



CHAPTER 17

DLPs A1 to A99



Note

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

DLP-A1 Unpack and Verify the Shelf Assembly

Purpose	This task removes the 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 ONS 15454 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 15454 shelf (wrapped in plastic) and a smaller box of items needed for installation.
- Step 3** To remove the shelf, grasp both rings of the shelf removal strap and slowly lift the shelf out of the box.
- Step 4** Open the smaller box of installation materials, and verify that you have all items listed in the [“Cisco-Supplied Materials” section on page 1-2](#).



Note The fan-tray assembly is shipped separately.

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

DLP-A2 Inspect the Shelf Assembly

Purpose	This task verifies that all parts of the shelf assembly are in good condition.
Tools/Equipment	Pinned hex (Allen) key for front door
Prerequisite Procedures	DLP-A1 Unpack and Verify the Shelf Assembly, page 17-1
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

-
- Step 1** Open the shelf using the pinned hex key. For more information, see the “[DLP-A8 Open the Front Door](#)” task on page 17-8.
- Step 2** Verify the following:
- The pins are not bent or broken.
 - The frame is not bent.
- Step 3** If the pins are bent or broken or the frame is bent, call your Cisco sales engineer for a replacement.
- Step 4** Close the front door before installing.
- Step 5** Return to your originating procedure (NTP).
-

DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack

Purpose	This task installs the mounting bracket to convert a 23-inch (584.2 mm) rack to a 19-inch (482.6 mm) rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None


Caution

Use only the fastening hardware provided with the ONS 15454 to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

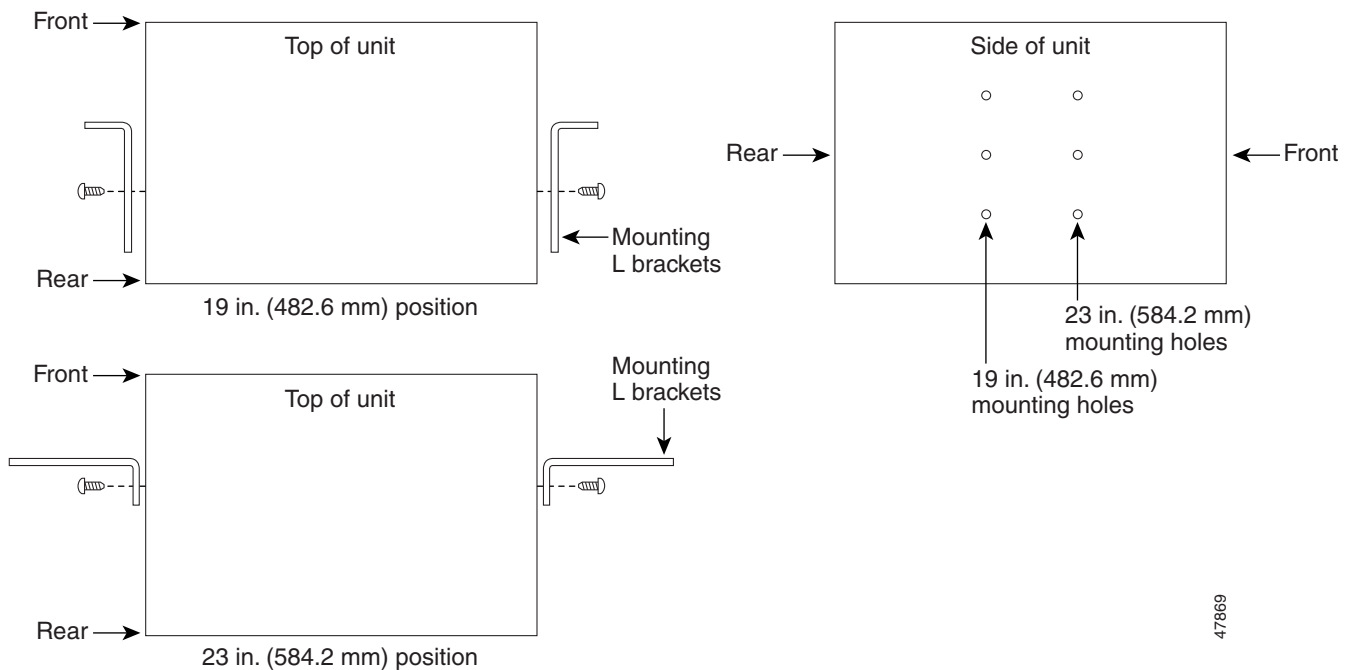

Caution

When mounting the ONS 15454 in a frame with a nonconductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the ONS 15454 shipping kit, or remove the coating from the threads to ensure electrical continuity.

-
- Step 1** Remove the screws that attach the mounting bracket to the side of the shelf assembly.

- Step 2** Flip the detached mounting bracket upside down.
Text imprinted on the mounting bracket will now also be upside down.
- Step 3** Place the widest side of the mounting bracket flush against the shelf assembly (see [Figure 17-1](#)).
The narrow side of the mounting bracket should be towards the front of the shelf assembly. Text imprinted on the mounting bracket should be visible and upside down.
- Step 4** Align the mounting bracket screw holes against the shelf assembly screw holes.
- Step 5** Insert the screws that were removed in [Step 1](#) and tighten them.
- Step 6** Repeat the task for the mounting bracket on the opposite side.

Figure 17-1 Reversing the Mounting Brackets (23-inch [584.2-mm] Position to 19-inch [482.6-mm] Position)



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

DLP-A4 Install the External Brackets and Air Filter

Purpose	This task installs the external brackets and air filter on the bottom of the shelf rather than below the fan-tray assembly. Installing the external brackets and air filter on the bottom of the shelf enables access to the air filter without removing the fan-tray assembly.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack , page 17-2, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None


Note

If you choose not to install the brackets, install the air filter by sliding it into the compartment at the bottom of the shelf assembly. Each time you remove and reinstall the air filter in the future, you must first remove the fan-tray assembly. Do not install an air filter in both filter locations on any shelf assembly.


Note

To install the air filter inside the air ramp unit (15454E-AIR-RAMP or 15454-AIR-RAMP), use the ETSI version of the air filter (15454-FTF2 or 15454E-FTF4).

Step 1 With the fan-tray assembly removed, place the ONS 15454 facedown on a flat surface.


Note

Although the filter will work if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

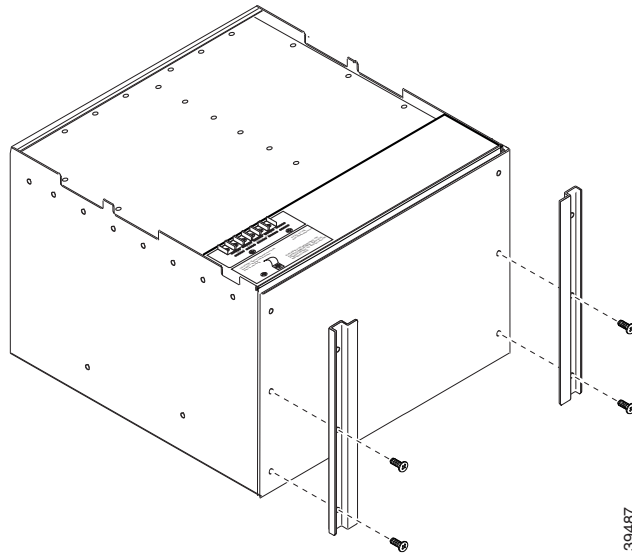
Step 2 Locate the three screw holes that run along the left and right sides of the bottom of the shelf assembly.

Step 3 Secure each bracket to the bottom of the shelf assembly using the screws (48-0003) provided in the backplane standoff kit (53-0795-XX).

Each bracket has a filter stopper and a flange on one end. Make sure to attach the brackets with the stoppers and flanges facing the rear of the shelf assembly (the top, if the ONS 15454 is facedown during installation).

[Figure 17-2](#) illustrates bottom bracket installation. If you do not use the brackets, in the future you must remove the fan-tray assembly before removing the air filter. The brackets enable you to clean and replace the air filter without removing the fan-tray assembly.

Figure 17-2 *Installing the External Brackets*



- Step 4** Slide the air filter into the shelf assembly.
- Step 5** Return to your originating procedure (NTP).

DLP-A5 Mount the Shelf Assembly in a Rack (One Person)

Purpose	This task allows one person to mount the shelf assembly in a rack.
Tools/Equipment	<p>Pinned hex tool</p> <p>Two set screws (48-1003-XX)</p> <p>Eight pan-head Phillips mounting screws (48-1004-XX, 48-1007-XX)</p> <p>#2 Phillips screwdriver</p>
Prerequisite Procedures	<p>DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 17-2, if applicable</p> <p>DLP-A4 Install the External Brackets and Air Filter, page 17-4, if applicable</p>
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

- Step 1** 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's instructions.
- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
 - If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.

- Step 2** Ensure that the shelf assembly is set for the desired rack size (either 23 inches [584.2 mm] or 19 inches [482.6 mm]).
- Step 3** Using the hex tool that shipped with the assembly, install the two set screws into the screw holes that will not be used to mount the shelf. Let the screws protrude sufficiently to hold the mounting bracket.
- Step 4** Lift the shelf assembly to the desired rack position and set it on the set screws.
- Step 5** Align the screw holes on the mounting bracket with the mounting holes in the rack.
- Step 6** Using the Phillips screwdriver, install one mounting screw in each side of the assembly.
- Step 7** When the shelf assembly is secured to the rack, install the remaining mounting screws.



Note Use at least one set of the horizontal screw slots on the ONS 15454 to prevent slippage.

- Step 8** Using the hex tool, remove the temporary set screws.
- Step 9** Return to your originating procedure (NTP).

DLP-A6 Mount the Shelf Assembly in a Rack (Two People)

Purpose	This task allows two people to mount the shelf assembly in a rack.
Tools/Equipment	Pinned hex tool Two set screws (48-1003-XX) Eight pan-head Phillips mounting screws (48-1004-XX, 48-1007-XX) #2 Phillips screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack, page 17-2 , if applicable DLP-A4 Install the External Brackets and Air Filter, page 17-4 , if applicable
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

- Step 1** 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's instructions.
- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
 - If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.
- Step 2** Ensure that the shelf assembly is set for the desired rack size (either 23 inches [584.2 mm] or 19 inches [482.6 mm]).
- Step 3** Using the hex tool that shipped with the shelf assembly, install the two set screws (48-1003-XX) into the screw holes that will not be used to mount the shelf. Let the set screws protrude sufficiently to hold the mounting brackets.

- Step 4** Lift the shelf assembly to the desired position in the rack.
- Step 5** Align the screw holes on the mounting brackets with the mounting holes in the rack.
- Step 6** While one person holds the shelf assembly in place, the other person can install one mounting screw in each side of the assembly using the Phillips screwdriver.
- Step 7** When the shelf assembly is secured to the rack, install the remaining mounting screws.



Note Use at least one set of the horizontal screw slots on the ONS 15454 to prevent slippage.

- Step 8** Using the hex tool, remove the temporary set screws.
- Step 9** Return to your originating procedure (NTP).

DLP-A7 Mount Multiple Shelf Assemblies in a Rack

Purpose	This task allows multiple shelves to be assembled in a rack.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A3 Reverse the Mounting Bracket to Fit a 19-inch (482.6 mm) Rack , page 17-2, if applicable DLP-A4 Install the External Brackets and Air Filter , page 17-4, if applicable
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note The ONS 15454 must have one inch (25.4 mm) of airspace below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 is installed underneath a shelf assembly, the air ramp on top of the bottom shelf assembly provides the desired space. However, if the ONS 15454 is installed above third-party equipment, you must provide a minimum spacing of one inch (25.4 mm) between the third-party shelf assembly and the bottom of the ONS 15454. The third-party equipment must not vent heat upward into the ONS 15454.

- Step 1** 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's instructions.
- If installing the 15454-SA-ANSI or 15454-SA-HD shelf assembly, a 100-A fuse panel (30-A fuse per shelf minimum) is required.
 - If installing the 15454-SA-NEBS3 shelf assembly, a standard 80-A fuse panel (20-A fuse per shelf minimum) is required.
- Step 2** Mount the first ONS 15454 directly below the fuse and alarm panel using the [“DLP-A5 Mount the Shelf Assembly in a Rack \(One Person\)”](#) task on page 17-5 or the [“DLP-A6 Mount the Shelf Assembly in a Rack \(Two People\)”](#) task on page 17-6.

