



## DLPs E1 to E99

---



### Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

---

## DLP-E1 Unpack and Verify the Bay Assembly

<b>Purpose</b>	This task removes the bay assembly from the package.
<b>Tools/Equipment</b>	Scissors Phillips screwdriver 3/4-in. Society of Automotive Engineers (SAE) socket wrench
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



### Warning

**In order to safeguard both equipment and personnel during the installation process, we recommend that four people participate in moving the unit. Using adequate manpower is the best guarantee that you will avoid harming people or equipment.** Statement 129

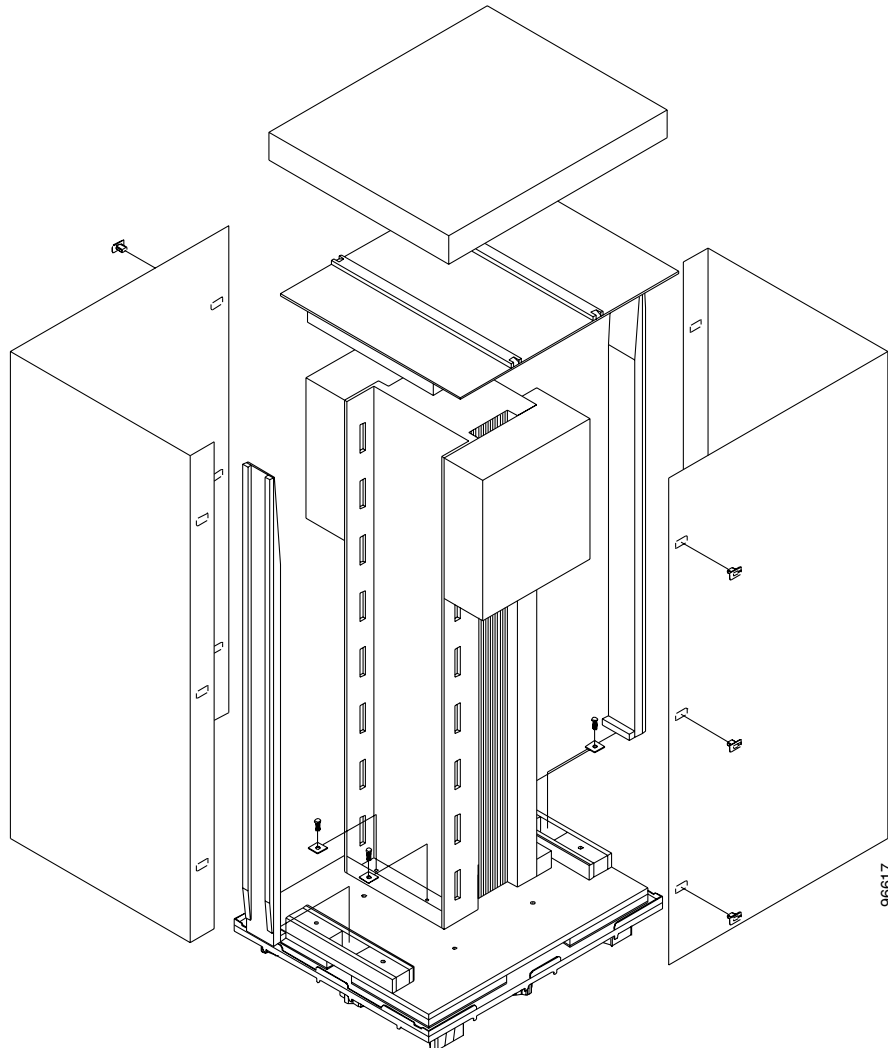
---

### Step 1

Use a pallet jack or forklift to place the shipping container as close to the installation location as possible. Ensure that the space is sufficient to unpack the ONS 15600.

[Figure 16-1](#) shows the packaging you must remove from the ONS 15600.

**Figure 16-1** ONS 15600 Bay Assembly Packaging



- Step 2** Cut all of the plastic banding off the cardboard shipping container.
- Step 3** Remove the cap from the corrugated container.
- Step 4** Pull the side panels away from the shipping pallet and set them aside.
- Step 5** Cut the banding that holds the top cap and ramps on the bay.
- Step 6** Remove the top cap and ramps and set them aside.
- Step 7** Carefully cut the plastic covering off the bay and remove.
- Step 8** Remove the four bolts that hold the rack to the pallet (rack base bolts) using a 3/4-in. socket wrench.
- Step 9** Open all other boxes shipped with this product. Verify that you have received all of the contents listed in the [“Included Materials”](#) section on page 1-2.
- Step 10** Return to your originating procedure (NTP).

## DLP-E2 Inspect the Bay Assembly

<b>Purpose</b>	This task verifies that all parts of the bay assembly are in good condition.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E1 Unpack and Verify the Bay Assembly, page 16-1</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- 
- Step 1** Look for any loose parts on the bay assembly.
- Step 2** Verify that the wire-wrap pins on the customer access panel (CAP) at the rear of the bay are not bent or broken.
- Step 3** Verify that the power distribution unit (PDU) is not damaged.
- Step 4** If the pins on the CAP are bent or broken or the PDU is damaged, call your Cisco sales engineer for a replacement.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-E3 Install the Dollies onto the Bay Assembly

<b>Purpose</b>	This task explains how to install the dollies on the bay assembly to assist with unloading the bay assembly at your site.
<b>Tools/Equipment</b>	Dollies (2) Ratchet 6-in. (or greater) ratchet extension (optional) 1-1/8-in. SAE socket 3/4-in. SAE socket 15/16-in. SAE socket
<b>Prerequisite Procedures</b>	<a href="#">NTP-E1 Unpack and Inspect the ONS 15600 Bay Assembly, page 1-4</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** For information about obtaining installation dollies, contact your Cisco sales engineer.

---

- Step 1** Inspect the dollies to make sure the caster wheels turn freely. If the wheels come in contact with the metal frame of the dolly, turn the screws at the top of the dolly until the wheels move freely.
- Step 2** Use a ratchet to unscrew and remove the bolts attached to the top of one of the dollies.
- Step 3** Line up the holes on one dolly with the holes at the front base of the bay.

**Step 4** Use a ratchet to install the screws that secure the dolly to the bay.



---

**Note** A 6-in. (or greater) ratchet extension might be helpful when you install the dolly screws.

---

**Step 5** Repeat Steps 2 through 4 to attach the other dolly to the rear base of the bay.

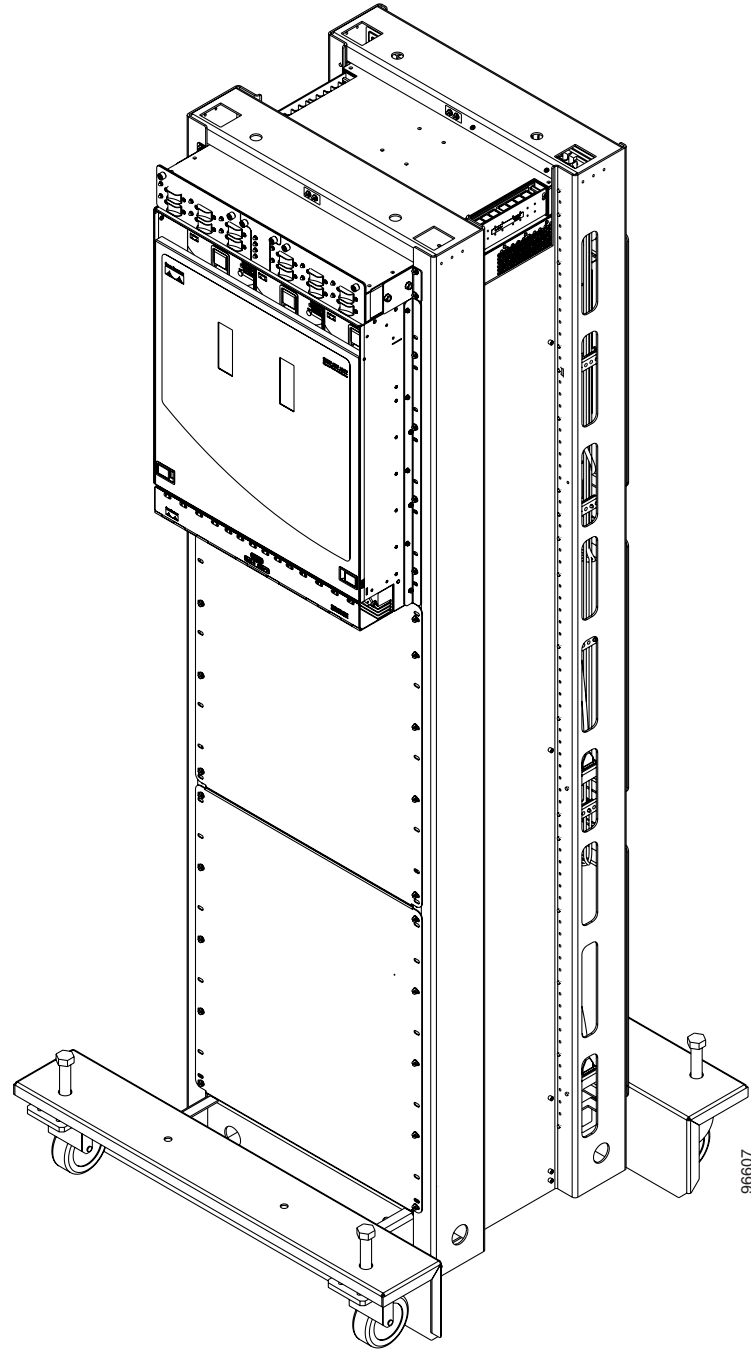
**Step 6** Use a socket wrench to turn one of the screws attached to a caster five turns to the right (clockwise). Repeat this at each screw and repeat in sequence so that the bay gradually rises to maximum height (1-3/4 in. [44.45 mm]) off the pallet.

**Step 7** Lay the wooden ramps down so that they line up with the dolly wheels.

**Step 8** Remove the wooden blocks from the pallet to allow the bay to roll down the wooden ramps.

**Step 9** With one person on each side of the bay assembly, carefully roll the bay down the ramps and onto the floor ([Figure 16-2](#)).

Figure 16-2 ONS 15600 with Dollies Installed



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

---

## DLP-E4 Install the Bay Assembly

<b>Purpose</b>	This task explains how to install the bay assembly at the installation site.
<b>Tools/Equipment</b>	<p>Ratchet</p> <p>6-in. (or greater) ratchet extension (optional)</p> <p>SAE socket wrench</p> <p>SAE torque wrench</p> <p>Phillips screwdriver, 6 in. long</p> <p>600-mm kick plate kit (53-2177-XX), or 900-mm kick plate kit (53-2178-XX)</p> <p>Rectangular seismic washers (4) (53-2141-XX)</p> <p>5/8-in. floor anchor bolts (4)</p>
<b>Prerequisite Procedures</b>	<p><a href="#">NTP-E1 Unpack and Inspect the ONS 15600 Bay Assembly, page 1-4</a></p> <p><a href="#">DLP-E109 Drill Holes to Anchor and Provide Access to the Bay Assembly, page 17-9</a></p> <p><a href="#">DLP-E3 Install the Dollies onto the Bay Assembly, page 16-3</a></p>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** This procedure describes how to install an ONS 15600 bay in an overhead power environment. Test and install according to local site practice.

- 
- Step 1** Place the bay directly over the bolt holes in the floor. (To install an ONS 15600 in a raised-floor environment, place the bay directly over the studs that protrude from the floor.)
- Step 2** Position the four rectangular seismic washers and floor bolts into the bolt holes.
- Step 3** Use a socket wrench to turn one of the screws attached to a caster five turns to the left (counter-clockwise). Repeat this at each screw and repeat in sequence so that the bay gradually lowers and firmly rests on the floor.
- Step 4** Use a ratchet and socket to remove the two bolts that attach the dolly to the bay.



**Note** A 6-in. (or greater) ratchet extension might be helpful when you remove the dolly bolts.

- Step 5** Repeat Steps 3 and 4 for the other dolly.
- Step 6** Use the torque wrench to torque the 5/8-in. floor bolts according to the bolt manufacturer's torque specification.
- Step 7** Install both kick plates at the front and rear base of the bay:
- Line up the kick plates with the holes on the bay's frame.
  - Use a Phillips screwdriver to tighten the five screws that fasten each kick plate to the bay.

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

---

## DLP-E5 Connect the Office Ground to the ONS 15600

<b>Purpose</b>	This task connects the office ground to the ONS 15600 bay assembly.
<b>Tools/Equipment</b>	<p>7/16-in. SAE socket</p> <p>Socket driver</p> <p>Ground cable, rated for at least 125-A delivery</p> <p>Crimp tool</p> <p>Wire strippers</p> <p>Wire cutters</p> <p>Listed pressure terminal connectors (two hole lug, 0.63-in. spaced, 1/4-in. bolt size); connectors must be suitable for at least 125-A delivery copper conductors</p> <p>Antioxidant compound</p>
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

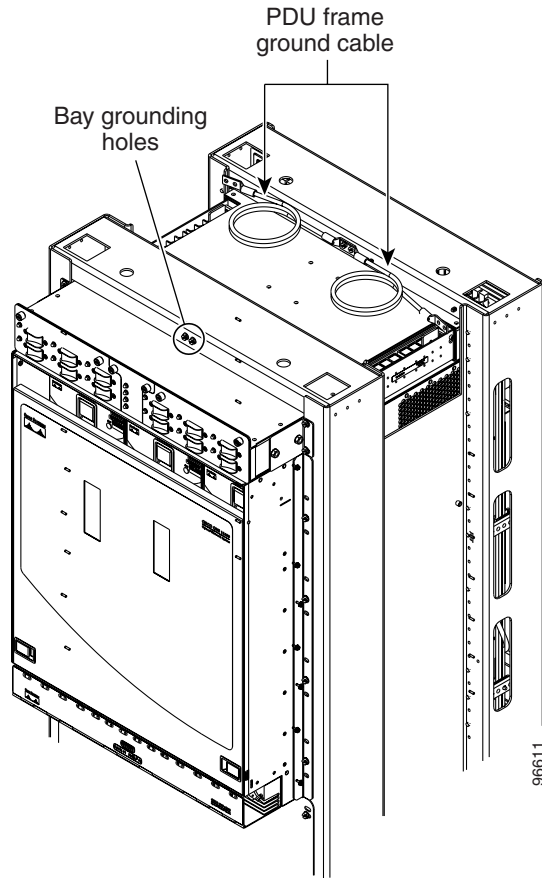


**Warning**

**Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 213

---

**Step 1** Remove any paint from the two-hole lug position on the bay front ground holes ([Figure 16-3](#)).

**Figure 16-3 PDU Ground Cables and Grounding Holes**

- Step 2** Apply the antioxidant compound to the two-hole lug position.
  - Step 3** Connect the office ground cable to the bay front two-hole lug position.
  - Step 4** Return to your originating procedure (NTP).
-



## DLP-E6 Create an IP-Encapsulated Tunnel

<b>Purpose</b>	This task creates a an IP-encapsulated tunnel to transport traffic from third-party SONET equipment across ONS 15600 networks. IP-encapsulated tunnels are created on the Section data communications channel (SDCC) channel (D1-D3) (if not used by the ONS 15600 as a terminated DCC).
<b>Tools/Equipment</b>	OC-N cards must be installed.
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a> <a href="#">NTP-E167 Verify Network Turn-Up, page 6-2</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

Each ONS 15600 can have up to 128 IP-encapsulated tunnel connections. Terminated Section DCCs (SDCCs) used by the ONS 15600 cannot be used as a tunnel endpoint, and a SDCC that is used as a tunnel endpoint cannot be terminated. All tunnel connections are bidirectional.

- 
- Step 1** Verify that IP addresses are provisioned at both the source and destination nodes of the planned tunnel. For more information, see the [“DLP-E30 Provision IP Settings” task on page 16-44](#).
- Step 2** In network view, click the **Provisioning > Overhead Circuits** tabs.
- Step 3** Click **Create**.
- Step 4** In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:
- Name—Type the tunnel name.
  - Type—Choose **IP Tunnel-D1-D3**.
  - Maximum Bandwidth—Type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).
- Step 5** Click **Next**.
- Step 6** In the Circuit Source area, complete the following:
- Node—Choose the source node.
  - Slot—Choose the source slot.
  - Port—If available, choose the source port.
  - Channel—Displays IPT (D1-D3).
- Step 7** Click **Next**.
- Step 8** In the Circuit Destination area, complete the following:
- Node—Choose the destination node.
  - Slot—Choose the destination slot.
  - Port—If available, choose the destination port.
  - Channel—Displays IPT (D1-D3).
- Step 9** Click **Finish**.

- Step 10** Put the ports that are hosting the IP-encapsulated tunnel in service. See the “[DLP-E115 Change the Service State for a Port](#)” task on page 17-16 for instructions.
- Step 11** Return to your originating procedure (NTP).
- 

## DLP-E7 Delete a Section DCC Termination

<b>Purpose</b>	This procedure deletes a Section DCC termination on the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC</a> , page 16-39
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** Deleting a SDCC termination might cause you to lose visibility of nodes that do not have other data communications channels (DCCs) or network connections to the Cisco Transport Controller (CTC) computer.

---



**Note** If you have circuits traversing the fiber on which you delete a DCC termination, the circuits will go to an Incomplete state.

---

- Step 1** In node view, click the **Provisioning > DCC/GCC** tabs.
- Step 2** Select the DCC termination and click **Delete**. The Delete SDCC Termination dialog box appears.
- Step 3** Check the **Set Port Out of Service** check box if you want to change the port state to out of service (this might be service affecting).
- Step 4** Click **Yes**. Confirm that the changes appear; if not, repeat the task.
- Step 5** Return to your originating procedure (NTP).
-

## DLP-E8 Connect Office Power to the ONS 15600 Bay

<b>Purpose</b>	This task connects power to the ONS 15600 bay assembly.
<b>Tools/Equipment</b>	<p>9/64-in. Allen wrench</p> <p>Wire-wrap tool (suitable for #22 to #28 AWG alarm wires)</p> <p>Wire cutters</p> <p>Wire strippers</p> <p>Crimp tool</p> <p>Power cables, rated for at least 125-A delivery</p> <p>Listed pressure terminal connectors (two hole lug, 0.63-in. spaced, 1/4-in. bolt size); connectors must be suitable for at least 125-A delivery copper conductors</p>
<b>Prerequisite Procedures</b>	<a href="#">DLP-E5 Connect the Office Ground to the ONS 15600, page 16-7</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



### Warning

**This warning applies only to units equipped with DC input power supplies. Wire the DC power supply using the appropriate lugs at the wiring end. The proper wiring sequence is ground to ground, positive to positive (line to L), and negative to negative (neutral to N). Note that the ground wire should always be connected first and disconnected last.** Statement 152



### Caution

Cisco supports only dual office-power feeds.



