



# CHAPTER 16

## DLPs F100 to F199

---

### DLP-F161 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

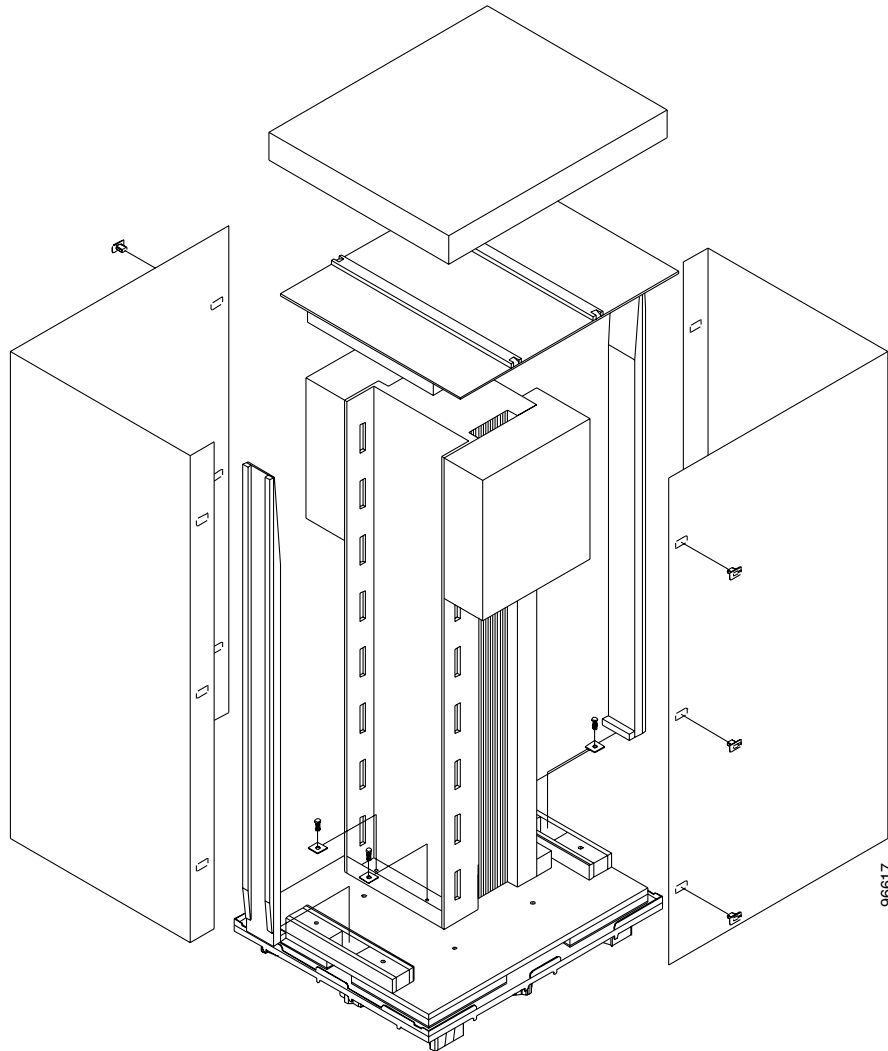
**In order to safeguard both equipment and personnel during the installation process, we recommend that four people participate in moving the unit. Using adequate manpower is the best guarantee that you will avoid harming people or equipment.** Statement 129

---

**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 SDH.

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

**Figure 16-1** ONS 15600 SDH 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, page 1-2](#).
- Step 10** Return to your originating procedure (NTP).

## DLP-F162 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-F161 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)/customer access panel version 2 (CAP2) 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/CAP2 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-F163 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-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4</a>
<b>Required/As Needed</b>	Required
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** 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.

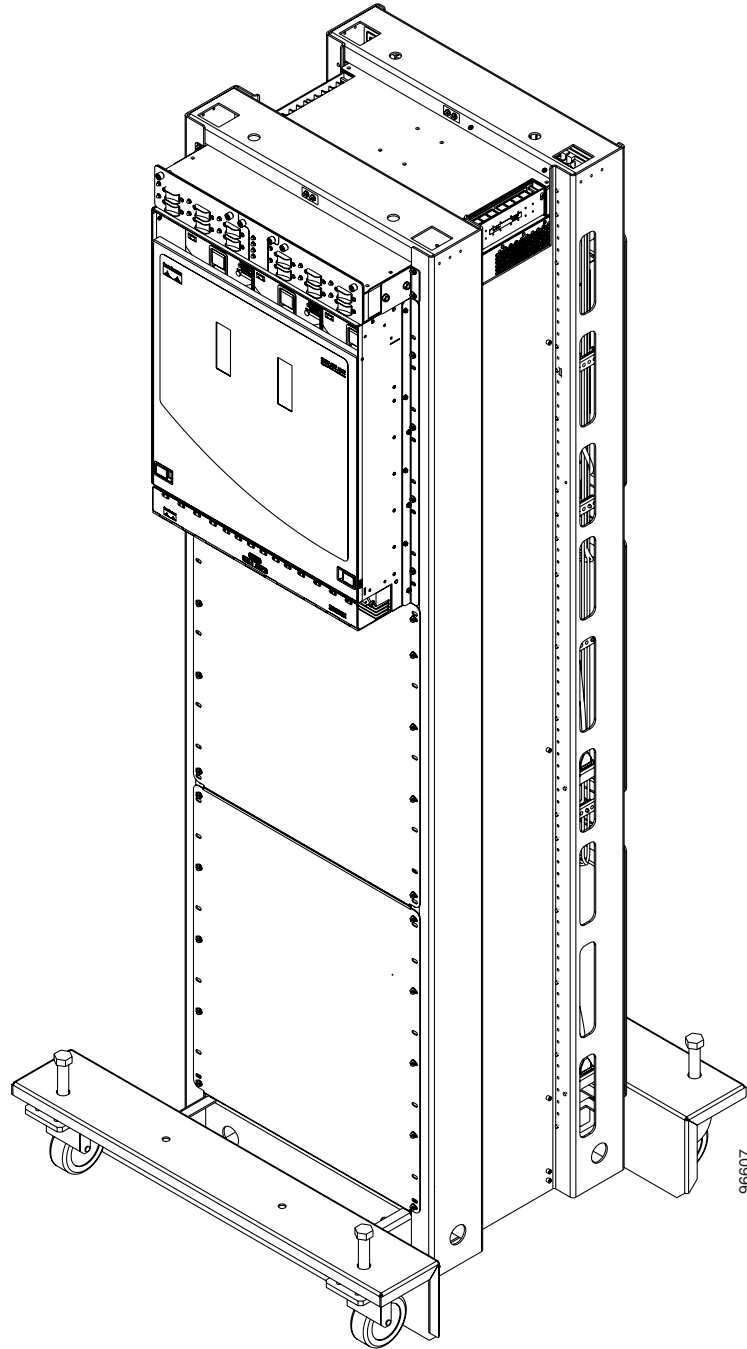
**Step 6** Use a socket wrench to turn one of the screws attached to a caster five turns to the right (clockwise). Repeat this at each screw and repeat in sequence so that the bay gradually rises to maximum height (1-3/4 in. [44.45 mm]) off the pallet.

**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 SDH with Dollies Installed



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

---

## DLP-F164 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-F108 Unpack and Inspect the ONS 15600 SDH Bay Assembly, page 1-4</a></p> <p><a href="#">DLP-F248 Drill Holes to Anchor and Provide Access to the Bay Assembly, page 17-41</a></p> <p><a href="#">DLP-F163 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 SDH 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 SDH 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-F166 Create an IP-Encapsulated Tunnel

<b>Purpose</b>	This task creates a an IP-encapsulated tunnel to transport traffic from third-party SDH equipment across ONS 15600 SDH networks. IP-encapsulated tunnels are created on the regenerator-section data communications channel (RS-DCC) channel (D1-D3) (if not used by the ONS 15600 SDH as a terminated DCC).
<b>Tools/Equipment</b>	STM-N cards must be installed.
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-32</a> <a href="#">NTP-F163 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 SDH can have up to 128 IP-encapsulated tunnel connections. Terminated Regenerator-Section DCCs (RS-DCCs) used by the ONS 15600 SDH cannot be used as tunnel endpoints, and an RS-DCC that is used as a tunnel endpoint cannot be terminated. All tunnel connections are bidirectional.

