



# CHAPTER 17

## DLPs F200 to F299

---

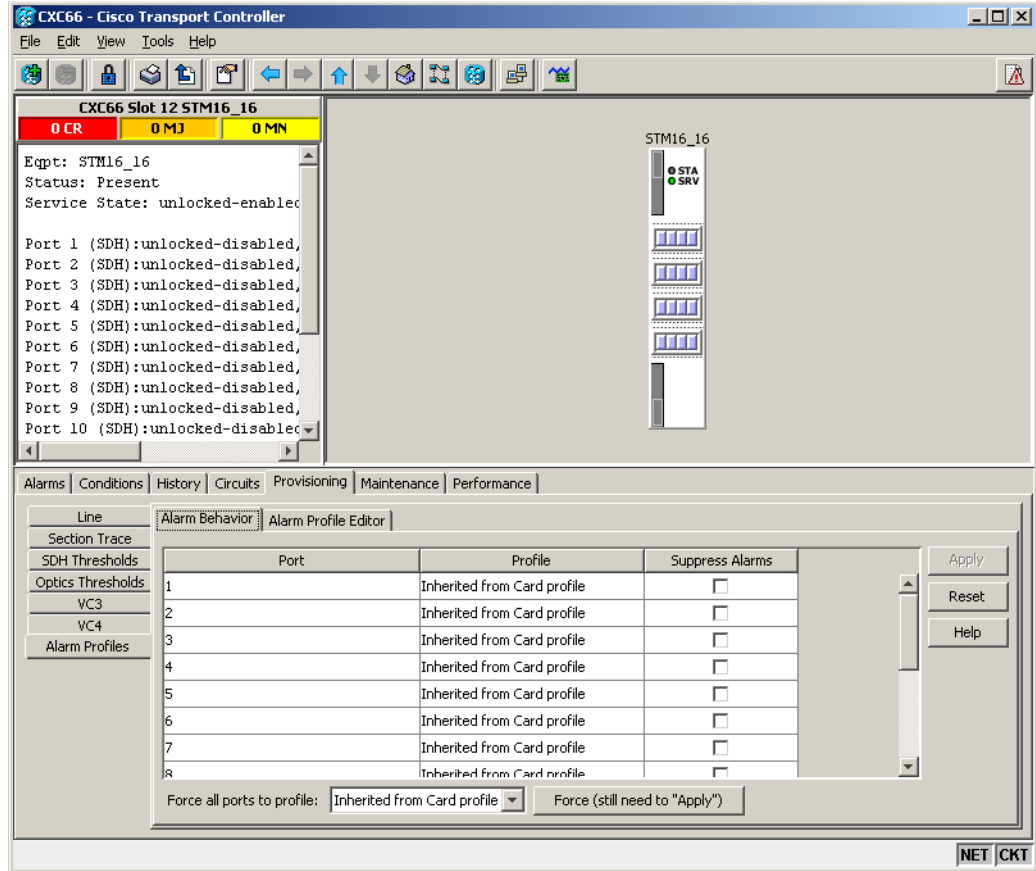
### DLP-F200 Apply Alarm Profiles for Ports and Cards

<b>Purpose</b>	This task applies alarm severity profiles to a port or a card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F199 Create Alarm Severity Profiles, page 16-59</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** In node view, double-click the card graphic.
- Step 2** Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs ([Figure 17-1](#)).

Figure 17-1 Card View Alarm Profiles



**Step 3** To apply alarm profiles on a port-by-port basis:

- Click the specific port row in the Profile column.
- Choose the profile from the drop-down list.  
You can select multiple port profiles.
- Click **Apply**.

**Step 4** To apply a profile for all the ports on a card:

- Click the **Force all ports to profile** drop-down list at the bottom of the window.
- Choose the profile.
- Click **Force (still need to "Apply")**.
- Click **Apply**.



**Tip**

If you choose the wrong profile, click **Reset** to return to the previous profile setting.

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

## DLP-F201 Apply Alarm Profiles to Cards and Nodes

<b>Purpose</b>	This task applies a custom or default alarm profile to cards or nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F199 Create Alarm Severity Profiles, page 16-59</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

**Step 2** To apply a profile to a card:

- Click the Profile column row for the card.
- Choose the profile from the drop-down list.  
You can select multiple profiles for multiple cards.
- Click **Apply**.

**Step 3** To apply the profile to an entire node:

- Click the **Node Profile** drop-down list.
- Choose the profile.
- Click **Apply**.




---

**Tip** If you choose the wrong profile, click **Reset** to return to the previous profile.

---

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

---

## DLP-F202 Suppress Alarm Reporting

<b>Purpose</b>	This task suppresses the reporting of ONS 15600 SDH alarms at the port, card, or node level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Caution**

---

Use alarm suppression with caution. Suppressing alarms in one session suppresses the alarms in all other open CTC and TL1 sessions.

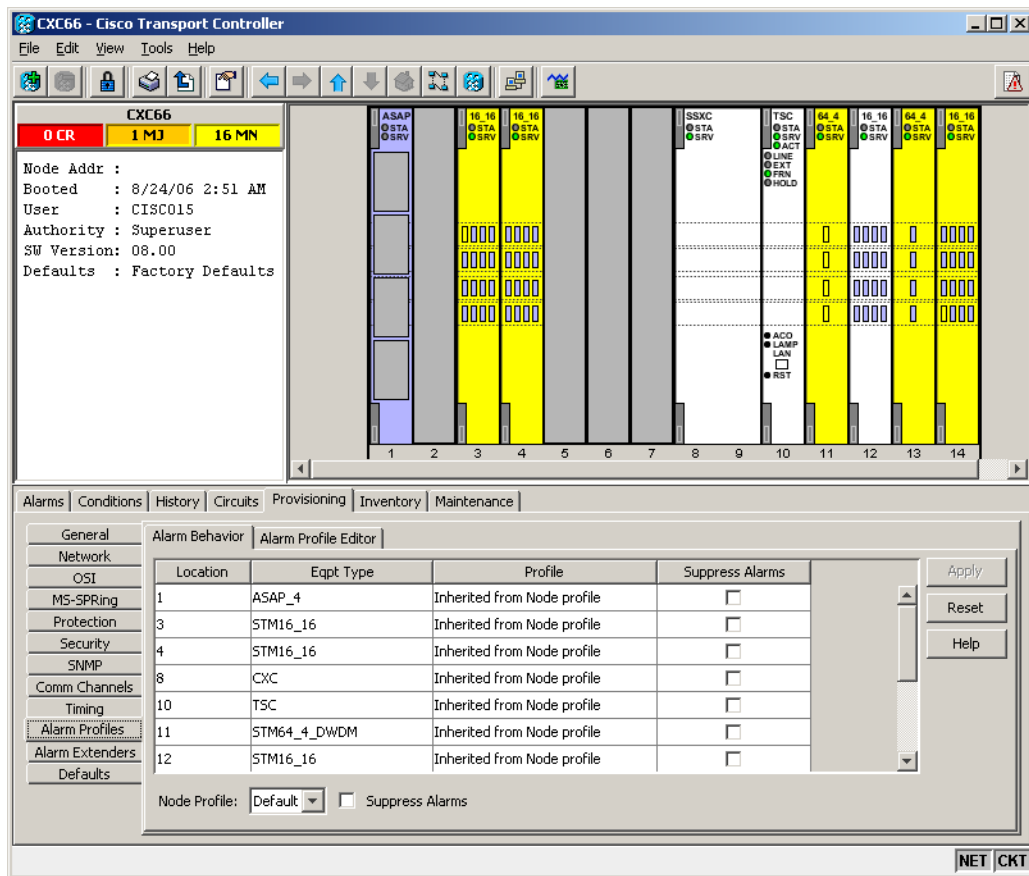
---

**Step 1** In node or card view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs (Figure 17-2).



**Note** Suppressing alarms for a card or node causes the alarms to appear on the CTC Conditions window instead of the Alarms window. The suppressed alarms on the Conditions window appear there with their alarm severities, color codes, and service-affecting status. But as conditions, their severities are overridden as NR severity. Suppressed alarms do not appear on the History window or in the Alarms window of any other clients.

**Figure 17-2 Suppress Alarms Check Box**



**Step 2** To suppress alarms, perform the following action, as needed:

- To suppress alarms for the entire node in the node view, check the **Suppress Alarms** check box next to the Node Profile drop-down list.
- To suppress alarms for a card in the node view, check the **Suppress Alarms** check box for the card you want to suppress.
- To suppress alarms for a port in the card view, check the **Suppress Alarms** check box for ports you want to suppress.

**Step 3** Click **Apply**.

The node sends out autonomous messages to clear any raised alarms.

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

---

## DLP-F203 Restore Alarm Reporting

<b>Purpose</b>	This task removes the alarm suppression command on a port, card, or node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F202 Suppress Alarm Reporting, page 17-3</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** In node view or card view, depending on where the alarms were suppressed, click the **Provisioning > Alarm Profiles > Alarm Behavior** tab.



**Note** Suppressed alarm reporting must be restored in the same view where it was suppressed.

---

**Step 2** In node view, uncheck the **Suppress Alarms** check box next to the Node Profile drop-down list, or uncheck the slot row for a card.

**Step 3** In card view, uncheck the **Suppress Alarms** check box for the ports you want to stop suppressing.

**Step 4** Click **Apply**. The node sends out autonomous messages to raise any actively suppressed alarms.

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

---

## DLP-F204 Provision External Alarms and Virtual Wires

<b>Purpose</b>	This task creates, enables, and sets severities for up to 16 alarms caused by external events (such as a low battery, fire detector failure, or low temperature).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F392 Install Alarm Wires on the CAP/CAP2, page 18-108</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** In node view, click the **Provisioning > Alarm Extenders > External Alarms** tabs.

**Step 2** Complete the following fields for each external device wired to the ONS 15600 SDH backplane:

- **Enabled**—Check the check box for the alarm input number that you want to configure.

- Alarm Type—Choose an alarm type, such as Low temp or Misc, from the drop-down list.
- Severity—Choose an alarm severity (CR, MJ, MN, NA, or NR) from the drop-down list. The severity determines how the alarm appears in the CTC Alarms and History windows and whether the LEDs are activated in the software.



**Note** When virtual wires are assigned in mixed ONS 15454 SDH and ONS 15600 SDH networks, only the last four virtual wires (13 through 16) are visible from the ONS 15454 SDH nodes.

- Virtual Wire—From the drop-down list, choose a virtual wire (1 through 16) for the alarm. If you choose None, the alarm is not activated in CTC.
- Raised When—From the drop-down list, choose the contact condition (open or closed) that will trigger the alarm in CTC.
- Description—Default descriptions are provided for each alarm. To change the description, which is how the alarm is identified in CTC, double-click the field and edit as necessary.

**Step 3** To provision additional devices, complete [Step 2](#) for each additional device.

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

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

## DLP-F205 Provision External Controls for External Alarms and Virtual Wires

<b>Purpose</b>	This task configures the external control outputs. An external control governs an external alarm.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F392 Install Alarm Wires on the CAP/CAP2, page 18-108</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Step 1** In node view, click the **Provisioning > Alarm Extenders > External Controls** tabs.

**Step 2** Complete the following fields for each external control wired to the ONS 15600 SDH backplane:

- Enabled—Check this check box for the alarm control output number that you want to configure.
- Control Type—In the drop-down list, choose the type of control, such as Engine or Heat. For example, if you set up a virtual wire in the “[DLP-F204 Provision External Alarms and Virtual Wires](#)” task on [page 17-5](#) as alarm type Low Temp, you would choose a control type in the External Controls tab such as “Heat.”
- Trigger Type—Choose a means for triggering the alarm from the drop-down list, such as a local or remote alarm of a particular severity or association with a particular virtual wire.
- Description—Enter a description to be shown in the Alarms window.

**Step 3** To provision additional controls, complete [Step 2](#) for each additional device.

- Step 4** Click **Apply**.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F206 View Optical STM-N PM Parameters

<b>Purpose</b>	This task enables you to view performance monitoring (PM) counts on a selected STM-N card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

- Step 1** In node view, double-click an STM-N card. The card view appears.
- Step 2** Click the **Performance** tab ([Figure 17-3](#)).



**Note** The performance window defaults to Port 1 (SDH), VC3/VC4 PM counts. You must select the specific port and/or VC where you want to view PM counts. See the [“DLP-F207 Refresh PM Counts for a Selected Port and VC” task on page 17-8](#).

---

Figure 17-3 Viewing Optical STM-N Performance Monitoring Information

Performance tab      Card view

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8	Prev-9	Pr
MS-EB	0	0	0	0	0	0	0	0	0	0	0	0
MS-ES	0	0	0	0	0	0	0	0	0	0	0	0
MS-SES	0	0	0	0	0	0	0	0	0	0	0	0
MS-LIAS	0	0	0	0	0	0	0	0	0	0	0	0
MS-FC	0	0	0	0	0	0	0	0	0	0	0	0
MS-BBE	0	0	0	0	0	0	0	0	0	0	0	0
RS-EB	0	0	0	0	0	0	0	0	0	0	0	0
RS-ES	0	0	0	0	0	0	0	0	0	0	0	0
RS-SES	0	0	0	0	0	0	0	0	0	0	0	0
RS-OFS	0	0	0	0	0	0	0	0	0	0	0	0
RS-BBE	0	0	0	0	0	0	0	0	0	0	0	0

- Step 3** The PM parameter names appear on the left portion of the window in the Param column. The parameter values appear on the right portion 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 15600 SDH Reference Manual*.
- Step 4** Return to your originating procedure (NTP).

## DLP-F207 Refresh PM Counts for a Selected Port and VC

<b>Purpose</b>	This task changes the window view to display PM counts for a selected optical (STM-N) card port and virtual container (VC).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34.</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** From node view, double-click an STM-N or Ethernet port. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** Click the Port drop-down list and choose the desired port.



- Step 4** Click **Refresh**. All PM counts occurring for the selected port appear. For PM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Step 5** Return to your originating procedure (NTP).

## DLP-F208 Refresh PM Counts at Fifteen-Minute Intervals

<b>Purpose</b>	This task changes the window view to display PM counts in 15-minute intervals.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34.</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- Step 1** In node view, double-click an STM-N or Ethernet port. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** Click the **15 min** radio button.
- Step 4** Click **Refresh**. The PM parameters appear in 15-minute intervals that are synchronized with the time of day.
- Step 5** View the Current column to find PM counts for the current 15-minute interval.  
Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The number represents the counter value for each specific performance monitoring parameter.
- Step 6** View the Prev-*n* columns to find PM counts for the preceding 15-minute intervals.



**Note** If a complete 15-minute interval count is not possible, the value has a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings, changing the count by using the clear function, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

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

## DLP-F209 Refresh PM Counts at One-Day Intervals

<b>Purpose</b>	This task changes the window view to display PM counts in one-day intervals.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- 
- Step 1** In node view, double-click an STM-N or Ethernet port. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** Click the **1 day** radio button.
- Step 4** Click **Refresh**. The PM parameters display in one-day (24-hour) intervals that are synchronized with the time of day. For PM parameter definitions refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Step 5** View the Current column to find PM counts for the current one-day interval.
- Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular one-day interval, a TCA is raised. The number represents the counter value for each specific performance monitoring parameter.
- Step 6** View the Prev-*n* columns to find PM counts for the preceding one-day intervals.




---

**Note** If a complete count over a one-day interval is not possible, the value has a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, changing port states, or adjusting and clearing the counter. When the problem is corrected, the subsequent one-day interval appears with a white background.

---

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

## DLP-F210 Monitor Near-End PM Counts

<b>Purpose</b>	This task changes the window view to show near-end PM counts for the selected card, port, and VC.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

- 
- Step 1** In node view, double-click an STM-N or Ethernet port. The card view appears.

- Step 2** Click the **Performance** tab.
- Step 3** Click the **Near End** radio button.
- Step 4** Click **Refresh**. All PM counts recorded by the near-end node for the incoming signal on the selected card/port/VC appear. For PM parameter definitions refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F211 Monitor Far-End PM Counts

<b>Purpose</b>	This task changes the window view to show far-end PM counts for the selected card, port, and VC.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

- Step 1** In node view, double-click an STM-N or Ethernet port. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** Click the **Far End** radio button.
- Step 4** Click **Refresh**. All PM counts that are recorded by the far-end node for the outgoing signal on the selected card/port/VC appear. For PM parameter definitions refer to the “Performance Monitoring” chapter in the *Cisco ONS 15600 SDH Reference Manual*.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F212 Reset Current PM Counts

<b>Purpose</b>	This task uses the Baseline button to clear the PM count shown in the current time interval, but it does not clear the cumulative PM count. This allows you to see how quickly the PM counts rise.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

- Step 1** From node view, double-click an STM-N or Ethernet port. The card view appears.
- Step 2** Click the **Performance** tab.