### Note

If you encounter problems with the power supply, refer to the *Cisco ONS 15600 Troubleshooting Guide*.

### Step 1

Measure and cut the cables as needed to reach the ONS 15600 PDU from the office power distribution panel. [Figure 17-5 on page 17-37](#) shows the ONS 15600 power terminal block on the right side (B side) of the bay.

### Step 2

If either PDU terminal cover is still installed, use the 9/64-in. Allen wrench to loosen the two screws that hold the plastic PDU. Pull the cover away from the shelf and set the cover aside.



### Note

Use only pressure terminal connectors, such as two-hole lug types, when terminating the battery, battery return, and frame ground conductors.



### Caution

Before you make any crimp connections, coat all bare conductors (battery, battery return, and frame ground) with an appropriate antioxidant compound. Bring all unplated connectors, braided strap, and bus bars to a bright finish, then coat with an antioxidant before you connect them. You do not need to prepare tinned, solder-plated, or silver-plated connectors and other plated connection surfaces, but always keep them clean and free of contaminants.



---

**Caution** When terminating power, return, and frame ground, do not use soldering lug, screwless (push-in) connectors, quick-connect, or other friction-fit connectors.

---

**Step 3** Strip 1/2 in. (12.7 mm) of insulation from all power cables that you will use.

**Step 4** If the bay is being installed in a raised-floor environment, complete the “[DLP-E9 Route and Terminate Raised-Floor Power Cables](#)” task on page 16-13.

**Step 5** Crimp the lugs onto the ends of all power leads.



---

**Note** When terminating battery and battery return connections as shown in [Figure 17-5 on page 17-37](#), follow a torque specification of 36 in-lb. When terminating a frame ground, use the Kepnut provided with the ONS 15600 and tighten it to a torque specification of 36 in-lb.

---

**Step 6** Put the 48 VDC power return wire on the third pair of screw posts (counting from the rear of the PDU).



---

**Note** All screw posts are labeled at the top of the PDU.

---

**Step 7** Put the 48 VDC power supply wire on the fourth pair of screw posts.

**Step 8** Hold the plastic safety cover in place over the power leads. Use the 9/64-in. Allen wrench to tighten the two screws that hold the plastic safety cover in place.

**Step 9** Repeat Steps 6 through 8 for the left (A) side of the bay.

**Step 10** Apply power to the node.

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

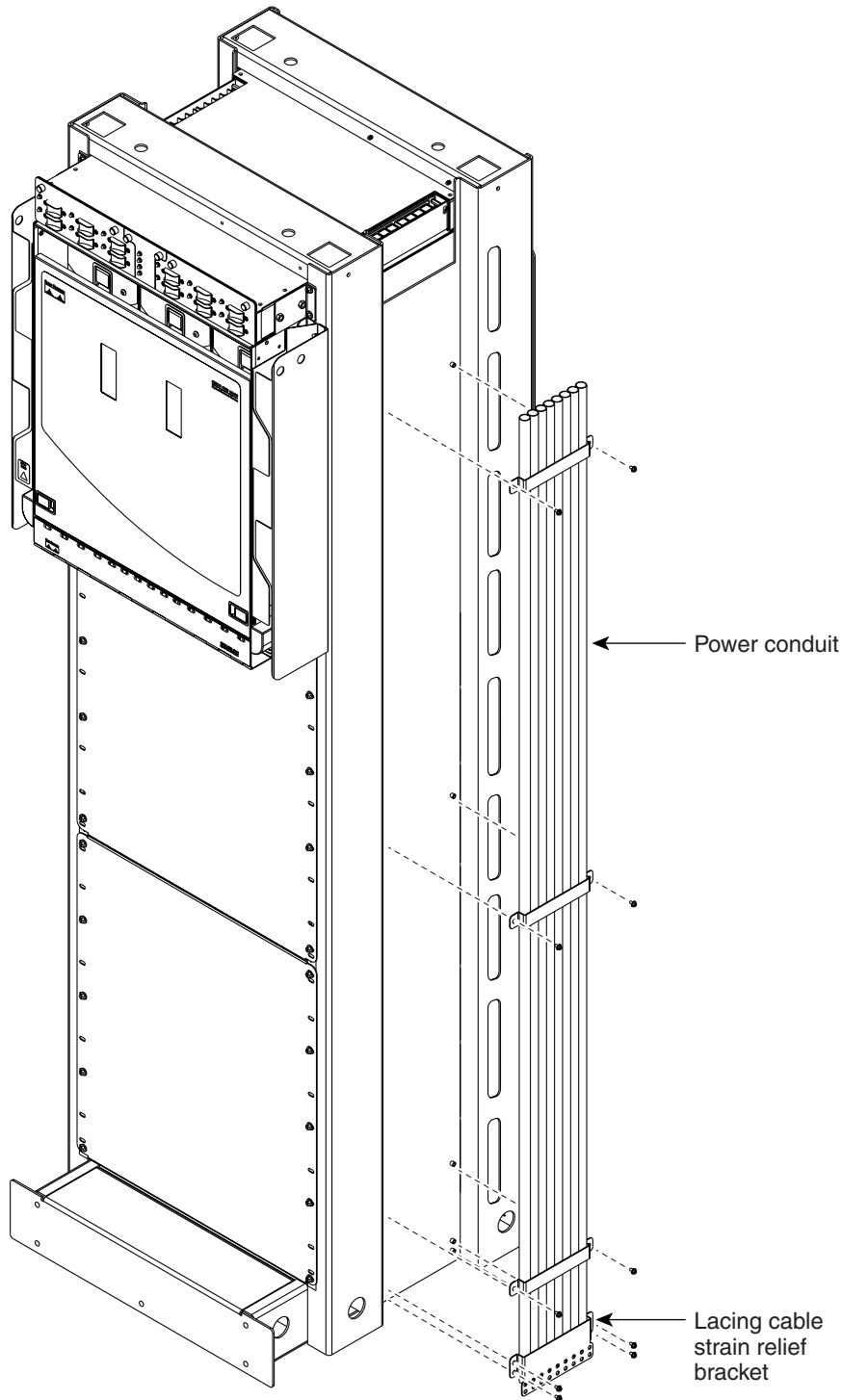
---

## DLP-E9 Route and Terminate Raised-Floor Power Cables

<b>Purpose</b>	This task installs the power conduit included in the raised-floor power kit and routes and terminates the power cables.
<b>Tools/Equipment</b>	<p>Screwdriver</p> <p>Ground cables, rated for at least 125-A capacity</p> <p>Two-hole power lugs, 0.625-in. hole spacing; 0.25-in. bolt holes (Panduit LCCF2-14AZFW-E) (for underfloor-routed power cables) (16)</p> <p><b>Note</b> You must use the specified lug type in order to terminate raised floor cables.</p> <p>Raised-floor power kit (800-23062-XX), which includes:</p> <ul style="list-style-type: none"> <li>• Screws and washers, #8 x 0.75 in. (12)</li> <li>• Screws and washers, #8 x 0.375 in. (8)</li> <li>• Power conduits (2)</li> <li>• Strain-relief cable brackets (2)</li> <li>• Panduit heat shrink #HSTT50-C</li> </ul>
<b>Prerequisite Procedures</b>	<p><a href="#">DLP-E5 Connect the Office Ground to the ONS 15600, page 16-7</a></p> <p><a href="#">DLP-E8 Connect Office Power to the ONS 15600 Bay, page 16-11</a></p>
<b>Required/As Needed</b>	As needed for bays installed in a raised-floor environment where the power cables originate from the floor.
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- 
- Step 1** On either side of the bay, locate the holes provided to mount the power conduit ([Figure 16-4](#)).
- Step 2** On one side of the bay, line up the conduit's braces with the mounting holes.
- Step 3** Use a screwdriver to install 6 screws (0.75 in.) into the mounting holes with one washer under the head of each screw.

**Figure 16-4** Installing the Power Conduit in a Raised-Floor Power Environment



78393

- Step 4** Line up the strain-relief cable bracket at the base of the conduit. Install four of the 0.375-in. screws.
- Step 5** Carefully push the power cables up through the conduit.
- Step 6** Place the heat shrink tube on the cable.

- Step 7** Crimp a lug onto one of the power cables.
  - Step 8** Put the heat shrink over the barrel of the power terminals to provide insulation.
  - Step 9** Secure the lug with the two nuts provided onto the PDU terminal. Torque to 36 in-lb.
  - Step 10** Lace or tie-wrap the cable to the cable strain relief bracket according to local site practice.
  - Step 11** Repeat Steps 7 through 10 for every power and ground cable on that side of the bay.
  - Step 12** Repeat this task for the other side of the bay.
  - Step 13** Return to your originating procedure (NTP).
- 

## DLP-E10 Verify Office Power

<b>Purpose</b>	This task measures the power to verify correct power and returns.
<b>Tools/Equipment</b>	Voltmeter
<b>Prerequisite Procedures</b>	<a href="#">DLP-E5 Connect the Office Ground to the ONS 15600, page 16-7</a> <a href="#">DLP-E8 Connect Office Power to the ONS 15600 Bay, page 16-11</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

- Step 1** Turn office power on to the A side of the PDU and turn office power off to the B side of the PDU.
- Step 2** Observe that the A side, Shelf 1 green LED is lit on the front face of the PDU. The green LED indicates the voltage is within the appropriate range and the polarity is correct. Reversed voltage will result in unlit LEDs. Red LEDs indicate the circuit breakers are off or voltage is too low. Diagnose any errors and correct before continuing with this procedure. Refer to the *Cisco ONS 15600 Troubleshooting Guide* for more information.
- Step 3** To verify power using a voltmeter, place the black test lead of the voltmeter to the PDU A-side frame ground input terminal. Place the red test lead to the PDU A-side supply input terminal. Verify that the voltage reading is between  $-40.5$  VDC and  $-57$  VDC.




---

**Note** All PDU terminals are labeled on the top of the PDU.

---

- Step 4** To verify ground, place the black test lead of the voltmeter to the PDU A-side frame ground input terminal. Place the red test lead to the PDU A-side logic ground terminal and verify that no voltage is present.
- Step 5** Turn office power on to the B side of the PDU and turn office power off to the A side of the PDU.
- Step 6** Observe that the B side, Shelf 1 green LED is lit on the front face of the PDU. Diagnose any errors and correct them before continuing with this task.
- Step 7** To verify power using a voltmeter, put the black test lead of the voltmeter to the PDU B-side frame ground input terminal. Put the red test lead to the PDU B-side supply input terminal. Verify that the voltage reading is between  $-40.5$  VDC and  $-57$  VDC.
- Step 8** To verify ground, put the black test lead of the voltmeter to the PDU B-side frame ground input terminal. Put the red test lead to the PDU B-side logic ground terminal and verify that no voltage is present.

- Step 9** Turn office power back on to the A side of the PDU.
- Step 10** Return to your originating procedure (NTP).
- 

## DLP-E11 Install Alarm Wires on the CAP

<b>Purpose</b>	This task installs the alarm wires on the CAP.
<b>Tools/Equipment</b>	Wire-wrap tool (suitable for #22 to #28 AWG alarm wires) #22 to #28 AWG wires Audible alarm cable with DB-15 connector
<b>Prerequisite Procedures</b>	<a href="#">NTP-E4 Install the Bay Power and Ground, page 1-9</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

- Step 1** Wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. [Figure 16-5](#) shows the backplane of the ONS 15600 shelf and the location of the alarm pin field on the CAP.



Figure 16-5 Rear of the ONS 15600, Including the CAP

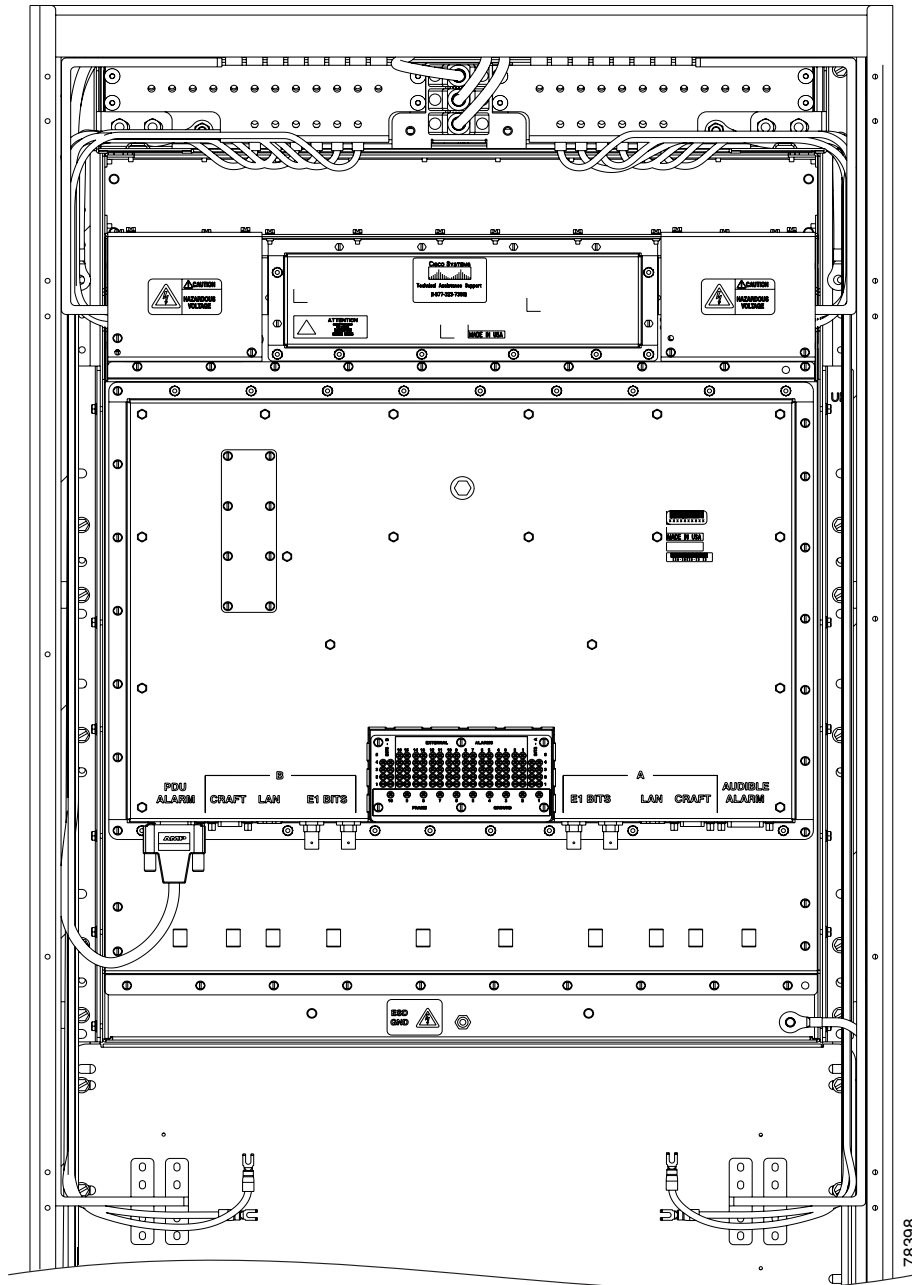
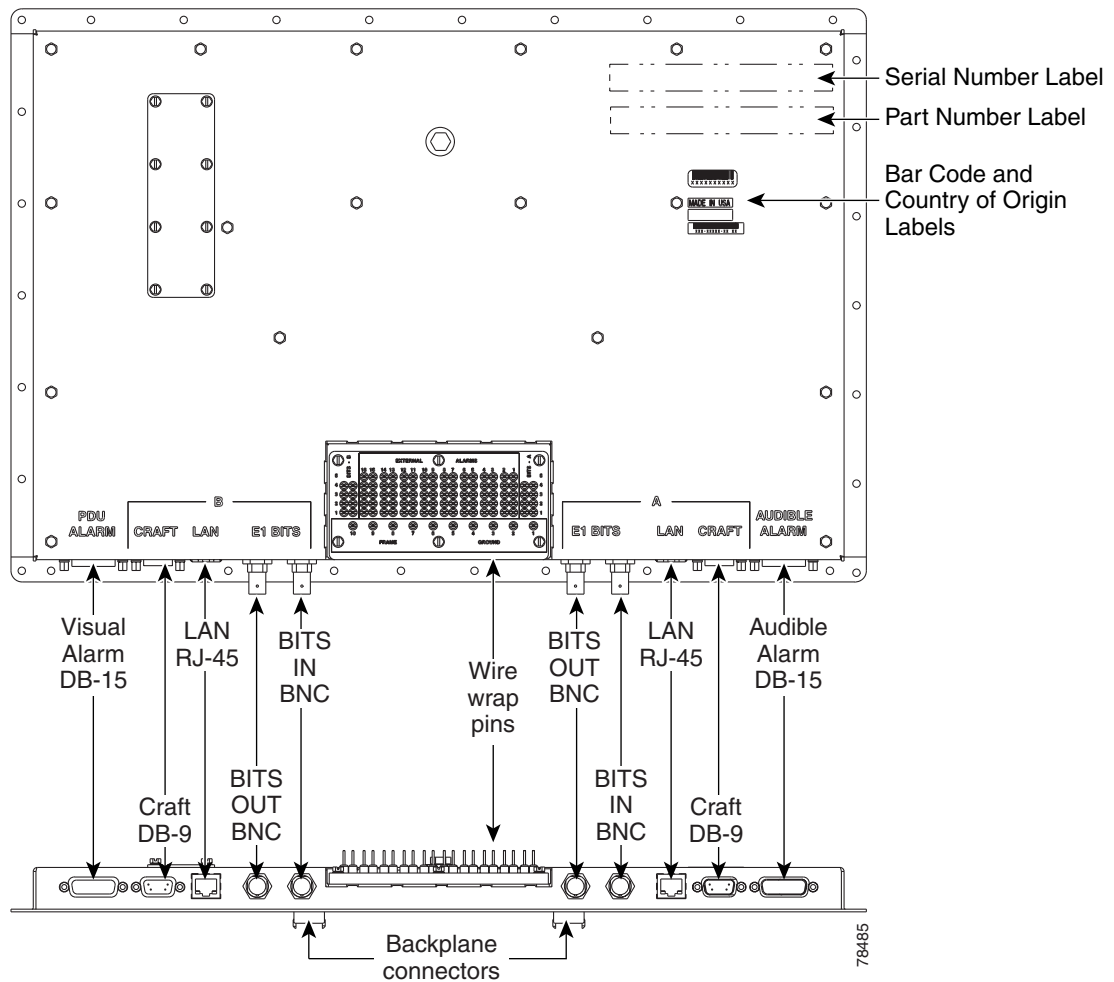


Figure 16-6 shows the CAP faceplate in detail.