---

- Step 1** Verify that IP addresses are provisioned at both the source and destination nodes of the planned tunnel. For more information, see the “[DLP-F185 Provision IP Settings](#)” task on page 16-36.
- 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 RS-DCC 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-F254 Change the Service State for a Port](#)” task on page 17-48 for instructions.

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

## DLP-F167 Connect Office Power to the ONS 15600 SDH Bay

<b>Purpose</b>	This task connects power to the ONS 15600 SDH 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>	Connect the bay assembly to the office ground. For detailed instructions on grounding the chassis, refer to the <a href="#">Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide</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 SDH Troubleshooting Guide*.



---

**Step 1** Measure and cut the cables as needed to reach the ONS 15600 SDH PDU from the office power distribution panel. [Figure 17-8 on page 17-72](#) shows the ONS 15600 SDH 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-F168 Route and Terminate Raised-Floor Power Cables” task on page 16-10](#).

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



---

**Note** When terminating battery and battery return connections as shown in [Figure 17-8 on page 17-72](#), follow a torque specification of 36 in-lb. When terminating a frame ground, use the Kepnut provided with the ONS 15600 SDH 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).

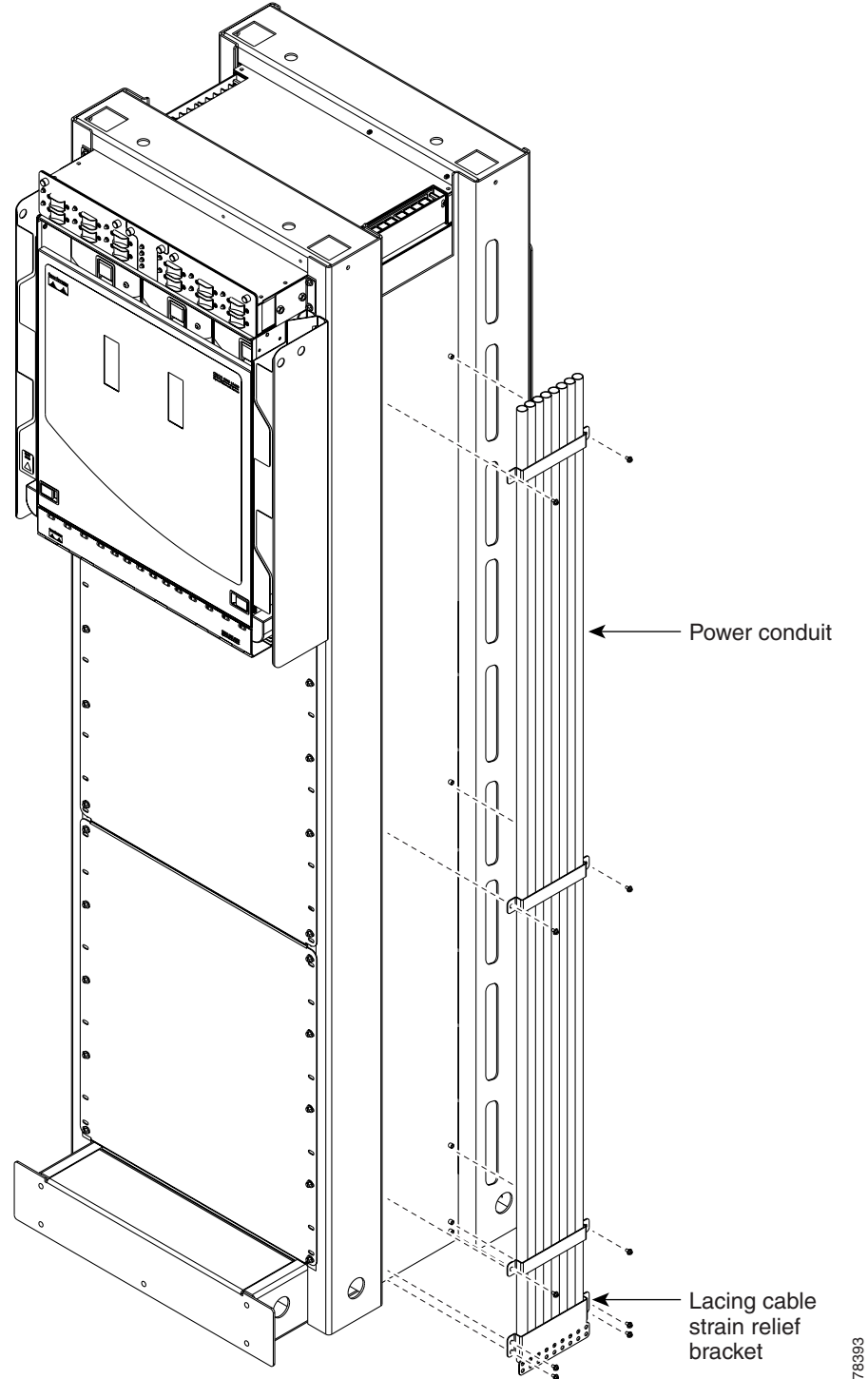
---

## DLP-F168 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>Connect the bay assembly to the office ground. For detailed instructions on grounding the chassis, refer to the <a href="#">Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide</a>.</p> <p><a href="#">DLP-F167 Connect Office Power to the ONS 15600 SDH Bay, page 16-8</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 16-3](#)).
- 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 16-3** *Installing the Power Conduit in a Raised-Floor Power Environment*



- 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-F169 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>	Connect the bay assembly to the office ground. For detailed instructions on grounding the chassis, refer to the <a href="#">Cisco ONS Electrostatic Discharge (ESD) and Grounding Guide</a> . <a href="#">DLP-F167 Connect Office Power to the ONS 15600 SDH Bay, page 16-8</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 SDH 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-F170 Install T1 (100 Ohm) Timing Connections on the CAP/CAP2

<b>Purpose</b>	This task installs timing connections from a 100-ohm T1 source to the CAP/CAP2; 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-F113 Install the Bay Power and Ground, page 1-10</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None

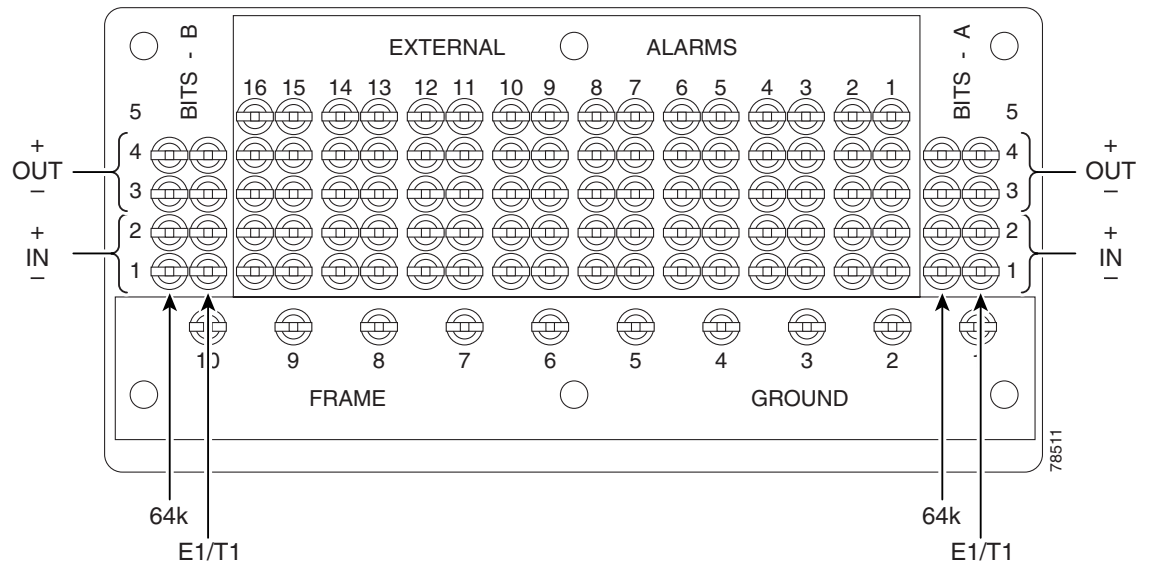
- Step 1** Wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

Figure 16-4 shows the location of the timing connections on the pin field.