- Step 3** Repeat the task with the remaining shelves.
- Step 4** Return to your originating procedure (NTP).
-

DLP-A8 Open the Front Door

Purpose	This task describes how to open the front cabinet compartment door.
Tools/Equipment	Pinned hex key
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

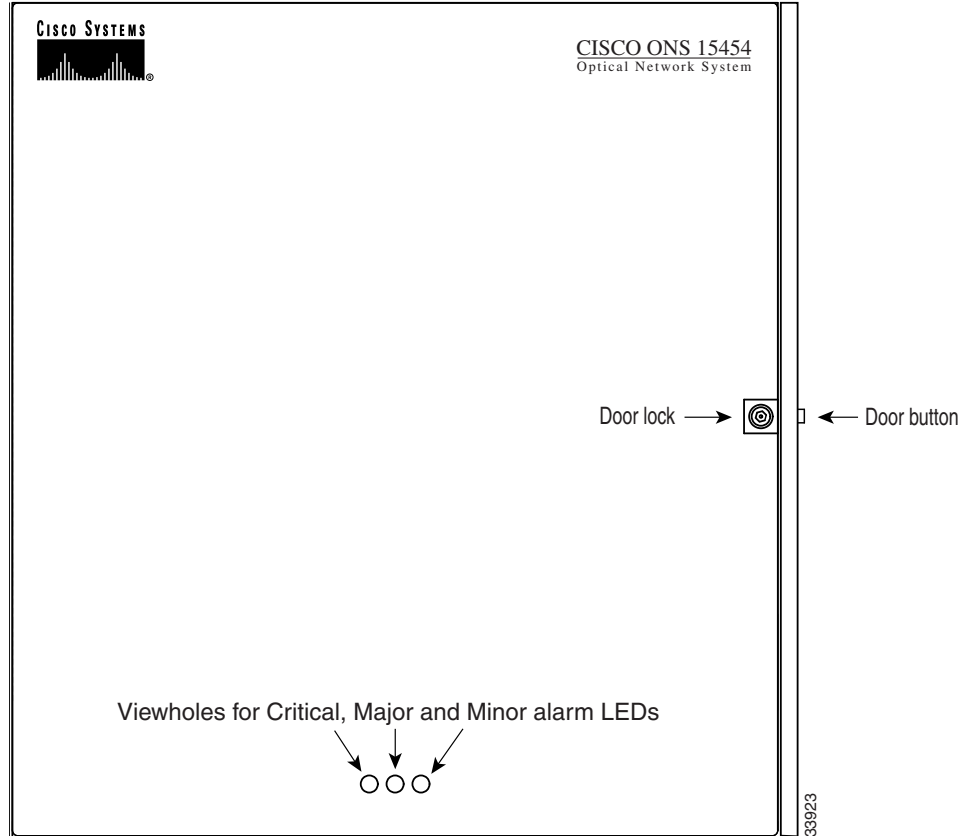


Caution

The ONS 15454 has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside edge of the shelf assembly on the right-hand side. It is labeled “ESD” on the top and bottom. Always wear an ESD wrist strap and connect the strap to the ESD plug when working on the ONS 15454.

- Step 1** Open the front door lock ([Figure 17-3](#)).
- The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.
- Step 2** Press the door button to release the latch.
- Step 3** Swing the door open.

Figure 17-3 Cisco ONS 15454 Front Door



Step 4 Return to your originating procedure (NTP).

DLP-A9 Remove the Front Door

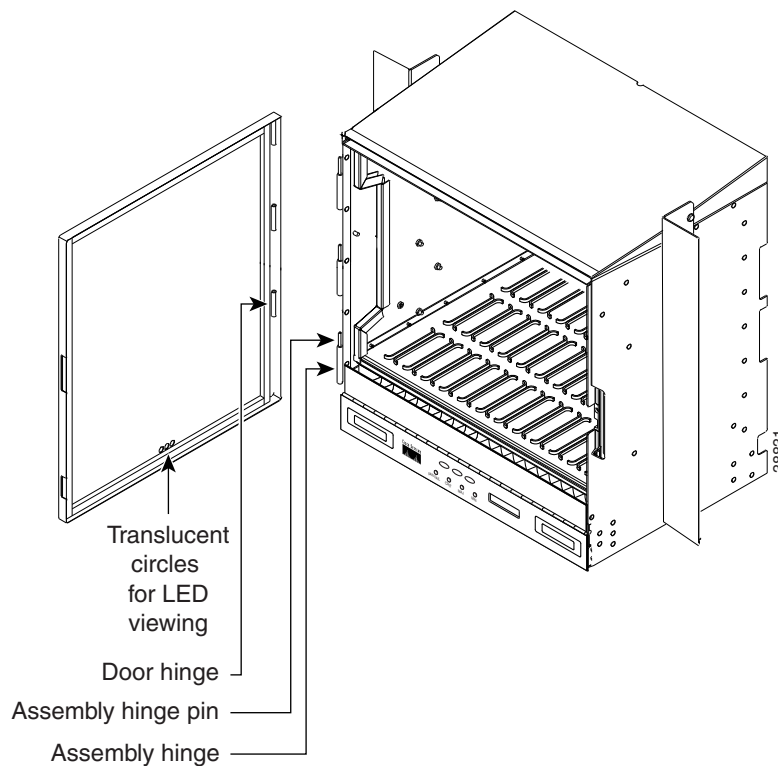
Purpose	This task removes the front cabinet compartment door.
Tools/Equipment	Open-end wrench
Prerequisite Procedures	DLP-A8 Open the Front Door, page 17-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

- Step 1** To remove the door ground strap (available in Release 3.3 and later), perform the following:
- To detach the ground strap from the front door, loosen the #6kepnut (49-0600-01) using the open-end wrench. Detach the end of the ground strap terminal lug (72-3622-01) from the male stud on the inside of the door.

- b. To detach the other end of the ground strap from the longer screw on the fiber guide, loosen the #4 kepnut (49-0337-01) on the terminal lug using the open-end wrench. Remove the terminal lug and lock washer.

Step 2 Lift the door from its hinges at the top left corner of the door (Figure 17-4).

Figure 17-4 Removing the ONS 15454 Front Door



Step 3 Return to your originating procedure (NTP).

DLP-A10 Remove the Lower Backplane Cover

Purpose	This task removes the lower backplane cover.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Step 1 Unscrew the five retaining screws that hold the cover in place.

- Step 2** Grasp the cover on each side.
- Step 3** Gently pull the cover away from the backplane.
- Step 4** Return to your originating procedure (NTP).
-

DLP-A11 Remove the Backplane Sheet Metal Cover

Purpose	This task removes the backplane sheet metal cover that is installed on the backplane when EIAs are not installed.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 17-10
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

- Step 1** To remove the backplane sheet metal cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- Step 2** Loosen the nine perimeter screws that hold the backplane sheet metal cover(s) in place.
- Step 3** Lift the panel by the bottom to remove it from the shelf assembly.
- Step 4** Store the panel for later use. Attach the backplane cover(s) whenever EIA(s) are not installed.
- Step 5** Return to your originating procedure (NTP).
-

DLP-A12 Install a BNC or High-Density BNC EIA

Purpose	This task installs a BNC or high-density BNC EIA. Use this task if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer a BNC interface to an SMB interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Perimeter screws (9) Inner screws (12) Backplane cover screws (5) BNC or high-density BNC card
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

-
- Step 1** Remove the BNC or high-density BNC card from the packaging. Line up the connectors on the card with the mating connectors on the backplane. Gently push the card until both sets of connectors fit together snugly.
- Step 2** Place the metal EIA panel over the card.
- Step 3** Insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the backplane.
- Step 4** Insert and tighten the twelve (BNC) or nine (high-density BNC) inner screws (P/N 48-0004) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the card and backplane.

[Figure 17-5](#) shows a BNC EIA installation.

Figure 17-5 *Installing the BNC EIA*

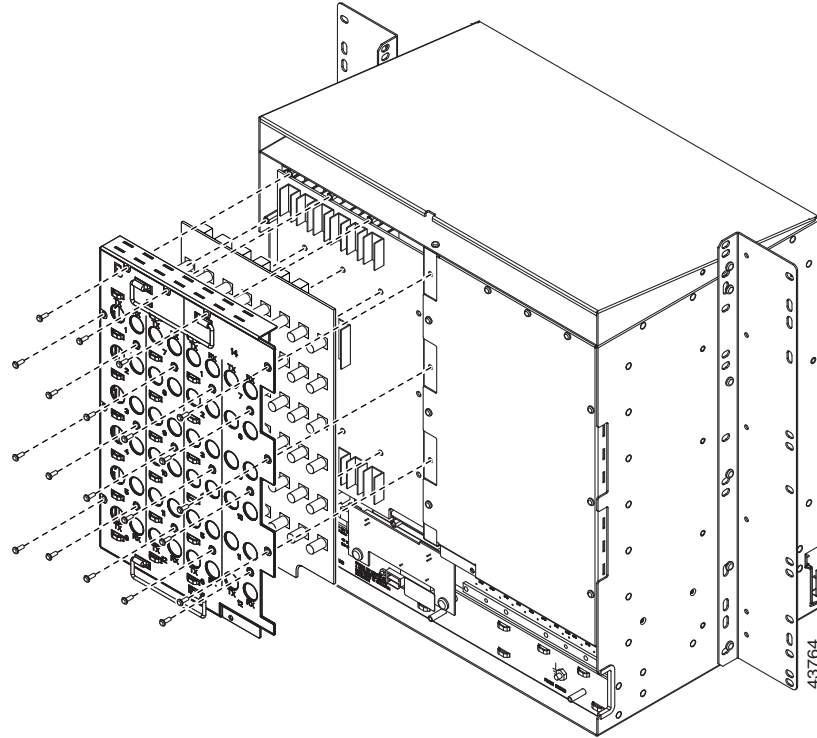
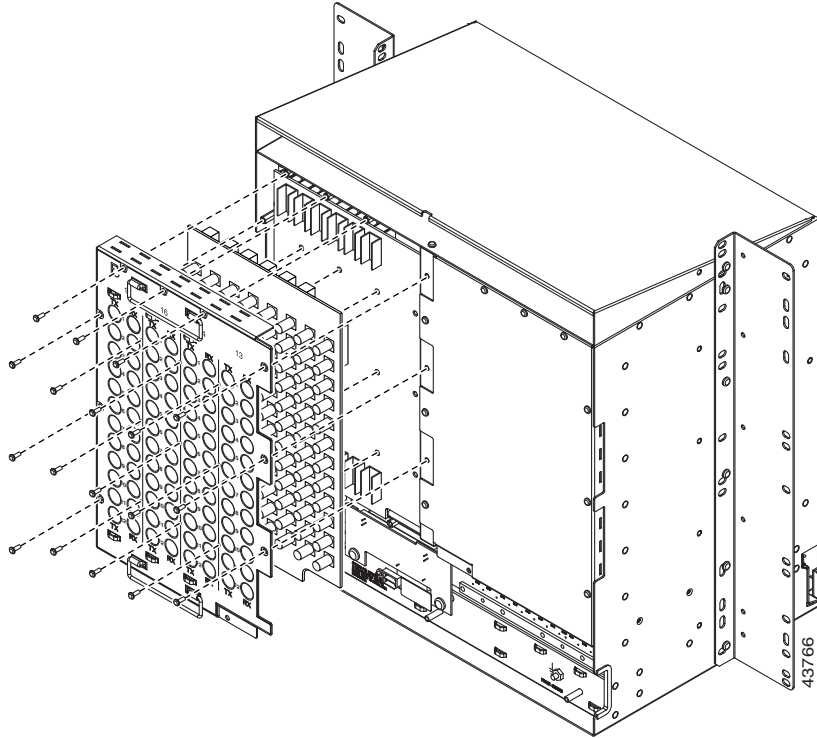


Figure 17-6 shows high-density BNC EIA installation.

Figure 17-6 Installing the High-Density BNC EIA



Step 5 Return to your originating procedure (NTP).

DLP-A13 Install an SMB EIA

Purpose	This task installs an SMB EIA. Use the SMB EIA if you are using DS1-14 cards and prefer an SMB interface to an AMP interface, or if you are using DS3-12, DS3XM-6, or EC-1 cards and prefer an SMB interface to a BNC interface.
Tools/Equipment	#2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws SMB card Foil EMI gasket (might already be installed on some SMB EIA assemblies) Metal SMB cover panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

-
- Step 1** Remove the SMB card from the packaging. Line up the connectors on the card with the mating connectors on the backplane. Gently push the card until both sets of connectors fit together snugly.
- Step 2** Place the foil EMI gasket over the SMB card so that the holes in the foil EMI gasket line up with the SMB connectors.