**Figure 16-6 CAP Faceplate and Connections**

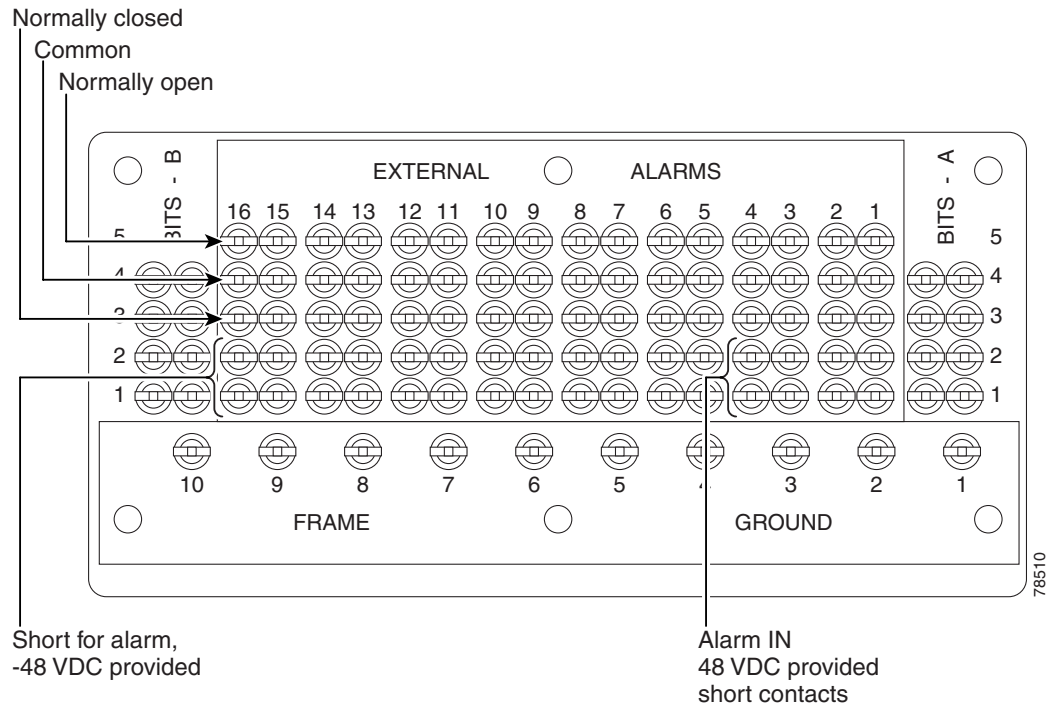


**Note**

BITS OUT and visual alarm DB-15 are not available in Software Release 5.0.

Figure 16-7 shows alarm pin assignments.

**Figure 16-7 Alarm Pin Assignments on the CAP**



See [Chapter 8, “Manage Alarms”](#) for instructions about assigning alarms to these pins.

Lace or tie wrap cables to the tie wrap features that are located below the connector pattern, according to local site practice.

- Step 2** To install the audible alarm cable, connect a DB-15 connector to the Audible Alarm plug at the lower right of the CAP. Connect the other end of the cable to the appropriate audible inputs of the connecting central office alarm circuit.
- Step 3** Return to your originating procedure (NTP).

## DLP-E12 Install T1 (100 Ohm) Timing Connections on the CAP

<b>Purpose</b>	This task installs timing connections from a 100-ohm T1 source to the CAP; it is required if the node is using a T1 timing source for external building integrated timing supply (BITS) timing.
<b>Tools/Equipment</b>	Wire-wrap tool (suitable for #22 to #28 AWG alarm wires) #22 or #24 AWG wire shielded twisted pair
<b>Prerequisite Procedures</b>	<a href="#">NTP-E4 Install the Bay Power and Ground, page 1-9</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

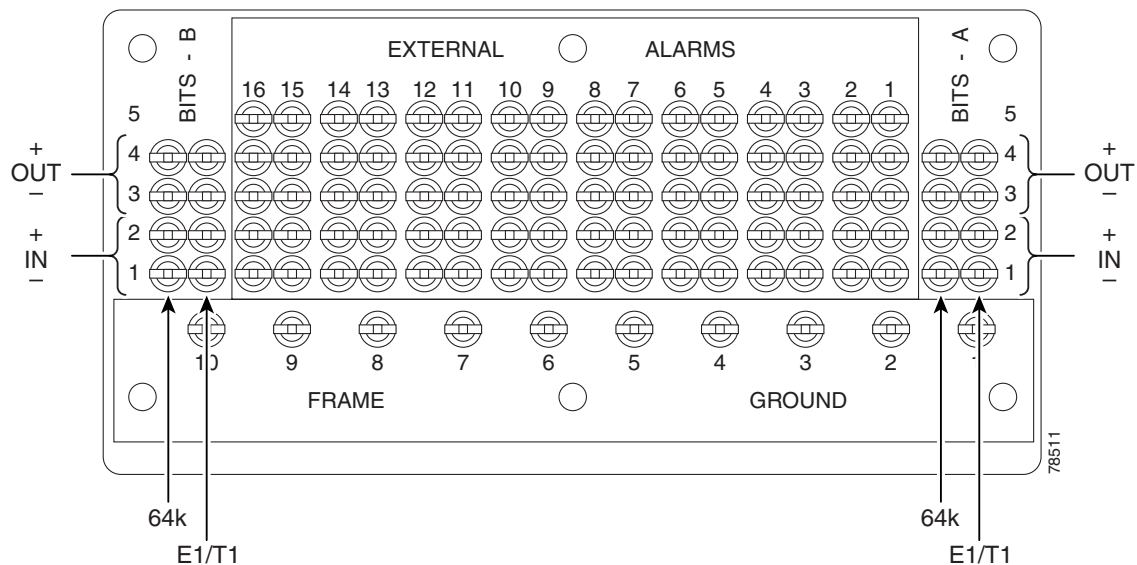
**Step 1** Wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

[Figure 16-8](#) shows the location of the timing connections on the pin field.



**Note** Only 100-ohm T1 BITS is supported in Release 6.0.

**Figure 16-8** BITS Timing Connections on the CAP



**Step 2** Wrap the ground shield of the alarm cable to one of the frame ground pins beneath the timing pin field.



**Note** For more detailed information about timing, refer to the *Cisco ONS 15600 Reference Manual*. To set up system timing, see the “[NTP-E24 Set Up Timing](#)” procedure on page 4-6.

- Step 3** Lace or tie wrap cables to the tie-wrap features that are located below the connector pattern, according to local site practice.
- Step 4** Return to your originating procedure (NTP).

## DLP-E13 Install LAN Cables on the CAP

<b>Purpose</b>	This task installs the LAN wires on the CAP; it is required to create external LAN connections.
<b>Tools/Equipment</b>	Straight-through (CAT-5) LAN cables
<b>Prerequisite Procedures</b>	<a href="#">NTP-E4 Install the Bay Power and Ground, page 1-9</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** Only the active Timing and Shelf Controller (TSC) card's connector is active. If you connect to the standby or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the CAP card so that connection to the ONS 15600 will not be lost during a TSC switch.

- Step 1** Plug the straight-through (CAT-5) LAN cable into one of the ports labeled "LAN" on the CAP ([Figure 16-6 on page 16-18](#)).



**Note** You can cable both LAN ports but only one will be active at a time.

- Step 2** Lace or tie wrap the cable to one of the tie-wrap features located below the connector pattern, according to local site practice.
- Step 3** Return to your originating procedure (NTP).

## DLP-E14 Install the TL1 Craft Interface Cable

<b>Purpose</b>	This task installs the TL1 craft interface cable on the CAP.
<b>Tools/Equipment</b>	EIA/TIA-232 cable (9 pin D-sub)
<b>Prerequisite Procedures</b>	<a href="#">NTP-E4 Install the Bay Power and Ground, page 1-9</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** Rather than using the craft pins, you can use a straight-through cable connected to the TSC RS-232 (EIA/TIA-232) port to access a TL1 craft interface.

---

**Step 1** Plug the EIA/TIA-232 cable into the port labeled “CRAFT” on the CAP.

[Figure 16-5 on page 16-17](#) shows the back of the ONS 15600, including the CAP and the location of the CRAFT ports.



**Note** Use a null-modem adapter if you will be connecting a UNIX-based computer to the ONS 15600. Refer to the *Cisco ONS 15600 TL1 Command Guide* for further information.

---

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

---

## DLP-E15 Inspect the Bay Installation and Connections

<b>Purpose</b>	This task inspects the bay installation and connections to verify that everything is installed and connected properly.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">Table 1-1 on page 1-13</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

**Step 1** Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the appropriate procedure in this chapter to correct it.

**Step 2** To check that the CAP is seated correctly, verify that the screws are secure and the pin field is firmly attached.

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

---

## DLP-E17 Delete a Card from CTC

<b>Purpose</b>	This task deletes a card from Cisco Transport Controller (CTC).
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** In node view, right-click the card you want to delete on the shelf graphic. A shortcut menu appears.

**Step 2** Choose **Delete Card** from the menu and click **Yes** in the confirmation dialog box.

You cannot delete a card if any of the following conditions apply:

- The card is part of a protection group; see the “[DLP-E87 Delete a 1+1 Protection Group](#)” task on [page 16-91](#).
- The card has any circuits; see the “[DLP-E163 Delete Circuits](#)” task on [page 17-49](#).
- The card is being used for timing; see the “[DLP-E89 Change the Node Timing Source](#)” task on [page 16-91](#).
- The card has a SONET DCC termination; see the “[NTP-E128 Modify or Delete Communications Channel Terminations and Provisionable Patchcords](#)” procedure on [page 11-8](#).



**Note** If the card that you deleted is still installed, it will reboot and reappear in CTC.

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

## DLP-E18 Install Fiber-Optic Cables in a 1+1 Configuration

<b>Purpose</b>	This task installs fiber-optic cables on optical (OC-N) cards in a 1+1 linear configuration.
<b>Tools/Equipment</b>	Fiber-optic cables
<b>Prerequisite Procedures</b>	<a href="#">NTP-E11 Install the OC-N Cards, page 2-4</a> <a href="#">NTP-E77 Clean Fiber Connectors and Adapters, page 14-15</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** With all fiber types, network planners/engineers should review the relative fiber type and optics specifications to determine attenuation, dispersion, and other characteristics to ensure appropriate deployment.

**Step 1** Align the white stripe of the cable connector with the white stripe on the receiving connector (OGI for OC-48 or OC-192 cards, LC for ASAP cards) of the faceplate connection point. Each card has four connectors on the faceplate.

[Table 16-1](#) shows the OGI connector pinouts on the OC-48 card faceplate.

**Table 16-1** OC48/STM16 Cards OGI Connector Pinout

Connector	OGI Pin and Card Port							
1	1	2	3	4	5	6	7	8
	Receive 4	Transmit 4	Receive 3	Transmit 3	Receive 2	Transmit 2	Receive 1	Transmit 1
2	1	2	3	4	5	6	7	8
	Receive 8	Transmit 8	Receive 7	Transmit 7	Receive 6	Transmit 6	Receive 5	Transmit 5

**Table 16-1** OC48/STM16 Cards OGI Connector Pinout

Connector	OGI Pin and Card Port							
3	1	2	3	4	5	6	7	8
	Receive 12	Transmit 12	Receive 11	Transmit 11	Receive 10	Transmit 10	Receive 9	Transmit 9
4	1	2	3	4	5	6	7	8
	Receive 16	Transmit 16	Receive 15	Transmit 15	Receive 14	Transmit 14	Receive 13	Transmit 13

Table 16-2 shows the OGI connector pinouts on the front of the OC-192 card faceplate.

**Table 16-2** OC192/STM64 Cards OGI Connector Pinout

Connector	OGI Pin and Card Port							
1	1	2	3	4	5	6	7	8
	—	—	Receive 1	Transmit 1	—	—	—	—
2	1	2	3	4	5	6	7	8
	—	—	Receive 2	Transmit 2	—	—	—	—
3	1	2	3	4	5	6	7	8
	—	—	Receive 3	Transmit 3	—	—	—	—
4	1	2	3	4	5	6	7	8
	—	—	Receive 4	Transmit 4	—	—	—	—

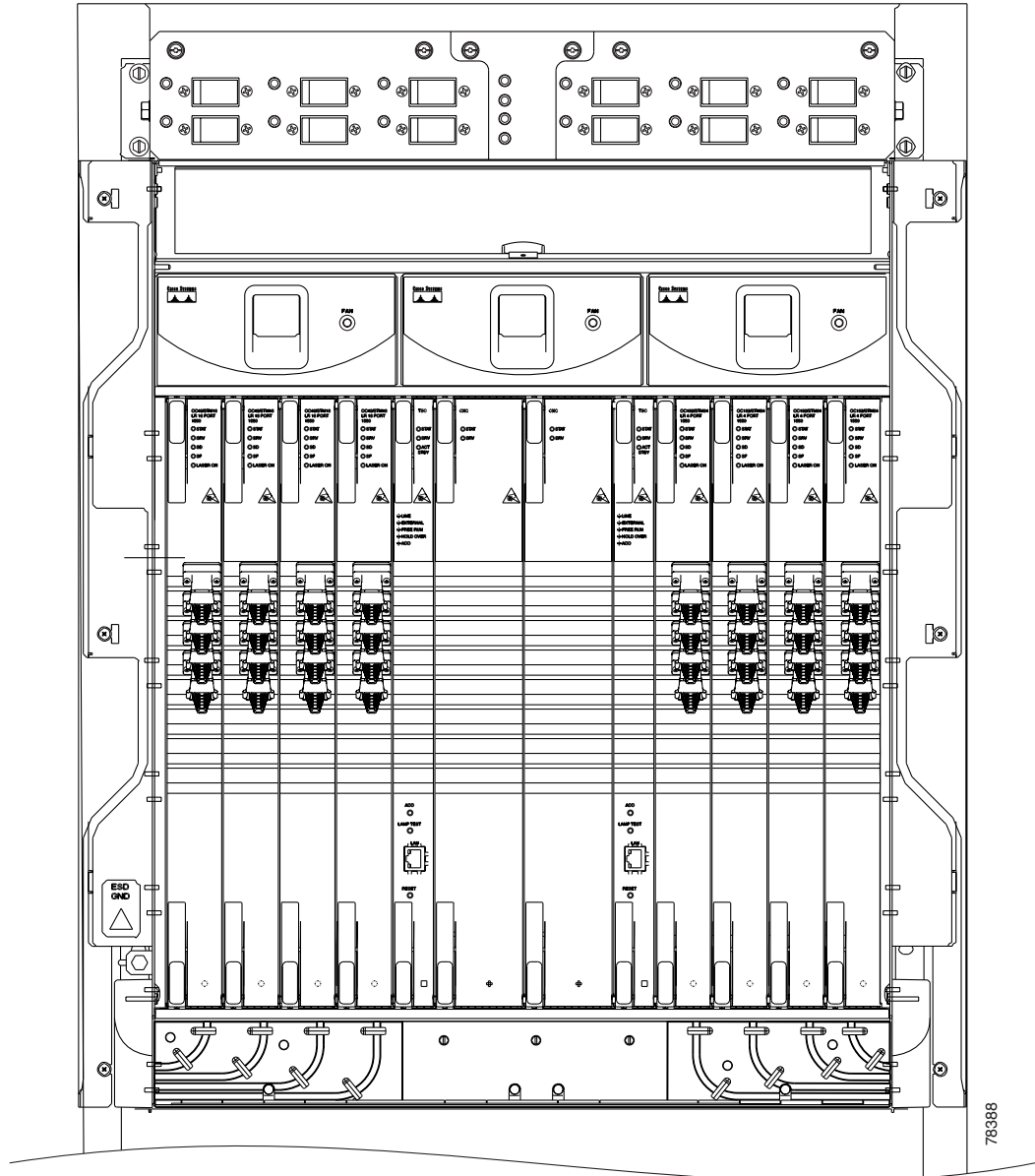
**Note**

Refer to the “Card Features and Functions” chapter of the *Cisco ONS 15600 Reference Manual* for information about the ASAP card connector numbering.

Figure 16-9 shows all of the cards installed in the shelf and the optical connectors.



Figure 16-9 ONS 15600 with Optical Cards Installed



- Step 2** Remove the dust cap from the OGI or LC connector adapter on the front of the card.
- Step 3** Plug the fiber into the connector (Tx and Rx) of a working (instead of protect) OC-N port at one node by squeezing the latches on either side of the connector and gently pushing it into the faceplate connection point until the connector snaps into place.
- Step 4** Plug the other end of the fiber into the connector of a working port on an OC-N card at an adjacent node.
- Step 5** Repeat Steps 2 through 4 for the protect ports on the two OC-N cards you are using, and then for each fiber-optic cable you require.
- Step 6** Return to your originating procedure (NTP).