**Note** Only 100-ohm T1 BITS is supported in Release 8.0.

**Figure 16-4** BITS Timing Connections on the CAP/CAP2



- 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 SDH Reference Manual*. To set up system timing, see the [NTP-F137 Set Up Timing, page 4-9](#).

- 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-F171 Install LAN Cables on the CAP/CAP2

<b>Purpose</b>	This task installs the LAN wires on the CAP/CAP2; 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-F113 Install the Bay Power and Ground, page 1-10</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<b>Security Level</b>	None



**Note** Only the active 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/CAP2 card so that connection to the ONS 15600 SDH 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/CAP2 ([Figure 16-5 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-F172 Install the TL1 Craft Interface Cable

<b>Purpose</b>	This task installs the Transaction Language One (TL1) craft interface cable on the CAP/CAP2.
<b>Tools/Equipment</b>	EIA/TIA-232 cable (9 pin D-sub)
<b>Prerequisite Procedures</b>	<a href="#">NTP-F113 Install the Bay Power and Ground, page 1-10</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/CAP2.  
[Figure 18-28 on page 18-110](#) shows the back of the ONS 15600 SDH, including the CAP/CAP2 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 SDH. Refer to the *Cisco ONS SDH TL1 Command Guide* for further information.

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

## DLP-F173 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 1-14</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/CAP2 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-F174 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-F181 Log into CTC, page 16-32</a>
<b>Required/As Needed</b>	As needed

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

**Step 1** In node view, 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-F229 Delete a 1+1 Protection Group](#)” task on [page 17-25](#).
- The card has any circuits; see the “[DLP-F293 Delete Circuits](#)” task on [page 17-83](#).
- The card is being used for timing; see the “[DLP-F230 Change the Node Timing Source](#)” task on [page 17-26](#).
- The card has an SDH DCC termination; see the [NTP-F209 Modify or Delete Communications Channel Terminations](#), [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-F175 Install Fiber-Optic Cables in a 1+1 Configuration

<b>Purpose</b>	This task installs fiber-optic cables on optical (STM-N) cards in a 1+1 linear configuration.
<b>Tools/Equipment</b>	Fiber-optic cables
<b>Prerequisite Procedures</b>	<a href="#">NTP-F119 Install the STM-N Cards</a> , <a href="#">page 2-4</a> <a href="#">NTP-F231 Clean Fiber Connectors and Adapters</a> , <a href="#">page 14-16</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 STM-16 or STM-64 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 STM-16 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
	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
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 STM-64 card faceplate.

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

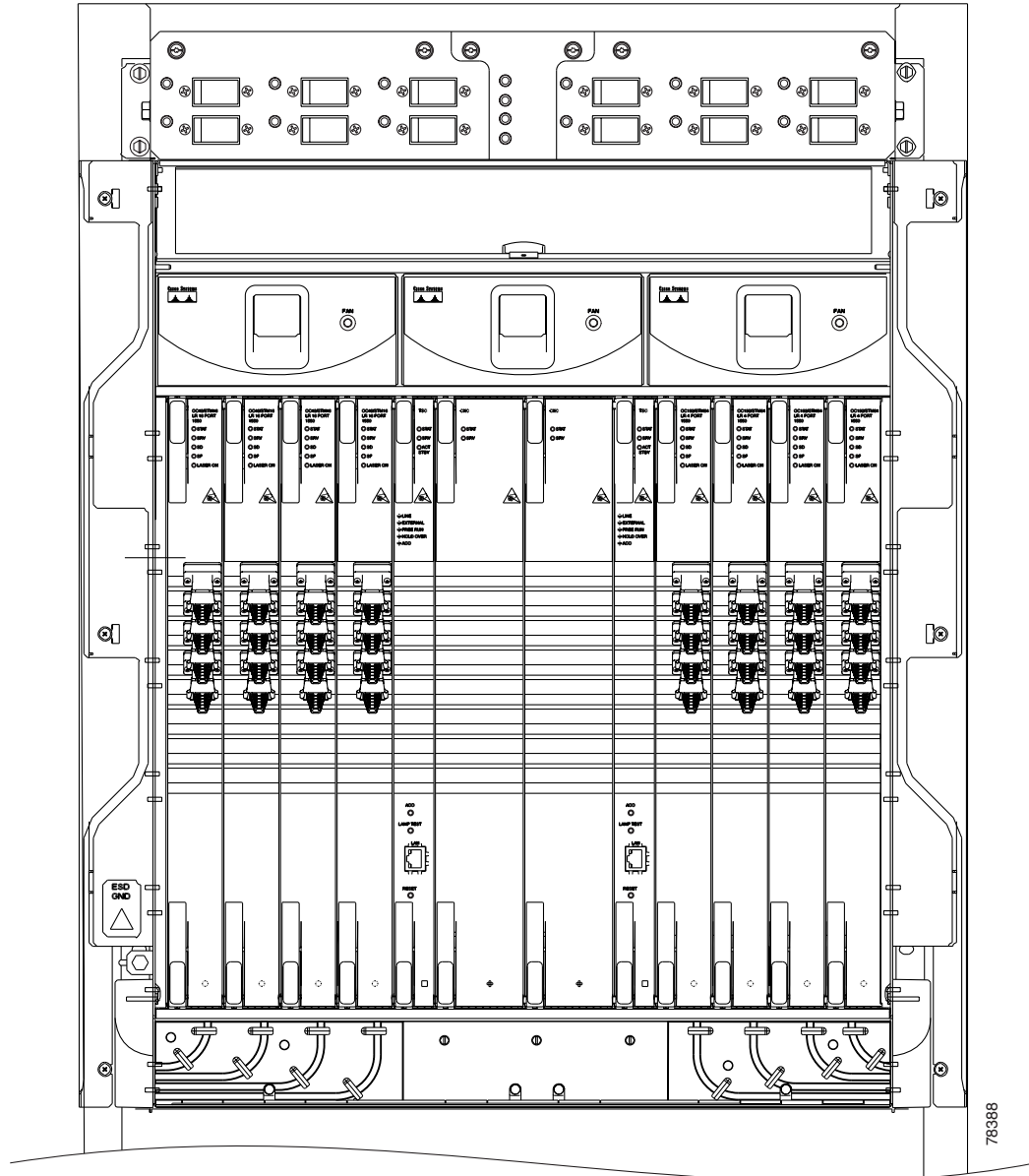
Connector	OGI Pin and Card Port							
	1	1	2	3	4	5	6	7
	—	—	Receive 1	Transmit 1	—	—	—	—
2	1	2	3	4	5	6	7	8
	—	—	Receive 2	Transmit 2	—	—	—	—
3	1	2	3	4	5	6	7	8
	—	—	Receive 3	Transmit 3	—	—	—	—
4	1	2	3	4	5	6	7	8
	—	—	Receive 4	Transmit 4	—	—	—	—

**Note**

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

Figure 16-5 shows all of the cards installed in the shelf and the optical connectors.

Figure 16-5 ONS 15600 SDH with Optical Cards Installed



78388

- 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) STM-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 STM-N card at an adjacent node.
- Step 5** Repeat Steps 2 through 4 for the protect ports on the two STM-N cards you are using, and then for each fiber-optic cable you require.

