CHAPTER 17

# DLPs C1 to C99

## DLP-C1 Unpack and Verify the Shelf Assembly

| | |
|---|---|
| **Purpose** | This task removes the ONS 15310-CL or ONS 15310-MA shelf assembly from the package. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** When you receive the system equipment at the installation site, open the top of the box. The Cisco Systems logo designates the top of the box.

**Step 2** Remove the foam inserts from the box. The box contains the shelf assembly (wrapped in plastic) and a smaller box containing items needed for installation.

**Step 3** To remove the shelf, grasp both sides of the shelf and slowly lift it out of the box.

**Step 4** Open the smaller box containing installation materials, and verify that you have all items listed in the "Included Materials" section on page 1-3 (ONS 15310-CL) or "Included Materials" section on page 2-3 (ONS 15310-MA).

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

## DLP-C2 Inspect the Shelf Assembly

| | |
|---|---|
| **Purpose** | This task verifies that all parts of the ONS 15310-CL or ONS 15310-ma shelf assembly are in good condition. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C1 Unpack and Verify the Shelf Assembly, page 17-1 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Verify the following:

- Pins are not bent or broken
- Frame is not bent

**Step 2** If the pins are bent or broken, or the frame is bent, call your Cisco sales engineer for a replacement.

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

## DLP-C3 Mount the ONS 15310-CL in a Rack

| | |
|---|---|
| **Purpose** | This task allows one person to mount the shelf assembly in a rack. |
| **Tools/Equipment** | Two sets of #12-24 mounting screws<br>#2 Phillips screwdriver<br>Fuse and alarm panel, if not installed (DC power only) |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Note** Mounting the ONS 15310-CL in a rack requires a minimum of 2.75 inches of vertical rack space (plus 1 inch for air flow). To ensure the mounting is secure, use two #12-24 mounting screws for each side of the shelf assembly.

**Step 1** If you will install DC power, verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to manufacturer instructions. A fuse panel with two fuses per shelf (amperage depends on the fuse and alarm panel you are using) is required for Power A and B feeds.

**Step 2** Install the appropriate bracket for the desired rack size (either 19 or 23 inches). Screw two screws through the bracket into the rack and 4 screws to adhere the bracket to the ONS 15310-CL chassis Figure 17-1 shows the mounting bracket orientations for a 19-inch rack.

*Figure 17-1 Mounting Brackets (19-Inch Orientation)*

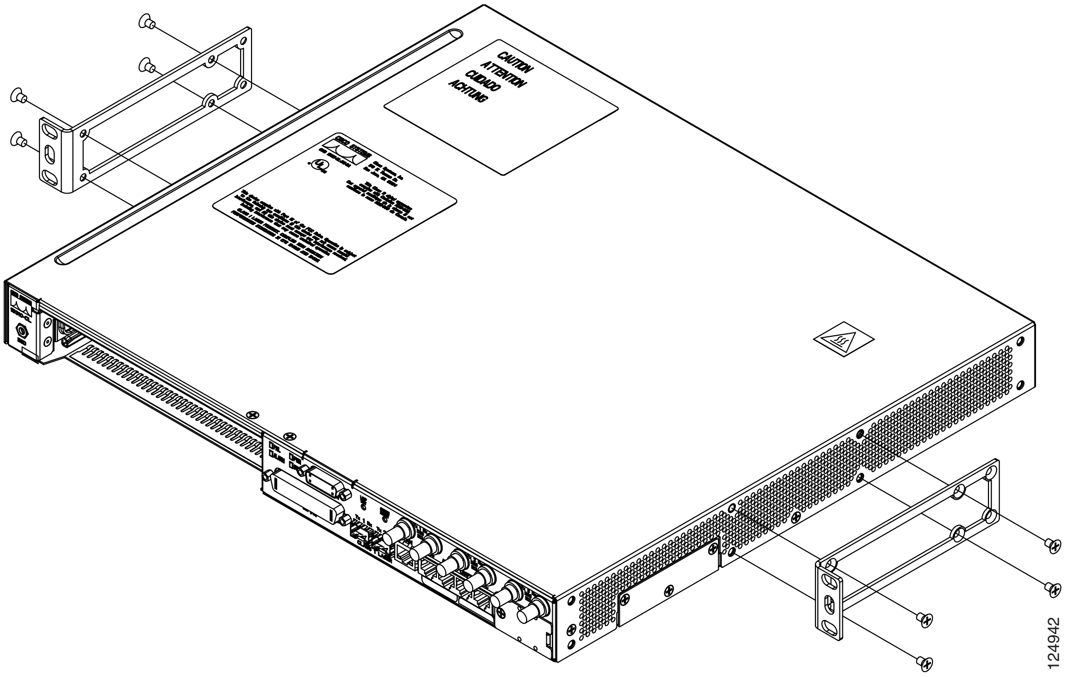
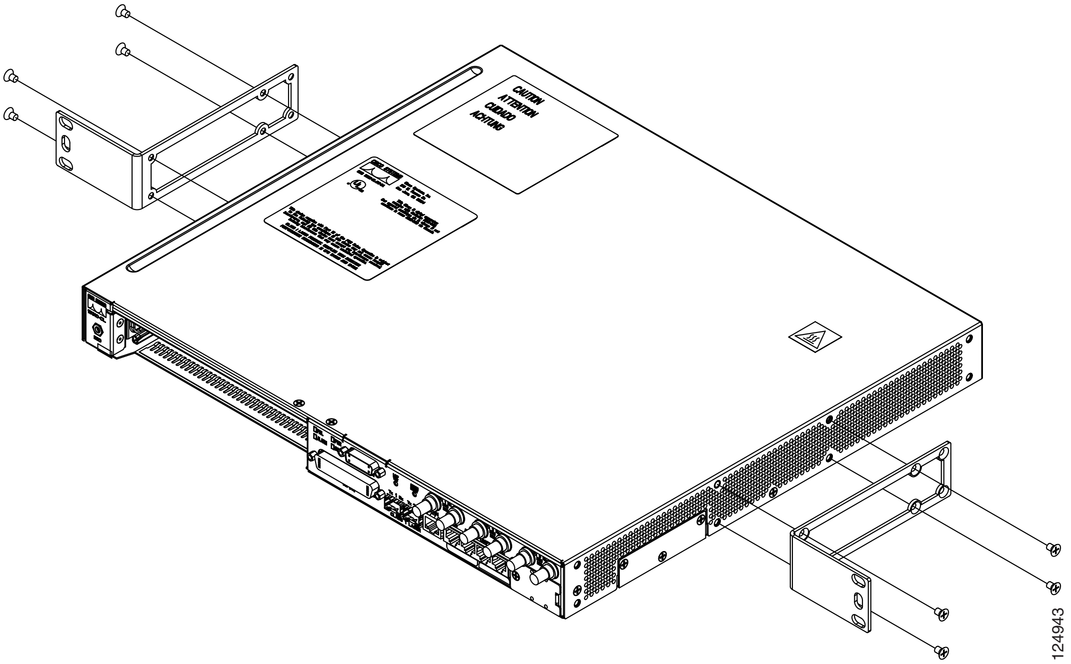


Figure 17-2 shows the mounting bracket orientations for a 23-inch rack. The brackets are installed in the same mounting holes.

*Figure 17-2 Mounting Brackets (23-Inch Orientation)*



**Step 3** Lift the shelf assembly to the desired rack position and set it on the set screws.

**Step 4** Align the screw holes on the mounting ears with the mounting holes in the rack.

**Step 5** Using the Phillips screwdriver, install one mounting screw in each side of the assembly.

**Step 6** When the shelf assembly is secured to the rack, install the remaining mounting screws.

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

# DLP-C4 Mount Multiple ONS 15310-CL Shelf Assemblies in a Rack

| | |
|---|---|
| **Purpose** | This task installs multiple ONS 15310-CL shelf assemblies in a rack. |
| **Tools/Equipment** | #2 Phillips screwdriver<br>Medium slot-head screwdriver<br>Small slot-head screwdriver |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** If DC power will be applied, verify that the proper fuse and alarm panel has been installed in the top mounting space. If a fuse and alarm panel is not present, you must install one according to manufacturer instructions. A fuse panel with two 5-amp (minimum) fuses per shelf is required for Power A and B feeds.

**Caution** Maximum amp rating of the fuse is determined by the rated ampacity of the selected power cable (refer to manufacturer's instructions). The fuse rating should not exceed 20 amps.

**Step 2** Mount the first ONS 15310-CL using the "DLP-C3 Mount the ONS 15310-CL in a Rack" task on page 17-2.

**Note** If you want to install a tie-down bar on the rack, be sure to leave 1 RU spacing between the ONS 15310-CL and any adjacent equipment you plan to install on the rack. This will provide adequate space for the tie-down bar and cabling.

**Step 3** Repeat the task with the remaining ONS 15310-CL nodes.

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

# DLP-C5 Connect the Office Ground to the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task connects ground to the ONS 15310-CL shelf assembly. |
| **Tools/Equipment** | #2 Phillips screwdriver<br>Medium slot-head screwdriver<br>Small slot-head screwdriver<br>Screws<br>Ground cable, #6 AWG, copper conductors, 194°F [90°C])<br>#6 AWG dual-hole, 5/8 in.-spaced grounding lug<br>10-32 screws<br>Crimp tool<br>Wire strippers<br>Wire cutter |
| **Prerequisite Procedures** | DLP-C3 Mount the ONS 15310-CL in a Rack, page 17-2 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Verify that the office ground cable (#6 AWG stranded) is connected to the top of the rack according to local site practice.

**Note** Additional ground cables may be added depending on the local site practice. The ONS 15310-CL is designated for a Common Bonding Network (CBN) only, according to definitions in section 9.3 of GR1089 issue 4.

**Step 2** Ensure to remove paint and other nonconductive coatings from the surfaces between the shelf ground and the rack frame ground posts. Clean the mating surfaces and apply an appropriate antioxidant compound to the bare conductors.

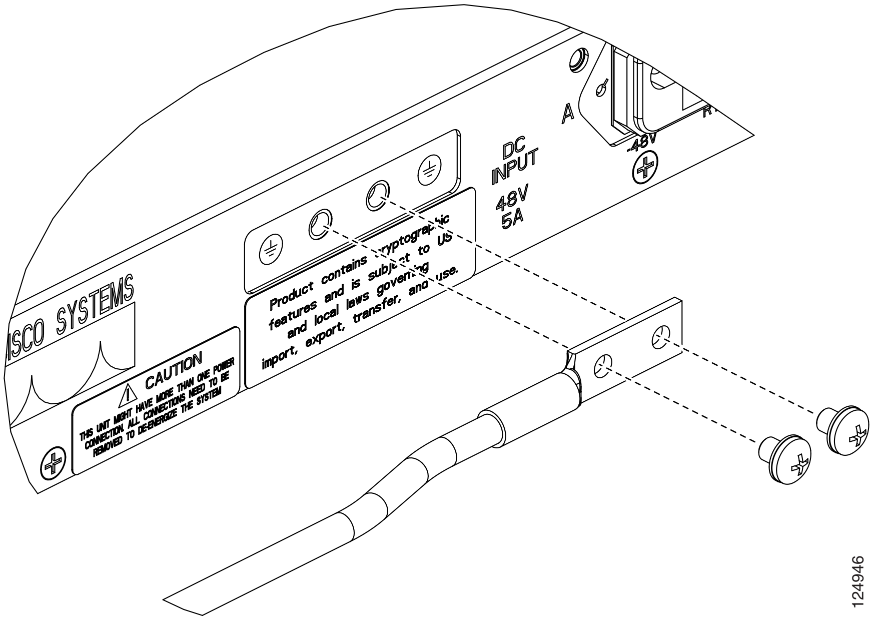
**Step 3** Using the 10-32 screws that came with the ship kit, attach one end of the shelf ground cable (#6 AWG) to the ground connection point located on the center of the rear panel as you face the ONS 15310-CL.

**Step 4** Using a wire stripper, strip 0.875 inches (2.22 cm) from the end of a #6 AWG ground cable.

**Step 5** Crimp the two-hole lug to the #6 AWG ground cable.

**Step 6** Line up the holes on the lug with the holes on the ground connection point, located at the center of the rear panel as you face the ONS 15310-CL. Use two 10-32 screws to attach the lug to the ground connection point (Figure 17-3).

*Figure 17-3 Installing the Chassis Ground*


DC
INPUT
48V
5A
A
-48V
ISCO SYSTEMS
CAUTION
THIS UNIT MIGHT HAVE MORE THAN ONE POWER CONNECTION. ALL CONNECTIONS NEED TO BE REMOVED TO DE-ENERGIZE THE SYSTEM
Product contains cryptographic features and is subject to US and local laws governing import, export, transfer, and use.
124946

**Step 7** Attach the other end of the shelf ground cable to the rack.

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

## DLP-C6 Connect AC Office Power to the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task connects AC power to the ONS 15310-CL shelf. |
| **Tools/Equipment** | #2 Phillips screwdriver<br>Medium slot-head screwdriver<br>Small slot-head screwdriver<br>AC power cord<br>Strain-relief bracket |
| **Prerequisite Procedures** | DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Warning** **Read the installation instructions before connecting the system to the power source.** Statement 1004

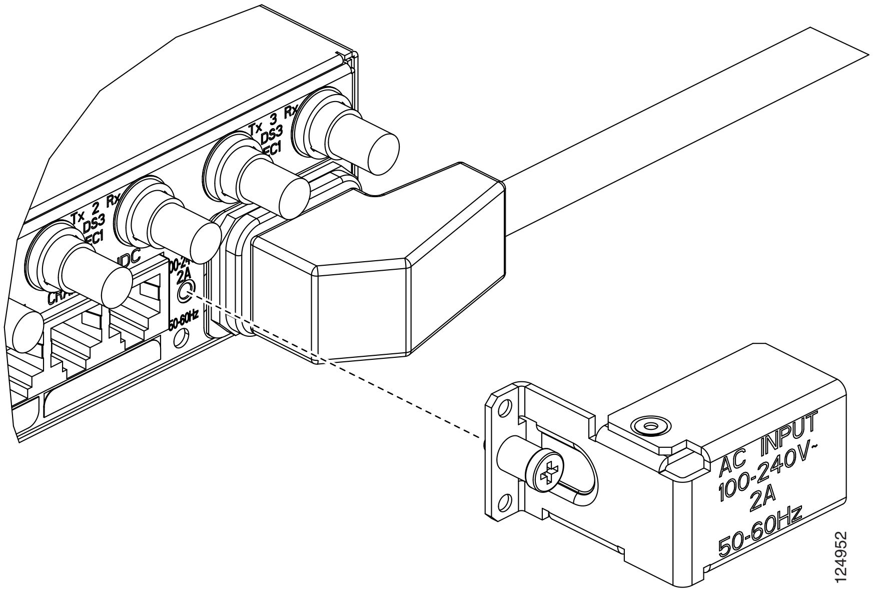
**Warning** **Use copper conductors only.** Statement 1025

**Note** If you encounter problems with the power supply, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

**Step 1** Plug the AC power cord into the AC power connection on the front of the ONS 15310-CL.

**Step 2** Install the strain-relief bracket over the power connector by using a Phillips screwdriver to screw the screw on the left of the bracket (Figure 17-4).

***Figure 17-4 Installed AC Power and Strain Relief Bracket***



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

# DLP-C7 Connect DC Office Power to the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task connects DC power to the ONS 15310-CL shelf. |
| **Tools/Equipment** | #2 Phillips screwdriver<br>Medium slot-head screwdriver<br>Small slot-head screwdriver<br>Wire wrapper<br>Wire cutters<br>Wire strippers<br>Hand crimper (Molex P/N 63811-1100)<br>Fuse and alarm panel<br>Connector housing (Cisco P/N 29-5116-01 or Molex P/N 50-29-1608)<br>Connector terminal (Cisco P/N 27-1919-01 or Molex P/N 18-12-1602))<br>Power cable (from fuse and alarm panel to assembly), 14 AWG, stranded (41 strands, 0.010 in.)<br>Listed pressure terminal connectors such as ring and fork types; 14 AWG, stranded (41 strands, 0.010 in.) |
| **Prerequisite Procedures** | DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**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 in this manner, but always keep them clean and free of contaminants.

**Note** If you encounter problems with the power supply, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

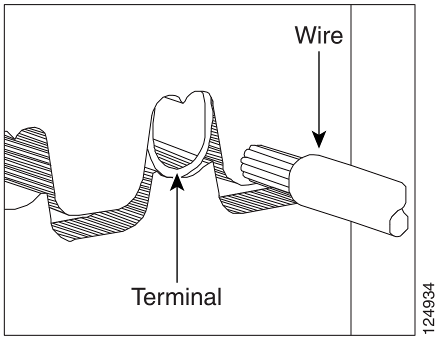
**Step 1** Connect the office power according to the fuse panel engineering specifications.

**Step 2** Measure and cut the cables as needed to reach the ONS 15310-CL from the fuse panel.

**Step 3** Strip away 0.2 inches of insulation at one end of two 14 AWG wires.

Figure 17-5 shows the stripped 14 AWG wires.

*Figure 17-5 Insulation Stripped from Wires*



**Step 4** Open the Molex crimping tool by squeezing the handles together. The ratchet mechanism will release the handles and the tool will open.

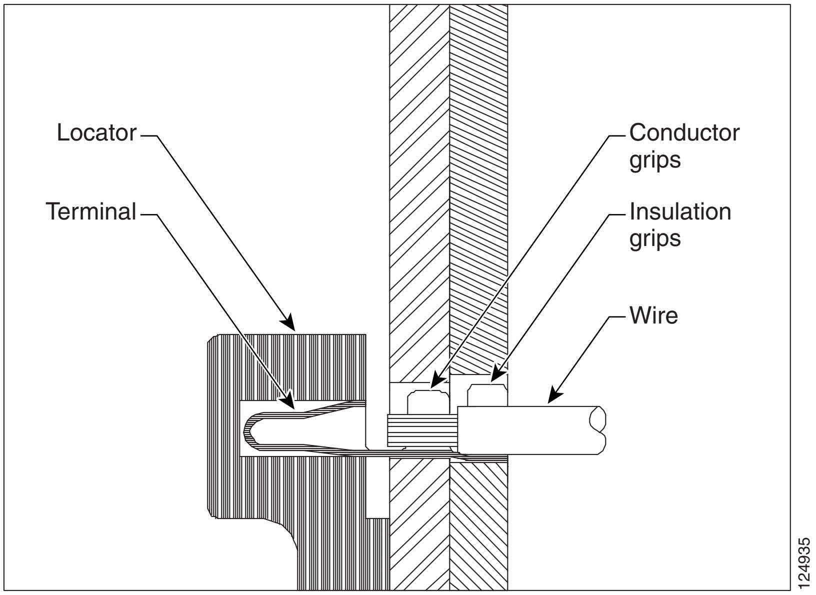
**Step 5** Place the terminal into the correct die profile A until it is stopped by the locator.

**Step 6** Partially close the tool until the terminal is held in place.

**Step 7** Place a wire into the terminal and align the wire with the conductor and insulation grips.

Figure 17-6 shows the location of conductor and insulation grips.

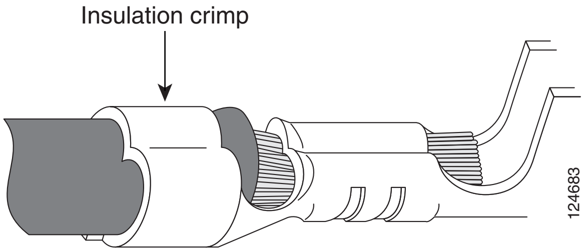
*Figure 17-6 Crimping Tool*



**Step 8** Close the tool until the ratchet releases.

Figure 17-7 shows the terminal crimped to the power cable.

*Figure 17-7 Terminal Connector Crimped to the Power Cable*



**Step 9** Carefully remove the crimped terminal.

**Step 10** Insert crimped terminal into outside holes of the supplied 3-pin receptacle. Leave the center hole empty. The D-shaped terminal is for BAT (–48V). The O-shaped terminal on the other side of the connector is for RET.

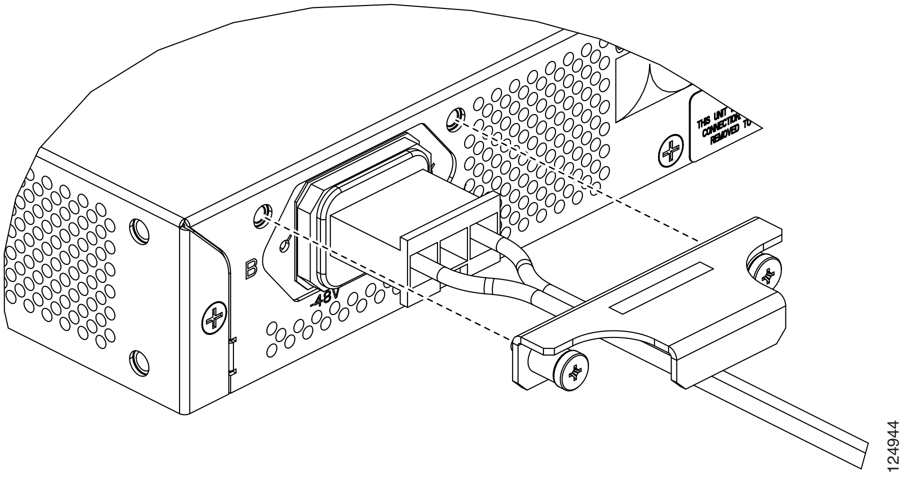
**Note** This power cable is suitable for maximum 5A, 60 VDC.

**Note** The battery return connection (+48Vdc) can be treated as DC-I , as defined in Telcordia GR-1089-CORE Issue 4. Connect the battery return (+48Vdc) to ground at the power source level.

**Step 11** Plug the DC power connector into either plug on the rear of the chassis at the outside corners of the ONS 15310-CL.

**Step 12** Install the strain-relief bracket over the power connector by using a Phillips screwdriver to screw the two screws at the top left and right of the bracket (Figure 17-8).

*Figure 17-8 Installed DC Power and Strain Relief Bracket*



**Step 13** If you want to provide redundant power supplies, repeat for the other power plug. If not, install the solid metal bracket over the extra plug, using two screws to the top left and right of the plug.

**Step 14** Return to your originating procedure (NTP).

# DLP-C8 Turn On and Verify DC Office Power on the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task verifies the ONS 15310-CL chassis LED activity and measures the DC power to verify correct power and returns. |
| **Tools/Equipment** | Voltmeter |
| **Prerequisite Procedures** | DLP-C5 Connect the Office Ground to the ONS 15310-CL, page 17-5<br>DLP-C7 Connect DC Office Power to the ONS 15310-CL, page 17-8 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** After applying power to the ONS 15310-CL chassis, verify the chassis LED activity (Figure 17-9 on page 17-12):

**a.** The FAIL LED blinks red for 20 to 30 seconds, then turns off.

**b.** The ALARM LED is off.

**c.** The PWR LED is green. (It is amber only if one DC power source is on and operating.)

**d.** The SYNC LED is green.

**Step 2** Using a voltmeter, verify the office battery and ground at the following points on the fuse and alarm panel:

**a.** To verify the power, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side connection and verify that it is between -44 VDC and -52 VDC. Next, place the red test lead on the B-side connection and verify that it is between -44 VDC and -52 VDC.

**Note** The voltages -44 VDC and -52 VDC are the minimum and maximum voltages required to power the chassis. The nominal steady-state voltage is -48 VDC.

**b.** To verify the ground, place the black test lead of the voltmeter to the frame ground. Place the red test lead on the A-side return ground and verify that no voltage is present. Place the red test lead on the B-side return ground and verify that no voltage is present.

**Step 3** According to site practice insert a fuse into the fuse position.

**Step 4** Using a voltmeter, verify the shelf for –48 VDC battery and ground:

**a.** To verify the A-side of the shelf, place the black lead of the voltmeter to the frame ground. Place the red test lead to the BAT1 (A-side battery connection) red cable. Verify that it reads between –44 VDC and –52 VDC. Then place the red test lead of the voltmeter to the RET1 (A-side return ground) black cable and verify that no voltage is present.

**b.** To verify the B-side of the shelf, place the black test lead of the voltmeter to the frame ground. Place the red test lead to the BAT2 (B-side battery connection) red cable. Verify that it reads between –44 VDC and -52 VDC. Then place the red test lead of the voltmeter to the RET2 (B-side return ground) black cable and verify that no voltage is present.

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

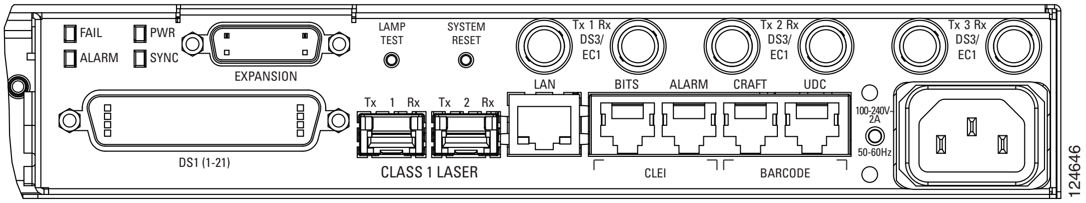
# DLP-C9 Install External Alarm Cables on the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task installs alarm cables on the ONS 15310-CL so that you can provision external (environmental) alarms and controls. |
| **Tools/Equipment** | Alarm cable, CAT-5 terminated with RJ-45 for all alarm connections |
| **Prerequisite Procedures** | NTP-C2 Install the Shelf Assembly, page 1-4 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Plug one end of the alarm cable into the ALARM port on the front of the ONS 15310-CL.