**Step 3** Click **Baseline**.



**Note** The Baseline button clears the PM count shown in the Current column, but does not clear the PM counts on the card. When the current time interval expires or the window view changes, the total number of PM counts on the card and on the window appear in the appropriate column. The baseline values are discarded if you change views to a different window and then return to the Performance tab window.

**Step 4** View the Current column to observe changes to PM counts for the current time interval.

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

## DLP-F213 Clear Selected PM Counts

<b>Purpose</b>	This task uses the Clear button to clear specified PM counts depending on the selected option.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher



### Caution

The Clear button can mask problems if used incorrectly. This button is commonly used for testing purposes.

**Step 1** In node view, double-click an STM-N or Ethernet port. The card view appears.

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

**Step 3** Click **Clear**.

**Step 4** In the Clear Statistics menu, choose one of the following options:

- **Displayed statistics:** This option erases from the window display all PM counts that currently appear in the Performance tab window.
- **All statistics for port *n*:** This option erases from the window display and card memory all PM counts associated with the selected port. This means the 15-minute/one-day and near-end/far-end PM counts for the selected port are cleared from the card and the window display.
- **All statistics for card:** This option erases from the window display and card memory all PM counts associated with the selected card. This means the 15-minute/one-day and near-end/far-end PM counts for the selected card are cleared from the card and the window display.
- **All statistics for selected parameters:** This option erases from the window display and card memory all PM counts associated with the selected parameters. For example, if the 15 min and the Near End radio buttons are selected, all near-end PM counts in the current 15-minute interval are erased from the card and the window display.

**Step 5** Click **Yes** to clear the selected statistics.

- Step 6** Verify that the selected PM counts have been cleared.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F214 Search for Circuits

<b>Purpose</b>	This task searches for an ONS 15600 SDH circuit at the network, node, or card level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

- Step 1** Navigate to the appropriate CTC view:
- To search the entire network, from the View menu choose **Go To Network View**.
  - To search for 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 search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to display the card in card view.
- Step 2** Click the **Circuits** tab.
- Step 3** If you are in node or card view, choose the scope for the search (**Network** or **Node**) from the Scope drop-down list.
- Step 4** Click **Search**.
- Step 5** In the Circuit Name Search dialog box, complete the following:
- **Find What**—Enter the text of the circuit name you want to find.
  - **Match Whole Word Only**—Check this box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.
  - **Match Case**—Check this box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
  - **Direction**—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.
- Step 6** Click **Find Next**.
- Step 7** Repeat Steps 5 and 6 until you are finished, then click **Cancel**.
- Step 8** Return to your originating procedure (NTP).
-

## DLP-F215 Filter the Display of Circuits

<b>Purpose</b>	This task filters the display of circuits in the ONS 15600 SDH network, node, or card view Circuits window based on circuit name, size, type, direction, and other attributes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	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 display the card in card view.
- Step 2** Click the **Circuits** tab.
- Step 3** Set the attributes for filtering the circuit display:
- Click the **Filter** button.
  - In the Circuit Filter dialog box, complete the following, as applicable:




---

**Note** You can use all of the Filter dialog box options, partial options, or a single option to create a filter.

---

- Name**—Enter a complete or partial circuit name to filter circuits based on circuit name; otherwise leave the field blank.
- Direction**—Choose one: **Any** (CTC will not use direction to filter circuits), **1-way** (CTC displays only one-way circuits), or **2-way** (CTC displays only two-way circuits).
- OCHNC Wlen**—(DWDM OCHNCs only; refer to the *Cisco ONS 15454 DWDM Procedure Guide*) Choose an optical channel network connection (OCHNC) wavelength to filter the circuits. For example, choosing 1530.33 will display channels provisioned on the 1530.33-nm wavelength.
- Status**—Choose a circuit status to filter the circuits. For more information about circuit statuses, see [Table 18-3 on page 18-53](#).
- State**—Choose one: **Locked** (display only out-of-service circuits), **Unlocked** (display only in-service circuits; optical channel network connections have Unlocked status only), or **Locked-PARTIAL** (display only circuits with cross-connects in mixed service states).
- Protection**—Choose the protection type from the drop-down list. For more information about protection types, see [Table 18-2 on page 18-52](#).
- Slot**—Enter a slot number to filter circuits based on source or destination slot; otherwise leave the field blank.

- Port—Enter a port number to filter circuits based on source or destination port; otherwise leave the field blank.
  - Type—Choose one:
    - Any** (CTC will not use circuit type to filter circuits)
    - VC\_HO\_PATH\_CIRCUIT** (CTC displays only high-order path circuits)
    - VC\_LO\_PATH\_CIRCUIT** (CTC displays only low-order path circuits)
    - VC\_LO\_PATH\_TUNNEL** (CTC displays only low-order tunnel circuits)
    - VC\_LO\_PATH\_AGGREGATION** (CTC displays only low-order path aggregation circuits)
    - VC\_HO\_PATH\_VCAT\_CIRCUIT** (CTC displays only high-order path VCAT circuits)
    - VC\_LO\_PATH\_VCAT\_CIRCUIT** (CTC displays only low-order path VCAT circuits)
    - OCHNC** (CTC displays only OCHNC circuits)
    - OCHTRAIL** (CTC displays only OCHTRAIL circuits)
    - OCHCC** (CTC displays only OCHCC circuits)
  - Size—Click the appropriate check boxes to filter circuits based on size: Equipped non-specific, VC3, VC4-8c, VC11, 2.5 Gb/s No FEC, 10 Gb/s No FEC, VC4-6c, VC4-2c, VC4-32c, VC4-64c, VC4-16c, VC4-3c, 10 Gb/s FEC, VC4, VC12, OCHCC, VC4-4c, 2.5 Gb/s FEC, VC4-12c, and/or Multi-rate.
- 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.
- Step 7** Return to your originating procedure (NTP).

## DLP-F216 View Circuits on a Span

<b>Purpose</b>	This task views circuits on an ONS 15600 SDH span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">Chapter 6, “Create Circuits”</a> <a href="#">DLP-F181 Log into CTC, page 16-34</a>

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

**Step 1** From the View menu, choose **Go To Network View**. If you are already in network view, continue with [Step 2](#).

**Step 2** Right-click the green line (span) containing the circuits you want to view and choose one of the following:

- **Circuits**—To view MS-SPRing, SNCP, 1+1, or unprotected circuits on the span.
- **PCA Circuits**—To view circuits routed on an MS-SPRing protected channel. (This option does not appear if the span you right-clicked is not an MS-SPRing span.)

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

- **VC**—Displays VCs used by the circuits.
- **SNCP**—Indicates whether the circuit is in an SNCP.
- **Circuit**—Displays the circuit name.
- **Switch State**—(SNCP span only) Displays the switch state of the circuit, that is, whether any span switches are active. For SNCP 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 complete other procedures from the Circuits on Span dialog box. If the span is in an SNCP, you can switch the span traffic. See [“DLP-F193 SNCP Protection Switching Test” task on page 16-51](#) for instructions. If you want to edit a circuit on the span, double-click the circuit. See the [“DLP-F264 Edit SNCP Circuit Path Selectors” task on page 17-55](#) for instructions.

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

## DLP-F217 Edit a Circuit Name

<b>Purpose</b>	This task edits a circuit name.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

**Step 1** Click the **Circuits** tab.

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



- Step 3** 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.
- Step 4** Click **Apply**.
- Step 5** From File menu, choose **Close**.
- Step 6** In the Circuits window, verify that the circuit was correctly renamed.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F218 Change Active and Standby Span Color

<b>Purpose</b>	This task changes the color of active (working) and standby (protect) circuit spans that appear on the detailed circuit map of the Edit Circuit window. By default, working spans are green and protect spans are purple.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the Edit menu, 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** Change the color of the active span:
- a. In the Span Colors area, click the colored square located near the word Active.
  - b. In the Pick a Color dialog box, click the color for the active span. 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.
  - d. 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** Change the color of the standby span:
- a. In the Span Colors area, click the colored square located near the word Standby.
  - b. In the Pick a Color dialog box, click the color for the standby span. Click the **Reset** button if you want the standby span to display the last applied (saved) color.
  - c. Click **OK** to close the Pick a Color dialog box.
  - 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 6** If you want to return the active and standby spans to their default colors:
- From the Edit menu, choose **Preferences**.
  - In the Preferences dialog box, click the **Circuit** tab.
  - Click the **Reset to Defaults** button.
  - Click **Apply** and click **OK** to close the Preferences dialog box.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F219 Change IP Settings

<b>Purpose</b>	This task changes the IPv4 address, subnet mask, default router, DHCP access, firewall Internet Inter-ORB Protocol (IIOP) listener port, LCD IP display, IPv6 Address, Prefix Length, IPv6 Default Router, and SOCKS proxy server settings for the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F185 Provision IP Settings, page 16-38</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

---

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

**Step 2** Change any of the following:

- Node Address
- Default Router
- IPv6 Configuration
  - IPv6 Address
  - Prefix Length
  - IPv6 Default Router
- Subnet Mask Length
- Forward DHCP Request To
- TSC CORBA (IIOP) Listener Port
- Gateway Settings

See the “[DLP-F185 Provision IP Settings](#)” task on page 16-38 for detailed field descriptions.

**Step 3** Click **Apply**.

If you changed any 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. Change in IPv6 configuration such as IPv6 Address, Prefix Length and IPv6 Default Router does not cause the node to reboot.

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

If you changed an IPv4 address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS TSC cards will reboot, one at a time. A TSC reboot causes a temporary loss of connectivity to the node, but traffic is unaffected.

- Step 5** Confirm that the changes appear on the Provisioning > Network > General tab. If the changes do not appear, repeat the task.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F220 Modify a Static Route

<b>Purpose</b>	This task modifies a static route on the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F186 Create a Static Route, page 16-41</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** In node view, click the **Provisioning > Network > Static Routing** tabs.
- Step 2** Click the static route 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-F186 Create a Static Route](#)” task on page 16-41 for detailed field descriptions.
- Step 5** Click **OK**.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F221 Delete a Static Route

<b>Purpose</b>	This task deletes a static route from the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Provisioning > 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-F222 Disable OSPF

<b>Purpose</b>	This task disables the OSPF routing protocol process for the LAN on the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F187 Set Up or Change Open Shortest Path First Protocol, page 16-42</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note**

If the ONS 15600 SDH has interfaces (DCC or LAN) in multiple OSPF areas, at least one ONS 15600 SDH interface (DCC or LAN) must be in the backbone area 0.0.0.0.

---



**Note**

When you are logged into a ONS 15600 SDH node, CTC will not allow both a DCC interface and a LAN interface in the same nonzero OSPF area.

---



**Note**

Cisco recommends limiting the number of link-state packets (LSPs) that will be forwarded over the DCC interfaces.

---

- Step 1** In node view, click the **Provisioning > Network > OSPF** tabs.
- Step 2** In the OSPF on LAN area, uncheck **OSPF active on LAN**.
- Step 3** Click **Apply**. Confirm that the changes appear; if not, repeat the task.



**Note**

Disabling OSPF can cause the TSCs to reboot. This results in a temporary loss of connectivity to the node, but traffic is unaffected.

---

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

## DLP-F223 Change the Network View Background Color

<b>Purpose</b>	This task changes the network view background color and the domain view background color (the area displayed when you open a domain).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher



### Note

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

- 
- 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, select a background color.
  - Step 4** Click **OK**.
  - Step 5** Return to your originating procedure (NTP).
- 

## DLP-F224 Change the Default Network View Background Map

<b>Purpose</b>	This task changes the default map of the CTC network view.
<b>Tools/Equipment</b>	None
<b>Prerequisite procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

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

- 
- Step 1** From the Edit menu, choose **Preferences > Map** and check the **Use Default Map** check box.
  - Step 2** In the node view, click the **Provisioning > Defaults** tabs.
  - Step 3** In the Defaults Selector area, choose **CTC** and then **network**.
  - Step 4** Click the **Default Value** field and choose a default map from the drop-down list. Map choices are: Germany, Japan, Netherlands, South Korea, United Kingdom, and the United States (default).
  - Step 5** Click **Apply**. The new default network map appears.
  - Step 6** Click **OK**.

- Step 7** If the ONS 15600 SDH icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until the ONS 15600 SDH 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 15600 SDH icons are displayed at the magnification you want.
- Step 10** Return to your originating procedure (NTP).

## DLP-F225 Apply a Custom Network View Background

<b>Purpose</b>	This task changes the background image of the CTC network view on your login workstation.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning 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 want to position nodes on the map based on the node coordinates, you will need the longitudes and latitudes for the edges of the map. You can obtain the longitude and latitude for cities and zip codes from the U.S. Census Bureau U.S. Gazetteer website ([www.census.gov/cgi-bin/gazetteer](http://www.census.gov/cgi-bin/gazetteer)). If you will use your mouse to position nodes, coordinates for the image edges are not necessary. The change does not affect other CTC users.

- 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** Click **Browse**. Navigate to the graphic file that you want to use as a background.
- Step 4** Select the file. Click **Open**.
- Step 5** Click **Apply** and then click **OK**.
- Step 6** If the ONS 15600 SDH icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15600 SDH icons are visible.



### Tip

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

- Step 7** If you want to change the magnification of the icons, right-click the network view and choose **Zoom In**. Repeat until the ONS 15600 SDH icons are displayed at the magnification you want.
- Step 8** At the network view, use the CTC toolbar Zoom buttons (or right-click the graphic area and select a Zoom command from the shortcut menu) to set the area of the image you want to view.

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

---

## DLP-F226 Create Domain Icons

<b>Purpose</b>	This task creates a domain icon, which can be used to group ONS 15600 SDH icons in CTC network view for all users.
<b>Tools/Equipment</b>	None
<b>Prerequisite procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser



**Note** Domains 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 that any user can maintain the domain information in his or her Preferences file, which means that 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-F244 Edit Network Element Defaults](#)” procedure on page 14-34 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-F227 Manage Domain Icons

<b>Purpose</b>	This task manages CTC network view domain icons, including moving, renaming, and removing domains.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F226 Create Domain Icons, page 17-23</a>
<b>Required/As needed</b>	As needed

<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

**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 that any user can maintain the domain information in his or her Preferences file, which means that 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-F244 Edit Network Element Defaults” procedure on page 14-34](#) 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 17-1](#) and complete the appropriate steps.

**Table 17-1** *Managing Domains*

Domain Action	Steps
Move a domain	Press <b>Ctrl</b> and drag and drop the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose <b>Rename Domain</b> 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 on the domain icon.
Move a node from a domain to the network map	Open the domain and right-click a node. Select <b>Move Node Back to Parent View</b> .
Open a domain	Double-click the domain icon, right-click the domain, and choose <b>Open Domain</b> .
Return to network view	Right-click the domain view area and choose <b>Go To Parent View</b> from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose <b>Show Domain Overview</b> . The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the overview and select <b>Show Domain Overview</b> .
Remove domain	Right-click the domain icon and choose <b>Remove Domain</b> . Any nodes residing in the domain are returned to the network map.

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



## DLP-F228 Modify a 1+1 Protection Group

<b>Purpose</b>	This task modifies a 1+1 protection group for any optical port.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Provisioning > Protection** tabs.
- Step 2** In the Protection Groups list, click the 1+1 protection group that you want to modify.
- Step 3** In the Selected Group area, you can modify the following:
- Name
  - Bidirectional switching
  - Revertive
  - Reversion time




---

**Note** The bidirectional switching and revertive settings must be identical at each end of the span.

---

See the “[NTP-F138 Create a 1+1 Protection Group](#)” procedure on page 4-10 for field descriptions.

- Step 4** Click **Apply**. Confirm that the changes appear; if not, repeat the task.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F229 Delete a 1+1 Protection Group

<b>Purpose</b>	This task deletes a 1+1 protection group for any optical port.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From node view, click the **Provisioning > Protection** tabs.
- Step 2** In the Protection Groups list, click the 1+1 protection group that you want to delete.
- Step 3** Click **Delete**. The Delete Protection Group window appears.
- Step 4** Click **Yes**.

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

---

## DLP-F230 Change the Node Timing Source

<b>Purpose</b>	This task changes the SDH timing source for the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Caution

The following procedure might be service affecting; complete during a scheduled maintenance window.

---

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

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

- Timing Mode
- Revertive
- Revertive Time

For detailed descriptions of these fields, see the “[NTP-F137 Set Up Timing](#)” procedure on page 4-9.