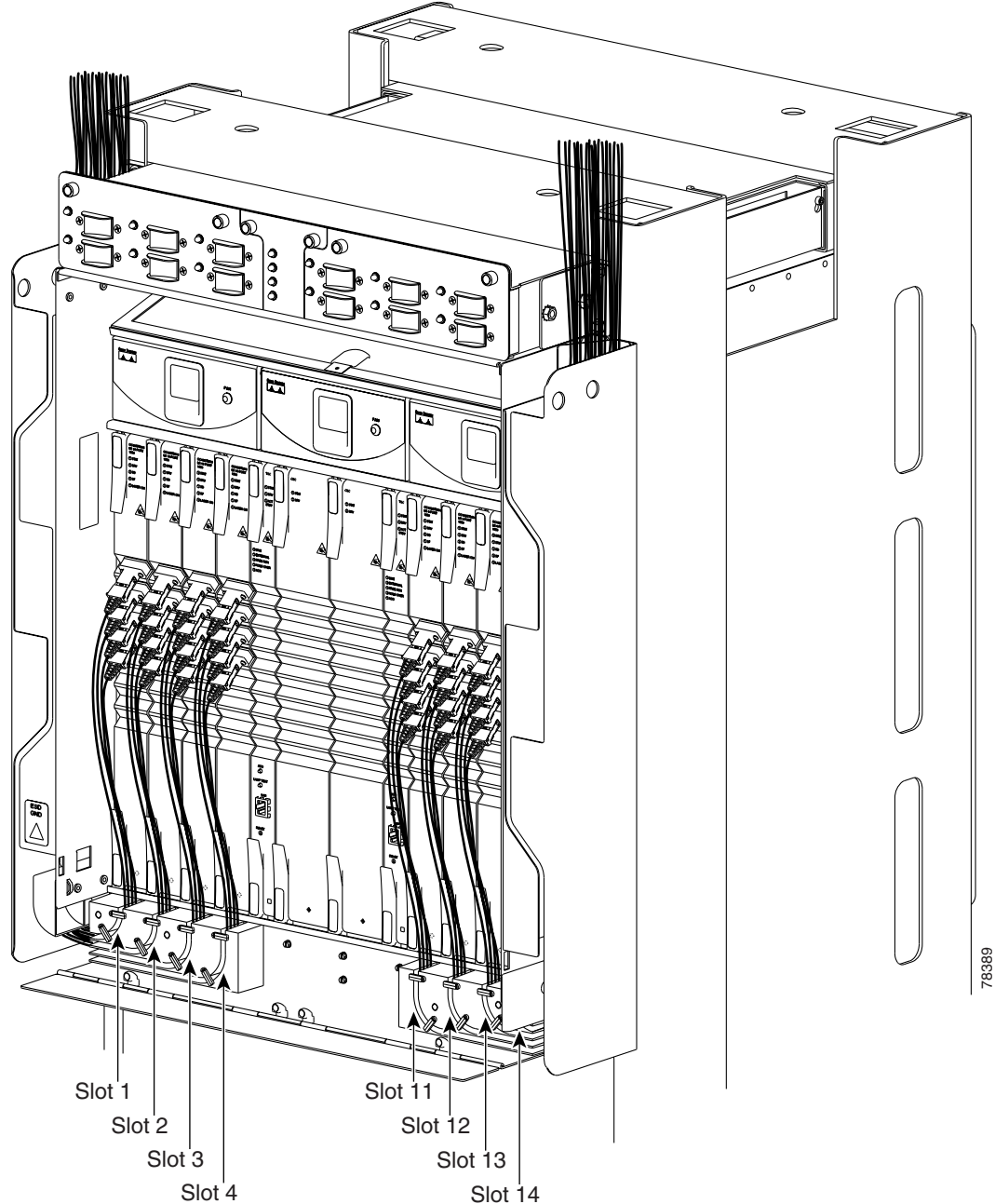
## DLP-E19 Route Fiber-Optic Cables

<b>Purpose</b>	This task explains how to route fiber-optic cables away from the card faceplates and onto the side of the shelf.
<b>Tools/Equipment</b>	Tie-wrap (Suggested: Panduit TAK-TAPE TTS-20R0 Nelcro tie-wraps)
<b>Prerequisite Procedures</b>	<a href="#">NTP-E15 Install the Fiber-Optic Cables, page 2-9</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

---

- Step 1** Open the fold-down front door on the cable-management tray.
- Step 2** For each optical card you plan to install, find the corresponding cable routing channel directly below that card ([Figure 16-10.](#))

Figure 16-10 ONS 15600 with All Optical Cards Cabled and Routed



- Step 3** Rotate the plastic cable latches for each optical card you will install to the open position so that they do not block the cable routing channels in the cable-management tray.
- Step 4** Route the fiber cable from the connector on the card through the corresponding cable routing channel in the cable-management tray. Start from the innermost card on one side of the shelf (Slot 4 on the left side, for instance).



**Note** If a slot is empty, leave the corresponding cable routing channel empty for later use.

- Step 5** If narrow cable routing modules (CRMs) are installed:
- a. Route the fiber cables through the cable-management tray toward the edge of the bay and then up through the narrow CRM attached to the side of the bay, inserting the fiber into the open tracks in the narrow CRM (Figure 16-10 on page 16-27). Make sure the cables line up directly in front of the corresponding card so the cables are not disturbed if later a card is removed.
  - b. Rotate the corresponding cable latch to the closed position so it secures the fiber cables within the corresponding cable routing channel.
  - c. Repeat Steps a and b for the fiber cables from each installed OC-N card, working from the innermost cards outward.

**Step 6** If wide CRMs are installed:

- a. Gently pull the spool flanges toward you until they click open.
- b. Route the fiber cables through the cable-management tray toward the edge of the bay and then up through the wide CRM attached to that side of the bay. Gently loop the cable around the spools. Store no more than one meter of slack (on average) for each cable that you route through the wide CRM.




---

**Note** If your site uses underfloor cabling, route the cables down to the CRM on the shelf directly below the node for which you are routing cables.

---

- c. Rotate the corresponding cable latch to the closed position so it secures the fiber cables within the corresponding cable routing channel.
- d. Repeat Steps a through c for the fiber cables from each installed OC-N card, working from the innermost cards outward. Distribute the cables as evenly as possible on the three storage spools of the CRM.
- e. Push any extended spool flanges away from you so that they click closed.
- f. Use tie wrap to secure the cable and minimize slack. Start with the cables closest to the outside edge of the CRM.

**Step 7** Make sure all the plastic cable latches are in the closed position.

**Step 8** Close the fold-down tray door when all fiber cables are properly routed.

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

---

## DLP-E20 Run the CTC Installation Wizard for Windows


<b>Purpose</b>	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, Java Runtime Environment (JRE) 1.4.2, and the CTC Java archive (JAR) files. JRE 1.4.2 is required to run Release 6.0. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TSC card the first time you log in.
<b>Tools/Equipment</b>	Cisco ONS 15600 Release 6.0 software or documentation CD
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	This task is required if any one of the following is true: <ul style="list-style-type: none"> <li>• JRE 1.4.2 is not installed.</li> <li>• CTC online user manuals are not installed and are needed.</li> <li>• CTC JAR files are not installed and are needed.</li> </ul>
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None


**Note**

If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 1.4.2 and reinstall JRE 1.3.1\_2. To run R5.0 and later, uninstall JRE 1.3.1\_2 and reinstall JRE 1.4.2.


**Note**

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

- Step 1** Verify that your computer has the following:
- Processor—Pentium III, 700 Mhz or faster
  - RAM—384 MB recommended, 512 MB optimum
  - Hard drive—20 GB hard drive recommended with at least 50 MB of space available
  - Operating System—Windows 98 (1st and 2nd editions), Windows NT 4.0 (with Service Pack 6a), Windows 2000 (with Service Pack 3), or Windows XP Home
- If your operating system is Windows NT 4.0, verify that Service Pack 5 or later is installed. From the Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site.
-  **Note** Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15600 Reference Manual* to find computer requirements needed for small, medium, and large ONS 15600 networks.
- Step 2** Insert the Cisco ONS 15600 Release 6.0 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's CD directory and double-click **setup.exe**.

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

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

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

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

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

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

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

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

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

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

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

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

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

**Step 10** Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in [Step 4](#) and did not check Java Runtime Environment 1.4.2, continue with [Step 12](#).

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

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

**Note**

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

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

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

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

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

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

**Note**

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

- h. Click **Next**.
- i. Click **Finish**.

**Note**

If you are uninstalling the JRE, click **Remove**.

**Step 12** In the Cisco Transport Controller Installation Wizard, click **Next**. The online user manuals are installed.

- Step 13** Click **Finish**.
- Step 14** Return to your originating procedure (NTP).

## DLP-E21 Run the CTC Installation Wizard for UNIX

<b>Purpose</b>	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 1.4.2, and the CTC JAR files. JRE 1.4.2 is required to run Release 6.0. Preinstalling the CTC JAR files saves time at initial login. If the JAR files are not installed, they are downloaded from the TSC card the first time you log in.
<b>Tools/Equipment</b>	ONS 15600 Release 6.0 software or documentation CD
<b>Prerequisite Procedures</b>	None
<b>Required/As Needed</b>	Required if any of the following are true: <ul style="list-style-type: none"> <li>• JRE 1.4.2 is not installed.</li> <li>• CTC online help is not installed and is needed.</li> <li>• JRE files are not installed and are needed.</li> </ul>
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	None



**Note**

If you will log into nodes running CTC software earlier than Release 4.6, uninstall JRE 1.4.2 and reinstall JRE 1.3.1\_2. To run Software R6.0 and later, uninstall JRE 1.3.1\_2 and reinstall JRE 1.4.2.



**Note**

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

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



**Note**

These requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM. Refer to the *Cisco ONS 15600 Reference Manual* for computer requirements needed for small, medium, and large ONS 15600 networks.

- Step 2** Change the directory. Type:

```
cd /cdrom/cdrom0/
```

- Step 3** From the techdoc600 CD directory, type:

```
./setup.bat
```

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



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

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

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

- Click **Typical** to install both the Java Runtime Environment and online user manuals. If you already have JRE 1.4.2 installed on your computer, choose **Custom**.
- Click **Custom** if you want to install either the JRE or the online user manuals.

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

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

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

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

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

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

**Step 10** Review the components that will be installed. If you want to change the components, complete one of the following:

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

**Step 11** Click **Next**. It might take a few minutes for the JRE installation wizard to appear. If you selected Custom in [Step 5](#) and did not check Java Runtime Environment 1.4.2, continue with [Step 13](#).

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

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




---

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

---

- b.** Click **Next**.
- c.** Choose one of the following:
  - Click **Typical** to install all JRE features. If you select **Typical**, the JRE version installed will automatically become the default JRE version for your browsers.
  - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

**d.** Click **Next**.

**e.** If you selected **Typical**, continue with Step **i**. If you selected **Custom**, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- **Java 2 Runtime Environment—(Default)** Installs JRE 1.4.2 with support for European languages.
- **Support for Additional Languages**—Adds support for non-European languages.
- **Additional Font and Media Support**—Adds Lucida fonts, Java Sound, and color management capabilities.

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

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

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

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




---

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

---

- h.** Click **Next**.
- i.** Click **Finish**.




---

**Note** If you are uninstalling the JRE, click **Remove**.

---

**Step 13** In the Cisco Transport Controller Installation Wizard, click **Next**. The Online Help installs.

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



**Note** Be sure to record the names of the directories you choose for JRE and the online help.

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

## DLP-E23 Set Up a Windows PC for Craft Connection to an ONS 15600 on the Same Subnet Using Static IP Addresses

<b>Purpose</b>	This task sets up your computer for a local craft connection to the ONS 15600 when: <ul style="list-style-type: none"> <li>You will connect to one ONS 15600; if you will connect to multiple ONS 15600s, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15600.</li> <li>You need to use non-ONS 15600 applications such as ping and tracert (trace route).</li> </ul>
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-E17 Set Up Computer for CTC, page 3-1</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

- Step 1** Verify the operating system that is installed on your computer:
- From the Windows Start menu, choose **Settings > Control Panel**.
  - In the Control Panel window, double-click the **System** icon.
  - On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows 2000, Windows NT 4.0, or Windows XP.
- Step 2** According to the Windows operating system installed on your computer, perform one of the following steps:
- For Windows 98, complete [Step 3](#).
  - For Windows NT 4.0, complete [Step 4](#).
  - For Windows 2000, complete [Step 5](#).
  - For Windows XP, complete [Step 6](#).
- Step 3** If you have Windows 98 installed on your PC, complete the following steps to change its TCP/IP configuration:
- From the Windows Start menu, choose **Settings > Control Panel**.
  - In the Control Panel dialog box, click the **Network** icon.
  - In the Network dialog box, choose **TCP/IP** for your network interface card (NIC), then click **Properties**.

- d. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.
- e. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.
- f. Click the **IP Address** tab.
- g. In the IP Address window, click **Specify an IP address**.
- h. In the IP Address field, enter an IP address that is identical to the ONS 15600 IP address except for the last octet. The last octet must be 1 or 3 through 254.
- i. In the Subnet Mask field, type the same subnet mask as the ONS 15600. The default is 255.255.255.0 (24 bit).
- j. Click **OK**.
- k. In the TCP/IP dialog box, click the **Gateway** tab.
  - l. In the New Gateway field, type the ONS 15600 IP address. Click **Add**.
- m. Verify that the IP address appears in the Installed Gateways field, then click **OK**.
- n. When the prompt to restart your PC appears, click **Yes**.

**Step 4** If you have Windows NT 4.0 installed on your PC, complete the following steps to change its TCP/IP configuration:

- a. From the Windows Start menu, choose **Settings > Control Panel**.
- b. In the Control Panel dialog box, click the **Network** icon.
- c. In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.
- d. Click the **IP Address** tab.
- e. In the IP Address window, click **Specify an IP address**.
- f. In the IP Address field, enter an IP address that is identical the ONS 15600 IP address except for the last octet. The last octet must be 1 or 3 through 254.
- g. In the Subnet Mask field, type **255.255.255.0**.
- h. Click **Advanced**.
- i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.
- j. Type the ONS 15600 IP address in the Gateway Address field.
- k. Click **Add**.
- l. Click **OK**.
- m. Click **Apply**.
- n. In some cases, Windows NT 4.0 prompts you to reboot your PC. If you receive this prompt, click **Yes**.

**Step 5** If you have Windows 2000 installed on your PC, complete the following steps to change its TCP/IP configuration:

- a. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.
- b. In the Local Area Connection Status dialog box, click **Properties**.
- c. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
- d. Click **Use the following IP address**.
- e. In the IP Address field, enter an IP address that is identical the ONS 15600 IP address except for the last octet. The last octet must be 1 or 3 through 254.

- f. In the Subnet Mask field, type **255.255.255.0**.
- g. In the Default Gateway field, type the ONS 15600 IP address.
- h. Click **OK**.
- i. In the Local Area Connection Properties dialog box, click **OK**.
- j. In the Local Area Connection Status dialog box, click **Close**.

**Step 6** If you have Windows XP installed on your PC, complete the following steps to change its TCP/IP configuration:

- a. From the Windows Start menu, choose **Control Panel > Network Connections**.



**Note** If the Network Connections menu is not available, click **Switch to Classic View**.

- b. From the Network Connections dialog box, click the **Local Area Connection** icon.
- c. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
- d. In the IP Address field, enter an IP address that is identical the ONS 15600 IP address except for the last octet. The last octet must be 1 or 3 through 254.
- e. In the Subnet Mask field, type **255.255.255.0**.
- f. In the Default Gateway field, type the ONS 15600 IP address.
- g. Click **OK**.
- h. In the Local Area Connection Properties dialog box, click **OK**.
- i. In the Local Area Connection Status dialog box, click **Close**.

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

## DLP-E24 Set Up a Solaris Workstation for a Craft Connection to an ONS 15600

<b>Purpose</b>	This task sets up a Solaris workstation for a craft connection to the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-E17 Set Up Computer for CTC, page 3-1</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

**Step 1** Log into the workstation as the root user.

**Step 2** Check to see if the interface is plumbed by typing:

```
# ifconfig device
```

For example:

```
# ifconfig hme1
```

If the interface is plumbed, a message similar to the following appears:

```
hme1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask 0
```

If a message similar to this one appears, go to [Step 5](#).

If the interface is not plumbed, a message similar to the following appears:

```
if config: status: SIOCGLIFFLAGS: hme1: no such interface.
```

If a message similar to this one appears, go to [Step 3](#).

**Step 3** Plumb the interface by typing:

```
# ifconfig device plumb
```

For example:

```
# ifconfig hme1 plumb
```

**Step 4** Configure the IP address on the interface by typing:

```
# ifconfig interface ip-address netmask netmask up
```

For example:

```
# ifconfig hme0 192.1.0.3 netmask 255.255.255.0 up
```




---

**Note** Enter an IP address that is identical to the ONS 15600 IP address except for the last octet. The last octet must be between 1 and 254.

---

**Step 5** In the Subnet Mask field, type **255.255.255.0**. Skip this step if you checked Craft Access Only at Provisioning > Network > General > Gateway Settings.

**Step 6** Test the connection:

- a. Start Netscape Navigator.
- b. Enter the Cisco ONS 15600 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box appear. If this occurs, go to Step 2 of the [“DLP-E26 Log into CTC” task on page 16-39](#) to complete the login. If the Login dialog box does not appear, complete Steps [c](#) and [d](#).
- c. At the prompt, type:

```
ping ONS-15600-IP-address
```

For example, to connect to an ONS 15600 with the default IP address 192.168.1.2, type:

```
ping 192.168.1.2
```

If your workstation is connected to the ONS 15600, the following message appears:

```
IP address is alive
```




---

**Note** Skip this step if you checked the Craft Access Only check box at Provisioning > Network > General > Gateway Settings.