Figure 17-9 shows the connectors located on the front panel of the ONS 15310-CL.

*Figure 17-9 ONS 15310-CL Front Panel*



**Step 2** Plug the other end of the cable into the alarm-collection equipment according to local site practice.

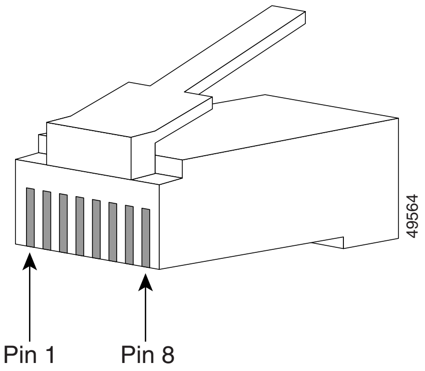
**Step 3** To define the six external alarm inputs and two external alarm outputs using CTC, see the "NTP-C63 Provision External Alarms and Controls" procedure on page 9-8. Table 17-1 shows the default input alarm pinouts and the corresponding alarm numbers assigned to each port. Refer to this table when connecting alarm cables to the ONS 15310-CL.

*Table 17-1 Default Alarm Pin Assignments*

| RJ-45 Pin Number | Function |
|---|---|
| 1 | Alarm Contact 1+ |
| 2 | Alarm Contact 1– |
| 3 | Alarm Contact 2+ |
| 4 | Alarm Contact 2– |
| 5 | Alarm Input 1 |
| 6 | Alarm Input 2 |
| 7 | Alarm Input 3 |
| 8 | Common (DC power return) |

Figure 17-10 shows RJ-45 pin numbering.

*Figure 17-10 Pins 1 and 8 on the RJ-45 Connector*



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

## DLP-C10 Install Timing Cables on the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task installs timing cables so that you can provide BITS timing to the ONS 15310-CL. |
| **Tools/Equipment** | Timing cable, CAT-5 RJ-45 connector |
| **Prerequisite Procedures** | NTP-C2 Install the Shelf Assembly, page 1-4 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

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

**Step 2** Plug the other end of the cable into the BITS clock according to local site practice. Table 17-2 shows the BITS cable pin assignments.

*Table 17-2 BITS Cable Pin Assignments*

| RJ-45 Pin Number | Function |
|---|---|
| 1 | BITS Output+ |
| 2 | BITS Output– |
| 3 | BITS Input+ |
| 4 | — |
| 5 | — |
| 6 | BITS Input– |

*Table 17-2 BITS Cable Pin Assignments (continued)*

| RJ-45 Pin Number | Function |
|---|---|
| 7 | — |
| 8 | — |

Figure 17-11 shows the BITS IN pins on the RJ-45 connector.

*Figure 17-11 BITS In Pins on the RJ-45 Connector*

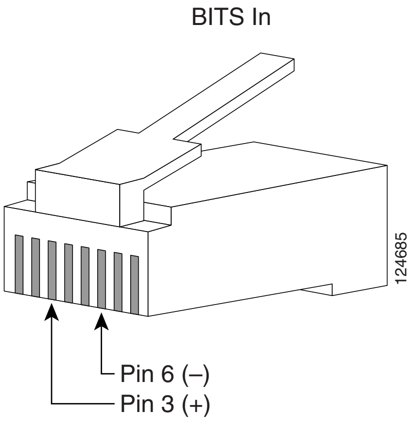
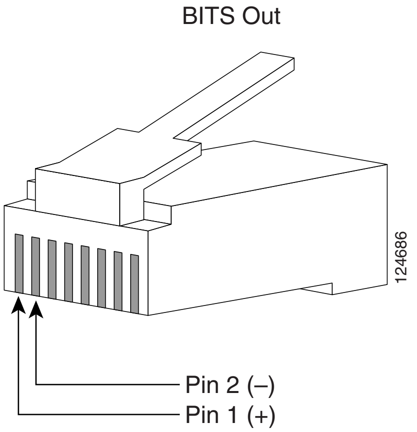


Figure 17-12 shows the BITS out pins on the RJ-45 connector.

*Figure 17-12 BITS Out Pins on the RJ-45 Connector*



**Note** For more detailed information about timing, refer to the “Timing” chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.* To set up system timing, see the “NTP-C23 Set Up Timing” procedure on page 4-11.

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

## DLP-C11 Install the Serial Cable for an ONS 15310-CL TL1 Craft Interface

| | |
|---|---|
| **Purpose** | This task installs the TL1 craft interface cable on an ONS 15310-CL. |
| **Tools/Equipment** | CAT-5 RJ-45 cable |
| **Prerequisite Procedures** | NTP-C2 Install the Shelf Assembly, page 1-4 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Plug one end of the TL1 cable into the CRAFT port on the front of the ONS 15310-CL (Figure 17-9 on page 17-12).

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

Table 17-3 shows the serial cable pin assignments.

*Table 17-3 TL1 Serial Cable Pin Assignments*

| RJ-45 Pin Number | Function |
|---|---|
| 1 | RTS |
| 2 | DTR |
| 3 | TXD |
| 4 | GND |
| 5 | GND |
| 6 | RXD |
| 7 | DSR |
| 8 | CTS |

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

## DLP-C12 Install the UDC Cable on the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task installs the user data channel (UDC) cable on the ONS 15310-CL. A UDC circuit allows you to create a dedicated data channel between nodes. |
| **Tools/Equipment** | CAT-5 RJ-45 cable |
| **Prerequisite Procedures** | NTP-C2 Install the Shelf Assembly, page 1-4 |

| | |
|---|---|
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

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

**Step 2** Connect the other end to terminating equipment, such as a 64-Kbps codirectional G.703 equipment interface or a RS-232-compliant equipment.

Table 17-4 shows the serial cable pin assignments.

*Table 17-4 UDC Cable Pin Assignments*

| RJ-45 Pin Number | RS-232 Mode | 64K Mode |
|---|---|---|
| 1 | NC | TX + |
| 2 | DTR | TX – |
| 3 | TXD | RX + |
| 4 | GND | GND |
| 5 | GND | GND |
| 6 | RXD | RX – |
| 7 | NC | NC |
| 8 | NC | NC |

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

# DLP-C13 Install LFH Cables for ONS 15310-CL DS-1 Connections

| | |
|---|---|
| **Purpose** | This task installs DS-1 cables on the ONS 15310-CL. |
| **Tools/Equipment** | 96-pin LFH connector terminated to a 21-pair #26 AWG cable |
| **Prerequisite Procedures** | NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

**Step 1** Prepare a 96-pin LFH connector terminated to a 21-pair #26 AWG cable.

**Step 2** See Table 17-5 for the ONS 15310-CL connector pin assignments.

**Note** Refer to the "Cisco ONS 15310-CL Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for specific information on DS-1 cables and DS-1 connectors, including product numbers and compatibility.

*Table 17-5 DS1 Connector Pin Assignments*

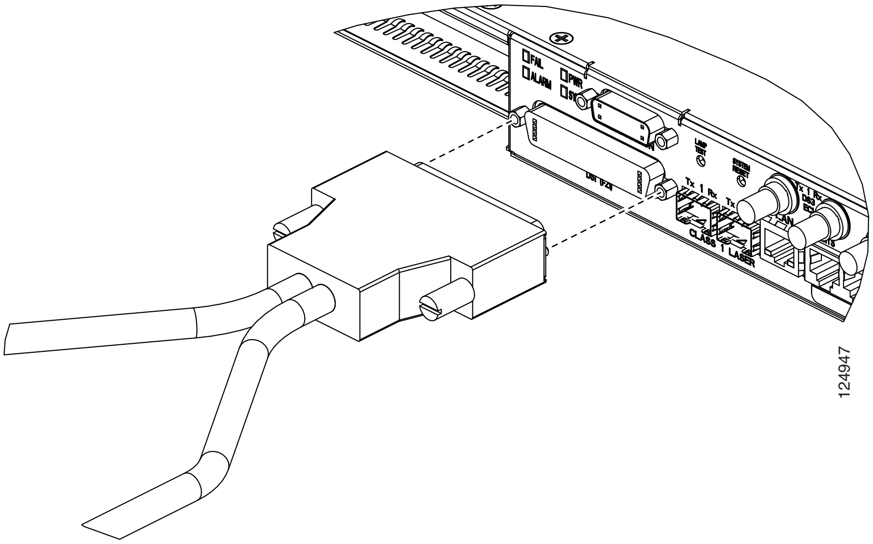
| Pin | Transmit Cable Signal Connection | Conductor Color | Pin | Receive Cable Signal Connection | Conductor Color |
|---|---|---|---|---|---|
| 1 | TX11- | blue-black | 49 | TX21- | blue-violet |
| 2 | TX11+ | black-blue | 50 | TX21+ | violet-blue |
| 3 | TX10- | gray-red | 51 | TX20- | gray-yellow |
| 4 | TX10+ | red-gray | 52 | TX20+ | yellow-gray |
| 5 | TX9- | brown-red | 53 | TX19- | brown-yellow |
| 6 | TX9+ | red-brown | 54 | TX19+ | yellow-brown |
| 7 | TX8- | green-red | 55 | TX18- | green-yellow |
| 8 | TX8+ | red-green | 56 | TX18+ | yellow-green |
| 9 | TX7- | orange-red | 57 | TX17- | orange-yellow |
| 10 | TX7+ | red-orange | 58 | TX17+ | yellow-orange |
| 11 | TX6- | blue-red | 59 | TX16- | blue-yellow |
| 12 | TX6+ | red-blue | 60 | TX16+ | yellow-blue |
| 13 | TX5- | gray-white | 61 | TX15- | gray-black |
| 14 | TX5+ | white-gray | 62 | TX15+ | black-gray |
| 15 | TX4- | brown-white | 63 | TX14- | brown-black |
| 16 | TX4+ | white-brown | 64 | TX14+ | black-brown |
| 17 | TX3- | green-white | 65 | TX13- | green-black |
| 18 | TX3+ | white-green | 66 | TX13+ | black-green |
| 19 | TX2- | orange-white | 67 | TX12- | orange-black |
| 20 | TX2+ | white-orange | 68 | TX12+ | black-orange |
| 21 | TX1- | blue-white | 69 | Unused | — |
| 22 | TX1+ | white-blue | 70 | Unused | — |
| 23 | Unused | — | 71 | Unused | — |
| 24 | Unused | — | 72 | Unused | — |
| 25 | RX11- | blue-black | 73 | RX21- | blue-violet |
| 26 | RX11+ | black-blue | 74 | RX21+ | violet-blue |
| 27 | RX10- | gray-red | 75 | RX20- | gray-yellow |
| 28 | RX10+ | red-gray | 76 | RX20+ | yellow-gray |
| 29 | RX9- | brown-red | 77 | RX19- | brown-yellow |
| 30 | RX9+ | red-brown | 78 | RX19+ | yellow-brown |
| 31 | RX8- | green-red | 79 | RX18- | green-yellow |

*Table 17-5 DS1 Connector Pin Assignments (continued)*

| Pin | Transmit Cable Signal Connection | Conductor Color | Pin | Receive Cable Signal Connection | Conductor Color |
|---|---|---|---|---|---|
| 32 | RX8+ | red-green | 80 | RX18+ | yellow-green |
| 33 | RX7- | orange-red | 81 | RX17- | orange-yellow |
| 34 | RX7+ | red-orange | 82 | RX17+ | yellow-orange |
| 35 | RX6- | blue-red | 83 | RX16- | blue-yellow |
| 36 | RX6+ | red-blue | 84 | RX16+ | yellow-blue |
| 37 | RX5- | gray-white | 85 | RX15- | gray-black |
| 38 | RX5+ | white-gray | 86 | RX15+ | black-gray |
| 39 | RX4- | brown-white | 87 | RX14- | brown-black |
| 40 | RX4+ | white-brown | 88 | RX14+ | black-brown |
| 41 | RX3- | green-white | 89 | RX13- | green-black |
| 42 | RX3+ | white-green | 90 | RX13+ | black-green |
| 43 | RX2- | orange-white | 91 | RX12- | orange-black |
| 44 | RX2+ | white-orange | 92 | RX12+ | black-orange |
| 45 | RX1- | blue-white | 93 | Unused | — |
| 46 | RX1+ | white-blue | 94 | Unused | — |
| 47 | Unused | — | 95 | Unused | — |
| 48 | Unused | — | 96 | Unused | — |

**Step 3** Connect the male connector on the cable to the female connector at the center of the front of the ONS 15310-CL (Figure 17-13).

*Figure 17-13 Installing the DS-1 Cable*



**Step 4** Tighten the two thumbscrews on the male connector.

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

# DLP-C14 Install DS-3/EC-1 Cables With MiniBNC Connectors on the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task installs the DS-3/EC-1 cables to connect DS-3/EC-1 signals to the ONS 15310-CL. The DS-3/EC-1 cables should be terminated with miniBNC connectors on the ONS 15310-CL side and BNC connectors on the client side. |
| **Tools/Equipment** | Shielded coaxial cable terminated with miniBNC connectors for DS-3/EC-1 ports |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

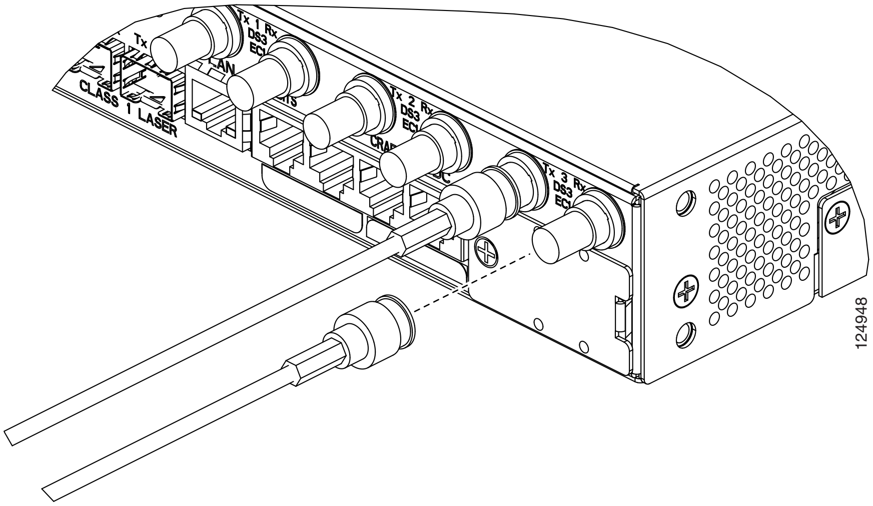
**Caution** Always use the supplied ESD wristband when working with a powered ONS 15310-CL. Plug the wristband cable into the ESD jack located to the left of the expansion slot.

**Note** Cisco recommends you use Cisco-orderable miniBNC cables to ensure interoperability between the cables and miniBNC connectors on the ONS 15310-CL.

**Step 1** Place a miniBNC cable connector over the connector on the front of the ONS 15310-CL.

Figure 17-14 shows how to connect a coaxial cable to an ONS 15310-CL.

*Figure 17-14 Installing a DS-3/EC-1 Cable with MiniBNC Connectors*



**Step 2** Position the cable connector so that the slot in the connector is above the corresponding notch on the ONS 15310-CL connection point.

**Step 3** Gently push the connector down until the notch on the ONS 15310-CL connector slides into the slot on the cable connector.

**Step 4** Turn the cable connector until the notch clicks into place.

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

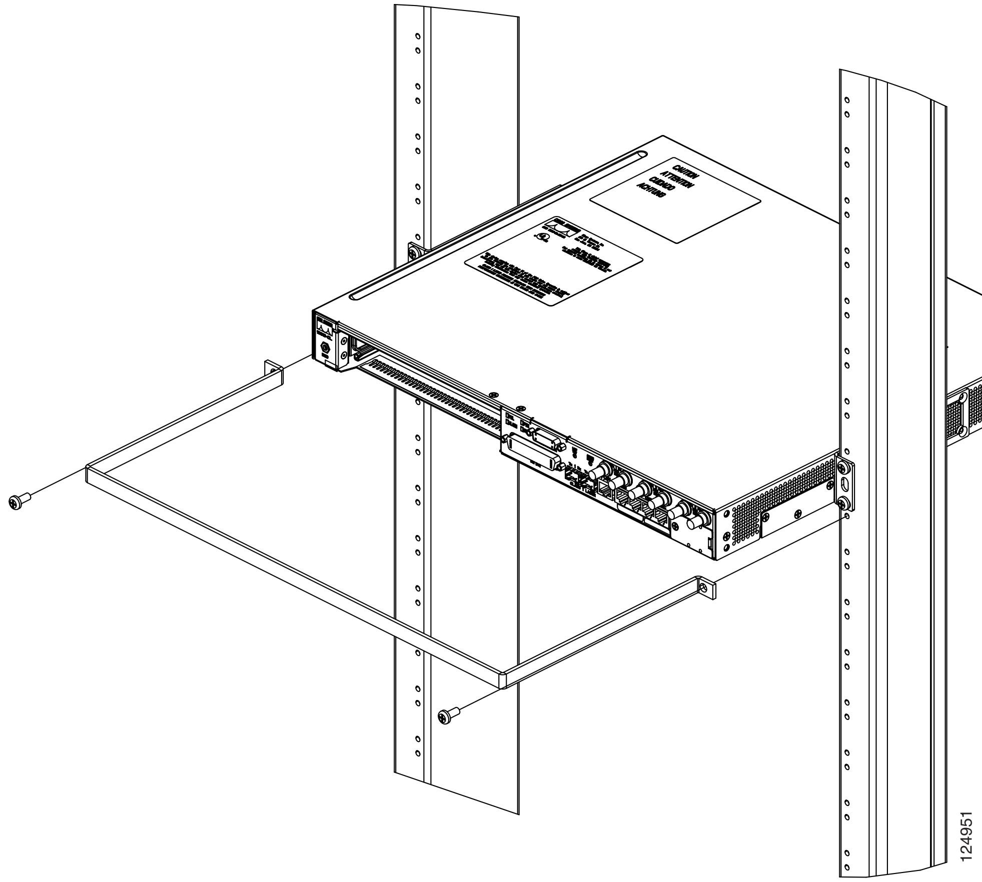
# DLP-C15 Route Cables on the ONS 15310-CL

| | |
|---|---|
| **Purpose** | This task routes electrical, optical, alarm, and timing cables away from the ONS 15310-CL. You can install optional tie-bars specifically designed for the ONS 15310-CL. |
| **Tools/Equipment** | Tie-wraps or other securing devices, according to local practice<br>Tie-bar(s) (15310-TIE-BAR-19; 15310-TIE-BAR-23) |
| **Prerequisite Procedures** | NTP-C6 Install the Electrical Cables, page 1-10<br>NTP-C8 Install Optical Cables, page 1-12<br>NTP-C5 Install Wires to Alarm, Timing, LAN, Craft, and UDC Pin Connections, page 1-9 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** As needed, install a tie-bar or other strain-relief device, according to local site practice.

Figure 17-15 shows how to install a tie-bar on an ONS 15310-CL rack.

*Figure 17-15 Installing a Tie-Bar*



**Caution** You must provide some type of strain-relief for the ONS 15310-CL cabling.

**Step 2** Route the cables to the right side of the shelf assembly according to local site practice, avoiding blocking the front of the expansion card.

**Step 3** Secure the cables to the strain-relief device using tie-wraps or other site-specific methods.

**Step 4** Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

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

# DLP-C16 Install SFP Connectors

| | |
|---|---|
| **Purpose** | This task installs OC-3, OC-12, OC-48, or OC-3/OC-12 (multirate) Small Form-factor Pluggables (SFPs). SFPs are hot-swappable input/output devices that plug into SFP slots on the ONS 15310-CL or ONS 15310-MA faceplate to link the port to the fiber-optic network. |
| **Tools/Equipment** | SFPs compatible with the ONS 15310-CL or ONS 15310-MA |
| **Prerequisite Procedures** | NTP-C2 Install the Shelf Assembly, page 1-4<br>NTP-C3 Install the Power and Ground, page 1-5 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Warning** **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments. Statement 1051**

**Warning** **Class 1 laser product.** Statement 1008

**Note** SFPs are hot-swappable and can therefore be installed and removed while the card/shelf assembly is powered and running.

**Note** SFPs are generically called pluggable port modules (PPMs) in CTC. After installing the SFP, multirate PPMs must be provisioned in CTC. See the "NTP-C130 Manage Pluggable Port Modules" procedure on page 10-3.

**Step 1** Verify that the SFP is correct for your network. Refer to the "Card Reference" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for card compatibility and SFP information.

**Step 2** Remove the SFP from its protective packaging.

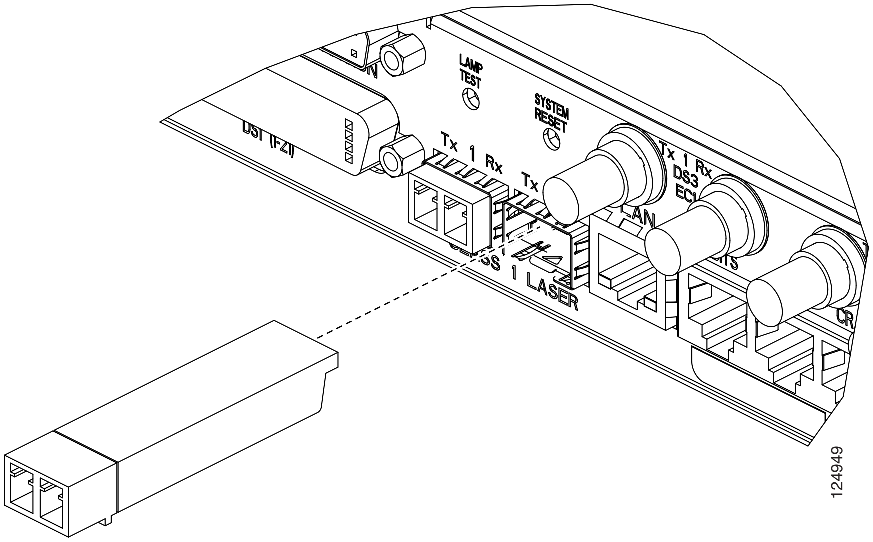
**Step 3** Orient the SFP so that the Cisco serial number label is facing away from the shelf (to the right).

**Step 4** Move the bail clasp to the left to unlatch it before inserting it into the slot.

**Step 5** Slide the SFP into the slot and move the bail clasp to the right to secure the SFP.

Figure 17-16 shows SFP installation on the ONS 15310-CL. (Installation on the ONS 15310-MA is similar. SFPs are installed on the faceplate of the CTX2500 card.)

*Figure 17-16 Installing the SFP on the ONS 15310-CL*



**Caution** Do not remove the protective caps until you are ready to attach the network fiber-optic cable.

**Note** You must set the normalized optical power received (OPR) value whenever you replace or insert an SFP. After you click Set for the port you are observing, the LBC (%), OPR (%), and OPT (%) values under the Performance > Optical tabs should be close to 100 percent. Only Cisco-approved SFPs should be used. See the "NTP-C87 Modify Line Settings and PM Parameter Thresholds for Optical Ports" procedure on page 10-2 for more information about changing optical port settings, and the "NTP-C66 Monitor Optical Performance" procedure on page 8-4 for more information about viewing performance monitoring parameters.

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

## DLP-C17 Remove SFP Connectors

| | |
|---|---|
| **Purpose** | This task disconnects fiber attached to an SFP and removes the SFP. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C16 Install SFP Connectors, page 17-22 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Warning** **Class 1 laser product.** Statement 1008

**Warning** **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

**Step 1** Disconnect the network fiber cable from the SFP connector. Squeeze the sides of the fiber cable firmly to unlatch it.

**Step 2** Pull the bail clasp to the left to release the SFP.

**Step 3** Slide the SFP out of the slot.

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

# DLP-C18 Install Fiber-Optic Cables in a 1+1 Configuration

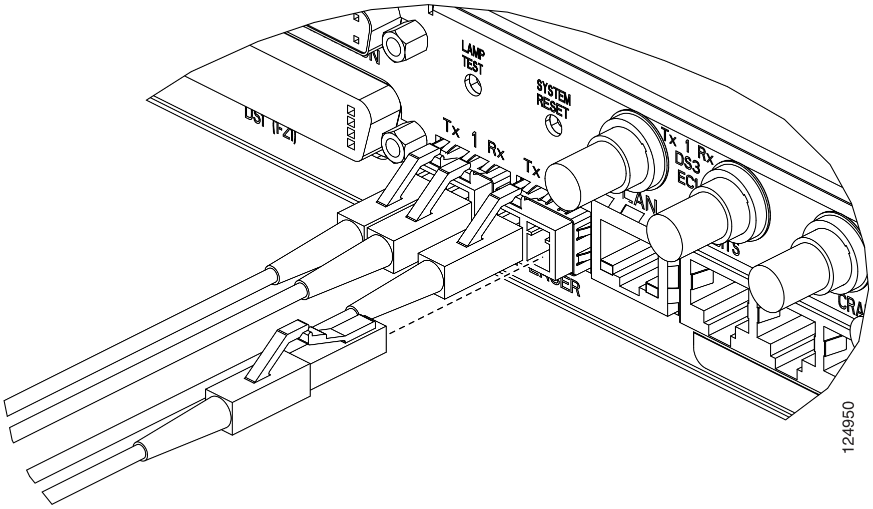
| | |
|---|---|
| **Purpose** | This task installs fiber-optic cables on optical (OC-N) ports in a 1+1 linear configuration. |
| **Tools/Equipment** | Fiber-optic cables |
| **Prerequisite Procedures** | NTP-C109 Clean Fiber Connectors, page 15-10 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Note** On ONS 15310-CL optical ports, the left connector is the transmit port and the right connector is the receive port. On ONS 15310-MA ports, the transmit and receive fiber for each optical signal are contained within a single SFP port.

