a Topology Upgrade

<b>Purpose</b>	This task creates a manually routed USPR circuit during a conversion from an unprotected point-to-point or linear ADM system to a path protection.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC</a> , page 17-60 <a href="#">NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Automatically</a> , page 13-10
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** In the Circuit Routing Preferences area of the Unprotected to path protection page, uncheck **Route Automatically**.
- Step 2** Click **Next**. In the Route Review and Edit area, node icons appear for you to route the circuit. The circuit source node is selected. Green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.
- Step 3** Click **Finish**.

**Step 4** Return to your originating procedure (NTP).

---

## DLP-A398 Automatically Route a Path Protection Circuit for a Topology Upgrade

<b>Purpose</b>	This task creates an automatically routed USPR circuit during a conversion from an unprotected point-to-point or linear ADM system to a path protection.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-A60 Log into CTC, page 17-60</a> <a href="#">NTP-A342 Convert a Point-to-Point or Linear ADM to a Path Protection Automatically, page 13-10</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



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

---

**Step 1** In the Circuit Routing Preferences area of the Unprotected to path protection page, check **Route Automatically**.

**Step 2** Two options are available; choose either, both, or none based on your preferences.

- Review Route Before Creation—Check this check box if you want to review and edit the circuit route before the circuit is created.
- VT-DS3 Mapped Conversion—(STS circuits only) Check this check box to create a circuit using the portless transmultiplexing interface of the DS3XM-12 card.

**Step 3** Choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path protection portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates fiber-diverse paths for the path protection portion of the complete circuit path.
- Link Diversity Only—Specifies that only fiber-diverse primary and alternate paths for path protection portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

**Step 4** If you selected VT-DS3 Mapped Conversion in [Step 2](#), complete the following substeps; otherwise, continue with [Step 5](#):

- Click **Next**.
- In the Conversion Circuit Route Constraints area, complete the following:
  - Node—Choose a node with a DS3XM-12 card installed.
  - Slot—Choose the slot where a DS3XM-12 card is installed.

- DS3 Mapped STS—If applicable, choose **Circuit Dest** to indicate that the STS is the circuit destination, or **Circuit Source** to indicate that the STS is the circuit source.
- Step 5** If you selected Review Route Before Creation in [Step 2](#), complete the following substeps. If not, continue with [Step 6](#).
- a. Click **Next**.
  - b. Review the circuit route. To add or delete a circuit span, choose a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.
  - c. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information. If the circuit needs to be routed to a different path, see the [“NTP-A182 Create a Manually Routed DS-1 Circuit” procedure on page 6-12](#).
- Step 6** Click **Finish**.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-A399 Install a UBIC-H EIA

<b>Purpose</b>	This task installs a Universal Backplane Interface Connector—Horizontal (UBIC-H) EIA.
<b>Tools/Equipment</b>	#2 Phillips screwdriver Small slot-head screwdriver 6 perimeter screws, 6-32 x 0.375-inch Phillips head (P/N 48-0422-01) UBIC-H, A side (15454-EIA-UBICH-A) EIA panel and/ or UBIC-H, B side (15454-EIA-UBICH-B) EIA panel
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



### Caution

Always use an electrostatic discharge (ESD) wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



### Note

UBIC EIAs can only be installed on shelf assembly 15454-SA-HD. 15454-SA-HD shelf assemblies are differentiated from other shelf assemblies by the blue hexagon symbol, which indicates the available high-density slots, found under Slots 1 through 3 and 15 through 17.

