CHAPTER 18

DLPs C100 to C199

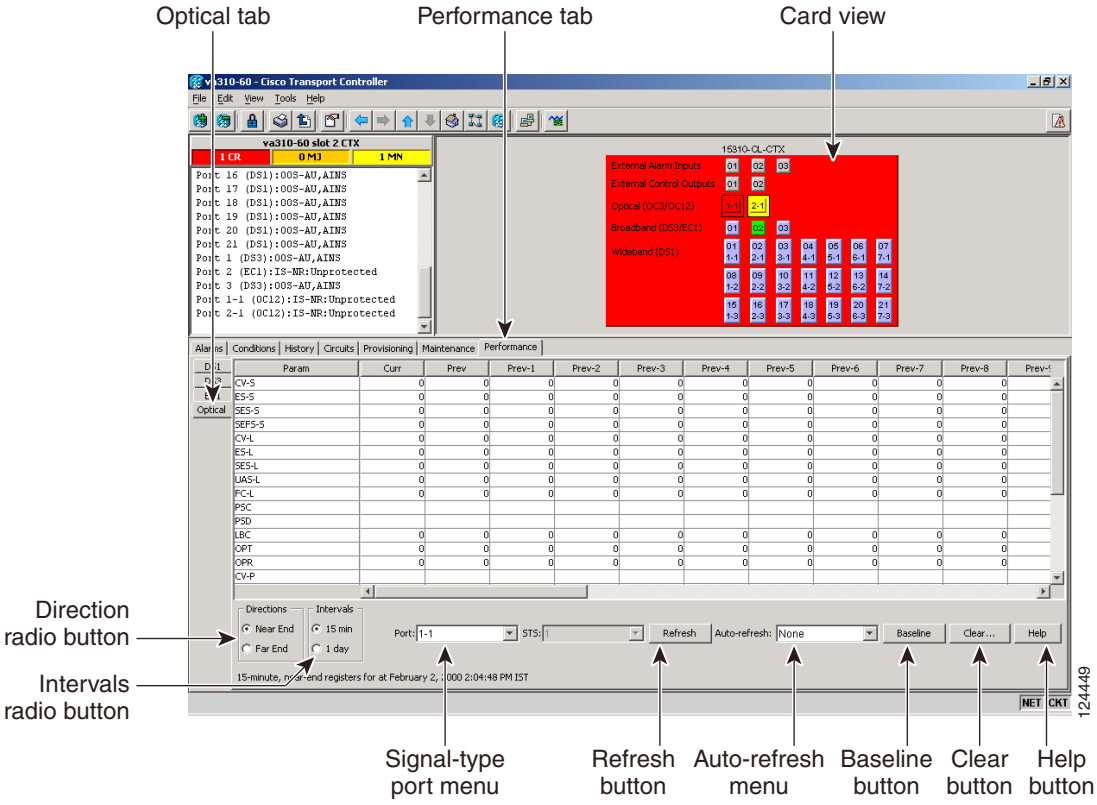
DLP-C100 View Optical OC-N PM Parameters

Purpose	This task enables you to view PM counts on an optical (OC-N) port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click the 15310-CL-CTX or CTX2500 card. The card view appears.

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

Figure 18-1 Viewing Optical Performance Monitoring Information



Step 3 The PM parameter names appear on the left side of the window in the Param column. The PM values appear on the right side of the window in the Curr (current) and Prev-*n* (previous) columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 Return to your originating procedure (NTP).

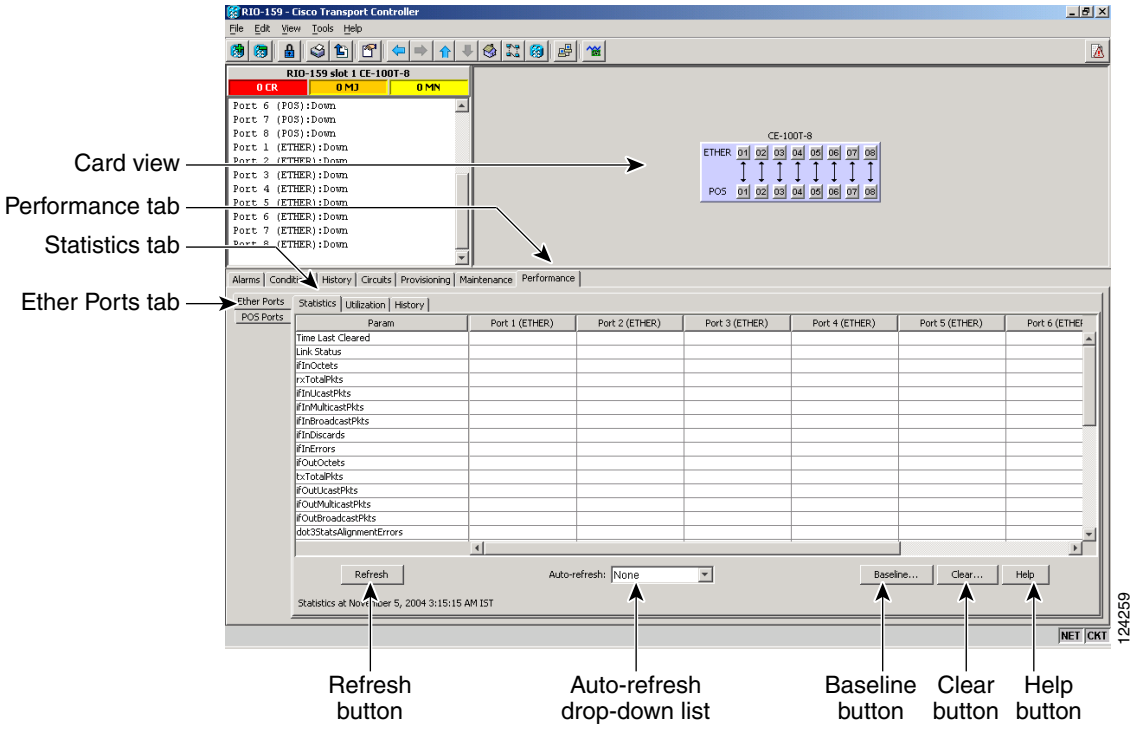
DLP-C101 View Ether Ports and POS Ports Statistics PM Parameters

Purpose	This task enables you to view current statistical PM counts on a CE-Series or ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports > Statistics** tabs or the **Performance > POS Ports > Statistics** tabs (Figure 18-2).

Figure 18-2 Statistics Window on the CE, ML Card View Performance Tab



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

The PM parameter names appear on the left side of the window in the Param column. The parameter numbers appear on the right side of the window in the Port # columns. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 View the Port # columns to see the current PM statistics for each port.

Step 5 Return to your originating procedure (NTP).

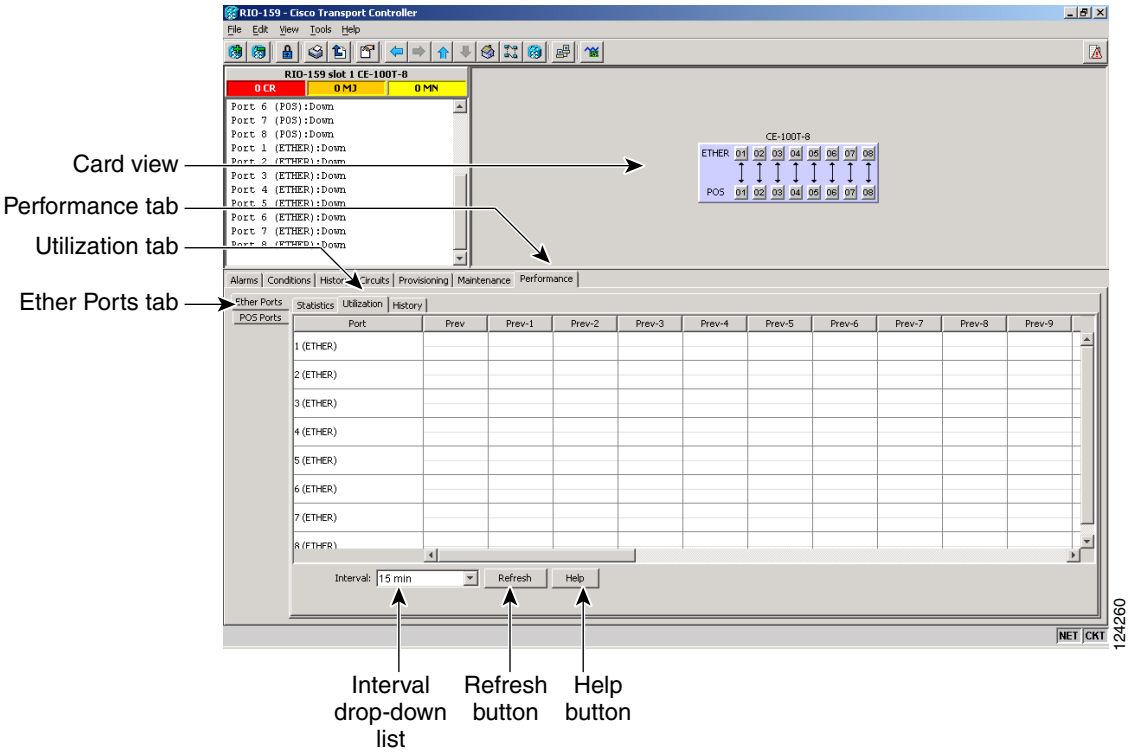
DLP-C102 View Ether Ports and POS Ports Utilization PM Parameters

Purpose	This task enables you to view line utilization PM counts on a CE-Series or an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports > Utilization** tabs or the **Performance > POS Ports > Utilization** tabs (Figure 18-3).

Figure 18-3 Utilization Window on the Card View Performance Tab for CE-Series and ML-Series Cards



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 View the Prev-*n* columns to find Tx and Rx bandwidth utilization values for the previous time intervals.

Step 6 Return to your originating procedure (NTP).

DLP-C103 Refresh Ethernet PM Counts at a Different Time Interval

Purpose	This task changes the window view to display specified PM counts in time intervals depending on the interval option selected.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports** tabs or the **Performance > POS Ports** tabs.

Step 3 Click the **Utilization** tab or the **History** tab.

Step 4 From the Interval drop-down list, choose one of four options:

- **1 min**: This option displays the specified PM counts in one-minute time intervals.
- **15 min**: This option displays the specified PM counts in fifteen-minute time intervals.
- **1 hour**: This option displays the specified PM counts in one-hour time intervals.
- **1 day**: This option displays the specified PM counts in one-day (24-hour) time intervals.

Step 5 Click **Refresh**. The PM counts refresh with values based on the chosen time interval.

Step 6 Return to your originating procedure (NTP).

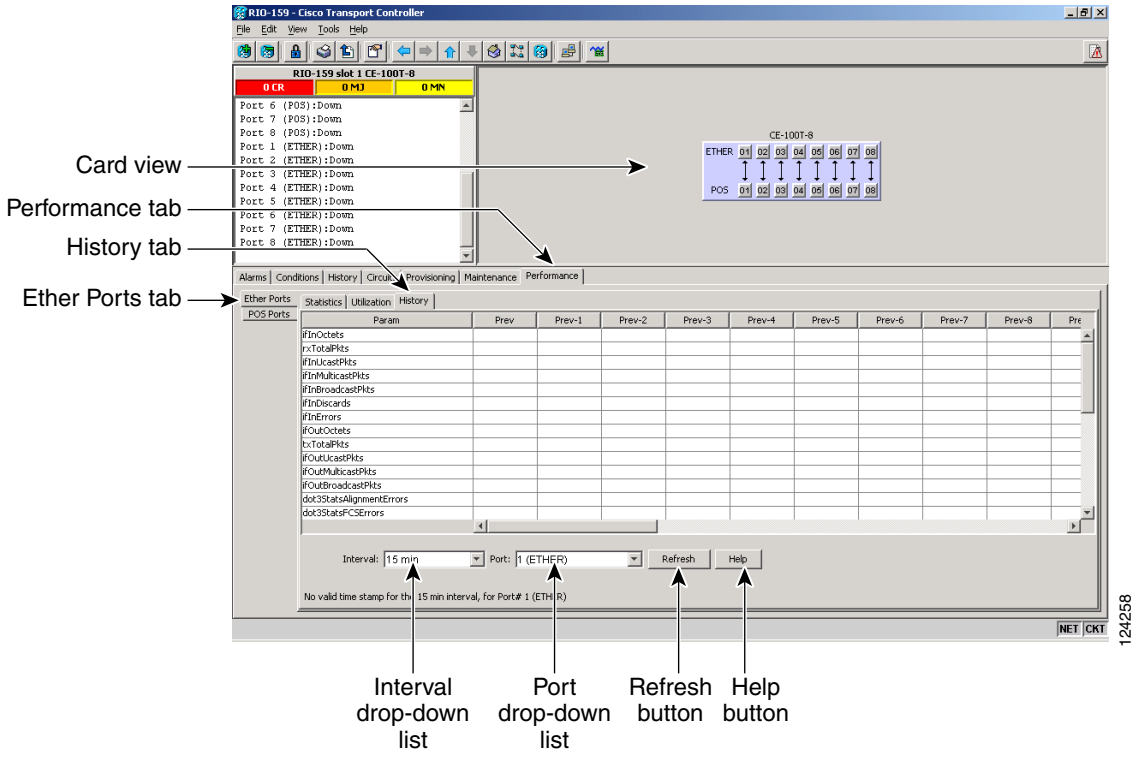
DLP-C104 View Ether Ports and POS Ports History PM Parameters

Purpose	This task enables you to view historical PM counts at selected time intervals on a CE-Series or an ML-Series Ethernet card and port to detect possible performance problems.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 In node view, double-click a CE-Series or an ML-Series Ethernet card. The card view appears.

Step 2 Click the **Performance > Ether Ports > History** tabs or the **Performance > POS Ports > History** tabs (Figure 18-4).

Figure 18-4 History Window on the Card View Performance Tab



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

The PM parameter names appear on the left side of the window in the Param column. The parameter numbers appear on the right side of the window in the Port # columns. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 4 View the Port # columns to see the current PM statistics for each port.

Step 5 Return to your originating procedure (NTP)

DLP-C105 Create Ethernet RMON Alarm Thresholds

Purpose	This task sets up RMON to allow network management systems to monitor Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The CE-100T-8 uses the ONG RMON. The ONG RMON contains the statistics, history, alarms, and events MIB groups from the standard RMON MIB.

Note ONG RMON is recommended for the ML-100T-8 card. The standard Cisco IOS RMON is also available.

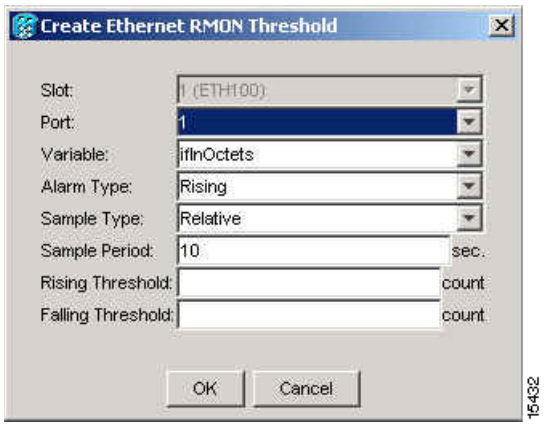
Step 1 Double-click the Ethernet card where you want to create the RMON alarm thresholds.

Step 2 In card view, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or the **Provisioning > POS Ports > RMON Thresholds** for CE-Series and ML-Series Ethernet cards.

Step 3 Click **Create**.

The Create Threshold dialog box appears (Figure 18-5).

Figure 18-5 Creating RMON Thresholds



Step 4 From the Slot drop-down list, choose the appropriate Ethernet card.

Step 5 From the Port drop-down list, choose the applicable port on the Ethernet card you selected.

Step 6 From the Variable drop-down list, choose the variable.

In the POS Ports Create Threshold window, the variables that appear in the Variable drop-down list depend on the framing mode used by the cards. The two framing modes for the POS port on the CE-Series and ML-Series cards are HDLC (High-Level Data Link Control) and GFP-F (frame-mapped generic framing procedure).

Table 18-1 provides a list of the Ether ports threshold variables available in this field.