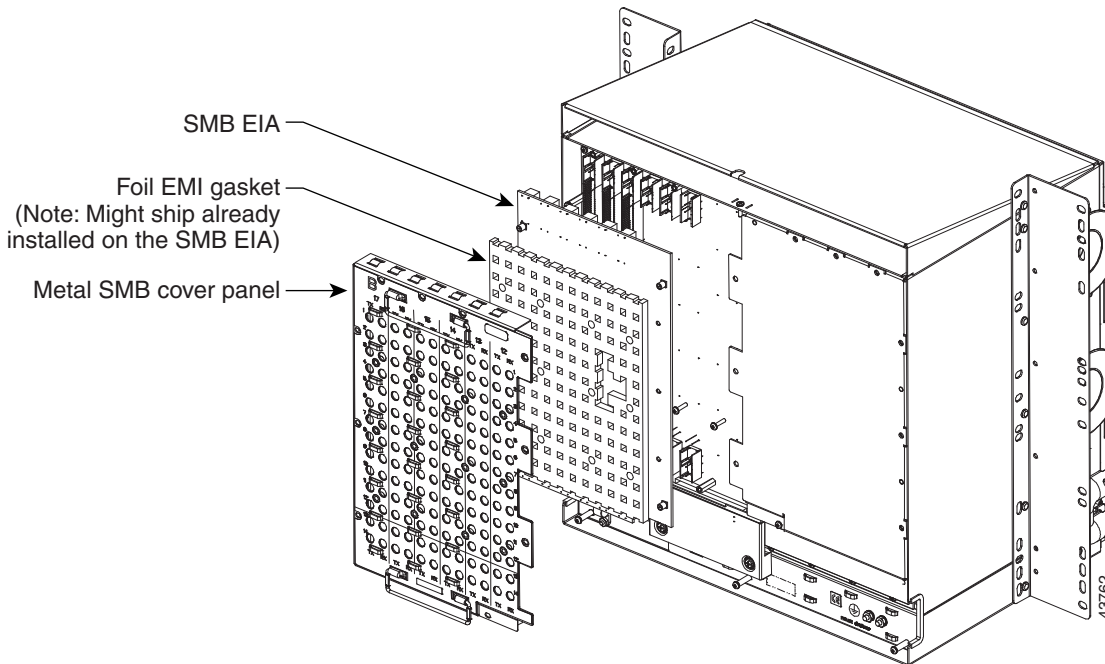


Caution The foil EMI gasket might ship already installed on the SMB EIA assembly. If it is not, you must install it to meet electromagnetic interference (EMI) guidelines.

- Step 3** Place the metal SMB cover panel over the card.
- Step 4** Insert and tighten the twelve inner screws (P/N 48-0004) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the card and backplane.
- Step 5** Insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb (3.6 to 4.5 kg) to secure the cover panel to the backplane.

If you are using SMB EIAs to make DS-1 connections, you need the DS-1 electrical interface adapter, commonly referred to as a balun (P/N 15454-WW-14=).

Figure 17-7 shows an SMB EIA installation.

Figure 17-7 Installing the SMB EIA (Use a Balun for DS-1 Connections)

Step 6 Return to your originating procedure (NTP).

DLP-A14 Install the AMP Champ EIA

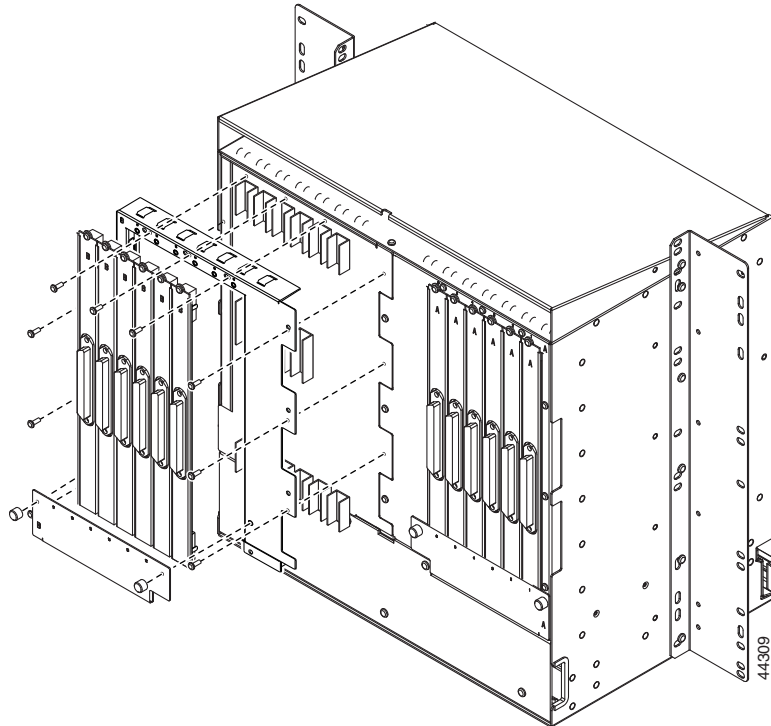
Purpose	This task installs an AMP Champ EIA. Use an AMP Champ EIA if you are using DS1-14 cards and prefer an AMP interface to an SMB interface.
Tools/Equipment	<ul style="list-style-type: none"> #2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver 9 perimeter screws 12 inner screws 5 backplane cover screws 6 AMP Champ cards EIA panel
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Align the AMP Champ panel with the backplane and insert and tighten the nine perimeter screws (P/N 48-0358) at 8 to 10 lb (3.6 to 4.5 kg).

- Step 2** Align an AMP Champ card with the backplane connector and push until it fits snugly. Repeat until you have installed all six AMP Champ cards.
- Step 3** To secure each AMP Champ card to the cover panel, insert and tighten a screw (P/N 48-0003) at the top of each card at 8 to 10 lb (3.6 to 4.5 kg).
- Step 4** Place the AMP Champ fastening plate along the bottom of the cover panel, and hand-tighten the two thumbscrews.

Figure 17-8 shows an AMP Champ EIA installation.

Figure 17-8 Installing the AMP Champ EIA



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

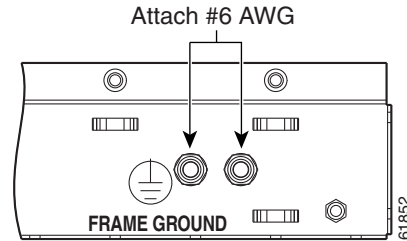
DLP-A16 Connect the Office Ground to the ONS 15454

Purpose	This task connects ground to the ONS 15454 shelf.
Tools/Equipment	<p>#2 Phillips screwdriver</p> <p>Medium slot-head screwdriver</p> <p>Small slot-head screwdriver</p> <p>Screws</p> <p>Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194 degrees F (90 degrees C) minimum</p> <p>Ground cable (from equipment frame to office ground), copper conductors, 194 degrees F (90 degrees C) minimum, according to local site practice</p> <p>Listed pressure terminal connectors, typically dual lug type; connectors must be suitable for #6 AWG copper conductors with stud size and spacing per equipment rack specifications; connection to office ground typically through H-TAP compression connector, according to site practice</p> <p>Wire cutters</p> <p>Wire strippers</p> <p>Crimp tool</p>
Prerequisite Procedures	DLP-A10 Remove the Lower Backplane Cover, page 17-10
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

-
- Step 1** Verify that the office ground cable is connected to the top of the bay and the office ground, according to local site practice.
- Since additional ground cables may be added according to local site practice, the ONS 15454 is designated for Common Bonding Network (CBN) installation only, as defined 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 bay frame ground posts. The mating surfaces must be cleaned and an appropriate antioxidant compound must be applied to the bare conductors.
- Step 3** Attach one end of the shelf ground cable (#6 AWG) to the frame ground posts on the shelf, using the specified dual-hole lug connector. See [Figure 17-9](#) for the location of the ground on the backplane.



Note When terminating a frame ground, use the kep nuts provided with the ONS 15454 and tighten it to a torque specification of 31 in-lb. The kep nut provides a frame ground connection that minimizes the possibility of loosening caused by rotation during installation and maintenance activity. The type of prevention the kep nut provides for the frame ground connection is inherently provided by the terminal block for battery and battery return connections.

Figure 17-9 Ground Location on the Backplane

- Step 4** Attach the other end of the shelf ground cable to the equipment bay frame using a dual-hole connector lug per equipment bay frame specifications.
- Step 5** Return to your originating procedure (NTP).

DLP-A17 Connect Office Power to the ONS 15454 Shelf

Purpose	This task connects power to the ONS 15454 shelf.
Tools/Equipment	<ul style="list-style-type: none"> #2 Phillips screwdriver Medium slot-head screwdriver Small slot-head screwdriver Wire cutters Wire strippers Crimp tool Fuse panel Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194 degrees F [90 degrees C] minimum) Ground cable #6 AWG stranded
Prerequisite Procedures	DLP-A16 Connect the Office Ground to the ONS 15454, page 17-18
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

Warning

When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 202



Note

The battery return connection is treated as DC-I, as defined in Telcordia GR-1089-CORE Issue 4.



Note

If the system loses power or both TCC2/TCC2P cards are reset and the system is not provisioned to get the time from a Network Time Protocol/Simple Network Time Protocol (NTP/SNTP) server, you must reset the ONS 15454 clock. After powering down, the date defaults to January 1, 1970, 00:04:15. To reset

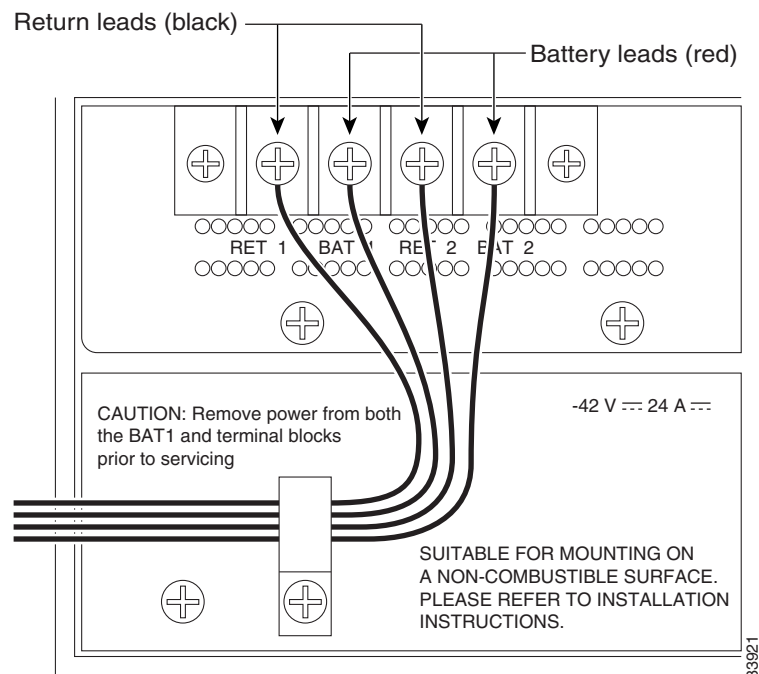
the clock, see the “NTP-A25 Set Up Name, Date, Time, and Contact Information” procedure on page 4-5. If you are using the TCC2/TCC2P cards, the system clock will be kept running for up to three hours. In this case, no action would be required.

**Note**

If you encounter problems with the power supply, refer to the *Cisco ONS 15454 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 15454 from the fuse panel. [Figure 17-10](#) shows the ONS 15454 power terminals.
- Step 3** Dress the power cabling according to local site practice.

Figure 17-10 Cisco ONS 15454 Power Terminals



- Step 4** Remove or loosen the #8 power terminal screws on the ONS 15454. To avoid confusion, label the cables connected to the BAT1/RET1 (A) power terminals as 1, and the cables connected to the BAT2/RET2 (B) power terminals as 2.

**Note**

Use only pressure terminal connectors, including ring, fork, and dual-lug types, when terminating the battery, battery return, and frame ground conductors.

**Caution**

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

**Caution**

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

Step 5 Strip 1/2 inch (12.7 mm) of insulation from all power cables that you will use.

Step 6 Crimp the lugs onto the ends of all power leads.

**Note**

When terminating battery and battery return connections as shown in [Figure 17-10](#), follow a torque specification of 10 in-lb.

Step 7 Terminate the return 1 lead to the RET1 backplane terminal. Use oxidation-prevention grease to keep connections noncorrosive.

Step 8 Terminate the negative 1 lead to the negative BAT1 backplane power terminal. Use oxidation prevention grease to keep connections noncorrosive.

Step 9 If you use redundant power leads, terminate the return 2 lead to the positive RET2 terminal on the ONS 15454. Terminate the negative 2 lead to the negative BAT2 terminal on the ONS 15454. Use oxidation-preventative grease to keep connections noncorrosive.

**Note**

The configured ONS 15454 shelf can work with a single power line since the ONS 15454 power configuration offers redundancy. When using the 15454-FTA3 fan tray, if the ONS15454 shelf is powered by a single power line, the BAT-FAIL alarm appears, the fans run at a maximum speed, and the system does not comply with NEBS GR-63 Issue 3 and GR-1089 Issue 4 and 5 requirements. In order to meet the above mentioned NEBS requirements, the ONS 15454 shelf must be powered by both the DC power lines.