**Step 3** In the Reference Lists area, you can change the NE Reference.

**Step 4** Click the **BITS Facilities** tab. In the BITS In area, you can change the following information:



**Note** The BITS Facilities area sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer.

---

- Facility Type
- BITS State
- Coding
- Framing
- Sync. Messaging
- Admin SSM
- Sa Bit
- Cable Type

**Step 5** In the BITS Out area, you can change the following information:

- Facility Type
- BITS State
- Coding

- Framing
- AIS Threshold
- Sa Bit
- Cable Type

**Step 6** Click **Apply**.



**Note** Both TSCs must acquire the new clock. The UNPROT-SYNCCLK alarm will occur for 700 seconds, and both TSCs will report the FSTSYNC alarm for the same period of time. This is normal.

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

## DLP-F231 Delete a User from a Single Node

<b>Purpose</b>	This task deletes an existing user from a single node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F269 Change User Password and Security Levels for a Single Node, page 17-61</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser

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

**Step 2** Choose the user you want to delete.

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

**Step 4** Verify that you selected the correct user to delete and click **OK**.

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

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

## DLP-F232 Delete a User From Multiple Nodes

<b>Purpose</b>	This procedure deletes an existing user from multiple nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">DLP-F270 Change User and Security Settings for Multiple Nodes, page 17-62</a>

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

**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 while they are logged in, complete the “[DLP-F272 Log Out a User on Multiple Nodes](#)” task on page 17-63.

- 
- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Provisioning > Security > Users** tabs.
- Step 3** Choose the user that you want to delete.
- Step 4** Click **Delete**. The Delete User dialog box appears.
- Step 5** In the Select Applicable Nodes area, uncheck any nodes where you do not want to delete this user.
- Step 6** Click **OK**. The User Deletion Results confirmation dialog box appears.
- Step 7** Click **OK**. Confirm that the changes appear; if not, repeat the task.
- Step 8** Return to your originating procedure (NTP).
- 

## DLP-F233 Modify SNMP Trap Destinations

<b>Purpose</b>	This task modifies Simple Network Management Protocol (SNMP) trap destinations on an ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , page 16-34
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Provisioning > SNMP** tabs.
- Step 2** Click a trap in the Trap Destinations list box.
- For a description of SNMP traps, refer to the “SNMP” chapter of the *Cisco ONS 15600 SDH Reference Manual*.
- Step 3** In the Selected Destination area, complete as needed:
- Type the SNMP community name in the Community Name field.

**Note**

The community name is a form of authentication and access control. The community name assigned to the ONS 15600 SDH is case-sensitive and must match the community name of the network management system (NMS).

---



**Note** The default UDP port for SNMP is 162.

- Set the Trap Version field to either SNMPv1 or SNMPv2.  
Refer to your NMS documentation to determine whether to use SNMPv1 or SNMPv2.

- Step 4** If you want the SNMP agent to accept SNMP SET requests on certain MIBs, click the **Allow SNMP Sets** check box. If this box is not checked, SET requests are rejected.
- Step 5** Click **Apply**. SNMP settings are now configured.
- Step 6** To view SNMP information for each node, click the node IP address in the Trap Destinations list.
- Step 7** Return to your originating procedure (NTP).

## DLP-F234 Delete SNMP Trap Destination

<b>Purpose</b>	This task deletes an SNMP trap destination on an ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** In node view, click the **Provisioning > SNMP** tabs.
- Step 2** Click the trap that you want to delete in the Trap Destination list box.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Confirm that the changes are correct and click **Yes**.
- Step 5** Return to your originating procedure (NTP).

## DLP-F235 Switch All SNCP Circuits on a Span

<b>Purpose</b>	This task applies a FORCE external switching command to all circuits on an SNCP span. The FORCE switches the traffic to another span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

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

- Step 2** Right-click the span where you want to switch SNCP traffic.
- Step 3** Choose **Circuits** from the shortcut menu.
- Step 4** In the Circuits on Span dialog box, select **Force**.




---

**Caution** The FORCE command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

---

- Step 5** In the confirmation dialog box, click **Yes**.  
In the Circuits on Span dialog box, the Switch State listed for all circuits is FORCE.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F236 Clear a Switch for all SNCP Circuits on a Span


<b>Purpose</b>	This task clears a Force traffic switch for all circuits on an SNCP span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Right-click the span where you want to clear the switch.
- Step 3** Choose **Circuits** from the shortcut menu.
- Step 4** In the Circuits on Span dialog box, select **CLEAR** to remove a previously set switch command.
- Step 5** In the confirmation dialog box, click **Yes**.  
In the Circuits on Span dialog box, the Switch State listed for all circuits is CLEAR.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F237 Verify Timing in a Reduced Ring

<b>Purpose</b>	This task verifies timing in a reduced ring.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite/remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Provisioning > Timing > General** tabs.
- Step 2** Observe the Timing Mode field to see the type of timing (Line, External) that has been set for that node.
- 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 BITS timing source, perform the following:
- a. Look for another node on the ring that can be used as a BITS source and set that node's Timing Mode to **External**. Choose that node as the primary timing source for all other nodes in the ring. See the [“DLP-F230 Change the Node Timing Source” task on page 17-26](#).
  - 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 that node's Timing Mode to **External** and set the BITS 1 and 2 State to **Locked**. Then choose line timing for all other nodes in the ring. This will force the first node to be their primary timing source. See the [“DLP-F230 Change the Node Timing Source” task on page 17-26](#).
-  **Note** This type of timing conforms to Stratum 3E requirements and is not considered optimal.
- 
- Step 5** If the removed node was not the BITS timing source, provision the adjacent nodes to line timing using SDH links (east and west) as timing sources, traceable to the node with external BITS timing.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F238 Initiate a Manual Switch on a Port in a 1+1 Protection Group

<b>Purpose</b>	This procedure applies the Manual external switching command to a 1+1 protection scheme.
<b>Tools/Equipment</b>	Installed optical (STM-N) cards
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Group area, select the protection group with the port you want to switch. In the Selected Group area each port is identified as Working or Protect. Each port also has a status:
- Active—The port is carrying traffic.
  - Standby—The port is not carrying traffic.
  - [MANUAL TO WORKING]—A Manual switch has moved traffic to the Working port.
  - [MANUAL TO PROTECT]—A Manual switch has moved traffic to the Protect port.
  - [FORCE TO WORKING]—A Force switch has moved traffic to the Working port.
  - [FORCE TO PROTECT]—A Force switch has moved traffic to the Protect port.

The normal assignment status is for one port assignment to say Working/Active and for the other to say Protect/Standby.

**Step 3** In the Selected Group, click the port that you want to switch. For example, if you want to switch traffic from the working port to the protect port, click the working port.

**Step 4** Click **Manual**.

If the Manual switch is successful, CTC shows both ports as [MANUAL TO PROTECT] (or [MANUAL TO WORKING]). This indicates that the ONS 15600 SDH system has been able to carry out the switch request and has moved traffic from one port to the other.

If the Bidirectional switching check box is checked, both the near-end and far-end nodes switch to the designated protection ports. For example, if the near-end node has a loss of signal (LOS), it switches to the protect port and transmits a switch request to the far-end node to switch to the protect port also. This ensures that both nodes process traffic from the same span.

If the Bidirectional switching check box is not selected, the near-end and far-end nodes switch independently of each other. For example, if the near-end node has an LOS on its working port, it switches to the protect port. If the far-end node does not have a LOS, traffic remains on the working port.

If the Manual switch is not successful, CTC continues to show the ports as active and standby, and an alarm such as FAILTOSWS is raised. This failure occurs because the target port is not available and troubleshooting is required. For information about troubleshooting, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

**Step 5** Click the **Conditions** tab and click **Retrieve** to see new events. The switch procedure raises a MANUAL-REQ-SPAN condition that is visible in the window unless Not Alarmed conditions have been filtered out from the view.

**Step 6** Click the **Alarms** tab.

If any traffic loss alarms occur or if a switching failure alarm such as FAILTOSWS occurs, troubleshoot the problems that have prevented the switch and attempt the switch procedure again.

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

## DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group

<b>Purpose</b>	This task applies the Force external switching command to a 1+1 protection scheme.
<b>Tools/Equipment</b>	Installed STM-N cards
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

**Step 2** In the Protection Group area, select the protection group with the port you want to switch.

In the Selected Group area, each port is identified as Working or Protect. Each port also has a status:

- Active—The port is carrying traffic.



- Standby—The port is not carrying traffic.
- [MANUAL TO WORKING]—A Manual switch has moved traffic to the working port.
- [MANUAL TO PROTECT]—A Manual switch has moved traffic to the protect port.
- [FORCE TO WORKING]—A Force switch has moved traffic to the working port.
- [FORCE TO PROTECT]—A Force switch has moved traffic to the protect port.

The normal status is for one port to be Working/Active and the other to be Protect/Standby.

**Step 3** In the Selected Group area, select the port that you want to switch. For example, if you want to switch traffic from the working port to the protect port, click the working port.

**Step 4** Click **Force**.

If the Force switch is successful, Cisco Transport Controller (CTC) shows both ports as [FORCE TO PROTECT] (or [FORCE TO WORKING]). This indication is shown whether or not the ONS 15600 SDH system has been able to move traffic from one port to the other.

If the Bidirectional switching check box is checked, both the near-end and far-end nodes switch to the designated protection ports. For example, if the near-end node has a loss of signal (LOS), it switches to the protection port and transmits a switch request to the far-end node to switch to the protection port also. This ensures that both nodes process traffic from the same span.

If the Bidirectional switching check box is not selected, the near-end and far-end nodes switch independently of each other. For example, if the near-end node has an LOS on its working port, it switches to the protection port. If the far-end node does not have a LOS, traffic remains on the working port.

If the Force switch is unsuccessful, clear the switch immediately using the “[DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group](#)” task on page 17-86, and then troubleshoot the problems preventing the switch by referring to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

**Step 5** Click the **Conditions** tab and click **Retrieve** to see new events. The switch procedure raises a FORCED-REQ-SPAN condition that is visible in the window unless Not Alarmed conditions have been filtered out from the view.

**Step 6** Click the **Alarms** tab.

No new traffic loss alarms or failure-to-switch alarms should appear.

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

## DLP-F240 Apply a Lock On in a 1+1 Group

<b>Purpose</b>	This task locks traffic onto a working port to prevent traffic from switching to the protect port in a protection group.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , page 16-34
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** A lock on can be applied to a working port only.

- 
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group where you want to apply a lock-on.
- Step 3** If you determine that the protect port is in standby and you want to apply the lock-on to the protect port, make the protect port active:
- In the Selected Group field, click the protect port.
  - In the Switch Commands field, click **Force**.
- Step 4** In the Selected Group area, choose the active port where you want to lock on traffic.
- Step 5** In the Inhibit Switching field, click **Lock On**.
- Step 6** Click **Yes** in the confirmation dialog box.
- The lock on has been applied and traffic cannot be switched from that port. See the [“DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group” task on page 17-86](#) as needed.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F241 Apply a Lockout in a 1+1 Group

<b>Purpose</b>	This task locks traffic out of a protect port in a 1+1 protection group, which prevents traffic from switching to that port.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** A lockout can be applied to a protect port only.

---

- 
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups field, click the protection group that contains the card you want to lock out.
- Step 3** In the Selected Group area, select the card you want to lock out.
- Step 4** In the Inhibit Switching field, 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 card. To clear the lockout, see the [“DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group” task on page 17-86](#).
- Step 6** Return to your originating procedure (NTP).
-

## DLP-F242 Initiate a Manual Switch on an SNCP Circuit

<b>Purpose</b>	This task switches traffic to the protect SNCP path using a Manual switch. A Manual switch will switch traffic if the path has an error rate less than the signal degrade.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Circuits > Circuits** tabs.
- Step 2** Click the path you want to switch and then click **Edit**.
- Step 3** In the Edit Circuit window, click the **SNCP Selectors** tab.
- Step 4** In the Switch State column, click the row for the path you want to switch and select **Manual to Protect** or **Manual to Working** as appropriate.
- Step 5** Click **Apply**.
- Step 6** To verify that the switch has occurred, view the SNCP Selectors tab Switch State column. The row for the circuit you switched will show a MANUAL status.
- Traffic switches from the working SNCP path to the protect path. If the path is configured for revertive switching, the traffic reverts to the working path when the Manual switch is cleared. See the “[DLP-F298 Clear a Switch or Lockout on an SNCP Circuit](#)” task on page 17-88 as needed.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F243 Initiate a Force Switch to an SNCP Circuit

<b>Purpose</b>	This task switches traffic to the working SNCP circuit using a Force switch. A Force switch will switch traffic even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch has a higher priority than a Manual switch.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Circuits > Circuits** tabs.
- Step 2** Click the path you want to switch and click **Edit**.
- Step 3** In the Edit Circuit window, click the **SNCP Selectors** tab.

- Step 4** In the Switch State column, click the row for the path you want to switch and select **Force to Working** or **Force to Protect** as appropriate.
- Step 5** Click **Apply**.
- Step 6** To verify that the switch has occurred, view the SNCP Selectors tab Switch State column. The circuit row shows a FORCE status.
- Traffic switches from the protect path to the working path. Protection switching cannot occur until the Force switch is cleared. See the “[DLP-F298 Clear a Switch or Lockout on an SNCP Circuit](#)” task on [page 17-88](#) as needed.
- Step 7** Return to your originating procedure (NTP).

## DLP-F244 Create a DCC Tunnel

<b>Purpose</b>	This task creates a data communications channel (DCC) tunnel to transport traffic from third-party SDH equipment across ONS 15600 SDH networks. Tunnels can be created on the RS-DCC channel (D1-D3) (if not used by a node as a terminated DCC), or any MS-DCC channel (D4-D6, D7-D9, or D10-D12).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , page 16-34 <a href="#">NTP-F144 Verify Node Turn-Up</a> , page 5-2 <a href="#">NTP-F209 Modify or Delete Communications Channel Terminations</a> , page 11-8, as needed
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

The ONS 15600 SDH can support up to 64 DCC tunnels. Terminated RS-DCCs cannot be used as DCC tunnel endpoints, and an RS-DCC that is used as a DCC tunnel endpoint cannot be terminated. You must delete the terminated RS-DCCs in a path before creating a DCC tunnel. All DCC tunnel connections are bidirectional.

- Step 1** In network view, click the **Provisioning > Overhead Circuits** tabs.
- Step 2** Click **Create**.
- Step 3** In the Circuit Creation dialog box, provision the DCC tunnel:
- Name—Type the tunnel name.
  - Type—Choose one:
    - **DCC Tunnel - D1-D3**—Allows you to choose either the RS-DCC (D1-D3) or a MS-DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
    - **DCC Tunnel - D4-D12**—Provisions the full MS-DCC as a tunnel.
- Step 4** In the Source area, complete the following:
- Node—Choose the source node.

- Slot—Choose the source slot.
- Port—Choose the source port.
- Channel—Shown if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - DCC1 (D1-D3)—RS-DCC
  - DCC2 (D4-D6)—MS-DCC 1
  - DCC3 (D7-D9)—MS-DCC 2
  - DCC4 (D10-D12)—MS-DCC 3

DCC options do not appear if they are used by the ONS 15600 SDH (DCC1) or other tunnels.

**Step 5** In the Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—Choose the destination port.
- Channel—Shown if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - DCC1 (D1-D3)—RS-DCC
  - DCC2 (D4-D6)—MS-DCC 1
  - DCC3 (D7-D9)—MS-DCC 2
  - DCC4 (D10-D12)—MS-DCC 3

DCC options do not appear if they are used by the ONS 15600 SDH (DCC1) or other tunnels.

**Step 6** Click **Finish**.

**Step 7** Put the ports that are hosting the DCC tunnel in service. See the [“DLP-F254 Change the Service State for a Port” task on page 17-48](#) for instructions.

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


## DLP-F245 Clean Fiber Connectors

<b>Purpose</b>	This task cleans the fiber connectors.
<b>Tools/Equipment</b>	Inspection microscope (suggested: Westover FBP-CIS-1) Desktop hand tool Scrub tool 3M high-performance fiber-optic wipes Compressed air/duster
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



### Note

Replace all dust caps whenever the equipment will be unused for 30 minutes or more.