---

- d. If CTC is not responding, a “Request timed out” (Windows) or a “no answer from x.x.x.x” (UNIX) message appears. Verify the IP and subnet mask information. Check that the cables connecting the workstation to the ONS 15600 are securely attached. Check the link status by typing:

```
# ndd -set /dev/device instance 0
# ndd -get /dev/device link_status
```

For example:

```
# ndd -set /dev/hme instance 0
# ndd -get /dev/hme link_status
```

A result of 1 means the link is up. A result of 0 means the link is down.



**Note** Check the man page for ndd. For example, type:

```
# man ndd
```

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

## DLP-E26 Log into CTC

<b>Purpose</b>	This task logs into CTC.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<p><a href="#">NTP-E17 Set Up Computer for CTC, page 3-1</a></p> <p>One of the following procedures:</p> <ul style="list-style-type: none"> <li>• <a href="#">NTP-E18 Set Up CTC Computer for Local Craft Connection to the ONS 15600, page 3-2</a></li> <li>• <a href="#">NTP-E111 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600, page 3-4</a></li> </ul>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher



**Note** For information about CTC views and navigation, see [Appendix A, “CTC Information and Shortcuts.”](#)

**Step 1** From the computer connected to the ONS 15600, start Netscape (PC or UNIX) or Internet Explorer (PC only):

- If you are using a PC, launch Netscape or Internet Explorer from the Windows Start menu or a shortcut icon.
- If you are using UNIX, launch Netscape from the command line by typing one of the following:
  - To install Netscape colors for Netscape use, type:
 

```
netscape -install
```
  - To limit Netscape to 32 colors so that if the requested color is not available, Netscape chooses the closest color option, type:
 

```
netscape -ncols 32
```

**Note**

CTC requires a full 24-color palette to run properly. When using color-intensive applications such as Netscape in UNIX, it is possible that UNIX could run out of colors to use for CTC. The `-install` and `-ncols 32` command line options limit the number of colors that Netscape uses.

- Step 2** In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15600 IP address. For initial setup, this is the default address: 192.168.1.2. Press **Enter**.

**Note**

If you are logging into ONS 15600 nodes running different releases of CTC software, log into the node running the most recent release. If you log into a node running an older release, you will receive an INCOMPATIBLE-SW alarm for each node in the network running a new release, and CTC will not be able to manage these nodes. To check the software version of a node, select About CTC from the CTC Help menu. To resolve an alarm, refer to the *Cisco ONS 15600 Troubleshooting Guide*.

- Step 3** If a Java Plug-in Security Warning dialog box appears, complete the “[DLP-E152 Install Public-Key Security Certificate](#)” task on page 17-40 to install the public-key security certificate.

After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15600, this process can take several minutes. After the download, the CTC Login dialog box appears ([Figure 16-11](#)).

**Figure 16-11** Logging into CTC

- Step 4** In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name **CISCO15** and password **otbu+1**.



**Note**

The CISCO15 user is provided with every ONS 15600. CISCO15 has superuser privileges, so you can create other users. You must create another superuser before you can delete the CISCO15 user. CISCO15 is delivered with the otbu+1 password. To change the password for CISCO15, click the **Provisioning > Security** tabs after you log in and change the password. To set up ONS 15600 users and assign security, go to the “[NTP-E26 Create Users and Assign Security](#)” procedure on page 4-3. For additional information, refer to the *Cisco ONS 15600 Reference Manual*.

- Step 5** Each time you log into an ONS 15600, you can make selections on the following login options:
- **Node Name**—Displays the IP address entered in the web browser and a drop-down list of previously entered ONS 15600 IP addresses. You can select any ONS 15600 on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
  - **Additional Nodes**—Displays a list of login node groups. To create a login node group or add additional groups, see the “[DLP-E27 Create Login Node Groups](#)” task on page 16-41.
  - **Disable Network Discovery**—Check this box to view only the ONS 15600 (and login node group members, if any) entered in the Node Name field. Nodes linked to this node through the DCC are not discovered and will not appear in CTC network view. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes and reduces memory consumption.
  - **Disable Circuit Management**—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. This option does not prevent the creation and management of new circuits.
- Step 6** Click **Login**.
- If login is successful, the CTC window appears. From here, you can navigate to other CTC views to provision and manage the ONS 15600. If you need to turn up a shelf for the first time, go to [Chapter 4, “Turn Up Node.”](#) If login problems occur, refer to the *Cisco ONS 15600 Troubleshooting Guide*.
- Step 7** Return to your originating procedure (NTP).

## DLP-E27 Create Login Node Groups

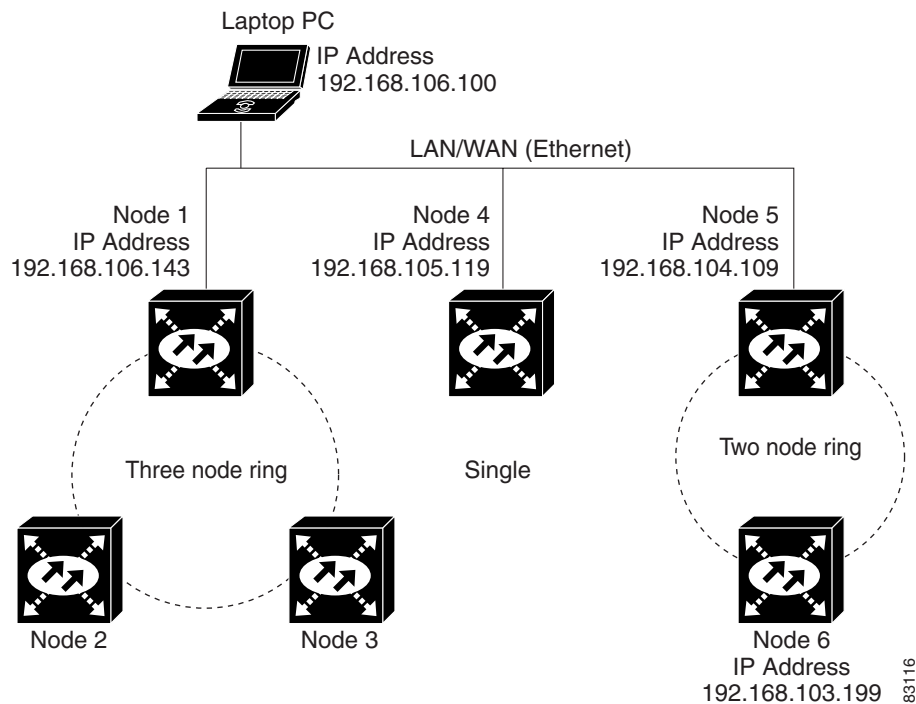
<b>Purpose</b>	This task creates a login node group to display ONS 15600s that have an IP connection but not a DCC connection to the login node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-E20 Log into the ONS 15600 GUI, page 3-5</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** From the Edit menu, choose **Preferences**.
- Step 2** Click the **Login Node Groups** tab.
- Step 3** Click **Create Group**.
- Step 4** Type a name for the group in the Create Login Group Name dialog box. Click **OK**.

- Step 5** In the Members field, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node you want to add to the group.
- Step 6** Click **OK**.

The next time you log into an ONS 15600, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in [Figure 16-12](#), a login node group is created that contains the IP addresses for Nodes 1, 4, and 5. During login, if you choose this group from the Additional Nodes list and Disable Network Discovery is not selected, all nodes in the figure appear. If the login group and Disable Network Discover are both selected, only Nodes 1, 4, and 5 appear. You can create as many login groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

**Figure 16-12 Login Node Group**



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

## DLP-E28 Add a Node to the Current Session or Login Group

<b>Purpose</b>	This task adds a node to the current CTC session or login node group.
<b>Tools</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 CTC File menu, choose **Add Node**.
- Step 2** In the Add Node dialog box, enter the node name (or IP address).
- Step 3** If you want to add the node to the current login group, check **Add Node to Current Login Group**. Otherwise, leave it unchecked.



**Note** The Add Node to Current Login Group check box is active only if you selected a login group when you logged into CTC.

- 
- Step 4** Click **OK**.  
After a few seconds, the new node will appear on the network view map.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-E29 Change the Login Legal Disclaimer

<b>Purpose</b>	This task modifies the legal disclaimer statement shown in the CTC login dialog box so that it will display customer-specific information when users log into the network.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 > Security > Legal Disclaimer > HTML** tabs.
- Step 2** The existing statement is a default, non-customer-specific disclaimer. If you want to edit this statement with specifics for your company, you can change the text. You can also use the HTML commands in [Table 16-3](#) to format the text.

**Table 16-3** HTML Commands Used to Format the Legal Disclaimer

Code	Description
<b>	Begins boldface font
</b>	Ends boldface font
<center>	Aligns type in the center of the window
</center>	Ends the center alignment
<font= <i>n</i> > (where <i>n</i> = point size)	Changes the font to the new size
</font>	Ends the font size command
<p>	Creates a line break
<sub>	Begins subscript
</sub>	Ends subscript
<sup>	Begins superscript
</sup>	Ends superscript
<u>	Starts underline
</u>	Ends underline

- Step 3** If you want to preview your changed statement and formatting, click the **Preview** subtab.
- Step 4** Click **Apply**.
- Step 5** Return to your originating procedure (NTP).

## DLP-E30 Provision IP Settings

<b>Purpose</b>	This task provisions IP settings, which include the IP address, default router, Dynamic Host Configuration Protocol (DHCP) access, firewall access, and SOCKS proxy server settings for an ONS 15600 node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Caution** All network changes should be approved by your network or LAN administrator.

- Step 1** From the View menu, choose **Go To Home View**.
- Step 2** Click the **Provisioning > Network > General** tabs.
- Step 3** Complete the following information in the fields listed:
- IP Address—Type the IP address assigned to the ONS 15600 node.

- **Default Router**— If the ONS 15600 is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the ONS 15600 cannot directly access. This field is ignored if any of the following are true:
  - The ONS 15600 is not connected to a LAN.
  - SOCKS proxy server is enabled and the ONS 15600 is provisioned as an end network element (ENE).
  - Open Shortcut Path First (OSPF) is enabled on both the ONS 15600 and the LAN where the ONS 15600 is connected.
- **Suppress CTC IP Display**—Check this check box if you want to prevent the node IP address from being shown in CTC to users with Provisioning, Maintenance, or Retrieve security levels. (The IP address suppression does apply to users with the Superuser security level.)
- **Forward DHCP Request To**—Check this check box to enable DHCP. Also, enter the DHCP server IP address in the Request To field. Unchecked is the default. If you will enable any of the gateway settings to implement the ONS 15600 SOCKS proxy server features, leave this field blank.




---

**Note** If you enable DHCP, computers connected to an ONS 15600 node can obtain temporary IP addresses from an external DHCP server. The ONS 15600 only forwards DHCP requests; it does not act as a DHCP server.

---

- **MAC Address**—(Read only) Displays the ONS 15600 IEEE 802 MAC address.
- **Net/Subnet Mask Length**—If the ONS 15600 is part of a subnet, type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15600s in the same subnet.
- **TSC CORBA (IIOP) Listener Port**—Sets the ONS 15600 Internet Inter-Orb Protocol (IIOP) listener port used for communication between the ONS 15600 and CTC computers. This field is generally not changed unless the ONS 15600 resides behind a firewall that requires a different port. See the [“NTP-E94 Set Up the ONS 15600 for Firewall Access” procedure on page 4-6](#) for more information.
- **Gateway Settings**—Provisions the ONS 15600 SOCKS proxy server features. (SOCKS is a standard proxy protocol for IP-based applications.) Do not change these options until you review the SOCKS proxy server scenario in the *Cisco ONS 15600 Reference Manual*. In SOCKS proxy server networks, the ONS 15600 is either an ENE, gateway network element (GNE), or proxy-only server. Provisioning must be consistent for each NE type.
- **Enable SOCKS proxy server on port**—If checked, the ONS 15600 serves as a proxy for connections between CTC clients and ONS 15600s that are connected by DCCs to the proxy ONS 15600. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client does not require IP connectivity to the DCC-connected nodes, only to the proxy ONS 15600. If Enable SOCKS proxy server on port is off, the node does not proxy for any CTC clients. When this box is checked, you can provision one of the following options:




---

**Note** For the ONS 15600, the ENE and GNE setting have the same behavior.

---

- **External Network Element (ENE) or Gateway Network Element (GNE)**—Choose this option when the ONS 15600 is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE through the TSC TCP/IP (craft) port can manage nodes that have DCC connections to the ENE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN/WAN that those nodes might be connected to.

- SOCKS Proxy-Only—Choose this option when the ONS 15600 is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS Proxy Only is the same as the GNE option, except the SOCKS Proxy Only option does not isolate the DCC network from the LAN.

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

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

Both ONS 15600 TSC cards will reboot, one at a time. Next, a “Lost node connection, switching to network view” message appears. The reset causes the standby TSC to become the active TSC.

**Step 6** If the cable was connected to the RJ-45 port on the active TSC (now the standby TSC), disconnect the cable and connect it to the RJ-45 port on the other TSC (now the active TSC).

**Step 7** Click **OK**. The network view appears with the node icon in gray, during which time you cannot access the node.

**Step 8** Double-click the node icon when it becomes green.

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

## DLP-E31 Create a Static Route

<b>Purpose</b>	This task creates a static route to establish CTC connectivity to a computer on another network.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	Required if either of the following conditions is true: <ul style="list-style-type: none"> <li>• You need to connect ONS 15600s to CTC sessions on one subnet connected by a router to ONS 15600s residing on another subnet when OSPF is not enabled and the ENE or GNE setting are not checked.</li> <li>• You need to enable multiple CTC sessions among ONS 15600s residing on the same subnet, and the Craft Access server feature is not enabled.</li> </ul>
<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 **Create**.

**Step 3** In the Create Static Route dialog box, enter the following:

- **Destination**—Enter the IP address of the computer running CTC. To limit access to one computer, enter the full IP address and a subnet mask of 255.255.255.255. To allow access to all computers on the 192.168.1.0 subnet, enter 192.168.1.0 and a subnet mask of 255.255.255.0. You can enter a destination of 0.0.0.0 to allow access to all CTC computers that connect to the router.
- **Mask**—Enter a subnet mask. If Destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If Destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If Destination is 0.0.0.0, CTC automatically enters a subnet mask of 0.0.0.0 to provide access to all CTC computers. You cannot change this value.

- Next Hop—Enter the IP address of the router port or the node IP address if the CTC computer is connected to the node directly.
- Cost—Enter the number of hops between the ONS 15600 and the computer.

**Step 4** Click **OK**. Verify that the static route appears in the Static Route window.



**Note** Static route networking scenarios are provided in the IP networking section of the *Cisco ONS 15600 Reference Manual*.

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

## DLP-E32 Set Up or Change Open Shortest Path First Protocol

<b>Purpose</b>	This task enables the OSPF routing protocol to include the ONS 15600 in OSPF-enabled networks.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
	You will need to know the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router to which the ONS 15600 is connected.
<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 has DCC or LAN interfaces in multiple OSPF areas, at least one ONS 15600 DCC or LAN interface must be in the backbone area 0.0.0.0.



**Note** CTC will not allow both a DCC interface and a LAN interface in the same non-zero OSPF area.



**Note** To create OSPF virtual links, OSPF must be enabled on the LAN.

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

**Step 2** In the top left side of the OSPF pane, complete the following:

- DCC/GCC OSPF Area ID Table—In dotted decimal format, enter the number that identifies the ONS 15600s as a unique OSPF area ID. The Area ID can be any number between 000.000.000.000 and 255.255.255.255, but must be unique to the LAN OSPF area.
- SDCC Metric—This value is normally unchanged. It sets a “cost” for sending packets across the Section DCC (SDCC), which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 100.

- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

**Step 3** In the OSPF on LAN area, complete the following:

- OSPF active on LAN—When checked, enables ONS 15600 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15600s that directly connect to OSPF routers.
- LAN Port Area ID —Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15600 is connected. (This number is different from the DCC/GCC OSPF Area ID.)

**Step 4** By default, OSPF is set to No Authentication. If the OSPF router requires authentication, complete the following steps. If not, continue with [Step 5](#).

- Click the **No Authentication** button.
- In the Edit Authentication Key dialog box, complete the following:
  - Type—Choose **Simple Password**.
  - Enter Authentication Key—Enter the password.
  - Confirm Authentication Key—Enter the same password to confirm it.
- Click **OK**.

The authentication button label changes to Simple Password.

**Step 5** Provision the OSPF priority and interval settings.

The OSPF priority and intervals default to values most commonly used by OSPF routers. In the Priority and Intervals area, verify that these values match those used by the OSPF router where the ONS 15600 is connected:

- Router Priority—Selects the designated router for a subnet.
- Hello Interval (sec)—Sets the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- Transit Delay (sec)—Indicates the service speed. One second is the default.
- Retransmit Interval (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Sets a cost for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

**Step 6** Under OSPF Area Range Table, create an area range table if one is needed.




---

**Note** Area range tables consolidate the information that is propagated outside an OSPF Area border. One ONS 15600 in the ONS 15600 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15600 OSPF area.

---

- Under OSPF Area Range Table, click **Create**.
- In the Create Area Range dialog box, enter the following:
  - Range Address—Enter the area IP address for the ONS 15600s that reside within the OSPF area. For example, if the ONS 15600 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.



- Range Area ID—Enter the OSPF area ID for the ONS 15600s. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
  - Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.
  - Advertise—Check this box if you want to advertise the OSPF range table.
- c. Click **OK**.
- Step 7** All OSPF areas must be connected to Area 0. If the ONS 15600 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:
- a. Under OSPF Virtual Link Table, click **Create**.
  - b. In the Create Virtual Link dialog box, complete the following fields (OSPF settings must match OSPF settings for the ONS 15600 OSPF area):
    - Neighbor—The router ID of the Area 0 router.
    - Transit Delay (sec)—The service speed. One second is the default.
    - Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
    - Auth Type—If the router where the ONS 15600 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
    - Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
    - Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.
  - c. Click **OK**.
- Step 8** After entering ONS 15600 OSPF area data, click **Apply**.
- If you changed the Area ID, the TSC cards will reset, one at a time. The reset will take approximately 10 to 15 minutes.
- Step 9** Return to your originating procedure (NTP).