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

---

## DLP-F176 Route Fiber-Optic Cables

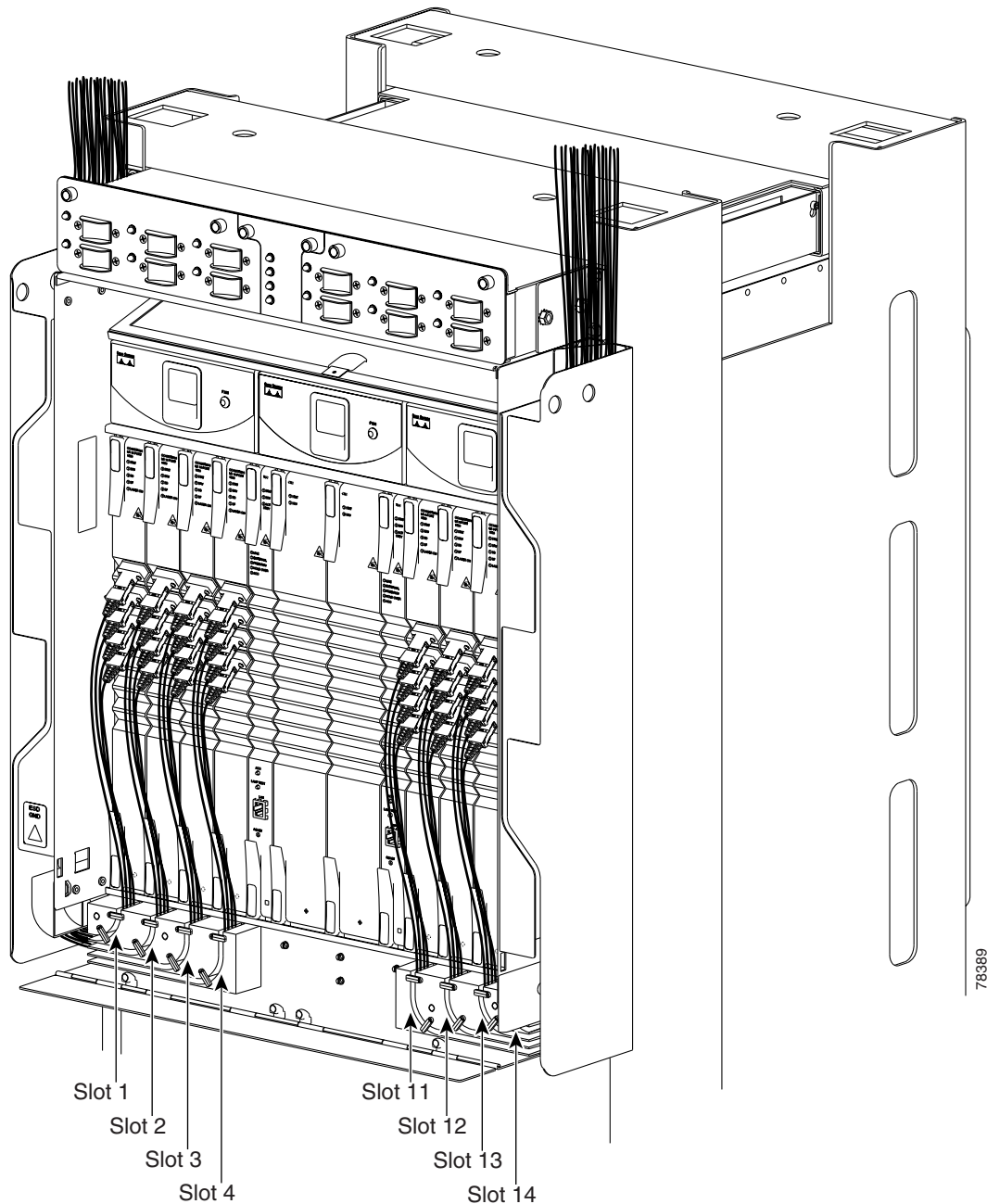
<b>Purpose</b>	This task explains how to route fiber-optic cables away from the card faceplates and onto the side of the shelf.
<b>Tools/Equipment</b>	Tie-wrap (Suggested: Panduit TAK-TAPE TTS-20R0 Nelcro tie-wraps)
<b>Prerequisite Procedures</b>	<a href="#">NTP-F124 Install the Fiber-Optic Cables, page 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 16-6](#).)

Figure 16-6 ONS 15600 SDH 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:
- 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 16-6 on page 16-20). 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.
  - Rotate the corresponding cable latch to the closed position so it secures the fiber cables within the corresponding cable routing channel.
  - Repeat Steps a and b for the fiber cables from each installed STM-N card, working from the innermost cards outward.

- Step 6** If wide CRMs are installed:
- Gently pull the spool flanges toward you until they click open.
  - 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.

---

- Rotate the corresponding cable latch to the closed position so it secures the fiber cables within the corresponding cable routing channel.
  - Repeat Steps a through c for the fiber cables from each installed STM-N card, working from the innermost cards outward. Distribute the cables as evenly as possible on the three storage spools of the CRM.
  - Push any extended spool flanges away from you so that they click closed.
  - 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-F177 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), and the CTC Java archive (JAR) files. JRE 5.0 is required to run Software Release 8.0 (JRE 1.6 for Release 9.2.1 and later). 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 SDH Release 9.1 or Release 9.2.1 software 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 5.0/JRE1.6 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 5.0/JRE 1.6 and reinstall JRE 1.3.1\_2. To run R5.0 and later, uninstall JRE 1.3.1\_2 and reinstall JRE 5.0. Software R8.0 requires JRE 5.0 (JRE 1.6 for Release 9.2.1 and later).


**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 (Windows Vista or Windows 7 for Release 9.2.1 and later)

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 SDH Reference Manual* to find computer requirements needed for small, medium, and large ONS 15600 SDH networks.

- Step 2** Insert the Cisco ONS 15600 SDH Release 9.1 or 9.2.1 software 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 5.0
  - 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 5.0/JRE 1.6 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 need to install a JRE, continue with [Step 12](#).
- Step 11** To install the JRE, complete the following:
- a. In the Java 2 Runtime Environment License Agreement dialog box, view the license agreement and choose one of the following:
    - **I accept the terms of the license agreement**—Accepts the license agreement. Continue with [Step b](#).

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




---

**Note** If JRE 5.0/JRE 1.6 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](#).

---

- Click **Next**.
- 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.
- Click **Next**.
- If you selected Typical, continue with [Step i](#). If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:
  - Java 2 Runtime Environment—(Default) Installs JRE 5.0 with support for European languages.
  - Support for Additional Languages—Adds support for non-European languages.
  - Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

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

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

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

- Click **Next**.
- 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.

---

- Click **Next**.
- 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-F178 Run the CTC Installation Wizard for UNIX

<b>Purpose</b>	This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE, and the CTC JAR files. JRE 5.0 is required to run Software R8.0 (JRE 1.6 for Release 9.2.1 and later). 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 SDH Release 9.1 or Release 9.2.1 software 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 5.0/JRE 1.6 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 5.0/JRE 1.6 and reinstall JRE 1.3.1\_2. To run Software R8.0 and later, uninstall JRE 1.3.1\_2 and reinstall JRE 5.0. Software R8.0 requires JRE 5.0 (JRE 1.6 for Release 9.2.1 and later).



**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 9 or 10



**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 SDH Reference Manual* for computer requirements needed for small, medium, and large ONS 15600 SDH networks.

- Step 2** Change the directory. Type:
- ```
cd /cdrom/cdrom0/
```
- Step 3** From the techdoc600 SDH 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 5.0/JRE 1.6 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/etc`.

- 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 need to install a JRE, continue with [Step 13](#).

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

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



---

**Note** If JRE 5.0/JRE 1.6 is already installed on your computer, the License Agreement page does not appear. You must click Next and then choose Modify to change the JRE installation or Remove to uninstall the JRE. If you choose Modify and click Next, continue with Step e. If you choose Remove and click Next, continue with Step i.