Step 10 Route the cables out below the power terminals using the plastic cable clamp, as shown in [Figure 17-10](#) on page 17-20.

Step 11 Connect the return cables to earth ground at power supply side.

Step 12 Return to your originating procedure (NTP).

DLP-A18 Turn On and Verify Office Power

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	DLP-A16 Connect the Office Ground to the ONS 15454, page 17-18 DLP-A17 Connect Office Power to the ONS 15454 Shelf, page 17-19
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

-
- Step 1** Using a voltmeter, verify the office battery and ground at the following points on the fuse and alarm panel:
- 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 -40.5 VDC and -57 VDC. Place the red test lead on the B-side connection and verify that it is between -40.5 VDC and -57 VDC.
-  **Note** The minimum and maximum voltages required to power the chassis are -40.5 VDC and -57 VDC respectively. The nominal voltage value is -48.0 V.
- 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. The voltmeter must read 0 VDC. Place the red test lead on the B-side return ground and verify that no voltage is present. The voltmeter must read 0 VDC.
- Step 2** Complete one of the following to power up the node:
- If you are using a 80-A fuse panel, insert a 20-A fuse into the fuse position according to site practice.
 - If you are using a 100-A fuse panel, insert a 30-A fuse into the fuse position according to site practice.
- Step 3** Return to your originating procedure (NTP).
-

DLP-A19 Install Alarm Wires on the Backplane

Purpose	This task installs alarm wires on the backplane so that you can provision external (environmental) alarms and controls with the Alarm Interface Controller–International (AIC-I) card. If you are using the alarm extension panel (AEP), do not perform this task.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm ² or 0.64 mm ²) wires 100-ohm shielded building integrated timing supply (BITS) clock cable pair #22 or #24 AWG (0.51 mm ² or 0.64 mm ²), twisted-pair T1-type
Prerequisite Procedures	None
Required/As Needed	As needed

Onsite/Remote	Onsite
Security Level	None

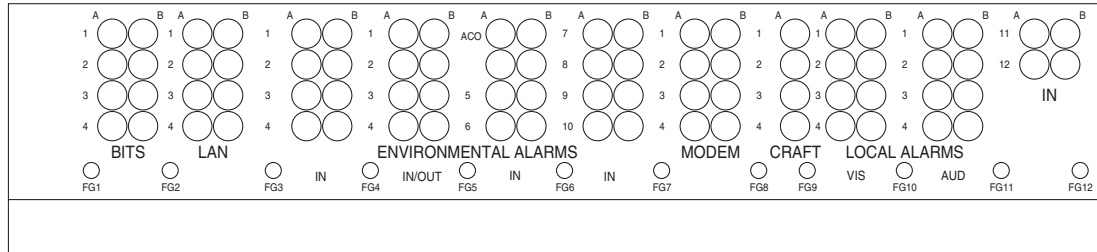
- Step 1** Using 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²) twisted-pair T1-type wires, wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. Ground the shield of the BITS Input cable at the BITS end. For BITS Output, wrap the ground shield of the BITS cable to the frame ground pin (FG1) located below the column of BITS pins.

[Figure 17-11](#) shows alarm pin assignments for the AIC-I in the Release 3.4 or higher ONS 15454 backplane.



Note The AIC-I requires a shelf assembly running Software Release 3.4.0 or later. The backplane of the ANSI shelf contains a wire-wrap field with pin assignment according to the layout in [Figure 17-11](#). The shelf assembly might be an existing shelf that has been upgraded to R3.4 or later. In this case, the backplane pin labeling will appear as indicated in [Figure 17-13 on page 17-25](#), but you must use the pin assignments provided by the AIC-I as shown in [Figure 17-11](#).

Figure 17-11 Cisco ONS 15454 Backplane Pinouts (Release 3.4 or Later)



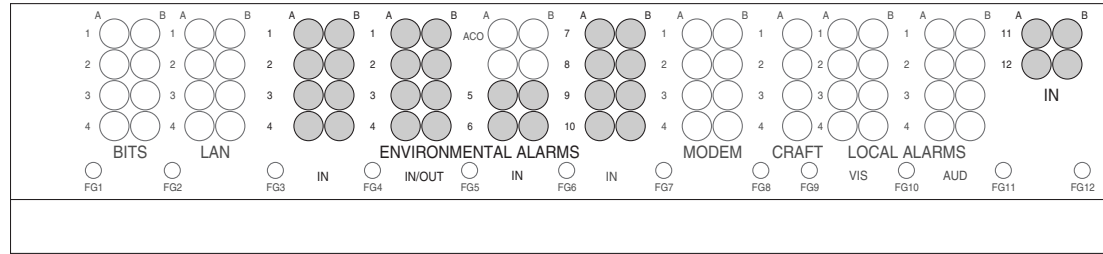
Field	Pin	Function	Field	Pin	Function	
BITS	A1	BITS Output 2 negative (-)	ENVIR ALARMS IN/OUT	A1/A13	Normally open output pair number 1	
	B1	BITS Output 2 positive (+)		B1/B13		
	A2	BITS Input 2 negative (-)		A2/A14	Normally open output pair number 2	
	B2	BITS Input 2 positive (+)		B2/B14		
	A3	BITS Output 1 negative (-)	N/O	A3/A15	Normally open output pair number 3	
	B3	BITS Output 1 positive (+)		B3/B15		
	A4	BITS Input 1 negative (-)		A4/A16	Normally open output pair number 4	
	B4	BITS Input 1 positive (+)		B4/B16		
LAN	Connecting to a hub, or switch		ACO	A1	Normally open ACO pair	
	A1	RJ-45 pin 6 RX-		B1		
	B1	RJ-45 pin 3 RX+	CRAFT	A1	Receive (PC pin #2)	
	A2	RJ-45 pin 2 TX-		A2	Transmit (PC pin #3)	
	B2	RJ-45 pin 1 TX+		A3	Ground (PC pin #5)	
	A1			Connecting to a PC/Workstation or router	A4	DTR (PC pin #4)
	B1	RJ-45 pin 2 RX-	LOCAL ALARMS AUD (Audible)		A1	Alarm output pair number 1: Remote audible alarm.
	A2	RJ-45 pin 6 TX-			A2	Alarm output pair number 2: Critical audible alarm.
B2	RJ-45 pin 3 TX+	B2				
A1	ENVIR ALARMS IN	Alarm input pair number 1: Reports closure on connected wires.		N/O	A3	Alarm output pair number 3: Major audible alarm.
B1		Alarm input pair number 2: Reports closure on connected wires.	B3		Alarm output pair number 3: Major audible alarm.	
A2		Alarm input pair number 3: Reports closure on connected wires.	A4		Alarm output pair number 4: Minor audible alarm.	
B2		Alarm input pair number 4: Reports closure on connected wires.	B4		Alarm output pair number 4: Minor audible alarm.	
A3		Alarm input pair number 5: Reports closure on connected wires.	LOCAL ALARMS VIS (Visual)	A1	Alarm output pair number 1: Remote visual alarm.	
B3		Alarm input pair number 6: Reports closure on connected wires.		B1	Alarm output pair number 2: Critical visual alarm.	
A4		Alarm input pair number 7: Reports closure on connected wires.		A2	Alarm output pair number 2: Critical visual alarm.	
B4		Alarm input pair number 8: Reports closure on connected wires.		B2		
A5		Alarm input pair number 9: Reports closure on connected wires.	N/O	A3	Alarm output pair number 3: Major visual alarm.	
B5		Alarm input pair number 10: Reports closure on connected wires.		B3	Alarm output pair number 3: Major visual alarm.	
A6		Alarm input pair number 11: Reports closure on connected wires.		A4	Alarm output pair number 4: Minor visual alarm.	
B6		Alarm input pair number 12: Reports closure on connected wires.		B4	Alarm output pair number 4: Minor visual alarm.	
A7	Alarm input pair number 7: Reports closure on connected wires.					
A8	Alarm input pair number 8: Reports closure on connected wires.					
A9	Alarm input pair number 9: Reports closure on connected wires.					
A10	Alarm input pair number 10: Reports closure on connected wires.					
A11	Alarm input pair number 11: Reports closure on connected wires.					
A12	Alarm input pair number 12: Reports closure on connected wires.					
A12	Alarm input pair number 12: Reports closure on connected wires.					

If you are using an AIC-I card, contacts provisioned as OUT are 1-4. Contacts provisioned as IN are 13-16.

83020

Figure 17-12 describes the environmental alarm pins on the backplane for Release 3.4 or later.

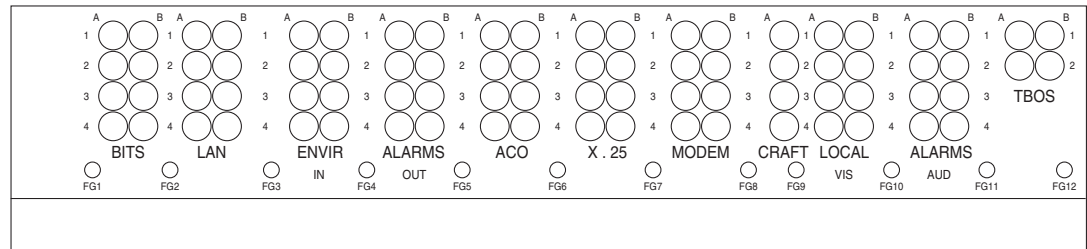
Figure 17-12 Highlighted Environmental Alarms



83020

Figure 17-13 shows alarm pin assignments in a shelf for Release 3.3 and earlier. The AIC-I is incompatible with shelves Release 3.3 or earlier.

Figure 17-13 Cisco ONS 15454 Backplane Pinouts (Release 3.3 or Earlier)



Field	Pin	Function	Field	Pin	Function	
BITS	A1	BITS Output 2 negative (-)	ENVIR ALARMS OUT	A1	Normally open output pair number 1	
	B1	BITS Output 2 positive (+)		B1		
	A2	BITS Input 2 negative (-)		N/O	A2	Normally open output pair number 2
	B2	BITS Input 2 positive (+)			B2	
	A3	BITS Output 1 negative (-)	A3		Normally open output pair number 3	
	B3	BITS Output 1 positive (+)	B3			
	A4	BITS Input 1 negative (-)	A4	Normally open output pair number 4		
	B4	BITS Input 1 positive (+)	B4			
LAN	Connecting to a hub, or switch		ACO	A1	Normally open ACO pair	
	A1	RJ-45 pin 6 RX-		B1		
	B1	RJ-45 pin 3 RX+	CRAFT	A1	Receive (PC pin #2)	
	A2	RJ-45 pin 2 TX-		A2	Transmit (PC pin #3)	
	B2	RJ-45 pin 1 TX+		A3	Ground (PC pin #5)	
	Connecting to a PC/Workstation or router			A4	DTR (PC pin #4)	
	A1	RJ-45 pin 2 RX-	LOCAL ALARMS AUD (Audible)	A1	Alarm output pair number 1: Remote audible alarm.	
	B1	RJ-45 pin 1 RX+		B1		
A2	RJ-45 pin 6 TX-	A2		Alarm output pair number 2: Critical audible alarm.		
B2	RJ-45 pin 3 TX+	B2				
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.	N/O	A3	Alarm output pair number 3: Major audible alarm.	
	B1	Alarm input pair number 2: Reports closure on connected wires.		B3		
	A2	Alarm input pair number 2: Reports closure on connected wires.		A4	Alarm output pair number 4: Minor audible alarm.	
	B2	Alarm input pair number 2: Reports closure on connected wires.		B4		
	A3	Alarm input pair number 3: Reports closure on connected wires.	LOCAL ALARMS VIS (Visual)	A1	Alarm output pair number 1: Remote visual alarm.	
	B3	Alarm input pair number 3: Reports closure on connected wires.		B1		
	A4	Alarm input pair number 4: Reports closure on connected wires.		A2	Alarm output pair number 2: Critical visual alarm.	
	B4	Alarm input pair number 4: Reports closure on connected wires.		B2		
		N/O	A3	Alarm output pair number 3: Major visual alarm.		
			B3			
			A4	Alarm output pair number 4: Minor visual alarm.		
			B4			

38533



Note The X.25, Modem, and TBOS pin fields are not active.

Step 2 Return to your originating procedure (NTP).

DLP-A20 Install Timing Wires on the Backplane

Purpose	This task installs the BITS timing wires on the backplane.
Tools/Equipment	Wire wrapper 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm ² or 0.64 mm ²), twisted-pair T1-type
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Using 100-ohm shielded BITS clock cable pair #22 or #24 AWG (0.51 mm² or 0.64 mm²), twisted-pair T1-type, wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

Ground the shield of the BITS input cable at the BITS end. For BITS output, wrap the ground shield of the BITS cable to the frame ground pin (FG1) located beneath the column of BITS Pins. [Table 17-1](#) lists the pin assignments for the BITS timing pin fields.