## DLP-E33 Set Up External or Line Timing

<b>Purpose</b>	This task defines the SONET timing source for the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-E21 Verify Card Installation, page 4-2</a> <a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Note

If you do not perform this procedure, the ONS 15600 defaults to its internal Stratum 3E clock.

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

**Step 2** In the General Timing area, complete the following information:

- **Timing Mode**—Choose **External** if the ONS 15600 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card that is optically connected to the timing node. A third option, **Mixed**, allows you to set external and line timing references.



**Note** Because Mixed timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.

- **SSM Message Set**—Choose the message set level supported by your network. If a Generation 1 node receives a Generation 2 message, the message will be mapped down to the next available Generation 1. For example, an ST3E message becomes an ST3.
- **Quality of RES**—If your timing source supports the reserved S1 byte, set the timing quality here. (Most timing sources do not use RES.) Qualities are listed in descending quality order as ranges. For example, ST3<RES<ST2 means the timing reference is higher than a Stratum 3 and lower than a Stratum 2. Refer to the “Synchronization Status Messaging” section in “Timing” chapter of the *Cisco ONS 15600 Reference Manual* for more information about synchronization status messaging (SSM), including definitions of the SONET timing levels.
- **Revertive**—Check this check box if you want the ONS 15600 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected. Five minutes is the default.
- **Reversion Time**—If Revertive is checked, choose the amount of time the ONS 15600 will wait before reverting back to its primary timing source.

**Step 3** In the Reference Lists area, complete the following information:

- **NE Reference**—Allows you to define three timing references (Ref-1, Ref-2, and Ref-3). The node uses Reference 1 unless a failure occurs to that reference, in which case, the node uses Reference 2. If that fails, the node uses Reference 3, which is typically set to Internal Clock. This is the Stratum 3E clock provided on the TSC. The options shown depend on the Timing Mode setting.
  - If the Timing Mode is External, your options are BITS1, BITS2, and Internal Clock.
  - If the Timing Mode is Line, your options are the node’s OC-N ports (except for ports that have been specified as protection ports in 1+1 protection groups) and Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node’s trunk cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 3/Port 16 is connected to the node wired to the BITS source, choose Slot 3 as Reference 1.
  - If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk cards as timing references.
- **BITS-1 Out/BITS-2 Out**—Sets the timing references for equipment wired to the BITS Out backplane pins. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to external, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

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



**Note** Refer to the *Cisco ONS 15600 Troubleshooting Guide* for timing-related alarms.

**Step 5** Click the **BITS Facilities** tab, and complete the following information:



**Note** The BITS Facilities section sets the parameters for your BITS-1 and BITS-2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

- **BITS In State**—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service) depending whether one or both BITS input pin pairs on the backplane are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).
- **BITS Out State**—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.

**Step 6** If the BITS In State for BITS-1 and BITS-2 is set to OOS, continue with [Step 8](#). If the BITS In State is set to IS for either BITS-1 or BITS-2, complete the following information:

- **Coding**—Set to the coding used by your BITS reference, either B8ZS (binary 8-zero substitution) or AMI (alternate mark inversion).
- **Framing**—Set to the framing used by your BITS reference, either ESF (Extended Super Frame) or SF (D4) (Super Frame).
- **Sync Messaging**—Check to enable SSM. SSM is not available if Framing is set to SF (D4).
- **AIS Threshold**—If SSM is disabled or SF (D4) is used, set the quality level where a node sends an alarm indication signal (AIS) from the BITS-1 Out and BITS-2 Out backplane pins. An alarm indication signal (AIS) is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.

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

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

## DLP-E34 Set Up Internal Timing

<b>Purpose</b>	This task sets up internal timing (Stratum 3E) for an ONS 15600 or sets up other nodes in the network to be line timed off of the node's internal clock.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	Not recommended; use only if no BITS source or line timing sources are available
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



### Caution

Internal timing is Stratum 3E and not intended for permanent use. All ONS 15600s should be timed to a Stratum 2 or better primary reference source.

- 
- Step 1** In node view, click the **Provisioning > Timing > General** tabs.
- Step 2** In the General Timing area, enter the following:
- Timing Mode—Set to **External**.
  - SSM Message Set—Set to **Generation 1**.
  - Quality of RES—Set to **DUS**.
  - Revertive—Not relevant for internal timing.
  - Reversion Time—Not relevant for internal timing.
- Step 3** In the Reference Lists area, enter the following information:
- Ref1—Set to **Internal Clock**.
  - Ref2—Set to **Internal Clock**.
  - Ref3—Set to **Internal Clock**.
  - BITS-1 Out/BITS-2 Out—Set to **None**.
- Step 4** Click **Apply**.
- Step 5** Click the **BITS Facilities** tab and change the BITS In State and BITS Out State to **OOS** (out of service). Disregard the other BITS Facilities settings; they are not relevant to internal timing.
- Step 6** Click **Apply**.
- Step 7** Log into a node that will be timed from the node set up in Steps 1 through 6 (the internally timed node).
- Step 8** Click the **Provisioning > Timing > General** tabs.
- Step 9** In the General Timing area, enter the same information as entered in [Step 2](#), except set Timing Mode to **Line**.
- Step 10** In the Reference Lists area, enter the same information as entered in [Step 3](#), except set NE Reference as follows:
- Ref1—Set to the OC-N trunk card with the closest connection to the internally timed node.
  - Ref2—Set to the OC-N trunk card with the next closest connection to the internally timed node.
  - Ref3—Set to **Internal Clock**.
  - BITS-1 Out/BITS-2 Out—Set to **None**.
- Step 11** Click **Apply**.
- Step 12** Repeat Steps 8 through 11 at each node that will be timed by the internally timed node.
- Step 13** Return to your originating procedure (NTP).
-

## DLP-E35 Create a New User on a Single Node

<b>Purpose</b>	This task creates a new user for one ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 **Create**.

**Step 3** In the Create User dialog box, enter the following:

- **Name**—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be 6 to 10 characters, and the first character must be an alpha character.
- **Password**—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special characters (+, #, %), where at least two characters are non alphabetic and at least one character is a special character. For Transaction Language One (TL1) compatibility, the password must be 6 to 10 characters, and the first character must be an alpha character. The password must not contain the user name.
- **Confirm Password**—Type the password again to confirm it.
- **Security Level**—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15600 Reference Manual* for information about the capabilities provided with each level.



**Note** Idle time is the length of time that CTC can remain unused before it locks and requires that a user reenter the password. Each security level has a different idle time: Retrieve is unlimited, Maintenance is 60 minutes, Provisioning is 30 minutes, and Superuser is 15 minutes. To change the idle times, refer to the “[NTP-E63 Modify Users and Change Security](#)” procedure on [page 11-6](#).

**Step 4** Click **OK**.

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

## DLP-E36 Create a New User on Multiple Nodes

<b>Purpose</b>	This task adds a new user to multiple ONS 15600s.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Superuser only



**Note** All nodes where you want to add users must be accessible in network view.

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Provisioning > Security > Users** tabs.
- Step 3** Click **Create**.
- Step 4** In the Create User dialog box, enter the following:
- **Name**—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must have no more than 10 characters, and the first character must be an alpha character.
  - **Password**—Type the user password. The password must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) and special characters (+, #, %), where at least two characters are nonalphanumeric and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters, and the first character must be an alpha character. The password must not contain the user name.
  - **Confirm Password**—Type the password again to confirm it.
  - **Security Level**—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the *Cisco ONS 15600 Reference Manual* for information about the capabilities provided with each level.



**Note** Idle time is the length of time that CTC can remain unused before it locks and requires that a user reenter the password. Each security level has a different idle time: Retrieve is unlimited, Maintenance is 60 minutes, Provisioning is 30 minutes, and Superuser is 15 minutes. To change the idle times, refer to the “[NTP-E63 Modify Users and Change Security](#)” procedure on [page 11-6](#).

- Step 5** In the Select applicable nodes area, uncheck any nodes where you do not want to add the user (all network nodes are checked by default).
- Step 6** Click **OK**.
- Step 7** In the User Creation Results dialog box, click **OK**.
- Step 8** Return to your originating procedure (NTP).

## DLP-E39 Optical 1+1 Manual Protection Switch Test

<b>Purpose</b>	This task verifies that a 1+1 protection group will switch properly.
<b>Tools/Equipment</b>	Optical test set and cables
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC</a> , page 16-39; a test circuit as part of the topology acceptance test
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher

- 
- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Click the **Alarms** tab.
- Verify that the alarm filter is not on. See the “[DLP-E157 Disable Alarm Filtering](#)” task on page 17-46 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 Troubleshooting Guide*.
- Step 3** Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15600 Troubleshooting Guide*.
- Step 4** Double-click the node containing the 1+1 protection group you are testing. The node view appears.
- Step 5** Click the **Maintenance > Protection** tabs.
- Step 6** In the Protection Groups area, click the 1+1 protection group.
- Step 7** Click the working port. Next to Switch Commands, click **Force**.
- Step 8** In the Confirm Manual Operation dialog box, click **Yes**.
- Step 9** In the Selected Group area, verify that the following appears:
- ```
Protect port - Protect/Active [FORCE_SWITCH_TO_PROTECT], [PORT STATE]
Working port - Working/Standby [FORCE_SWITCH_TO_PROTECT], [PORT STATE]
```
- Step 10** Verify that the traffic on the test set connected to the node is still running. Some bit errors are normal. The traffic flow can be interrupted for less than 50 ms. If a traffic interruption of more than 50 ms occurs, complete [Step 11](#) to clear the switch, then repeat Steps 6 through 9, monitoring traffic on your test set. If the problem remains, contact your next level of support.
- Step 11** Next to Switch Commands, click **Clear**.
- Step 12** In the Confirm Clear Operation confirmation dialog box, click **Yes**.
- Step 13** In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.
- Step 14** In the Confirm Force Operation dialog box, click **Yes**.
- Step 15** In the Selected Group area, verify that the following appears:
- ```
Protect port - Protect/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]
Working port - Working/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]
```

- Step 16** Verify that traffic on the test set connected to the node is still running. The traffic flow can be interrupted for less than 50 ms. If a traffic interruption of more than 50 ms occurs, complete [Step 11](#) and [Step 12](#) to clear the switch, then repeat Steps [13](#) through [15](#), monitoring traffic on your test set. If the problem remains, contact your next level of support.
- Step 17** Return to your originating procedure (NTP).

## DLP-E40 Path Protection Switching Test

<b>Purpose</b>	This task verifies that a path protection span is switching correctly.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	Provisioning or higher



**Note** Although a service interruption under 60 ms might occur, the test circuit should continue to work before, during, and after the switches. If the circuit stops working, do not continue. Contact your next level of support.

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Right-click the span where you want to switch path protection traffic and choose **Circuits**.  
The Circuits on Span dialog box displays the path protection circuits, including circuit names, location, and a color code showing which circuits are active on the span.
- Step 3** Initiate a Force switch for all circuits on the span:



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

- a. Click the **Perform UPSR span switching** field.
  - b. Choose **FORCE** from the drop-down list.
  - c. Click **Apply**.
  - d. In the confirmation dialog box, click **Yes**.
  - e. In the Protection Switch Result dialog box, click **OK**.
- In the Circuits on Span dialog box, the Switch State for all circuits is FORCE.



**Note** Unprotected circuits will not switch.

- Step 4** Clear the Force switch:
- a. Click the **Perform UPSR span switching** field.
  - b. Choose **CLEAR** from the drop-down list.



- c. Click **Apply**.
- d. In the confirmation dialog box, click **Yes**.
- e. In the Protection Switch Result dialog box, click **OK**.

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

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

## DLP-E41 Provision an Optical Circuit Source and Destination

<b>Purpose</b>	This task provisions the source and destination cards for an optical circuit.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	Perform this task during one of the following procedures: <a href="#">NTP-E160 Create an Automatically Routed Optical Circuit, page 6-4</a> <a href="#">NTP-E161 Create a Manually Routed Optical Circuit, page 6-9</a> <a href="#">NTP-E40 Create a Unidirectional Optical Circuit with Multiple Drops, page 6-12</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 Node drop-down list, choose the node where the circuit will originate.

**Step 2** From the Slot drop-down list, choose the slot containing the optical card where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)

**Step 3** Choose the source port from the Port drop-down list.

**Step 4** Choose the synchronous transport signal (STS) from the STS drop-down list. STSs do not appear if they are already in use by other circuits.



**Note** The STSs that appear depend on the card, circuit size, and protection scheme.

**Step 5** If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection, click **Use Secondary Source** and repeat Steps 1 through 4 to define the secondary source.

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

**Step 7** From the Node drop-down list, choose the destination node.

**Step 8** From the Slot drop-down list, choose the slot containing the optical card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

**Step 9** Choose the destination port from the Port drop-down list.

**Step 10** Choose the STS from the STS drop-down list. STSs do not appear if they are already in use by other circuits.




---

**Note** The STSs that appear depend on the card, circuit size, and protection scheme.

---

- Step 11** If you need to create a secondary destination, for example, a path protection bridge-selector circuit entry point in a multivendor path protection, click **Use Secondary Destination** and repeat Steps 7 through 10 to define the secondary destination.
- Step 12** Click **Next**.
- Step 13** Return to your originating procedure (NTP).
- 

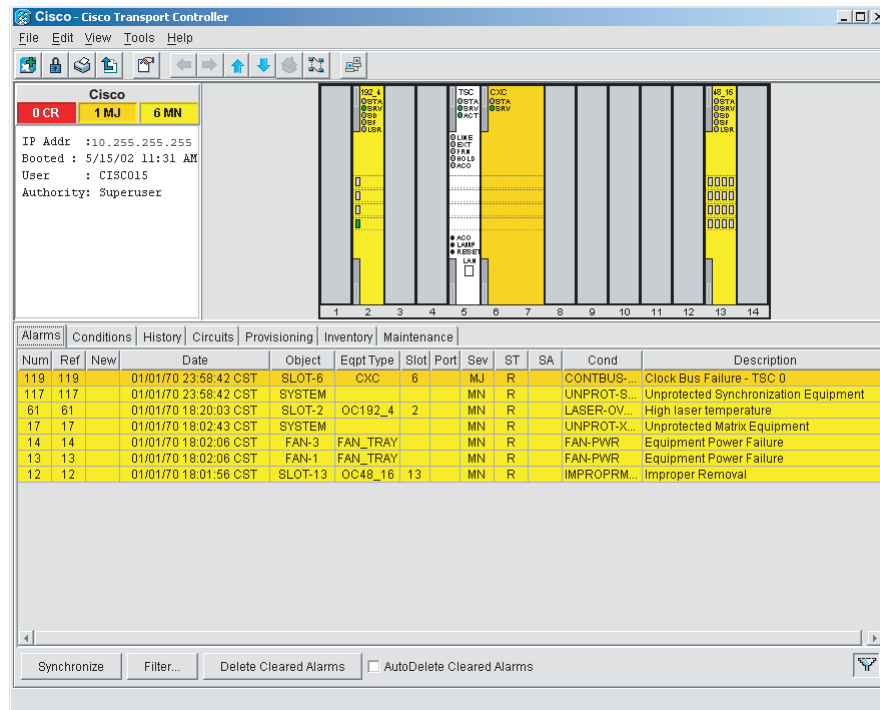
## DLP-E43 View Alarms

<b>Purpose</b>	This task displays ONS 15600 alarms at the card, node, or network level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

- Step 1** In the card, node, or network view, click the **Alarms** tab to display the alarms for that card, node, or network. [Figure 16-13](#) shows the Alarms window.

Figure 16-13 Viewing Alarms in CTC Node View



78449

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

## DLP-E44 View Alarm History

<b>Purpose</b>	This task displays past cleared and uncleared ONS 15600 alarms at the card, node, or network level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

**Step 1** To view history for the login node, go to [Step 2](#).

To view alarm history for the network, go to [Step 3](#).

To view alarm history for the card, go to [Step 4](#).

**Step 2** To display the node-level alarm history:

- Click the **History > Session** tabs if you want to see only the alarms and events that have occurred since you logged into the current CTC session.
- Click the **History > Node** tabs if you want to retrieve all available alarms for the node.
- Go to [Step 5](#).



**Note** At the network-level view, CTC displays only network alarms and events that occur during your current login session.

**Step 3** To view alarm information for the network level:

- a. From the View menu, choose **Go to Network View**.
- b. Click the **History** tab.

Alarms and events that have occurred on the network since you logged into CTC appear.

- c. Go to [Step 5](#).

**Step 4** To view alarm information for the card level:

- a. In node view, double-click a card on the shelf graphic to display the card view.
- b. Click the **History > Session** tabs if you want to see only the alarms and events that have occurred since you logged into CTC.
- c. Click the **History > Card** tabs if you want to retrieve all available alarms for the card.
- d. Go to [Step 5](#).



**Note** The ONS 15600 can store up to 3,000 total alarms and events: 750 Critical (CR) alarms, 750 Major (MJ) alarms, 750 Minor (MN) alarms, and 750 events. When the limit is reached for an alarm or event type, the ONS 15600 overwrites the oldest alarms and events.

**Step 5** Verify that the Alarms check box is selected. Alarms are events with a severity of Minor (MN), Major (MJ), or Critical (CR).

**Step 6** If you want to retrieve events, check the **Events** check box.

Events include both alarms and conditions. Conditions are events with a severity of Not Alarmed (NA) or Not Reported (NR).