---

- b. Click **Next**.
- c. Choose one of the following:
  - Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
  - Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.
- d. Click **Next**.
- e. If you selected Typical, continue with Step i. If you selected Custom, click the drop-down list for each program feature that you want to install and choose the desired setting. The program features include:

- Java 2 Runtime Environment—(Default) Installs JRE 5.0/JRE 1.6 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-F179 Set Up a Windows PC for Craft Connection to an ONS 15600 SDH 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 SDH when: <ul style="list-style-type: none"> <li>You will connect to one ONS 15600 SDH; if you will connect to multiple ONS 15600 SDHs, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15600 SDH.</li> <li>You need to use non-ONS 15600 SDH applications such as ping and tracert (trace route).</li> </ul>
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F126 Set Up Computer for CTC, page 3-1</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<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 SDH 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 SDH. 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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 SDH 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-F180 Set Up a Solaris Workstation for a Craft Connection to an ONS 15600 SDH

<b>Purpose</b>	This task sets up a Solaris workstation for a craft connection to the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F126 Set Up Computer for CTC, page 3-1</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite
<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 SDH 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 Enable Socks Proxy on Port and External Network Element (ENE) at Provisioning > Network > General > Gateway Settings.

**Step 6** Test the connection:

- a. Start Netscape Navigator.
- b. Enter the Cisco ONS 15600 SDH 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-F181 Log into CTC](#)” task on [page 16-32](#) 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-SDH-IP-address
```

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