**Step 1** Plan your fiber connections. Use the same plan for all 1+1 nodes.

**Step 2** Align the keyed ridge of the cable connector with the transmit (Tx) connector of a working OC-N port at one node (Figure 17-17) and plug the other end of the fiber into the receive (Rx) connector of a working OC-N port at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port to a receive port, or a transmit port to a transmit port).

*Figure 17-17 Installing an Optical Cable in the ONS 15310-CL*



**Step 3** Repeat Steps 1 and 2 for the corresponding protect ports on the two nodes and all other working/protect port pairs you want to place in a 1+1 configuration.

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

# DLP-C19 Install Fiber-Optic Cables for Path Protection Configurations

| | |
|---|---|
| **Purpose** | This task installs the fiber-optic cables to the east and west path protection ports at each node. See Chapter 5, "Turn Up a Network" to provision and test path protection configurations. |
| **Tools/Equipment** | Fiber-optic cables |
| **Prerequisite Procedures** | NTP-C109 Clean Fiber Connectors, page 15-10 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Note** You can install the fiber immediately after installing the node, or wait until you are ready to turn up the network. See Chapter 5, "Turn Up a Network."

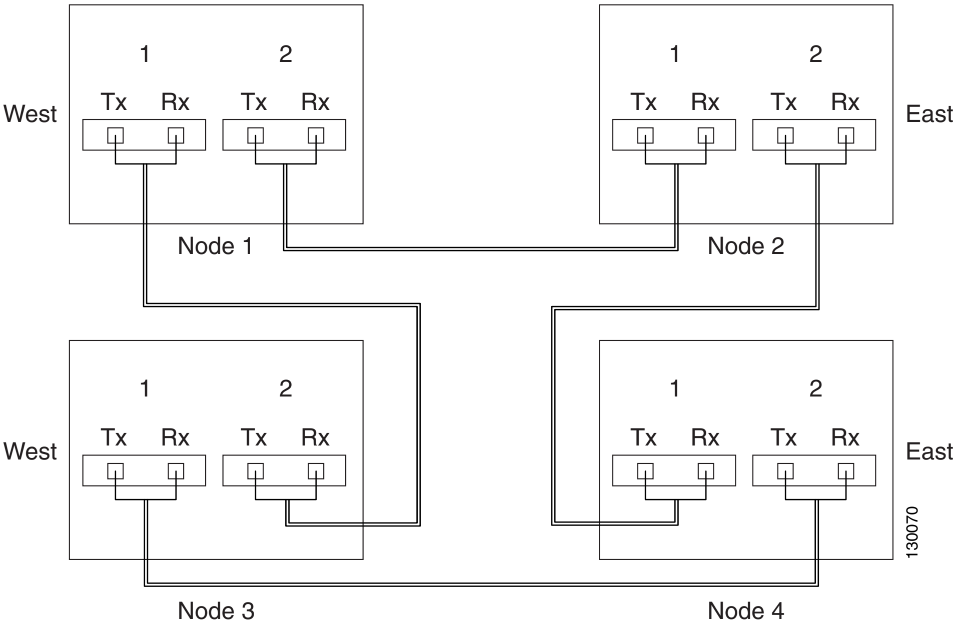
**Step 1** Plan your fiber connections. Use the same plan for all path protection nodes.

**Step 2** Plug the fiber into the Tx port at one node and plug the other end of the fiber into the Rx port at the adjacent node. The card will display a signal fail (SF) LED if the transmit and receive fibers are mismatched (for example, one fiber connects a receive port to a receive port, or a transmit port to a transmit port).

**Step 3** Repeat Step 2 until you have configured the entire ring.

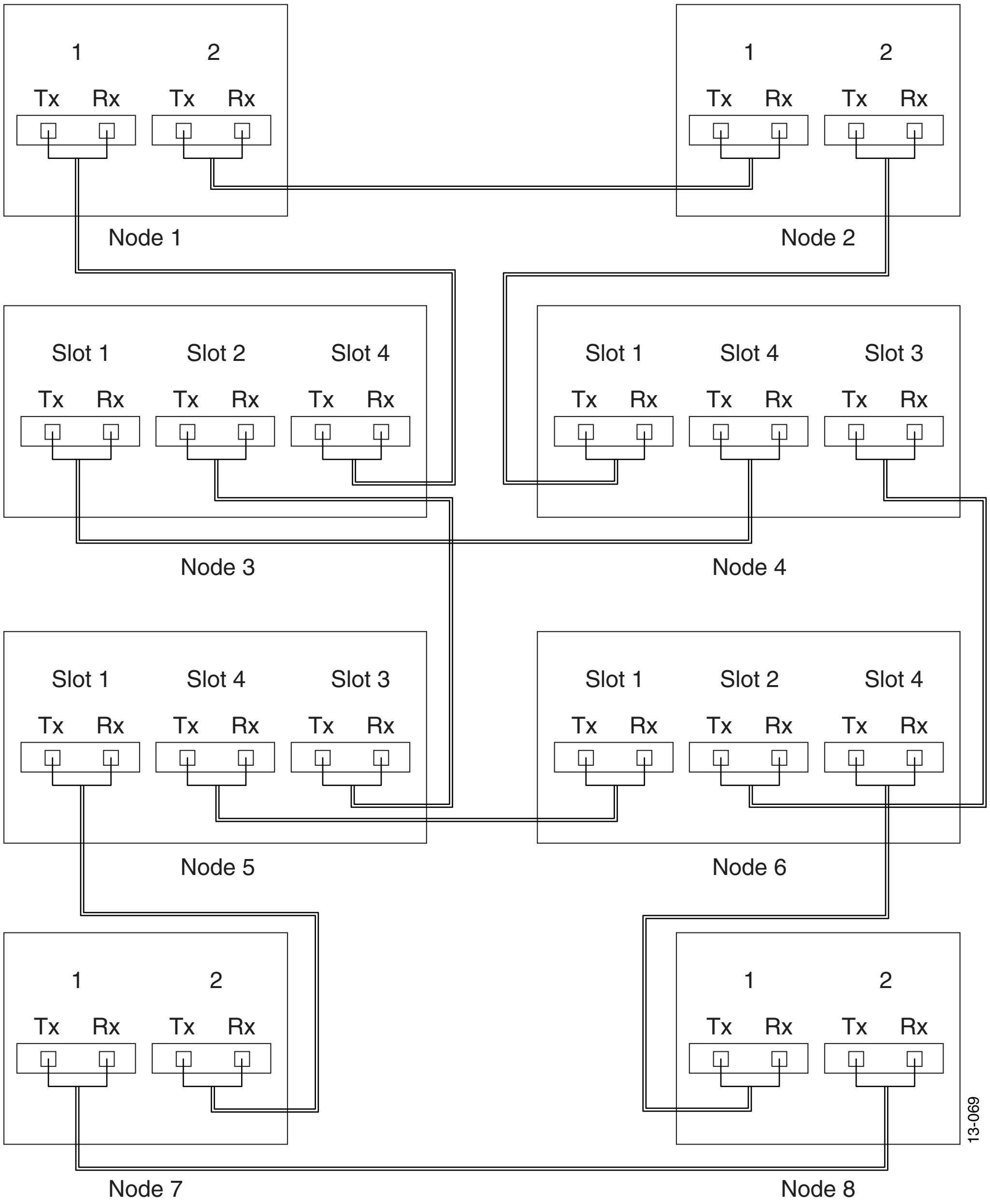
Figure 17-18 shows fiber connections for a four-node path protection with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

*Figure 17-18 Connecting Fiber to a Four-Node Path Protection Configuration*



If you are creating a path protection dual-ring interconnect (DRI), Figure 17-19 shows a traditional DRI example. Because the ONS 15310-CL has only two optical ports, in Figure 17-19 it can be represented by Nodes 1, 2, 7, or 8. Nodes 3, 4, 5, and 6 must represent other terminating equipment, such as the ONS 15310-MA, ONS 15327, ONS 15454, or ONS 15600.

*Figure 17-19 Connecting Fiber to an Eight-Node Traditional Path Protection DRI*



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

# DLP-C20 Measure Voltage

| | |
|---|---|
| **Purpose** | This task measures power so you can verify correct power and returns. |
| **Tools/Equipment** | Voltmeter |
| **Prerequisite Procedures** | NTP-C3 Install the Power and Ground, page 1-5 or NTP-C151 Install the Power and Ground, page 2-12<br>Table 1-2 on page 1-17 or Table 2-2 on page 2-30 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Using a voltmeter, verify the office ground and power shows the power terminals:

**a.** Place the black lead (positive) on the frame ground on the rack. Hold it there while completing Step b.

**b.** Place the red lead (negative) on the fuse power points and alarm panel to verify that they read between –44 VDC and –52 VDC (power) and 0 (return ground).

**Step 2** Using a voltmeter, verify the shelf ground and power wiring:

**a.** Place the black lead (positive) on the RET1 and the red lead on the BAT1 point. Verify a reading between –44 VDC and –52 VDC. If there is no voltage, check the following:

- Battery and ground reversed to the shelf
- Battery is open or missing
- Return is open or missing

**b.** Repeat Step 2 for the RET2 and BAT2 if the B power feed is provided.

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

# DLP-C21 Run the CTC Installation Wizard for Windows

| | |
|---|---|
| **Purpose** | This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 5.0, and the CTC JAR (Java Archive) files. JRE 5.0 is required to run Release 8.5. The CTC JAR files contain the ONS 15310-CL and ONS 15310-MA client software. CTC JAR files are normally downloaded from the ONS 15310-CL or ONS 15310-MA the first time you log in. Pre-installing the JAR files saves time at initial login. It also allows you to log into ONS 15454s running earlier CTC software releases to manage ONS 15310-CL or ONS 15310-MA nodes that are connected to the ONS 15454 network. |
| **Tools/Equipment** | Cisco ONS 15310-CL System Software CD, Version 8.5 or<br>Cisco ONS 15310-MA System Software CD, Version 8.5 |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | This task is required if any one of the following is true:<br>• JRE 5.0 is not installed<br>• CTC online user manuals are not installed and are needed<br>• CTC JAR files are not installed and are needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | None |

**Step 1** Verify that your computer has the following:

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

  If your operating system is Windows NT 4.0, verify that Service Pack 6a or later is installed. From the Start menu, choose **Programs > Administrative Tools > Windows NT Diagnostics** and check the service pack on the Version tab of the Windows NT Diagnostics dialog box. If Service Pack 6a or later is not installed, do not continue. Install Service Pack 6a following the computer upgrade procedures for your site. If your operating system is Windows Vista please complete DLP-C276 Configuring Windows Vista to Support CTC, page 19-91 before proceeding further.
- Processor and RAM requirements are guidelines. CTC performance is faster if your computer has a faster processor and more RAM.

**Step 2** Insert the 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 1.4.2
- Acrobat Reader 6.0.1
- Online User Manuals
- CTC JAR files

**Note** If you use the delete CTC cache function at any later time, the JAR files will be removed. You must complete this task again to re-install the JAR files.

**Note** You can also install the JAR files by starting a command prompt session, changing to the CD directory, and typing **Run java -jar LDCACHE.jar**.

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

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

- Click **Typical** to install all three components. If you already have JRE version 5.0 installed on your computer, choose Custom.
- Click **Custom** if you want to install either the JRE or the online user manuals.

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

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

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

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

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

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

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

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

**Step 10** Click **Next**. It may take a few minutes for the JRE installation wizard to appear. If you selected Custom in Step 4 need to install the JRE, continue with Step 12.

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

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

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

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

**b.** Click **Next**.

**c.** Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

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

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

- Java 2 Runtime Environment—(Default) Installs JRE 5.0 with support for European languages.
- Support for Additional Languages—Adds support for non-European languages.
- Additional Font and Media Support—Adds Lucida fonts, Java Sound, and color management capabilities.

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

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

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

**f.** Click **Next**.

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

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

**h.** Click **Next**.

**i.** Click **Finish**.

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

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

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

**Step 14** Return to your originating procedure (NTP).

## DLP-C22 Run the CTC Installation Wizard for UNIX

| | |
|---|---|
| **Purpose** | This task installs the CTC online user manuals, Acrobat Reader 6.0.1, JRE 5.0, and the CTC JAR (Java Archive) files. JRE 5.0 is required to run Software Release 8.5. The CTC JAR files contain the ONS 15310-CL and ONS 15310-MA client software. CTC JAR files are normally downloaded from the ONS 15310-CL or ONS 15310-MA the first time you log in. Pre-installing the JAR files saves time at initial login. It also allows you to log into ONS 15454s running earlier CTC software releases to manage ONS 15310-CL or ONS 15310-MA nodes that are connected to the ONS 15454 network. |
| **Tools/Equipment** | Cisco ONS 15310-CL System Software CD, Version 8.5.x or<br>Cisco ONS 15310-MA System Software CD, Version 8.5.x |
| **Prerequisite Procedures** | None |
| **Required/As Needed** | Required if any of the following are true:<br>• JRE 5.0 is not installed.<br>• CTC online user manuals are not installed and are needed. |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | None |

**Step 1** Verify that your computer has the following:

- RAM—384 MB recommended, 512 MB optimum
- Hard drive—20 GB hard drive recommended with at least 50 MB of space available
- Operating System—Solaris 8 or 9

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

**Step 2** Change the directory, type:

**cd /cdrom/cdrom0/**

**Step 3** From the techdoc310 CD directory, type:

**./setup.bat**

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

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

**Note** If you use the delete CTC cache function at any later time, the JAR files will be removed. You must complete this task again to re-install the JAR files.

**Note** You can also install the JAR files by starting a command prompt session, changing to the CD directory, and typing **Run java -jar LDCACHE.jar**.

**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 version 5.0 installed on your computer, choose Custom.
- Click **Custom** if you want to install either the JRE or the online user manuals.

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

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

- If you selected Typical, continue with Step 8.
- If you selected Custom in Step 5, check the CTC component that you want to install and click **Next**. If you will ever need to log into a node running an ONS release earlier than Software Release 5.0, uncheck Java Runtime Environment 1.4.2.
  - If you selected Online User Manuals, continue with Step 8.
  - If you did not select Online User Manuals, continue with Step 10.

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

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

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

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

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

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

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

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

- I accept the terms of the license agreement—Accepts the license agreement. Continue with Step b.
- I do not accept the terms of the license agreement—Disables the Next button on the Java 2 Runtime Environment License Agreement dialog box. Click **Cancel** to return to the CTC installation wizard. CTC will not install the JRE. Continue with Step 13.

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

b. Click **Next**.

c. Choose one of the following:

- Click **Typical** to install all JRE features. If you select Typical, the JRE version installed will automatically become the default JRE version for your browsers.
- Click **Custom** if you want to select the components to install and select the browsers that will use the JRE version.

d. Click **Next**.

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

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

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

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

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

f. Click **Next**.

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

**Note** Setting the JRE version as the default for these browsers may 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 user manuals install.

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

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

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

# DLP-C23 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-MA on the Same Subnet Using Static IP Addresses

| | |
|---|---|
| **Purpose** | This task sets up your computer for a local craft connection to the ONS 15310-CL when:<br>• You will connect to one ONS 15310-CL or ONS 15310-MA; if you will connect to multiple nodes, you might need to reconfigure your computer's IP settings each time you connect to a node.<br>• You need to use non-ONS 15310-CL or 15310-MA applications such as ping and tracert (trace route). |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C13 Set Up Computer for CTC, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, 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:

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, select **TCP/IP** for your PC Ethernet card, 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 15310-CL/ONS 15310-MA IP address except for the last octet. For example, if the node IP address is 209.165.201.30, your IP address must be 209.165.201.xxx, where xxx is any number up to 255 excluding 30, which is used in the node IP address.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL or ONS 15310-MA. 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 15310-CL/ONS 15310-MA 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 to the ONS 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA 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 to the current node ONS 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA 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 to the ONS 15310-CL/ONS 15310-MA 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 15310-CL/ONS 15310-MA 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-C24 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-CL Using Dynamic Host Configuration Protocol

| | |
|---|---|
| **Purpose** | This task sets up your computer for craft connection to the ONS 15310-CL/ONS 15310-MA using DHCP. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C13 Set Up Computer for CTC, page 3-2<br>NTP-C21 Set Up CTC Network Access, page 4-6 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Caution** Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15310-CL/ONS 15310-MA. By default, DHCP is not enabled. To enable it, see the "NTP-C21 Set Up CTC Network Access" procedure on page 4-6.

**Note** The ONS 15310-CL/ONS 15310-MA does not provide the IP addresses. If DHCP forwarding is enabled, it passes DCHP requests to an external DHCP server.

**Step 1** Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, 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:

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, select **TCP/IP** for your 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 **Obtain an IP address automatically**.

h. Click **OK**.

i. 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 **Obtain an IP address from a DHCP server**.

f. Click **OK**.

g. Click **Apply**.

h. If Windows prompts you to restart your PC, 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 **Obtain an IP address from a DHCP server**.

e. Click **OK**.

f. In the Local Area Connection Properties dialog box, click **OK**.

g. 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. In the Network Connections dialog box, click **Local Area Connection**.

c. In the Local Area Connection Status dialog box, click **Properties**.

d. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.

e. Click **Obtain an IP address from a DHCP server**.

f. Click **OK**.

g. In the Local Area Connection Properties dialog box, click **OK**.

h. In the Local Area Connection Status dialog box, click **Close**.

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

# DLP-C25 Set Up a Windows PC for Craft Connection to an ONS 15310-CL or ONS 15310-MA Using Automatic Host Detection

| | |
|---|---|
| **Purpose** | This task sets up your computer for local craft connection to the ONS 15310-CL/ONS 15310-MA when:<br>• You will connect to the ONS 15310-CL/ONS 15310-MA CRAFT port or its LAN port either directly or through a hub.<br>• You will connect to multiple ONS 15310-CL/ONS 15310-MA nodes and do not want to reconfigure your IP address each time.<br>• You do not need to access non-ONS 15310-CL/ONS 15310-MA applications such as ping and tracert (trace route). |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C13 Set Up Computer for CTC, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite |
| **Security Level** | None |

**Step 1** Verify the operating system that is installed on your computer:

a. From the Windows Start menu, choose **Settings > Control Panel**.

**Note** In Windows XP, you can select Control Panel directly from the Start menu. Make sure you are in Classic View before continuing with this procedure.

b. In the Control Panel window, double-click the **System** icon.

c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows NT 4.0, Windows 2000, 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:

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, select **TCP/IP** for your 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 any legitimate IP address other than the node IP address. The default node IP address is 192.1.0.2.

i. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. 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 address entered in Step g. 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 any legitimate IP address other than the node IP address. The default node IP address is 192.1.0.2.

g. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. The default is **255.255.255.0** (24 bit).

h. Click **Advanced**.

i. In the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box appears.

j. Type the IP address entered in Step f in the Gateway Address field.

k. Click **Add**.

l. Click **OK**.

m. Click **Apply**.

n. Reboot your PC.

**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 any legitimate IP address other than the current node IP address. The default node IP address is 192.1.0.2.

f. In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. The default is **255.255.255.0** (24 bit).

g. Type the IP address entered in Step e in the Gateway Address field.

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 any legitimate IP address other than the current node IP address. The default node IP address is 192.1.0.2.
- **e.** In the Subnet Mask field, type the same subnet mask as the ONS 15310-CL/ONS 15310-MA. The default is **255.255.255.0** (24 bit).
- **f.** Type the IP address entered in Step d in the Gateway Address field.
- **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-C27 Disable Proxy Service Using Internet Explorer (Windows)

| | |
|---|---|
| **Purpose** | This task disables proxy service for PCs running Internet Explorer. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C13 Set Up Computer for CTC, page 3-2 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | None |

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

**Note** If your computer is running Windows XP, you can select Control Panel directly from the Start menu. Make sure that you are in Classic View before continuing with this procedure. To switch to Classic View, right-click the Windows screen and choose **Properties** from the popup menu. Click the **Appearance** tab, then under Scheme, choose **Classic View**.

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

**Step 3** In the Internet Properties dialog box, click **Connections** > **LAN Settings**.

**Step 4** In the LAN Settings dialog box, complete one of the following tasks:

- Uncheck **Use a proxy server** to disable the service.
- To bypass the service, leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15310-CL/ONS 15310-MA nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS 15310-CL/ONS 15310-MA nodes on your network. Click **OK** to close each open dialog box.

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

## DLP-C28 Disable Proxy Service Using Netscape (Windows)

| | |
|---|---|
| **Purpose** | This task disables proxy service for Windows PCs running Netscape. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C13 Set Up Computer for CTC, page 3-2 |
| **Required/As Needed** | Required if your computer is connected to a network computer proxy server and your browser is Netscape. |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | None |

**Step 1** Open Netscape.

**Step 2** From the Edit menu, choose **Preferences**.

**Step 3** In the Preferences dialog box under Category, choose **Advanced > Proxies**.

**Step 4** On the right side of the Preferences dialog box under Proxies, perform one of the following options:

- Choose **Direct connection to the Internet** to bypass the proxy server.
- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15310-CL/ONS 15310-MA nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

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

# DLP-C29 Log into CTC

| | |
|---|---|
| **Purpose** | Use this task to log into CTC, the graphical user interface software used to manage the ONS 15310-CL or ONS 15310-MA. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C13 Set Up Computer for CTC, page 3-2<br>One of the following procedures:<br>• NTP-C14 Set Up CTC Computer for Local Craft Connection to the Node, page 3-3, or<br>• NTP-C15 Set Up a CTC Computer for a Corporate LAN Connection to the Node, page 3-5, or<br>• NTP-C16 Set Up a Remote Access Connection to the Node, page 3-6 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Note** The ONS 15310-CL can be networked with ONS 15454 nodes running Software Release 4.1, 4.6, or later. The ONS 15310-MA can be networked with ONS 15454 nodes running Software Release 8.5 or later. You can log into the ONS 15454 nodes to manage the ONS 15310-CL or ONS 15310-MA nodes. However, you must complete the "DLP-C21 Run the CTC Installation Wizard for Windows" task on page 17-29 or the "DLP-C22 Run the CTC Installation Wizard for UNIX" task on page 17-32. These tasks install the Release 8.5 software JAR files on your computer. The tasks must be repeated anytime you delete the CTC cache.

**Note** For information about CTC views and navigation, see Appendix A, "CTC Information and Shortcuts."

**Step 1** From the computer connected to the ONS 15310-CL or ONS 15310-MA, start Netscape (PC or UNIX) or Internet Explorer (PC only):

- If you are using a PC, launch Netscape or Internet Explorer from the Windows Start menu or a shortcut icon.
- If you are using UNIX, launch Netscape from the command line by typing:
  - 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 might run out of colors to use for CTC. The **-install** and **-ncols 32** command line options limit the number of colors that Netscape uses.

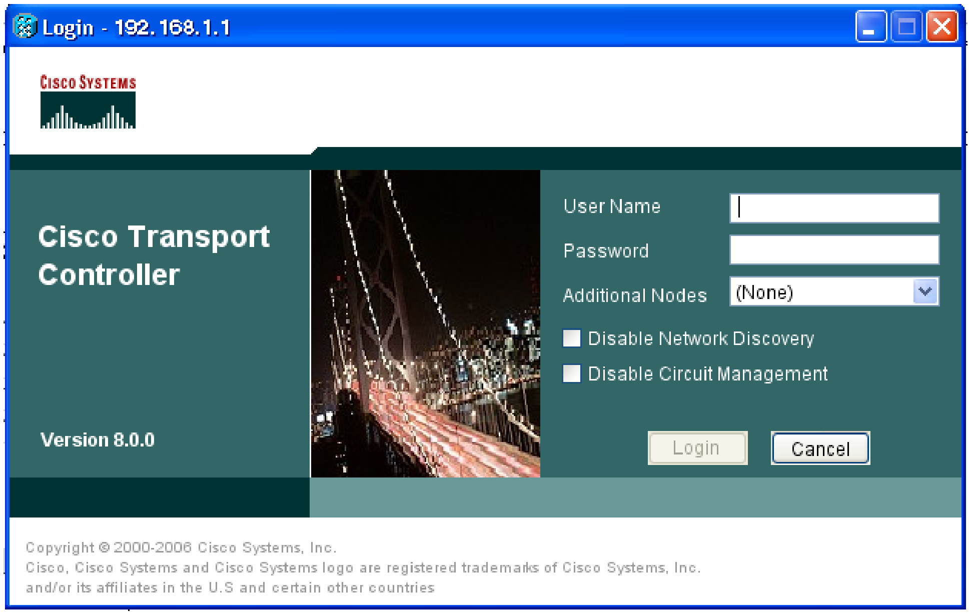
**Step 2** In the Netscape or Internet Explorer web address (URL) field, enter the ONS 15310-CL or ONS 15310-MA IP address. For initial setup, this is the default address, 192.1.0.2. Press **Enter**.