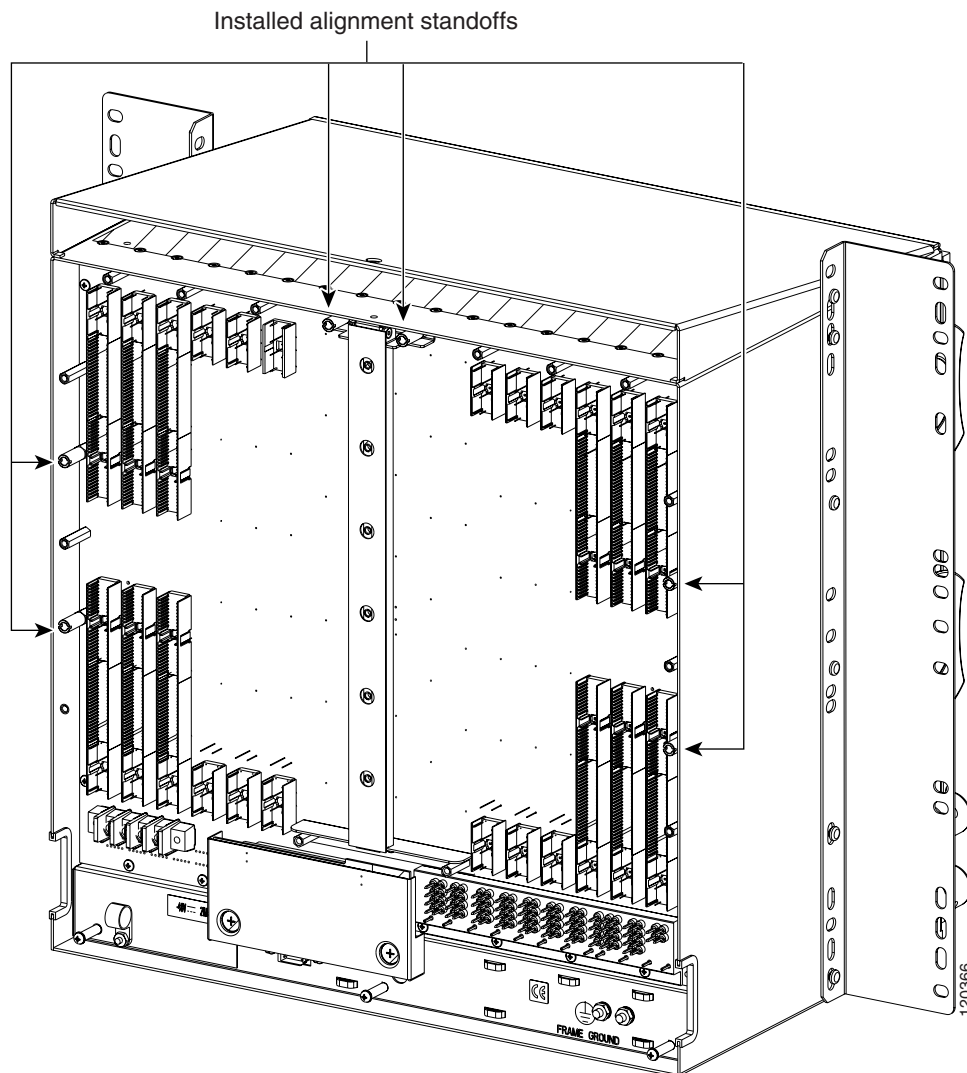


### Note

UBIC-V or UBIC-H EIAs are required when using high-density (48-port DS-3 and 12-port DS3XM) electrical cards.

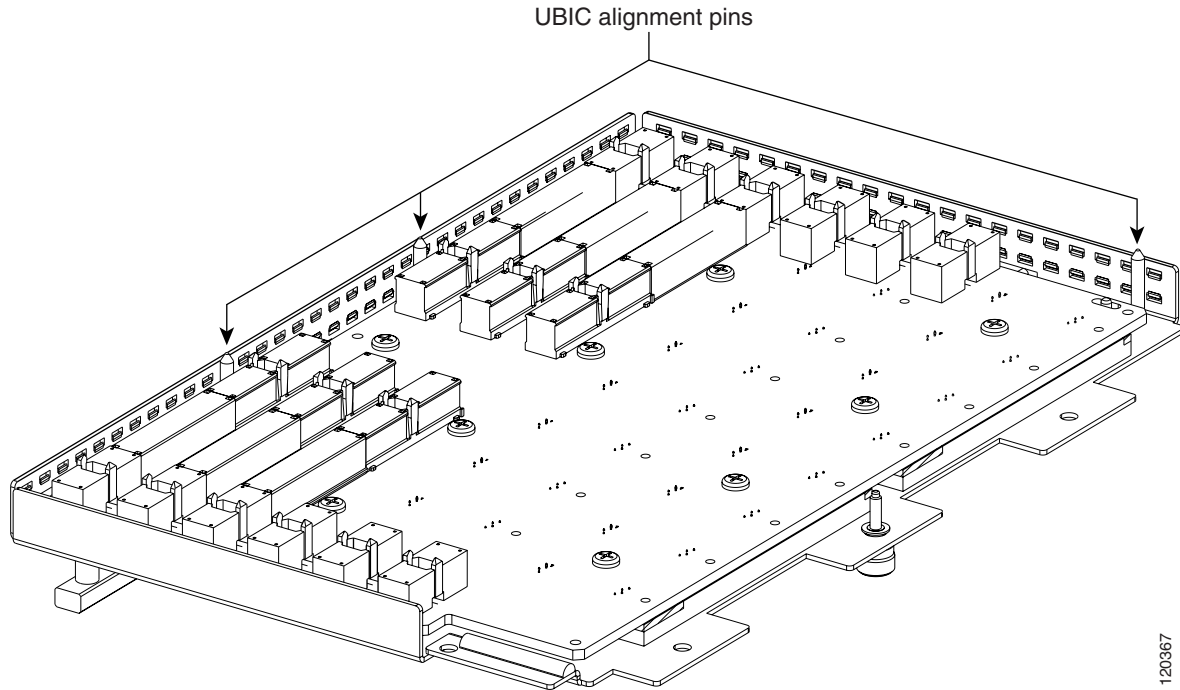
- Step 1** Locate the correct UBIC-H EIA for the side you want to install and remove the UBIC-H EIA from the packaging.
- Step 2** Verify that none of the pins on the UBIC-H EIA are bent.
- Step 3** If present, remove the yellow connector protectors.
- Step 4** If screws are present in the alignment standoff holes, use a Phillips screwdriver to remove them.
- Step 5** Use a flathead screwdriver or 5/16-inch deep socket wrench to tighten the standoffs at 8 to 10 inch pound-force (lbf-in) (9.2 to 11.5 centimeter kilogram-force[kgf-cm]). [Figure 20-22](#) shows the alignment standoffs installed on the shelf.