Table 18-1 Ethernet Threshold Variables (MIBs)

Variable	Definition
ifInOctets	Total number of octets received on the interface, including framing octets
ifInUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInMulticastPkts	Number of multicast frames received error free

Table 18-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
ifInBroadcastPkts	The number of packets, delivered by this sublayer to a higher (sub)layer, which were addressed to a broadcast address at this sublayer
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
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts	Number of multicast frames transmitted error free
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sublayer, including those that were discarded or not sent
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets
dot3statsAlignmentErrors	Number of frames with an alignment error, that is, frames with a length that is not an integral number of octets and where the frame cannot pass the frame check sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, that is, where there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 1518 octets in length
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address; this does not include multicast packets

Table 18-1 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address; this number does not include packets directed to the broadcast
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets)
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length
etherStatsDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources. This number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected

Table 18-2 provides a list of the POS ports threshold variables for HDLC mode.

Table 18-2 POS Threshold Variables for HDLC Mode (MIBs)

Parameter	Definition
iflnOctets	The total number of octets received on the interface, including framing octets
txTotalPkts	The total number of transmit packets
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
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	The total number of transmitted octets, including framing packets
rxTotalPkts	The total number of receive packets
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET; packets larger than 1600 bytes do not get transmitted.
mediaIndStatsRxFramesBadCRC	A count of the received Fibre Channel frames with errored cyclic redundancy checks (CRCs).
hdlcRxAborts	Number of received packets aborted before input

Table 18-2 POS Threshold Variables for HDLC Mode (MIBs) (continued)

Parameter	Definition
ifInPayloadCRCErrors	The number of receive data frames with payload CRC errors
ifOutPayloadCRCErrors	The number of transmit data frames with payload CRC errors

Table 18-3 provides a list of the POS ports threshold variables for GFP-F mode.

Table 18-3 POS Threshold Variables for GFP-F Mode (MIBs)

Variable	Definition
iflnOctets	The total number of octets received on the interface, including framing octets
txTotalPkts	The total number of transmit packets
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
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	The total number of transmitted octets, including framing packets
rxTotalPkts	The total number of receive packets
ifOutOversizePkts	Number of packets larger than 1518 bytes sent out into SONET; packets larger than 1600 bytes do not get transmitted.
gfpStatsRxSBitErrors	Receive frames with Single Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxMBitErrors	Receive frames with Multi Bit Errors (cHEC, tHEC, eHEC)
gfpStatsRxTypeInvalid	Receive frames with invalid type (PTI, EXI, UPI)
gfpStatsRxCRCErrors	Receive data frames with Payload CRC errors
gfpStatsRxCIDInvalid	Receive frames with Invalid CID
gfpStatsCSFRaised	Number of receive (Rx) client management frames with Client Signal Fail indication
ifInPayloadCRCErrors	The number of receive data frames with payload CRC errors
ifOutPayloadCRCErrors	The number of transmit data frames with payload CRC 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 **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 Enter an appropriate number of seconds for the Sample Period.

Step 10 Enter the appropriate number of occurrences for the Rising Threshold.

Note 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 seconds and a problem causes 1001 collisions in 15 seconds, 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.

Note 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 seconds subsides and creates only 799 collisions in 15 seconds, 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-second 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** to complete the procedure.

Step 13 Return to your originating procedure (NTP).

DLP-C106 Delete Ethernet RMON Alarm Thresholds

Purpose	This task deletes RMON threshold crossing alarms for Ethernet ports.
Tools/Equipment	None
Prerequisite Procedures	NTP-C68 Create or Delete Ethernet RMON Thresholds, page 8-5 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Double-click the Ethernet card where you want to delete the RMON alarm thresholds.

Step 2 In card view, click the **Provisioning > Ether Ports > RMON Thresholds** tabs or the **Provisioning > POS Ports > 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 that threshold.

Step 6 Return to your originating procedure (NTP).

DLP-C107 View Circuit Information

Purpose	This task provides information about ONS 15310-CL and ONS 15310-MA circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate Cisco Transport Controller (CTC) view:

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

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

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

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—Circuit types are: STS (STS circuit), VT (VT circuit), VTT (VT tunnel), VAP (VT aggregation point), STS-V (STS virtual concatenated [VCAT] circuit), or VT-V (VT VCAT circuit).
- Size—Circuit size. VT circuits are 1.5. ONS 15310-CL STS circuits are 1, 3c, 6c, 9c, or 12c. ONS 15310-MA STS circuits are 1, 3c, 6c, 9c, 12c, 24c, and 48c. VCAT circuits are VT1.5-*n*v or STS-1-*n*v, where *n* is the number of members.
- Protection—The type of circuit protection. See Table 18-4 for a list of protection types.

Table 18-4 Circuit Protection Types

Protection Type	Description
1+1	The circuit is protected by a 1+1 protection group.
N/A	A circuit with connections on the same node is not protected.
Protected	The circuit is protected by diverse SONET topologies, for example, a path protection configuration and a 1+1 protection group.
Unknown	A circuit has a source and destination on different nodes and communication is down between the nodes. This protection type appears if not all circuit components are known.
Unprot (black)	A circuit with a source and destination on different nodes is not protected.

Table 18-4 Circuit Protection Types (continued)

Protection Type	Description
Unprot (red)	A circuit created as a fully protected circuit is no longer protected due to a system change, such as removal of a 1+1 protection group.
Path protection	The circuit is protected by a path protection configuration.

- Dir—The circuit direction, either two-way or one-way.
- Status—The circuit status. Table 18-5 lists the circuit statuses that may appear.

Table 18-5 ONS 15310-CL and ONS 15310-MA Circuit Status

Status	Definition/Activity
CREATING	CTC is creating a circuit.
DISCOVERED	CTC created a circuit. All components are in place and a complete path exists from circuit source to destination.
DELETING	CTC is deleting a circuit.
PARTIAL	A CTC-created circuit is missing a cross-connect or network span or a complete path from source to destinations does not exist. In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is PARTIAL. However, an PARTIAL status does not necessarily mean a circuit traffic failure has occurred, because traffic may flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans appear as green lines, and down spans appear as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray to indicate that the span is down. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line does not appear on the network map. Subsequently, circuits routed on a network span that goes down appear as DISCOVERED during the current CTC session, but appear as PARTIAL to users who log in after the span failure.
DISCOVERED_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is complete. A complete path from source to destination(s) exists.
PARTIAL_TL1	A TL1-created circuit or a TL1-like, CTC-created circuit is missing a cross-connect or circuit span (network link), and a complete path from source to destinations does not exist.
CONVERSION_PENDING	An existing circuit in a topology upgrade is set to this status. The circuit returns to the DISCOVERED status when the topology upgrade is complete.

Table 18-5 ONS 15310-CL and ONS 15310-MA Circuit Status (continued)

Status	Definition/Activity
PENDING_MERGE	Any new circuits created to represent an alternate path in a topology upgrade are set to this status to indicate that they are temporary circuits. These circuits can be deleted if a topology upgrade fails.
DROP_PENDING	A circuit is set to this status when a new circuit drop is being added.

- Source—The circuit source in the format: *node/slot/port "port name"/STS/VT*. (Port name appears in quotes.) Node and slot always appear; *port "port name"/STS/VT* might appear, depending on the source card, circuit type, and whether a name is assigned to the port. If the port uses a pluggable port module (PPM), the port format is *PPM-port number*, for example, p2-1. If the port is a DS-1, DS-3, or EC-1 port, port type is indicated, for example, pDS1. If the circuit size is a concatenated size (3c, 6c, 9c, 12c), STSs used in the circuit are indicated by an ellipsis, for example, S7..9, (STSs 7, 8, and 9) or S10..12 (STSs 10, 11, and 12).
- Destination—The circuit destination in same format as the circuit source.
- # of Spans—The number of inter-node links that constitute the circuit. Right-clicking the column shows a shortcut menu from which you can choose Span Details to show or hide circuit span detail.
- State—The circuit service state, which is an aggregate of the service states of its cross-connects:
  - IS—All cross-connects are in the In-Service and Normal (IS-NR) service state.
  - OOS—All cross-connects are in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) and/or Out-of-Service and Management, Maintenance (OOS-MA,MT) service state.
  - OOS-PARTIAL—At least one cross-connect is IS-NR and others are OOS-MA,DSBLD and/or OOS-MA,MT.

Step 3 Return to your originating procedure (NTP).

DLP-C109 Filter the Display of Circuits

Purpose	This task filters the display of circuits in the ONS network, node, or card view Circuits window based on circuit name, size, type, direction, and other attributes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 Navigate to the appropriate CTC view:

- To filter network circuits, from the View menu choose **Go to Network View**.

- To filter circuits that originate, terminate, or pass through a specific node, from the View menu. choose **Go to Other Node**, then choose the node you want to search and click **OK**.
- To filter circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

Step 2 Click the **Circuits** tab.

Step 3 Set the attributes for filtering the circuit display:

a. Click the **Filter** button.

b. In the General tab of the Circuit Filter dialog box, set the following filter attributes, as necessary:

- Name—Enter a complete or partial circuit name to filter circuits based on the circuit name; otherwise leave the field blank.
- Direction—Choose one: **Any** (direction not used to filter circuits), **1-way** (display only one-way circuits), or **2-way** (display only two-way circuits).
- Status—Choose a circuit status to filter the circuits. For more information about circuit statuses, see Table 18-5 on page 18-13.
- State—Choose one: **OOS** (display only out-of-service circuits), **IS** (display only in-service circuits; OCHNCs have IS status only), or **OOS-PARTIAL** (display only circuits with cross-connects in mixed service states).
- Protection—Choose a protection type to filter the circuits. For more information about protection types, see Table 18-4 on page 18-12.
- Slot—Enter a slot number to filter circuits based on the source or destination slot; otherwise leave the field blank.
- Port—Enter a port number to filter circuits based on the source or destination port; otherwise leave the field blank.
- Type—Choose one: **Any** (type not used to filter circuits), **STS** (displays only STS circuits), **VT** (displays only VT circuits), **VT Tunnel** (displays only VT tunnels), **STS-V** (displays STS VCAT circuits), **VT-V** (displays VT VCAT circuits), or **VT Aggregation Point** (displays only VT aggregation points).
- Size—Click the appropriate check boxes to filter circuits based on size: VT circuits are 1.5. ONS 15310-CL STS circuits are 1, 3c, 6c, 9c, or 12c. ONS 15310-MA STS circuits are 1, 3c, 6c, 9c, 12c, 24c, and 48c. VCAT circuits are VT1.5-*n*v or STS-1-*n*v, where *n* is the number of members.

  The check boxes shown depend on the Type field selection. If you chose Any, all sizes are available. If you chose VT, VT1.5 or VT2 are available. If you chose VT-V, only VT1.5 is available. If you chose STS, only STS sizes are available, and if you chose VT Tunnel or VT Aggregation Point, only STS-1 is available.

Step 4 To set the filter for ring, node, link, and source and drop type, click the **Advanced** tab and complete the following. If you do not want to make advanced filter selections, continue with Step 5.

a. If you made selections on the General tab, click **Yes** in the confirmation box to apply the settings.

b. In the Advanced tab of the Circuit Filter dialog box, set the following filter attributes as necessary:

- Ring—Choose the ring from the drop-down list.
- Node—Click the check boxes by each node in the network to filter circuits based on node.
- Link—Choose the desired link in the network.

- Source/Drop—Choose one of the following to filter circuits based on whether they have one or multiple sources and drops: **One Source and One Drop Only** or **Multiple Sources or Multiple Drops**.

Step 5 Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box appear in the Circuits window.

Step 6 To turn filtering off, click the Filter icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on, and click the **Filter** button to change the filter attributes.

Step 7 Return to your originating procedure (NTP).

DLP-C110 View Circuits on a Span

Purpose	This task displays circuits routed on an ONS 15310-CL or ONS 15310-MA span.
Tools/Equipment	None
Prerequisite Procedures	Circuits must be created on the span; see Chapter 6, "Create Circuits and VT Tunnels" DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Step 1 From the View menu in node view, choose **Go to Network View**. If you are already in network view, continue with Step 2.

Step 2 Right-click the green line containing the circuits you want to view and choose **Circuits** to view path protection, 1+1, or unprotected circuits on the span.

In the Circuits on Span dialog box, you can view the following information for circuits provisioned on the span:

- STS—Displays STSs used by the circuits.
- VT—Displays VTs used by the circuits (VT circuits).
- Path Protection—(Path protection span only) If checked, path protection circuits are on the span.
- Circuit—Displays the circuit name.
- Switch State—(Path protection span only) Displays the switch state of the circuit, that is, whether any span switches are active. For path protection spans, switch types include: CLEAR (no spans are switched), MANUAL (a Manual switch is active), FORCE (a Force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).

Note You can perform other procedures from the Circuits on Span dialog box. If the span is in a path protection configuration, you can switch the span traffic. See the "DLP-C166 Initiate a Path Protection Force Switch on a Span" task on page 18-60 for instructions. If you want to edit a circuit on the span, double-click the circuit. See the "DLP-C112 Edit a Circuit Name" task on page 18-18 or the "DLP-C114 Edit Path Protection Circuit Path Selectors" task on page 18-20 for instructions.

Step 3 Return to your originating procedure (NTP).

DLP-C111 Change a Circuit Service State

Purpose	This task changes the service state of a circuit. For more information about circuit states, refer to the "Circuits and Tunnels" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the circuit with the service state that you want to change.

Step 3 From the Tools menu, choose **Circuits > Set Circuit State**.

Step 4 In the Set Circuit State dialog box, choose the administrative state from the Target Circuit Admin State drop-down list:

- **IS**—Puts the circuit cross-connects in the IS-NR service state.
- **OOS,DSBLD**—Puts the circuit cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- **IS,AINS**—Puts the circuit cross-connects in the 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 OOS-MA,MT service state. This service state does not interrupt traffic flow and allows loopbacks to be performed on the circuit, but suppresses alarms and conditions. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; OOS; or IS,AINS when testing is complete.
- **OOS,OOG**—(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. OOS-MA,OOG applies only to the cross-connects on an end node where VCAT resides. The cross-connects on intermediate nodes are in the OOS-MA,MT service state.

Note You can also change the administrative state by clicking the **Edit** button on the Circuits tab, then clicking the **State** tab on the Edit Circuits window.

For additional information about circuit service states, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

Step 5 If you want to apply the administrative state to the circuit source and destination ports, check the **Apply to drop ports** check box.

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.

Step 6 Click **Apply**.

Step 7 If a confirmation dialog box appears, click **Yes** to continue. If the Circuit State Transitions dialog box appears, view the results and click **OK**.

CTC will not change the service state of the circuit source and destination port in certain circumstances. For example, if a port is in loopback (OOS-MA,LPBK & MT), CTC will not change the port to IS-NR. In another example, if the circuit size is smaller than the port, CTC will not change the port service state from IS-NR to OOS-MA,DSBLD. If CTC cannot change the port service state, you must change the port service state manually. For more information, see the "DLP-C50 Change the Service State for a Port" task on page 17-67.

Step 8 Return to your originating procedure (NTP).

DLP-C112 Edit a Circuit Name

Purpose	This task edits a circuit name, including VCAT circuit member names.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the circuit you want to rename, then click **Edit**.

Step 3 If you want to edit a VCAT circuit member name, complete the following steps in the Edit Circuit window. If not, continue with the Step 4.

- **a.** Click the **Members** tab.
- **b.** Click the VCAT member that you want to edit, then click **Edit Member**. The Edit Member window opens.

Step 4 In the General tab, click the **Name** field and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters.

Note If you will create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits add "_MON" (four characters) to the circuit name.

Step 5 Click **Apply**.

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

Step 7 If you changed the name of a VCAT circuit member, repeat Step 6 for the Edit Circuit window.

Step 8 In the Circuits window, verify that the circuit was correctly renamed.

Step 9 Return to your originating procedure (NTP).

DLP-C113 Change Active and Standby Span Color

Purpose	This task changes the color of active (working) and standby (protect) circuit spans on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the Edit menu in node view, choose **Preferences**.

Step 2 In the Preferences dialog box, click the **Circuit** tab.

Step 3 Complete one or more of the following steps, as required:

- To change the color of the active (working) span, continue with Step 4.
- To change the color of the standby (protect) span, continue with Step 5.
- To return active and standby spans to their default colors, continue with Step 6.

Step 4 As needed, change the color of the active span:

a. In the Span Colors area, click the colored square next to Active.

b. In the Pick a Color dialog box, click the color for the active span, or click the **Reset** button if you want the active span to display the last applied (saved) color.

c. Click **OK** to close the Pick a Color dialog box. If you want to change the standby span color, continue with Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 5 As needed, change the color of the standby span:

a. In the Span Colors area, click the colored square next to Standby.

b. In the Pick a Color dialog box, click the color for the standby span, or click the **Reset** button if you want the standby span to display the last applied (saved) color.

c. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 6 Return the active and standby spans to their default colors:

a. From the Edit menu, choose **Preferences**.

b. In the Preferences dialog box, click the **Circuits** tab.

c. Click the **Reset to Defaults** button.

d. Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box open.