- 
- Step 1** Remove the dust cap from the fiber connector.
- Step 2** To use the desktop hand tool:
- a. Advance the 3M high-performance fiber-optic wipe in the desktop hand tool to access the unused wipe area.
-  **Note** To replace the fiber-optic wipe in the desktop hand tool, remove the frame cover. Put a new wipe over the base of the desktop hand tool with the stitching of the wipe aligned lengthwise with the tool. Place the frame cover on the tool and press firmly to reattach.
- 
- b. Place the connector tip at the top of the slot at a slight angle. In a single stroke, move the connector down the wipe without lifting the connector from the wipe. Before lifting the connector from the wipe, straighten the connector.
  - c. Repeat the single stroke motion on each side of the alignment pins to clean the entire connector face.
  - d. Blow off any wipe lint left on the fiber connector using the compressed air.
- Step 3** To use the scrub tool:
- a. Connect the grounding strap to the scrub tool and to suitable ground.
  - b. Install or replace the scrub wipe in the scrub tool with a new wipe. Avoid handling the wipe excessively.
  - c. Scrub between the alignment pins of the fiber connector, and then wipe around the outside of each alignment pins.
- Step 4** Inspect the connector for cleanliness. Repeat Steps 2 and 3 as necessary.
- Step 5** Replace the dust cap on the fiber connector until ready for use.
- Step 6** Return to your originating procedure (NTP).
-

## DLP-F246 Clean the Fiber Adapters

<b>Purpose</b>	This task cleans the fiber adapters.
<b>Tools/Equipment</b>	<p>Inspection microscope (suggested: Westover FBP-CIS-1)</p> <p>Scrub tool</p> <p>Grounding strap</p> <p>Wipes</p> <p>Rinse tool</p> <p>HFE-based cleaning fluid and pump head assembly</p> <p>Replacement scrub tool wipes</p> <p>Replacement rinse tool absorbent pads</p> <p>Empty disposable container</p>
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

**Step 1** Remove the dust plugs from the fiber adapter.

**Step 2** To remove stubborn particles from the fiber adapter:

- a. Connect the grounding strap to the scrub tool and to suitable ground.
- b. Install or replace the scrub wipe in the scrub tool with a new wipe. Avoid handling the wipe excessively.
- c. Insert the scrub tool tip into the fiber adapter.
- d. Remove and insert the scrub tool tip several times to clean the fiber adapter.

**Step 3** To remove loose particles from the fiber adapter:

- a. Remove the dust cap from the rinse tool.



**Note** If the absorbent pad on the rinse tool needs replacement, slide the old pad and mesh retainer off of the rinse tool tube. Slide the new absorbent pad and mesh retainer over the rinse tip onto the rinse tool tube. Roll the absorbent pad and mesh retainer between your hands until the opening on the absorbent pad is closed. Discard the old absorbent pad and mesh retainer.

- b. Connect the grounding strap to the rinse tool and to suitable ground.
- c. Connect the rinse tool to the HFE-based cleaning fluid bottle and pump head assembly.
- d. Turn the aluminum nozzle on the pump one-half turn counterclockwise and squirt the cleaning fluid into an empty container to soak the rinse tool.
- e. Remove the dust cover from the fiber adapter.
- f. Insert the rinse tool tip into the fiber adapter with the bent part of the handle pointing downwards. Squirt twice.

- g. Remove the rinse tool and replace the dust cover on the adapter. Replace the dust cap on the rinse tool.
  - h. Turn the aluminum nozzle on the pump clockwise until it is tight and disconnect the HFE bottle from the pump.
- Step 4** Inspect the fiber adapter to ensure it is clean. If it is not clean, repeat Steps 2 and 3.
- Step 5** Replace the dust plug in the fiber adapter until ready for use.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F247 Verify that a 1+1 Working Port is Active

<b>Purpose</b>	This task verifies that a working slot in a 1+1 protection scheme is active (and that the protect slot is in standby).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Both
<b>Security Level</b>	Maintenance or higher

---

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Selected Group area, verify that the working slot/port is shown as Working/Active. If so, this task is complete.
- Step 3** If the working slot says Working/Standby, perform a Manual switch on the working port:
- a. In the Selected Group area, choose the Protect/Active port.
  - b. In the Switch Commands field, choose **Manual**.
  - c. Click **Yes** in the confirmation dialog box.
- Step 4** Verify that the working slot is carrying traffic (Working/Active).



**Note** If the slot is not active, look for conditions or alarms that might be preventing the card from carrying working traffic. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures to clear alarms.

---

- Step 5** When the working port is carrying traffic, clear the Manual switch:
- a. In the Switch Commands field, choose **Clear**.
  - b. Click **Yes** in the confirmation dialog box.
- Step 6** Verify that the working port does not revert to Standby, which might indicate a problem on the working span.
- Step 7** Return to your originating procedure (NTP).
-



## DLP-F248 Drill Holes to Anchor and Provide Access to the Bay Assembly

<b>Purpose</b>	This task describes how to use the floor template to locate and drill the appropriate holes that are needed to anchor and provide additional access to the bay assembly at your site.
<b>Tools/Equipment</b>	Floor template (53-2141-XX) Marking pen Concrete drill Reciprocating saw
<b>Prerequisite Procedures</b>	<a href="#">NTP-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None


**Note**

If the bay will use wide cable routing modules (CRMs) for cable routing, you need to use 900-mm (35.4-in) spacing between bays.

**Step 1**

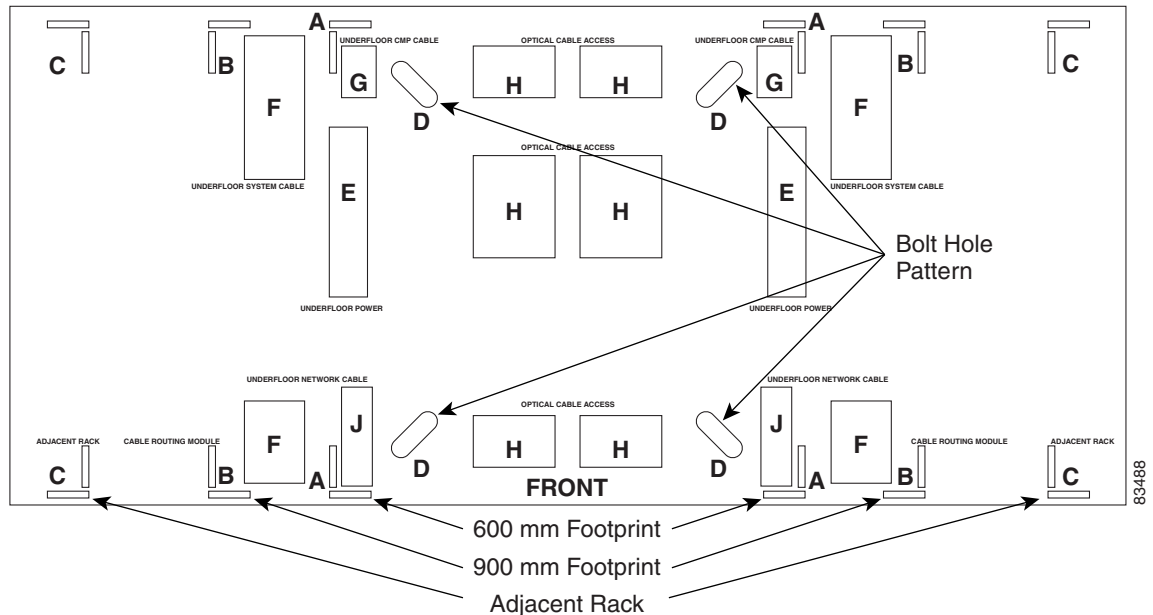
Determine the proper location of your bay:

- a. For a 900-mm (35.4-inch) wide bay, position the floor template so that corner indicators “B” fall where you want the corners of the bay to reside ([Figure 17-4](#)).
- b. For a 600-mm (23.6-inch) wide bay, position the floor template so that corner indicators “A” fall where you want the corners of the bay to reside ([Figure 17-4](#)).


**Note**

If space allows, Cisco recommends you reserve an additional 1/4 inch (6.35 mm) of space on each side of the bay assembly you are installing.

Figure 17-4 Floor Template



- Step 2** Use the corner indicators “C” to determine the closest recommended position of an adjacent 900-mm (35.4-inch) bay assembly.
- Step 3** Use a marking pen to mark the floor with the corner indicators appropriate to your installation.
- Step 4** At the four locations marked “D,” drill floor bolt holes according to the bolt manufacturer’s recommendation for bolt hole size.
- Step 5** If you will use under-floor power, use the drill and saw to cut out the rectangular floor areas marked “E.”
- Step 6** If you will route optical cables in a 900-mm (35.4-inch) bay from under the floor, use the drill and saw to cut out the rectangular floor areas marked “F.”
- Step 7** If you will route optical cables in a 600-mm (23.6-inch) bay from under the floor, use the drill and saw to cut out the rectangular floor areas marked “J.”
- Step 8** If you will route any timing, alarm, or LAN cables through the floor to the customer access panel (CAP), use the drill to cut out the floor areas marked “G.”
- Step 9** (Optional.) If you want to create other access holes for under-floor access (for AC power, for example), use the reciprocating saw to cut sufficient holes within any of the locations marked “H.”
- Step 10** Return to your originating procedure (NTP).

## DLP-F249 Assign a Name to a Port

<b>Purpose</b>	This task assigns a name to a port on any ONS 15600 SDH card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">NTP-F131 Verify Card Installation, page 4-2</a>

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

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

## DLP-F250 Provision SNCP Selectors During Circuit Creation

<b>Purpose</b>	This task provisions SNCP selectors during circuit creation. Use this task only if the circuit will be routed on an SNCP.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	You must have the Circuit Creation wizard open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

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

- 
- Step 1** In the Circuit Attributes area of the Circuit Creation wizard, set the SNCP path selectors:
- Provision working go and return on primary path—Check this box to route the working path on one fiber pair and the protect path on a separate fiber pair. This feature only applies to bidirectional SNCP circuits.
  - Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
  - Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
  - SF threshold—For high-order circuits, set the SNCP path-level signal failure bit error rate (BER) thresholds.
  - SD threshold—For high-order circuits, set the SNCP path-level signal degrade BER thresholds.

- Switch on PDI-P—For high-order circuits, check this box if you want traffic to switch when a high-order payload defect indication–path is received. Unavailable for low-order circuits.

**Step 2** Return to your originating procedure (NTP).

---

## DLP-F251 Provision a Half Circuit Source and Destination on an MS-SPRing or 1+1 Protection Group

<b>Purpose</b>	This task provisions a half circuit source and destination for MS-SPRings and 1+1 protection groups.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F168 Create a Half Circuit on an MS-SPRing or 1+1 Node, page 6-17</a> The Source page of the Circuit Creation wizard must be open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the Node drop-down list, choose the node that will contain the half circuit.
- Step 2** From the Slot drop-down list, choose the slot containing the card where the circuit will originate.
- Step 3** From the Port drop-down list, choose the port where the circuit will originate.
- Step 4** Click **Next**.
- Step 5** From the Node drop-down list, choose the node chosen in [Step 1](#).
- Step 6** From the Slot drop-down list, choose the STM-N card to map the STM-N high-order circuit to a virtual container (VC).
- Step 7** Choose the destination VC from the additional drop-down lists that appear based on your choices.
- Step 8** Return to your originating procedure (NTP).
-

## DLP-F252 Provision a Half Circuit Source and Destination on an SNCP

<b>Purpose</b>	This task provisions a half circuit source and destination for an SNCP ring. This task is used to create SNCP selectors on the node. Depending on the specific network configuration, the SNCP selector can be created on the source side (two sources, one destination); the destination side (one source, two destinations); or both (two sources, two destinations). Selectors are required on both the source and destination sides when two VC SNCP paths (rings) are interconnected at a single node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F169 Create a Half Circuit on an SNCP Node, page 6-19</a> The Source page of the Circuit Creation wizard must be open.
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From the Node drop-down list, choose the node that will contain the half circuit.
- Step 2** From the Slot drop-down list, choose the slot containing the card where the circuit will originate.
- Step 3** From the Port drop-down list, choose the port where the circuit will originate. This field might not be available, depending on the card chosen in [Step 2](#).
- Step 4** Complete one of the following:
- For low-order VC12 circuits, choose VC4, TUG3, TUG2, and VC12.
  - For low-order VC11 circuits, choose VC4, TUG3, TUG2, and VC11.
  - For low-order VC3 circuits, choose VC4 and VC3.
  - For high-order circuits, choose VC4.
- Step 5** If you want to create an SNCP ring with two sources, click **Use Secondary Source** and repeat Steps [1](#) through [4](#). If not, skip this step and continue with [Step 6](#).
- Step 6** Click **Next**.
- Step 7** From the Node drop-down list, choose the node chosen in [Step 1](#).
- Step 8** From the Slot drop-down list, choose the optical (STM-N) card to map the low-order VC3, VC11, or VC12 circuit for optical transport or to map the VC4 circuit to a synchronous transport module (STM).
- Step 9** From the Port drop-down list, choose the destination port.
- Step 10** If applicable, choose the destination VC.
- Step 11** If you want to create an SNCP ring with two destinations, click **Use Secondary Destination** and repeat Steps [7](#) through [10](#).
- Step 12** Return to your originating procedure (NTP).
-

## DLP-F253 Provision RS-DCC Terminations

<b>Purpose</b>	This task creates SDH RS-DCC terminations required for alarms, administration data, signal control information, and messages.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

The RS-DCCs and MS-DCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the [“DLP-F244 Create a DCC Tunnel” task on page 17-36](#) to create a DCC tunnel.

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



### Note

RS-DCC refers to the regenerator-section DCC, which is used for ONS 15600 SDH DCC terminations. You can provision the SDH MS-DCCs and RS-DCC (when not used as a DCC termination by the ONS 15600 SDH) as DCC tunnels. See the [“DLP-F244 Create a DCC Tunnel” task on page 17-36](#). You can provision RS-DCCs and MS-DCCs on different ports in the same node. In the Port Admin State area, click **Set to unlocked** to put the port in service. When RS-DCC is provisioned, an MS-DCC termination is allowed on the same port, but is not recommended. Changing configuration of a port having RS-DCC termination to MS-DCC termination is allowed. During this upgrade both MS-DCC and RS-DCC terminations can be present on the same port. Once the MS-DCC termination is configured see [“DLP-F314 Provision MS-DCC Terminations” task on page 18-14](#), delete the RS-DCC terminations as specified in [“DLP-F321 Delete an RS-DCC Termination” task on page 18-20](#), and enable the OSPF on MS-DCC termination if not enabled see [“DLP-F320 Change an MS-DCC Termination” task on page 18-19](#)

- Step 4** Verify that the Disable OSPF on RS-DCC Link is unchecked.
- Step 5** If the RS-DCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the [“DLP-F319 Change an RS-DCC Termination” task on page 18-19](#).
- Step 6** In the Layer 3 area, perform one of the following:
- Check the IP box only—If the RS-DCC is between the ONS 15600 SDH and another ONS node and only ONS nodes reside on the network. The RS-DCC will use Point-to-Point Protocol (PPP).

- Check the IP and OSI boxes—If the RS-DCC is between the ONS 15600 SDH and another ONS node and third party NEs that use the Open System Interconnection (OSI) protocol stack are on the same network. The RS-DCC will use PPP.
- Check OSI box only—If the RS-DCC is between an ONS node and a third party NE that uses the OSI protocol stack. The RS-DCC will use the Link Access Protocol on the D Channel (LAP-D) protocol.



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

- Step 7** If you checked OSI, complete the following steps. If you checked IP only, continue with [Step 9](#).
- Click **Next**.
  - Provision the following fields:
    - Router—Choose the OSI router.
    - ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
    - ISH—Sets the Intermediate System Hello (ISH) PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
    - IIH—Sets the Intermediate System to Intermediate System Hello (IIH) PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
    - Metric—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.
- Step 8** If the OSI and IP boxes are both checked, continue with [Step 9](#). If only the OSI is checked, click **Next** and provision the following fields:
- Mode
    - AITS—(Acknowledged Information Transfer Service) (Default) Does not exchange data until a logical connection between two LAP-D users is established. This service provides reliable data transfer, flow control, and error control mechanisms.
    - UITS—(Unacknowledged Information Transfer Service) Transfers frames containing user data with no acknowledgement. The service does not guarantee that the data presented by one user will be delivered to another user, nor does it inform the user if the delivery attempt fails. It does not provide any flow control or error control mechanisms.
  - Role—Set to the opposite of the mode of the NE at the other end of the RS-DCC.
  - MTU—(Maximum transmission unit) Sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets. The default is 512. You normally should not change it.
  - T200—Sets the time between Set Asynchronous Balanced Mode (SABME) frame retransmissions. The default is 0.2 seconds. The range is 0.2 to 20 seconds.
  - T203—Provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D “keep-alive” Receive Ready (RR) frames. The default is 10 seconds. The range is 4 to 120 seconds.
- Step 9** Click **Finish**.

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

---

## DLP-F254 Change the Service State for a Port

<b>Purpose</b>	This task puts a port in service or removes a port from service.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** In node view, double-click the card with the port(s) you want to put in or out of service. The card view appears.