```
ping 192.168.1.2
```

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

```
IP address is alive
```



**Note** Skip this step if you checked Enable Socks Proxy on Port and External Network Element (ENE) 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 SDH 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-F181 Log into CTC

<b>Purpose</b>	This task logs into CTC.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F126 Set Up Computer for CTC, page 3-1</a> One of the following procedures: <ul style="list-style-type: none"> <li>• <a href="#">NTP-F127 Set Up CTC Computer for Local Craft Connection to the ONS 15600 SDH, page 3-3</a></li> <li>• <a href="#">NTP-F128 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15600 SDH, 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 SDH, start Mozilla Firefox (PC or UNIX) or Netscape (PC only):

- If you are using a PC, launch Netscape or Mozilla Firefox 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 Mozilla Firefox Web address (URL) field, enter the ONS 15600 SDH IP address. For initial setup, this is the default address: 192.168.1.2. Press **Enter**.



**Note** Netscape or Internet Explorer can be used for IPv4 address and Mozilla Firefox or Netscape can be used for IPv6 address.

To log into CTC using an IPv6 address, you must first log into CTC using an IPv4 or IPv6 address and assign an IPv6 address to the node. Then, use the IPv6 address that you assigned to the node to log into CTC. For more information about configuring IPv6 address, see [“DLP-F185 Provision IP Settings” section on page 16-36](#). Enter the IPv6 address in the address bar of the browser, enclosed in square brackets.



**Note** If you are logging into ONS 15600 SDH 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 SDH Troubleshooting Guide*.

**Step 3** If a Java Plug-in Security Warning dialog box appears, complete the [“DLP-F283 Install Public-Key Security Certificate” task on page 17-74](#) 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 <sup>1</sup>, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15600 SDH, this process can take several minutes. After the download, a warning message window appears ([Figure 16-7](#)).

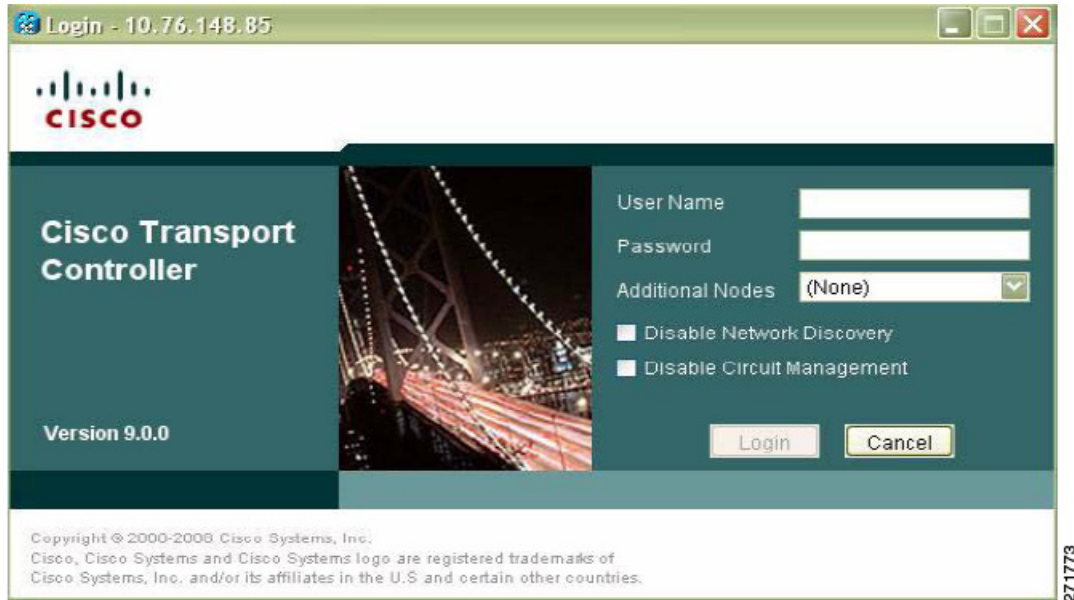
**Figure 16-7** Warning Message Window



**Step 4** Click OK. The CTC Login dialog box appears ([Figure 16-8](#)).

1.

Figure 16-8 Logging into CTC



- Step 5** 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 SDH. 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 SDH users and assign security, go to the “[NTP-F132 Create Users and Assign Security](#)” procedure on page 4-3. For additional information, refer to the *Cisco ONS 15600 SDH Reference Manual*.

- Step 6** Each time you log into an ONS 15600 SDH, you can select the following login options:
- **Additional Nodes**—Displays a list of login node groups. To create a login node group or add additional groups, see the “[DLP-F307 Create Login Node Groups](#)” task on page 18-9.
  - **Disable Network Discovery**—Check this box to view only the ONS 15600 SDH (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.  
If you keep **Disable Network Discovery** unchecked, CTC attempts to upgrade the CTC software by downloading more recent versions of the JAR files it finds during the network discovery. Click **Yes** to allow CTC to download the newer JAR files, or **No** to prevent CTC from downloading the JAR files.
  - **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 7** 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 SDH. If you need to turn up a shelf for the first time, go to [Chapter 4, “Turn Up a Node.”](#) If login problems occur, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.

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

---

## DLP-F183 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-F181 Log into CTC, page 16-32</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

---

**Step 1** 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-F184 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-F181 Log into CTC, page 16-32</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-F185 Provision IP Settings

<b>Purpose</b>	This task provisions IP settings, which include the IP address, IP address version, default router, Dynamic Host Configuration Protocol (DHCP) access, firewall access, and SOCKS proxy server settings for an ONS 15600 SDH node.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-32</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.

**Caution**

Verify that any IPv4 or IPv6 addresses assigned to the node are unique in the network. Duplicate IP addresses in the same network cause loss of visibility.

**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:

- Node Address—Type the IP address assigned to the ONS 15600 SDH node.
- Default Router— If the ONS 15600 SDH 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 SDH cannot directly access. This field is ignored if any of the following are true:
  - The ONS 15600 SDH is not connected to a LAN.
  - SOCKS proxy server is enabled and the ONS 15600 SDH is provisioned as an end network element (ENE).
  - Open Shortcut Path First (OSPF) is enabled on both the ONS 15600 SDH and the LAN where the ONS 15600 SDH is connected.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IPv4 address and IPv6 address (if enabled) from being displayed in CTC (IP Address field, information area) to users with Provisioning, Maintenance, or Retrieve security levels. If the IP address is not suppressed, both the IPv4 address and IPv6 addresses are shown in the IP Address field.
- IPv6 Configuration—Allows provisioning of IPv6 addresses. After you provision an IPv6 address, you can access the device using the IPv6 address. Configure these settings only if you want to enable IPv6 on the node. IPv6 cannot be configured using the LCD push buttons.
  - Enable IPv6—Select this check box to assign an IPv6 address to the node. The IPv6 Address, Prefix Length, and IPv6 Default Router fields are enabled only if this check box is selected. The check box is disabled by default.

**Note**

If TCC2P cards are installed, dual IPv4 addressing through secure mode is available for IPv4 only. If IPv6 is enabled on ONS 15600 with TCC2P in secure mode, IPv6 address support applies to the backplane LAN port only. There is no IPv6 address for the front TCC2P TCP/IP (LAN) port. However, when the TCC2P card is in normal mode (repeater mode), the IPv6 address support applies to both the backplane LAN port as well as the TCC2P TCP/IP (LAN) port.

**Note**

IPv6 address can be enabled only when 'Enable SOCKS Proxy on Port' checkbox is enabled. For IPv6 connectivity, once the SOCKS Proxy is enabled, the ONS 15600 node can be configured as 'External Network Element (ENE)' or 'Gateway Network Element (GNE)' or 'SOCKS proxy only' by enabling the suitable radio button.

**Note**

By default, when IPv6 is enabled, the node processes both IPv4 and IPv6 packets on the LAN interface. If you want the node to process only IPv6 packets, you need to disable IPv4 on the node. For more information, see [DLP-F332 Change Node Access and PM Clearing Privilege, page 18-31](#)

- IPv6 Address—Enter the IPv6 address that you want to assign to the node. This IP address is the global unicast IPv6 address. This field is disabled if the Enable IPv6 check box is not selected.
- Prefix Length—Enter the prefix length of the IPv6 address. This field is disabled if the Enable IPv6 check box is not selected. The valid range for Prefix Length is 0 - 128.
- IPv6 Default Router—Enter the IPv6 address of the default router of the IPv6 NE. This field is disabled if the Enable IPv6 check box is not selected. This field can be set to 0 or 0::0 or 0:0:0:0:0:0:0:0 if any of the following are true:

The ONS 15600 is not connected to a LAN.

The ONS 15600 is provisioned as an end network element (ENE).

**Note**

ONS platforms use NAT-PT internally to support native IPv6. NAT-PT uses the IPv4 address range 128.x.x.x for packet translation. Do not use this address range when you enable IPv6 feature.

**Note**

You can provision IPv6 in secure or nonsecure mode. To enable secure mode, see [“NTP-F248 Set Up the ONS 15600 in EMS Secure Access”](#) section on page 4-7.

- 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 SDH SOCKS proxy server features, leave this field blank.

**Note**

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

- MAC Address—(Read only) Displays the ONS 15600 SDH IEEE 802 MAC address.
- Net/Subnet Mask Length—If the ONS 15600 SDH 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 15600 SDHs in the same subnet.
- Gateway Settings—Provisions the ONS 15600 SDH 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 SDH Reference Manual*. In SOCKS proxy server networks, the ONS 15600 SDH 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 SDH serves as a proxy for connections between CTC clients and ONS 15600 SDHs that are connected by DCCs to the proxy ONS 15600 SDH. 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 SDH. 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 SDH, the ENE and GNE settings have the same behavior.

- External Network Element (ENE) or Gateway Network Element (GNE)—Choose either of these options when the ONS 15600 SDH is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE/GNE through the TSC TCP/IP (craft) port can manage nodes that have DCC connections to the ENE/GNE. 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 SDH 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 ENE/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 SDH 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-F186 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-F181 Log into CTC, page 16-32</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 15600 SDHs to CTC sessions on one subnet connected by a router to ONS 15600 SDHs residing on another subnet when OSPF is not enabled and the ENE or GNE setting is not checked.</li> <li>• You need to enable multiple CTC sessions among ONS 15600 SDHs 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 SDH 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 “Management Network Connectivity” chapter in the *Cisco ONS 15600 SDH Reference Manual*.