Step 7 Return to your originating procedure (NTP).

DLP-C114 Edit Path Protection Circuit Path Selectors

Purpose	This task changes the path protection signal fail and signal degrade thresholds, the reversion and reversion time, and the PDI-P settings for one or more path protection circuits.
Tools/Equipment	None
Prerequisite Procedures	NTP-C31 Provision Path Protection Nodes, page 5-10 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the **Circuits** tab.

Step 3 Click the path protection circuits you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose non-adjoining circuits) and click each circuit you want to change.

Step 4 From the Tools menu, choose **Circuits > Set Path Selector Attributes**.

Note Alternatively, for single circuits you can click the **Edit** button, then click the **Path Protection Selectors** tab on the Edit Circuits window.

Step 5 In the Path Selectors Attributes dialog box, edit the following path protection selectors, as needed:

- Revertive—If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If this check box is not checked, traffic does not revert.
- Reversion Time (Min)—If Revertive is checked, this value sets the amount of time that will elapse before traffic reverts to the working path. The range is 0.5 to 12 minutes in 0.5 minute increments.
- In the VT Circuits Only area, set the following thresholds:
  - SF Ber Level—Sets the path protection signal failure BER threshold.
  - SD Ber Level—Sets the path protection signal degrade BER threshold.
- In the STS Circuits Only area, set the following thresholds:
  - SF Ber Level—Sets the path protection signal failure BER threshold.

- SD Ber Level—Sets the path protection signal degrade BER threshold.
- Switch on PDI-P—When checked, traffic switches if an STS payload defect indication is received.

Step 6 Click **OK** and verify that the changed values are correct.

Step 7 Return to your originating procedure (NTP).

DLP-C115 Delete Circuits

Purpose	This task deletes circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
	Circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Complete the "NTP-C102 Back Up the Database" procedure on page 15-2 to preserve the existing database and circuits.

Step 2 Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.

Step 3 Click the **Alarms** tab.

a. Verify that the alarm filter is not on. See the "DLP-C88 Disable Alarm Filtering" task on page 17-109 as necessary.

b. Verify that no unexplained alarms appear on the network. If alarms are present, investigate and resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

Step 4 From the View menu, choose **Go to Network View**.

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:

- **Set drop ports to OOS**—Puts the circuit source and destination ports to OOS-MA,DSBLD if the circuit is the same size as the port or is the only circuit using the port. 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.
- **Notify when completed**—If checked, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are in OOS-MA,DSBLD and the circuit is deleted. During this time, you cannot perform other CTC functions. If you are deleting many circuits, waiting for confirmation can take a few minutes. 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 checkbox. For more information, see the "DLP-C36 Configure the CTC Alerts Dialog for Automatic Popup" task on page 17-51. If the CTC Alerts dialog 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 next step.

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-C102 Back Up the Database" procedure on page 15-2.

Step 12 Return to your originating procedure (NTP).

DLP-C116 Add a Member to a VCAT Circuit

Purpose	This task adds a member to non-LCAS and LCAS circuits on CE-100T-8 or ML-100T-8 cards. 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 fiber) specified during the VCAT circuit creation procedure.
Tools/Equipment	CE-100T-8 or ML-100T-8 card
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 VCAT circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Caution Adding a member to 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 use a Cisco ONS 15454 ML-Series card as a source or destination.

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 an 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.

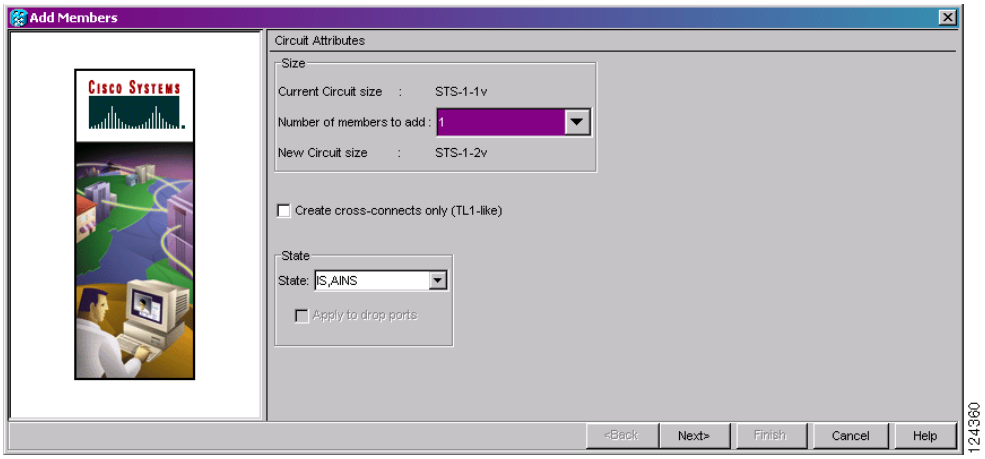
Step 5 Click **Add Member**. The Add Member button is enabled if the VCAT circuit has sufficient bandwidth for an added member.

Step 6 Define the number of members and member attributes (Figure 18-6):

- 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 15310-CL and Cisco ONS 15310-MA 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 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 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. IS,AINS is the default state.
- OOS,MT—Puts the member cross-connects in the OOS-MA,MT service state. This service state does not interrupt traffic flow and allows loopbacks to be performed on the circuit, but suppresses alarms and conditions. Use the OOS,MT administrative state for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; OOS; or IS,AINS when testing is complete. See the "DLP-C180 Change a VCAT Member Service State" task on page 18-73.
- OOS,OOG—(LCAS VCAT only) Puts VCAT member cross-connects in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to put a member circuit out of the group and to stop sending traffic.

Figure 18-6 Adding a VCAT Member



Step 7 Click **Next**.

Step 8 To route the members 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 from the drop-down list to identify the member.
- Name—Enter 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—(Future use) Routes the member on a BLSR protection channel.

Note Although ONS 15310-CLs do not support BLSR, you can route an LCAT VCAT circuit over a BLSR network of ONS 15600s, ONS 15454s, or ONS 15327s.

  - 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—(Future use) Routes the member on a BLSR protection channel.

Note Although ONS 15310-CL and ONS 15310-MAs do not support BLSR, you can route an LCAT VCAT circuit over a BLSR network of ONS 15600, ONS 15454, or ONS 15327 nodes.

  - 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 or unprotected portions of the member route from the source to the destination.
- Add one span for all 1+1 portions of the route from the source to the destination.
- For members routed on path protection dual ring interconnect topologies, provision the working and protect paths.

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 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for the procedure to clear the alarm. If it does not, continue with b.

b. Complete the "DLP-C180 Change a VCAT Member Service State" task on page 18-73 to put the member in the IS service state.

Step 15 Return to your originating procedure (NTP).

DLP-C117 Delete a Member from a VCAT Circuit

Purpose	This task removes a member from a non-LCAS or LCAS VCAT circuit on CE-100T-8 or ML-100T-8 cards. This task reduces the size of the VCAT circuit. You cannot delete members from VCAT circuits that use ONS 15454 ML-Series cards as a circuit source or destination.
Tools/Equipment	CE-100T-8 or ML-100T-8 card
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 VCAT circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures. As necessary, complete the "DLP-C180 Change a VCAT Member Service State" task on page 18-73 to change a LCAS member state to OOS-MA,OOG.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Caution Deleting LCAS members in the IS-NR or OOS-AU,AINS service state can be service affecting. Cisco recommends putting the LCAS 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.

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**.

You cannot delete members from VCAT circuits that use ONS 15454 ML-Series cards as a circuit source or destination.

Step 6 In the confirmation dialog box, click **Yes**.

Step 7 Return to your originating procedure (NTP).

DLP-C118 Change Tunnel Type

Purpose	This task converts a traditional DCC tunnel to an IP-encapsulated tunnel or an IP-encapsulated tunnel to a traditional DCC tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C67 Create a DCC Tunnel, page 17-84 or DLP-C69 Create an IP-Encapsulated Tunnel, page 17-86 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the **Provisioning > 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%).
- 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-C119 Repair an IP Tunnel

Purpose	This task repairs circuits that have a OOS-PARTIAL status as a result of node IP address changes.
Tools/Equipment	None
Prerequisite Procedures	See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures. DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	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.
- 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-C120 Delete Overhead Circuits

Purpose	This task deletes overhead circuits. Overhead circuits include DCC tunnels, IP-encapsulated tunnels, and user data channels.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	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-C50 Change the Service State for a Port" task on page 17-67.

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: 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-C121 Provision Path Trace on Circuit Source and Destination Ports

Purpose	This task creates a path trace on STS circuit source ports and destination ports.
Tools/Equipment	Cards capable of transmitting and receiving path trace must be installed at the circuit source and destination. See Table 18-6 on page 18-29 for a list of cards.
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note This task assumes you are setting up path trace on a bidirectional circuit and setting up transmit strings at the circuit source and destination.

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

Step 2 Click the **Circuits** tab.

For the STS circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string. Table 18-6 shows the ONS 15310-CL and ONS 15310-MA cards and/or ports that support J1 and/or J2 path trace.

Table 18-6 ONS 15310-CL and ONS 15310-MA Cards/Ports Capable of J1/J2 Path Trace

Trace Function	J1 or J2	Cards/Ports
Transmit and receive	J1	ONS 15310-CL DS-1 and DS-3 ports
		ML-100T-8
	J1 and J2	CE-100T-8
	J2	ONS 15310-MA OC-N and DS1 ports
Receive	J1	ONS 15310-CL EC-1, OC-3, and OC-12 ports
		ONS 15310-MA OC-N, EC-1, DS1, and DS3 ports

Step 3 If neither port is transmit/receive, you will not be able to complete this task. If one port is transmit/receive and the other is a receive-only port, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

Step 4 Choose the STS circuit you want to trace, then double-click it (or click **Edit**).

Step 5 If you chose a VCAT circuit, complete the following. If not, continue with Step 6.

a. In the Edit Circuit window, click the **Members** tab.

b. Click **Edit Member** and continue with Step 6.

Step 6 In the Edit Circuit window, click the **Show Detailed Map** check box at the bottom of the window. A detailed map of the source and destination ports appears.

Step 7 Provision the circuit source transmit string:

a. In the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit J1 Path Trace (port)** from the shortcut menu.

b. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**, then click **Close**.

Step 8 Provision the circuit destination transmit string:

a. In the detailed circuit map, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu.

b. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**.

Step 9 Provision the circuit destination expected string:

a. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—The first string received from the source port is the baseline. An alarm is raised when a string that differs from the baseline is received.
- Manual—The string entered in the Current Expected String is the baseline. An alarm is raised when a string that differs from the Current Expected String is received.

b. If you set the Path Trace Mode field to Manual, enter the string that the circuit destination should receive from the circuit source in the New Expected String field. If you set the Path Trace Mode field to Auto, skip this step.

c. Check the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and RDI when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for descriptions of alarms and conditions.

d. (Check box visibility depends on card selection.) Check the **Disable AIS on C2 Mis-Match** check box if you want to suppress the Alarm Indication Signal when a C2 mis-match occurs.

e. Click **Apply**, then click **Close**.

Note It is not necessary to set the format (16 bytes for VT circuits or 64 bytes for STS circuits) for the circuit destination expected string; the path trace process automatically determines the format.

Step 10 Provision the circuit source expected string:

a. In the Edit Circuit window (with Show Detailed Map chosen) right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

b. In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

c. If you set Path Trace Mode to Manual, enter the string that the circuit source should receive from the circuit destination in the New Expected String field. If you set Path Trace Mode to Auto, skip this step.

d. Check the **Disable AIS and RDI if TIM-P is detected** check box if you want to suppress the alarm indication signal (AIS) and RDI when the STS Path Trace Identifier Mismatch Path (TIM-P) alarm appears. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for descriptions of alarms and conditions.

e. (Check box visibility depends on card selection.) Check the **Disable AIS on C2 Mis-Match** check box if you want to suppress the Alarm Indication Signal when a C2 mis-match occurs.

f. Click **Apply**.

Note It is not necessary to set the format (16 or 64 bytes) for the circuit destination expected string; the path trace process automatically determines the format.

Step 11 After you set up the path trace, the received string appears in the Received field on the path trace setup window. The following options are available:

- Click **Hex Mode** to display path trace in hexadecimal format. The button name changes to ASCII Mode. Click it to return the path trace to ASCII format.
- Click **Reset** to reread values from the port.
- Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

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

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

Step 12 Click **Close**.

When you display the detailed circuit window, path trace is indicated by an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.

Step 13 Return to your originating procedure (NTP).

DLP-C122 Provision Path Trace on OC-N Ports

Purpose	This task monitors a path trace on OC-N ports within the circuit path.
Tools/Equipment	The OC-N ports you want to monitor must be on OC-N cards capable of receiving path trace. See Table 18-6 on page 18-29.
Prerequisite Procedures	DLP-C121 Provision Path Trace on Circuit Source and Destination Ports, page 18-29 DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 From the View menu, choose **Go to Other Node**. In the Select Node dialog box, choose the node where path trace was provisioned on the circuit source and destination ports.

Step 2 In node view, click **Circuits**.

Step 3 Choose the STS circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4 In the Edit Circuit window, check the Show Detailed Map check box at the bottom of the window. A detailed circuit graphic showing source and destination ports appears.

Step 5 In the detailed circuit map, right-click the circuit OC-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

Step 6 In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down list:

- Auto—Uses the first string received from the port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received. For OC-N ports, Auto is recommended, since Manual mode requires you to trace the circuit on the Edit Circuit window to determine whether the port is the source or destination path.
- Manual—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 7 If you set the Path Trace Mode field to Manual, enter the string that the OC-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit window to determine whether the port is in the circuit source or destination path, then set the New Expected String field to the string transmitted by the circuit source or destination. If you set the Path Trace Mode field to Auto, skip this step.

Step 8 Click **Apply**, then click **Close**.

Step 9 Return to your originating procedure (NTP).

DLP-C123 Change the Node Name, Date, Time, and Contact Information

Purpose	This task changes basic information such as node name, date, time, and contact information.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Changing the date, time, or time zone might invalidate the node's performance monitoring counters.

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

Step 2 Change any of the following:

- General: Node Name
- General: Contact
- Location: Latitude
- Location: Longitude
- Location: Description

Note To see changes to longitude or latitude on the network map, you must go to network view and right-click the specified node, then click **Reset Node Position**.

- Time: Use NTP/SNTP Server
- Time: Date (M/D/Y)
- Time: Time (H:M:S)
- Time: Time Zone
- Time: Use Daylight Saving Time

See the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 for detailed field descriptions.

Step 3 Click **Apply**.

Step 4 Return to your originating procedure (NTP).

DLP-C124 Change the Login Legal Disclaimer

Purpose	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, click the **Provisioning > Security > Legal Disclaimer > HTML** tabs.

Step 2 The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. Use the following HTML commands to format the text as needed:

- Begins boldface font
- Ends boldface font
- Aligns type in the center of the window
- Ends the center alignment
- <font=n, where n = point size> Changes the font to the new size
- Ends the font size command
- <p> Creates a line break
- <sub> Begins subscript
- </sub> Ends subscript
- <sup> Begins superscript
- </sup> Ends superscript
- <u> Begins underline
- </u> Ends underline

Step 3 If you want to preview your changed statement and format, click the **Preview** subtab.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C125 Change IP Settings

Purpose	This task explains how to change the IP address, subnet mask, default router, dynamic host configuration protocol (DHCP) access, firewall access, and SOCKS proxy server settings for the ONS 15310-CL and Cisco ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C39 Provision IP Settings, page 17-53
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If you assign one ONS 15310 node an IP address that is in use on another node, both nodes might retain the duplicated IP addresses even after you attempt to change them. Duplicated IP addresses raises the DUP-IPADDR alarm. Refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* to troubleshoot the DUP-IPADDR alarm.

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

Step 2 Change any of the following:

- IP Address
- Suppress CTC IP Display
- Default Router
- Forward DHCP Request To
- Net/Subnet Mask Length
- CTX CORBA (IIOP) Listener Port
- Gateway Settings

See the "DLP-C39 Provision IP Settings" task on page 17-53 for detailed field descriptions.

Step 3 Click **Apply**.