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

**Step 3** In the Admin State column for the target port, choose one of the following from the drop-down list:

- **Unlocked**—Puts the port in the Unlocked-enabled service state.
- **Locked,disabled**—Puts the port in the Locked-enabled,disabled service state. In this service state, traffic is not passed on the port until the service state is changed to Unlocked-enabled; Locked-enabled,maintenance; or Unlocked-disabled,automaticInService.
- **Locked,maintenance**—Puts the port in the Locked-enabled,maintenance service state. This service state does not interrupt traffic flow and loopbacks are allowed, but alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use the Locked-enabled,maintenance service state for testing or to suppress alarms temporarily. A port must be in this service state before you can apply a loopback. Change to the Unlocked-enabled or Unlocked-disabled,automaticInService when testing is complete.
- **Unlocked,automaticInService**—Puts the port in the Unlocked-disabled,automaticInService service state. In this service state, alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. After the soak period passes, the port changes to Unlocked-enabled. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.



**Note** CTC will not allow you to change a port service state from Unlocked-enabled to Locked-enabled,disabled. You must first change a port to the Locked-enabled,maintenance service state before putting it in the Locked-enabled,disabled service state.

---

For more information about service states, refer to the “Administrative and Service States” appendix of the *Cisco ONS 15600 SDH Reference Manual*.

**Step 4** If the port is in loopback (Locked-enabled,loopback & maintenance) and you set the Admin State to Unlocked-enabled, a confirmation window appears indicating that the loopback will be released and that the action could be service affecting. To continue, click **Yes**.



- Step 5** If you set Admin State to Unlocked,automaticInService, set the soak period time in the AINS Soak field. This is the amount of time that the port will stay in Unlocked-disabled,automaticInService service state after the signal is continuously received before changing to Unlocked-enabled.
- Step 6** Click **Apply**.
- Step 7** As needed, repeat this task for each port.
- Step 8** Return to your originating procedure (NTP).
- 

## DLP-F255 Remap the K3 Byte

<b>Purpose</b>	This task provisions the K3 byte. Do not remap the K3 byte unless specifically required to run an ONS 15600 SDH MS-SPRing through third-party equipment. This task is unnecessary for most users.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher



### Caution

If you remap the K3 byte, remap to the same extended byte (Z2, E2, or F1) on either side of the span.

---

- Step 1** In node view, double-click the card that connects to the third-party equipment.
- Step 2** Click the **Provisioning > Line** tabs.
- Step 3** Click **MS-SPRing Ext Byte** and choose the alternate byte: Z2, E2, or F1.
- Step 4** Click **Apply**.
- Step 5** Repeat Steps 1 through 4 at the node and card on the other end of the MS-SPRing span.



### Note

The extension byte set in Step 3 should match at both ends of the span.

---

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

## DLP-F256 Set Auto-Refresh Interval for Displayed PM Counts

<b>Purpose</b>	This task changes the window auto-refresh intervals for updating the PM counts.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34.</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

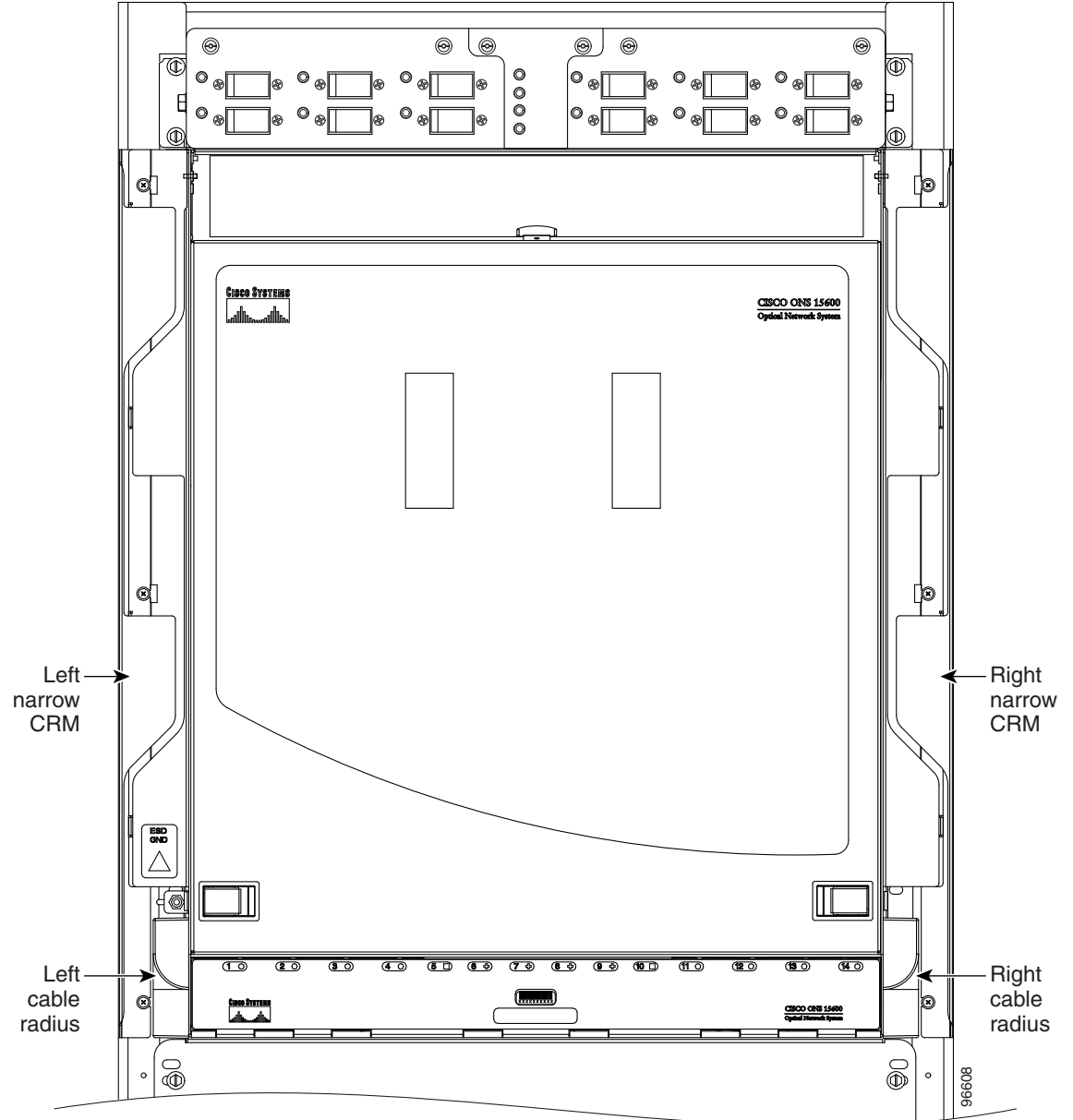
- 
- Step 1** In node view, double-click an STM-N or Ethernet port. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** From the **Auto-refresh** drop-down list choose one of the following options:
- **None:** This option disables the auto-refresh feature.
  - **15 Seconds:** This option sets the window auto-refresh to 15-second time intervals.
  - **30 Seconds:** This option sets the window auto-refresh to 30-second time intervals.
  - **1 Minute:** This option sets the window auto-refresh to one-minute time intervals.
  - **3 Minutes:** This option sets the window auto-refresh to three-minute time intervals.
  - **5 Minutes:** This option sets the window auto-refresh to five-minute time intervals.
- Step 4** Click **Refresh**. The PM counts for the new time interval appear.
- Depending on the selected auto-refresh interval, the PM counts shown automatically update when each refresh interval is complete. If the auto-refresh interval is set to None, the PM counts are not updated unless you click the Refresh button.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F257 Remove the Narrow CRMs

<b>Purpose</b>	This task removes existing narrow CRMs on the ONS 15600 SDH bay so that you can install the wide CRMs.
<b>Tools/Equipment</b>	Phillips screwdriver, 6 inches long Retaining screws
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- 
- Step 1** Use a Phillips screwdriver to loosen the three screws (approximately five revolutions each) on the existing cable routers ([Figure 17-5](#)).

Figure 17-5 Narrow CRMs



- Step 2** Lift the cable router slightly and pull it away from the bay.
- Step 3** Repeat this procedure for the router on the other side.
- Step 4** Unscrew and remove the cable radius pieces at the lower right and left sides of the shelf.
- Step 5** Return to your originating procedure (NTP).

## DLP-F258 Replace the Existing 600-mm Kick Plates with 900-mm Kick Plates

<b>Purpose</b>	This task removes the existing 600-mm (23.6-inch) kick plates so you can install the 900-mm (35.4-inch) kick plates. You should install 900-mm (35.4-inch) kick plates if you plan to install the wide CRMs.
<b>Tools/Equipment</b>	900-mm kick plate kit (53-2178-XX) Screwdriver Retaining screws
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- 
- Step 1** Using the screwdriver, remove the five screws located on the 600-mm (23.6-inch) kick plate on the front of the bay.
- Step 2** Repeat [Step 1](#) for the kick plate at the rear of the bay.
- Step 3** Place a 900-mm (35.4-inch) kick plate (700-16756-XX) at the front of the bay and use a screwdriver to install the five screws.
- Step 4** On the right side of the bay, install the side kick plate (700-16758-XX) using the two appropriate screws.




---

**Note** Make sure the side kick plate's larger flange is on the floor.

---

- Step 5** Repeat [Step 4](#) for the left and rear kick plates.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-F259 Manual Switch the Node Timing Reference

<b>Purpose</b>	This task commands the network element (NE) to switch to the timing reference you have selected if the synchronization status message (SSM) quality of the requested reference is not less than the current reference.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

- 
- Step 1** In node view, click the **Maintenance > Timing > Source** tabs. The Timing source window appears.
- Step 2** In the Reference drop-down list for the desired Clock, choose the desired reference.
- Step 3** In the Operation drop-down list, choose **Manual**.

This operation commands the node to switch to the reference you have selected if the SSM quality of the reference is not lower than the current timing reference.

- Step 4** Click **Apply**.
  - Step 5** Click **Yes** in the confirmation dialog box. If the selected timing reference is an acceptable valid reference, the node switches to the selected timing reference.
  - Step 6** If the selected timing reference is invalid, a warning dialog box appears. Click **OK**; the timing reference does not revert.
  - Step 7** Return to your originating procedure (NTP).
- 

## DLP-F260 Clear a Manual Switch on a Node Timing Reference

<b>Purpose</b>	This task clears a Manual switch on a node timing reference and reverts the timing reference to its provisioned reference.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Maintenance or higher

---

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

## DLP-F261 Set the Optical Power Received Nominal Value

<b>Purpose</b>	This task sets the optical power received (OPR) threshold for each optical card. The ONS 15600 SDH node uses the value set as a performance monitoring parameter to determine if the power level has degraded.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, double-click the optical (STM-N) card that you want to provision. The card view appears.
- Step 2** Click the **Provisioning > Optics Thresholds** tabs.
- Step 3** From the Types list, choose **TCA or Alarm** and click **Refresh**.
- Step 4** For Port 1, click **Set** in the Set OPR column. The OPR is set automatically. In the confirmation dialog box, click **OK**.
- Step 5** Repeat [Step 4](#) for each port on the card.
- Step 6** Repeat this task for each optical card.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F262 Provision the IIOP Listener Port on the ONS 15600 SDH

<b>Purpose</b>	This task provisions the IIOP listener port on the ONS 15600 SDH, which enables you to access ONS 15600 SDHs that reside behind a firewall.
<b>Tools/Equipment</b>	IIOP listener port number provided by your LAN or firewall administrator
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** If the Enable Proxy Server on port 1080 check box is checked, CTC will use Port 1080 and ignore the configured IIOP port setting. If Enable Proxy Server is subsequently unchecked, the configured IIOP listener port is used.

---

- Step 1** Click the **Provisioning > Security > Access** subtabs.
- Step 2** In the TSC CORBA (IIOP) Listener Port area, choose a listener port option:
- **Default - TSC Fixed**—(Default) Uses Port 57790 to connect to ONS 15600 SDHs on the same side of the firewall or if no firewall is used. This option can be used for access through a firewall if Port 57790 is open.
  - **Standard Constant**—Uses Port 683, the CORBA default port number.

- **Other Constant**—If Port 683 is not used, type the IIOP port specified by your firewall administrator.
- Step 3** Click **Apply**.
- Step 4** When the Change Network Configuration message appears, click **Yes**.  
Both TSCs reboot, one at a time. The reboot will take approximately 15 minutes.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F263 Provision the IIOP Listener Port on the CTC Computer

<b>Purpose</b>	This task selects the IIOP listener port on CTC. You must perform this procedure if the computer running CTC resides behind a firewall.
<b>Tools/Equipment</b>	IIOP listener port number from LAN or firewall administrator
<b>Prerequisite Procedures</b>	<a href="#">NTP-F131 Verify Card Installation, page 4-2</a> <a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	Required if the computer running CTC resides behind a firewall
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** From the Edit menu, choose **Preferences**.
- Step 2** In the Preferences dialog box, click the **Firewall** tab.
- Step 3** In the CTC CORBA (IIOP) Listener Port area, choose a listener port option:
- **Default - Variable**—(Default) Use to connect to ONS 15600 SDHs from within a firewall or if no firewall is used.
  - **Standard Constant**—Use Port 683, the CORBA default port number.
  - **Other Constant**—If Port 683 is not used, enter the IIOP port defined by your administrator.
- Step 4** Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.
- Step 5** Click **OK**.
- Step 6** In the Preferences dialog box, click **OK**.
- Step 7** To access the ONS 15600 SDH using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit** from the File menu.)
- Step 8** Return to your originating procedure (NTP).
- 

## DLP-F264 Edit SNCP Circuit Path Selectors

<b>Purpose</b>	This task changes the SNCP SF and SD thresholds, the reversion time, and PDI-P settings.
<b>Tools/Equipment</b>	None

<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a> <a href="#">NTP-F152 Provision SNCP Nodes, page 5-13</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From the View menu, choose **Go to Network View**.
- Step 2** Click the **Circuits** tab.
- Step 3** In the Circuits tab, click the SNCP circuit that you want to edit. To change the settings for multiple circuits, press the **Shift** key (to choose adjoining circuits) or the **Ctrl** key (to choose nonadjoining circuits) and click each circuit you want to change.
- Step 4** From the Tools menu, choose **Circuits > Set Path Selector Attributes**.




---

**Note** Alternatively, for single circuits, you can click Edit, then click the SNCP Selectors tab in the Edit Circuits window.

---

- Step 5** In the Path Selectors Attributes dialog box, edit the following SNCP selectors, as needed:
- Revertive—If checked, traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If not checked, traffic does not revert.
  - Reversion Time (Min)—If Revertive is checked, 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.
- Step 6** In the VC Circuits Only area, set the following thresholds:
- (Low-order circuits only) In the VC LO Circuits Only area, set the following thresholds:
    - SF threshold—Sets the SNCP signal failure BER threshold.
    - SD threshold—Sets the SNCP signal degrade BER threshold.
  - (High-order circuits only) In the VC4 Circuits Only area, set the following thresholds:
    - SF Ber Level—Sets the SNCP signal failure BER threshold.
    - SD Ber Level—Sets the SNCP signal degrade BER threshold.
    - Switch on PDI-P—When checked, traffic switches if a VC4 payload defect indication is received.
- Step 7** Click **OK** and verify that the changed values are correct.
- Step 8** Return to your originating procedure (NTP).
- 

## DLP-F265 Change the Node Name, Date, Time, and Contact Information

<b>Purpose</b>	This task changes basic node information such as node name, date, time, and contact information.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>



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



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

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

**Step 2** Change any of the following:

- General: Node Name/TID
- 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-F133 Set Up Date, Time, and Contact Information](#)” procedure on page 4-4 for detailed field descriptions.

**Step 3** Click **Apply**. Confirm that the changes appear; if not, repeat the task.

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

## DLP-F266 Enable Dialog Box Do-Not-Display Option

<b>Purpose</b>	This task enables or disables the “Do not show this dialog again” dialog box preference for subsequent sessions or disables the do-not-display option.
<b>Tools/Equipment</b>	None
<b>Prerequisite procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , page 16-34
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	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 is not displayed 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 field 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-F267 Change Security Policy on a Single Node

<b>Purpose</b>	This task changes the security policy for a single node, including idle user timeouts, user lockouts, password changes, and concurrent login policies.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** In node view, click the **Provisioning > Security > 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—Choose 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—Check this box if you want to allow a user with Superuser privileges to manually unlock a user who has been locked out from a node. The user will remain locked out until a Superuser manually unlocks the user.
  - Automatic Unlock After—Choose 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).
- Step 4** In the Password Change area, you can modify the following:

- Prevent Reusing Last [nn] Password(s)—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
- New Password must Differ from the Old Password by [nn] Characters—Choose a value between 1 and 5 to determine how many characters must change between the old and new passwords.
- Cannot Change New Password for [nn] Days—If checked, prevents users from changing their password for the specified period. Choose a value between 20 and 95 days.
- Require Password Change on First Login to New Account—Check the check box to require all new users to change their password the first time they log into their account.