Table 17-1 External Timing Pin Assignments for BITS

BITS Pin	Tip/Ring	CTC/TL1 Name	Function
A4	ring	BITS-1	Input from BITS device 1
B4	tip	BITS-1	Input from BITS device 1
A3	ring	BITS-1	Output to external device 1
B3	tip	BITS-1	Output to external device 1
A2	ring	BITS-2	Input from BITS device 2
B2	tip	BITS-2	Input from BITS device 2
A1	ring	BITS-2	Output to external device 2
B1	tip	BITS-2	Output to external device 2



Note For more detailed information about timing, refer to the “Timing” chapter of the *Cisco ONS 15454 Reference Manual*. To set up system timing, see the “NTP-A28 Set Up Timing” procedure on page 4-12.

Step 2 Return to your originating procedure (NTP).

DLP-A21 Install LAN Wires on the Backplane

Purpose	This task installs the LAN wires on the backplane.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm ² or 0.64 mm ²) wire, preferably CAT-5 UTP
Prerequisite Procedures	None
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note

Rather than using the LAN wires, you can use the LAN connection port on the TCC2/TCC2P if preferred. Use either the backplane connection or the TCC2/TCC2P front connection. You cannot use the LAN backplane pins and the LAN connection port on the TCC2/TCC2P simultaneously; however, it is possible for you to make a direct connection from a computer to the LAN connection port on the TCC2/TCC2P while the LAN backplane pins are in use, as long as the computer that is connected directly to the TCC2/TCC2P is not connected to the same LAN. The LAN ports of the ONS15454 are suitable for connection only to shielded intra-building cabling grounded at both ends (STP cables).

Step 1

Using #22 or #24 AWG (0.51 mm² or 0.64 mm²) wire or CAT-5 STP Ethernet cable, wrap the wires on the appropriate wire-wrap pins according to local site practice.



Caution

Crosstalk might result if both receive (Rx) and transmit (Tx) pins connect on the same twisted pair of wires from the CAT-5 cable. The two Tx pins need to be on one twisted pair, and the two Rx pins need to be on another twisted pair.

A frame ground pin is located beneath each pin field (FG2 for the LAN pin field). Wrap the ground shield of the LAN interface cable to the frame ground pin. [Table 17-2](#) shows the LAN pin assignments.

Table 17-2 LAN Pin Assignments

Pin Field	Backplane Pins	RJ-45 Pins	Function/Color
LAN 1 Connecting to data circuit-terminating equipment (DCE*) (a hub or switch); the ONS 15454 is a DCE	B2	1	TX+ white/green
	A2	2	TX- green
	B1	3	RX+ white/orange
	A1	6	RX- orange
LAN 1 Connecting to data terminal equipment (DTE) (a PC/workstation or router)	B1	1	RX+ white/green
	A1	2	RX- green
	B2	3	TX+ white/orange
	A2	6	TX- orange



Note The TCC2/TCC2P does not support Ethernet polarity detection. If your Ethernet connection has incorrect polarity (this can only occur with cables that have the receive wire pairs flipped), a “Lan Connection Polarity Reversed” condition is raised. This condition usually occurs during an upgrade or initial node deployment. To correct the situation, ensure that your Ethernet cable has the correct mapping of the wire-wrap pins.

Step 2 Return to your originating procedure (NTP).

DLP-A22 Install the TL1 Craft Interface

Purpose	This task installs the TL1 craft interface using the craft backplane pins. You can also use a LAN cable connected to the EIA/TIA-232 port on the TCC2/TCC2P card to access a TL1 craft interface.
Tools/Equipment	Wire wrapper #22 or #24 AWG (0.51 mm ² or 0.64 mm ²) alarm wires
Prerequisite Procedures	NTP-A4 Remove the Backplane Covers, page 1-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note Rather than using the craft pins, you can use a LAN cable connected to the EIA/TIA-232 port on the TCC2/TCC2P card to access a TL1 craft interface.

Step 1 Using #22 or #24 AWG (0.51 mm² or 0.64 mm²) wire, wrap the craft interface wires on the appropriate wire-wrap pins according to local site practice.

Step 2 Wrap the ground shield of the craft interface cable to the frame-ground pin.
Wrap the ground wire of your computer cable to Pin A3 on the craft pin field. [Table 17-3](#) shows the pin assignments for the CRAFT pin field.



Note You cannot use the craft backplane pins and the EIA/TIA-232 port on the TCC2/TCC2P card simultaneously. Using a combination prevents access to the node or causes a loss in connectivity.

Table 17-3 *Craft Interface Pin Assignments*

Pin Field	Contact	Function
Craft	A1	Receive
	A2	Transmit
	A3	Ground
	A4	DTR

Step 3 Return to your originating procedure (NTP).

DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun)

Purpose	This task installs the DS-1 cables on an SMB EIA using the electrical interface adapters.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-A13 Install an SMB EIA, page 17-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note All DS-1 cables connected to the ONS 15454 DS-1 ports must terminate with twisted-pair cables to connect to the DS-1 electrical interface adapter. The DS-1 electrical interface adapters project 1.72 inches (43.7 mm) beyond the SMB EIA. Refer to the “Shelf and Backplane Hardware” chapter in the *Cisco ONS 15454 Reference Manual* for more information.

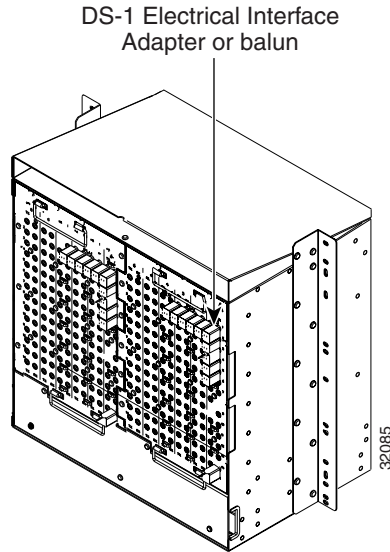
- Step 1** Attach the SMB connector on an adapter to the SMB connector for the port’s transmit pair on the backplane.
- Step 2** Attach the SMB connector on an adapter to the SMB connector for the port’s receive pair on the backplane.
- Step 3** Terminate the DS-1 transmit and receive cables for the port to the wire-wrap posts on the adapter:
- a. Using a wire-wrap tool, connect the receive cables to the receive adapter pins on the backplane connector for the desired port.
 - b. Connect the transmit cables to the transmit adapter pins on the backplane connector for the desired port.
 - c. Terminate the shield ground wire on the DS-1 cable to ground according to local site practice.



Note If you put DS1N-14 cards in Slots 3 and 15 to form 1:N protection groups, do not wire Slots 3 and 15 for DS-1 electrical interface adapters.

[Figure 17-14](#) shows a ONS 15454 backplane with an SMB EIA. DS-1 electrical interface adapters are attached on both sides of the shelf assembly to create DS-1 twisted-pair termination points.

Figure 17-14 Backplane with an SMB EIA for DS-1 Cables



Step 4 Return to your originating procedure (NTP).

DLP-A24 Install DS-1 AMP Champ Cables on the AMP Champ EIA

Purpose	This task installs the DS-1 AMP Champ cables on the AMP Champ EIA.
Tools/Equipment	Wire wrapper Twisted-pair cables
Prerequisite Procedures	DLP-A14 Install the AMP Champ EIA, page 17-16
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Prepare a 56-wire cable for each DS1-14/DS1N-14 card you will install in the shelf assembly.

Step 2 Connect the male AMP Champ connector on the cable to the female AMP Champ connector on the ONS 15454 backplane.

Step 3 Use the clips on the male AMP Champ connector to secure the connection.

The female connector has grooves on the outside edge for snapping the clips into place.

[Table 17-4](#) shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA.



Note In [Table 17-4](#), the shaded area corresponds to the white/orange binder group. A binder group is a set of 25 pairs of wires coded with an industry-standard color scheme.

Table 17-4 Pin Assignments for AMP Champ Connectors

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 yellow/orange	17	49	Rx Ring 1 orange/yellow
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 yellow/green	18	50	Rx Ring 2 green/yellow
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 yellow/brown	19	51	Rx Ring 3 brown/yellow
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 yellow/slate	20	52	Rx Ring 4 slate/yellow
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 ¹ white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare0+ Not applicable	15	47	Tx Spare0- Not applicable	Rx Spare0+ Not applicable	31	63	Rx Spare0- Not applicable
Tx Spare1+ Not applicable	16	48	Tx Spare1- Not applicable	Rx Spare1+ Not applicable	32	64	Rx Spare1- Not applicable

1. Pins 26, 27, 28, 29, 30, 58, 59, 60, 61, and 62 correspond to the white/orange binder group. A binder group is a set of 25 pairs of wires coded with an industry-standard color scheme.

Table 17-5 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA for a shielded DS-1 cable.

Table 17-5 Pin Assignments for AMP Champ Connectors (Shielded DS1 Cable)

64-Pin Blue Bundle				64-Pin Orange Bundle			
Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 white/blue	17	49	Rx Ring 1 blue/white
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 white/orange	18	50	Rx Ring 2 orange/white
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 white/green	19	51	Rx Ring 3 green/white
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 white/brown	20	52	Rx Ring 4 brown/white
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 white/slate	21	53	Rx Ring 5 slate/white
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 red/blue	22	54	Rx Ring 6 blue/red
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 red/orange	23	55	Rx Ring 7 orange/red
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 red/green	24	56	Rx Ring 8 green/red
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 red/brown	25	57	Rx Ring 9 brown/red
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 red/slate	26	58	Rx Ring 10 slate/red
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 black/blue	27	59	Rx Ring 11 blue/black
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 black/orange	28	60	Rx Ring 12 orange/black
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 black/green	29	61	Rx Ring 13 green/black
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 black/brown	30	62	Rx Ring 14 brown/black
Tx Tip 15 black/slate	15	47	Tx Tip 15 slate/black	Rx Tip 15 black/slate	31	63	Rx Tip 15 slate/black
Tx Tip 16 yellow/blue	16	48	Tx Tip 16 blue/yellow	Rx Tip 16 yellow/blue	32	64	Rx Tip 16 blue/yellow

Step 4 Return to your originating procedure (NTP).

DLP-A25 Install Coaxial Cable With BNC Connectors

Purpose	This task installs the coaxial cable with BNC connectors.
Tools/Equipment	None
Prerequisite Procedures	DLP-A12 Install a BNC or High-Density BNC EIA, page 17-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

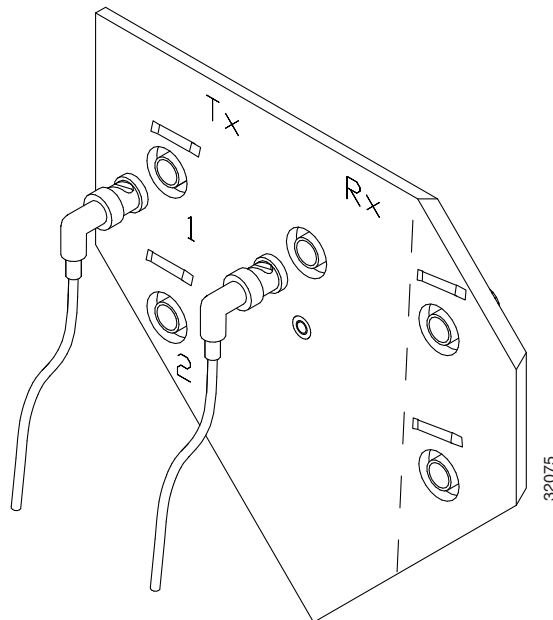


Warning

Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3 etc.) must be connected through a registered or approved device such as CSU/DSU or NT1. Statement 290

- Step 1** Place the BNC cable connector over the desired connection point on the backplane.
- [Figure 17-15](#) shows how to connect a coaxial cable to the BNC EIA using a right-angle BNC cable connector.

Figure 17-15 Using a Right-Angle Connector to Install Coaxial Cable with BNC Connectors



- Step 2** Position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.
- Step 3** Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.
- Step 4** Turn the cable connector clockwise to lock it into place.
- Step 5** Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.