If you changed any of the network fields that will cause the node to reboot, the Change Network Configuration confirmation dialog box appears. If you changed a gateway setting, a confirmation appropriate to the gateway field appears. If you only changed the IP address fields, no confirmation dialog box appears.

Step 4 If a confirmation dialog box appears, click **Yes**.

If you changed the IP address, subnet mask length, or CTX CORBA (IIOP) listener port, the 15310-CL-CTX card (in the ONS 15310-CL) or CTX2500 card (in the ONS 15310-MA) will reboot.

Step 5 Return to your originating procedure (NTP).

DLP-C126 Modify a Static Route

Purpose	This task modifies a static route on an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C40 Create a Static Route, page 17-55
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > Static Routing** tabs.

Step 2 Click the static route that you want to edit.

Step 3 Click **Edit**.

Step 4 In the Edit Selected Static Route dialog box, enter the following:

- Mask
- Next Hop
- Cost

See the "DLP-C40 Create a Static Route" task on page 17-55 for detailed field descriptions.

Step 5 Click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-C127 Delete a Static Route

Purpose	This task deletes a static route on an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C40 Create a Static Route, page 17-55
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > Static Routing** tabs.

Step 2 Click the static route you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-C128 Disable Open Shortest Path First Protocol

Purpose	This task disables the Open Shortest Path First (OSPF) routing protocol for an ONS 15310-CL or ONS 15310-MA local area network (LAN).
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C41 Set Up or Change Open Shortest Path First Protocol, page 17-56
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, click the **Provisioning > Network > OSPF** tabs. The OSPF subtab has several options.

Step 2 In the OSPF on LAN area, uncheck the **OSPF active on LAN** check box.

Step 3 Click **Apply**.

Note Disabling OSPF can cause an 15310-CL-CTX or CTX2500 reboot, which causes a temporary loss of connectivity to the node but does not affect traffic.

Step 4 Return to your originating procedure (NTP).

DLP-C129 Delete a Proxy Tunnel

Purpose	This task removes a proxy tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	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 Continue with your originating procedure (NTP).

DLP-C130 Delete a Firewall Tunnel

Purpose	This task removes a firewall tunnel.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 In node view, 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-C131 Change the Network View Background Color

Purpose	This task changes the network view background color and the domain view background color (the area shown when you open a domain).
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

Note If you modify background colors, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

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

Step 2 Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 3 In the Choose Color dialog box, click a background color.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C132 Change to the Default Network View Background Map

Purpose	This task changes the background map to the default map of the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note If you modify the background image, the change is stored in your CTC user profile on the local computer. The change does not affect other CTC users on different computers.

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

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

Step 3 Under Defaults Selector, choose **CTC** and then **Network**.

Step 4 Click the **Default Value** field and choose a default map from the drop-down list. The map choices are Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).

Step 5 Click **Apply**. The new network map appears.

Step 6 Click **OK**.

Step 7 If the ONS 15310-CL or ONS 15310-MA icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all the node icons are visible. (You can also choose **Fit Graph to Window**.)

Step 8 If you need to reposition the node icons, drag and drop them one at a time to a new location on the map.

Step 9 If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15310-CL or ONS 15310-MA icons appear at the magnification you want.

Step 10 Return to your originating procedure (NTP).

DLP-C133 Apply a Custom Network View Background Map

Purpose	This task changes the background image or map on the CTC network view.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher

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

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

Step 2 Right-click the network or domain map and choose **Set Background Image**.

Step 3 Navigate to the graphic file you want to use as a background.

Step 4 Select the file and click **Open**. The graphic file appears as the CTC background image.

Step 5 As needed, complete the following to view and move the node icons:

- If the node icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until all of the node icons are visible.
- If you want to reposition the node icons, drag and drop them one at a time to a new location on the map.
- It you want to change the magnification of the icons, right-click the network view and choose **Zoom In** or **Zoom Out**. Repeat until the node icons appear at the magnification you want.

Step 6 Return to your originating procedure (NTP).

DLP-C134 Create Domain Icons

Purpose	This task creates a domain icon to group ONS 15310-CL or ONS 15310-MA icons in CTC network view. By default, domains are visible on all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note All domain changes, such as added or removed nodes, are visible to all users who log into the network.

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, Superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means any user can maintain the domain information in his or her Preferences file, meaning domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only superusers can create a domain or put a node into a domain.) See the "NTP-C137 Edit Network Element Defaults" procedure on page 15-18 to change NE default values.

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

Step 2 Right-click the network map and choose **Create New Domain** from the shortcut menu.

Step 3 When the domain icon appears on the map, click the map name and type the domain name.

Step 4 Press **Enter**.

Step 5 Return to your originating procedure (NTP).

DLP-C135 Manage Domain Icons

Purpose	This task manages CTC network view domain icons. By default, domains are visible on all CTC sessions that log into the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C134 Create Domain Icons, page 18-40
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note To allow users of any security level to create local domains, that is, domains that are visible on the home CTC session only, superusers can change the CTC.network.LocalDomainCreationAndViewing NE default value to TRUE. A TRUE value means any user can maintain the domain information in his or her Preferences file, meaning domain changes will not affect other CTC sessions. (The default value is FALSE, meaning domain information affects all CTC sessions and only superusers can create a domain or put a node into a domain.) See the "NTP-C137 Edit Network Element Defaults" procedure on page 15-18 to change NE default values.

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

Step 2 Locate the domain action you want in Table 18-7 and complete the appropriate steps.

Table 18-7 Managing Domains

Domain action	Steps
Move a domain	Drag and drop the node icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag and drop the node icon to the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Choose **Move Node Back to Parent View**.
Open a domain	• Double-click the domain icon. • Right-click the domain and choose **Open Domain**.
Return to network view	Right-click the domain view area and choose **Go to Parent View** from the shortcut menu.

Table 18-7 Managing Domains (continued)

Domain action	Steps
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and choose **Show Domain Overview**.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes in the domain are returned to the network map.

Step 3 Return to your originating procedure (NTP).

DLP-C136 Enable Dialog Box Do-Not-Display Option

Purpose	This task enables or disables the "Do not display" dialog box preference for subsequent sessions.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note If any user who has rights to perform an operation (for example, creating a circuit) selects the "Do not show this dialog again" check box on a dialog box, the dialog box does not appear for any other users who perform that operation on the network unless the command is overridden using the following task.

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

Step 2 In the Preferences dialog box, click the **General** tab.

The Preferences Management area lists all dialog boxes where "Do not show this dialog again" was checked.

Step 3 Choose one of the following:

- **Don't Show Any**—Hides all do-not-display check boxes.
- **Show All**—Overrides do-not-display check box selections and displays all dialog boxes.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C137 Modify a 1+1 Protection Group

Purpose	This task modifies a 1+1 protection group for any optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Protection Groups area, double click the 1+1 protection group you want to modify or click **Edit**.

Step 3 In the Edit Protection Group dialog box, you can modify the following as needed:

- Name—Type the changes to the protection group name. The name can have up to 32 alphanumeric characters.
- Bidirectional switching—Check or uncheck.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions stay corrected for the amount of time chosen from the Reversion Time menu. Uncheck if you do not want traffic to revert.
- Reversion Time—If the Revertive check box is checked, choose the reversion time from the Reversion Time drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working card. Traffic can revert when conditions causing the switch are cleared.

See the "NTP-C141 Create Optical Protection Groups for the ONS 15310-CL" procedure on page 4-12 or "NTP-C142 Create Protection Groups for the ONS 15310-MA" procedure on page 4-13 for field descriptions.

Step 4 Click **Apply**.

Step 5 Return to your originating procedure (NTP).

DLP-C138 Delete a Protection Group

Purpose	This task deletes a protection group.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note 1:1 electrical protection groups are created automatically in the ONS 15310-MA and can only be deleted after the protect card of a 1:1 protection group is deleted.

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

Step 2 In the Protection Groups list, click the protection group you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** in the Delete Protection Group dialog box to confirm deletion.

Step 5 Return to your originating procedure (NTP).

DLP-C139 Change the Node Timing Source

Purpose	This task changes the SONET timing source for the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution The following task can be service affecting; perform it during a scheduled maintenance window.

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

Step 2 In the General Timing area, change any of the following information:

- Timing Mode

Note Because mixed timing can cause timing loops, Cisco does not recommend using the Mixed Timing option. Use this mode with care.

- SSM Message Set
- Quality of RES
- Revertive
- Reversion Time

See the "DLP-C45 Set Up External or Line Timing" task on page 17-61 for field descriptions.

Step 3 In the Reference Lists area, you can change the following information:

Note Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's Mechanical Interface Cards (MICs). If you attach equipment to the BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference

- BITS 1 Out

Step 4 In the BITS Facilities area, you can change the following information:

Note The BITS Facilities section sets the parameters for your BITS1 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- In/Out State
- Coding
- Framing
- Sync Messaging
- AIS Threshold
- Admin SSM
- LBO

Step 5 Click **Apply**.

Step 6 Return to your originating procedure (NTP).

DLP-C140 Verify Timing in a Reduced Ring

Purpose	Use this task to verify timing in the ring where you removed a node.
Tools/Equipment	None
Prerequisite Procedures	NTP-C98 Remove a Path Protection Node, page 14-4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Identify the type of timing (Line, External, Mixed) in the Timing Mode field.

Step 3 Scroll down to the Reference Lists and observe the NE Reference fields to see the timing references provisioned for that node.

Step 4 If the removed node was the only BITS timing source, perform the following:

a. Look for another node on the ring that can be used as a BITS source and set the Timing Mode for that node to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the "DLP-C139 Change the Node Timing Source" task on page 18-44.

b. If no node in the reduced ring can be used as a BITS source, choose one node to be your internal timing source. Set the Timing Mode for that node to **External**, set the BITS 1 and 2 State field to **OOS**, and set the NE Reference to **Internal Clock**. Then, choose line timing for all other nodes in the ring. This forces the first node to be the primary timing source. See the "DLP-C139 Change the Node Timing Source" task on page 18-44.

Note Internal timing conforms to Stratum 3 requirements and is not considered optimal.

Step 5 If the removed node was not the only BITS timing source, provision the adjacent nodes to line timing using SONET links (east and west) as timing sources, traceable to the node with external BITS timing. See the "NTP-C23 Set Up Timing" procedure on page 4-11.

Step 6 Return to your originating procedure (NTP).

DLP-C141 Change the Security Policy on a Single Node

Purpose	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 3 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—Displays the number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to unlock a user manually who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals). If you checked Manual Unlock by Superuser, Lockout Duration is disabled.

Step 4 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before he or she can reuse a password.
- New Password must Differ from the Old Password—Choose the number of characters that must differ between the old and new password. The default number is 1.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change their password the first time they log into their account.

Step 5 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.

Step 6 In the Other area, you can provision the following:

- Single Session Per User—If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 45 to 90 days.

Step 7 Click **Apply**.

Step 8 Return to your originating procedure (NTP).

DLP-C142 Change the Security Policy on Multiple Nodes

Purpose	This task changes the security policy for multiple nodes, including idle user timeouts, user lockouts, password change, and concurrent login policies.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Click the **Provisioning > Security > Policy** tabs. A read-only table of nodes and their policies appears.

Step 3 Click a node on the table that you want to modify, then click **Change**.

Step 4 If you want to modify the idle user timeout period, click the hour (H) and minute (M) arrows in the Idle User Timeout area for the security level you want to provision: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. The idle period time range is 0 and 16 hours, and 0 and 59 minutes. The user is logged out after the idle user timeout period is reached.

Step 5 In the User Lockout area, you can modify the following:

- Failed Logins Before Lockout—Displays the number of failed login attempts a user can make before the user is locked out from the node. You can choose a value between 0 and 10.
- Manual Unlock by Superuser—Allows a user with Superuser privileges to manually unlock a user who has been locked out from a node.
- Lockout Duration—Sets the amount of time the user will be locked out after a failed login. You can choose a value between 0 and 10 minutes, and 0 and 55 seconds (in five-second intervals). If you checked Manual Unlock by Superuser, Lockout Duration is disabled.

Step 6 In the Password Change area, you can modify the following:

- Prevent Reusing Last [ ] Passwords—Choose a value between 1 and 10 to set the number of different passwords the user must create before he or she can reuse a password.

- New Password must Differ from the Old Password—Choose the number of characters that must differ between the old and new password. The default number is 1.
- Cannot Change New Password for [ ] days—If checked, prevents users from changing their password for the specified period. The range is 20 to 95 days.
- Require Password Change on First Login to New Account—If checked, requires users to change his or her password the first time they log into the account.

Step 7 To require users to change their password at periodic intervals, check the Enforce Password Aging check box in the Password Aging area. If checked, provision the following parameters:

- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONER, SUPERUSER. The range is 20 to 95 days.
- Warning—Sets the number days the user will be warned to change his or her password for each security level. The range is 2 to 20 days.

Step 8 In the Other area, you can provision the following:

- Single Session Per User**—**If checked, limits users to one login session at one time.
- Disable Inactive User—If checked, disables users who do not log into the node for the period of time specified in the Inactive Duration box. The Inactive Duration range is 45 to 90 days.

Step 9 In the Select Applicable Nodes area, uncheck any nodes where you do not want to apply the changes.

Step 10 Click **OK**.

Step 11 In the Security Policy Change Results dialog box, confirm that the changes are correct, then click **OK**.

Step 12 Return to your originating procedure (NTP).

DLP-C143 Change Node Access and PM Clearing Privilege

Purpose	This task provisions the physical access points and shell programs used to connect to the ONS 15310-CL or ONS 15310-MA and sets the user security level that can clear node performance monitoring data.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 In the Access area, provision the following:

- LAN access—Choose one of the following options to set the access paths to the node:
  - **No LAN Access**—Allows access to the node only through data communications channel (DCC) connections. Access through the TCC2/TCC2P RJ-45 port and backplane is not permitted.
  - **Front only**—Allows access through the TCC2/TCC2P RJ-45 port. Access through the DCC and the backplane is not permitted.

  - **Backplane only**—Allows access through DCC connections and the backplane. Access through the TCC2/TCC2P RJ-45 port is not allowed.
  - **Front and Backplane**—Allows access through DCC, TCC2/TCC2P RJ-45, and backplane connections.
- Restore Timeout—Sets a time delay for enabling of front and backplane access when DCC connections are lost and "DCC only" is chosen in LAN Access. Front and backplane access is enabled after the restore timeout period has passed. Front and backplane access is disabled as soon as DCC connections are restored.

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

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

Step 4 In the TL1 Access area, select the desired level of TL1 access. Disabled completely disables all TL1 access; Non-Secure allows telnet access through ports 2361, 3082 and 3083; Secure allows SSH access through port 4083.

Step 5 In the PM Clearing Privilege field, choose the minimum security level that can clear node PM data: PROVISIONING or SUPERUSER.

Step 6 Select the Enable Craft Port check box to turn on the shelf controller serial ports.

Step 7 Select the EMS access state from the list. Available states are Non-secure (allows access using IIOP and HTTP), and Secure (allows access using SSLIOP and HTTPS).

In the TCC CORBA (IIOP/SSLIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Uses Port 57790 (non-secure IIOP port) and Port 57791 (secure SSLIOP port) to connect to ONS 15454s on the same side of the firewall or if no firewall is used (default). This option can be used for access through a firewall if Port 57790 or Port 57791 is open. 57790 is the non-secure IIOP port, 57791 is the secure SSLIOP port.
- **Standard Constant**—Uses Port 683 (IIOP) or Port 684 (SSLIOP), the Common Object Request Broker Architecture (CORBA) default port number.
- **Other Constant**—If the default port is not used, type the Internet Inter-ORB Protocol (IIOP) or SSLIOP port specified by your firewall administrator.

Step 8 In the SNMP Access area, set the Simple Network Management Protocol (SNMP) access state to Non-Secure or Disabled (disables SNMP access).

Step 9 Click **Apply**.

Step 10 Return to your originating procedure (NTP).

DLP-C144 Change User Password and Security Settings on a Single Node

Purpose	This task changes settings for an existing user at one node.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C37 Create a New User on a Single Node, page 17-51
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Click the user whose settings you want to modify.

Step 3 Click **Change**.

Step 4 In the Change User dialog box, you can:

- Change a user password
- Modify the user security level
- Lock out or disable the user

See the "DLP-C37 Create a New User on a Single Node" task on page 17-51 for field descriptions.

Step 5 Click **OK**.

Note User settings that you changed during this task will not appear until that user logs off and logs back in.

Step 6 Return to your originating procedure (NTP).

DLP-C145 Change User Password and Security Settings on Multiple Nodes

Purpose	This task changes settings for an existing user on multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C38 Create a New User on Multiple Nodes, page 17-52
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note You must add the same user name and password to each node the user will access.