**Note** “Require [nn] password change on first login to new account” or “Cannot change new password for [nn] days” is an OR statement, meaning that either one of the two conditions that you set can be satisfied for a password to be reused.

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

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

**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 0 to 99 days.



**Note** If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.

**Step 7** Click **Apply**. Confirm that the changes appear; if not, repeat the task.

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

## DLP-F268 Change Security Policy on Multiple Nodes

<b>Purpose</b>	This task changes the security policy for multiple nodes including idle user timeouts, user lockouts, password change, and concurrent login policies.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** From the View menu, 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 in the table that you want to modify, then click **Edit**.
- Step 4** In the Idle User Timeout area, you can modify the timeout values for each security level by clicking the hour (H) and minute (M) arrows. You can choose values between 0 and 16 hours and 0 and 59 minutes.
- Step 5** In the User Lockout area, you can modify the following:
- Failed Logins Allowed Before Lockout—Choose the number 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—Check this box if you want to allow a user with Superuser privileges to manually unlock a user who has been locked out from a node. The user will remain locked out until a Superuser manually unlocks the user.
  - Automatic Unlock After—Choose 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).
- Step 6** In the Password Change area, you can modify the following:
- Prevent Reusing Last [nn] Password(s)—Choose a value between 1 and 10 to set the number of different passwords the user must create before they can reuse a password.
  - New Password must Differ from the Old Password by [nn] Characters—Choose a value between 1 and 5 to determine how many characters must change between the old and new passwords.
  - Cannot Change New Password for [nn] Days—If checked, prevents users from changing their password for the specified period. Choose a value between 20 and 95 days.
  - Require Password Change on First Login to New Account—Check the check box to require all new users to change their password the first time they log into their account.




---

**Note** “Require [nn] password change on first login to new account” or “Cannot change new password for [nn] days” is an OR statement, meaning that either one of the two conditions that you set can be satisfied for a password to be reused.

---

- Step 7** In the Password Aging area, check the Enforce Password Aging check box to require users to change their password at periodic intervals. If checked, provision the following parameters:
- Aging Period—Sets the amount of time that must pass before the user must change his or her password for each security level: RETRIEVE, MAINTENANCE, PROVISIONING, and SUPERUSER. The range is 20 to 95 days.
  - Warning—Sets the number of days the user will be warned to change their password for each security level. The range is 2 to 20 days.
- 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 0 to 99 days.




---

**Note** If you advance the node date to a date beyond the threshold in the Inactive Duration box, the user account is disabled. User accounts are not reenabled if you revise the node date backwards, and the account has already been disabled.

---

- Step 9** In the Select applicable nodes list dialog box, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).
- Step 10** Click **OK**. The Security Policy Change Results dialog box appears.
- Step 11** Confirm that the changes are correct and click **OK**.
- Step 12** Return to your originating procedure (NTP).
- 

## DLP-F269 Change User Password and Security Levels for a Single Node

<b>Purpose</b>	This task changes settings for an existing user at one node. Use this procedure to change a user's password, modify the user's security level, lock out the user, disable the user, or require the user to change their password on next login.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

---

- Step 1** In node view, click the **Provisioning > Security > Users** tabs.
- Step 2** Click the user whose settings you want to modify, then click **Edit**.
- Step 3** In the Edit User dialog box, you can modify:
- New Password
  - Security Level
  - Lock Out
  - Disable
  - Change Password on Next Login

See the “[DLP-F269 Change User Password and Security Levels for a Single Node](#)” task on page 17-61 and the “[DLP-F270 Change User and Security Settings for Multiple Nodes](#)” task on page 17-62 for field descriptions.

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



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

---

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

## DLP-F270 Change User and Security Settings for Multiple Nodes

<b>Purpose</b>	This task changes an existing user's settings for multiple nodes. Use this procedure to change passwords, modify security levels, lock out users, disable users, or require users to change their passwords on next login.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	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 all the nodes where you want to add users are accessible in network view.
- Step 2** Click the **Provisioning > Security > Users** tabs. Click the user's name whose settings you want to change.
- Step 3** Click **Edit**. The Change User window appears.
- Step 4** In the Change User dialog box, you can:
- New Password
  - Security Level
  - Lock Out
  - Disable
  - Change Password on Next Login
- See the “[DLP-F269 Change User Password and Security Levels for a Single Node](#)” task on page 17-61 and “[DLP-F270 Change User and Security Settings for Multiple Nodes](#)” task on page 17-62 for field descriptions.
- Step 5** In the Select applicable nodes list dialog box, uncheck any nodes where you do not want to change the user's settings (all network nodes are selected by default).
- Step 6** Click **OK**. The User Change Results confirmation dialog box appears.
- Step 7** Click **OK**. Confirm that the changes appear; if not, repeat the task.
- Step 8** Return to your originating procedure (NTP).
- 

## DLP-F271 Log Out a User on a Single Node

<b>Purpose</b>	This task logs out a user from a single node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed

<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** In node view, click the **Provisioning > Security > Active Logins** tabs.
- Step 2** Choose the user you want to log out.
- Step 3** Click **Logout**.
- Step 4** In the Logout User dialog box, check **Lockout before Logout** if you want to lock the user out before logout. This prevents the user from logging in after logout based on parameters set under User Lockouts in the Policy tab. Either a manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the “[DLP-F267 Change Security Policy on a Single Node](#)” task on page 17-58 for more information.
- Step 5** Click **OK**. A confirmation dialog box appears.
- Step 6** Click **OK**. Confirm that the changes appear; if not, repeat the task.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F272 Log Out a User on Multiple Nodes

<b>Purpose</b>	This task logs out a user from multiple nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

- 
- Step 1** From the View menu, chose **Go To Network View**.
- Step 2** Click the **Provisioning > Security > Active Logins** tabs.
- Step 3** Choose the user you want to log out.
- Step 4** Click **Logout**.
- Step 5** In the Logout User dialog box, uncheck the nodes where you do not want to log out the user.
- Step 6** Check **Lockout before Logout** if you want to lock the user out before logout. This prevents the user from logging in after logout based on parameters set under User Lockouts in the Policy tab. Either a manual unlock by a Superuser is required, or the user is locked out for the amount of time specified in the Lockout Duration field. See the “[DLP-F267 Change Security Policy on a Single Node](#)” task on page 17-58 for more information.
- Step 7** Click **OK**. A confirmation dialog box appears.
- Step 8** Click **OK**.
- Step 9** Return to your originating procedure (NTP).
-

## DLP-F273 Check the Network for Alarms and Conditions

<b>Purpose</b>	This task verifies that no alarms or conditions exist on the network.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Remote
<b>Security Level</b>	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.
- Another way you can verify that no active switches exist is to click the **Conditions** tab, and click **Retrieve**. Make sure the Filter button is not selected.
- Step 3** Click the **Alarms** tab.
- Verify that the alarm filter is not on. See the [“DLP-F288 Disable Alarm Filtering” task on page 17-80](#) for instructions.
  - Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for procedures.
- Step 4** Return to your originating procedure (NTP).
- 

## DLP-F274 Disable Proxy Service Using Internet Explorer (Windows)

<b>Purpose</b>	This task disables proxy service for PCs running Internet Explorer. It is required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None

- 
- Step 1** From the Start menu, select **Settings > Control Panel**.



**Note** If your computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure that you are in Classic View before continuing with this procedure.

---

- Step 2** In the Control Panel window, choose **Internet Options**.



- Step 3** From the Internet Properties dialog box, click **Connections > LAN Settings**.
- Step 4** In the LAN Settings dialog box, complete one of the following tasks:
- Uncheck **Use a proxy server** to disable the service.
  - Leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15600 SDH nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS nodes on your network. Click **OK** to close each open dialog box.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F275 Disable Proxy Service Using Netscape (Windows and UNIX)

<b>Purpose</b>	This task disables proxy service for PCs and UNIX workstations running Netscape. It is required if your computer is connected to a network computer proxy server and your browser is Netscape.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required if your computer is connected to a network computer proxy server and your browser is Netscape.
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None

---

- Step 1** Open Netscape.
- Step 2** From the Edit menu, choose **Preferences**.
- Step 3** In the Preferences dialog box under Category, choose **Advanced > Proxies**.
- Step 4** In the right side of the Preferences dialog box under Proxies, perform one of the following options:
- Choose **Direct connection to the Internet** to bypass the proxy server.
  - Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15600 SDH nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.
- Step 5** Return to your originating procedure (NTP).
-

## DLP-F416 Disable Proxy Service Using Mozilla Firefox (Windows and UNIX)

<b>Purpose</b>	This task disables proxy service for PCs and UNIX workstations running Mozilla Firefox.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F126 Set Up Computer for CTC, page 3-1</a>
<b>Required/As Needed</b>	As Needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None


**Note**

You must perform this task if your computer is connected to a network computer proxy server and your browser is Mozilla Firefox.

- 
- Step 1** Open Mozilla Firefox.
- Step 2** From the Tools menu, choose **Options**.
- Step 3** In the Options dialog box under the Network tab, click **Settings**.
- Step 4** In the Connection Settings dialog box, perform one of the following options, as applicable:
- Choose the **No Proxy** radio button to disable the proxy service.
  - Choose **Manual proxy configuration** to add exceptions to the proxy server. In the **No Proxy for** option under the Manual Proxy Configuration, enter the IP addresses of the ONS 15454 nodes that you access. Separate each address with a comma. Click **OK** to close each open dialog box.


**Note**

For ONS 15454 nodes that have TCC2P cards installed with the TCC2P secure mode option enabled, enter the backplane LAN port IP addresses. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual* for additional information about secure mode.

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

## DLP-F276 Install the Narrow CRMs

<b>Purpose</b>	This task installs narrow CRMs on the ONS 15600 SDH bay.
<b>Tools/Equipment</b>	Narrow CRM kit (53-2193-01) (optional) <ul style="list-style-type: none"> <li>• Fiber radiuses (2 left and 2 right)</li> <li>• Narrow CRMs (2 left and 2 right)</li> <li>• 6x32 panhead screws for fiber radiuses (4)</li> <li>• 8x32 panhead screws for narrow CRMs (6)</li> </ul> Phillips screwdriver, 6 inches long Retaining screws
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- 
- Step 1** On the bottom left and bottom right, install the cable radius (2 screws).
- Step 2** Lift the right-side narrow CRM and align it with the three screw holes you will use to mount the CRM.
- Step 3** Use a Phillips screwdriver to tighten the three screws, starting with the bottom screw and moving up ([Figure 17-5 on page 17-51](#)).
- Step 4** Repeat this procedure for the router on the other side.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-F277 Install the Wide CRMs

<b>Purpose</b>	This task installs the wide CRMs.
<b>Tools/Equipment</b>	Wide CRM kit (53-2181-XX) (optional) <ul style="list-style-type: none"> <li>• Latch catches (2 left and 2 right)</li> <li>• Velcro tie-wrap (26)</li> <li>• Wide CRMs (2 left and 2 right)</li> <li>• 6x32 panhead screws for latch catches (8)</li> <li>• 8x32 panhead screws for wide CRMs (10)</li> </ul> Screwdriver Retaining screws
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** If you are installing CRMs on more than one shelf, it is easiest to install the lowest CRMs first.



**Note** If your site uses under-floor cabling, mount the CRMs on the sides of the bay directly next to the shelf below the node for which you want to route cables. (For instance, if you are routing cables that originate in the top shelf, mount the CRMs that will route those cables on the sides of the bay at the middle shelf level.)

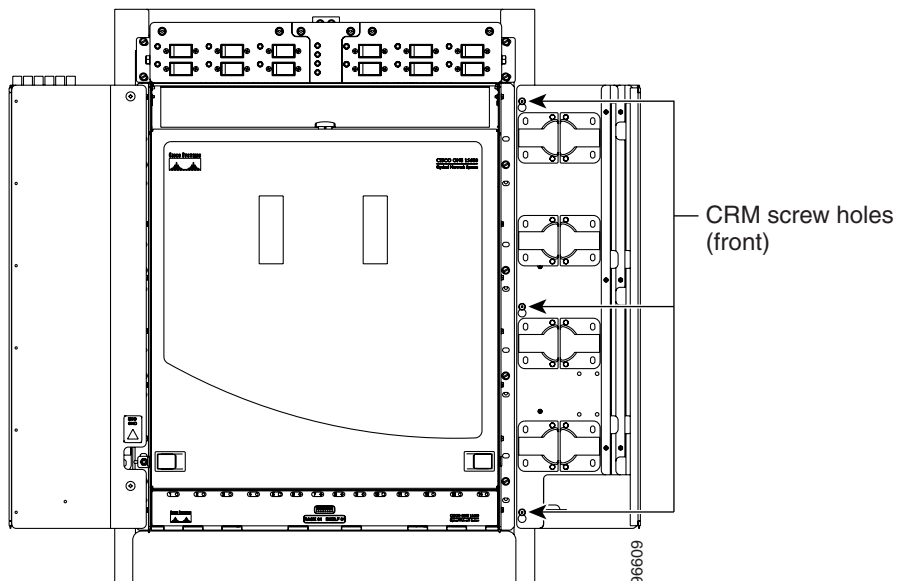
- Step 1** To install the lower latch bracket for the right-side CRM, line up the holes with the holes on the shelf where you removed the plastic cable radius.
- Step 2** Screw the two screws through the brackets into the shelf.
- Step 3** Repeat for the right-side CRM's top latch bracket.
- Step 4** Repeat Steps 1 through 3 for the left-side latch brackets.
- Step 5** On the front right edge of the bay, locate the three screw holes that will be used to secure the right-side CRM to the bay. Insert a #8 screw in the top hole and turn five revolutions. Do not tighten the screw completely, but make sure it is started enough so that it is secure in the bay (Figure 17-6).



**Note** Only the left-side CRM front door has the cutout and label for the ESD jack.

- Step 6** Repeat for the two remaining screws on that side of the bay.

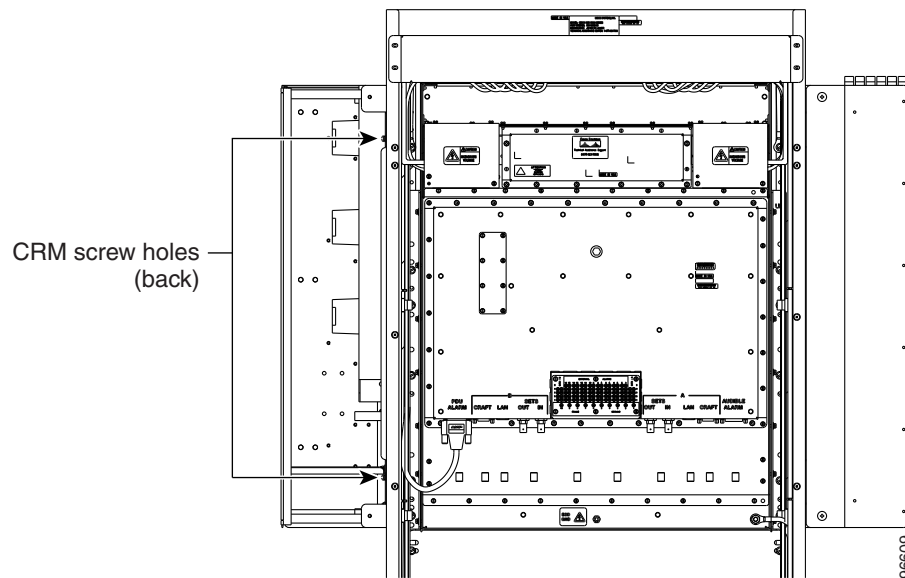
**Figure 17-6 CRM Screw Holes (Front)**



- Step 7** Align the front of the CRM keyholes with the screws and carefully slide the CRM down so it rests on the screws. Tighten the screws, starting with the bottom screw and proceeding up to the middle and top screws.

- Step 8** Locate the two screw holes on the side of the shelf toward the rear of the bay and make sure they are aligned with the holes on the CRM. Install and tighten the bottom screw and then the top screw (Figure 17-7).

**Figure 17-7 CRM Screw Holes (Back)**



- Step 9** Repeat Steps 5 through 8 for the left-side CRM.
- Step 10** Return to your originating procedure (NTP).

## DLP-F278 Use the Reinitialization Tool to Clear the Database and Upload Software (Windows)

<b>Purpose</b>	This task reinitializes the ONS 15600 SDH using the CTC reinitialization (reinit) tool on a Windows computer. Reinitialization uploads a new software package to the TSC cards, clears the node database, and restores the factory default parameters.
<b>Tools/Equipment</b>	ONS 15600 SDH System Software CD, Version 8.0 JRE 5.0 must be installed on the computer to log into the node at the completion of the reinitialization. The reinitialization tool can run on JRE 1.3.1_02, JRE 1.4.2, or JRE 5.0.
<b>Prerequisite procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only



### Note

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

- 
- Step 1** Insert the ONS 15600 SDH System Software CD, Version 8.0, 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 CISCO15600SDH 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 Reinitialization window appears.
- 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 CISCO 15600 SDH 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 TSC cards, "Complete" appears in the status bar and the TSC cards will reboot. Wait a few minutes for the reboot to complete.