**Figure 20-22** Installed Alignment Standoffs



- Step 6** Line up the alignment pins on the UBIC-H EIA ([Figure 20-23](#)) with the alignment standoffs on the shelf and push the UBIC-H EIA with consistent pressure until the pins and standoffs fit together firmly.

Figure 20-23 UBIC-H Alignment Pins

**Caution**

Do not force the UBIC-H EIA onto the shelf if you feel strong resistance.

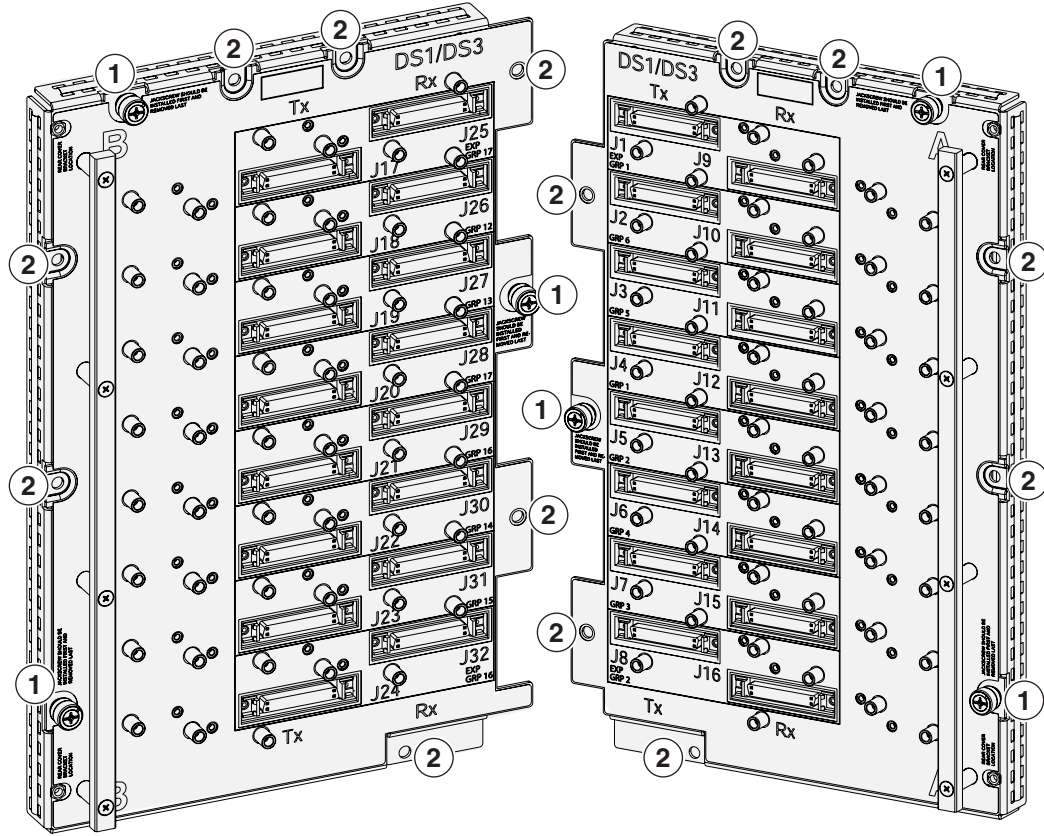
**Step 7**

Locate the three jack screws on the UBIC-H (Figure 20-24). Starting with any jack screw, tighten the thumb screw a few turns and move to the next one, turning each thumb screw a few turns at a time until all three screws are hand tight (Figure 20-25).