Step 1 From the View menu, choose **Go to Network View**. Verify that you can access all the nodes where you want to add users.

Step 2 Click the **Provisioning > Security > Users** tabs. Click the user's name whose settings you want to change.

Step 3 Click **Change**. The Change User dialog box appears.

Step 4 In the Change User dialog box, you can:

- Change a user password
- Modify the user security level
- Lock out or disable the user

See the "DLP-C38 Create a New User on Multiple Nodes" task on page 17-52 for field descriptions.

Step 5 Click **OK**. A Change Results confirmation dialog box appears.

Step 6 Click **OK** to acknowledge the changes.

Step 7 Return to your originating procedure (NTP).

DLP-C146 Delete a User on a Single Node

Purpose	This task deletes an existing user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-C148 Log Out a User on a Single Node" task on page 18-52.

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

Step 2 Choose the user you want to delete.

Step 3 In the Delete User dialog box, complete the following:

a. To log the user out before the deleting the user, check **Logout before delete**.

b. Click **OK**.

Step 4 In the User Deletion Results dialog box, click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-C147 Delete a User on Multiple Nodes

Purpose	This task deletes an existing user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Note CTC will allow you to delete other Superuser IDs if one Superuser ID remains. For example, you can delete the CISCO15 user if you have created another Superuser ID. Use this option with caution.

Note Users who are logged in when you delete them will not be logged out. The delete user action will take effect after the user logs out. To log out a user who is currently logged in, complete the "DLP-C149 Log Out a User on Multiple Nodes" task on page 18-53.

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

Step 2 Click the **Provisioning > Security > Users** tabs. Click the name of the user you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete User dialog box, complete the following:

a. To log the user out before the deleting the user, check **Logout before delete**.

b. Click **OK**.

Step 5 In the User Deletion Results dialog box, click **OK**.

Step 6 Return to your originating procedure (NTP).

DLP-C148 Log Out a User on a Single Node

Purpose	This task logs out a user from a single node.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 2 Choose the user you want to log out and click **Logout**.

Step 3 In the Logout User dialog box, check **Lockout before Logout** if you want to prevent the user from logging in after logout. User lockout parameters provisioned in the Policy tab determine when the user can log back in. A user is locked out for the amount of time specified in the Lockout Duration field unless a Superurser manually unlocks the lockout. See the "DLP-C141 Change the Security Policy on a Single Node" task on page 18-46 for more information.

Step 4 Click **OK**.

Step 5 Click **Yes** to confirm the logout.

Step 6 Return to your originating procedure (NTP).

DLP-C149 Log Out a User on Multiple Nodes

Purpose	This task logs out a user from multiple nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Step 1 From the view menu, choose **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 prevent the user from logging in after logout. User lockout parameters provisioned in the Policy tab determine when the user can log back in. A user is locked out for the amount of time specified in the Lockout Duration field unless a Superurser manually unlocks the lockout. See the "DLP-C141 Change the Security Policy on a Single Node" task on page 18-46 for more information.

Step 7 Click **OK**.

Step 8 Click **Yes** to confirm the logout.

Step 9 Return to your originating procedure (NTP).

DLP-C150 Modify SNMP Trap Destination

Purpose	This task modifies the SNMP trap destinations on an ONS 15310-CL or ONS 15310-MA including community name, default UDP port, and SNMP trap version.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the trap that you want to modify in the Trap Destinations dialog box.

For a description of SNMP traps, refer to the "SNMP" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Step 3 In the Selected Destination area, you can modify the following:

- Community
- UDP port
- Trap version (SNMPv1 or SNMPv2)

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15310-CL or ONS 15310-MA is case-sensitive and must match the community name of the NMS.

Note The default UDP port for SNMP is 162.

Note Refer to your NMS documentation to determine which trap version to use.

Step 4 If you want to allow the ONS 15310-CL or ONS 15310-MA SNMP agent to accept SNMP SET requests on certain MIBs, check the **Allow SNMP Sets** check box. If the box is not checked, SET requests are rejected.

Step 5 If you want to set up the SNMP proxy feature to allow network management, message reporting, and performance statistic retrieval across firewalls, check the **Allow SNMP Proxy** check box.

Step 6 Click **Apply**. SNMP settings are now configured.

Step 7 To view SNMP information for each node, click the node IP address in the Trap Destinations area of the Trap Destinations screen.

Step 8 Return to your originating procedure (NTP).

DLP-C151 Delete SNMP Trap Destinations

Purpose	This task deletes SNMP trap destinations on an ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Trap Destinations list, click the trap you want to delete.

Step 3 Click **Delete**. A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 Return to your originating procedure (NTP).

DLP-C152 Change a Section DCC Termination

Purpose	This task modifies a SONET data communications channel (SDCC). You can also enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Provisioning or higher

Step 1 In node view, 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, Open Shortest Path First 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-C153 Change a Line DCC Termination

Purpose	This task modifies a line data communications channel (LDCC). You can also enable or disable OSPF and enable or disable the foreign node setting.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	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, Open Shortest Path First 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-C154 Delete a Section DCC Termination

Purpose	This task deletes a SONET Section DCC termination on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the SDCC termination that you want to delete and click **Delete**. The Delete SDCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-C155 Delete a Line DCC Termination

Purpose	This task deletes a SONET Line DCC termination on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	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 In node view, click the **Provisioning > Comm Channels > LDCC** tabs.

Step 2 Click the LDCC termination that you want to delete and click **Delete**. The Delete LDCC Termination dialog box appears.

Step 3 Click **Yes** in the confirmation dialog box.

Step 4 Return to your originating procedure (NTP).

DLP-C156 Delete a Provisionable Patchcord

Purpose	This task deletes a provisionable patchcord.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	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 > PPCs** tabs. If you are in network view, click **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-C163 Check the Network for Alarms and Conditions

Purpose	This task verifies that no alarms or conditions exist on the network.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Remote
Security Level	Retrieve or higher

Step 1 From the View menu, choose **Go to Network View**. Verify that all affected spans on the network map are green.

Step 2 Verify that the affected spans do not have active switches on the network map. Span ring switches are graphically displayed on the span with the letters “L” for lockout ring, “F” for FORCE ring, “M” for MANUAL ring, and “E” for EXERCISE ring.

Step 3 A second verification method can be performed from the Conditions tab. Click **Retrieve Conditions** and verify that no switches are active. Make sure the Filter button is not selected.

Step 4 Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, AIS-P, SF, and SD. Make sure the Filter button is not selected.

If trouble is indicated (for example, a major alarm exists), resolve the problem before proceeding. See Chapter 9, “Manage Alarms,” or, if necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

Step 5 Return to your originating procedure (NTP).

DLP-C164 Manually Route a Path Protection Circuit in a Topology Upgrade

Purpose	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 configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 NTP-C96 Convert an Unprotected Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the Circuit Routing Preferences area of the Uprotected 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-C165 Automatically Route a Path Protection Circuit in a Topology Upgrade

Purpose	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 configuration.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 NTP-C96 Convert an Unprotected Point-to-Point or Linear ADM to a Path Protection Configuration Automatically, page 13-6
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Check **Review Route Before Creation** if you want to review and edit the circuit route before the circuit is created.

Step 2 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 3 If you selected Review Route Before Creation, complete the following substeps. If not, continue with Step 4.

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 4 Click **Finish**.

Step 5 Return to your originating procedure (NTP).

DLP-C166 Initiate a Path Protection Force Switch on a Span

Purpose	This task switches all circuits on a path protection span to another span.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Caution Traffic is not protected during Force path protection switches.

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

Step 2 Right-click the span where you want to Force switch path protection traffic. Choose **Circuits** from the shortcut menu.

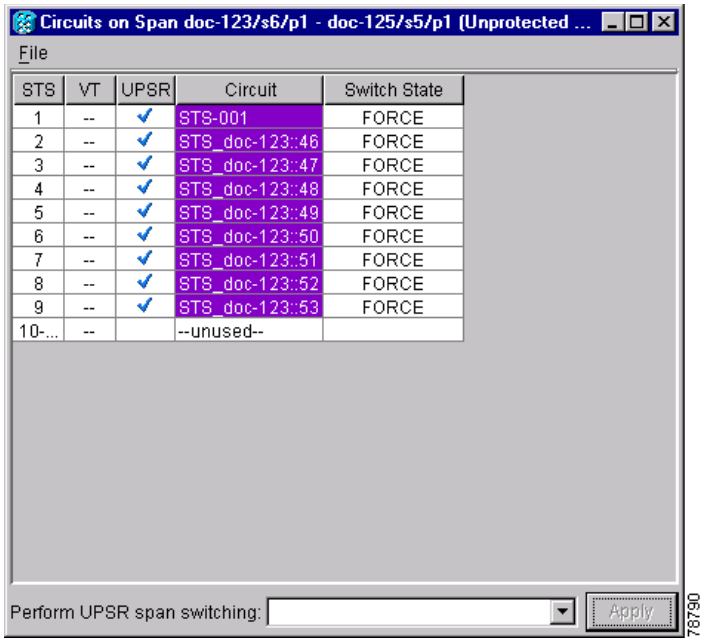
Step 3 In the Circuits on Span dialog box, choose **FORCE SWITCH AWAY**. Click **Apply**.

Step 4 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all circuits is FORCE. Figure 18-7 shows an example.

Figure 18-7 Circuits on Span Dialog Box with a Force Switch



Note A Force switch request on a span or card causes CTC to raise a FORCED-REQ condition. The condition clears when you clear the Force switch; it is informational only.

Step 6 Return to your originating procedure (NTP).

DLP-C167 Clear a Path Protection Force Switch

Purpose	This task clears a path protection Force switch.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.

Step 3 In the Circuits on Span dialog box, choose **CLEAR** to remove the switch. Click **Apply**.

Step 4 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 5 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span window, the Switch State for all path protection circuits is CLEAR.

Step 6 Return to your originating procedure (NTP).

DLP-C168 Verify Pass-Through Circuits

Purpose	This task verifies that circuits passing through a node that will be removed enter and exit the node on the same STS and/or VT.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In the CTC Circuits window, choose a circuit that passes through the target node and click **Edit**.

Step 2 In the Edit Circuits window, check **Show Detailed Map**.

Step 3 Verify that the STS and VT mapping on the node's east and west ports are the same. For example, if a circuit mapping on the west port s5/p1-1/S1 (Slot 5, Port 1-1, STS 1), verify that the mapping is STS 1 on the east port. If the circuit appears different STSs and/or VTs on the east and west ports, write down the name of the circuit.

Step 4 Repeat Steps 1 through 3 for each circuit displayed in the Circuits tab.

Delete and recreate each circuit recorded in Step 3 that entered/exited the node on different STSs. To delete the circuit, complete the "DLP-C115 Delete Circuits" task on page 18-21. To create circuits, complete the appropriate procedures in Chapter 6, "Create Circuits and VT Tunnels."

Step 5 Return to your originating procedure (NTP).

DLP-C169 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

Purpose	This task reinitializes the ONS 15310-CL or the ONS 15310-MA using the CTC reinitialization tool on a Windows computer. Reinitialization uploads a new software package to the 15310-CL-CTX (on the ONS 15310-CL) or CTX2500 (ONS 15310-MA) card, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15310-CL System Software CD, Version 8.5.x ONS 15310-MA System Software CD, Version 8.5.x Java Runtime Environment (JRE) 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitializtion tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2 NTP-C13 Set Up Computer for CTC, page 3-2 One of the following: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3 • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

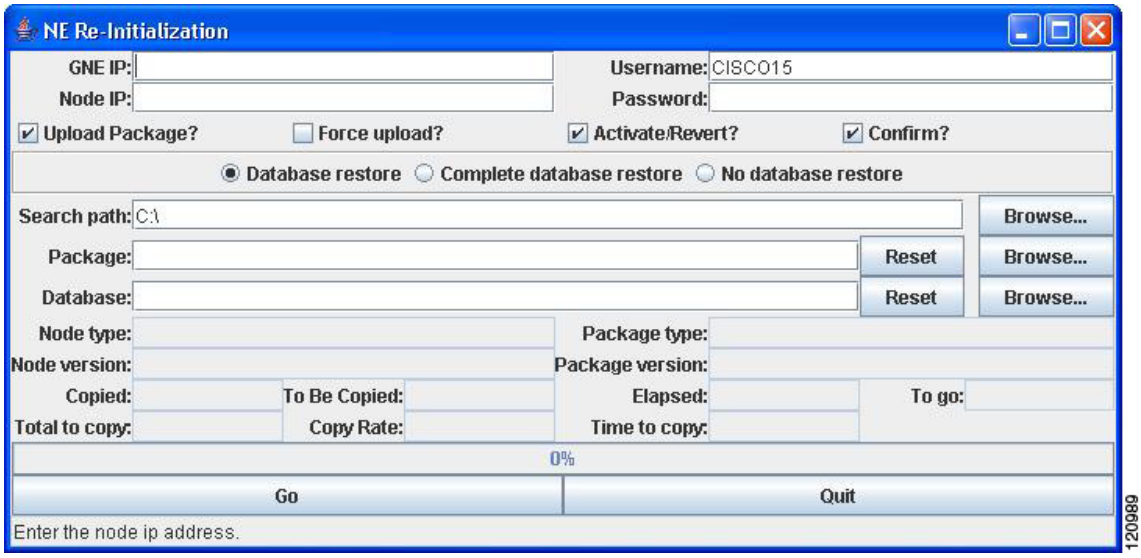
Step 1 Insert the ONS 15310-CL System Software CD, Version 8.5.x into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 From the Windows Start menu, choose **Run.** In the Run dialog box, click **Browse** and navigate to the CISCO15310 folder on the software CD.

Step 3 In the Browse dialog box Files of Type field, choose **All Files**.

Step 4 Choose the RE-INIT.jar file and click **Open**. The NE Re-Initialization window appears (Figure 18-8).

Figure 18-8 Reinitialization Tool in Windows



Step 5 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a gateway network element (GNE), enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tab.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Database restore—Check this box if you want to send a new database to the node and to restore node provision values. (This is equivalent to the CTC database restore with the "Complete Database" check box unchecked.)
- Complete database restore—Check this option to send a new database to the node and to restore node provision and system values. (This is equivalent to the CTC database restore with the "Complete Database" check box checked.)
- No database restore—Check this box if you do not want the node database to be modified.
- Search Path—Enter the path to the CISCO15310 folder on the CD drive.

Step 6 Click **Go**.

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

Step 7 Review the information on the Confirm NE Re-Initialization dialog box, then click **Yes** to start the reinitialization.

The reinitialization begins. After the software is downloaded and activated, and the database is uploaded to the 15310-CL-CTX card, "Complete" appears in the status bar and the 15310-CL-CTX (CL) or CTX2500 (MA) card will reboot. Wait a few minutes for the reboot to complete.

Step 8 After the reboot is complete, log into the node using "DLP-C29 Log into CTC" task on page 17-44.

Step 9 Manually set the node name and network configuration to site-specific values. See the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 and the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 for information on setting the node name, IP address, subnet mask and gateway, and IIOP port.

Step 10 Return to your originating procedure (NTP).

DLP-C170 Use the Reinitialization Tool to Clear the Database and Upload Software (UNIX)

Purpose	This task reinitializes the ONS 15310-CL or ONS 15310-MA using the CTC reinitialization tool on a UNIX computer. Reinitialization uploads a new software package to the 15310-CL-CTX or CTX2500 card, clears the node database, and restores the factory default parameters.
Tools/Equipment	ONS 15310-CL System Software CD, Version 8.5.x or ONS 15310-MA System Software CD, Version 8.5.x JRE 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitializtion tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
Prerequisite Procedures	NTP-C102 Back Up the Database, page 15-2 NTP-C13 Set Up Computer for CTC, page 3-2 One of the following: • NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3 • NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

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

Step 1 Insert the system software CD into the computer CD-ROM drive. If the CTC Installation Wizard appears, click **Cancel**.

Step 2 To find the recovery tool file, go to the CISCO15310 directory on the CD (usually /cdrom/cdrom0/CISCO15310).

Step 3 If you are using a file explorer, double-click the **RE-INIT.jar** file. If you are working with a command line, run **java -jar RE-INIT.jar**. The NE Re-Initialization window appears (Figure 18-8 on page 18-64).