**Note** If you are logging into ONS 15310-CL or ONS 15310-MA 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. This will display the ONS 15310-CL or ONS 15310-MA software version for each node visible on the network view. To resolve an alarm, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

If a Java Plug-in Security Warning dialog box appears, complete the "DLP-C30 Install Public-Key Security Certificate" task on page 17-47 to install the public-key security certificate required by Software Release 4.1 and later.

After you complete the security certificate dialog box (or if the certificate is already installed), a Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages appear while CTC files are downloaded to your computer. The first time you connect to an ONS 15310-CL or ONS 15310-MA, this process can take several minutes. After the download, the CTC Login dialog box appears (Figure 17-20).

***Figure 17-20 Logging into CTC***



Login - 192.168.1.1

Cisco Transport Controller

Version 8.0.0

User Name

Password

Additional Nodes (None)

□ Disable Network Discovery

□ Disable Circuit Management

Copyright © 2000-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
and/or its affiliates in the U.S and certain other countries

**Step 3** In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name **CISCO15** and the password **otbu+1**.

**Note** The CISCO15 user is provided with every ONS 15310-CL or ONS 15310-MA. 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 15310-CL or ONS 15310-MA users and assign security, go to the "NTP-C19 Create Users and Assign Security" procedure on page 4-4. Additional information about security is provided in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

**Step 4** Each time you log into an ONS 15310-CL or ONS 15310-MA, you can make selections for the following login options:

- Node Name—Displays the IP address entered in the web browser and a drop-down list of previously entered ONS 15310-CL/ONS 15310-MA IP addresses. You can select any ONS 15310-CL or ONS 15310-MA on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
- Additional Nodes—Displays a list of current login node groups. To create a login node group or to add additional groups, see the "DLP-C31 Create Login Node Groups" task on page 17-47).
- Disable Network Discovery—Check this box to view only the ONS 15310-CL or ONS 15310-MA (and login node group members, if any) entered in the Node Name field. Nodes linked to this node through DCCs are not discovered and will not appear in CTC network view. Using this option can decrease the CTC start-up time in networks with many DCC-connected nodes and reduces memory consumption.
- Disable Circuit Management—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits and reduces memory consumption. This option does not prevent the creation and management of new circuits.

**Step 5** 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.

**Note** Upgrading the CTC software will overwrite your existing software. You must restart CTC after the upgrade is complete.

**Step 6** Click **Login**.

If the login is successful, the CTC window appears. From here, you can navigate to other CTC views to provision and manage the ONS 15310-CL or ONS 15310-MA. If you need to turn up the shelf for the first time, see Chapter 4, "Turn Up a Node." If login problems occur, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

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

# DLP-C30 Install Public-Key Security Certificate

| | |
|---|---|
| **Purpose** | This task installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run Software Release 4.1 or later. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | This task is performed during the "DLP-C29 Log into CTC" task on page 17-44. You cannot perform it outside of this task. |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Yes (Grant This Session)—Installs the public-key certificate to your PC only for the current session. After the session is ended, the certificate is deleted. This dialog box will appear the next time you log into the ONS 15310-CL/ONS 15310-MA.
- No (Deny)—Denies permission to install certificate. If you choose this option, you cannot log into the ONS 15310-CL/ONS 15310-MA.
- Always (Grant Always)—Installs the public-key certificate and does not delete it after the session is over. Cisco recommends this option.
- More Details (View Certificate)—Allows you to view the public-key security certificate.

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

# DLP-C31 Create Login Node Groups

| | |
|---|---|
| **Purpose** | This task creates a login node group to display ONS 15310-CL or ONS 15310-MA nodes that have an IP connection but not a DCC connection to the login node. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Click **Login Node Group** and **Create Group**.

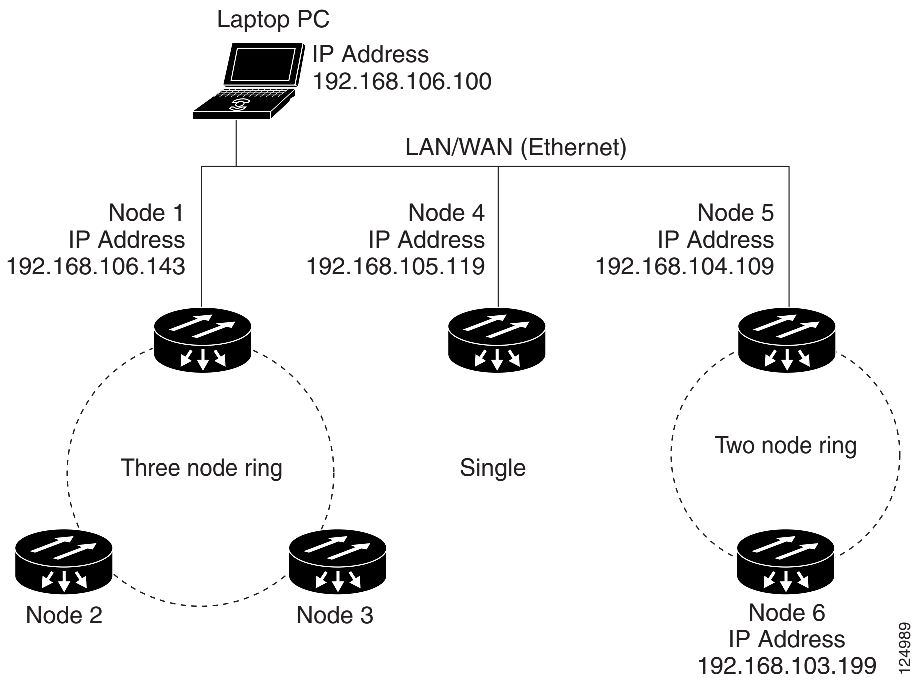
**Step 3** Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

**Step 4** In the Members area, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node you want to add to the group.

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

The next time you log into an ONS 15310-CL/ONS 15310-MA, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in Figure 17-21, a login node group is created that contains the IP addresses for Nodes 1, 4, and 5. During login, if you choose this group from the Additional Nodes list and Disable Network Discovery is not selected, all nodes in the figure appear. If the login group and Disable Network Discovery are both selected, only Nodes 1, 4, and 5 appear. You can create as many login groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

*Figure 17-21 Login Node Group*



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

# DLP-C32 Add a Node to the Current Session or Login Group

| | |
|---|---|
| **Purpose** | This task adds a node to the current CTC session or login node group. |
| **Tools** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** From the CTC File menu, click **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** This 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 appears on the network view map.

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

## DLP-C33 Delete a Node from the Current Session or Login Group

| | |
|---|---|
| **Purpose** | This task removes a node from the current CTC session or login node group. To remove a node from a specified login node group, see the "DLP-C34 Delete a Node from a Specified Login Node Group" task on page 17-49. |
| **Tools** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Click the node that you want to delete.

**Step 3** From the CTC File menu, click **Delete Selected Node**.

After a few seconds, the node disappears from the network view map.

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

## DLP-C34 Delete a Node from a Specified Login Node Group

| | |
|---|---|
| **Purpose** | This task removes a node from a specified login node group. To remove a node from the current login node group, see the "DLP-C33 Delete a Node from the Current Session or Login Group" task on page 17-49. |
| **Tools** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** In the Preferences dialog box, click the **Login Node Groups** tab.

**Step 3** Click the login node group tab containing the node you want to remove.

**Step 4** Select the node you want to remove, then click **Remove**.

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

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

# DLP-C35 Change the JRE Version

| | |
|---|---|
| **Purpose** | This task changes the JRE version, which is useful if you would like to upgrade to a later JRE version from earlier one without using the software or documentation CD. This does not affect the browser default version. After selecting the desired JRE version, you must exit CTC. The next time you log into a node, the new JRE version will be used. |
| **Tools** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Click the **JRE** tab. The JRE tab shows the current JRE version and the recommended version.

**Step 3** Click the **Browse** button and navigate to the JRE directory on your computer.

**Step 4** Choose the JRE version.

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

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

**Step 7** In the confirmation dialog box, click **Yes**.

**Step 8** Complete the "DLP-C29 Log into CTC" task on page 17-44.

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

# DLP-C36 Configure the CTC Alerts Dialog for Automatic Popup

| | |
|---|---|
| **Purpose** | This task sets up the CTC Alerts dialog box to open for all alerts, circuit deletion errors only, or never. The CTC Alerts dialog box displays network disconnection, Send-PDIP inconsistency, circuit deletion status, condition retrieval errors, and software download failure. |
| **Tools** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Click the CTC Alerts toolbar icon.

**Step 2** In the CTC Alerts dialog box, choose one of the following:

- All alerts—Sets the CTC Alerts dialog box to open automatically for all notifications.
- Error alerts only—Sets the CTC Alerts dialog box to open automatically for circuit deletion errors only.
- Never—Sets the CTC Alerts dialog box to never open automatically.

**Step 3** Click **Close**.

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

# DLP-C37 Create a New User on a Single Node

| | |
|---|---|
| **Purpose** | This task creates a new user for one ONS 15310-CL or ONS 15310-MA. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

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

**Step 2** In the Security window, click **Create**.

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

- Name—Type the user name. The name must have a minimum of six and a maximum of 20 alphanumeric characters (a-z, A-Z, 0-9). For TL1 compatibility, the user name must have 6 to 10 characters.
- Password—Type the user password. The password length, by default, is set to a minimum of six and a maximum of 20 characters. You can configure the default values in CTC node view using the Provisioning > NE Defaults > Node > security > password Complexity tabs. 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 have 6 to 10 characters, and the first character must be an alpha character. The password cannot 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 "Security" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for information about the capabilities provided with each level.

**Note** Each security level has a different idle time. The idle time is the length of time that CTC can remain idle before it locks up and the password must be reentered. Default idle times are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes.

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

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

# DLP-C38 Create a New User on Multiple Nodes

| | |
|---|---|
| **Purpose** | This task adds a new user to multiple ONS 15310-CL or ONS 15310-MA nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

**Note** 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** In the Security window, click **Create**.

**Step 4** In the Create User dialog box, enter the following:

- Name—Type the user name. The name must have a minimum of six and a maximum of 20 alphanumeric characters (a-z, A-Z, 0-9). For TL1 compatibility, the user name must have no more than 10 characters, and the first character must be an alpha character.
- Password—Type the user password. The password must have a minimum of 6 and a maximum of 20 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 cannot 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 "Security" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for information about the capabilities provided with each level.

**Note** Each security level has a different idle time. The idle user timeout is the length of time that CTC can remain idle before it locks up and the password must be reentered. The default times are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle user timeout values, see the "NTP-C83 Modify Users and Change Security" procedure on page 11-6.

**Step 5** Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected 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-C39 Provision IP Settings

| | |
|---|---|
| **Purpose** | This task provisions IP settings, which includes the IP address, default router, DHCP access, firewall access, and SOCKS proxy server settings. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

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

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

**Step 2** Complete the following information in the fields listed:

- Node Address—Type the IP address assigned to the ONS 15310-CL or ONS 15310-MA node.
- Net/Subnet Mask Length—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 15310-CL/ONS 15310-MA nodes in the same subnet.
- MAC Address—(Display only) Displays the ONS 15310-CL/ONS 15310-MA IEEE 802 MAC address.
- Default Router— If the ONS 15310-CL or ONS 15310-MA is connected to a LAN, enter the IP address of the default router. The default router forwards packets to network devices that the ONS 15310-CL or ONS 15310-MA cannot directly access. This field is ignored if any of the following are true:

  - The ONS 15310 is not connected to a LAN.
  - SOCKS proxy server is enabled and the ONS 15310 is provisioned as an ENE.
  - OSPF is enabled on both the ONS 15310 and the LAN where the ONS 15310 is connected.
- Suppress CTC IP Display—Check this check box if you want to prevent the node IP address from being displayed in CTC to users with Provisioning, Maintenance, or Retrieve security levels. (The IP address suppression is not applied to users with Superuser security level.)
- Forward DHCP Request To—Check this check box to enable Dynamic Host Configuration Protocol (DHCP). Also, enter the DHCP server IP address in the Request To field. The check box is unchecked by default. If you will enable any of the gateway settings to implement the ONS 15310-CL/ONS 15310-MA SOCKS proxy server features, leave this field blank.

**Note** If you enable DHCP, computers connected to an ONS 15310-CL or ONS 15310-MA node can obtain temporary IP addresses from an external DHCP server. The ONS 15310 only forwards DHCP requests; it does not act as a DHCP server.

- CTX CORBA (IIOP) Listener Port—Sets the ONS 15310 IIOP (Internet Inter-Orb Protocol) listener port used for communication between the ONS 15310 and CTC computers. This field is generally not changed unless the ONS 15310 resides behind a firewall that requires a different port. See the "NTP-C22 Set Up the ONS 15310-CL or ONS 15310-MA for Firewall Access" procedure on page 4-8 for more information.
- Gateway Settings—Provisions the ONS 15310-CL or ONS 15310-MA SOCKS proxy server features. Do not select any of these options until you review the SOCKS proxy server scenario in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. In SOCKS proxy server networks, the ONS 15310 is either an external network element (ENE), a gateway network element (GNE), or a proxy-only server. Provisioning must be consistent for each NE type.
- Enable SOCKS proxy server on port—If checked, the ONS 15310-CL or ONS 15310-MA serves as a proxy for connections between CTC clients and ONS 15310 nodes that are DCC-connected to the proxy ONS 15310. The CTC client establishes connections to data communications channel (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 15310. 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 set the node as an ENE or a GNE:
  - External Network Element (ENE)—Choose this option when the ONS 15310 is not connected to a LAN but has DCC connections to other ONS nodes. A CTC computer connected to the ENE through the CRAFT or LAN port can manage nodes that have DCC connections to the ENE. However, the CTC computer does not have direct IP connectivity to these nodes or to any LAN/WAN that those nodes might be connected to.
  - Gateway Network Element (GNE)—Choose this option when the ONS 15310 is connected to a LAN and has DCC connections to other nodes. A CTC computer connected to the LAN can manage all nodes that have DCC connections to the GNE, but the CTC computer does not have direct IP connectivity to them. The GNE option isolates the LAN from the DCC network so that IP traffic originating from the DCC-connected nodes and any CTC computers connected to them is prevented from reaching the LAN.
  - SOCKS Proxy-Only—Choose this option when the ONS 15310 is connected to a LAN and the LAN is separated from the node by a firewall. The SOCKS Proxy Only is the same as the GNE option, except the SOCKS Proxy Only option does not isolate the DCC network from the LAN. Click **Apply**.

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

The 15310-CL-CTX or CTX2500 reboots, which takes 4 to 6 minutes. Eventually, a "Lost node connection, switching to network view" message appears.

**Step 4** Click **OK**. The network view appears. The node icon is displayed in gray, during which time you cannot access the node.

**Step 5** Double-click the node icon when it becomes green.

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

## DLP-C40 Create a Static Route

| | |
|---|---|
| **Purpose** | This task creates a static route to establish CTC connectivity to a computer on another network. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | Required if either of the following is true:<br>• CTC computers on one subnet need to connect to ONS 15310-CL or ONS 15310-MA nodes that are connected by a router to ONS 15310 nodes residing on another subnet. OSPF is not enabled and the External Network Element gateway setting is not checked.<br>• You need to enable multiple CTC sessions among ONS 15310-CL and ONS 15310-MA nodes residing on the same subnet and the External Network Element gateway setting is not enabled. |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Click **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 the destination is a host route (that is, one CTC computer), enter a 32-bit subnet mask (255.255.255.255). If the destination is a subnet, adjust the subnet mask accordingly, for example, 255.255.255.0. If the 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 15310-CL or ONS 15310-MA and the computer.

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

**Note** Static route networking examples are provided in the “Management Network Connectivity” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

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

# DLP-C41 Set Up or Change Open Shortest Path First Protocol

| | |
|---|---|
| **Purpose** | This task enables the Open Shortest Path First (OSPF) routing protocol on the ONS 15310-CL or ONS 15310-MA. Perform this task if you want to include the ONS 15310 in OSPF-enabled networks. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>You will need the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) provisioned on the router that the ONS 15310 is connected to. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** On 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 15310 nodes as a unique OSPF area ID. It can be any number between 000.000.000.000 and 255.255.255.255. The number must be unique to the LAN OSPF area.
- SDCC Metric—This value is normally unchanged. It sets a cost for sending packets across the DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default SDCC metric is 100.
- LDCC Metric—Sets a cost for sending packets across the Line DCC. This value should always be lower than the SDCC metric. The default LDCC metric is 33. It is usually not changed.

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

- OSPF active on LAN—When checked, enables the ONS 15310-CL or ONS 15310-MA OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15310 nodes 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 15310-CL or ONS 15310-MA is connected. (This number is different from the DCC 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** Verify that the OSPF priority and intervals settings match the priority and interval settings used by the OSPF router where the ONS 15310-CL or ONS 15310-MA is connected. If not, change the settings, as needed.

- 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 outside an OSPF area border. One ONS 15310 in the ONS 15310 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 15310 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 15310-CL or ONS 15310-MA nodes that reside within the OSPF area. For example, if the ONS 15310 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 15310-CL or ONS 15310-MA nodes. 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.
- Mask—The static route subnet mask value.
- Advertise—Check if you want to advertise the OSPF range table.

**c.** Click **OK**.

**Step 7** If the ONS 15310-CL or ONS 15310-MA 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 15310 OSPF area):

- Neighbor—The router ID of the Area 0 router.

- Transmit Delay (sec)—The service speed. One second is the default.
- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten 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.
- Auth Type—If the router where the ONS 15310-CL or ONS 15310-MA is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- Auth Key—If authentication type is set to Simple Password, the authentication key (password) is listed here.

**c.** Click **OK**.

**Step 8** After entering ONS 15310-CL or ONS 15310-MA OSPF area data, click **Apply**.

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

# DLP-C42 Set Up or Change Routing Information Protocol

| | |
|---|---|
| **Purpose** | This task enables Routing Information Protocol (RIP) on the ONS 15310-CL or ONS 15310-MA. Perform this task if you want to include the node in RIP-enabled networks. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>You need to create a static route to the router adjacent to the ONS 15310-CL or ONS 15310-MA if the ONS 15310 needs to communicate its routing information to non-DCC-connected nodes. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Check the **RIP Active** check box if you are activating RIP.

**Step 3** Choose either RIP Version 1 or RIP Version 2 from the drop-down list, depending on which version is supported in your network.

**Step 4** Set the RIP metric. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

**Step 5** By default, RIP is set to No Authentication. If the router that the ONS 15310-CL or ONS 15310-MA is connected to requires authentication, complete the following steps. If not, continue with Step 6.

**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 6** If you want to complete an address summary, complete the following steps. If not, continue with Step 7. Complete the address summary only if the ONS 15310-CL or ONS 15310-MA is a GNE with multiple ONS 15310 ENEs attached with IP addresses in different subnets.

a. In the RIP Address Summary area, click **Create**.

b. In the Create Address Summary dialog box, complete the following:

- Summary Address—Enter the summary IP address.
- Mask Length—Enter the subnet mask length using the up and down arrows.
- Cost—The RIP Priority level. The smaller the number, the higher the priority.

c. Click **OK.**

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

# DLP-C43 Provision the IIOP Listener Port on the ONS 15310-CL or ONS 15310-MA

| | |
|---|---|
| **Purpose** | This task sets the IIOP listener port on the ONS 15310-CL or ONS 15310-MA, which enables you to access ONS 15310 nodes that reside behind a firewall. |
| **Tools/Equipment** | IIOP listener port number provided by your LAN or firewall administrator |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

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

**Step 2** In the CTX CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - CTX Fixed—Select this option if the ONS 15310-CL or ONS 15310-MA nodes are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the listener port to Port 57790. It can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Select this option to use Port 683, the CORBA default port number, as the listener port.
- Other Constant—If Port 683 is not used, type the IIOP port specified by your firewall administrator.

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

**Step 4** When the Change Network Configuration message appears, click **Yes**.

The 15310-CL-CTX or CTX2500 card reboots. The reboot takes approximately 4 to 6 minutes.

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

# DLP-C44 Provision the IIOP Listener Port on the CTC Computer

| | |
|---|---|
| **Purpose** | This task selects the IIOP listener port on CTC. |
| **Tools/Equipment** | IIOP listener port number provided by your LAN or firewall administrator |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

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

**Step 3** In the TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- Default - Variable—Select this option if the ONS 15310-CL or ONS 15310-MA nodes are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the CTX listener port to Port 57790. It can be used for access through a firewall if Port 57790 is open.
- Standard Constant—Select this option to use Port 683, the CORBA default port number, as the CTC computer listener port.
- Other Constant—If Port 683 is not used, enter the IIOP port provided by your administrator. Unavailable ports are listed in the "Management Network Connectivity" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

**Step 4** Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.

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

**Step 6** To access the ONS 15310-CL or ONS 15310-MA using the IIOP port, log out of CTC by choosing Exit from the File menu.

**Step 7** Log back into CTC. See the "DLP-C29 Log into CTC" task on page 17-44 for instructions.

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

# DLP-C45 Set Up External or Line Timing

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

**Step 1** In the 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 15310-CL or ONS 15310-MA derives its timing from a BITS source wired to the port on the 15310; choose **Line** if timing is derived from the OC-N, DS1-28, or DS1-84 port. A third option, Mixed, allows you to set external and line timing references.

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

- SSM Message Set—Choose a synchronization status messaging (SSM) message set. All ONS 15310-CL and ONS 15310-MA nodes can translate Generation 2 message sets, so choose Generation 2 if the ONS 15310 is connected to other ONS 15310 nodes. Choose Generation 1 only when the ONS 15310 is connected to equipment that does not support Generation 2. If a node that has its SSM Message Set set to Generation 1 receives a Generation 2 message, it maps the message down to the next available Generation 1 message. The transit node clock (TNC) and ST3E become an ST3.
- Quality of RES—If your timing source supports the reserved S1 byte, set the timing quality here. (Most timing sources do not use RES.) Qualities are displayed in descending quality order as ranges. For example, ST3<RES<ST2 means the timing reference is higher than a Stratum 3 and lower than a Stratum 2. Refer to the "Timing" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- Revertive—Check this check box if you want the ONS 15310-CL or ONS 15310-MA to revert 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, choose the amount of time the ONS 15310-CL or ONS 15310-MA will wait before reverting to its primary timing source. Five minutes is the default.

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

**Note** You can define up to three timing references for the node and up to three BITS-1 Out references. BITS-1 Out reference defines the timing reference used by equipment that can be attached to the node's BITS Out connection. If you attach equipment to the BITS Out connection, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference—Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. The internal clock is the Stratum 3 clock provided on the 15310-CL-CTX or the CTX2500. The options displayed depend on the Timing Mode setting.
- If the Timing Mode is set to External, your options are BITS1 and Internal Clock.
- If the Timing Mode is set to Line, your options are the 15310-CL-CTX or the CTX2500 and Internal Clock. Choose the port that is directly or indirectly connected to the node wired to the BITS source, that is, the BITS port on the ONS 15310-CL or ONS 15310-MA. Set Reference 1 to the port that is closest to the BITS source. For example, if the DS1 port is connected to the node wired to the BITS source, choose Slot 2 (CTX), Port 1 (DS1) as Reference 1.
- If the Timing Mode is set to Mixed, both BITS and the 15310-CL-CTX or CTX2500 are available, allowing you to set a mixture of external BITS and the CTX as timing references.
- BITS-1 Out—Define the timing references for equipment wired to the BITS Out connection on the 15310-CL-CTX or CTX2500. BITS-1 Out is enabled when BITS-1 facilities are put in service. If Timing Mode is set to external, choose the port used to set the timing. If Timing Mode is set to Line, you can choose a port or choose NE Reference to have the BITS-1 Out follow the same timing references as the NE.

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

**Note** Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for timing-related alarms.

**Step 5** In the node view, click the **Provisioning > Timing > BITS Facilities** tabs.

**Step 6** In the BITS Facilities area, complete the following information:

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

- BITS In Facility Type—Provisions the BITS In facility type (DS1).
- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 to **IS** (in service) if the BITS input port is connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).
- BITS Out Facility Type—Provisions the BITS Out facility type (DS1).
- BITS Out State—If equipment is connected to the node's BITS output pins and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 to **IS**, if the BITS Out connection is used for the external equipment. If equipment is not attached to the BITS output connector, set the BITS Out State to **OOS**.

**Step 7** If the state is set to OOS, continue with Step 8. If the state is set to IS, complete the following information:

- Coding—Choose the coding used by your BITS reference, either B8ZS (binary 8-zero substitution) or AMI (alternate mark inversion).
- Framing—Choose the framing used by your BITS reference, either ESF (Extended Super Frame) or SF (D4) (Super Frame).

- Sync Messaging—Check this check box to enable SSM. SSM is not available if Framing is set to Super Frame.
- AIS Threshold—If SSM is disabled or Super Frame is used, choose the quality level where a node sends an alarm indication signal (AIS) from the BITS 1 Out pins. An AIS alarm is raised when the optical source for the BITS reference falls to or below the SSM quality level defined in this field.
- LBO—If you are timing an external device connected to the BITS Out pins, choose the distance between the device and the ONS 15310-CL/ONS 15310-MA. Options are: 0-133 ft. (default), 124-266 ft., 267-399 ft., 400-533 ft., and 534-655 ft. Line build out (LBO) relates to the BITS cable length.