**Caution**

Tightening the jack screws unevenly could cause damage to the UBIC-H connectors.

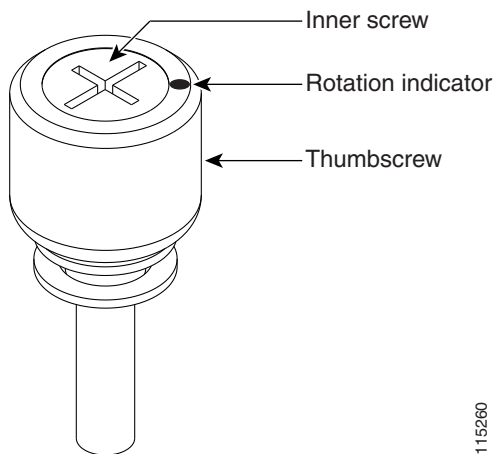
Figure 20-24 UBIC-H EIA Screw Locations



- 1 Jack screws (3)
- 2 Perimeter screws, 6-32 x 0.375-inch Phillips head (7)

120075

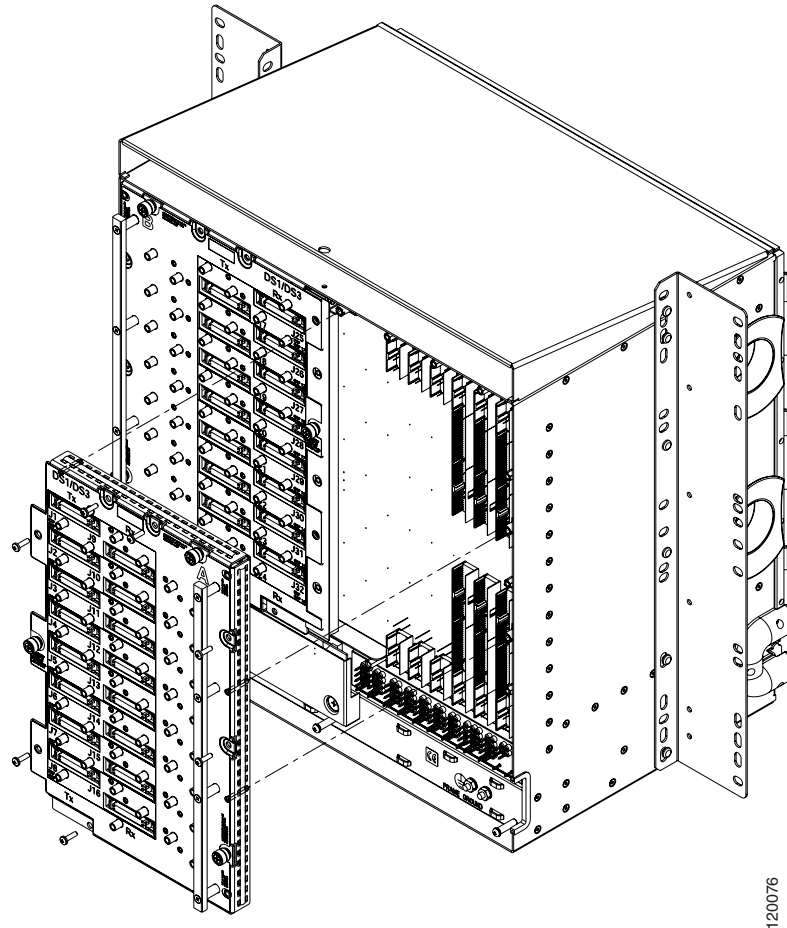
Figure 20-25 UBIC-H EIA Jack Screw



115260

- Step 8** Use a Phillips screwdriver to install five of the six perimeter screws (Figure 20-26), leaving the lower perimeter screw out, and torque to 8 to 10 lbf-inch (9.2 to 11.5 kgf-cm) to secure the cover panel to the backplane.

**Figure 20-26** Installing the UBIC-H EIA



- Step 9** Reinstall the lower backplane cover using a Phillips screwdriver, inserting five screws and tightening until seated.
- Step 10** Return to your originating procedure (NTP).