Step 4 Complete the following fields:

- GNE IP—If the node you are reinitializing is accessed through another node configured as a GNE, enter the GNE IP address. If you have a direct connection to the node, leave this field blank.
- Node IP—Enter the node name or IP address of the node that you are reinitializing.
- User ID—Enter the user ID needed to access the node.
- Password—Enter the password for the user ID.
- Upload Package—Check this box to send the software package file to the node. If unchecked, the software stored on the node is not modified.
- Force Upload—Check this box to send the software package file to the node even if the node is running the same software version. If unchecked, reinitialization will not send the software package if the node is already running the same version.
- Activate/Revert—Check this box to activate the uploaded software (if the software is a later than the installed version) or revert to the uploaded software (if the software is earlier than the installed version) as soon as the software file is uploaded. If unchecked, the software is not activated or reverted after the upload, allowing you to initiate the functions later from the node view Maintenance > Software tab.
- Confirm—Check this box if you want a warning message displayed before any operation is performed. If unchecked, reinitialization does not display a warning message.
- Database restore—Check this box if you want to send a new database to the node and to restore node provision values. (This is equivalent to the CTC database restore with the "Complete Database" check box unchecked.)
- Complete database restore—Check this option to send a new database to the node and to restore node provision and system values. (This is equivalent to the CTC database restore with the "Complete Database" check box checked.)
- No database restore—Check this box if you do not want the node database to be modified.
- Search Path—Enter the path to the CISCO15310 folder on the CD drive.

Step 5 Click **Go**.

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

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

The reinitialization begins. After the software is downloaded and activated and the database is uploaded to the 15310-CL-CTX or CTX2500 card, “Complete” appears in the status bar and the 15310-CL-CTX or CTX2500 card will reboot. Wait a few minutes for the reboot to complete.

Step 7 After the reboot is complete, log into the node using DLP-C29 Log into CTC, page 17-44.

Step 8 Manually set the node name and network configuration to site-specific values. See the "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 and "NTP-C20 Set Up Name, Date, Time, and Contact Information" procedure on page 4-4 for information on setting the node name, IP address, subnet mask and gateway, and IIOP port.

Step 9 Return to your originating procedure (NTP).

DLP-C171 Apply a Lock-on

Purpose	This task prevents traffic from being switched from one port to another.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Note For a 1+1 optical protection group, only the working port can be placed in the lock on state.

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

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock on.

Step 3 If you determine that the protect port is in standby mode and you want to apply the lock on to the protect port, make the protect port active:

a. In the Selected Group list, click the protect port.

b. In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active port where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

The lock-on has been applied and traffic cannot be switched to the working port. To clear the lock on, see the "DLP-C173 Clear a Lock-on or Lockout" task on page 18-68.

Step 7 Return to your originating procedure (NTP).

DLP-C172 Apply a Lockout

Purpose	This task switches traffic from one port to another using a lockout, which is a switching mechanism that overrides other manual switching connections (Force or Manual).
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

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

Note For a 1+1 optical protection group, only the protect port can be locked out.

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

Step 2 In the Protection Groups list, click the protection group that contains the port you want to lock out.

Step 3 In the Selected Group list, click the port where you want to lock out traffic.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The Lock Out has been applied and traffic is switched to the opposite port. To clear the lockout, see the "DLP-C173 Clear a Lock-on or Lockout" task on page 18-68.

Note Provisioning a lockout raises a LOCKOUT-REQ or an FE-LOCKOUTOFPR condition in CTC. Clearing the lockout switch request clears these conditions.

Step 6 Return to your originating procedure (NTP).

DLP-C173 Clear a Lock-on or Lockout

Purpose	This task clears a lock on or lockout.
Tools/Equipment	None
Prerequisite Procedures	DLP-C171 Apply a Lock-on, page 18-67 or DLP-C172 Apply a Lockout, page 18-68
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

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

Step 2 In the Protection Groups list, click the protection group that contains the port you want to clear.

Step 3 In the Selected Group list, click the port you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock on or lockout is cleared.

Step 6 Return to your originating procedure (NTP).

DLP-C174 Clean Multi Fiber-Optic Cable Connectors

Purpose	This task cleans the multi fiber optic connectors
Tools/Equipment	Cleaning Cartridge for multi fiber optic connectors
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments.** Statement 1051

Step 1 Remove the protective cap on the optical fiber cable connector.

Step 2 Read the manufacturer (cleaning cartridge) instructions to insert the connector into the cleaning cartridge.

Step 3 Slide the lever on the cartridge to swipe the connector surface.

Step 4 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean.

Step 5 Return to your originating procedure (NTP).

DLP-C175 Clean Fiber Connectors with CLETOP

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

Step 1 Remove the dust cap from the fiber connector.

Step 2 Press the lever down to open the shutter door. Each time you press the lever, you expose a clean wiping surface.

Step 3 Insert the connector into the CLETOP cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.

Step 4 Use an inspection microscope to inspect each fiber connector for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 1 through 3.

Step 5 Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.

Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry lint free wipe and the inside of the dust cap using a CLETOP stick swab (14100400).

Step 6 Return to your originating procedure (NTP).

DLP-C176 Clean the Fiber Adapters

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

Step 1 Remove the dust plug from the fiber adapter.

Step 2 Insert a CLETOP stick swab (14100400) into the adapter opening and rotate the swab.

Step 3 Place dust plugs on the fiber adapters when not in use.

Step 4 Return to your originating procedure (NTP).

DLP-C177 Manual or Force Switch the Node Timing Reference

Purpose	This task commands the node to switch to the timing reference that you have selected if the synchronization status message (SSM) quality of the reference is not less than the quality of the reference that the node is currently running.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Timing > Source** tabs. The Timing Source window appears.

Step 2 Click the Reference drop-down list for the desired Clock, and choose the desired reference.

Step 3 Click the Operation drop-down list for the desired Clock, and choose one of the following options:

- **Manual**—This operation commands the NE to switch to the reference you have selected, if the SSM quality of the reference is not less than the quality of the reference that the node is currently running.
- **Force**—This operation commands the NE to switch to the reference you have selected, regardless of the SSM quality, if the reference is valid.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box.

- If the selected timing reference is invalid, a warning dialog appears. Click **OK**; the NE remains on the original timing reference without performing the switch.
- If the selected timing reference is an acceptable valid reference, the NE switches to the selected timing reference.

Step 6 Return to your originating procedure (NTP).

DLP-C178 Clear a Manual or Force Switched Node Timing Reference

Purpose	This task clears a Manual or Force switch on a node timing reference and reverts the timing reference to its provisioned reference.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

Step 1 In node view, click the **Maintenance > Timing > Source** tabs. The Timing Source window appears.

Step 2 Find the Clock reference that is currently set to Manual or Force in the Operation drop-down list.

Step 3 Click the Operation drop-down list for the clock and choose **Clear**.

Step 4 Click **Apply**.

Step 5 Click **Yes** in the confirmation dialog box.

- If the normal timing reference is invalid or has failed, a warning dialog appears. Click **OK**; the NE remains on the previous timing reference without performing the switch.
- If the normal timing reference is an acceptable valid reference, the NE reverts to the normal timing reference as defined by the system configuration.

Step 6 Return to your originating procedure (NTP).

DLP-C179 Initiate an Optical Protection Switch

Purpose	This procedure initiates a Manual or Force switch on an optical port.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Maintenance or higher

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

Step 2 In the Protection Groups area, select the protection group that you want to switch.

Step 3 In the Selected Group area, select the card and port that 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 (SD) bit error rate (BER) threshold. A Force switch will switch traffic even if the path has SD or signal fail (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-C180 Change a VCAT Member Service State

Purpose	This task changes a VCAT member service state on the Edit Circuit window.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 VCAT circuits must exist on the network. See Chapter 6, "Create Circuits and VT Tunnels" for circuit creation procedures.
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

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

Step 3 Click the **Members** tab.

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

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

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

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

- IS—Puts the member cross-connects in the IS-NR service state.
- OOS,DSBLD—Puts the member cross-connects in the OOS-MA,DSBLD service state. Traffic is not passed on the circuit.
- IS,AINS—Puts the member cross-connects in the OOS-AU,AINS service state and suppresses alarms and conditions. When the connections receive a valid signal, the service state automatically changes to IS-NR.
- OOS,MT—Puts the member cross-connects in the OOS-MA,MT service state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS,MT for circuit testing or to suppress circuit alarms temporarily. Change the administrative state to IS; IS,AINS; or OOS,DSBLD when testing is complete.
- OOS,OOG—(LCAS and Sw-LCAS VCAT only.) Puts VCAT member cross-connects in the Out-of-Service and Management, Out-of-Group (OOS-MA,OOG) service state. This administrative state is used to put a member circuit out of the group and to stop sending traffic.

Step 7 Click **Apply**.

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

Step 9 Return to your originating procedure (NTP).

DLP-C181 Install the LAN Cable for CTC Interface

Purpose	This task installs the LAN cable to provide a 10/100 Mbps Ethernet interface for CTC/TL1 provisioning.
Tools/Equipment	CAT-5 RJ-45 cable
Prerequisite Procedures	NTP-C2 Install the Shelf Assembly, page 1-4
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug one end of the LAN cable into the LAN port on the front of the ONS 15310-CL (Figure 17-9 on page 17-12).

Step 2 Connect the other end to the PC you want to use to access CTC.

Table 18-8 shows the LAN cable pin assignments.

Table 18-8 LAN Cable Pin Assignments

RJ-45 Pin Number	Function
1	TX +
2	TX –
3	RX +
4	NC
5	NC
6	RX –
7	NC
8	NC

Step 3 Return to your originating procedure (NTP).

DLP-C182 Turn On and Verify AC Office Power

Purpose	This task verifies the chassis LED activity and verifies power on the AC ONS 15310-CL chassis.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5 DLP-C6 Connect AC Office Power to the ONS 15310-CL, page 17-6
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Plug the power cord into an AC wall socket or UPS power supply outlet.

Step 2 Verify the chassis LED activity (Figure 17-9 on page 17-12):

- **a.** The FAIL LED blinks red for 20 to 30 seconds, then turns off.
- **b.** The ALARM LED is off.
- **c.** The PWR LED is green.
- **d.** The SYNC LED is green.

Step 3 If the ONS 15310-CL does not power up, check the voltage at the power source using a voltmeter. The voltage should be 100-240VAC +/–10 percent.

Step 4 Return to your originating procedure (NTP).

DLP-C183 Roll the Source or Destination of One Optical Circuit

Purpose	This task reroutes traffic from one source or destination to another on the same circuit, thus changing the original source or destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the **Circuits** tab.

Step 3 Click the circuit that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.

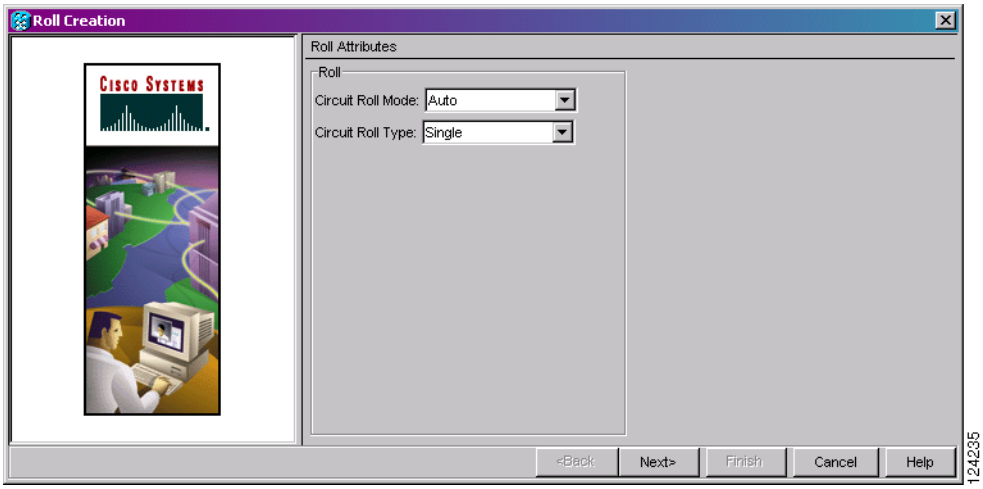
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-9):

- **a.** From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for a 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Single** to indicate that you want to roll one cross-connect on the chosen circuit.

Figure 18-9 Selecting Single Roll Attributes

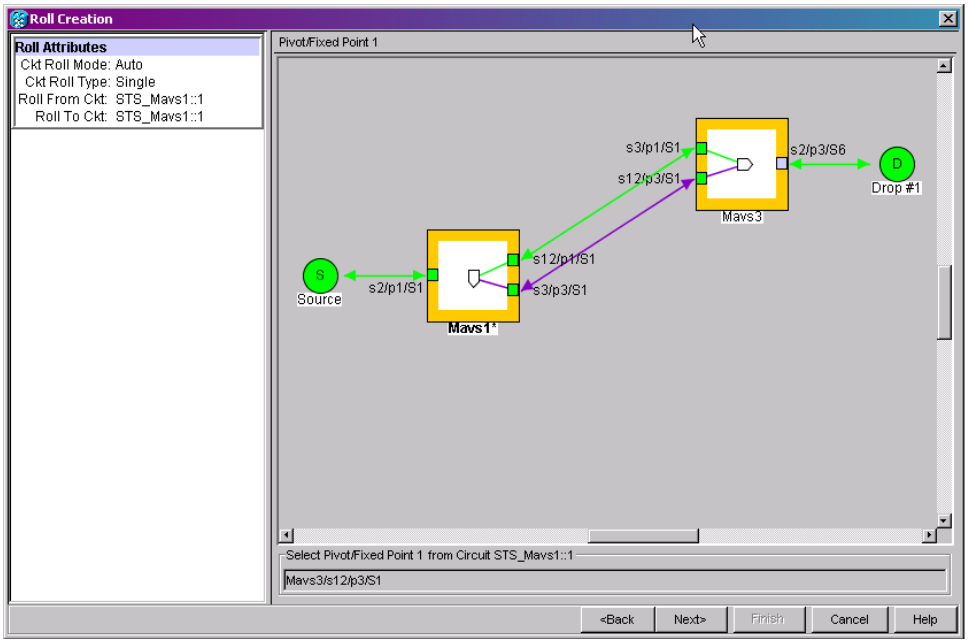


Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square in the graphic image that represents the facility that you want to keep (Figure 18-10).

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

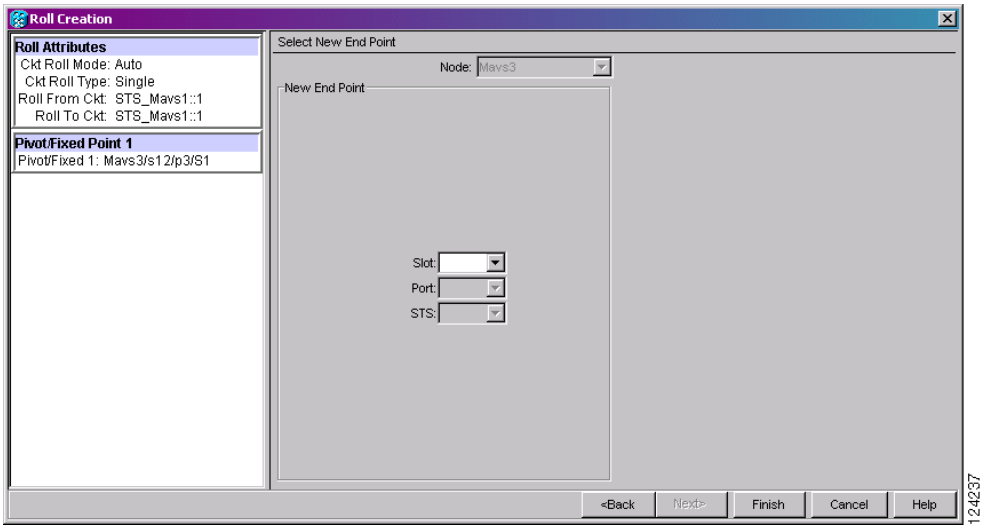
Figure 18-10 Selecting a Path



Step 8 Click **Next**.

Step 9 In the Select New End Point area, choose the **Slot**, **Port**, and **STS** from the drop-down lists to select the Roll To facility (Figure 18-11).