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

## DLP-C46 Set Up Internal Timing

| | |
|---|---|
| **Purpose** | This task sets up internal Stratum 3 timing for an ONS 15310-CL or ONS 15310-MA. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed (use only if a BITS source is not available) |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Caution** Internal timing is Stratum 3 and not intended for permanent use. All ONS 15310-CL or ONS 15310-MA nodes should be timed to a Stratum 2 or better primary reference source.

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

**Step 2** In the General Timing area, enter the following:

- Timing Mode—Set to External.
- SSM Message Set—Set to Generation 1.
- Quality of RES—Not relevant to internal timing; ignore this field.
- Revertive—Not relevant to internal timing; ignore this field.
- Reversion Time—Not relevant to internal timing; ignore this field.

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

- NE Reference
  - Ref 1—Set to Internal Clock.
  - Ref 2—Set to Internal Clock.
  - Ref 3—Set to Internal Clock.
- BITS 1 Out—Set to None.

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

**Step 5** In node view, click the **Provisioning > Timing > BITS Facilities** tabs.

**Step 6** In the BITS In State drop-down list, change State to **OOS**. Disregard the other BITS Facilities settings; they are not relevant to internal timing.

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

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

# DLP-C47 Provision a Proxy Tunnel

| | |
|---|---|
| **Purpose** | This task sets up a proxy tunnel to communicate with a non-ONS far-end node. Proxy tunnels are only necessary when the SOCKS proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 proxy server tunnels. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>DLP-C52 Provision Section DCC Terminations, page 17-68 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

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

**Step 1** Click the **Provisioning > Network > Proxy** subtabs.

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

**Step 3** In the Create Tunnel dialog box, complete the following:

- Source Address—Type the IP address of the source node (32 bit length) or source subnet (any other length).
- Source Length—Choose the length of the source subnet mask.
- Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
- Destination Length—Choose the length of the destination subnet mask.

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

**Step 5** Continue with your originating procedure (NTP).

# DLP-C48 Provision a Firewall Tunnel

| | |
|---|---|
| **Purpose** | This task provisions destinations that will not be blocked by the firewall. Firewall tunnels are only necessary when the SOCKS proxy server is enabled and a foreign DCC termination exists, or if static routes exist so that the DCC network is used to access remote networks or devices. You can provision a maximum of 12 firewall tunnels. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>DLP-C52 Provision Section DCC Terminations, page 17-68 or<br>DLP-C40 Create a Static Route, page 17-55 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

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

**Step 1** Click the **Provisioning > Network > Firewall** subtabs.

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

**Step 3** In the Create Tunnel dialog box, complete the following:

- Source Address—Type the IP address of the source node (32-bit length) or source subnet (any other length).
- Source Length—Choose the length of the source subnet mask.
- Destination Address—Type the IP address of the destination node (32 bit length) or destination subnet (any other length).
- Destination Length—Choose the length of the destination subnet mask.

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

**Step 5** Continue with your originating procedure (NTP).

# DLP-C49 Create a Provisionable Patchcord

| | |
|---|---|
| **Purpose** | This task creates a provisionable patchcord, also called a virtual link. Patchcords are used for network communication when a DCC/GCC is not available. They appear as dashed lines in CTC network view.<br>For the specific situations in which a patchcord is necessary, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. |
| **Tools/Equipment** | For for information about patchcords, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** To set up a provisionable patchcord between an optical port and an ONS node transponder/muxponder, an add/drop multiplexer, or multiplexer/demultiplexer port, the optical port must have an SDCC/LDCC termination provisioned. If the port is the protection port in a 1+1 group, the working port must have an SDCC/LDCC termination provisioned. As needed, complete the "DLP-C52 Provision Section DCC Terminations" task on page 17-68.

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

**Step 1** In node view, click the **Provisioning > Comm Channels > PPCs** tabs. If you are in network view, click the **Provisioning > Provisionable Patchcords (PPC)** tabs.

**Step 2** Click **Create**. The Provisionable Patchcord dialog box appears.

**Step 3** In the Origination Node area, complete the following:

a. If you are in node view, the Origination Node defaults to the current node. If you are in network view, click the desired origination node from the drop-down list.

b. Type a patchcord identifier (0 through 32767) in the TX/RX ID field.

c. Click the desired origination slot/port from the list of available slots/ports.

**Step 4** In the Termination Node area, complete the following:

a. Click the desired termination node from the drop-down list. If the remote node has not previously been discovered by CTC but is accessible by CTC, type the name of the remote node.

b. Type a patchcord identifier (0 through 32767) in the TX/RX ID field. The origination and termination IDs must be different if the patchcord is set up between two cards on the same node.

c. Click the desired termination slot/port from the list of available slots/ports. The origination port and the termination port must be different.

**Step 5** If you need to provision Tx and Rx separately for multiplexer/demultiplexer cards, check the **Separate Tx/Rx** check box. If not, continue with Step 6. The origination and termination TX ports are already provisioned. Complete the following to provision the RX ports:

a. In the Origination Node area, type a patchcord identifier (0 through 32767) in the RX ID field. The origination Tx and Rx and termination Tx and Rx IDs must be different.

b. Click the desired origination slot/port from the list of available slots/ports.

c. In the Termination Node area, type a patchcord identifier (0 through 32767) in the RX ID field. The origination Tx and Rx and termination Tx and Rx IDs must be different.

d. Click the desired termination slot/port from the list of available slots/ports.

**Step 6** Click **OK**.

**Step 7** If you provisioned a patchcord on a port in a 1+1 protection group, a dialog box appears to ask if you would like to provision the peer patchcord. Click **Yes**. Repeat Steps 3 through 6.

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

## DLP-C50 Change the Service State for a Port

| | |
|---|---|
| **Purpose** | This task puts a port in service or removes a port from service. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** On the node view shelf graphic, double-click the card that contains the ports that you want to put in or out of service. The card view appears.

**Step 2** Click the **Provisioning > DS1**, **DS3**, **EC1**, or **Optical** tabs.

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

- **IS**—Puts the port in the In-Service and Normal (IS-NR) service state.
- **OOS,DSBLD**—Puts the port in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. In this service state, traffic is not passed on the port until the service state is changed to IS-NR; Out-of-Service and Management, Maintenance (OOS-MA,MT); or Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS).
- **OOS,MT**—Puts the port in the OOS-MA,MT service state. This service state does not interrupt traffic flow and loopbacks are allowed, but alarm reporting is suppressed. Raised fault conditions, whether or not their alarms are reported, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use the OOS-MA,MT service state for testing or to suppress alarms temporarily. Change to the IS-NR or OOS-AU,AINS service states when testing is complete.
- **IS,AINS**—Puts the port in the OOS-AU,AINS service state. In this service state, alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. After the soak period passes, the port changes to IS-NR. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command.

**Note** CTC will not allow you to change a port service state from IS-NR to OOS-MA,DSBLD. You must first change a port to the OOS-MA,MT service state before putting it in the OOS-MA,DSBLD service state.

For more information about port service states, refer to the "Administrative and Service States" appendix of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

**Step 4** If the port is in loopback (OOS-MA,LPBK & MT) and you set the Admin State to IS, a confirmation window displays indicating that the loopback will be released and that the action could be service affecting. To continue, click **Yes**.

**Step 5** If you set the Admin State to IS,AINS, set the soak period time in the AINS Soak field. This is the amount of time that the port will stay in the OOS-AU,AINS service state after a signal is continuously received. When the soak period elapses, the port changes to the IS-NR service state.

**Note** A continuously valid signal must be received for the duration of the soak period before the OOS-AU,AINS port makes a transition to the IS-NR state. For example, if the soak timer is set for eight hours, and you receive an error after two hours, the timer is reset for another eight-hour period. This cycle continues until an error-free signal is received for an eight-hour period.

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

**Step 7** As needed, repeat this task for each port.

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

# DLP-C52 Provision Section DCC Terminations

| | |
|---|---|
| **Purpose** | This task creates the SONET Data Communications Channel (DCC) terminations required for alarms, administration, data, signal control information, and messages. In this task, you can also set up the node so that it has direct IP access to a far-end non-ONS node over the DCC network. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the "DLP-C67 Create a DCC Tunnel" task on page 17-84 to create a DCC tunnel.

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

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

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

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

**Note** SDCC refers to the Section DCC, which is used for ONS 15310-CL or ONS 15310-MA DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS 15310-CL or ONS 15310-MA) can be provisioned as DCC tunnels. See the "DLP-C67 Create a DCC Tunnel" task on page 17-84.

**Step 4** In the Port Admin State area, click the **Set to IS** radio button.

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

**Step 6** If the SDCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end. To change the default to a specific the IP address, see the "DLP-C152 Change a Section DCC Termination" task on page 18-55.

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

- Check the IP box only—if the SDCC is between the ONS 15310-CL or ONS 15310-MA and another ONS node and only ONS nodes reside on the network. The SDCC will use PPP (point-to-point protocol).
- Check the IP and OSI boxes—if the SDCC is between the ONS 15310-CL or ONS 15310-MA and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The SDCC will use PPP.
- Check OSI box only—if the SDCC is between an ONS node and a third party NE that uses the OSI protocol stack. The SDCC will use the LAP-D protocol.

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

**Step 8** If you checked OSI, complete the following steps. If you checked IP only, continue with Step 9.

a. Click **Next**.

b. Provision the following fields:

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

c. If the OSI and IP boxes are checked, continue with Step 9. If only the OSI is checked, click **Next** and provision the following fields:

- Mode

  AITS—(Default) Acknowledged Information Transfer Service. Does not exchange data until a logical connection between two LAP-D users is established. This service provides reliable data transfer, flow control, and error control mechanisms.

  UITS—Unacknowledged Information Transfer Service. Transfers frames containing user data with no acknowledgement. The service does not guarantee that the data presented by one user will be delivered to another user, nor does it inform the user if the delivery attempt fails. It does not provide any flow control or error control mechanisms.
- Role—Set to the opposite of the mode of the NE at the other end of the SDCC.
- MTU—Maximum transmission unit. Sets the maximum number of octets in a LAP-D information frame. The range is 512 to 1500 octets. The default is 512. You normally should not change it.
- T200—Sets the time between Set Asynchronous Balanced Mode (SABME) frame retransmissions. The default is 0.2 seconds. The range is 0.2 to 20 seconds.
- T203—Provisions the maximum time between frame exchanges, that is, the trigger for transmission of the LAP-D “keep-alive” Receive Ready (RR) frames. The default is 10 seconds. The range is 4 to 120 seconds.

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

**Note** EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms are present until you create all network DCC terminations and put the DCC termination optical ports in service.

**Note** There are four possibilities for the appearance of DCCs: green/solid, green/dashed, gray/solid, gray/dashed. DCC appearance corresponds to the following states: active/routable, active/nonroutable, failed/routable, or failed/nonroutable. Circuit provisioning uses active/routable links. Selecting a node or span in the graphic area displays information about the node and span in the status area.

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

# DLP-C53 Provision Line DCC Terminations

| | |
|---|---|
| **Purpose** | This task creates the Line Data Communications Channel (LDCC) terminations required for alarms, administration, data, signal control information, and messages. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** The SDCCs and LDCCs should not be provisioned between SONET (ANSI) and SDH (ETSI) nodes using CTC or TL1 because they cannot operate between SONET and SDH nodes. These communication channels should be provisioned on similar nodes, such as SONET-to-SONET or SDH-to-SDH. To establish communication channels between SONET and SDH nodes, create a DCC tunnel. See the "DLP-C67 Create a DCC Tunnel" task on page 17-84 to create a DCC tunnel.

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

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

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

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

> **Note** LDCC refers to the Line DCC, which is used for ONS node DCC terminations. The SONET Line DCCs and the Section DCC (when not used as a DCC termination by the ONS node) can be provisioned as DCC tunnels. See the "DLP-C67 Create a DCC Tunnel" task on page 17-84.

**Step 4** In the Port Admin State area, click the **Set to IS** radio button.

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

**Step 6** If the LDCC termination is to include a non-ONS node, check the **Far End is Foreign** check box. This automatically sets the far-end node IP address to 0.0.0.0, which means that any address can be specified by the far end.

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

- Check the IP box only—if the LDCC is between the ONS 15310-CL/ONS 15310-MA and another ONS node and only ONS nodes reside on the network. The LDCC will use PPP (point-to-point protocol).
- Check the IP and OSI boxes—if the LDCC is between the ONS 15310-CL/ONS 15310-MA and another ONS node and third party NEs that use the OSI protocol stack are on the same network. The LDCC will use PPP.

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

**Step 8** If you checked OSI, complete the following steps. If you checked IP only, continue with Step 9.

a. Click **Next**.

b. Provision the following fields:

   - Router—Choose the OSI router
   - ESH—Sets the End System Hello (ESH) propagation frequency. End system NEs transmit ESHs to inform other ESs and ISs about the NSAPs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.

- ISH—Sets the Intermediate System Hello PDU propagation frequency. Intermediate system NEs send ISHs to other ESs and ISs to inform them about the IS NETs it serves. The default is 10 seconds. The range is 10 to 1000 seconds.
- IIH—Sets the Intermediate System to Intermediate System Hello PDU propagation frequency. The IS-IS Hello PDUs establish and maintain adjacencies between ISs. The default is 3 seconds. The range is 1 to 600 seconds.
- IS-IS Cost—Sets the cost for sending packets on the LAN subnet. The IS-IS protocol uses the cost to calculate the shortest routing path. The default metric cost for LAN subnets is 20. It normally should not be changed.

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

**Note** EOC (DCC Termination Failure) and LOS (Loss of Signal) alarms are present until you create all network DCC terminations and put the DCC termination optical ports in service.

**Note** There are four possibilities for the appearance of DCCs: green/solid, green/dashed, gray/solid, gray/dashed. DCC appearance corresponds to the following states: active/routable, active/nonroutable, failed/routable, or failed/nonroutable. Circuit provisioning uses active/routable links. Selecting a node or span in the graphic area displays information about the node and span in the status area.

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

# DLP-C54 Optical 1+1 Protection Test

| | |
|---|---|
| **Purpose** | This task verifies that a 1+1 protection group will switch traffic properly. |
| **Tools/Equipment** | The test set specified by the acceptance test procedure. |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44;<br>a test circuit created as part of the topology acceptance test. |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite |
| **Security Level** | Provisioning or higher |

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

**Step 2** Click the **Alarms** tab.

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

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

**Step 3** Click the **Conditions** tab. Verify that the network does not have any unexplained conditions. If unexplained conditions are present, resolve them before continuing. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* if necessary.

**Step 4** On the network map, double-click the node containing the 1+1 protection group you are testing to open the node in node view.

**Step 5** Click the **Maintenance > Protection** tabs.

**Step 6** Initiate a Force switch on the working port:

- **a.** In the Protection Groups area, click the 1+1 protection group.
- **b.** Click the working port. Next to Switch Commands, click **Force**.
- **c.** In the Confirm Force Operation dialog box, click **Yes**.
- **d.** 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 7** Verify that traffic on the test set connected to the node is still running. Some bit errors are normal, but traffic flow should not be interrupted. If a traffic interruption occurs, complete Step 8, then refer to your next level of support. If a traffic interruption does not occur, complete Steps 8 through 12.

**Step 8** Clear the switch on the working port:

- **a.** Next to Switch Commands, click **Clear**.
- **b.** In the Confirm Clear Operation dialog box, click **Yes**.

**Step 9** Initiate a Force switch on the protect port:

- **a.** In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.
- **b.** In the Confirm Force Operation dialog box, click **Yes**.
- **c.** In the Selected Group area, verify that the following appears:

  Protect port - Protect/Active [FORCE_SWITCH_TO_WORKING], [PORT STATE]

  Working port - Working/Standby [FORCE_SWITCH_TO_WORKING], [PORT STATE]

**Step 10** Verify that the traffic on the test set connected to the node is still running. If a traffic interruption occurs, complete Step 11 and then refer to your next level of support. If a traffic interruption does not occur, complete Steps 11 and 12.

**Step 11** Clear the switch on the protect port:

- **a.** Next to Switch Commands, click **Clear**.
- **b.** In the Confirm Clear Operation dialog box, click **Yes**.
- **c.** In the Selected Group area, verify the following states:

  Protect port - Protect/Standby, IS-NR

  Working port - Working/Active, IS-NR

**Step 12** Return to your originating procedure (NTP).

# DLP-C55 Path Protection Switching Test

| | |
|---|---|
| **Purpose** | This task verifies that a path protection span is switching correctly. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | Required |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** 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 a network span and choose **Circuits**.

The Circuits on Span dialog box displays the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

**Step 3** Initiate a Force switch:

a. Click the **Perform path protection span switching** field and choose **FORCE SWITCH AWAY** from the drop-down list.

b. Click **Apply**.

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

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

In the Circuits on Span dialog box, the Switch State for all circuits is Force. Unprotected circuits will not switch.

**Step 4** Clear the Force switch:

a. Click the **Perform Path Protection span switching** field and choose **CLEAR** from the drop-down list.

b. Click **Apply**.

c. Click **Yes** to confirm.

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

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

In the Circuits on Span window, the Switch State for all Path Protection circuits is CLEAR.

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

# DLP-C56 Assign a Name to a Port

| | |
|---|---|
| **Purpose** | This task assigns a name to a port on any ONS 15310-CL or ONS 15310-MA card. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C18 Verify Ethernet Card and SFP Installation for the ONS 15310-CL, page 4-2<br>NTP-C148 Verify Card and SFP Installation for the ONS 15310-MA, page 4-3<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** Double-click the card that has the port you want to provision.

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

**Step 3** Complete the following, as necessary:

- For 15310-CL-CTX DS-1 ports, click the **DS1** subtab.
- For 15310-CL-CTX DS-3 ports, click the **DS3** subtab.
- For 15310-CL-CTX EC-1 ports, click the **EC1** subtab.
- For 15310-CL-CTX OC-N ports, click the **Optical** subtab.
- For CE-100T-8 or ML-100T-8 cards, click the **Ether Ports** or **POS Ports** subtab.

**Step 4** Click the **Port Name** column for the port number you are assigning a name to and enter the desired port name.

The port name can be up to 32 alphanumeric/special characters and is blank by default.

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

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

# DLP-C57 Provision Path Protection Selectors During Circuit Creation

| | |
|---|---|
| **Purpose** | This task provisions path protection selectors during circuit creation. Complete this task only if the circuit will be routed on a path protection configuration. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Circuit Attributes page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 1** In the Circuit Attributes area of the Circuit Creation wizard, set the path protection path selectors:

- Provision working go and return on primary path—Check this box to route the working path on one fiber pair and the protect path on a separate fiber pair. This feature only applies to bidirectional path protection circuits.
- Revertive—Check this check box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If you do not choose Revertive, traffic remains on the protect path after the switch.
- Reversion time—If Revertive is checked, click the Reversion time field and choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
- SF threshold—Set the path protection path-level signal failure (SF) bit error rate (BER) thresholds. VT thresholds only apply to circuits with 15310-CL-CTX or CTX2500 ports as path protection selectors.
- SD threshold—Set the path protection path-level signal degrade BER thresholds. VT thresholds only apply to circuits with 15310-CL-CTX or CTX2500 ports as path protection selectors.
- Switch on PDI-P—For STS circuits, check this check box if you want traffic to switch when an STS payload defect indicator is received. Unavailable for VT circuits.

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

# DLP-C58 Provision a DS-1 Circuit Source and Destination

| | |
|---|---|
| **Purpose** | This task provisions an electrical circuit source and destination for a DS-1 circuit. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Circuit Source page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 1** From the Node drop-down list, choose the node where the source will originate.

**Step 2** From the Slot drop-down list, choose the slot where the circuit will originate.

**Step 3** From the Port drop-down list, choose **DS1**.

**Step 4** If you are creating a VT circuit, choose the source DS-1 port from the DS-1 drop-down list.

**Step 5** If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Source** and repeat Steps 1 through 4 to define the secondary source. If you do not need to create a secondary source, continue with Step 6.

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

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

**Step 8** From the Slot drop-down list, choose the slot containing the destination card.

**Step 9** Depending on the destination card, choose the destination port, STS, VT, or DS-1 from the drop-down lists that appear based on the card selected in Step 8. See Table 6-2 on page 6-2 for a list of valid options. CTC does not display ports, STSs, VTs, or DS-1s already used by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS-1 simultaneously, one of you will receive a Path in Use error and be unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.

**Step 10** If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 7 through 9 to define the secondary destination.

**Step 11** Click **Next**.

**Step 12** Return to your originating procedure (NTP).

# DLP-C59 Provision STS and VT Grooming Nodes

| | |
|---|---|
| **Purpose** | This task provisions the STS and VT grooming nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard VT Optimization Matrix page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In the Select Optimization area of the VT Matrix Optimization page, choose one of the following:

- Create VT tunnel on transit nodes—This option is available if the circuit passes through a node that does not have a VT tunnel or if an existing VT tunnel is full. VT tunnels allow VT circuits to pass through ONS nodes without consuming cross-connect card resources. VT tunnels can carry 28 VT1.5 circuits. In general, creating VT tunnels is a good idea if you are creating many VT circuits from the same source and destination. Refer to the “Circuits and Tunnels” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information.
- Create VT aggregation point—This option is available if the circuit source or destination is on an OC-N port on a 1+1 or unprotected node. VAPs aggregate circuits onto an STS for handoff to non-ONS networks or equipment, such as an IOF, switch, or digital access and cross-connect system

(DACS). It allows VT1.5 circuits to be routed through the node using one STS connection on the 15310-CL-CTX (cross-connect) card matrix rather than multiple VT connections on the 15310-CL-CTX card VT matrix. If you want to aggregate the circuit you are creating with others onto an STS for transport outside the ONS network, choose one of the following:

  - STS grooming node is *source node*, VT grooming node is *destination node*—Creates the VAP on the circuit source node. This option is available only if the circuit originates on an OC-N port.
  - STS grooming node is *destination node*, VT grooming node is *source node*—Creates the VAP on the circuit destination node. This option is available only if the circuit terminates on an OC-N port.

- None—Choose this option if you do not want to create a VT tunnel or a VAP. This is the only available option if CTC cannot create a VT tunnel or VAP.

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

# DLP-C60 Provision a DS-1, DS-3, or EC-1 Circuit Route

| | |
|---|---|
| **Purpose** | This task provisions the circuit route for manually routed DS-1, DS-3, or EC-1 circuits. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| | The Circuit Creation wizard Route Review and Edit page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields display span information. The source STS and VT appear.

- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination.
- Add one span for all 1+1 portions of the route from the source to the destination.
- For circuits routed on path protection dual ring interconnect topologies, provision the working and protect paths as well as the spans between the DRI nodes.

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

**Step 4** If you want to change the source VT, adjust the Source VT field; otherwise, continue with Step 5.

**Step 5** Repeat Steps 2 through 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

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

# DLP-C61 Provision a DS-3 or EC-1 Circuit Source and Destination

| | |
|---|---|
| **Purpose** | This task provisions an electrical circuit source and destination for a DS-3 or EC-1 circuit. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Circuit Source page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 1** From the Node drop-down list, choose the node where the source will originate.

**Step 2** From the Slot drop-down list, choose the slot where the circuit will originate.

**Step 3** From the Port drop-down list, choose the source port as appropriate.

**Step 4** If you are creating a VT circuit, choose the VT from the VT drop-down list.

**Step 5** If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, click **Use Secondary Source** and repeat Steps 1 through 4 to define the secondary source. If you do not need to create a secondary source, continue with Step 6.

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

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

**Step 8** From the Slot drop-down list, choose the slot containing the destination card.

**Step 9** Depending on the destination card, choose the destination port or STS from the drop-down lists that display based on the card selected in Step 2. See Table 6-2 on page 6-2 for a list of valid options. CTC does not display ports, STSs, VTs, or DS-1s if they are already in use by other circuits. If you and a user working on the same network choose the same port, STS, VT, port, or DS-1 simultaneously, one of you will receive a Path in Use error and be unable to complete the circuit. The user with the incomplete circuit needs to choose new destination parameters.

**Step 10** If you need to create a secondary destination, for example, a path protection bridge/selector circuit exit point in a multivendor path protection configuration, click **Use Secondary Destination** and repeat Steps 7 through 9 to define the secondary destination.

**Step 11** Click **Next**.

**Step 12** Return to your originating procedure (NTP).

## DLP-C62 Provision a VT Tunnel Route

| | |
|---|---|
| **Purpose** | This task provisions the route for a manually routed VT tunnel. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Route Review and Edit page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In the Circuit Creation wizard in the Route Review and Edit area, click the source node icon if it is not already selected. Arrows indicate the available spans for routing the tunnel from the source node.

**Step 2** Click the arrow of the span you want the VT tunnel to travel. The arrow turns white. In the Selected Span area, the From and To fields display the slot and port that will carry the tunnel. The source STS appears.

**Step 3** If you want to change the source STS, change it in the Source STS field; otherwise, continue with the next step.

**Step 4** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

**Step 5** Repeat Steps 3 and 4 until the tunnel is provisioned from the source to the destination node through all intermediary nodes.

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

## DLP-C63 Provision an OC-N Circuit Source and Destination

| | |
|---|---|
| **Purpose** | This task provisions the source and destination cards for an OC-N circuit. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Circuit Source page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | 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 where the circuit originates. (If a card's capacity is fully utilized, it does not appear in the list.)