- Step 8** After the reboot is complete, log into the node using the “[DLP-F181 Log into CTC](#)” task on page 16-34.
- Step 9** Complete the “[NTP-F133 Set Up Date, Time, and Contact Information](#)” procedure on page 4-4.
- Step 10** Return to your originating procedure (NTP).
- 

## DLP-F279 Connect the PDU Ground Cables to the PDU

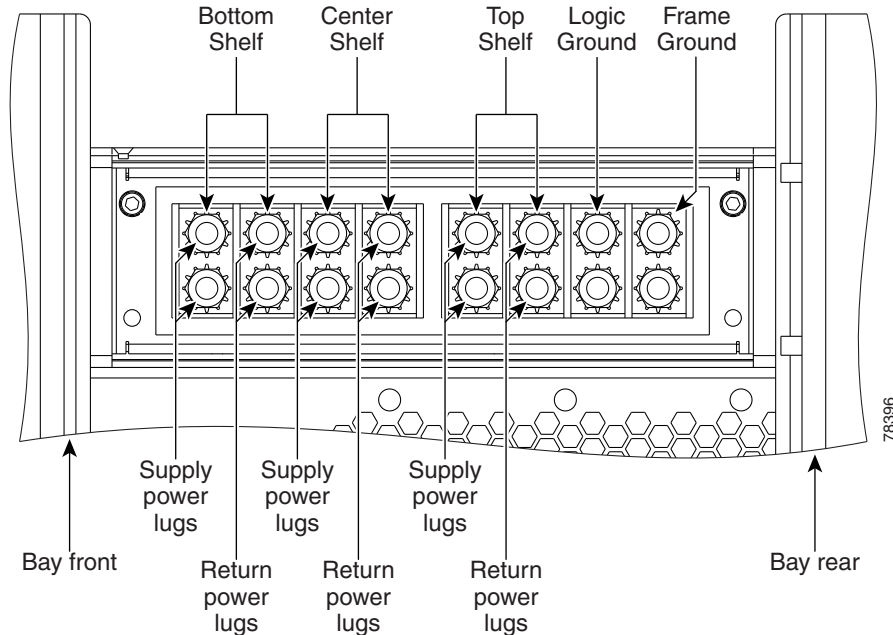
<b>Purpose</b>	This task connects the preinstalled power distribution unit (PDU) ground cables to the PDU.
<b>Tools/Equipment</b>	Screwdriver 7/16-inch (11.11 mm) socket Torque wrench calibrated to inch-pounds 9/64-inch (3.57 mm) Allen wrench
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- Step 1** Locate the PDU ground cables ([Figure 16-3 on page 16-8](#)). Remove the PDU safety cover on the right side and install the free end of the green terminal closest to the rear of the rack. This terminal is labeled “Frame Ground” in [Figure 17-8](#).



**Note** A shunt is preinstalled between logic and frame ground to bond the two grounds. If you are providing a separate logic ground, remove this shunt on both sides before installing the PDU frame ground.

---

**Figure 17-8 Power Terminal Block (Right Side Shown)**

- Step 2** Tighten the nuts to 36 in-lb.
- Step 3** Repeat Steps 1 and 2 for the left side of the PDU.
- Step 4** Replace the PDU safety covers.
- Step 5** Return to your originating procedure (NTP).

## DLP-F280 Install Isolated Logic Ground

<b>Purpose</b>	This task isolates logic ground from frame ground if required by site specifications. The ONS 15600 SDH ships with the frame ground strapped to the logic ground with metal shunts at the PDU input terminals.
<b>Tools/Equipment</b>	<ul style="list-style-type: none"> <li>Screwdriver</li> <li>Ground wire</li> <li>Two-hole power lugs, 0.625-inch hole spacing, 0.25-inch bolt holes (2) (Panduit LCCF2-14AZFW-E)</li> </ul>
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- Step 1** Remove the PDU safety cover on the right side.
- Step 2** Remove the metal shunt connecting the frame ground to the logic ground terminals. Terminal designations are marked on the top of the PDU.



- Step 3** Replace the green ground wire on the frame ground terminals and secure the wire with two Kepnuts torqued to 36 in-lb.
- Step 4** Repeat Steps 1 through 3 for the left side of the bay.
- Step 5** Build a 36-inch-long logic ground strap with two-hole lugs on each side. Use AWG #2 cable with green insulation and crimp lugs on the terminals at each end.




---

**Note** Lugs must be no wider than 0.60 inches (15.24 mm) to fit on the PDU terminals.

---

- Step 6** Put one end of the strap on the left-side PDU logic ground terminals and secure the strap with two Kepnuts torqued to 36 in-lb.
- Step 7** Put the other end of the ground strap on the right-side PDU logic ground terminals.
- Step 8** Put the two-hole lug from the office logic ground cable on the right-side PDU logic ground terminals and secure it with two Kepnuts torqued to 36 in-lb.
- Step 9** Secure the other end of the office logic ground cable to the office logic ground bar.
- Step 10** Return to your originating procedure (NTP).
- 

## DLP-F281 Check MS-SPRing or SNCP Alarms and Conditions

<b>Purpose</b>	This task checks an MS-SPRing or an SNCP for alarms and conditions before performing any major administrative change to the ring such as adding and removing nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

- Step 1** From the View menu, choose **Go to Network View**. Verify that all MS-SPRing or SNCP spans on the network map are green.
- Step 2** Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms or conditions, such as loss of signal (LOS), loss of frame alignment (LOF), alarm indication signal–line (AIS-L), SF, and SD. In an MS-SPRing, these facility conditions might be reported as minor alarms. Make sure the Filter button in the lower right corner of the window is off (not indented).
- Step 3** Click the **Conditions** tab and click **Retrieve**. Verify that no ring switches are active. Make sure the Filter button in the lower right corner of the window is off (not indented).
- Step 4** Return to the originating procedure (NTP).
-

## DLP-F282 Clear an MS-SPRing Force Ring Switch

<b>Purpose</b>	This task removes a Force switch from an MS-SPRing port.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

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

**Step 2** Click the **Provisioning > MS-SPRing** tabs.

**Step 3** Select the MS-SPRing and click **Edit**.



**Note** If node icons overlap, drag and drop the icons to a new location or return to network view and change the positions of the network node icons. MS-SPRing node icons are based on the network view node icon positions.

**Step 4** To clear a Force switch on the west line:

- a. Right-click the MS-SPRing west port where you want to clear the protection switch and choose **Set West Protection Operation**. Ports with a Force switch applied are marked with an F.
- b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.
- c. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

**Step 5** To clear a Force switch on the east line:

- a. Right-click the MS-SPRing east port where you want to clear the protection switch and choose **Set East Protection Operation**. Ports with a Force switch applied are marked with an F.
- b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list. Click **OK**.
- c. In the Confirm MS-SPRing Operation dialog box, click **Yes**.

On the MS-SPRing network graphic, a green and a purple span line connects each node. This is normal for MS-SPRings when protection operations are not invoked.

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

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

## DLP-F283 Install Public-Key Security Certificate

<b>Purpose</b>	This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 1.1 or later.
<b>Tools/Equipment</b>	None

<b>Prerequisite Procedures</b>	This task is performed during the “ <a href="#">DLP-F181 Log into CTC</a> ” procedure on page 16-34. You cannot perform it outside of this task.
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

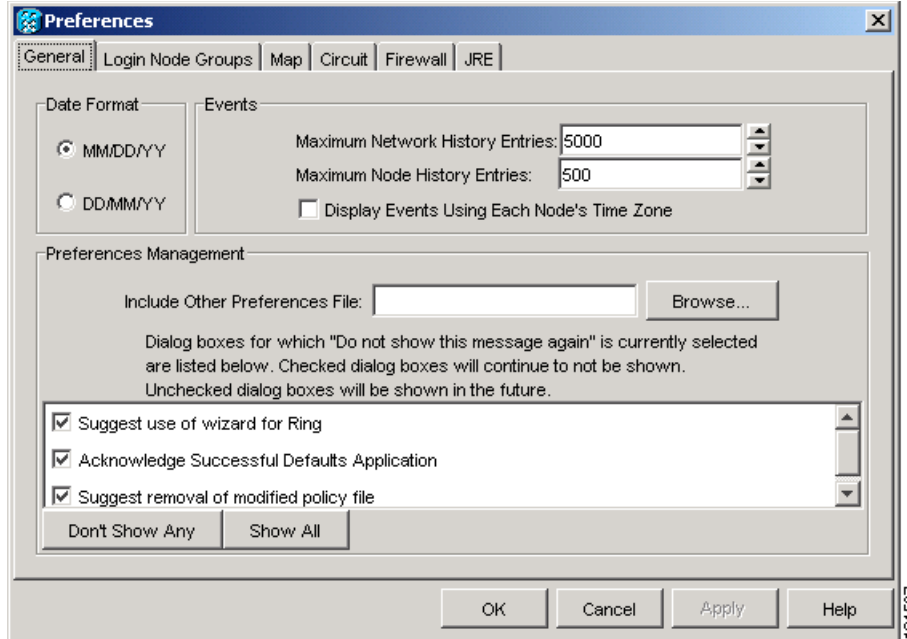
- 
- Step 1** If the Java Plug-in Security Warning dialog box appears, choose one of the following options:
- **Yes (Grant This Session)**—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15600 SDH.
  - **No (Deny)**—Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15600 SDH.
  - **Always (Grant Always)**—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
  - **More Details (View Certificate)**—Allows you to view the public-key security certificate.
- Step 2** If the Login dialog box appears, continue with [Step 3](#). If the Change Java Policy File dialog box appears, complete this step. The Change Java Policy File dialog box appears if CTC finds a modified Java policy file (.java.policy) on your PC. In Software Release 1.0, the Java policy file was modified to allow CTC software files to be downloaded to your PC. The modified Java policy file is not needed in Software R1.1 and later, so you can remove it. Choose one of the following options:
- **Yes**—Removes the modified Java policy file from your PC. Choose this option only if you will log into ONS 15600 SDHs running Software R1.4 (the first ONS 15600 SDH release) or later.
  - **No**—Does not remove the modified Java policy file from your PC. If you choose No, this dialog box will appear every time you log into the ONS 15600 SDH. If you do not want it to appear, check the **Do not show the message again** check box.
- Step 3** Return to your originating procedure (NTP).
- 

## DLP-F284 Changing the Maximum Number of Session Entries for Alarm History

<b>Purpose</b>	This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , page 16-34
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From the Edit menu, choose **Preferences**.  
The CTC Preferences Dialog box appears ([Figure 17-9](#)).

Figure 17-9 CTC Preferences Dialog Box



**Step 2** Click the up or down arrow buttons next to the Maximum History Entries field to change the entry.

**Step 3** Click **Apply** and **OK**.



**Note** Setting the Maximum History Entries value to the high end of the range uses more CTC memory and could impair CTC performance.



**Note** This task changes the maximum history entries recorded for CTC sessions. It does not affect the maximum number of history entries viewable for a network, node, or card.

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

## DLP-F285 Delete Alarm Severity Profiles

<b>Purpose</b>	This task deletes a custom or default alarm severity profile.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

**Step 2** Click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

**Step 3** Click the column heading for the profile column you want to delete.  
The selected alarm profile name appears in the Description field.

**Step 4** Click **Delete**.  
The Select Node/Profile Combination for Delete dialog box appears.

**Step 5** Click the node name(s) in the Node Names list to highlight the profile location.



**Tip** If you hold the Shift key down, you can select consecutive node names. If you hold the Ctrl key down, you can select any combination of nodes.

**Step 6** Click the profile name(s) that you want to delete in the Profile Names list.

**Step 7** Click **OK**.  
The Delete Alarm Profile confirmation dialog box appears.

**Step 8** Click **Yes** for each Delete Alarm Profile confirmation dialog box.



**Note** If you delete a profile from a node, it is still displayed in the network view Provisioning > Alarm Profiles > Alarm Profile Editor window unless you remove it by choosing Remove.

**Step 9** To remove the alarm profile from the Provisioning > Alarm Profiles > Alarm Profile Editor window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.



**Note** If a node and profile combination is selected but does not exist, a warning appears: “One or more of the profile(s) selected do not exist on one or more of the node(s) selected.” For example, if Node A has only Profile 1 and the user tries to delete both Profile 1 and Profile 2 from Node A, this warning appears. However, the operation still removes Profile 1 from Node A.



**Note** The Default and Inherited special profiles cannot be deleted and do not appear in the Select Node/Profile Combination for Delete window.

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

## DLP-F286 Enable Alarm Filtering

<b>Purpose</b>	This task filters the display of alarms, history, or conditions on the login workstation.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed

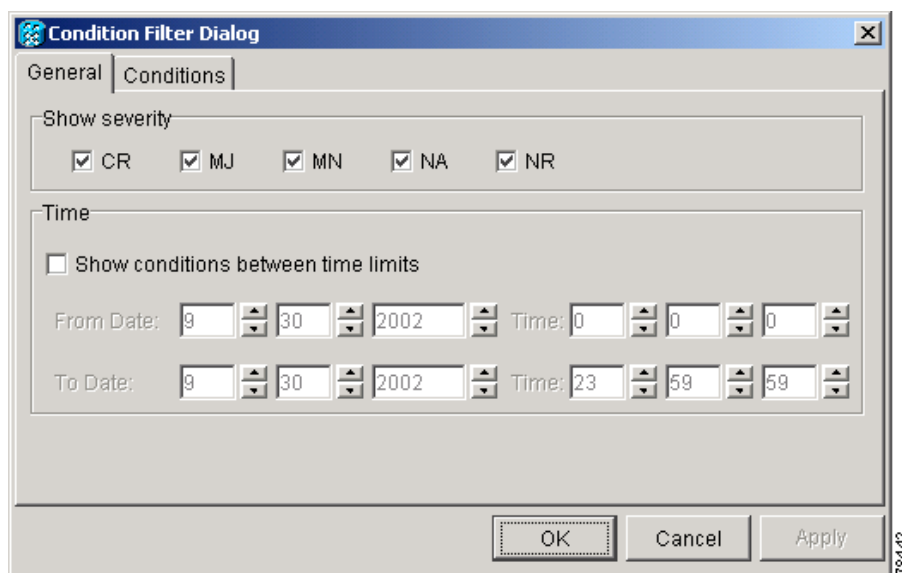
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

**Note**

The Filter button in the Alarms, History, and Conditions windows allows you to display data that meets a certain severity level, time frame, and/or condition. CTC retains user filter activation. The filter button remains active when the user logs out and logs back in.

- Step 1** In the node view Alarms, History, or Conditions windows, click **Filter**.
- Step 2** In the Filter Dialog window, click the **General** tab. The Filter Dialog box appears (Figure 17-10).

**Figure 17-10** Conditions Window Filter Dialog Box



- Step 3** In the Show Severity area, alarm severities appear. All of the applicable severities are checked by default. If a severity is checked, it appears in the alarm list.

**Note**

The Alarms window and History window have Critical (CR), Major (MJ), Minor (MN), and Not Alarmed (NA) severities available. The Conditions window also has the Not Reported (NR) severity.

Uncheck a severity to prevent it from appearing in the alarm list.

- Step 4** In the Time area:
- Check the **Enable Time** check box to establish time as a parameter in the filter.
  - Click the **From Date** and **To Date** up and down arrows to set the date range for the filter.
  - Click the **From Time** and **To Time** up and down arrows to set the time range for the filter.
- Step 5** To set conditions, click the **Conditions** tab.
- Step 6** In the Available list, double-click the desired conditions to move them to the Selected list.
- Step 7** Click **OK**.

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

---

## DLP-F287 Modify Alarm and Condition Filtering Parameters

<b>Purpose</b>	This task modifies alarm and condition reporting in all network nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F286 Enable Alarm Filtering, page 17-77</a> <a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

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

**Step 2** Click the **Filter** button at the lower-left of the bottom toolbar.

The Alarm Filter Dialog box appears, showing the General tab.

In the General tab Show Severity area, you can choose which alarm severities will show through the alarm filter and provision a time period during which filtered alarms show through the filter. To change the alarm severities shown in the filter, go to [Step 3](#). To change the time period filter for the alarms, go to [Step 4](#).

**Step 3** In the Show Severity area, click the check boxes for the severities [Critical (CR), Major (MJ), Minor (MN), or Not Alarmed (NA)] that you want to be reported at the network level. Leave severity check boxes unchecked to prevent them from appearing.