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

## DLP-F187 Set Up or Change Open Shortest Path First Protocol

<b>Purpose</b>	This task enables the OSPF routing protocol to include the ONS 15600 SDH in OSPF-enabled networks.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-32</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 SDH 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 SDH has DCC or LAN interfaces in multiple OSPF areas, at least one ONS 15600 SDH 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 15600 SDHs 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.
- RS-DCC Metric—This value is normally unchanged. It sets a “cost” for sending packets across the regenerator-section DCC (RS-DCC), which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default RS-DCC metric is 100.
- MS-DCC Metric—Sets a cost for sending packets across the MS-DCC. This value should always be lower than the RS-DCC metric. The default MS-DCC 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 SDH OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15600 SDHs 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 SDH 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](#).

- a. Click the **No Authentication** button.
- b. 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.
- c. 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 SDH 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 SDH in the ONS 15600 SDH 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 SDH OSPF area.

---

- a. Under OSPF Area Range Table, click **Create**.
- b. In the Create Area Range dialog box, enter the following:
  - Range Address—Enter the area IP address for the ONS 15600 SDHs that reside within the OSPF area. For example, if the ONS 15600 SDH 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 15600 SDHs. 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 SDH 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 SDH 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 SDH 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 SDH 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-F188 Set Up External or Line Timing

<b>Purpose</b>	This task defines the SDH timing source for the ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">NTP-F131 Verify Card Installation, page 4-2</a> <a href="#">DLP-F181 Log into CTC, page 16-32</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 SDH 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 SDH derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an STM-N card that is optically connected to the timing node. A third option, **Mixed**, allows you to set external and line timing references. (Because **Mixed** timing might cause timing loops, Cisco does not recommend its use. Use this mode with care.)
  - **Revertive**—If this check box is selected, the ONS 15600 SDH reverts to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
  - **Reversion Time**—If **Revertive** is checked, indicate the amount of time the ONS 15600 SDH will wait before reverting 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.
    - Timing Mode is set to **External**—Your options are BITS1, BITS2, and Internal Clock.
    - Timing Mode is set to **Line**—Your options are the node’s STM-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.
    - Timing Mode is set to **Mixed**—Both BITS and STM-N cards are available, allowing you to set a mixture of external BITS and STM-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 STM-N card used to set the timing. If Timing Mode is set to Line, you can choose an STM-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**.
- 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.

- Step 6** In the BITS In area, complete the following information:
- Facility Type—Choose **E1, 2 MHz, 64KHz+8KHz, or DS1** depending on the signal supported in your market. E1, 2 MHz, 64KHz+8KHz, and DS1 are physical signal modes used to transmit the external clock (from a global positioning satellite [GPS], for example) to BITS.
  - 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 **unlocked** 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 **locked**.
- Step 7** If the BITS In State for BITS-1 and BITS-2 is set to **locked**, continue with [Step 8](#). If the BITS In State is set to **unlocked** for either BITS-1 or BITS-2, complete the following information:
- Coding—Choose the coding used by your BITS reference, either **HDB3** or **AMI** (alternate mark inversion). HDB3 coding is only for the E1 facility type. If you selected 2 MHz, the coding option is disabled.
  - Framing—Choose the framing used by your BITS reference, either **unframed, FAS, FAS + CAS, FAS + CRC, or FAS + CAS + CRC**. FAS + CAS + CRC is only for the E1 facility type. If you selected 2 MHz or 64KHz+8KHz, the framing option is disabled.
  - Sync Messaging—Select the check box to enable synchronization status messages (SSMs). SSM is used to deliver clock quality. The SSMs supported in SDH are G811, STU, G812T, G812L, SETS, and DUS (ordered from high quality to low quality).
  - Admin SSM—If the Sync Messaging check box is not checked, you can choose the SSM from the drop-down list: G811, STU, G812T, G812L, SETS, or DUS (ordered from high quality to low quality). If you selected DS1, the Admin SSM option is disabled.
  - Sa bit—Choose one of 5 Sa bits (**Sa4, Sa5, Sa6, Sa7, or Sa8**). The Sa bit setting is only for the E1 facility type. The Sa bit transmits the SSM message. If you selected 2 MHz, the Sa bit option is disabled.
  - Cable Type—Choose **75 ohm** or **120 ohm**. The cable type is fixed at 100 ohm for DS1.
- Step 8** In the BITS Out area, complete the following information, as needed:
- Facility Type—Choose **E1, 2 MHz, 64KHz+8KHz, or DS1** depending on the signal supported in your market.
  - 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 **unlocked**, 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 **locked**.
- Step 9** If the BITS Out State is set to **locked**, continue with [Step 10](#). If BITS Out State is set to **unlocked**, complete the following information:
- Coding—Choose the coding used by your BITS reference, either **HDB3** or **AMI**. If you selected 2 MHz, the coding option is disabled.
  - Framing—Choose the framing used by your BITS reference. If the facility type is set to DS1, the options are either **ESF** or **SF (D4)**. If the facility type is set to E1, the options are **Unframed, FAS, FAS+CAS, FAS+CRC, or FAS+CAS+CRC**. If you selected 2 MHz or 64KHz+8KHz, the framing option is disabled.

- AIS Threshold—Sets the quality level at which a node sends an alarm indication signal (AIS) from the BITS-1 Out and BITS-2 Out connectors. When a node times at or below the AIS threshold quality, an AIS is raised. (The AIS threshold is used when SSM is disabled or framing is set to unframed, FAS, or FAS + CAS.)
- Sa bit—Choose one of 5 Sa bits (**Sa4**, **Sa5**, **Sa6**, **Sa7**, or **Sa8**). The Sa bit transmits the SSM message. If you selected 2 MHz, the Sa bit option is disabled.
- Cable Type—Choose **75 ohm** or **120 ohm**.

**Step 10** Click **Apply**.



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

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

## DLP-F189 Set Up Internal Timing

<b>Purpose</b>	This task sets up internal timing (Stratum 3E) for an ONS 15600 SDH 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-F181 Log into CTC, page 16-32</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 synchronous equipment (SETS) timing, and is not intended for permanent use. All ONS 15600 SDH nodes should be timed to a SETS 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—Choose **External**.
- Revertive—Not applicable for internal timing; the default setting (checked) is sufficient.
- Reversion Time—Not applicable; leave unchanged. For internal timing, the default setting (5 minutes) is sufficient.

**Step 3** In the Reference Lists section, enter the following information:

- NE Reference
  - 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 **Provisioning > Timing > BITS Facilities** tabs.
- Step 6** In the BITS Facilities area, enter the following information:
- Facility Type—Choose **E1, 2 MHz, 64KHz+8KHz, or DS1** depending on the signal supported in your market. E1, 2 MHz, 64KHz+8KHz, and DS1 are physical signal modes used to transmit the external clock (from a GPS, for example) to BITS.
  - BITS In State—Set BITS-1 and BITS-2 to **locked**.
  - BITS Out State—Set BITS-1 and BITS-2 to **locked**.
  - Coding—Not relevant for internal timing; the default (HDB3) is sufficient.
  - Framing—Not relevant for internal timing; the default is sufficient.
  - Sync Messaging—The box is checked automatically. SSM is used to deliver clock quality. The SSMs supported in SDH are G811, STU, G812T, G812L, SETS, and DUS (ordered from high quality to low quality). If you selected 2 MHz, the SSM option is disabled.
  - AIS Threshold—Not relevant for internal timing.
  - Sa bit—Not applicable for internal timing.
- Step 7** Click **Apply**.
- Step 8** Log into a node that will be timed from the node set up in Steps 1 through 7 (the internally timed node).
- Step 9** Click the **Provisioning > Timing > General** tabs.
- Step 10** In the General Timing area, enter the same information as entered in [Step 2](#), except set Timing Mode to **Line**.
- Step 11** In the Reference Lists area, enter the same information as entered in [Step 3](#), except set NE Reference as follows:
- Ref1—Set to the STM-N trunk card with the closest connection to the internally timed node.
  - Ref2—Set to the STM-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 12** Click **Apply**.
- Step 13** Repeat Steps 9 through 12 at each node that will be timed by the internally timed node.
- Step 14** Return to your originating procedure (NTP).
- 