**Step 3** Depending on the circuit origination card, choose the source port and/or STS from the Port and STS drop-down lists. STSs do not appear if they are already in use by other circuits.

**Step 4** If you are creating a VT circuit, choose the VT from the VT drop-down list.

**Step 5** If you need to create a secondary source, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, 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 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** Depending on the card selected in Step 2, choose the destination port and/or STS from the Port and STS drop-down lists.

**Step 10** If you are creating a VT circuit, choose the VT from the VT drop-down list.

**Step 11** If you need to create a secondary destination, for example, a path protection bridge/selector circuit entry point in a multivendor path protection configuration, 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-C64 Provision an OC-N Circuit Route

| | |
|---|---|
| **Purpose** | This task provisions the circuit route for manually routed OC-N circuits. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Route Review and Edit page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields display span information. The source STS and if applicable, VT appears.

**Step 3** If you want to change the source STS, choose a different STS from the Source STS drop-down list; otherwise, continue with Step 4.

**Step 4** If you want to change the source VT, choose a different VT from the Source VT drop-down list; otherwise, continue with Step 5.

**Step 5** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

**Step 6** Repeat Steps 2 through 5 until the circuit is provisioned from the source to the destination node through all intermediary nodes. If Fully Protect Path is checked on the Circuit Routing Preferences page, you must complete the following:

- Add two spans for all path protection or unprotected portions of the circuit route from the source to the destination.
- Add one span for all 1+1 portions of the route from the source to the destination.

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

# DLP-C65 Provision a VCAT Circuit Source and Destination

| | |
|---|---|
| **Purpose** | This task provisions a VCAT circuit source and destination. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Circuit Source page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | 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 ML-100T-8 or CE-100T-8 card where the circuit will originate. (If a card's capacity is fully utilized, it does not appear in the list.)

**Step 3** Depending on the circuit origination card, choose the source port and/or STS and, if applicable, VT from the Port, STS, and VT drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits or if they are already in use by other circuits.

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

**Step 5** From the Node drop-down list, choose the destination node.

**Step 6** From the Slot drop-down list, choose the slot containing the ML-100T-8 or CE-100T-8 card where the circuit will terminate (destination card). (If a card's capacity is fully utilized, the card does not appear in the list.)

**Step 7** Depending on the card selected in Step 6, choose the source port and/or STS and, if applicable, VT from the Port, STS, and VT drop-down lists. The Port drop-down list is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits. VTs do not appear for STS-V circuits or if they are already in use by other circuits.

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

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

# DLP-C66 Provision a VCAT Circuit Route

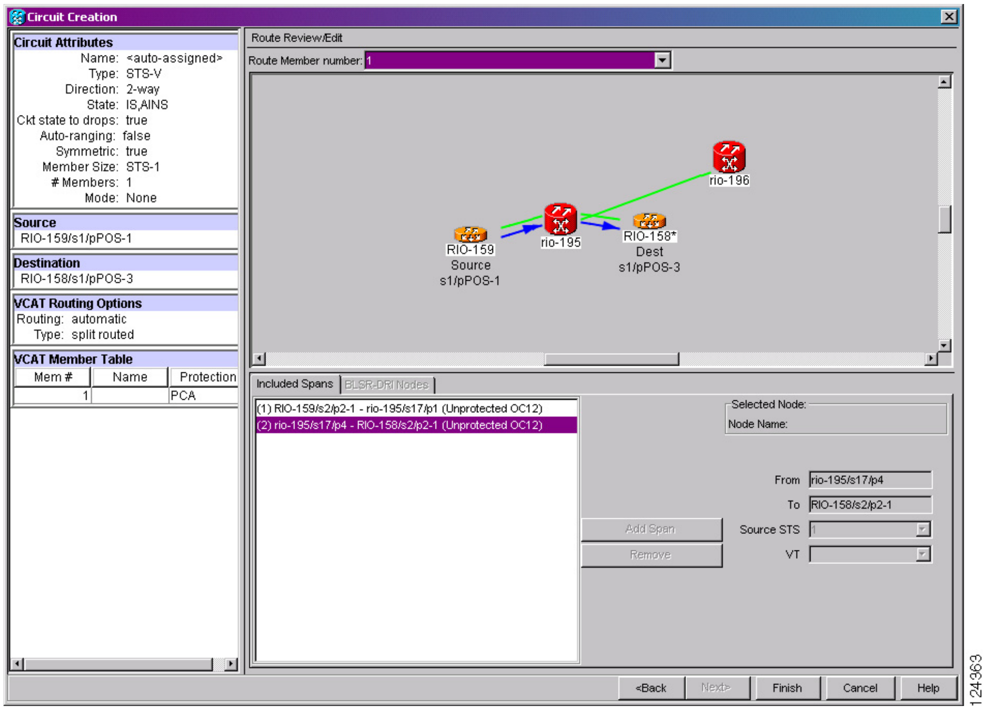
| | |
|---|---|
| **Purpose** | This task provisions the circuit route for manually routed OC-N circuits. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44<br>The Circuit Creation wizard Route Review/Edit page must be open. |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In the Circuit Creation wizard in the Route Review and Edit area, choose the member number from the Route Member Number drop-down list.

**Step 2** Click the source node icon if it is not already selected.

**Step 3** Starting with a span on the source node, click the arrow of the span you want the circuit to travel. The arrow turns white. In the Selected Span area, the From and To fields provide span information. The source STS appears. Figure 17-22 shows an example.

*Figure 17-22 Manually Routing a VCAT Circuit*



Circuit Creation

**Circuit Attributes**

Name: <auto-assigned>
Type: STS-V
Direction: 2-way
State: IS,AINS
Ckt state to drops: true
Auto-ranging: false
Symmetric: true
Member Size: STS-1
# Members: 1
Mode: None

**Source**

RIO-159/s1/pPOS-1

**Destination**

RIO-158/s1/pPOS-3

**VCAT Routing Options**

Routing: automatic
Type: split routed

**VCAT Member Table**

| Mem # | Name | Protection |
|---|---|---|
| 1 | | PCA |

Route Review/Edit

Route Member number: 1

Included Spans

(1) RIO-159/s2/p2-1 - rio-195/s17/p1 (Unprotected OC12)
(2) rio-195/s17/p4 - RIO-158/s2/p2-1 (Unprotected OC12)

Selected Node:
Node Name:

From: rio-195/s17/p4
To: RIO-158/s2/p2-1
Source STS: 1
VT:

**Step 4** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.

**Step 5** Repeat Steps 3 and 4 until the circuit is provisioned from the source to the destination node through all intermediary nodes.

**Step 6** Repeat this task for each member.

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

# DLP-C67 Create a DCC Tunnel

| | |
|---|---|
| **Purpose** | This task creates a DCC tunnel to transport traffic from third-party SONET equipment across ONS networks. Tunnels can be created on the Section DCC (SDCC) channel (D1-D3) (if not used by the ONS 15310-CL/ONS 15310-MA as a terminated DCC), or any Line DCC (LDCC) channel (D4-D6, D7-D9, or D10-D12). |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | NTP-C36 Verify Network Turn-Up, page 6-4<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** Each ONS 15310-CL/ONS 15310-MA can have two DCC tunnel connections. Terminated SDCCs used by the ONS 15310-CL/ONS 15310-MA cannot be used as DCC tunnel endpoints, and an SDCC that is used as a DCC tunnel endpoint cannot be terminated. All DCC tunnel connections are bidirectional.

**Step 1** In network view, click the **Provisioning > Overhead Circuits** tabs.

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

**Step 3** In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Circuit Type—Choose one:
  - **DCC Tunnel-D1-D3**—Allows you to choose either the Section DCC (D1-D3) or a Line DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.
  - **DCC Tunnel-D4-D12**—Provisions the full Line DCC as a tunnel.

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

**Step 5** In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—Section DCC
  - **DCC2 (D4-D6)**—Line DCC 1
  - **DCC3 (D7-D9)**—Line DCC 2
  - **DCC4 (D10-D12)**—Line DCC 3

DCC options do not appear if they are being used by the ONS 15310-CL/ONS 15310-MA (DCC1) or other tunnels.

**Step 6** In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.
- Channel—These options appear if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:
  - **DCC1 (D1-D3)**—Section DCC
  - **DCC2 (D4-D6)**—Line DCC 1
  - **DCC3 (D7-D9)**—Line DCC 2
  - **DCC4 (D10-D12)**—Line DCC 3

DCC options do not appear if they are used by the ONS 15310-CL/ONS 15310-MA (DCC1) or other tunnels.

**Step 7** Click **Finish**.

**Step 8** Put the ports that are hosting the DCC tunnel in service. See the "DLP-C50 Change the Service State for a Port" task on page 17-67 for instructions.

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

# DLP-C68 Create a User Data Channel Circuit

| | |
|---|---|
| **Purpose** | This task creates a user data channel (UDC) circuit on the ONS 15310-CL/ONS 15310-MA. A UDC circuit allows you to create a dedicated data channel between nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C12 Install the UDC Cable on the ONS 15310-CL, page 17-15<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In network view, click the **Provisioning > Overhead Circuits** tabs.

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

**Step 3** In the Overhead Circuit Creation dialog box, complete the following fields in the Circuit Attributes area:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces).
- Type—Choose either **User Data-F1** or **User Data D-4-D-12** from the drop-down list. In the Endpoints area, choose the source and destination nodes and the source and destination OC-N ports and slots from the drop-down lists.

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

**Step 5** In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.

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

**Step 7** In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.

**Step 8** Click **Finish**.

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

## DLP-C69 Create an IP-Encapsulated Tunnel

| | |
|---|---|
| **Purpose** | This task creates an IP-encapsulated tunnel to transport traffic from third-party SONET equipment across ONS networks. IP-encapsulated tunnels are created on the Section DCC channel (D1-D3) (if not used by the ONS node as a terminated DCC). |
| **Tools/Equipment** | OC-N cards must be installed. |
| **Prerequisite Procedures** | NTP-C36 Verify Network Turn-Up, page 6-4<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** Each ONS 15310-CL or ONS 15310-MA can have one IP-encapsulated tunnel. Terminated Section DCCs used by the ONS 15310-CL or ONS 15310-MA cannot be used as tunnel endpoints, and a Section DCC that is used as a tunnel endpoint cannot be terminated. A tunnel connection is 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-C39 Provision IP Settings" task on page 17-53.

**Step 2** In network view, click the **Provisioning > Overhead Circuits** tabs.

**Step 3** Click **Create**.

**Step 4** In the Overhead Circuit Creation dialog box, complete the following in the Circuit Attributes area:

- Name—Type the tunnel name.
- Type—Choose **IP Tunnel-D1-D3**.
- Maximum Bandwidth—Type the percentage of total SDCC bandwidth used in the IP tunnel (the minimum percentage is 10 percent).

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

**Step 6** In the Circuit Source area, complete the following:

- Node—Choose the source node.
- Slot—Choose the source slot.
- Port—If displayed, choose the source port.
- Channel—Displays IPT (D1-D3).

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

**Step 8** In the Circuit Destination area, complete the following:

- Node—Choose the destination node.
- Slot—Choose the destination slot.
- Port—If displayed, choose the destination port.
- Channel—Displays IPT (D1-D3).

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

**Step 10** Put the ports that are hosting the IP-encapsulated tunnel in service. See the "DLP-C50 Change the Service State for a Port" task on page 17-67 for instructions.

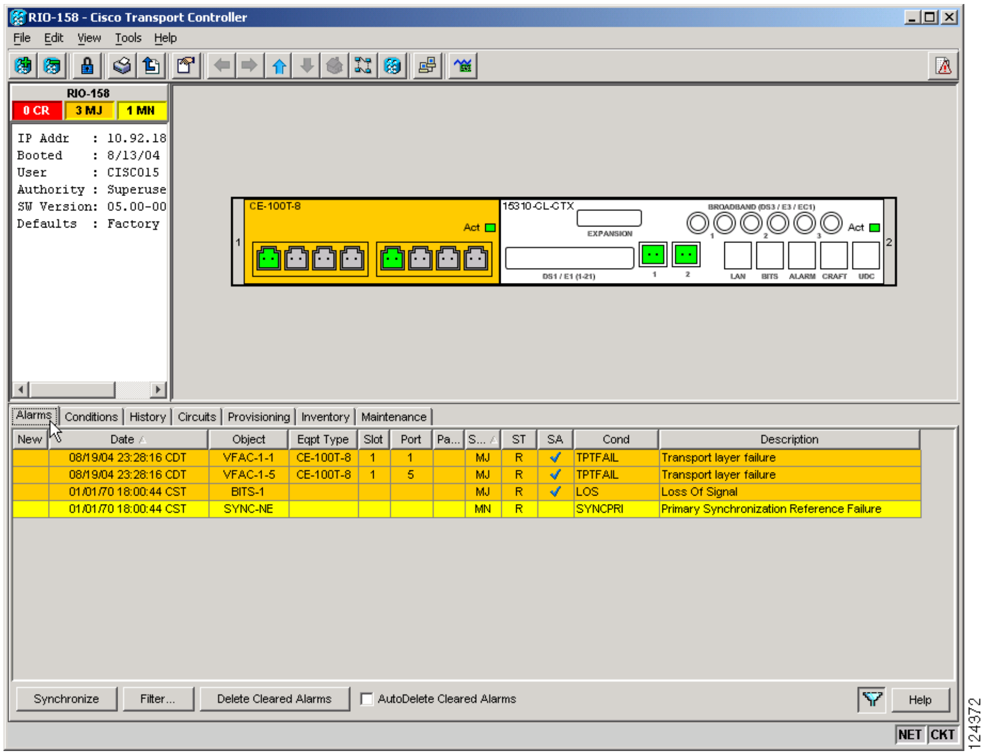
**Step 11** Return to your originating procedure (NTP).

# DLP-C72 View Alarms

| | |
|---|---|
| **Purpose** | This task views current alarms on a card, node, or network. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In the card, node, or network view, click the **Alarms** tab to view the alarms for that card, node, or network (Figure 17-23). The ONS 15310-CL window is shown, and the ONS 15310-MA Alarms window is very similar to it.

*Figure 17-23 ONS 15310-CL Alarms in Node View*



```
IP Addr   : 10.92.18
Booted    : 8/13/04
User      : CISCO15
Authority : Superuse
SW Version: 05.00-00
Defaults  : Factory
```

| New | Date | Object | Eqpt Type | Slot | Port | Pa... | S... | ST | SA | Cond | Description |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 08/19/04 23:28:16 CDT | VFAC-1-1 | CE-100T-8 | 1 | 1 | | MJ | R | ✓ | TPTFAIL | Transport layer failure |
| | 08/19/04 23:28:16 CDT | VFAC-1-5 | CE-100T-8 | 1 | 5 | | MJ | R | ✓ | TPTFAIL | Transport layer failure |
| | 01/01/70 18:00:44 CST | BITS-1 | | | | | MJ | R | ✓ | LOS | Loss Of Signal |
| | 01/01/70 18:00:44 CST | SYNC-NE | | | | | MN | R | | SYNCPRI | Primary Synchronization Reference Failure |

☐ AutoDelete Cleared Alarms

Table 17-6 lists the columns in the Alarms window and their descriptions.

*Table 17-6 Alarm Column Descriptions*

| Column | Information Recorded |
|---|---|
| Num | Sequence number of the original alarm |
| Ref | Reference number of the original alarm |
| New | Indicates a new alarm; to change this status, click either the Synchronize button or the Delete Cleared Alarms button. |
| Date | Date and time of the alarm. |
| Node | The name of the node where the alarm is located. (In dense wavelength-division multiplexing [DWDM] configurations, one node can contain multiple shelves.) Visible in network view. |
| Object | TL1 access identifier (AID) for the alarmed object. Table 17-8 on page 17-89 lists these identifiers. For an STSmon or VTmon, this is the monitored STS or VT object. |
| Eqpt Type | If an alarm is raised on a card, the card type in this slot. |
| Shelf | For DWDM configurations, the shelf where the alarmed object is located. Visible in network view. |
| Slot | If an alarm is raised on a card, the slot where the alarm occurred (appears only in network and node view). |
| Port | If an alarm is raised on a card, the port where the alarm is raised; for STSTerm and VTTerm, the port refers to the upstream card it is partnered with. |

Table 17-6 Alarm Column Descriptions (continued)

| Column | Information Recorded |
|---|---|
| Path Width | Indicates how many STSs are contained in the alarmed path. This information complements the alarm object notation, which is explained in Table 17-8 on page 17-89. |
| Sev | Severity level: CR (Critical), MJ (Major), MN (minor), NA (Not Alarmed), NR (Not Reported). |
| ST | Status: R (raised), C (clear). |
| SA | When checked, indicates a service-affecting alarm. |
| Cond | The error message/alarm name; these names are alphabetically defined in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*. |
| Description | Description of the alarm. |

Table 17-7 lists the color codes for alarm and condition severities.

Table 17-7 Color Codes for Alarms and Condition Severities

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

In network view, CTC identifies STS and VT alarm objects using a TL1-type access identifier (AID). Table 17-8 lists these AIDs.

Table 17-8 STC and VT Alarm Object Identification

| STS and VT Alarm Numbering | |
|---|---|
| **MON Object (Optical)** | **Syntax and Examples** |
| OC3/OC12 STS | Syntax: STS-<Slot>-<Ppm>-<Port>-<STS><br>Ranges: STS-{2}-{1-2}-{1}-{1-*n*[1]}<br>Example: STS-2-1-1-6 |
| OC3/OC12 VT | Syntax: VT1-<Slot>-<Ppm>-<Port>-<STS>-<VT Group>-<VT><br>Ranges: VT1-{2}-{1-2}-{1}-{1-*n*[1]}-{1-7}-{1-4}<br>Example: VT1-2-1-1-6-1-1 |
| EC1 STS | Syntax: STS-<Slot>-<Port>-<STS><br>Ranges: STS-{2}-{1-3}-{1-*n*[1]}<br>Example: STS-2-1-6 |

*Table 17-8 STC and VT Alarm Object Identification (continued)*

| STS and VT Alarm Numbering | |
|---|---|
| **MON Object (Optical)** | **Syntax and Examples** |
| EC1 VT | Syntax: VT1-<Slot>-<Port>-<STS>-<VT Group>-<VT><br>Ranges: VT1-{2}-{1-3}-{1-*n*[1]}-{1-7}-{1-4}<br>Example: VT1-2-1-6-1-1 |
| **TERM Object (Electrical)** | **Syntax and Examples** |
| T1 STS | Syntax: STS-<Slot>-<STS><br>Ranges: STS-{2}-{1-*n*[1]}<br>Example: STS-2-6 |
| T1 VT | Syntax: VT1-<Slot>-<STS>-VT Group>-<VT><br>Ranges: VT1-{2}-{1-*n*[1]}-{1-7}-{1-3}<br>Example: VT1-2-6-1-1 |
| T3 STS | Syntax: STS-<Slot>-<Port>-<STS><br>Ranges: STS-{2}-{1-3}-{1-*n*[1]}<br>Example: STS-2-1-6 |
| T3 VT | VT not supported |

[1] Maximum STS number depends on the rate and size of the STS.

**Step 2** If alarms are present, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* for information and troubleshooting procedures.

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

# DLP-C73 View Alarm or Event History

| | |
|---|---|
| **Purpose** | This task views past cleared and uncleared ONS 15310-CL or ONS 15310-MA alarm messages at the card, node, or network level. This task is useful for troubleshooting configuration, traffic, or connectivity issues that are indicated by alarms. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** To view node alarm history, proceed to Step 2. To view network alarm history, proceed to Step 3. To view card alarm history, proceed to Step 4.

**Step 2** To view node alarm history:

a. Click the **History > Session** tabs to view the alarms and conditions (events) raised during the current session.

b. Click the **History > Shelf** tabs to view the alarm and condition history for the node.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

c. Click **Retrieve** to view all available messages for the History > Shelf tabs.

**Note** Alarms can be unreported when they are filtered out of the display using the **Filter** button in either tab. See the "DLP-C84 Enable Alarm Filtering" task on page 17-104 for information.

**Tip** Double-click an alarm in the alarm table or an event (condition) message in the history table to display the view that corresponds to the alarm message. 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.

**Step 3** To view network alarm history, from node view:

a. From the **View menu choose Go to Network View**.

b. Click the **History** tab.

Alarms and conditions (events) raised during the current session appear.

**Step 4** To view card alarm history from node view:

a. From the View menu choose **Go to Previous View**.

b. Double-click a card on the shelf graphic to display the card-level view.

c. Click the **History > Session** tab to view the alarm messages raised during the current session.

d. Click the **History > Card** tab to retrieve all available alarm messages for the card and click **Retrieve**.

If you check the **Alarms** check box, the node's alarm history appears. If you check the **Events** check box, the node's Not Alarmed and transient event history appears. If you check both check boxes, you will retrieve node history for both alarms and events.

**Note** The ONS 15310-CL and ONS 15310-MA can store up to 640 critical alarm messages, 640 major alarm messages, 640 minor alarm messages, and 640 condition messages. When any of these limits is reached, the oldest events in that category are discarded.

Raised and cleared alarm messages (and events, if selected) appear.

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

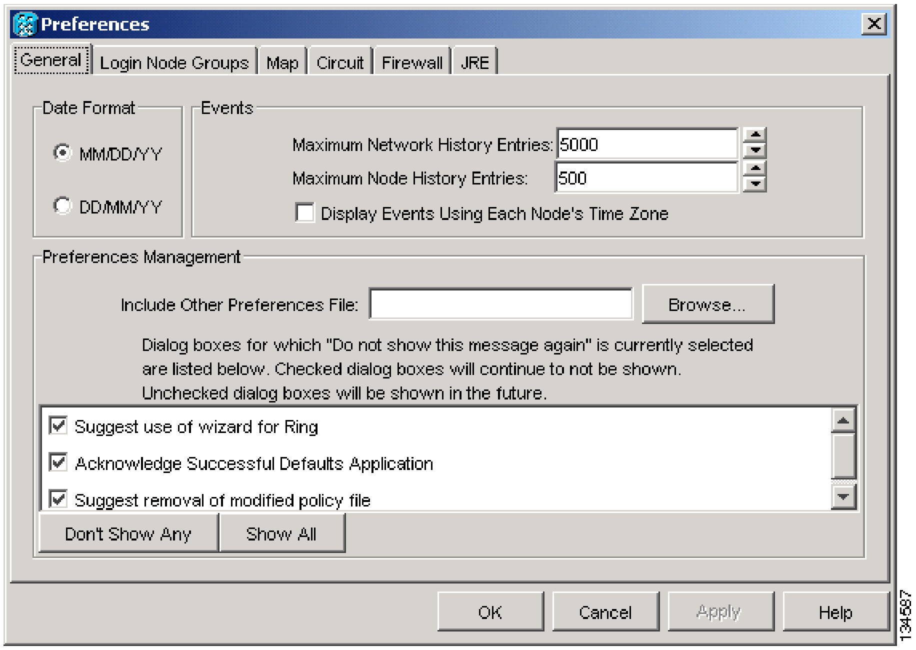
# DLP-C74 Change the Maximum Number of Session Entries for Alarm History

| | |
|---|---|
| **Purpose** | This task changes the maximum number of session entries included in the alarm history. Use this task to extend the history list in order to save information for future reference or troubleshooting. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

The CTC Preferences Dialog box appears (Figure 17-24).

*Figure 17-24 CTC Preferences Dialog Box*



Date Format

● MM/DD/YY

○ DD/MM/YY

Events

Maximum Network History Entries: 5000

Maximum Node History Entries: 500

□ Display Events Using Each Node's Time Zone

Preferences Management

Include Other Preferences File:

Dialog boxes for which "Do not show this message again" is currently selected are listed below. Checked dialog boxes will continue to not be shown. Unchecked dialog boxes will be shown in the future.

☑ Suggest use of wizard for Ring

☑ Acknowledge Successful Defaults Application

☑ Suggest removal of modified policy file

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

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

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

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

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

## DLP-C75 Display Alarms and Conditions Using Time Zone

| | |
|---|---|
| **Purpose** | This task changes the time stamp for events to the time zone of the ONS 15310-CL or ONS 15310-MA node reporting the alarm. By default, the events time stamp is set to the time zone for the CTC workstation. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

The CTC Preferences Dialog box appears (Figure 17-24).

**Step 2** Check 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-C76 Synchronize Alarms

| | |
|---|---|
| **Purpose** | This task is used to view ONS 15310-CL and ONS 15310-MA events at the card, node, or network level and to refresh the alarm listing so that you can check for new and cleared alarms and conditions. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

**Step 2** Click **Synchronize**.

This button causes CTC to retrieve a current alarm summary for the card, node, or network. This step is optional because CTC updates the Alarms window automatically as messages arrive from the node.

Alarms that have been raised during the session will have a check mark in the Alarms window New column. When you click Synchronize, the check mark disappears.