- Step 6** Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice. The rubber-coated edges of the side cutouts prevent the cables from chafing.
- Step 7** Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.
- Step 8** Return to your originating procedure (NTP).
-

DLP-A26 Install Coaxial Cable With High-Density BNC Connectors

Purpose	This task installs the coaxial cable with high-density BNC connectors.
Tools/Equipment	BNC insertion tool
Prerequisite Procedures	DLP-A12 Install a BNC or High-Density BNC EIA, page 17-12
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

- Step 1** Place the cable connector over the desired connection point on the backplane.
- Step 2** Using the BNC insertion tool, position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.
- Step 3** Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.
- Step 4** Turn the cable connector clockwise to lock it into place.
- Step 5** Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.
- Step 6** Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice.
The rubber-coated edges of the side cutouts prevent the cables from chafing.
- Step 7** Return to your originating procedure (NTP).
-

DLP-A27 Install Coaxial Cable with SMB Connectors

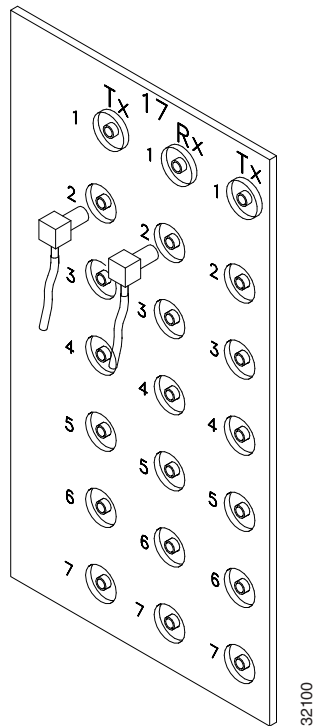
Purpose	This task installs the coaxial cable with SMB connectors.
Tools/Equipment	SMB cable connector
Prerequisite Procedures	DLP-A13 Install an SMB EIA, page 17-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

**Warning**

Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3 etc.) must be connected through a registered or approved device such as CSU/DSU or NT1. Statement 290

- Step 1** Place the SMB cable connector over the desired connection point on the backplane (Figure 17-16).

Figure 17-16 *Installing Coaxial Cable with SMB Connectors*



- Step 2** Gently push the connector until it clicks into place.
- Step 3** Tie wrap or lace the cables to the EIA according to Telcordia standards (GR-1275-CORE) or local site practice.
- Step 4** Route the cables to the nearest side of the shelf assembly into rack runs according to local site practice.
- Step 5** Label the transmit, receive, working, and protect cables at each end of the connection to avoid confusion with cables that are similar in appearance.
- Step 6** Return to your originating procedure (NTP).

DLP-A28 Route Coaxial Cables

Purpose	This task routes the coaxial cables.
Tools/Equipment	RG179, RG59 (735A) #26 AWG cable, or RG59 (734A) #20 AWG cable
Prerequisite Procedures	One or more of the following tasks, as needed: <ul style="list-style-type: none"> • DLP-A25 Install Coaxial Cable With BNC Connectors, page 17-33 • DLP-A26 Install Coaxial Cable With High-Density BNC Connectors, page 17-34 • DLP-A27 Install Coaxial Cable with SMB Connectors, page 17-34
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Tie wrap or lace the coaxial cables according to local site practice and route the cables through the side cutouts on either side of the ONS 15454. The rubber coated edges of the side cutouts prevent the cables from chafing.

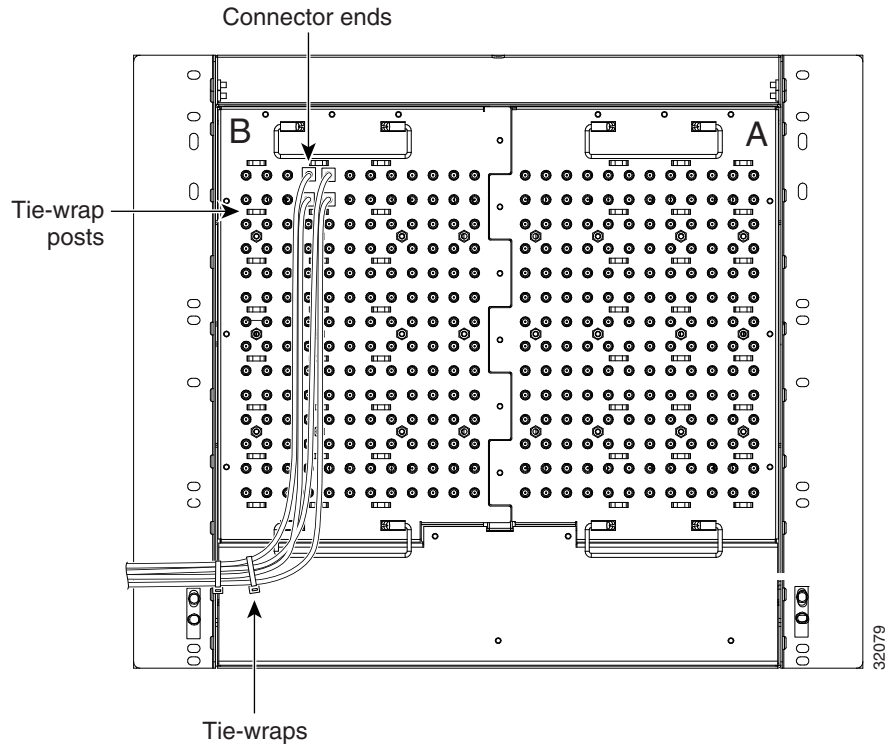
Step 2 Use short lengths of pigtail RG179 to terminate the shelf assembly.

Step 3 Use standard RG59 (735A) cable connected to the RG179 for the remainder of the cable run. When using a 10-foot (3.05-m) section of the RG179, you can attach a maximum length of 437 feet (133 m) of RG59 (735A). When using a 30-foot (9.1-m) section of RG179, you can attach a maximum length of 311 feet (94.8 m) of RG59 (735A).

When using the RG179 cable, the maximum distance available (122 feet, 37.2 m) is less than the maximum distance available with standard RG59 (735A) cable (306 feet, 93.3 m). The maximum distance when using the RG59 (734A) cable is 450 feet (137.2 m). The shorter maximum distance available with the RG179 is due to a higher attenuation rate for the thinner cable. Attenuation rates are calculated using a DS-3 signal:

- For RG179, the attenuation rate is 59 dB/kft (dB per kilo-foot) at 22 MHz.
- For RG59 (735A), the attenuation rate is 23 dB/kft at 22 MHz.

Use a figure of 5.0 for total cable loss when making calculations. [Figure 17-17](#) shows an example of proper coaxial cable routing.

Figure 17-17 Routing Coaxial Cable (SMB EIA Backplane)

Step 4 Return to your originating procedure (NTP).

DLP-A29 Route DS-1 Twisted-Pair Cables

Purpose	This task routes the DS-1 twisted-pair cables.
Tools/Equipment	None
Prerequisite Procedures	DLP-A23 Install DS-1 Cables Using Electrical Interface Adapters (Balun) , page 17-29
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Verify the following:

- DS-1 electrical interface adapters are installed on every transmit and receive connector for DS-1 ports.
- Wire-wrap posts on the DS-1 electrical interface adapters are used to connect the terminated incoming cables.

Step 2 Tie-wrap or lace the twisted-pair cables according to local site practice and route the cables into the side cutouts on either side of the ONS 15454.



Note SMB EIAs feature cable-management eyelets for tie wrapping or lacing cables to the cover panel.

Step 3 Return to your originating procedure (NTP).

DLP-A32 Inspect the Shelf Installation and Connections

Purpose	Use this task to inspect the shelf installation and connections and to verify that everything is installed and connected properly.
Tools/Equipment	None
Prerequisite Procedures	Complete Table 1-5 on page 1-31
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

- Step 1** Check each wire and cable connection to make sure all cables are locked securely. If a wire or cable is loose, return to the applicable installation procedure to correct it.
- Step 2** To check that the backplane is seated correctly, verify that the screw holes and the backplane interface card holes align properly and that the A and B connectors interlock.
- Step 3** Return to your originating procedure (NTP).
-

DLP-A33 Measure Voltage

Purpose	This task measures the power to verify correct power and returns.
Tools/Equipment	Voltmeter
Prerequisite Procedures	Complete Table 1-5 on page 1-31 .
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None

- Step 1** Using a voltmeter, verify the office ground and power. [Figure 17-10 on page 17-20](#) shows the power terminals.
- Place the black lead (positive) on the frame ground on the bay. Hold it there while completing Step **b**.
 - Place the red lead (negative) on the fuse power points and alarm panel to verify that they read between -40.5 VDC and -57 VDC (power) or 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 -40.5 VDC and -57 VDC. If there is no voltage, check the following and correct if necessary:
 - Battery and ground are 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-A36 Install the TCC2/TCC2P Cards

Purpose	This task installs redundant TCC2/TCC2P cards. The first card you install in the ONS 15454 must be a TCC2/TCC2P card, and it must initialize before you install any cross-connect or traffic cards.
Tools/Equipment	Two TCC2/TCC2P cards
Prerequisite Procedures	None
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None



Note When installing cards, allow each card to boot completely before installing the next card.

- Step 1** Open the latches/ejectors of the TCC2/TCC2P card that you will install.
- Step 2** Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 7 or 11).
- Step 3** Verify that the card is inserted correctly and close the latches/ejectors on the card.



Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

If you insert a card into a slot provisioned for a different card, all LEDs turn off.

- Step 4** Go to [Step a](#) to verify the LED activity on the TCC2 card. For the TCC2P card, go to [Step b](#).
- a. For the TCC2 card:
 - All LEDs turn on briefly. The red FAIL LED and the yellow ACT/STBY LED turn on for about 15 seconds.
 - The red FAIL LED and the green ACT/STBY LED turn on for about 40 seconds.
 - The red FAIL LED blinks for about 15 seconds.
 - The red FAIL LED turns on for about 15 seconds. All LEDs turn on for about 3 seconds before turning off for about 3 seconds.

- Both green PWR LEDs turn on for 10 seconds. The PWR LEDs then turn red for 2 to 3 minutes before going to steady green.
- While the PWR LEDs are red for two to three minutes, the ACT/STBY, MJ, and MN LEDs turn on, followed by the SNYC LED.
- The boot up process is complete when the PWR LEDs turn green and the ACT/STBY remains on. (The ACT/STBY LED will be green if this is the first TCC2 card installed, and amber if this is the second TCC2 card installed.)



Note It might take up to 4 minutes for the A and B power alarms to clear.



Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into Cisco Transport Controller (CTC) and can view the Alarms tab.



Note If you are logged into CTC, the SFTWDOWN alarm might appear as many as two times while the TCC2 card initializes. The alarm should clear after the card completely boots.



Note If the FAIL LED is on continuously, see the tip in [Step 8](#) about the TCC2 card automatic upload.

b. For the TCC2P card:

- All LEDs turn on briefly. The red FAIL LED, the yellow ACT/STBY LED, the green SYNC LED, and the green ACO LED turn on for about 15 seconds.
- The red FAIL LED and the green ACT/STBY LED turn on for about 30 seconds.
- The red FAIL LED blinks for about 3 seconds.
- The red FAIL LED turns on for about 15 seconds.
- The red FAIL LED blinks for about 10 seconds and then becomes solid.
- All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for about 5 seconds.
- Both green PWR LEDs turn on for 10 seconds. The PWR LEDs then turn red for 2 to 3 minutes before going to steady green. During this time, the ACT/STBY, MJ, and MN LEDs might turn on, followed by the SNYC LED briefly.
- The boot up process is complete when the PWR LEDs turn green and the yellow ACT/STBY remains on. (The ACT/STBY LED will be green if this is the first TCC2 card installed, and yellow if this is the second TCC2 card installed.)



Note It might take up to 3 minutes for the A and B power alarms to clear.



Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.



Note If you are logged into CTC, the SFTWDOWN alarm might appear as many as two times while the TCC2P card initializes. The alarm should clear after the card completely boots.



Note If the FAIL LED is on continuously, see the tip in [Step 8](#) about the TCC2P card automatic upload.

- Step 5** Verify that the ACT/STBY LED is green if this is the first powered-up TCC2/TCC2P card being installed, or yellow for standby if this is the second powered-up TCC2/TCC2P. The IP address, temperature of the node, and time of day appear on the LCD. The default time and date is 12:00 AM, January 1, 1970.
- Step 6** The LCD cycles through the IP address (the default is 192.1.0.2), node name, and software version. Verify that the correct software version displays on the LCD. The software text string indicates the node type (SDH or SONET) and software release. (For example: SDH 08.50-05L-20.10 indicates it is an SDH software load, Release 8.50. The numbers following the release number do not have any significance.)
- Step 7** If the LCD shows the correct software version, continue with [Step 8](#). If the LCD does not show the correct software version, upgrade the software or remove the TCC2/TCC2P card and install a replacement card.
- Refer to the release-specific software upgrade document to replace the software. To exchange the TCC2/TCC2P card, see the *Cisco ONS 15454 Troubleshooting Guide*.
- Step 8** Repeat Steps [1](#) through [7](#) for the redundant TCC2/TCC2P card.