**Step 7** Click **Retrieve**.



**Tip**

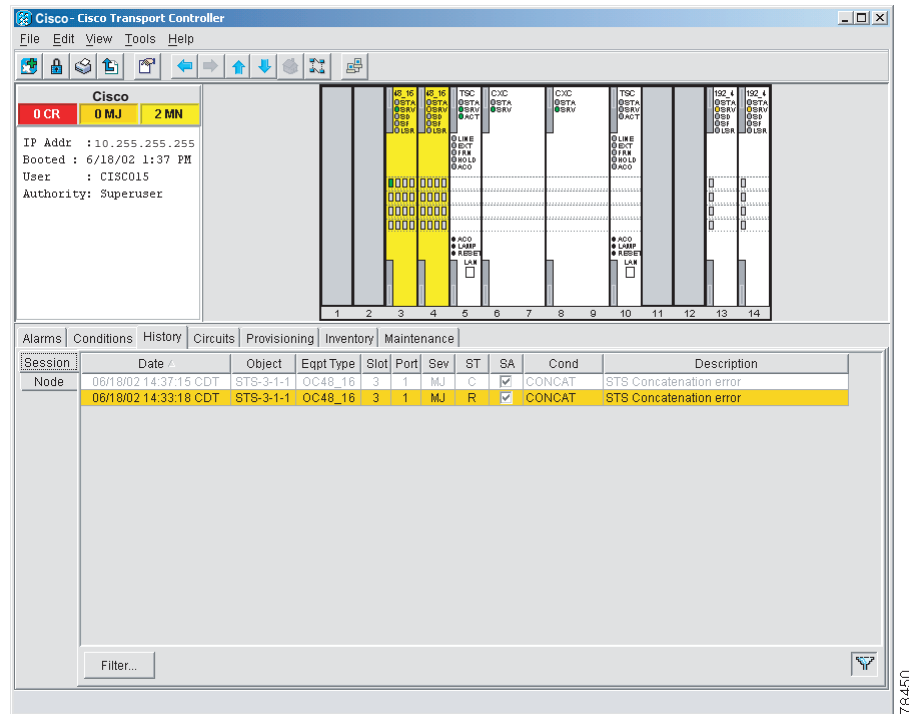
Double-click an alarm in the alarm table or an event in the history table to display the corresponding view for the alarm. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Beginning with Software Release 1.1, alarms have specifically numbered STS object identifiers based upon the object TL1 access identifiers (AIDs). The port-based alarm numbering scheme is shown in [Table 16-4](#). [Figure 16-14 on page 16-61](#) shows an example of viewing all alarms reported for the current session in CTC.

**Table 16-4** Release 1.1 and Later Port-Based Alarm Numbering Scheme

Object	STS AID	Port Number
MON object	STS-<Slot>-<Port>-<STS> For example, STS-6-1-6	Port=1

Figure 16-14 Viewing All Alarms Reported for Current Session



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

76450

## DLP-E45 View Conditions

<b>Purpose</b>	This task displays conditions (events with an NR severity) at the card, node, or network level. Conditions give you a record of changes or events that did not result in alarms.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

**Step 1** To view alarm history for the login node, go to [Step 2](#).

If you want to view alarm history for the network, go to [Step 3](#).

If you want to view alarm history for the card, go to [Step 4](#).

**Step 2** To display the node-level conditions:

- Click the **Conditions** tab if you want to see only the conditions that apply to the node.
- Go to [Step 5](#).

- Step 3** To view network-level conditions:
- From the View menu, choose **Go to Network View**.
  - Click the **Conditions** tab if you want to see only the conditions that apply to the network.



**Note** If you are not in the node (default) CTC view, you can also click the Conditions tab in the card and network views to obtain the same results.

- Step 4** To view card-level conditions:
- Double-click a card on the shelf graphic to display the card view.
  - Click the **Conditions** tab if you want to see only the conditions that apply to the card.

- Step 5** Click **Retrieve**. (See Figure 16-15.)

Conditions include both alarms and events. Alarms are conditions with a severity of MN, MJ, or CR. Events are conditions with a severity of NA or NR.

**Figure 16-15** Viewing Retrieved Fault Conditions in the Conditions Window

Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	SA	Cond	Description
07/20/05 09:50:09 PDT	FAC-14-16	OC48_16	14	16		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-15	OC48_16	14	15		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-14	OC48_16	14	14		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-13	OC48_16	14	13		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-12	OC48_16	14	12		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-11	OC48_16	14	11		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-10	OC48_16	14	10		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-9	OC48_16	14	9		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-8	OC48_16	14	8		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-7	OC48_16	14	7		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-6	OC48_16	14	6		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-5	OC48_16	14	5		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-4	OC48_16	14	4		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-3	OC48_16	14	3		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-2	OC48_16	14	2		NR	LOF		Loss of Frame
07/20/05 09:50:09 PDT	FAC-14-1	OC48_16	14	1		NR	LOF		Loss of Frame

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

## DLP-E46 Display Events Using Each Node's Time Zone

<b>Purpose</b>	This task changes the time stamp for events to the time zone of the ONS node reporting the alarm. By default, the events time stamp is set to the time zone for the CTC workstation.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Retrieve or higher

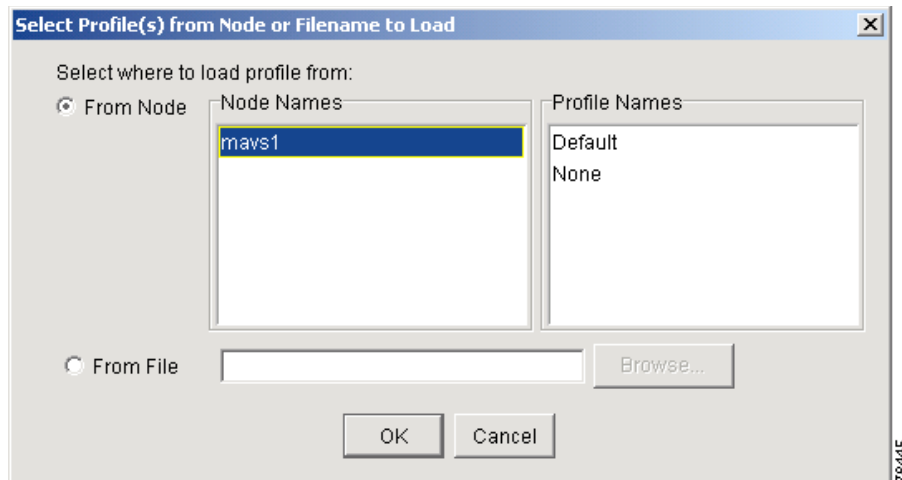
- 
- Step 1** From the Edit menu, choose **Preferences**.  
The CTC Preferences Dialog appears.
- Step 2** Click the **Display Events Using Each Node's Timezone** check box.
- Step 3** Click **Apply** and **OK**.
- Step 4** Return to your originating procedure (NTP).
- 

## DLP-E48 Create Alarm Severity Profiles

<b>Purpose</b>	This task creates severity profiles for alarms by modifying the default severity profile.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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** tabs.
- Step 3** In the Node/Profile Ops area, click **Load**.
- Step 4** Highlight the node name you are logged into in the Node Names field and highlight **Default** in the Profile Names field ([Figure 16-16](#)).

**Figure 16-16** Select Profile(s) from Node or Filename to Load Dialog Box



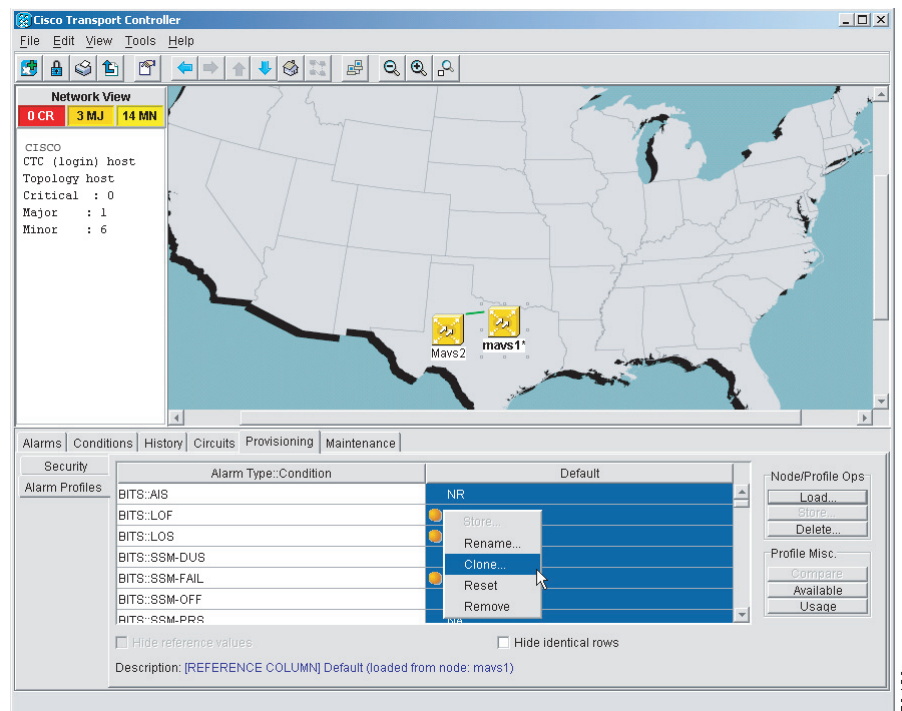
**Step 5** Click **OK**.

**Step 6** Right-click in the Default column to display the profile editing shortcut menu.

**Step 7** Choose **Clone** in the shortcut menu (Figure 16-17).

In the profile editing shortcut menu, any profile other than Inherited can be cloned.

**Figure 16-17** Alarm Profiles Window Showing the Default Profile of the Listed Alarms



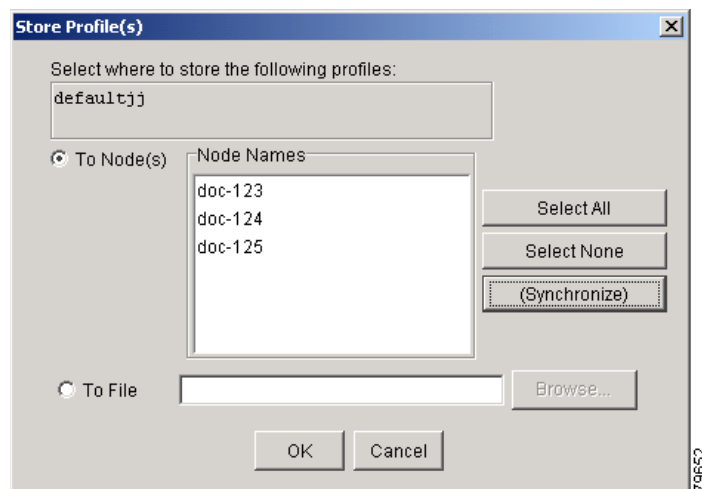
**Step 8** In the Clone Profile Default dialog box, type a name in the New Profile Name field.

Alarm profile names must be unique. If you try to import or name a profile that has the same name as another profile, CTC adds a suffix to create a new name.



- Step 9** Click **OK**. A new alarm profile (named in [Step 8](#)) is created. This profile duplicates the severities of the default profile and appears as a new column on the right side.
- Step 10** Modify the alarm profile:
- In the new alarm profile column, left-click the alarm severity you want to change in the alarm profile column.
  - Select the desired severity from the drop-down list.
  - Repeat Steps [a](#) and [b](#) for each alarm severity that needs to be changed.
  - After you have chosen severities for your new alarm profile, click anywhere in new alarm profile column to highlight it.
  - Click **Store** in the Node/Profile Ops area or select Store from the shortcut menu.
- Step 11** If you want to save the profile to one or more nodes, click the **To Node(s)** radio button ([Figure 16-18](#)) and choose the node(s) where you want to save the profile:
- If you want to save the profile to only one node, click the node in the Node Names list.
  - If you want to save the profile to all nodes, click **Select All**.
  - If you do not want to save the profile to any nodes, click **Select None**.
  - If you want to update alarm profile information, click **(Synchronize)**.

**Figure 16-18** Store Profiles Dialog Box



- Step 12** If you want to save the profile to a file:
- Click the **To File** radio button.
  - Click **Browse** and navigate to the profile save location.
  - Enter a name in the File name field.
  - Click the **Select** button to choose this name and location.



**Note** Long file names are supported. CTC supplies a suffix of \*.pfl to stored files.

- Step 13** Click **OK** to store the profile.




---

**Note** Click the **Hide identical rows** check box to configure the Alarm Profiles window to display rows with dissimilar severities.

---




---

**Note** Click the **Hide reference values** check box to configure the Alarm Profiles window to display severities that do not match the Default profile.

---

**Step 14** As needed, complete the “[DLP-E49 Apply Alarm Profiles for Ports and Cards](#)” task on page 16-66.

**Step 15** As needed, complete the “[DLP-E50 Apply Alarm Profiles to Cards and Nodes](#)” task on page 16-68.

**Step 16** Return to your originating procedure (NTP).

---

## DLP-E49 Apply Alarm Profiles for Ports and Cards

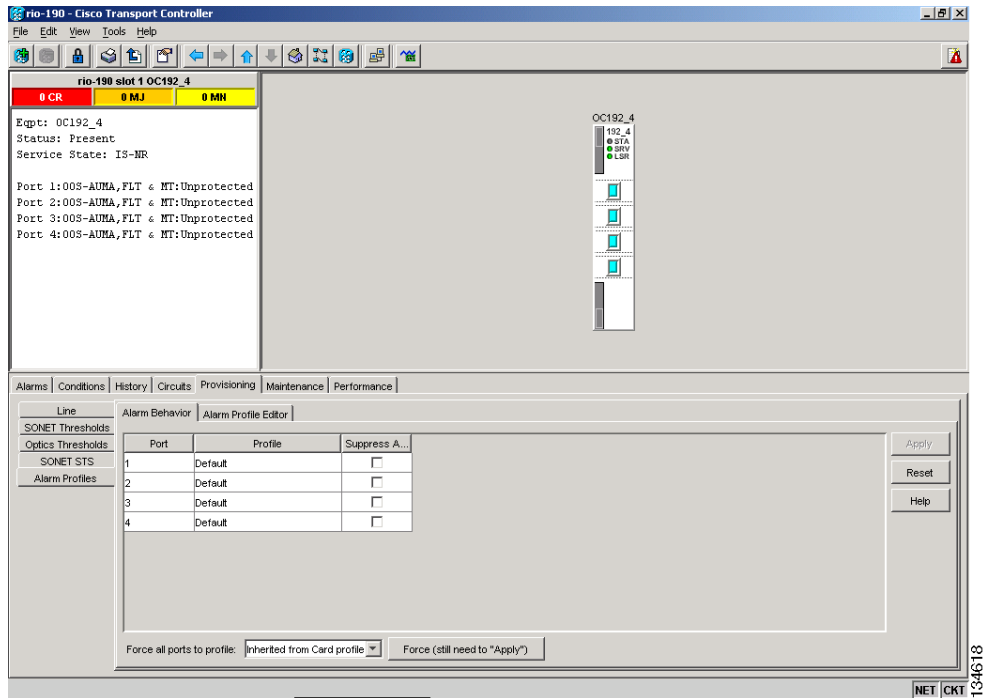
<b>Purpose</b>	This task applies alarm severity profiles to a port or a card.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E48 Create Alarm Severity Profiles, page 16-63</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</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 Behavior** tabs ([Figure 16-19](#)).

Figure 16-19 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-E50 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E48 Create Alarm Severity Profiles, page 16-63</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 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-E51 Suppress Alarm Reporting

<b>Purpose</b>	This task suppresses the reporting of ONS 15600 alarms at the port, card, or node level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 Behavior** tabs.

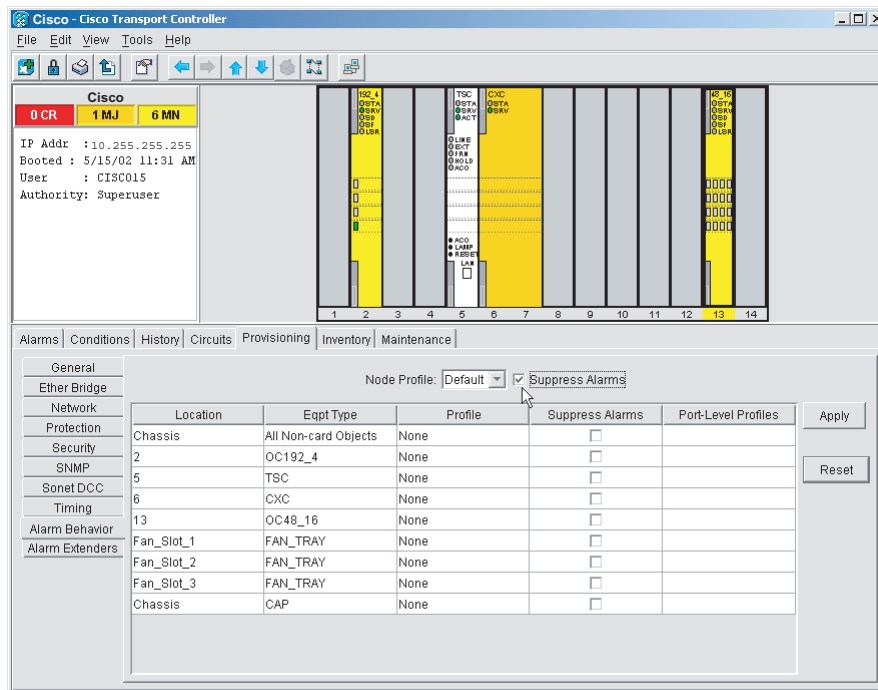


**Note** Suppressing alarms for a card or node causes the alarms to appear on the CTC Conditions window instead of the Alarms window. The suppressed alarms on the Conditions window appear there with their alarm severities, color codes, and service-affecting status. But as conditions, their severities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

**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 (Figure 16-20).
- 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.

**Figure 16-20 Suppress Alarms Check Box**



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

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

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

## DLP-E52 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E51 Suppress Alarm Reporting, page 16-68</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 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-E53 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E11 Install Alarm Wires on the CAP, page 16-16</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 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 and ONS 15600 networks, only the last four virtual wires (13 through 16) are visible from the ONS 15454 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-E54 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E11 Install Alarm Wires on the CAP, page 16-16</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 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-E53 Provision External Alarms and Virtual Wires](#)” task on page 16-70 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-E55 View Optical OC-N PM Parameters

<b>Purpose</b>	This task enables you to view performance monitoring (PM) counts on a selected OC-N card and port to detect possible performance problems.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 OC-N card. The card view appears.
- Step 2** Click the **Performance** tab ([Figure 16-21](#)).