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

# DLP-C77 View Conditions

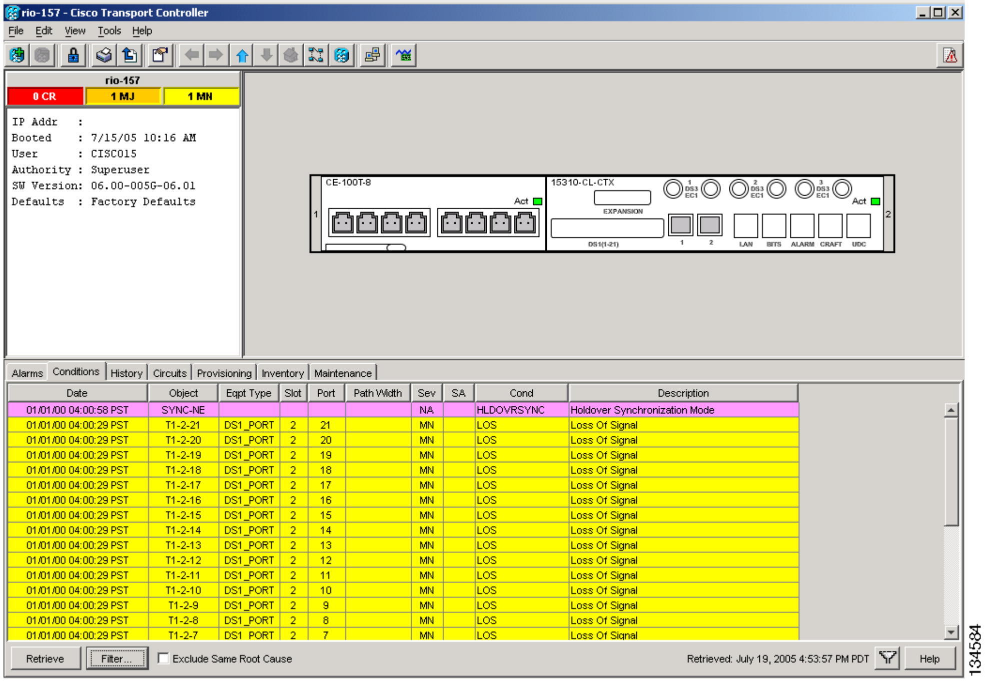
| | |
|---|---|
| **Purpose** | This task is used to view conditions [events with a Not-Reported (NR) severity] at the card, node, or network level. Conditions give you a clear record of changes or events that do not result in alarms. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

**Step 2** Click **Retrieve** (Figure 17-25).

The Retrieve button requests the current set of fault conditions from the node, card, or network. The window is not updated when conditions change on the node. You must click Retrieve to see any changes.

*Figure 17-25 ONS 15310-CL Node View Conditions Window*



```
IP Addr   :
Booted    : 7/15/05 10:16 AM
User      : CISCO15
Authority : Superuser
SW Version: 06.00-005G-06.01
Defaults  : Factory Defaults
```

| Date | Object | Eqpt Type | Slot | Port | Path Width | Sev | SA | Cond | Description |
|---|---|---|---|---|---|---|---|---|---|
| 01/01/00 04:00:58 PST | SYNC-NE | | | | | NA | | HLDOVRSYNC | Holdover Synchronization Mode |
| 01/01/00 04:00:29 PST | T1-2-21 | DS1_PORT | 2 | 21 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-20 | DS1_PORT | 2 | 20 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-19 | DS1_PORT | 2 | 19 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-18 | DS1_PORT | 2 | 18 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-17 | DS1_PORT | 2 | 17 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-16 | DS1_PORT | 2 | 16 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-15 | DS1_PORT | 2 | 15 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-14 | DS1_PORT | 2 | 14 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-13 | DS1_PORT | 2 | 13 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-12 | DS1_PORT | 2 | 12 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-11 | DS1_PORT | 2 | 11 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-10 | DS1_PORT | 2 | 10 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-9 | DS1_PORT | 2 | 9 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-8 | DS1_PORT | 2 | 8 | | MN | | LOS | Loss Of Signal |
| 01/01/00 04:00:29 PST | T1-2-7 | DS1_PORT | 2 | 7 | | MN | | LOS | Loss Of Signal |

☐ Exclude Same Root Cause

Retrieved: July 19, 2005 4:53:57 PM PDT

Conditions include all fault conditions raised on the node, whether or not they are reported.

**Note** Alarms can be unreported when they are filtered out of the display. See the "DLP-C84 Enable Alarm Filtering" task on page 17-104 for information.

Events that are reported as Major (MJ), Minor (MN), or Critical (CR) severities are alarms. Events that are reported as Not-Alarmed (NA) are conditions. Conditions that are not reported at all are marked Not-Reported (NR) in the Conditions window severity column.

Conditions that have a default severity of Critical (CR), Major (MJ), Minor (MN), or Not-Alarmed (NA) but are not reported due to exclusion or suppression are shown as NR in the Conditions window.

**Note** For more information about alarm suppression, see the "DLP-C86 Suppress Alarm Reporting" task on page 17-107.

Current conditions are shown with the severity chosen in the alarm profile, if used. (For more information about alarm profiles, see the "NTP-C60 Create, Download, and Assign Alarm Severity Profiles" procedure on page 9-6.)

**Note** When a port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state, it raises an Alarms Suppressed for Maintenance (AS-MT) condition. For information about alarm and condition troubleshooting, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide*.

**Note** When a port is placed in the Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) service state but is not connected to a valid signal, it generates a loss of signal (LOS) alarm.

**Step 3** If you want to apply exclusion rules, check the **Exclude Same Root Cause** check box at the node or network view, but do not check the Exclude Same Root Cause check box in card view.

An exclusion rule eliminates all lower-level alarms or conditions that originate from the same cause. For example, a fiber break may cause an LOS alarm, an AIS condition, and an SF condition. If you check the Exclude Same Root Cause check box, only the LOS alarm will appear. According to Telcordia, exclusion rules apply to a query of all conditions from a node.

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

# DLP-C78 Search for Circuits

| | |
|---|---|
| **Purpose** | This task searches for ONS 15310-CL and ONS 15310-MA circuits at the network, node, or card level. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** Navigate to the appropriate CTC view:

- To search the entire network, click **View > Go to Network View**.
- To search for circuits that originate, terminate, or pass through a specific node, click **View > Go to Other Node**, then choose the node you want to search and click **OK**.

- To search for circuits that originate, terminate, or pass through a specific card, double-click the card on the shelf graphic in node view to open the card in card view.

**Step 2** Click the **Circuits** tab.

**Step 3** If you are in node or card view, choose the scope for the search, **Node or Network (All)**, in the Scope drop-down list located at the bottom right-hand side of the screen.

**Step 4** Click **Search**.

**Step 5** In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the text of the circuit name you want to find.
- Match whole word only—Check this check box to instruct CTC to select circuits only if the entire word matches the text in the Find What field.
- Match case—Check this check box to instruct CTC to select circuits only when the capitalization matches the capitalization entered in the Find What field.
- Direction—Choose the direction for the search. Searches are conducted up or down from the currently selected circuit.

**Step 6** Click **Find Next**. If a match is found, click **Find Next** again to find the next circuit.

**Step 7** Repeat Steps 5 and 6 until you are finished, then click **Cancel**.

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

# DLP-C79 Create a Cloned Alarm Severity Profile

| | |
|---|---|
| **Purpose** | This task creates a custom severity profile or clones and modifies the default severity profile |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

**Step 2** To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

**Step 3** To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

**Step 4** If you want to create a profile using an existing profile located on the node, click **Load** and **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of an existing profile in the Profile Names list, such as **Default**. Then go to Step 6.

**Step 5** If you want to create a profile using an existing profile located in a file that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

**Note** All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

**Step 6** Click **OK**.

The alarm severity profile appears in the Alarm Profiles window.

**Step 7** Right-click anywhere in the profile column to display the profile editing shortcut menu. (Refer to Step 11 for further information about the Default profile.)

**Step 8** Click **Clone** in the shortcut menu.

**Tip** To see the full list of profiles, including those available for loading or cloning, click Available. You must load a profile before you can clone it.

**Step 9** In the New Profile or Clone Profile dialog box, enter a name in the New Profile Name field.

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. Long file names are supported.

**Step 10** Click **OK**.

A new alarm profile (named in Step 9) is created. This profile duplicates the default profile severities and appears at the right of the previous profile column in the Alarm Profiles window. You can select it and drag it to a different position.

**Note** Up to 10 profiles, including the two reserved profiles, Inherited and Default, can be stored in CTC.

The Default profile sets severities to standard Telcordia GR-474-CORE settings. If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm's severity at the higher level. For example, if you choose the Inherited profile from the network view, the severities at the lower levels (node, card, and port) will be copied from this selection. A card with an Inherited alarm profile copies the severities used by the node that contains the card. (If you are creating profiles, you can apply these separately at any level. To do this, refer to the "DLP-C82 Apply Alarm Profiles to Cards and Nodes" task on page 17-101.)

**Step 11** Modify (customize) the new alarm profile:

a. In the new alarm profile column, click the alarm severity you want to change in the custom profile.

b. Choose a severity from the drop-down list.

c. Repeat Steps a and b for each severity you want to customize. Refer to the following guidelines when you view the alarms or conditions after making modifications:

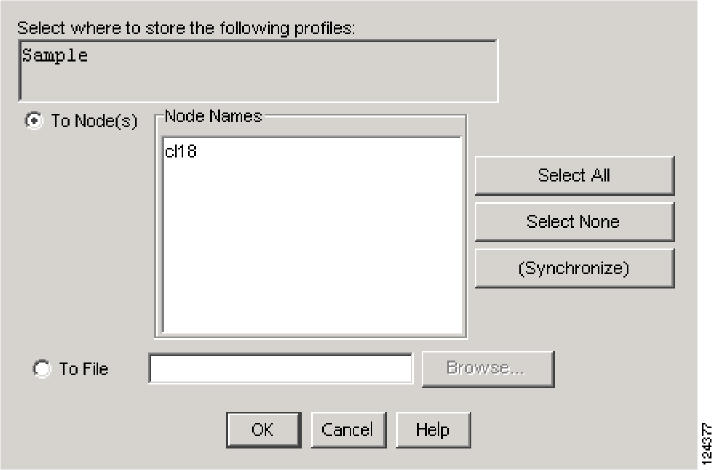
- All Critical (CR) or Major (MJ) default or user-defined severity settings are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.
- Default severities are used for all alarms and conditions until you create and apply a new profile.
- Changing a severity to inherited (I) or unset (U) does not change the severity of the alarm.

**Step 12** After you have customized the new alarm profile, right-click the profile column to highlight it.

**Step 13** Click **Store**.

**Step 14** In the Store Profile(s) dialog box, click **To Node(s)** and go to Step a or click **To File** and go to Step b (Figure 17-26).

*Figure 17-26 Store Profile(s) Dialog Box*



Select where to store the following profiles:

Sample

● To Node(s)

Node Names

cl18

○ To File

a. 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**).

b. Save the profile:
   - Click **Browse** and navigate to the profile save location.
   - Enter a name in the File name field.
   - Click **Select** to choose this name and location. Long file names are supported. CTC supplies a suffix of *.pfl to stored files.
   - Click **OK** to store the profile.

**Step 15** As needed, perform any of the following actions:

- Click the **Hide Identical Rows** check box to configure the Alarm Profiles window to display rows with dissimilar severities.
- Click the **Hide Reference Values** check box to configure the Alarm Profiles window to display severities that do not match the Default profile.
- Click the **Only show service-affecting severities** check box to configure the Alarm Profiles window not to display Minor and some Major alarms that will not affect service.

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

# DLP-C80 Download an Alarm Severity Profile

| | |
|---|---|
| **Purpose** | This task downloads a custom alarm severity profile from a network-drive accessible CD-ROM, floppy disk, or hard disk location. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

**Step 2** To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

**Step 3** To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

**Step 4** Click **Load**.

**Step 5** If you want to download a profile that exists on the node, click **From Node** in the Load Profile(s) dialog box.

a. Click the node name you are logged into in the Node Names list.

b. Click the name of the profile in the Profile Names list, such as **Default**.

**Step 6** If you want to download a profile that is stored locally or on a network drive, click **From File** in the Load Profile(s) dialog box.

a. Click **Browse**.

b. Navigate to the file location in the **Open** dialog box.

c. Click **Open**.

**Note** All default or user-defined severity settings that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.

**Step 7** Click **OK**.

The downloaded profile appears at the right side of the Alarm Profiles window.

**Step 8** Right-click anywhere in the downloaded profile column to display the profile editing shortcut menu.

**Step 9** Click **Store**.

**Step 10** In the Store Profile(s) dialog box, click **To Node(s)**.

a. Choose the nodes 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**.

b. **Click OK**.

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

# DLP-C81 Apply Alarm Profiles to Ports

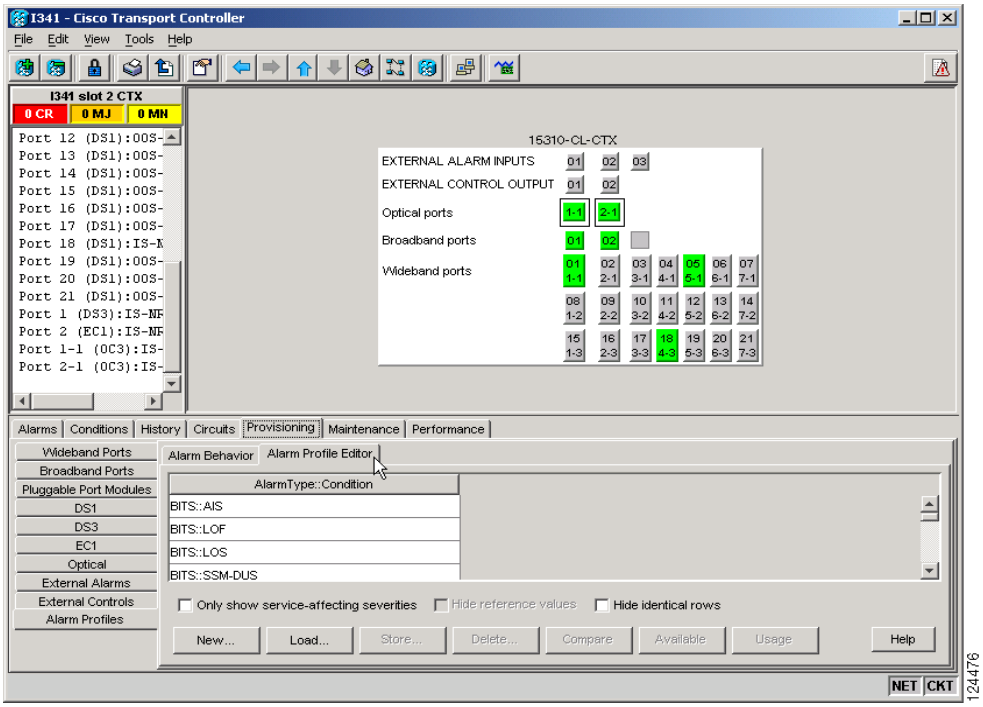
| | |
|---|---|
| **Purpose** | This task applies a custom or default alarm severity profile to a port or ports. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C79 Create a Cloned Alarm Severity Profile, page 17-96<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In the node view, double-click a card to open the card view.

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

An ONS 15310-MA optical port profile is shown in Figure 17-27. CTC shows Parent Card Profile: Inherited.

*Figure 17-27 ONS 15310-MA Card View Optical Port Alarm Profile*



```
Port 12 (DS1):OOS-
Port 13 (DS1):OOS-
Port 14 (DS1):OOS-
Port 15 (DS1):OOS-
Port 16 (DS1):OOS-
Port 17 (DS1):OOS-
Port 18 (DS1):IS-N
Port 19 (DS1):OOS-
Port 20 (DS1):OOS-
Port 21 (DS1):OOS-
Port 1 (DS3):IS-NR
Port 2 (EC1):IS-NR
Port 1-1 (OC3):IS-
Port 2-1 (OC3):IS-
```

| AlarmType::Condition |
|---|
| BITS::AIS |
| BITS::LOF |
| BITS::LOS |
| BITS::SSM-DUS |

**Step 3** To apply profiles on a port basis:

a. In card view, click the port row in the Profile column.

b. Choose the new profile from the drop-down list.

c. Click **Apply**.

**Step 4** To apply profiles to all ports on a card:

a. In card view, click the **Force all ports to profile** menu arrow at the bottom of the window.

b. Choose the new profile from the drop-down list.

c. Click **Force (still need to "Apply").**

d. Click **Apply**.

**Step 5** To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

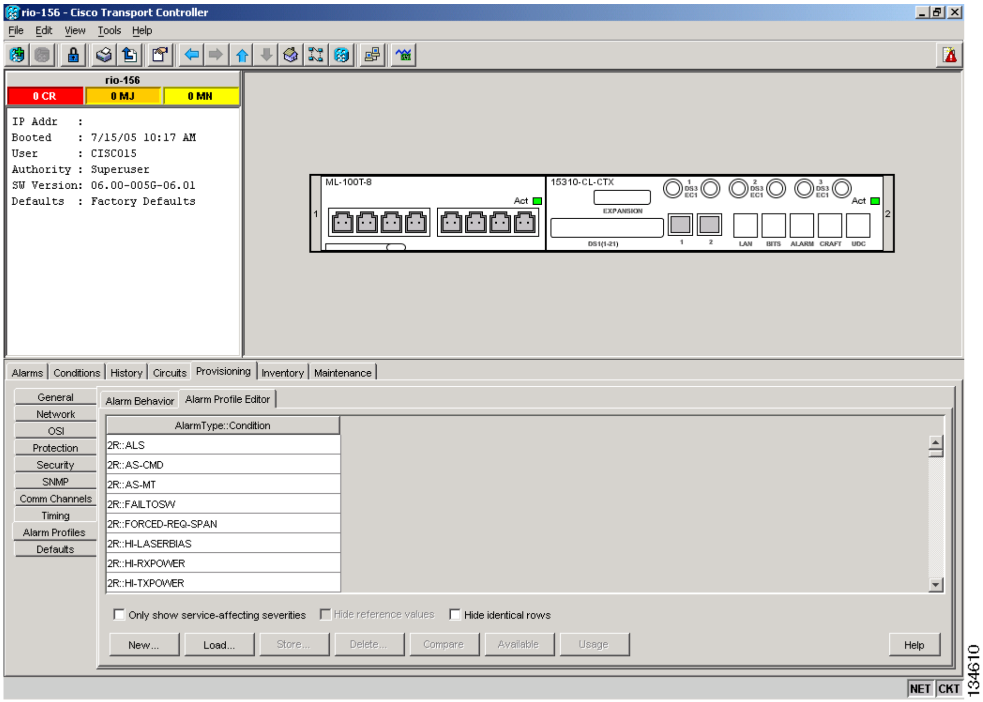
**Step 6** Return to your originating procedure (NTP).

## DLP-C82 Apply Alarm Profiles to Cards and Nodes

| | |
|---|---|
| **Purpose** | This task applies a custom or default alarm profile to cards or nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C79 Create a Cloned Alarm Severity Profile, page 17-96<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Step 1** In node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs (Figure 17-28). In the figure, and ONS 15310-CL is shown.

*Figure 17-28 Example Card View Alarm Profile of an ONS 15310-CL-CTX Card*



```
IP Addr    :
Booted     : 7/15/05 10:17 AM
User       : CISCO15
Authority  : Superuser
SW Version: 06.00-005G-06.01
Defaults   : Factory Defaults
```

| AlarmType::Condition |
|---|
| 2R::ALS |
| 2R::AS-CMD |
| 2R::AS-MT |
| 2R::FAILTOSW |
| 2R::FORCED-REQ-SPAN |
| 2R::HI-LASERBIAS |
| 2R::HI-RXPOWER |
| 2R::HI-TXPOWER |

□ Only show service-affecting severities □ Hide reference values □ Hide identical rows

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

**a.** Click the Profile row for the card.

**b.** Choose the new profile from the drop-down list.

**c.** Click **Apply**.

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

**a.** Click the **Node Profile** menu arrow at the bottom of the window (Figure 17-28).

**b.** Choose the new alarm profile from the drop-down list.

**c.** Click **Apply**.

**Step 4** To reapply a previous alarm profile after you have applied a new one, select the previous profile and click **Apply** again.

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

# DLP-C83 Delete Alarm Severity Profiles

| | |
|---|---|
| **Purpose** | This task deletes a custom or default alarm severity profile. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

**Step 2** To access the alarm profile editor from network view, click the **Provisioning > Alarm Profiles** tabs.

**Step 3** To access the profile editor from node view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

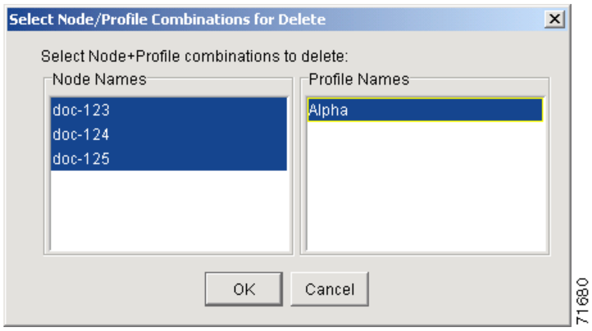
**Step 4** To access the profile editor from a card view, click the **Provisioning > Alarm Profiles > Alarm Profile Editor** tabs.

**Step 5** Click the profile you are deleting to select it.

**Step 6** Click **Delete**.

The Select Node/Profile Combination for Delete dialog box appears (Figure 17-29).

*Figure 17-29 Select Node/Profile Combination For Delete Dialog Box*



Select Node/Profile Combinations for Delete

Select Node+Profile combinations to delete:

Node Names: doc-123, doc-124, doc-125

Profile Names: Alpha

**Note** You cannot delete the Inherited or Default alarm profiles.

**Note** A previously created alarm profile cannot be deleted unless it has been stored on the node. If the profile is visible on the Alarm Profiles tab but is not listed in the Select Node/Profile Combinations to Delete dialog box, continue with Step 11.

**Step 7** Click the node name(s) in the Node Names list to highlight the profile location.

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

**Step 8** Click the profile name(s) you want to delete in the Profile Names list.

**Step 9** Click **OK**.

**Step 10** Click **Yes** in the Delete Alarm Profile dialog box.

**Note** If you delete a profile from a node, it still appears in the network view Provisioning > Alarm Profile Editor window unless you remove it using the following step.

**Step 11** To remove the alarm profile from the window, right-click the column of the profile you deleted and choose **Remove** from the shortcut menu.

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

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

**Step 12** Return to your originating procedure (NTP).

# DLP-C84 Enable Alarm Filtering

| | |
|---|---|
| **Purpose** | This task enables alarm filtering for alarms, conditions, or event history in all network nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

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

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

Alarm filtering will be enabled in the card, node, and network views of the Alarms tab at the node and for all other nodes in the network. If, for example, the Alarm Filter tool is enabled in the Alarms tab of the node view at one node, the Alarms tab in the network view and card view of that node will also show the tool enabled. All other nodes in the network will also have the tool enabled.

If you filter an alarm in card view, the alarm will still be displayed in node view. In this view, the card will display the color of the highest-level alarm. The alarm is also shown for the node in the network view.

**Step 3** If you want alarm filtering enabled when you view conditions, repeat Steps 1 and 2 using the Conditions window.

**Step 4** If you want alarm filtering enabled when you view alarm history, repeat Steps 1 and 2 using the History window.

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

## DLP-C85 Modify Alarm and Condition Filtering Parameters

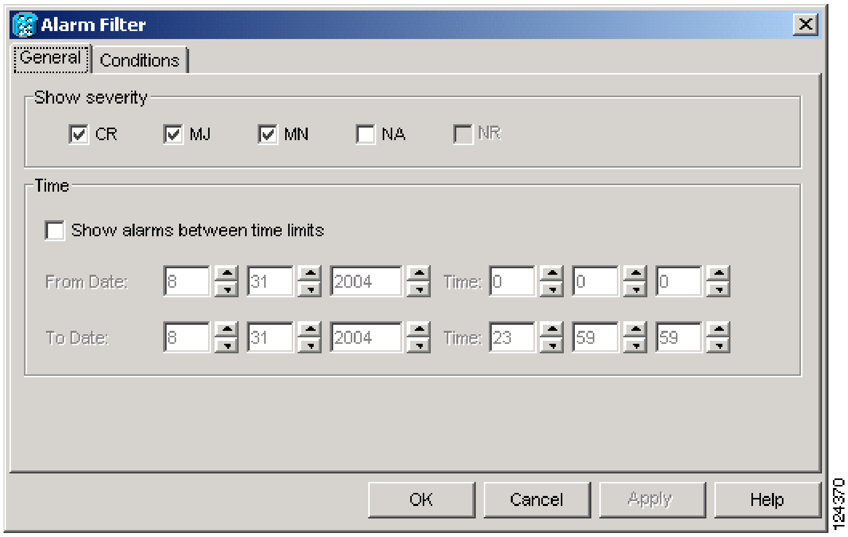
| | |
|---|---|
| **Purpose** | This task changes alarm and condition reporting in all network nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C84 Enable Alarm Filtering, page 17-104<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** At the node, network, or card view, click the **Alarms** tab, **Conditions** tab, or **History** tab.

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

The filter dialog box appears, displaying the General tab. Figure 17-30 shows the Alarm Filter dialog box; the Conditions and History tabs have similar dialog boxes.