Figure 18-11 Selecting a New Endpoint



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

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

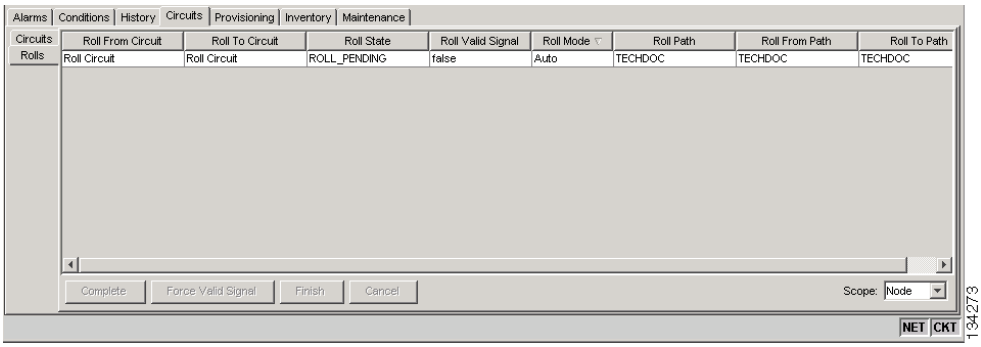
- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a "true" Roll Valid Signal status for a one-way destination roll.

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

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

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

Figure 18-12 Viewing the Rolls Tab



Step 12 If you selected Manual in Step 5, click the rolled facility on the Rolls tab and then click **Complete**. If you selected Auto, continue with Step 13.

Step 13 For both Manual and Auto rolls, click **Finish** to complete the circuit roll process. The roll clears from the Rolls tab and the rolled circuit now appears on the Circuits tab in the DISCOVERED status.

Step 14 Return to your originating procedure (NTP).

DLP-C184 Roll One Cross-Connect from an Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a cross-connect on one circuit onto another circuit resulting in a new destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C52 Provision Section DCC Terminations, page 17-68 for the ports involved in the roll
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the **Circuits** tab.

Step 3 Press **Ctrl** and click the two circuits that you want to use in the roll process.

The circuits must have a DISCOVERED status; in addition, they must be the same size and direction for you to complete a roll. The planned Roll To circuit must not carry traffic.The Roll To facility should be DCC connected to the source node of the Roll To circuit.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

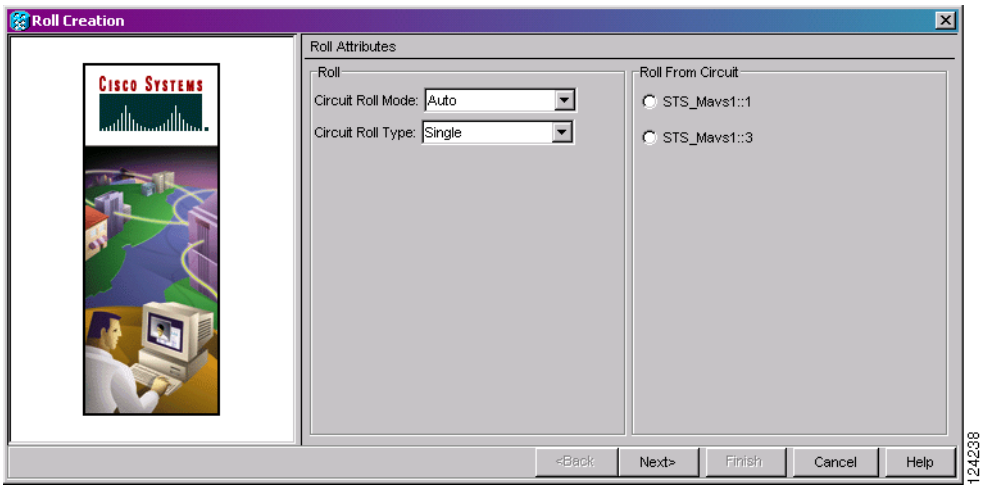
Step 5 In the Roll Attributes area, complete the following (Figure 18-13):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

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

c. In the Roll From Circuit area, click the circuit that contains the Roll From connection.

Figure 18-13 Selecting Roll Attributes for a Single Roll onto a Second Circuit



Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the facility that you want to keep (Figure 18-10 on page 18-76).

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

Step 8 Click **Next**.

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

Step 10 Click **Finish.**

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

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

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- The roll is a one-way destination roll and the Roll Valid Signal is false. It is not possible to get a "true" Roll Valid Signal status for a one-way destination roll.

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

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

Step 12 If you selected Manual in Step 5, click the roll on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 13.

Step 13 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

The roll is cleared from the Rolls tab and the new rolled circuit on Circuits tab returns to the DISCOVERED status.

Step 14 Return to your originating procedure (NTP).

DLP-C185 Roll Two Cross-Connects on One Optical Circuit Using Automatic Routing

Purpose	This task reroutes the network path while maintaining the same source and destination. This task allows CTC to automatically select a Roll To path.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the **Circuits tab**.

Step 3 Click the circuit that has the connections that you want to roll. The circuit must have a DISCOVERED status for you to start a roll.

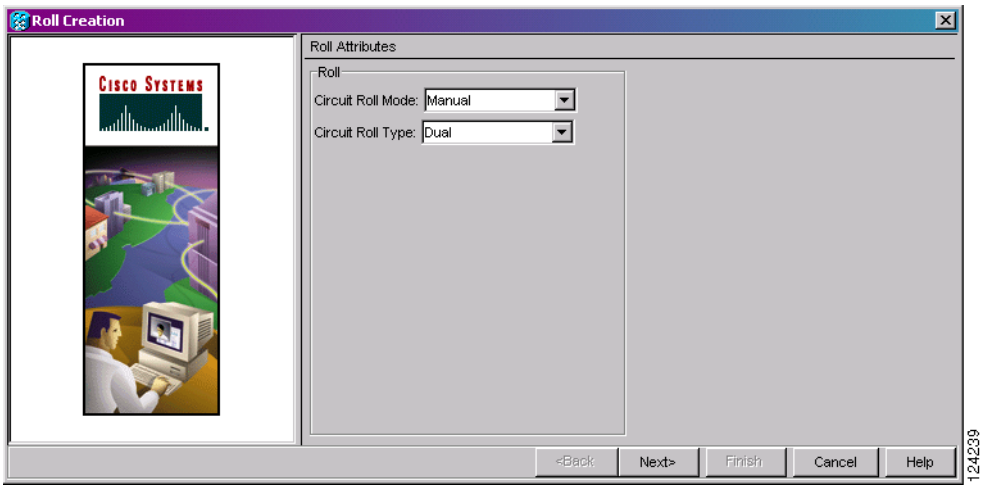
Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-14):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.

b. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Figure 18-14 Selecting Dual Roll Attributes



Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first connection to be rolled (Figure 18-10 on page 18-76).

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

Step 8 Click **Next**.

Step 9 Complete one of the following:

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

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

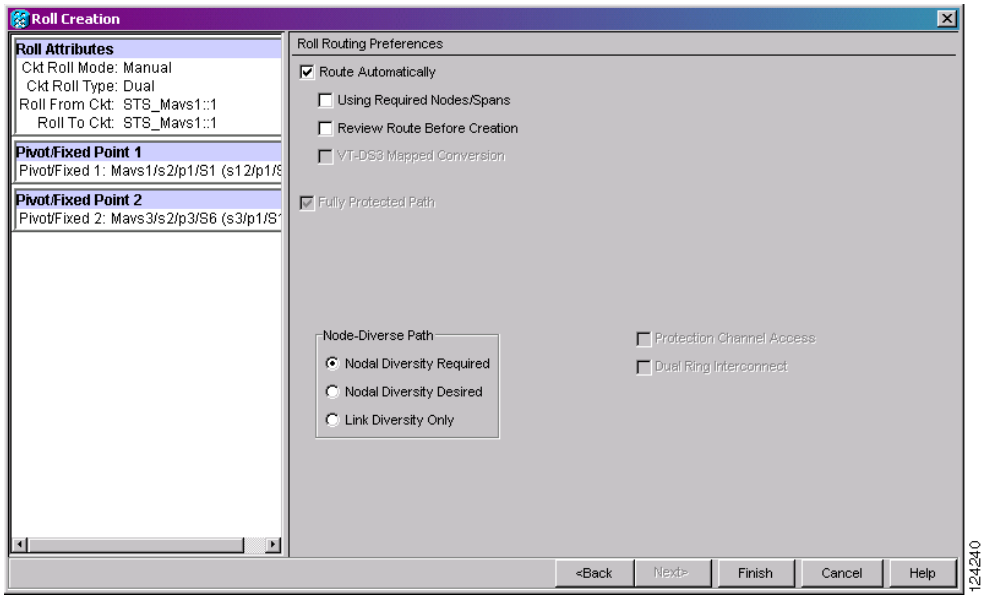
The path that is not selected is the Roll From path. The Roll From path is deleted after the roll is completed. The path identifier appears in the text box below the graphic image.

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, check **Route Automatically** to allow CTC to find the route (Figure 18-15). If you check Route Automatically, the following options are available:

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

Figure 18-15 Setting Roll Routing Preferences



Step 13 To route the circuit over a protected path, check **Fully Protected Path**. (If you do not want to route the circuit on a protected path, continue with Step 14.) CTC creates a primary and alternate circuit route (virtual path protection) based on the following nodal diversity options. Select one of the following choices and follow subsequent window prompts to complete the routing:

- Nodal Diversity Required—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse.
- Nodal Diversity Desired—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.
- Link Diversity Only—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you checked Route Automatically in Step 12:

- If you checked Using Required Nodes/Spans, continue with Step 15.
- If you checked only Review Route Before Creation, continue with Step 16.
- If you did not check Using Required Nodes/Spans or Review Route Before Creation, continue with Step 17.

Step 15 If you checked Using Required Nodes/Spans in Step 12:

a. In the Roll Route Constraints area, click a node or span on the circuit map.

b. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node/span from the circuit. The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction.

c. Repeat Step b for each node or span you wish to include or exclude.

d. Review the circuit route. To change the circuit routing order, select a node in the Required Nodes/Lines or Excluded Nodes Links lists, then click the **Up** or **Down** buttons to change the circuit routing order. Click **Remove** to remove a node or span.

Step 16 If you checked Review Route Before Creation in Step 12:

a. In the Roll Route Review and Edit area, review the circuit route. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

b. If the provisioned circuit does not reflect the routing and configuration you want, click **Back** to verify and change circuit information.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the port mentioned in this statement. If the termination port is the DS-1 port, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS-1 port it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view, Provisioning > Line tabs. On the DS-1 port, Send AIS-V for Ds1 AIS only works for VT circuits.

Step 17 Click **Finish**.

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

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

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. If a valid signal is not found, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

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

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

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

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

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

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

Step 21 Return to your originating procedure (NTP).

DLP-C186 Roll Two Cross-Connects on One Optical Circuit Using Manual Routing

Purpose	This task reroutes a network path of an optical circuit using manual routing.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

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

Step 2 Click the **Circuits tab.**

Step 3 Click the circuit that you want to roll to a new path. The circuit must have a DISCOVERED status for you to start a roll.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following (Figure 18-14 on page 18-81):

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll or **Manual** to create a manual roll.

b. From the Circuit Type drop-down list, choose **Dual** to indicate that you want to roll two connections on the chosen circuit.

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 18-10 on page 18-76).

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

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK**, then click **Next** (Figure 18-15 on page 18-82).
- If multiple Roll From paths do not exist, click **Next** and continue with Step 10. The circuit status for the Roll From path changes from DISCOVERED to ROLL_PENDING.

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

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

Step 11 Click **Next**.

Step 12 In the Circuit Routing Preferences area, uncheck **Route Automatically**.

Step 13 Set the circuit path protection:

- To route the circuit on a protected path, leave **Fully Protected Path** checked and continue with Step 14.
- To create an unprotected circuit, uncheck **Fully Protected Path** and continue with Step 15.

Step 14 If you checked Fully Protected Path, choose one of the following:

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

Step 15 Click **Next**. Beneath Route Review and Edit, node icons appear for you to route the circuit manually.

The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 16 Complete the "DLP-C64 Provision an OC-N Circuit Route" task on page 17-81.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the port mentioned in this statement. If the termination port is the DS-1 port, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS-1 port it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view, Provisioning > Line tabs. On the DS-1 port, Send AIS-V for Ds1 AIS only works for VT circuits.

Step 17 Click **Finish**. In the Circuits tab, verify that a new circuit appears.

This circuit is the Roll To circuit. It is designated with the Roll From circuit name appended with ROLL**.

Step 18 Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 19.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

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

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

Step 19 If you selected Manual in Step 5, click each roll and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 20.

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

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

Step 21 Return to your originating procedure (NTP).

DLP-C187 Roll Two Cross-Connects from One Optical Circuit to a Second Optical Circuit

Purpose	This task reroutes a network path using two optical circuits by allowing CTC to select the Roll To path on the second circuit automatically.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning and higher

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

Step 2 Click the **Circuits** tab.

Step 3 Press **Ctrl** and click the two circuits that you want to use in the roll process.

The Roll From path will be on one circuit and the Roll To path will be on the other circuit. The circuits must have a DISCOVERED status and must be the same size and direction for you to complete a roll. The planned Roll To circuit must not carry traffic.The first Roll To path must be DCC connected to the source node of the Roll To circuit, and the second Roll To path must be DCC connected to the destination node of the Roll To circuit.

Step 4 From the Tools menu, choose **Circuits > Roll Circuit**.

Step 5 In the Roll Attributes area, complete the following:

a. From the Circuit Roll Mode drop-down list, choose **Auto** to create an automatic roll (required for a 1-way source roll) or **Manual** to create a manual roll (required for 1-way destination roll).

b. From the Circuit Roll Type drop-down list, choose **Dual.**

c. In the Roll From Circuit area, click the circuit that contains the Roll From path.

Step 6 Click **Next**.

Step 7 In the Pivot/Fixed Point 1 window, click the square representing the fixed path of the first cross-connect to be rolled (Figure 18-10 on page 18-76).

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

Step 8 Click **Next**.

Step 9 Complete one of the following:

- If multiple Roll From paths exist, the Select Roll From dialog box appears. Select the path from which you want to roll traffic and click **OK** (Figure 18-15 on page 18-82).
- If multiple Roll From paths do not exist, continue with Step 10.

The circuit status for the Roll From path changes from DISCOVERED to ROLL PENDING.

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

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

Step 11 Click **Next**.

Caution The following is only seen with DUAL roll mode when both ends of the circuit use the port mentioned in this statement. If the termination port is the DS-1 port, a roll will occur even if a valid signal is not detected on the Roll To port. The absence of PDI-P downstream for LOS, LOF, and AIS line defects causes the roll to continue without a valid signal. On the DS-1 port it is possible to check the Send AIS-V For Ds1 AIS check box to properly generate PDI-P downstream for the LOS and LOF AIS line defects. This check box is selected from the card view, Provisioning > Line tabs. On the DS-1 port, Send AIS-V for Ds1 AIS only works for VT circuits.

Step 12 Click **Finish**. In the Circuits tab, the Roll From and Roll To circuits change from the DISCOVERED status to ROLL RENDING.

Step 13 Click the **Rolls** tab. Two new rolls now appear on the Rolls tab. For each pending roll, view the Roll Valid Signal status. When one of the following conditions are met, continue with Step 14.

- If the Roll Valid Signal status is true, a valid signal was found on the new port.
- If the Roll Valid Signal status is false, a valid signal was not found. Wait until the signal is found before continuing with the next step. To cancel the roll, see the "DLP-C189 Cancel a Roll" task on page 18-88.
- The roll is a one-way destination roll and the Roll Valid signal status is false. It is not possible to get a Roll Valid Signal status of true for a one-way destination roll.

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

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

Step 14 If you selected Manual in Step 5, click both rolls on the Rolls tab and click **Complete** to route the traffic to the new port. If you selected Auto, continue with Step 15.

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

Step 15 For both manual and automatic rolls, click **Finish** to complete the circuit roll process.

Step 16 Return to your originating procedure (NTP).

DLP-C188 Delete a Roll

Purpose	This task deletes a roll. Use caution when selecting this option, traffic may be affected. Delete a roll only if it cannot be completed or cancelled in normal ways. Circuits may have a PARTIAL status when this option is selected. See Table 18-5 on page 18-13 for a description of circuit statuses.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 NTP-C129 Bridge and Roll Traffic, page 7-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 Click the **Circuits > Rolls** tabs.

Step 3 Click the rolled circuit that you want to delete.

Step 4 From the Tools menu, choose **Circuits > Delete Rolls.**

Step 5 In the confirmation dialog box, click **Yes**.

Step 6 Return to your originating procedure (NTP).

DLP-C189 Cancel a Roll

Purpose	This task cancels a roll. When the roll mode is Manual, you can only cancel a roll before you click the Complete button. When the roll mode is Auto, cancel roll is only allowed before a good signal is detected by the node or before clicking the Force Valid Signal button. A dual or single roll can be cancelled before the roll state changes to ROLL_COMPLETED.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 NTP-C129 Bridge and Roll Traffic, page 7-10
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 1 From the Node or Network view, click the **Circuits > Rolls** tabs.