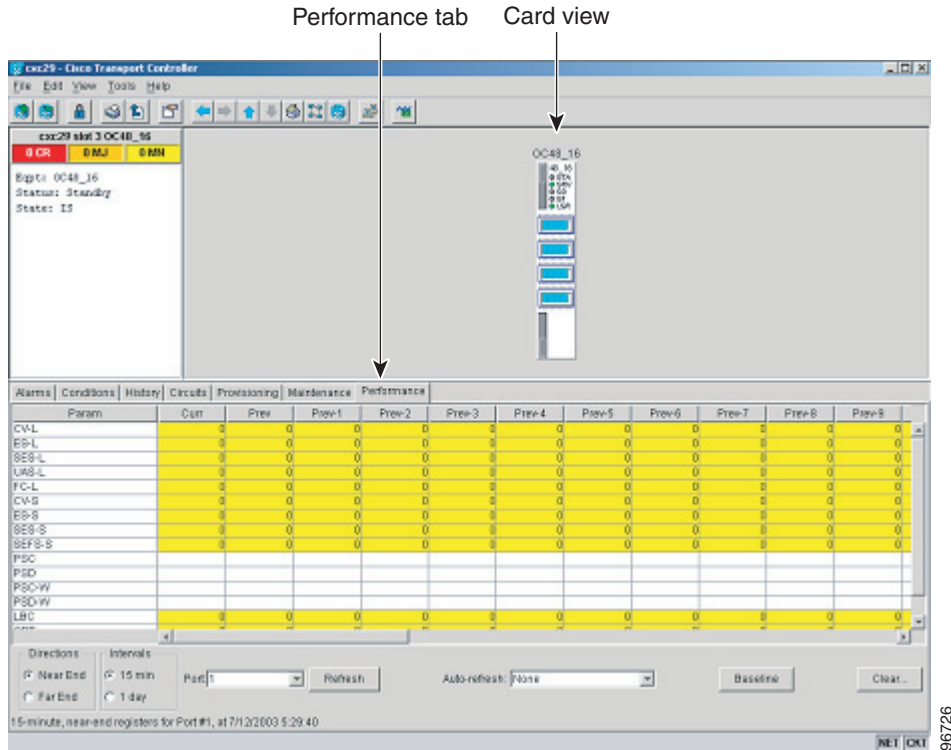


**Note** The performance window defaults to Port 1, STS 1 PM counts. Depending on the OC-N card, there are 48 STSs or 192 STSs per port. You must select the specific port and STS for which you want to view PM counts. See the “[DLP-E56 Refresh PM Counts for a Selected Port and STS](#)” task on page 16-73.

---



**Figure 16-21 Viewing Optical OC-N Performance Monitoring Information**



- 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 *Cisco ONS 15600 Reference Manual*.
- Step 4** Return to your originating procedure (NTP).

96726

## DLP-E56 Refresh PM Counts for a Selected Port and STS

<b>Purpose</b>	This task changes the window view to display PM counts for a selected OC-N card port and STS.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39.</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 OC-N card. The card view appears.
- Step 2** Click the **Performance** tab.
- Step 3** Click the Port drop-down list and click the desired port.
- Step 4** Click the STS drop-down list and click the desired STS ([Figure 16-22](#)).

Figure 16-22 Port and STS Fields on the Card View Performance Tab

Port drop-down list      STS drop-down list

- Step 5** Click **Refresh**. All PM counts occurring for the selected port and STS appear. For PM parameter definitions, refer to the *Cisco ONS 15600 Reference Manual*.
- Step 6** Return to your originating procedure (NTP).

## DLP-E57 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-E26 Log into CTC, page 16-39.</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 OC-N card. 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-E58 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-E26 Log into CTC, page 16-39.</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 OC-N card. 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 *Cisco ONS 15600 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-E59 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 STS.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39.</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 OC-N card. 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/STS appear. For PM parameter definitions refer to the *Cisco ONS 15600 Reference Manual*.

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

## DLP-E60 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 STS.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39.</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 OC-N card. 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/STS appear. For PM parameter definitions refer to the *Cisco ONS 15600 Reference Manual*.
- Step 5** Return to your originating procedure (NTP).
- 

## DLP-E62 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-E26 Log into CTC, page 16-39</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 OC-N card. 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-E63 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-E26 Log into CTC, page 16-39.</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 OC-N card. 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 are currently displayed 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 and one-day, near-end and 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 and one-day, near-end and 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** View the displayed columns to verify that the selected PM counts have been cleared.
- Step 7** Return to your originating procedure (NTP).
-

## DLP-E64 Search for Circuits

<b>Purpose</b>	This task searches for an ONS 15600 circuit at the network, node, or card level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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-E65 Filter the Display of Circuits

<b>Purpose</b>	This task filters the display of circuits in the ONS 15600 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-E26 Log into CTC, page 16-39</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** Click **Filter**.
- Step 4** 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 Dir—(dense wavelength division multiplexing [DWDM] optical channel network connections [OCHNC] only; refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*) Choose one: **East to West** (displays only east-to-west circuits); **West to East** (displays only west-to-east circuits).
- OCHNC Wlen—(DWDM OCHNCs only; refer to the *Cisco ONS 15454 DWDM Installation and Operations 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 one: **Any** (status not used to filter circuits), **DISCOVERED** (display only discovered circuits), **DISCOVERED\_TL1** (display only TL1-created or TL1-like, CTC-created circuits), **PARTIAL** (display only partial circuits, that is, circuits missing a connection or span to form a complete path), or **PARTIAL\_TL1** (display only TL1-created circuit or a TL1-like CTC-created circuits that are missing a cross-connect or span to form a complete path). For more information about circuit statuses, see [Table 18-2 on page 18-45](#). Although other statuses are described in the table, filtering is only supported for DISCOVERED, DISCOVERED\_TL1, PARTIAL, and PARTIAL\_TL1 circuits.



- State—Choose one: **OOS** (display only out-of-service circuits), **IS** (display only in-service circuits; optical channel network connections have IS status only), or **OOS-PARTIAL** (display only circuits with cross-connects in mixed service states).
  - Protection—Choose the protection type from the drop-down list.
  - 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) or **STS** (CTC displays only STS circuits).
  - Size—Click the appropriate check boxes to filter circuits based on size: STS-1, STS3c, STS-6c, STS-9c, STS-12c, STS-24c, STS-48c, STS-192c. The check boxes shown depend on the entry in the Type field.
- Step 5** Click **OK**. The Circuits tab displays only the circuits that meet the criteria set in the Filter dialog box.
- 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-E66 View Circuits on a Span

<b>Purpose</b>	This task views circuits on an ONS 15600 span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">Chapter 6, “Create Circuits”</a> <a href="#">DLP-E26 Log into CTC, page 16-39</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 BLSR, path protection, 1+1, or unprotected circuits on the span.
  - PCA Circuits—To view circuits routed on a BLSR protected channel. (This option does not appear if the span you right-clicked is not a BLSR span.)

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

- STS—Displays STSs used by the circuits.
- VT—(Not applicable for the ONS 15600) Displays Virtual Tributaries (VTs) used by the circuits.
- Path Protection—Indicates whether the circuit is in a path protection.

- **Circuit**—Displays the circuit name.
- **Switch State**—(path protection span only) Displays the switch state of the circuit, that is, whether any span switches are active. For path protection spans, switch types include: **CLEAR** (no spans are switched), **MANUAL** (a Manual switch is active), **FORCE** (a Force switch is active), and **LOCKOUT OF PROTECTION** (a span lockout is active).



**Note** You can complete other procedures from the Circuits on Span dialog box. If the span is in a path protection, you can switch the span traffic. See [“DLP-E40 Path Protection Switching Test” task on page 16-56](#) for instructions. If you want to edit a circuit on the span, double-click the circuit. See the [“DLP-E127 Edit Path Protection Circuit Path Selectors” task on page 17-24](#) for instructions.

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

---

## DLP-E67 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-E26 Log into CTC, page 16-39</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-E68 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-E26 Log into CTC, page 16-39</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:
- a. From the Edit menu, choose **Preferences**.
  - b. In the Preferences dialog box, click the **Circuit** tab.
  - c. Click the **Reset to Defaults** button.
  - d. Click **Apply** and click **OK** to close the Preferences dialog box.
- Step 7** Return to your originating procedure (NTP).
-

## DLP-E77 Change IP Settings

<b>Purpose</b>	This task changes the IP address, subnet mask, default router, and network defaults for the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E30 Provision IP Settings, page 16-44</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:

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

See the “[DLP-E30 Provision IP Settings](#)” task on page 16-44 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.

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

If you changed an IP address, subnet mask length, or TCC CORBA (IIOP) Listener Port, both ONS 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 tabs. If the changes do not appear, repeat the task.

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

---

## DLP-E78 Modify a Static Route

<b>Purpose</b>	This task modifies a static route on the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E31 Create a Static Route, page 16-46</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-E31 Create a Static Route](#)” task on page 16-46 for detailed field descriptions.
- Step 5** Click **OK**.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-E79 Delete a Static Route

<b>Purpose</b>	This task deletes a static route from the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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**. Confirm that the static route is deleted; if not, repeat the task.
- Step 5** Return to your originating procedure (NTP).
-

## DLP-E80 Disable OSPF

<b>Purpose</b>	This task disables the OSPF routing protocol process for the LAN on the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E32 Set Up or Change Open Shortest Path First Protocol, page 16-47</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 has interfaces (DCC or LAN) in multiple OSPF areas, at least one ONS 15600 interface (DCC or LAN) must be in the backbone area 0.0.0.0.



**Note** When you are logged into a ONS 15600 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-E81 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-E26 Log into CTC, page 16-39</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-E82 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-E26 Log into CTC, page 16-39</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 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat until the ONS 15600 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 icons are displayed at the magnification you want.
- Step 10** Return to your originating procedure (NTP).
- 

## DLP-E83 Apply a Customer 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-E26 Log into CTC, page 16-39</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 icons are not visible, right-click the network view and choose **Zoom Out**. Repeat this step until all the ONS 15600 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 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-E84 Create Domain Icons

<b>Purpose</b>	This task creates a domain icon, which can be used to group ONS 15600 icons in CTC network view.
<b>Tools/Equipment</b>	None
<b>Prerequisite procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



**Note** Domains are visible to all users who log into the network.

- 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-E85 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E84 Create Domain Icons, page 16-89</a>
<b>Required/As needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher



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

- Step 1** From the View menu, choose **Go To Network View**.
- Step 2** Locate the domain action you want in [Table 16-5](#) and complete the appropriate steps.

**Table 16-5** 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-E86 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-E26 Log into CTC, page 16-39</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-E25 Create a 1+1 Protection Group](#)” procedure on page 4-7 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-E87 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-E26 Log into CTC, page 16-39</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**. Confirm that the changes appear; if not, repeat the task.
- Step 5** Return to your originating procedure (NTP).

## DLP-E89 Change the Node Timing Source

<b>Purpose</b>	This task changes the SONET timing source for the ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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** tabs.
- Step 2** In the General Timing area, change any of the following information:
- Timing Mode
  - SSM Message Set
  - Quality of RES
  - Revertive

- Revertive Time

For detailed descriptions of these fields, see the “[NTP-E24 Set Up Timing](#)” procedure on page 4-6.

**Step 3** In the BITS Facilities 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.

- State
- Coding
- Framing
- Sync Messaging

**Step 4** In the Reference Lists area, you can change the NE Reference.

**Step 5** Click **Apply**. Confirm that the changes appear; if not, repeat the task.



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

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

## DLP-E91 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E35 Create a New User on a Single Node, page 16-53</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**. Confirm that the changes appear; if not, repeat the task.

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

## DLP-E93 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-E26 Log into CTC, page 16-39</a> <a href="#">DLP-E36 Create a New User on Multiple Nodes, page 16-54</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-E136 Log Out a User on Multiple Nodes](#)” task on page 17-30.

- 
- 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-E94 Modify SNMP Trap Destinations

<b>Purpose</b>	This task modifies Simple Network Management Protocol (SNMP) trap destinations on an ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 a trap in the Trap Destinations list box.  
For a description of SNMP traps, refer to the *Cisco ONS 15600 Troubleshooting Guide*.
  - 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 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** Click **Apply**. SNMP settings are now configured.
- Step 5** To view SNMP information for each node, click the node IP address in the Trap Destinations list.
- Step 6** Return to your originating procedure (NTP).
- 

## DLP-E95 Delete SNMP Trap Destination

<b>Purpose</b>	This task deletes an SNMP trap destination on an ONS 15600.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

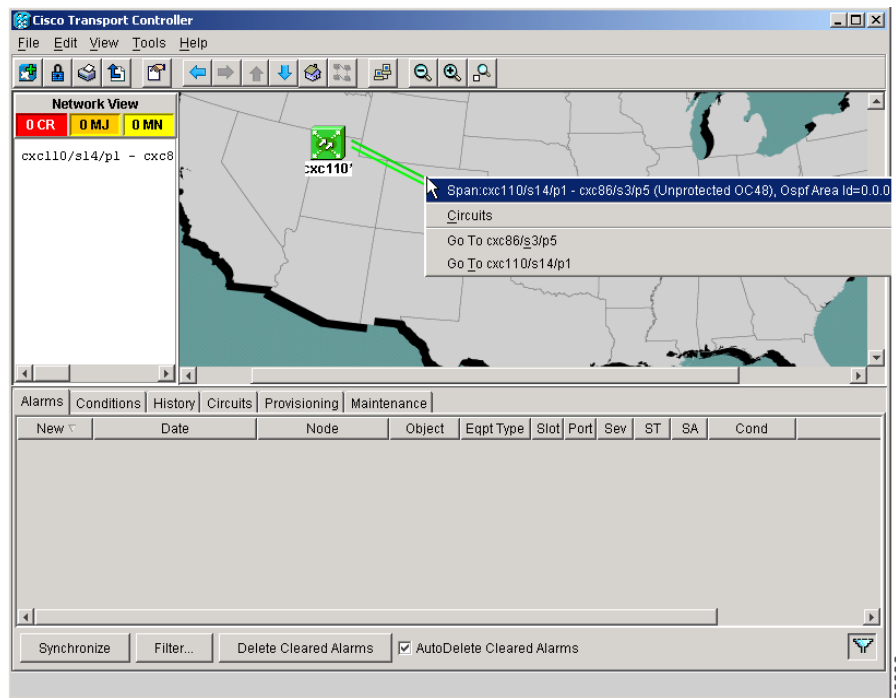
- Step 1** In node view, click the **Provisioning > SNMP** tabs.
- Step 2** Click the trap that you want to delete in the Trap Destination list box.
- Step 3** Click **Delete**. A confirmation dialog box appears.
- Step 4** Confirm that the changes are correct and click **Yes**. Confirm that the changes appear; if not, repeat the task.
- Step 5** Return to your originating procedure (NTP).
-

## DLP-E96 Switch All Path Protection Circuits on a Span

<b>Purpose</b>	This task applies a FORCE external switching command to all circuits on a path protection span. The FORCE switches the traffic to another span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC</a> , page 16-39
<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 path protection traffic ([Figure 16-23](#)).

**Figure 16-23** Using the Span Shortcut Menu to Display Circuits



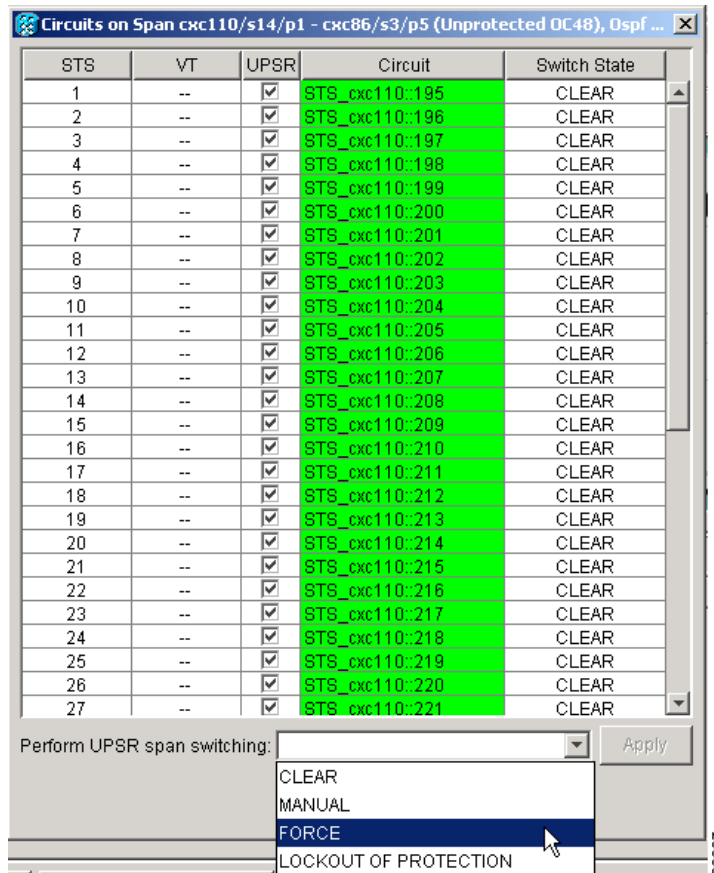
- Step 3** Choose **Circuits** from the shortcut menu.
- Step 4** In the Circuits on Span dialog box, select **Force** ([Figure 16-24](#)).



**Caution**

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

Figure 16-24 Switching a Path Protection Path



- 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-E97 Clear a Switch for all Path Protection Circuits on a Span

<b>Purpose</b>	This task clears a Force traffic switch for all circuits on a path protection span.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</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 ([Figure 16-23](#)).



- 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-E98 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-E26 Log into CTC, page 16-39</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** 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:
- 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-E89 Change the Node Timing Source](#)" task on page 16-91.
  - 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 **OOS**. 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-E89 Change the Node Timing Source](#)" task on page 16-91.



**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 SONET links (east and west) as timing sources, traceable to the node with external BITS timing.
- Step 6** Return to your originating procedure (NTP).
-

## DLP-E99 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 OC-N cards
<b>Prerequisite Procedures</b>	<a href="#">DLP-E26 Log into CTC, page 16-39</a>
<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 allows a Manual switch on a port in the OOS-MA,DSBLD service state.

- 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 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 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).
-