*Figure 17-30 Alarm Filter Dialog Box General Tab*



Show severity

☑ CR ☑ MJ ☑ MN ☐ NA ☐ NR

Time

☐ Show alarms between time limits

From Date: 8 31 2004 Time: 0 0 0

To Date: 8 31 2004 Time: 23 59 59

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

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

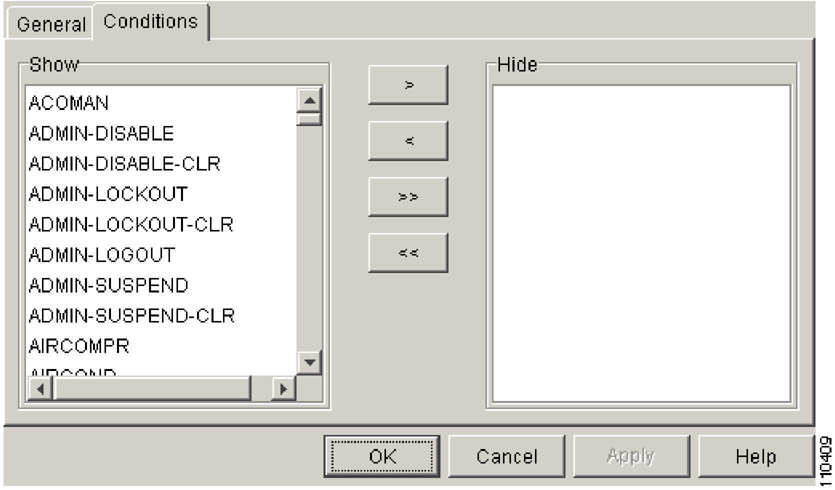
When alarm filtering is disabled, all alarms show.

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

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

**Step 5** Click the filter dialog box **Conditions** tab (Figure 17-31).

***Figure 17-31 Alarm Filter Dialog Box Conditions Tab***



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

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

**Note** Conditions include alarms.

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

Alarm and condition filtering parameters are enforced when alarm filtering is enabled (see the "DLP-C84 Enable Alarm Filtering" task on page 17-104), and the parameters are not enforced when alarm filtering is disabled (see the "DLP-C88 Disable Alarm Filtering" task on page 17-109).

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

# DLP-C86 Suppress Alarm Reporting

| | |
|---|---|
| **Purpose** | This task suppresses the reporting of ONS 15310-CL/ONS 15310-MA alarms at the node, card, or port level. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Caution** If multiple CTC/TL1 sessions are open, suppressing alarms in one session suppresses the alarms in all other open sessions.

**Note** Alarm suppression at the node level does not supersede alarm suppression at the card or port level. Suppression can exist independently for all three entities, and each entity will raise separate alarms suppressed by the user command (AS-CMD) alarm.

**Step 1** If you are in node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

**Step 2** To suppress alarms for the entire node:

a. Check the **Suppress Alarms** check box.

b. Click **Apply**.

All raised alarms for the node will change color to white in the Alarms window and their status will change to cleared. After suppressing alarms, clicking **Synchronize** in the Alarms window will remove cleared alarms from the window. However, an AS-CMD alarm will show in node or card view to indicate that node-level alarms were suppressed; this alarm will show System in the Object column.

**Note** The only way to suppress BITS, power source, or system alarms is to suppress alarms for the entire node. These cannot be suppressed separately, but the shelf backplane can be.

**Step 3** To suppress alarms for individual cards:

a. Locate the card row (using the Location column for the slot number or the Eqpt Type column for the equipment name).

b. Check the **Suppress Alarms column** check box on that row (Figure 17-23 on page 17-88).

Alarms that directly apply to this card will change appearance as described in Step 2. For example, if you suppressed raised alarms for a CE 100T-8 card in Slot 2, raised alarms for this card will change in node or card view. The AS-CMD alarm will show the slot number in the Object number (i.e., the AS-CMD object will be “SLOT-2.”

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

**Step 5** To suppress alarms for individual card ports double-click the card in node view.

**Step 6** Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

**Step 7** Check the **Suppress Alarms** column check box for the port row where you want to suppress alarms (Figure 17-23 on page 17-88).

**Step 8** Click **Apply**.

Alarms that apply directly to this port will change appearance as described in Step 2. (However, alarms raised on the card will remain raised.) A raised AS-CMD alarm that shows the port as its object will appear in either alarm window. For example, if you suppressed alarms for Port 1 on the Slot 2 CE 100T-8 card, the alarm object will show "FAC-2-1."

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

# DLP-C87 Discontinue Alarm Suppression

| | |
|---|---|
| **Purpose** | This task discontinues alarm suppression and reenables alarm reporting on a port, card, or node. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C86 Suppress Alarm Reporting, page 17-107<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Caution** If multiple CTC sessions are open, discontinuing suppression in one session will discontinue suppression in all other open sessions.

**Step 1** To discontinue alarm suppression for the entire node:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tab.

b. Uncheck the **Suppress Alarms** check box.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The alarms suppressed by user command (AS-CMD) condition with the System object will be cleared in all views.

**Step 2** To discontinue alarm suppression for individual cards:

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

b. Locate the card that was suppressed in the slot list.

c. Uncheck the Suppress Alarms column check box for that slot.

d. Click **Apply**.

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD condition with the slot object (for example, SLOT-2) will be cleared in all views.

**Step 3** Uncheck the **Suppress Alarms** check box for the ports you no longer want to suppress.

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

Suppressed alarms will reappear in the Alarms window. (They may have previously been cleared from the window using the Synchronize button.) The AS-CMD condition with the port object (for example, FAC-2-1) will be cleared in all views.

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

## DLP-C88 Disable Alarm Filtering

| | |
|---|---|
| **Purpose** | This task turns off specialized alarm filtering in all network nodes so that all severities are reported in CTC. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C84 Enable Alarm Filtering, page 17-104<br>DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

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

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

**Step 3** If you want alarm filtering disabled when you view conditions, click the **Conditions** tab and click the Filter tool.

**Step 4** If you want alarm filtering disabled when you view alarm history, click the **History** tab and click the Filter tool.

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

## DLP-C89 Refresh PM Counts for a Different Port

| | |
|---|---|
| **Purpose** | This task changes the window view to display PM counts for another port on a multiport card. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

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

- To refresh PM Counts for optical ports, click the **Optical** tab.
- To refresh PM Counts for ML-Series and CE-Series Ethernet cards, click the **Ether Ports > History** tabs or **POS Ports > History** tabs.

**Step 3** From the Port drop-down list, choose the target port to highlight your selection.

**Step 4** Click **Refresh**. The PM counts for the newly selected port appear.

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

# DLP-C90 Refresh Electrical or Optical PM Counts at Fifteen-Minute Intervals

| | |
|---|---|
| **Purpose** | This task changes the window view to display PM counts in 15-minute intervals. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports.

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

**Step 3** Click the **DS1**, **DS3**, **EC1**, or **Optical** tabs.

**Step 4** Click the **15 min** radio button.

**Step 5** Click **Refresh**. Performance monitoring parameters appear in 15-minute intervals synchronized with the time of day.

**Step 6** View the Curr column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) is raised. The PM number represents the counter value for each specific performance monitoring parameter.

**Step 7** View the Prev-*n* columns to find PM counts for the previous 15-minute intervals.

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

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

# DLP-C91 Refresh Electrical or Optical PM Counts at One-Day Intervals

| | |
|---|---|
| **Purpose** | This task changes the window to display PM parameters in 1-day intervals. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports.

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

**Step 3** Click the **DS1**, **DS3**, **EC1**, or **Optical** tabs

**Step 4** Click the **1 day** radio button.

**Step 5** Click **Refresh**. Performance monitoring appears in 1-day intervals synchronized with the time of day.

**Step 6** View the Curr column to find PM counts for the current 1-day interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 1-day interval, a TCA is raised. The PM number represents the counter value for each performance monitoring parameter.

**Step 7** View the Prev-*n* columns to find PM counts for the previous 1-day intervals.

If a complete count over a 1-day interval is not possible, the value appears with a yellow background. An incomplete or incorrect count can be caused by monitoring for less than 24 hours after the counter started, changing node timing settings, changing the time zone settings, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 1-day interval appears with a white background.

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

# DLP-C92 Monitor Near-End PM Counts

| | |
|---|---|
| **Purpose** | This task enables you to view near-end PM counts for the selected card and port. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

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

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

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

**Step 3** Click the **DS1**, **DS3**, or **Optical** tabs.

**Step 4** Click the **Near End** radio button.

**Step 5** Click **Refresh**. All PM parameters for the selected card on the incoming signal appear. For PM parameter definitions refer to the “Performance Monitoring” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

**Step 6** View the Curr column to find PM counts for the current time interval.

**Step 7** View the Prev-*n* columns to find PM counts for the previous time intervals.

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

# DLP-C93 Monitor Far-End PM Counts

| | |
|---|---|
| **Purpose** | Use this task to view far-end PM parameters for the selected card and port. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** In node view, double-click an 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

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

**Step 3** Click the **DS1**, **DS3**, or **Optical** tabs

**Step 4** Click the **Far End** radio button.

**Note** Only cards that allow far-end performance monitoring have this button as an option.

**Step 5** Click **Refresh**. All PM parameters recorded by the far-end node for the selected card on the outgoing signal appear. For PM parameter definitions refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual.*

**Step 6** View the Curr column to find PM counts for the current time interval.

**Step 7** View the Prev-*n* columns to find PM counts for the previous time intervals.

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

# DLP-C94 Reset Current PM Counts

| | |
|---|---|
| **Purpose** | This task uses the Baseline button to clear the PM count displayed in the current time interval, but it does not clear the cumulative PM count. This task allows you to see how quickly PM counts rise. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** In node view, double-click a 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

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

- To reset current PM Counts for optical ports click the **Optical** tab.
- To reset current PM Counts for electrical ports click the **DS1, DS3,** or **EC1** tabs.

- To reset current PM counts for ML-Series and CE-Series Ethernet cards click the **Ether Ports > Statistics** tabs or **POS Ports > Statistics** tabs.

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

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

**Step 4** View the current statistics columns to observe changes to PM counts for the current time interval.

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

# DLP-C95 Clear Selected PM Counts

| | |
|---|---|
| **Purpose** | This task uses the Clear button to clear specified PM counts depending on the option selected. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Superuser only |

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

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

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

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

- To clear selected PM Counts for optical ports, click the **Optical** tab.
- To clear selected PM Counts for electrical ports, click the **DS1, DS3,** or **EC1** tab.
- To clear selected PM counts for ML-Series and CE-Series Ethernet cards, click the **Ether Ports > Statistics** tabs or the **POS Ports > Statistics** tabs.

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

**Step 4** On the Clear Statistics dialog box, choose one of three options:

- **Displayed statistics**: Clearing displayed statistics erases from the card and the window all PM counts associated with the current combination of statistics on the selected port. This means that the selected time interval, direction, and signal type counts are erased from the card and the window.

  **Note** This option is available only for electrical and optical ports.

- **All statistics for port** *x*: Clearing all of the statistics for port *x* erases from the card and the window all PM counts associated with all combinations of the statistics on the selected port. This means that all time intervals, directions, and signal type counts are erased from the card and the window.
- **All statistics for card**: Clearing all of the statistics for the card erases from the card and the window display all PM counts for all ports.

**Step 5** Click **Ok**. In the confirmation dialog box, click **Yes** to clear the selected statistics.

**Step 6** View the displayed columns to verify that the selected PM counts have been cleared.

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

## DLP-C96 Set Auto Refresh Interval for Displayed PM Counts

| | |
|---|---|
| **Purpose** | This task changes the window auto-refresh intervals for updating the displayed PM counts. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** In node view, double-click an electrical, Ethernet, 15310-CL-CTX, or CTX2500 card. The card view appears.

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

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

- To set the auto-refresh interval for optical ports click the **Optical** tab.
- To set the auto-refresh interval for electrical ports click the **DS1, DS3,** or **EC1** tabs.
- To set the auto-refresh interval for ML-Series and CE-Series Ethernet cards click the **Ether Ports > Statistics** tabs or **POS Ports > Statistics** tabs.

**Step 3** Click the Auto-refresh drop-down list and choose one of six options:

- **None**: This option disables the auto-refresh feature.
- **15 Seconds**: This option sets the window auto-refresh to 15-second time intervals.

- **30 Seconds**: This option sets the window auto-refresh to 30-second time intervals.
- **1 Minute**: This option sets the window auto-refresh to 1-minute time intervals.
- **3 Minutes**: This option sets the window auto-refresh to 3-minute time intervals.
- **5 Minutes**: This option sets the window auto-refresh to 5-minute time intervals.

**Step 4** Click **Refresh**. The PM counts for the newly selected auto-refresh time interval appear.

Depending on the selected auto-refresh interval, the displayed PM counts automatically update when each refresh interval completes. If the auto-refresh interval is set to None, the displayed PM counts are not updated unless you click the Refresh button.

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

# DLP-C97 Monitor PM Counts for Selected Signal Types

| | |
|---|---|
| **Purpose** | This task enables you to monitor near-end or far-end PM counts for specific signals on a selected card and port. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Retrieve or higher |

**Step 1** In node view, double-click a 15310-CL-CTX, CTX2500, electrical, or Ethernet card. The card view appears.

**Note** In an ONS 15310-CL node, the 15310-CL-CTX card provides optical and electrical ports. In an ONS 15310-MA node, the CTX2500 card provides optical ports and the DS1-28/DS3-EC1-3 and DS1-84/DS3-EC1-3 cards provide electrical ports. The ONS 15310-CL and ONS 15310-MA both support Ethernet cards.

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

**Step 3** Click the **DS1, DS3, EC1,** or **Optical** tabs.

**Note** Different port and signal-type drop-down lists appear depending on the port type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path, OC-N section, and OC-N line) appear based on the card.

**Step 4** Click the **Port/Line** drop-down list and highlight the desired port/line. (Options vary depending on the port.)

**Step 5** Click the **signal type** drop-down list and highlight the desired signal. (Options vary depending on the port.)

**Step 6** Click **Refresh**. All PM counts recorded by the near-end or far-end node appear for the specified outgoing signal type on the selected card and port. For PM parameter definitions, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

**Step 7** View the Curr column to find PM counts for the current time interval.

**Step 8** View the Prev-*n* columns to find PM counts for the previous time intervals.

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

# DLP-C98 Enable Pointer Justification Count Performance Monitoring

| | |
|---|---|
| **Purpose** | This task enables pointer justification counts, which provide a way to align the phase variations in STS and VT payloads and to monitor the clock synchronization between nodes. A consistent, large pointer justification count indicates clock synchronization problems between nodes. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

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

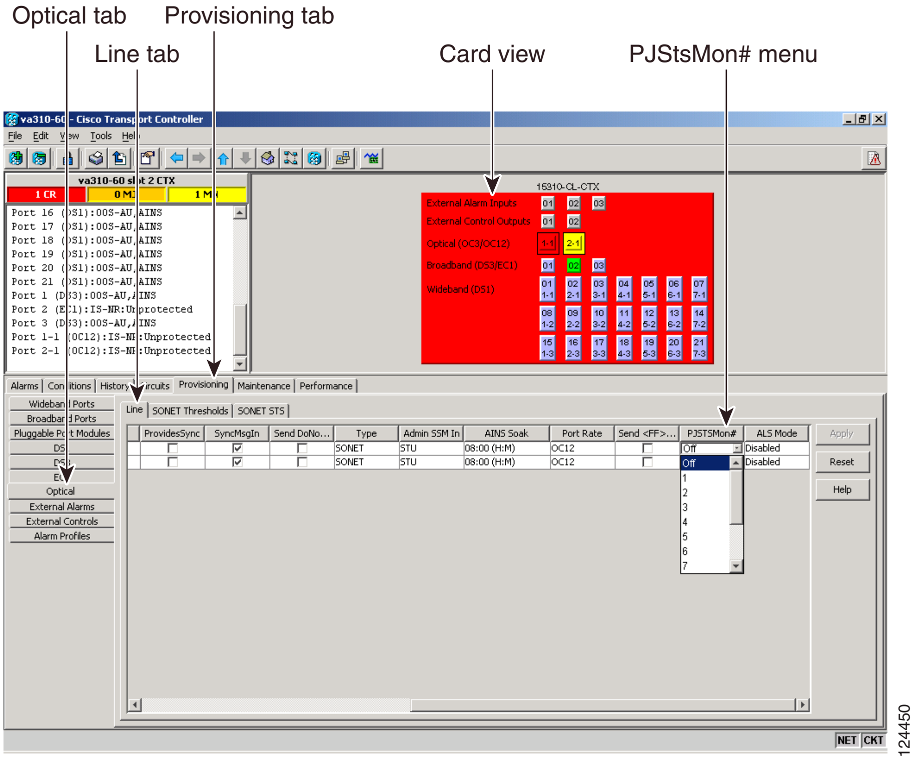
**Step 2** Click the **Provisioning > Optical > Line** tabs.

**Step 3** Click the **PJStsMon#** menu and make a selection based on the following rules:

- The default value Off means pointer justification monitoring is disabled.
- The values 1 to N are the number of STSs on the port. One STS per port can be enabled from the PJStsMon# card drop-down list.

Figure 17-32 shows the PJStsMon# drop-down list on the Provisioning window.

*Figure 17-32 Line Tab for Enabling Pointer Justification Count Parameters*



```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

| | ProvidesSync | SyncMsgIn | Send DoNo... | Type | Admin SSM In | AINS Soak | Port Rate | Send <FF>... | PJSTSMon# | ALS Mode |
|---|---|---|---|---|---|---|---|---|---|---|
| | □ | ☑ | □ | SONET | STU | 08:00 (H:M) | OC12 | □ | Off | Disabled |
| | □ | ☑ | □ | SONET | STU | 08:00 (H:M) | OC12 | □ | Off<br>1<br>2<br>3<br>4<br>5<br>6<br>7 | Disabled |

**Step 4** In the Service State field, confirm that the port is in the In-Service and Normal (IS-NR) service state.

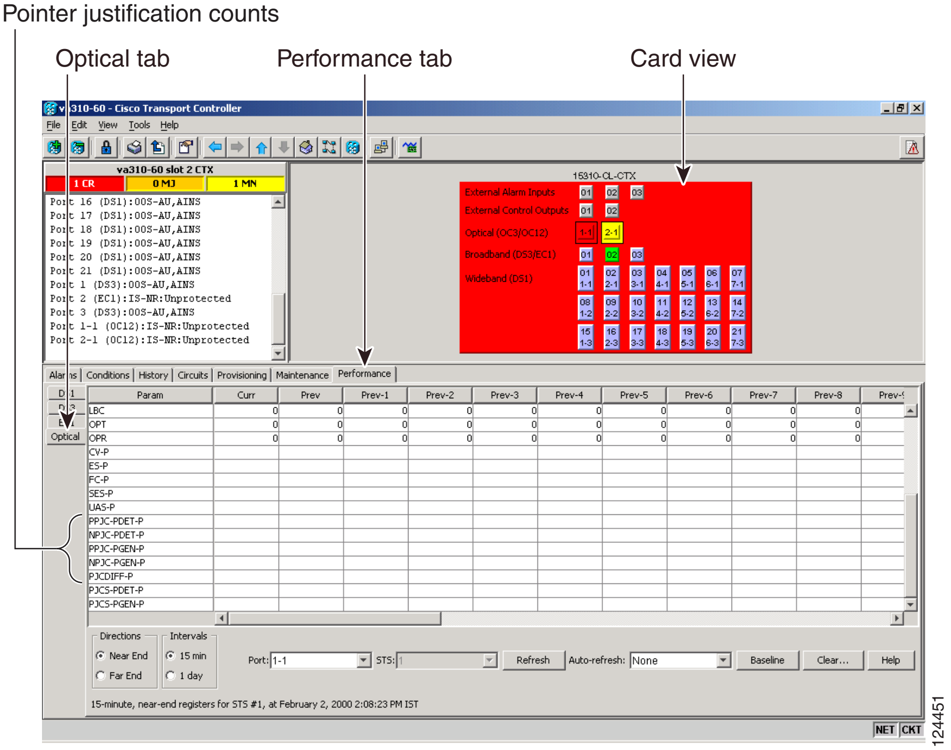
**Step 5** If the port is IS-NR, click **Apply** and go to Step 7.

**Step 6** If the port is in the Out-of-Service and Disabled (OOS,DSLBD); Out-of-Service and Maintenance (OOS,MT); or In-Service and Automatic In-Service (IS,AINS), select **IS** in the Admin State field and click **Apply**.

**Step 7** Click the **Performance** tab to view PM parameters. Figure 17-33 shows pointer justification counts. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more PM information, details, and definitions.

**Note** In CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Optical > Line tabs.

*Figure 17-33 Viewing Pointer Justification Counts*



```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

| Param | Curr | Prev | Prev-1 | Prev-2 | Prev-3 | Prev-4 | Prev-5 | Prev-6 | Prev-7 | Prev-8 | Prev-9 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LBC | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| OPT | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| OPR | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| CV-P | | | | | | | | | | | |
| ES-P | | | | | | | | | | | |
| FC-P | | | | | | | | | | | |
| SES-P | | | | | | | | | | | |
| UAS-P | | | | | | | | | | | |
| PPJC-PDET-P | | | | | | | | | | | |
| NPJC-PDET-P | | | | | | | | | | | |
| PPJC-PGEN-P | | | | | | | | | | | |
| NPJC-PGEN-P | | | | | | | | | | | |
| PJCDIFF-P | | | | | | | | | | | |
| PJCS-PDET-P | | | | | | | | | | | |
| PJCS-PGEN-P | | | | | | | | | | | |

Directions: ● Near End ○ Far End

Intervals: ● 15 min ○ 1 day

Port: 1-1 STS: 1 [Refresh] Auto-refresh: None [Baseline] [Clear...] [Help]

15-minute, near-end registers for STS #1, at February 2, 2000 2:08:23 PM IST

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

# DLP-C99 Enable Intermediate-Path Performance Monitoring

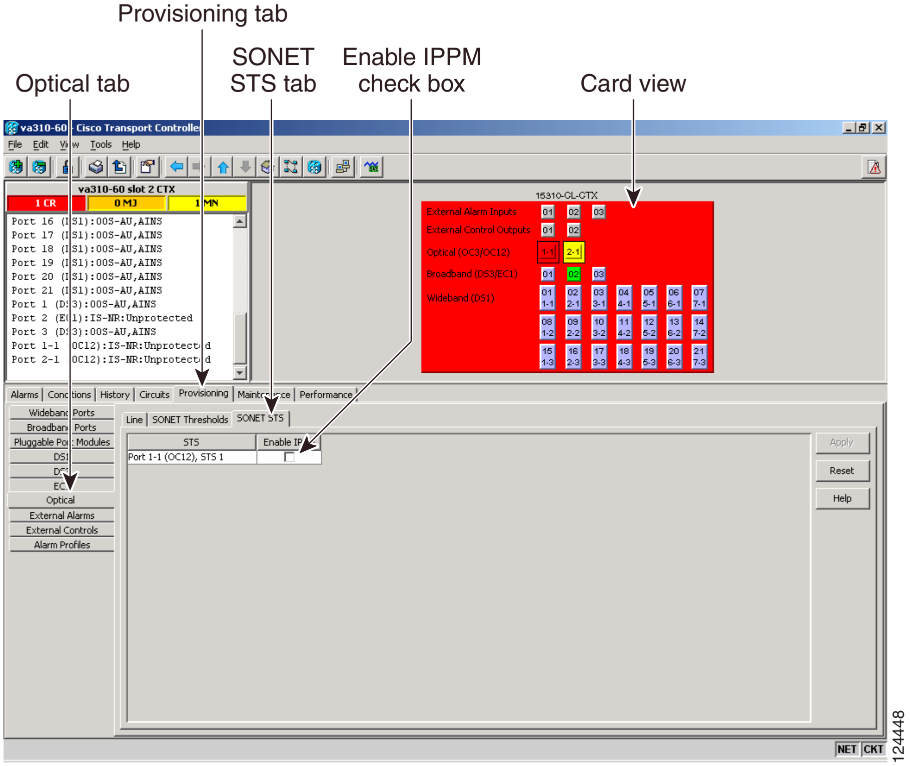
| | |
|---|---|
| **Purpose** | This task enables intermediate-path performance monitoring (IPPM), which allows you to monitor large amounts of STS traffic through intermediate nodes. This task also enables IIPM VT in the ONS 15310-MA. |
| **Tools/Equipment** | None |
| **Prerequisite Procedures** | DLP-C29 Log into CTC, page 17-44 |
| **Required/As Needed** | As needed |
| **Onsite/Remote** | Onsite or remote |
| **Security Level** | Provisioning or higher |

**Note** The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. For more information about IPPM parameters, refer to the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

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

**Step 2** Click the **Provisioning > Optical > SONET STS** tabs. Figure 17-34 shows the SONET STS tab in the Provisioning window.

*Figure 17-34 SONET STS Tab for Enabling IPPM*



```
Port 16 (DS1):OOS-AU,AINS
Port 17 (DS1):OOS-AU,AINS
Port 18 (DS1):OOS-AU,AINS
Port 19 (DS1):OOS-AU,AINS
Port 20 (DS1):OOS-AU,AINS
Port 21 (DS1):OOS-AU,AINS
Port 1 (DS3):OOS-AU,AINS
Port 2 (EC1):IS-NR:Unprotected
Port 3 (DS3):OOS-AU,AINS
Port 1-1 (OC12):IS-NR:Unprotected
Port 2-1 (OC12):IS-NR:Unprotected
```

| STS | Enable IPPM |
|---|---|
| Port 1-1 (OC12), STS 1 | □ |

**Step 3** Check the check box in the Enable IPPM column for the STS you want to monitor.

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

**Step 5** Click the **Performance** tab to view PM parameters. For IPPM parameter definitions, refer to the “Performance Monitoring” chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

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