Step 2 Click the rolled circuit that you want to cancel.

Step 3 Click **Cancel.**

Step 4 Return to your originating procedure (NTP).

DLP-C190 Provision CE-100T-8 Card Ethernet Ports

Purpose	This task provisions the CE-100T-8 card Ethernet ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note The user can provision SONET CCAT or VCAT circuits for the CE-100T-8 card before or after provisioning the card's Ethernet ports or POS ports. See the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34 or the "NTP-C51 Create an Automatically Routed VCAT Circuit" procedure on page 6-46, as needed.

Step 1 In the node view, double-click the CE-100T-8 card graphic to open the card.

Step 2 Click the **Provisioning > Ether Ports** tabs.

Step 3 For each CE-100T-8 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.
- Admin State—Choose **IS** to put the port in service. Putting an Ethernet port into IS-NR also puts the mapped POS port in IS-NR.
- Expected Speed—Choose the expected speed of the device that is or will be attached to the Ethernet port. If you know the speed, choose **100 Mbps** or **10 Mbps** (for CE-100T-8), or **1000 Mbps**, **100 Mbps** to match the attached device. If you do not know the speed, choosing **Auto** enables autonegotiation for the speed of the port, and the CE-100T-8 port will attempt to negotiate a mutually acceptable speed with the attached device. If the expected speed is set to **Auto**, you cannot enable selective autonegotiation.

- Expected Duplex—Choose the expected duplex of the device that is or will be attached to the Ethernet port. If you know the duplex, choose **Full** or **Half** to match the attached device. If you do not know the duplex, choosing **Auto** enables autonegotiation for the duplex of the port, and the CE-100T-8 port will attempt to negotiate a mutually acceptable duplex with the attached device. If the expected duplex is set to **Auto**, you cannot enable selective autonegotiation.
- Enable Selective Auto Negotiation—Click this check box to enable selective autonegotiation on the Ethernet port. If you do not want to enable selective autonegotiation, uncheck the box. If checked, the CE-100T-8 port attempts to autonegotiate only to the selected expected speed and duplex. The link will come up if both the expected speed and duplex of the attached autonegotiating device matches that of the port. You cannot enable selective autonegotiation if either the expected speed or expected duplex is set to **Auto**.
- Enable Flow Control—Click this check box to enable flow control on the port (default). If you do not want to enable flow control, uncheck the box. The CE-100T-8 card attempts to negotiate symmetrical flow control with the attached device.
- 802.1Q VLAN CoS—For a CoS-tagged frame, the CE-100T-8 card can map the eight priorities specified in CoS for either priority or best effort treatment. Any CoS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the CoS is set to 7, which is the highest CoS value. The default results in all traffic being treated as best effort.
- IP ToS—The CE-100T-8 card can also map any of the 256 priorities specified in IP ToS to either priority or best effort treatment. Any ToS class higher than the class specified in CTC is mapped to priority, which is the treatment geared towards low latency. By default, the ToS is set to 255, which is the highest ToS value. This results in all traffic being sent to the best effort queue by default.

Note Untagged traffic is treated as best effort.

Note If traffic is tagged with both CoS and IP ToS, then the CoS value is used, unless the CoS value is 7.

Step 4 Click **Apply**.

Step 5 Refresh the Ethernet statistics:

a. In card view, click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Note Reprovisioning an Ethernet port on the CE-100T-8 card does not reset the Ethernet statistics for that port.

Step 6 Return to your originating procedure (NTP).

DLP-C191 Provision CE-100T-8 Card POS Ports

Purpose	This task provisions CE-100T-8 card POS ports to carry traffic.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note You can provision SONET CCAT or VCAT circuits for the CE-100T-8 card before or after provisioning the card's Ethernet ports or POS ports. See the "NTP-C47 Create an Automatically Routed Optical Circuit" procedure on page 6-34 or the "NTP-C51 Create an Automatically Routed VCAT Circuit" procedure on page 6-46, as needed.

Step 1 In the node view, double-click the CE-100T-8 card graphic to open the card.

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

Step 3 For each CE-100T-8 port, provision the following parameters:

- Port Name—If you want to label the port, enter the port name.
- Admin State—Choose **IS** to put the port in the IS-NR service state. Putting a POS port in IS-NR also puts the mapped Ethernet port in IS-NR.
- Framing Type—Choose **GPF-F** POS framing (the default) or **HDLC** POS framing. The framing type needs to match the framing type of the POS device at the end of the SONET circuit.
- Encap CRC—With GFP-F framing, the user can configure a **32-bit** CRC (the default) or **none** (no CRC). HDLC framing provides a set 32-bit CRC. The CRC should be set to match the CRC of the POS device on the end of the SONET circuit.

Note For more details on the interoperabilty of ONS Ethernet cards, including information on encapsulation, framing, and CRC, refer to the "POS on ONS Ethernet Cards" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Note The CE-100T-8 card use LEX encapsulation, which is the primary POS encapsulation used in ONS Ethernet cards.

Step 4 Click **Apply**.

Step 5 Refresh the POS statistics:

a. In card view, click the **Performance > POS Ports > Statistics** tabs.

b. Click **Refresh**.

Step 6 Return to your originating procedure (NTP).

DLP-C192 Provision a Multirate Pluggable Port Module

Purpose	This task provisions a multirate (OC-3/OC-12/OC-48) PPM in CTC. If a multirate PPM was preprovisioned, skip this procedure and go directly to the "DLP-C193 Provision the Optical Line Rate" task on page 18-92.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Note Multirate PPMs for the ONS 15310-CL support OC-3 and OC-12 line rates. Multirate PPMs for the ONS 15310-MA support OC-3, OC-12, and OC-48 line rates.

Step 1 In node view, double-click the 15310-CL-CTX card (ONS 15310-CL) or the CTX2500 card (ONS 15310-MA).

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

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

Step 4 In the Create PPM dialog box, complete the following:

- PPM—Click the slot number where the SFP is installed from the drop-down list.
- PPM Type—Click the number of ports supported by your SFP from the drop-down list. If only one port is supported, **PPM (1 port)** is the only option.

Step 5 Click **OK**. The newly created port appears in the Pluggable Port Modules area. The row on the Pluggable Port Modules area turns white and the Actual Equipment Type column lists the equipment name.

Step 6 Verify that the PPM appears in the list in the Pluggable Port Modules area. If it does not, repeat Steps 3 through 5.

Step 7 Repeat the task to provision a second PPM.

Step 8 Click **OK**.

Step 9 Continue with the "DLP-C193 Provision the Optical Line Rate" task on page 18-92 to provision the multirate PPM for OC-3 or OC-12.

Step 10 Return to your originating procedure (NTP).

DLP-C193 Provision the Optical Line Rate

Purpose	This task provisions the line rate on the ONS 15310-CL (OC-3 or OC-12) or ONS 15310-MA (OC-3, OC-12, or OC-48) on a multirate PPM. Single-rate PPMs do not need to be provisioned.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C192 Provision a Multirate Pluggable Port Module, page 18-92

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

Note If you plug in a single-rate SFP, the PPM will autoprovision and no further steps are necessary. If you plug in a multirate SFP, you need to provision the PPM and then provision the rate on the PPM tab by following this task. This is the node default behavior, but it can be changed by NE default settings. Refer to the "NTP-C137 Edit Network Element Defaults" procedure on page 15-18.

Step 1 In node view, for the ONS 15310-CL, double-click the 15310-CL-CTX card; for the ONS 15310-MA, double-click the CTX2500 card.

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

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

Step 4 In the Create Port dialog box, complete the following:

- Port—Select the PPM number and port number from the drop-down list. The first number indicates the PPM and the second number indicates the port number on the PPM. For example, the first PPM with one port displays as 1-1 and the second PPM with one port displays as 2-1. The PPM number can be 1 to 4, but the port number is always 1.
- Port Type—Click the type of port from the drop-down list. The port type list displays the supported port rates on your PPM. For the 15310-CL-CTX card, OC-3 (155 Mbps) and OC-12 (622 Mbps) rates are supported. For the CTX2500 in the 15310-MA, OC-3, OC-12, and OC-48 rates are supported.

Step 5 Click **OK**.

Step 6 Repeat Steps 3 through 5 to configure the port rates as needed.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).

DLP-C194 Change the Optical Line Rate

Purpose	This task changes the port rate on a multirate PPM. Multirate PPMs for the ONS 15310-CL support OC-3 and OC-12 line rates. Multirate PPMs for the ONS 15310-MA support OC-3, OC-12, and OC-48 line rates.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C192 Provision a Multirate Pluggable Port Module, page 18-92
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 In node view, double-click the 15310-CL-CTX card or CTX2500 card.

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

Step 3 Click the port with the port rate that you want to change in the Pluggable Ports area. The highlight changes to dark blue.

Step 4 Click **Edit**. The Edit Port Rate dialog box appears.

Step 5 In the Change To field, use the drop-down list to select the new port rate and click **OK**.

Step 6 Click **Yes** in the Confirm Port Rate Change dialog box.

Step 7 Return to your originating procedure (NTP).

DLP-C195 Delete Pluggable Port Modules

Purpose	This task deletes PPM provisioning for SFPs on the ONS 15310-CL or ONS 15310-MA.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44 DLP-C192 Provision a Multirate Pluggable Port Module, page 18-92
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that you can delete the PPM. You cannot delete a port on a PPM if it is in service, part of a protection group, has a communications channel termination in use, is used as a timing source, has circuits, or has overhead circuits. As needed, complete the following procedures and task:

- NTP-C143 Modify or Delete Card Protection Settings, page 11-5
- NTP-C82 Change Node Timing, page 11-6
- NTP-C85 Modify or Delete Communications Channel Terminations and Provisionable Patchcords, page 11-8
- NTP-C71 Modify and Delete Circuits, page 7-3
- NTP-C72 Modify and Delete Overhead Circuits and Server Trails, page 7-4
- DLP-C50 Change the Service State for a Port, page 17-67

Step 2 In node view, for the ONS 15310-CL, double-click the 15310-CL-CTX card; for the ONS 15310-MA, double-click the CTX2500 card.

Step 3 Click the **Provisioning > Pluggable Port Modules** tabs.

Step 4 To delete a PPM and the associated ports:

a. Click the PPM line that appears in the Pluggable Port Modules area. The highlight changes to dark blue.

b. Click **Delete**. The Delete PPM dialog box appears.

c. Click **Yes**. The PPM provisioning is removed from the Pluggable Port Modules area and the Pluggable Ports area.

Step 5 Verify that the PPM provisioning is deleted:

- If the PPM was preprovisioned, CTC shows an empty slot in CTC after it is deleted.

- If the SFP is physically present when you delete the PPM provisioning, CTC transitions to the deleted state, the ports (if any) are deleted, and the PPM is represented as a gray graphic in CTC. The SFP can be provisioned again in CTC, or the equipment can be removed, in which case the removal causes the graphic to disappear.

Step 6 If you need to remove the SFP, complete the "DLP-C17 Remove SFP Connectors" task on page 17-23.

Step 7 Return to your originating procedure (NTP).

DLP-C196 Configure the Node for RADIUS Authentication

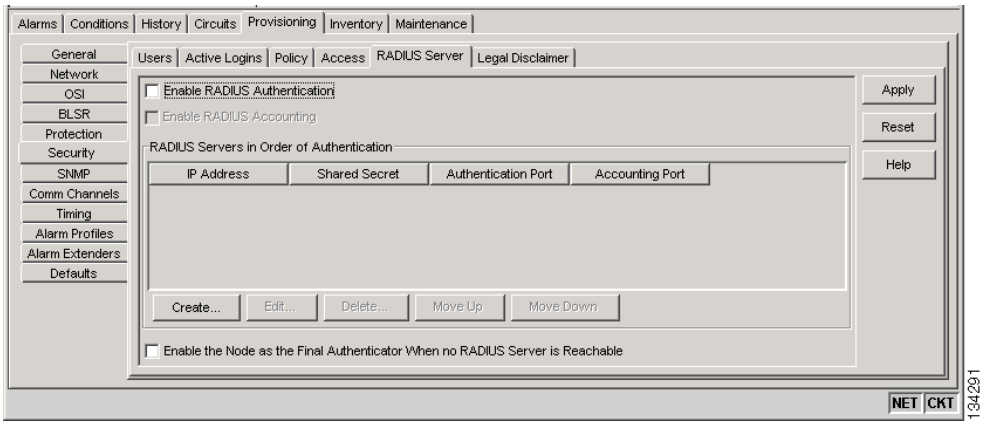
Purpose	This task allows you to configure a node for Remote Authentication Dial In User Service (RADIUS) authentication. RADIUS validates remote users who are attempting to connect to the network.
Tools/Equipment	None
Prerequisite procedures	DLP-C29 Log into CTC, page 17-44 Before configuring the node for RADIUS authentication, you must first add the node as a network device on the RADIUS server. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about configuring a RADIUS server.
Required/As needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only

Caution Do not configure a node for RADIUS authentication until after you have added that node to the RADIUS server and added the RADIUS server to the list of authenticators. If you do not add the node to a RADIUS server prior to activating RADIUS authentication, no user will be able to access the node. Refer to the *User Guide for Cisco Secure ACS for Windows Server* for more information about adding a node to a RADIUS server.

Note The following Cisco vendor-specific attribute (VSA) needs to be specified when adding users to the RADIUS server:
shell:priv-lvl=N, where N is:
0 for Retrieve User
1 for Maintenance User
2 for Provisioning User
3 for Super User.

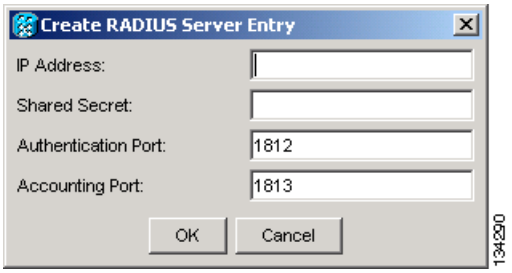
Step 1 In node view, click the **Provisioning > Security > RADIUS Server** tabs (Figure 18-16).

Figure 18-16 RADIUS Server Tab



Step 2 Click **Create** to add a RADIUS server to the list of authenticators. The Create RADIUS Server Entry window appears (Figure 18-17).

Figure 18-17 Create RADIUS Server Entry Window



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

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

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

Step 4 Enter the shared secret in the Shared Secret field. A shared secret is a text string that serves as a password between a RADIUS client and RADIUS server.

Step 5 Enter the RADIUS authentication port number in the Authentication Port field. The default port is 1812. If the node is an ENE, set the authentication port to a number within the range of 1860 to 1869.

Step 6 Enter the RADIUS accounting port in the Accounting Port field. The default port is 1813. If the node is an ENE, set the accounting port to a number within the range of 1870 to 1879.

Step 7 Click **OK**. The RADIUS server is added to the list of RADIUS authenticators.

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

Step 8 Click **Edit** to make changes to an existing RADIUS server. You can change the IP address, the shared secret, the authentication port, and the accounting port.

Step 9 Click **Delete** to delete the selected RADIUS server.

Step 10 Click **Move Up** or **Move Down** to reorder the list of RADIUS authenticators. The node requests authentication from the servers sequentially from top to bottom. If one server is unreachable, the node will request authentication from the next RADIUS server on the list.

Step 11 Click the **Enable RADIUS Authentication** check box to activate remote-server authentication for the node.

Step 12 Click the **Enable RADIUS Accounting** check box if you want to show RADIUS authentication information in the audit trail.

Step 13 Click the **Enable the Node as the Final Authenticator** check box if you want the node to be the final autheticator. This means that if every RADIUS authenticator is unavailable, the node will authenticate the login rather than locking the user out.

Step 14 Click **Apply** to save all changes or **Reset** to clear all changes.

Step 15 Return to your originating procedure (NTP).

DLP-C197 View and Terminate Active Logins

Purpose	This task allows you to view active CTC logins, retrieve the last activity time, and terminate all current logins.
Tools/Equipment	None
Prerequisite Procedures	DLP-C29 Log into CTC, page 17-44
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher for viewing; Superuser for session termination

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

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

Step 2 Click **Logout** to end the session of every logged-in user. This will log out all current users, excluding the initiating Superuser.

Step 3 Click **Retrieve Last Activity Time** to display the most recent activity date and time for users in the Last Activity Time field.

Step 4 Return to your originating procedure (NTP).