When alarm filtering is disabled, all alarms show.

**Step 4** In the Time area, click the **Show alarms between time limits** check box to enable it; then click the up and down arrows in the From Date, To Date, and Time fields to modify the period of alarms shown.

To modify filter parameters for conditions, continue with [Step 5](#). If you do not need to modify them, continue with [Step 6](#).

**Step 5** Click the **Conditions** tab.

When alarm filtering is enabled, conditions in the Show list are visible and conditions in the Hide list are invisible.

- To move conditions individually from the Show list to the Hide list, click the > button.
- To move conditions individually from the Hide list to the Show list, click the < button.
- To move conditions collectively from the Show list to the Hide list, click the >> button.
- To move conditions collectively from the Hide list to the Show list, click the << button.



**Note** Conditions include alarms.

---

**Step 6** Click **Apply** and **OK**.

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the “[DLP-F286 Enable Alarm Filtering](#)” task on page 17-77), and are not enforced when alarm filtering is disabled (see the “[DLP-F288 Disable Alarm Filtering](#)” task on page 17-80).

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

---

## DLP-F288 Disable Alarm Filtering

<b>Purpose</b>	This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F286 Enable Alarm Filtering, page 17-77</a> <a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

---

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

**Step 2** Click the **Filter** tool at the lower-right side of the bottom toolbar.

Alarm filtering is enabled if the tool is selected and disabled if the tool is raised (not selected).

**Step 3** If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and repeat [Step 2](#).

**Step 4** If you want alarm filtering disabled when you view alarm history, click the **History** tab and repeat [Step 2](#).

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

---

## DLP-F289 Manually Lock or Unlock a User on a Single Node

<b>Purpose</b>	This task manually locks out or unlocks a user from a single node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

---

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

**Step 2** Choose the user you want to lock out or unlock.

**Step 3** Click **Edit**.

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



- To lock a user out so the user cannot log into the node, check the **Locked out** check box.
- If the user is currently locked out, uncheck the **Locked out** check box.

See the “[DLP-F267 Change Security Policy on a Single Node](#)” task on page 17-58 for more information about manual lockouts and lockout duration.

- Step 5** Click **OK**. A confirmation dialog box appears.
- Step 6** Click **OK**.
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F290 Manually Lock or Unlock a User on Multiple Nodes

<b>Purpose</b>	This task manually locks out or unlocks a user from multiple nodes.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only

---

- Step 1** From the View menu, chose **Go To Network View**.
- Step 2** Click the **Provisioning > Security > Users** tabs.
- Step 3** Click the user you want to lock out or unlock.
- Step 4** Click **Edit**.
- Step 5** Complete one of the following:
- To lock a user out so the user cannot log into nodes on the network, check the **Locked out** check box.
  - If the user is currently locked out, uncheck the **Locked out** check box.
- See the “[DLP-F267 Change Security Policy on a Single Node](#)” task on page 17-58 for more information about manual lockouts and lockout duration.
- Step 6** Click **OK**. A confirmation dialog box appears.
- Step 7** Click **OK**. Confirm that the changes appear; if not, repeat the task.
- Step 8** Return to your originating procedure (NTP).
-

## DLP-F291 Verify MS-SPRing Extension Byte Mapping

<b>Purpose</b>	This task verifies that the extension byte mapping is the same on MS-SPRing trunk (span) cards that will be connected after a node is removed from an MS-SPRing. K3 extension byte mapping is supported on all ONS 15600 SDH STM-16 and STM-64 line cards, as well as the ONS 15454 SDH STM-16 card.
<b>Tools/Equipment</b>	STM-N cards must be installed at one or both ends of the MS-SPRing span that will be connected.
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In network view, double-click one of the MS-SPRing nodes with STM-N trunk cards that will be reconnected after an MS-SPRing node removal.
- Step 2** Double-click one STM-N MS-SPRing trunk card to open the card view.
- Step 3** Click the **Provisioning > Line** tab.
- Step 4** Record on paper the byte in the MS-SPRing Ext Byte column.
- Step 5** Repeat Steps 2 through 4 for the second STM-N trunk card.
- Step 6** If the trunk cards on each end of the new span are not mapped to the same MS-SPRing extension byte, remap the extension byte of the trunk card at one of the nodes. See the [“DLP-F255 Remap the K3 Byte” task on page 17-49](#).
- Step 7** Return to your originating procedure (NTP).
- 

## DLP-F292 Single Shelf Control Card Switch Test

<b>Purpose</b>	This task tests the SSXC diagnostics and the switching functionality of the TSC and SSXC cards.
<b>Tools/Equipment</b>	The test set specified by the acceptance test procedure, connected and configured as specified in the acceptance test procedure.
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Test the SSXC card switch functionality:
- Connect the test set to an STM-N slot/port on the node.
  - Create a one-way VC4-16c or VC4-64c circuit (based on the STM-N card connected in Step a) to monitor with the test set. See [Chapter 6, “Create Circuits.”](#)

- c. Verify that the test set is alarm and error free.
- d. In node view, click the **Maintenance > Preferred Copy** tabs.
- e. From the Set Preferred drop-down list, choose **Copy B**. Click **Apply**.
- f. Remove the SSXC card from Slot 8. (The SSXC card faceplate extends to cover Slot 9.)
- g. Verify that the traffic switches to Copy A. You will experience an interruption of less than 50 ms, and after that the test set should remain error free. If not, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.
- h. Replace the SSXC card and allow it to recover.
- i. Remove the SSXC card from Slot 6. (The SSXC card faceplate extends to cover Slot 7.)
- j. Verify that the traffic switches to Copy B. You will experience an interruption of less than 50 ms, and after that the test set should remain error free. If not, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.
- k. Replace the SSXC card and allow it to recover.
- l. From the Set Preferred drop-down list, choose **Copy A**. Click **Apply**.

**Step 2** Test the TSC card switch functionality:

- a. Make a note of which TSC card is active and which is standby by moving the mouse over the TSC cards on the CTC shelf graphic and viewing the tooltips. TSC cards are installed in Slot 5 and Slot 10.
- b. On the shelf graphic, right-click the active TSC card and choose **Soft-reset Card** from the shortcut menu.
- c. In the Resetting Card confirmation dialog box, click **Yes**. After 20 to 40 seconds, a “lost node connection, changing to network view” message appears.
- d. Click **OK**. On the network view map, the node with the reset TSC card will be gray.
- e. After the node icon turns yellow (from 1 to 2 minutes), double-click it. The node will remain yellow because of the UNPROT-SYNCCLK alarm for about 12 minutes. Move the mouse over the TSC cards on the shelf graphic and observe the following in the tooltips:
  - The previous standby TSC card is active.
  - The previously active TSC card is now standby.
- f. Verify that the traffic on the test set connected to the node is still running. If a traffic interruption occurs, do not continue. Refer to your next level of support.
- g. Repeat Steps **b** through **f** to return the active/standby TSC cards to their configuration at the start of the procedure.
- h. Verify that the TSC cards appear as they did in Step **a**.

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

## DLP-F293 Delete Circuits

<b>Purpose</b>	This task deletes circuits.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>

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

- 
- Step 1** Complete the “[NTP-F221 Back Up the Database](#)” procedure on page 14-4.
- Step 2** Investigate all network alarms and resolve any problems that could be affected by the circuit deletion. If necessary, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.
- Step 3** Verify that traffic is no longer carried on the circuit and that the circuit can be safely deleted.
- Step 4** Click the **Circuits** tab.
- Step 5** Choose the circuit you want to delete, then click **Delete**.
- Step 6** In the Delete Circuits confirmation dialog box, check one or both of the following, as needed:

- Check **Change drop port admin state** and choose **Locked,disabled** from the drop-down list to put the circuit source and destination ports out of service 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 state.
- If you check **Notify when completed**, the CTC Alerts confirmation dialog box indicates when all circuit source/destination ports are in the Locked,disabled service state 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 does not automatically open to show a deletion error unless you checked All alerts or Error alerts only in the CTC Alerts dialog box. For more information, see the “[DLP-F309 Configure the CTC Alerts Dialog Box for Automatic Popup](#)” task on page 18-11. If the CTC Alerts dialog box is not set to open automatically with a notification, a red triangle inside the CTC Alerts toolbar icon indicates that a notification exists.

- Step 7** 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 8](#). If you do not want to save the information, continue with [Step 9](#).
  - If you did not check “Notify when completed,” the Circuits window appears. Continue with [Step 10](#).
- Step 8** 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.
- Click **Save**.
  - Click **Browse** and navigate to the directory where you want to save the file.
  - Type the file name using a TXT file extension, and click **OK**.
- Step 9** Click **Close** to close the CTC Alerts dialog box.
- Step 10** Complete the “[NTP-F221 Back Up the Database](#)” procedure on page 14-4, if needed.

**Note**

If a schedule is established for database backup, you do not need to complete a backup after every circuit addition and deletion.

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

---

## DLP-F294 Change an STM-N Card

<b>Purpose</b>	This task describes how to change an optical (STM-N) card. To change a card, you must first delete all circuits, DCCs, and timing references on the card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher



### Caution

Physically removing an STM-N card can cause a loss of working traffic.

---



### Note

Do not use this procedure to replace a card with an identical card. Instead, use the [“DLP-F174 Delete a Card from CTC” task on page 16-17](#).

---

- Step 1** If the card the active card in a 1+1 protection group, switch traffic away from the card:
- Log into a node on the network. If you are already logged in, go to Step [b](#).
  - Display the CTC node (login) view.
  - Click the **Maintenance > Protection** tabs.
  - Double-click the protection group that contains the reporting card.
  - Click the active card of the selected group.
  - Click **Switch** in the Confirmation dialog box.
  - Click **Yes** in the Confirmation dialog box.
- Step 2** Delete all circuits, DCCs, and timing references on the card.
- Step 3** In CTC, right-click the card that you want to remove and choose **Change Card**.
- Step 4** From the Change Card drop-down list, choose the desired card type and click **OK**. A Mismatched Equipment Alarm (MEA) appears until you replace the card.
- Step 5** Physically remove the card:
- Open the card latches/ejectors.
  - Use the latches/ejectors to pull the card forward and away from the shelf.
- Step 6** Complete the [“NTP-F119 Install the STM-N Cards” procedure on page 2-4](#).
- Step 7** Return to your originating procedure (NTP).
-

## DLP-F295 Clear a Manual or Force Switch in a 1+1 Protection Group

<b>Purpose</b>	For ports configured for revertive switching, this task clears the Manual or Force switch and restores traffic to the pre-switch port. For nonrevertive ports, it clears the switch but does not revert traffic to the previous port.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F238 Initiate a Manual Switch on a Port in a 1+1 Protection Group, page 17-31</a> or <a href="#">DLP-F239 Initiate a Force Switch on a Port in a 1+1 Protection Group, page 17-32</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

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

## DLP-F296 Clear a Lock On or Lockout in a 1+1 Protection Group

<b>Purpose</b>	This task clears the lock on or lockout to resume normal protection switching capability.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F240 Apply a Lock On in a 1+1 Group, page 17-33</a> or <a href="#">DLP-F241 Apply a Lockout in a 1+1 Group, page 17-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, choose the protection group that contains the card you want to clear.
- Step 3** In the Selected Group area, choose the card 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 Lock Out is cleared.

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

## DLP-F297 Initiate a Lockout on an SNCP Path

<b>Purpose</b>	This task applies a lock out of protection to an SNCP circuit so that working traffic cannot switch to the protection path. Lockouts prevent traffic from switching under any circumstance and have a higher priority than Manual or Force switches.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-34</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** In node view, click the **Circuits > Circuits** tabs.
- Step 2** Click the path you want to switch and click **Edit**.
- Step 3** In the Edit Circuit window, click the **SNCP Selectors** tab.
- Step 4** In the Switch State column, click the row for the path you want to switch and select **Lockout of Protection**.



**Note** Refer to the *Cisco ONS 15600 SDH Reference Manual* for a description of protection switching and switch state priorities.

---

- Step 5** Click **Apply**.
- Working traffic is prevented from switching to the protect path. To clear the SNCP path Lock Out, complete the [“DLP-F298 Clear a Switch or Lockout on an SNCP Circuit” task on page 17-88](#).
- Step 6** Return to your originating procedure (NTP).
-

## DLP-F298 Clear a Switch or Lockout on an SNCP Circuit

<b>Purpose</b>	This task clears an external switching command on an SNCP circuit.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F242 Initiate a Manual Switch on an SNCP Circuit, page 17-35</a> , or <a href="#">DLP-F243 Initiate a Force Switch to an SNCP Circuit, page 17-35</a> , or <a href="#">DLP-F297 Initiate a Lockout on an SNCP Path, page 17-87</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** Click the **Circuits > Circuits** tabs.
- Step 2** Click the path you want to switch and click **Edit**.
- Step 3** In the Edit Circuit window, click the **SNCP Selectors** tab.
- Step 4** In the Switch State column, click the row for the path you want to switch and select **Clear**.
- Step 5** Click **Apply**.




---

**Note** This task does revert traffic unless ports are configured for revertive switching.

---

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

## DLP-F299 Verify Fan Operation

<b>Purpose</b>	This task verifies that all fans are working before you insert the cards. Insufficient cooling by the fans can damage the equipment.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Warning**

---

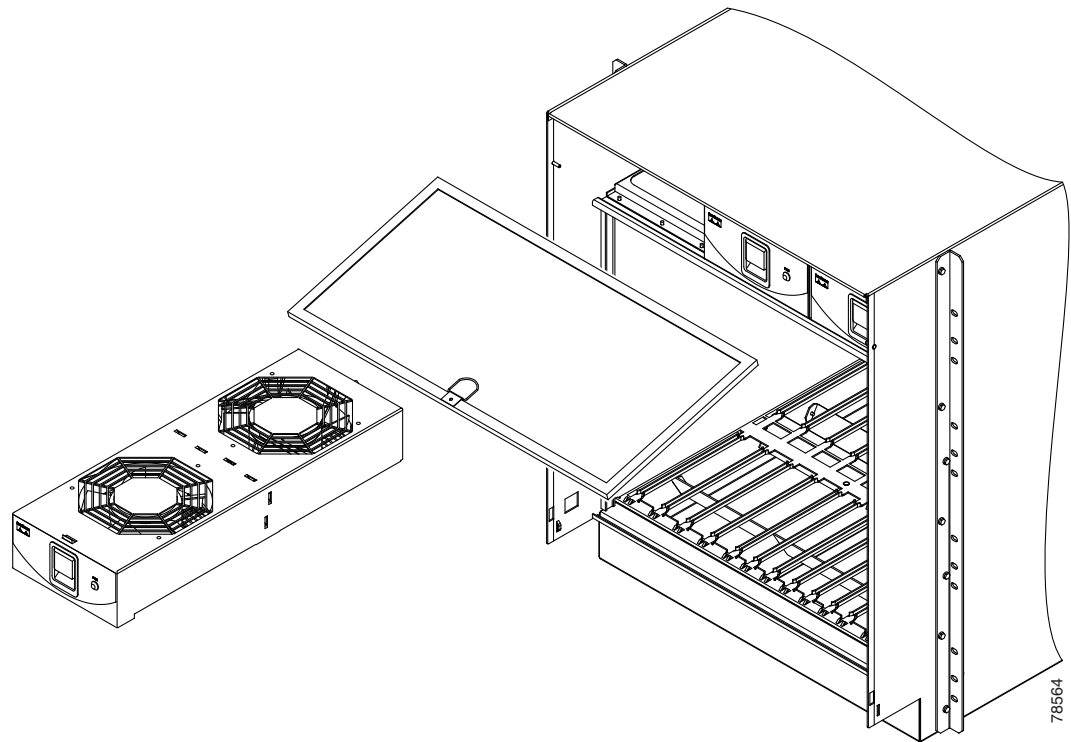
**Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.** Statement 166

---

- Step 1** Locate the three fan trays at the front of the bay. [Figure 17-11](#) shows an unpopulated ONS 15600 SDH with one of the three fan trays and the fan-tray air filter removed.



**Figure 17-11** ONS 15600 SDH Shelf with One Fan Tray and Air Filter Removed



- Step 2** To ensure the three front fans are operating, carefully place your hand in the card cage two to three inches (50 to 76 mm) from the top of the cage, palm up, to feel for air flow from each fan. If you do not feel air flow from one or more fans, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* and make sure all fans work before you install any cards.
- Step 3** To ensure the three rear fans are operating, at the back of the bay carefully place your hand in the fan outlet area above the CAP and place your palm face down on the grate to feel for air flow from each fan. If you do not feel air flow from one or more fans, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* and make sure all fans work before you install any cards.
- Step 4** Return to your originating procedure (NTP).
-