Tip If you install a standby TCC2/TCC2P card that has a different software version than the active card, the newly installed standby TCC2/TCC2P card automatically copies the software version from the active TCC2/TCC2P card. You do not need to do anything in this situation, but the loading TCC2/TCC2P card does not boot up in the normal manner. When the standby card is first inserted, the LEDs follow most of the sequence listed in [Step 4](#). However, after the red FAIL LED turns on for about 5 seconds, the FAIL LED and the ACT/STBY LED begin to flash alternately for up to 30 minutes while the new software loads onto the active TCC2/TCC2P card. After loading the new software, the upgraded TCC2/TCC2P card's LEDs repeat the sequence from [Step 4](#), and the amber ACT/STBY LED turns on.



Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.



Note Alarm LEDs might be on; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.

- Step 9** Verify that the ACT/STBY LED is amber for standby.
- Step 10** Return to your originating procedure (NTP).
-

DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards

Purpose	This task installs the cross-connect (XCVT/XC10G/XC-VXC-10G) cards.
Tools/Equipment	XCVT/XC10G/XC-VXC-10G (cross-connect) cards
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-39
Required/As Needed	Required
Onsite/Remote	Onsite
Security Level	None



Note Do not use this procedure to upgrade cross-connect cards. If you are upgrading an XCVT card to an XC10G card, or an XC10G card to an XC-VXC-10G card, see [Chapter 12, “Upgrade Cards and Spans.”](#)



Note When installing cards, let each card boot completely before installing the next card.

- Step 1** Open the latches/ejectors of the first XCVT, XC10G, or XC-VXC-10G card that you will install.
- Step 2** Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).
- Step 3** Verify that the card is inserted correctly and close the latches/ejectors on the card.



Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

- Step 4** Verify the LED activity:
- The red FAIL LED turns on for 20 to 30 seconds.
 - The red FAIL LED blinks for 35 to 45 seconds.
 - The red FAIL LED turns on for 5 to 10 seconds.
 - All LEDs blink once and turn on.
 - The ACT/STBY LED turns on.



Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.



Note If the red FAIL LED does not turn on, check the power.



Note If the red FAIL LED is on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 1 to 4.

- Step 5** Verify that the ACT/STBY LED is green for active.
- Step 6** Use the latches/ejectors to firmly slide the second cross-connect card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).

Step 7 Verify that the card is inserted correctly and close the latches/ejectors on the card.



Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 8 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- The red FAIL LED turns on for 5 to 10 seconds.
- All LEDs blink once and turn on.
- The ACT/STBY LED turns on.



Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.



Note If the red FAIL LED does not turn on, check the power.



Note If the red FAIL LED is turned on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 6 through 8.

Step 9 Verify that the ACT/STBY LED is amber for standby.

Step 10 Return to your originating procedure (NTP).

DLP-A39 Install Ethernet Cards

Purpose	This task installs the Ethernet cards (E100T-12, E100T-G, E1000-2, E1000-2-G, G1K-4, ML100T-12, ML1000-2, ML100X-8, ML-MR-10, CE-100T-8, CE-1000-4, and CE-MR-10).
Tools/Equipment	Ethernet cards
Prerequisite Procedures	NTP-A15 Install the Common Control Cards, page 2-2
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

Step 1 Open the card latches/ejectors.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot.

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.



Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the LED activity:

- The red FAIL LED turns on for 20 to 30 seconds.
- The red FAIL LED blinks for 35 to 45 seconds.
- All LEDs blink once and turn off for 1 to 5 seconds.
- The ACT or ACT/STBY LED turns on. The SF LED can persist until all card ports connect to their far end counterparts and a signal is present.



Note If the red FAIL LED does not turn on, check the power.



Note If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 5 Return to your originating procedure (NTP).

DLP-A41 Install the Alarm Interface Controller–International Card

Purpose	This task installs the Alarm Interface Controller–International (AIC-I) card. The AIC-I card provides connections for external alarms and controls (environmental alarms).
Tools/Equipment	AIC-I card
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-39 DLP-A37 Install the XCVT, XC10G, or XC-VXC-10G Cards, page 17-42
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note When installing cards, allow each card to boot completely before installing the next card.

Step 1 Open the latches/ejectors on the card.

Step 2 Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 9).

Step 3 Verify that the card is inserted correctly and close the latches/ejectors on the card.



Note It is possible to close the latches/ejectors when the card is not completely plugged into the backplane. Ensure that you cannot insert the card any further.

Step 4 Verify the following:

- The red FAIL LED turns on for 1 second, then blinks for 1 to 5 seconds.
- The PWR A and PWR B LEDs become red and the two INPUT/OUTPUT LEDs become green for approximately 3 seconds.
- The PWR A LED turns green, the INPUT/OUTPUT LEDs turn off, and the ACT LED turns on. If the red FAIL LED does not turn on, check the power.



Note It might take up to 3 minutes for the PWR A and PWR B LEDs to update.



Note If you insert a card into a slot provisioned for a different card, no LEDs turn on.



Note If the red FAIL LED is on continuously or the LEDs act erratically, the card is not installed properly. Remove the card and repeat Steps 1 to 4.

Step 5 Return to your originating procedure (NTP).

DLP-A43 Install Fiber-Optic Cables for Path Protection Configurations

Purpose	This task connects 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-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note

To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.



Caution

Do not provision the path protection east and west ports on the same OC-N card.

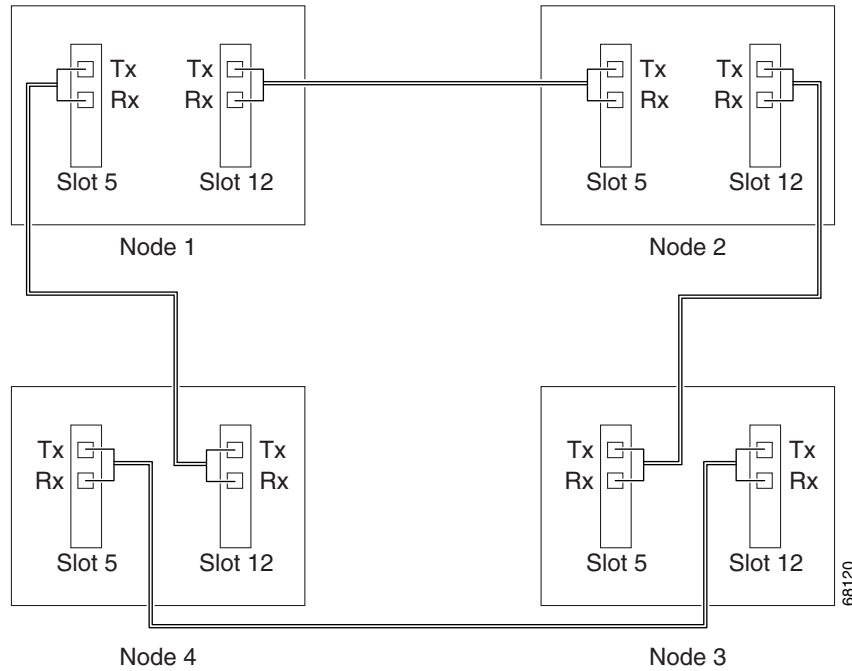
Step 1 Plan your fiber connections. Use the same plan for all path protection nodes.

Step 2 Plug the fiber into the Tx connector of an OC-N card at one node and plug the other end of the fiber into the Rx connector of an OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched (one fiber connects a receive port on one card to a receive port on another card, or the same situation with transmit ports).

Step 3 Repeat [Step 2](#) until you have configured the ring.

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

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



[Figure 17-19](#) shows a traditional path protection dual-ring interconnect (DRI) example.

Figure 17-19 Connecting Fiber to an Eight-Node Traditional Path Protection Dual-Ring Interconnect

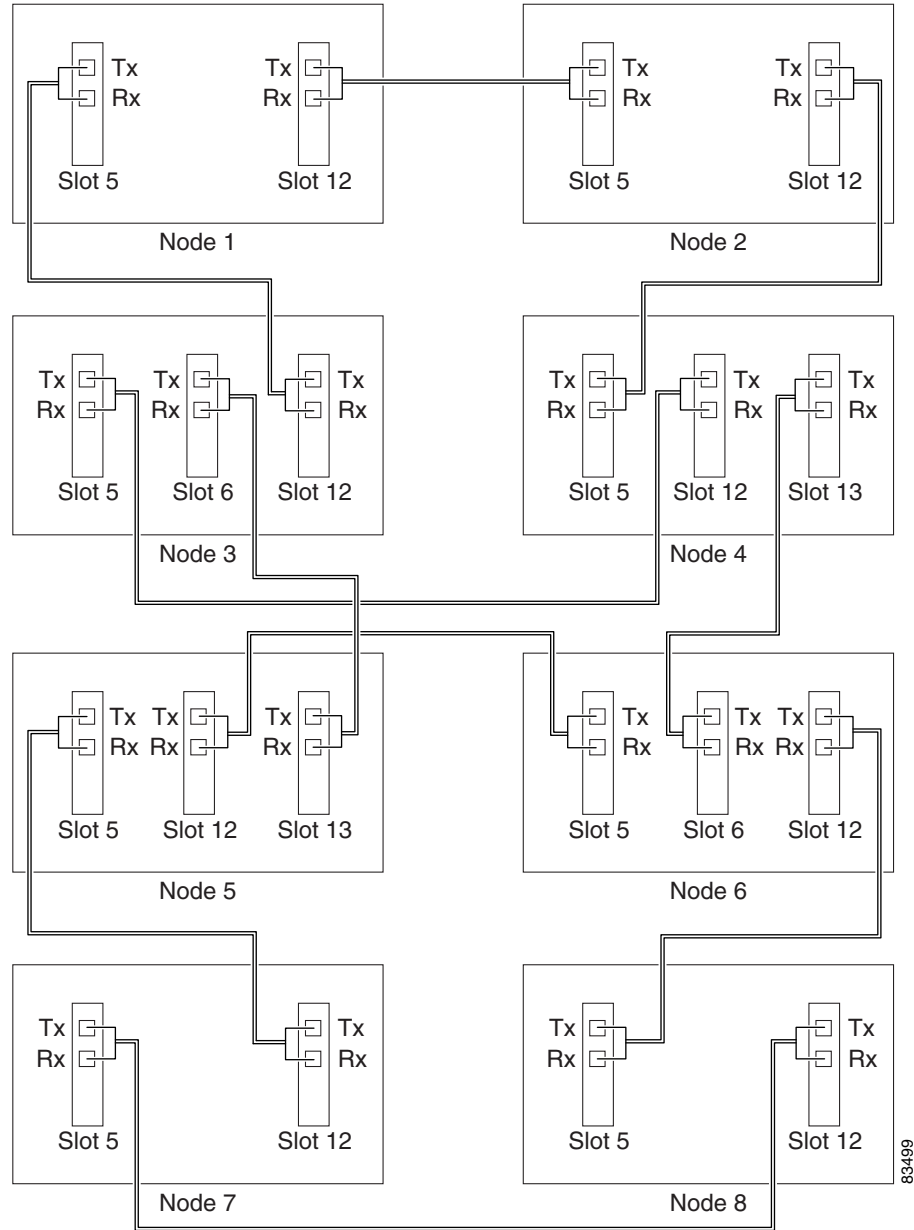
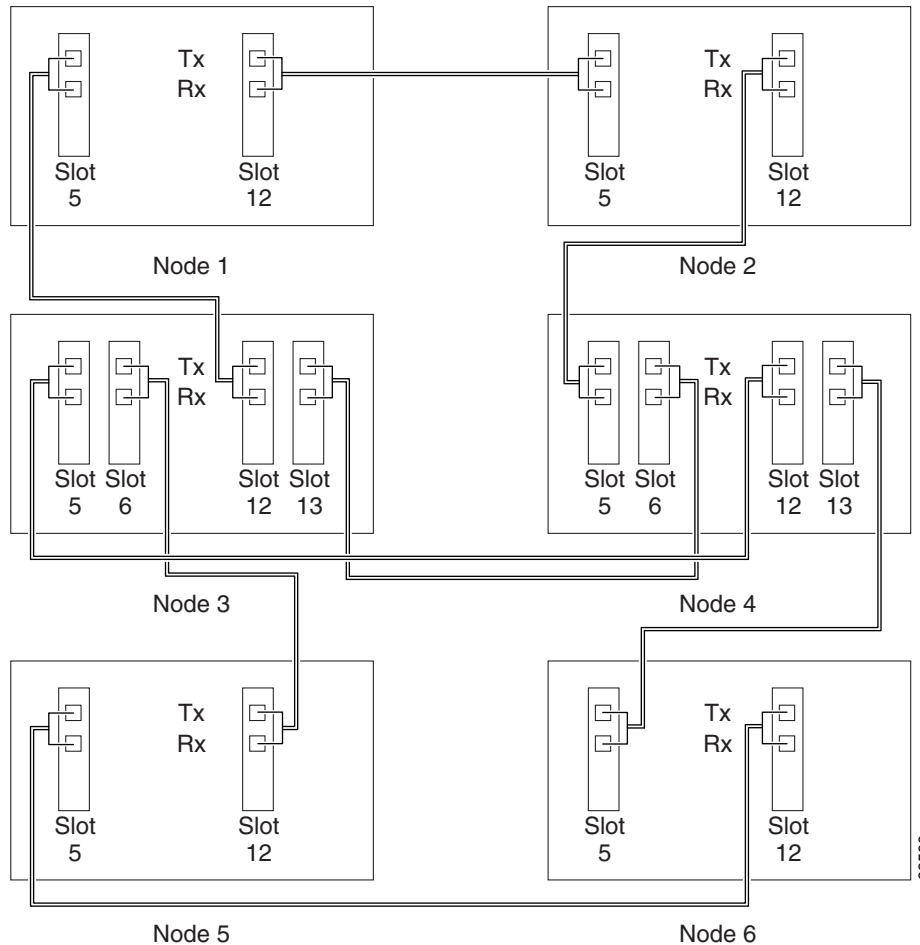


Figure 17-20 shows an integrated dual-ring interconnect (DRI) example.