## DLP-F190 Create a New User on a Single Node

<b>Purpose</b>	This task creates a new user for one ONS 15600 SDH.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-32</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 Transaction Language One (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 length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #, %) characters, where at least two characters are nonalphabetic 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 SDH 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-F206 Modify Users and Change Security” procedure on page 11-6](#).

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

## DLP-F191 Create a New User on Multiple Nodes

<b>Purpose</b>	This task adds a new user to multiple ONS 15600 SDHs.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-32</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 length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of 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 TL1 compatibility, the password must be six to ten 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 SDH 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-F206 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-F192 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-F181 Log into CTC</a> , page 16-32; 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-F288 Disable Alarm Filtering](#)” task on [page 17-80](#) for instructions.
  - Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*.
- 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 SDH 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-F193 SNCP Protection Switching Test

<b>Purpose</b>	This task verifies that an SNCP span is switching correctly.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , <a href="#">page 16-32</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 SNCP traffic and choose **Circuits**.

The Circuits on Span dialog box displays the SNCP 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 SNCP 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 SNCP 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 SNCP circuits is CLEAR.

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

## DLP-F194 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

**Prerequisite Procedures** [DLP-F181 Log into CTC, page 16-32](#)

Perform this task during one of the following procedures:

[DLP-F291 Verify MS-SPRing Extension Byte Mapping, page 17-82](#)

[DLP-F292 Single Shelf Control Card Switch Test, page 17-82](#)

Circuit creation procedures in [Chapter 6, “Create Circuits”](#)

<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 virtual container (VC) from the VC drop-down list. VCs do not appear if they are already in use by other circuits.




---

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

---

- Step 5** If you need to create a secondary source, for example, an SNCP bridge/selector circuit entry point in a multivendor SNCP, 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 VC from the VC drop-down list. VCs do not appear if they are already in use by other circuits.




---

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

---

- Step 11** If you need to create a secondary destination, for example, an SNCP bridge/selector circuit entry point in a multivendor SNCP, 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-F195 View Alarms

<b>Purpose</b>	This task displays ONS 15600 SDH alarms at the card, node, or network level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC</a> , page 16-32
<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 16-9](#) shows the Alarms window.

**Figure 16-9** Viewing Alarms in CTC Node View

The screenshot shows the CTC Node View for a CXC66 node. The rack contains several cards: ASAP (Slot 1), STA (Slots 3, 4), SSKC (Slot 8), TSC (Slot 10), and STM64 (Slots 11, 12, 13, 14). The Alarms table is displayed below the rack view.

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Wavelength	Path Width	Sev	ST	SA	Cc
944	944	✓	08/24/06 20:38:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-RS-SES
943	943	✓	08/24/06 20:38:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-RS-ES
942	942	✓	08/24/06 20:38:19 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-RS-OFS
941	941	✓	08/24/06 20:38:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-RS-SES
940	940	✓	08/24/06 20:38:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-RS-ES
939	939	✓	08/24/06 20:38:19 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-RS-OFS
938	938	✓	08/24/06 20:38:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-RS-SES
937	937	✓	08/24/06 20:38:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-RS-ES
936	936	✓	08/24/06 20:38:19 PDT	FAC-11-2	STM64_4...	11	2	1529.55 nm		NA	T		T-RS-OFS
935	935	✓	08/24/06 20:30:02 PDT	FAC-11-4	STM64_4...	11	4	1529.55 nm		NA	T		T-MS-UAES
934	934	✓	08/24/06 20:30:02 PDT	FAC-11-3	STM64_4...	11	3	1529.55 nm		NA	T		T-MS-UAES

Buttons at the bottom: Synchronize, Filter..., Delete Cleared Alarms,  AutoDelete Cleared Alarms, Help.

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

## DLP-F196 View Alarm History

<b>Purpose</b>	This task displays past cleared and uncleared ONS 15600 SDH alarms at the card, node, or network level.
<b>Tools/Equipment</b>	None
<b>Prerequisite Procedures</b>	<a href="#">DLP-F181 Log into CTC, page 16-32</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:

- a. 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.
- b. Click the **History > Shelf** tabs if you want to retrieve all available alarms for the node.
- c. 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 SDH 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 SDH 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.

Alarms have specifically numbered VC object identifiers based upon the object TL1 access identifiers (AIDs). The port-based alarm numbering scheme is shown in Table 16-4. Figure 16-10 on page 16-54 shows an example of viewing all alarms reported for the current session in CTC.

**Table 16-4** Port-Based Alarm Numbering Scheme

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

**Figure 16-10** Viewing All Alarms Reported for Current Session

The screenshot shows the CTC interface for a Cisco Transport Controller (CXC66). The top left pane displays system information: Node Addr, Booted (8/24/06 2:51 AM), User (CISCO15), Authority (Superuser), SW Version (08.00), and Defaults (Factory Defaults). The main pane shows a rack of equipment with slots 1-14. Slots 3, 4, 11, 12, 13, and 14 are highlighted in yellow, indicating active or alarmed components. The bottom pane shows a table of alarms.

Session	Date	Object	Eqpt Type	Slot	Port	Path Width	Sev	ST	SA	Cond
Shelf	08/24/06 20:45:02 PDT	FAC-11-2	STM64_4...	11	2		NA	T	T-M5-UAS	PM
	08/24/06 20:45:02 PDT	FAC-11-3	STM64_4...	11	3		NA	T	T-M5-UAS	PM
	08/24/06 20:45:02 PDT	FAC-11-4	STM64_4...	11	4		NA	T	T-M5-UAS	PM
	08/24/06 20:45:01 PDT	FAC-11-2	STM64_4...	11	2		NA	T	T-RS-EB	PM
	08/24/06 20:45:01 PDT	FAC-11-3	STM64_4...	11	3		NA	T	T-RS-EB	PM
	08/24/06 20:45:01 PDT	FAC-11-4	STM64_4...	11	4		NA	T	T-RS-EB	PM
	08/24/06 20:45:00 PDT	FAC-3-1	STM16_16	3	1		NA	T	T-OPRN-HWT	PM
	08/24/06 20:45:00 PDT	FAC-14-13	STM16_16	14	13		NA	T	T-OPRN-HWT	PM
	08/24/06 20:45:00 PDT	FAC-11-1	STM64_4...	11	1		NA	T	T-OPTN-LWT	PM
	08/24/06 20:45:00 PDT	FAC-11-2	STM64_4...	11	2		NA	T	T-OPRN-LWT	PM

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

---

## DLP-F197 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-F181 Log into CTC, page 16-32</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:

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

**Step 3** To view network-level conditions:

- a. From the View menu, choose **Go to Network View**.
- b. 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:

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

**Step 5** Click **Retrieve**. (See [Figure 16-11](#).)

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 16-11 Viewing Retrieved Fault Conditions in the Conditions Window

Date	Object	Eqpt Type	Slot	Port	Wavelength	Path Width	Sev	SA	Cond
08/24/06 03:20:17 PDT	SYSTEM						NR		DBOSYNC
08/24/06 03:11:08 PDT	BITS-2						NR		SYNC-FREQ
08/24/06 03:11:08 PDT	BITS-1						NR		SYNC-FREQ
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		CONTBUS-CLK-A
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		CTNEQPT-PB-A
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		CONTBUS-IO-A
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				NR		PWR-FAIL-B
08/24/06 03:07:56 PDT	SLOT-13	STM64_4	13				MN		EQPT-HITEMP
08/24/06 03:07:53 PDT	SLOT-14	STM16_16	14				NR		CONTBUS-CLK-A
08/24/06 03:07:53 PDT	SLOT-14	STM16_16	14				NR		CTNEQPT-PB-A
08/24/06 03:07:53 PDT	SLOT-14	STM16_16	14				NR		CONTBUS-IO-A

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

## DLP-F198 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-F181 Log into CTC, page 16-32</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 Time Zone** check box.



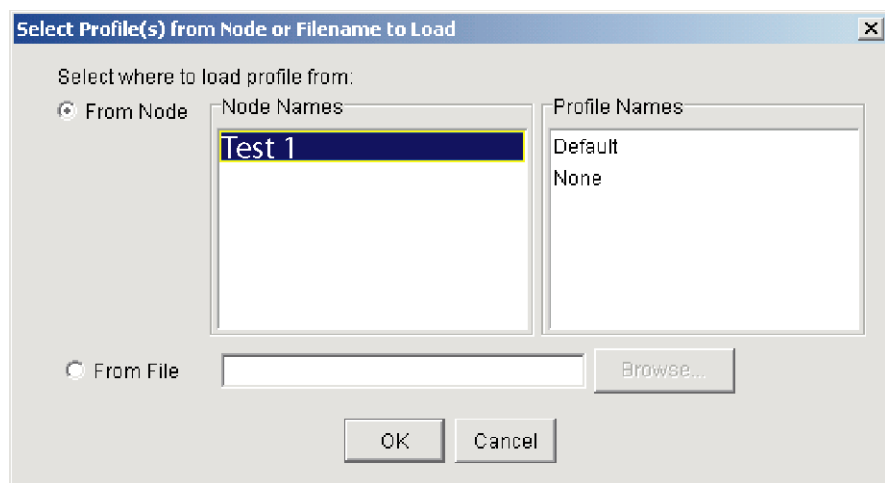
- Step 3** Click **Apply** and **OK**.
- Step 4** Return to your originating procedure (NTP).

## DLP-F199 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-F181 Log into CTC, page 16-32</a>
<b>Required/As Needed</b>	As needed
<b>Onsite/Remote</b>	Onsite or remote
<b>Security Level</b>	Provisioning or higher

- Step 1** 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 16-12](#)).

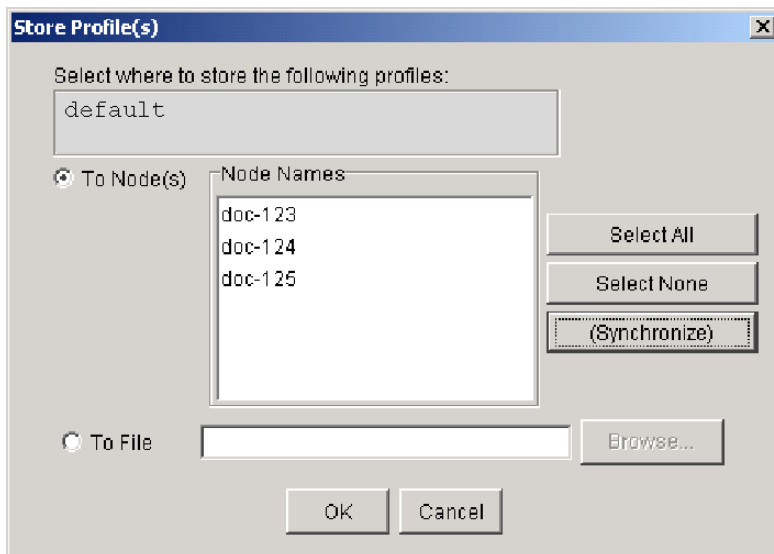
**Figure 16-12** Select Profile(s) from Node or Filename to Load Dialog Box



- 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.  
In the profile editing shortcut menu, any profile other than Inherited can be cloned.
- 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 16-13](#)) 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 16-13** 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-F200 Apply Alarm Profiles for Ports and Cards”](#) task on page 17-1.
- Step 15** As needed, complete the [“DLP-F201 Apply Alarm Profiles to Cards and Nodes”](#) task on page 17-3.
- Step 16** Return to your originating procedure (NTP).
-