Figure 17-20 Connecting Fiber to a Six-Node Integrated Path Protection Dual-Ring Interconnect

Step 4 Return to your originating procedure (NTP).

DLP-A44 Install Fiber-Optic Cables for BLSR Configurations

Purpose	This task installs the fiber-optic cables to the east and west bidirectional line switched ring (BLSR) ports at each node. See Chapter 5, “Turn Up a Network” to provision and test BLSR configurations.
Tools/Equipment	Fiber-optic cables
Prerequisite Procedures	NTP-A112 Clean Fiber Connectors, page 15-15
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

**Note**

To avoid error, connect fiber-optic cable so that the farthest slot to the right represents the east port, and the farthest slot to the left represents the west port. Fiber connected to an east port at one node must plug into the west port on an adjacent node.

**Caution**

Do not provision the BLSR east and west ports on the same OC-N card.

Step 1

Plan your fiber connections. Use the same plan for all BLSR nodes.

Step 2

Plug the fiber into the Tx connector of an OC-N card at one node and plug the other end into the Rx connector of an OC-N card at the adjacent node. The card displays an SF LED if the transmit and receive fibers are mismatched.

**Note**

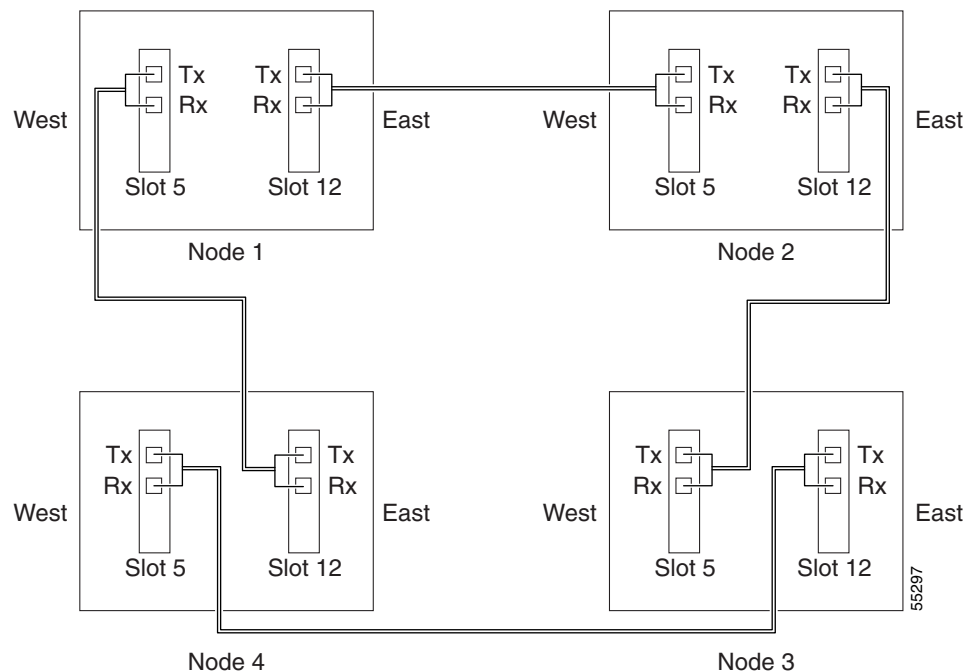
Do not mix working and protect card connections when connecting a four-fiber BLSR. The BLSR does not function if working and protect cards are interconnected. See [Figure 17-22 on page 17-50](#) for an example of correct four-fiber BLSR cabling.

Step 3

Repeat [Step 2](#) until you have configured the ring.

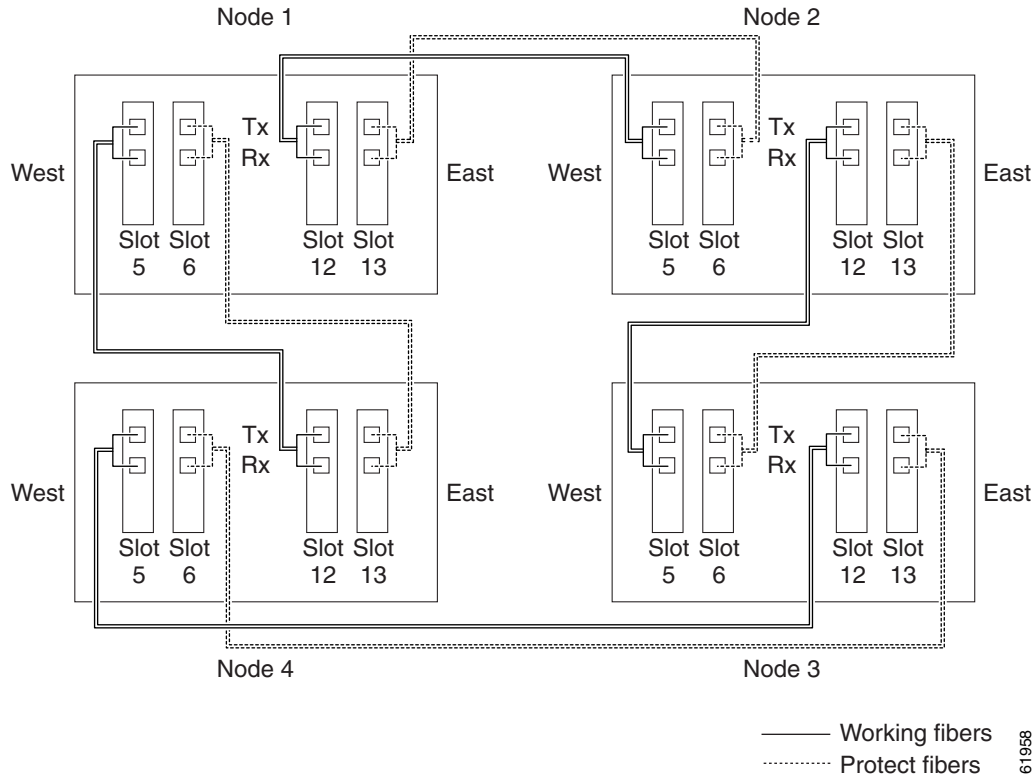
[Figure 17-21](#) shows fiber connections for a two-fiber BLSR with trunk (span) cards in Slot 5 (west) and Slot 12 (east).

Figure 17-21 Connecting Fiber to a Four-Node, Two-Fiber BLSR



[Figure 17-22](#) shows fiber connections for a four-fiber BLSR. Slot 5 (west) and Slot 12 (east) carry the working traffic. Slot 6 (west) and Slot 13 (east) carry the protect traffic.

Figure 17-22 Connecting Fiber to a Four-Node, Four-Fiber BLSR



Step 4 Return to your originating procedure (NTP).

DLP-A45 Install the Fiber Boot

Purpose	This task installs the fiber boot, which protects fiber from excessive bending. Fiber boots are required for all OC-N cards except the OC-192, OC192-XFP, and OC-48 AS cards. The boots are not necessary for these cards because of the angled SC connectors on the cards.
Tools/Equipment	Fiber boot
Prerequisite Procedures	NTP-A16 Install Optical Cards and Connectors, page 2-8
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note

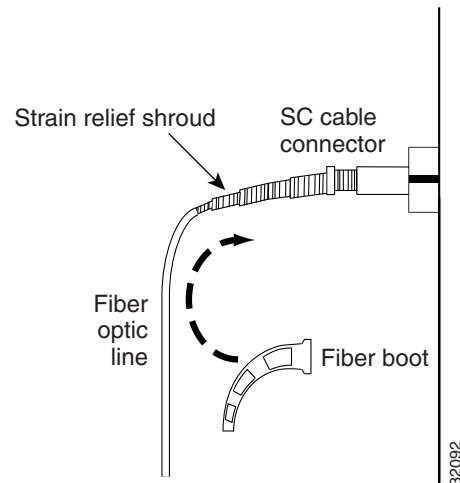
You can install the fiber boots on the fiber-optic cables before or after the cables are attached to the OC-N card.



Note On the OC3IR/STM1SH 1310-8 card, you must use a fiber clip instead of a fiber boot on the Port 8 Rx fiber connector.

- Step 1** Position the open slot of the fiber boot underneath the fiber cable.
- Step 2** Push the fiber cable down into the fiber boot. [Figure 17-23](#) shows the fiber boot attachment.

Figure 17-23 Attaching a Fiber Boot



- Step 3** Twist the fiber boot to lock the fiber cable into the tail end of the fiber boot.
- Step 4** Slide the fiber boot forward along the fiber-optic cable until the fiber boot fits snugly onto the end of the SC cable connector.
- Step 5** Return to your originating procedure (NTP).

DLP-A50 Set Up a Windows PC for Craft Connection to an ONS 15454 on the Same Subnet Using Static IP Addresses

Purpose	This task sets up your computer for a local craft connection to the ONS 15454 when: <ul style="list-style-type: none"> You will access nodes running software releases earlier than Software Release 3.3. You will connect to one ONS 15454; if you will connect to multiple ONS 15454s, you might need to reconfigure your computer's IP settings each time you connect to an ONS 15454. You need to use non-ONS 15454 applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

-
- Step 1** Verify the operating system that is installed on your computer:
- From the Windows Start menu, choose **Settings > Control Panel**.
 - In the Control Panel window, double-click the **System** icon.
 - On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows 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:
- From the Windows Start menu, choose **Settings > Control Panel**.
 - In the Control Panel dialog box, click the **Network** icon.
 - In the Network dialog box, choose **TCP/IP** for your NIC card, then click **Properties**.
 - In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.
 - Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.
 - Click the **IP Address** tab.
 - In the IP Address window, click **Specify an IP address**.
 - In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

- i. In the Subnet Mask field, type the same subnet mask as the ONS 15454. 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 15454 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 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.
- 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 15454 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 ONS 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.
- f. In the Subnet Mask field, type **255.255.255.0**.
- g. In the Default Gateway field, type the ONS 15454 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 15454 IP address except for the last octet. The last octet must be 1 or 3 through 254. This IP address appears on the LCD unless its display is suppressed during node provisioning.

e. In the Subnet Mask field, type **255.255.255.0**.

f. In the Default Gateway field, type the ONS 15454 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-A51 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Dynamic Host Configuration Protocol

Purpose	This task sets up your computer for craft connection to the ONS 15454 using Dynamic Host Configuration Protocol (DHCP).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1 NTP-A169 Set Up CTC Network Access, page 4-7
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None



Note

Do not use this task for initial node turn-up. Use the task only if DHCP forwarding is enabled on the ONS 15454. By default, DHCP is not enabled. To enable it, see the [“NTP-A169 Set Up CTC Network Access” procedure on page 4-7](#).



Note

The ONS 15454 does not provide the IP addresses. If DHCP forwarding is enabled, it passes DHCP requests to an external DHCP server.

-
- Step 1** Verify the operating system that is installed on your computer:
- From the Windows Start menu, choose **Settings > Control Panel**.
 - In the Control Panel window, double-click the **System** icon.
 - On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 98, Windows 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:
- From the Windows Start menu, choose **Settings > Control Panel**.
 - In the Control Panel dialog box, click the **Network** icon.
 - In the Network dialog box, select **TCP/IP** for your NIC, then click **Properties**.
 - In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.
 - Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.
 - Click the **IP Address** tab.
 - In the IP Address window, click **Obtain an IP address automatically**.
 - Click **OK**.
 - 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:
- From the Windows Start menu, choose **Settings > Control Panel**.
 - In the Control Panel dialog box, click the **Network** icon.
 - In the Network dialog box, click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.
 - Click the **IP Address** tab.
 - In the IP Address window, click **Obtain an IP address from a DHCP server**.
 - Click **OK**.
 - Click **Apply**.
 - 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:
- From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.
 - In the Local Area Connection Status dialog box, click **Properties**.
 - On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
 - 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-A52 Set Up a Windows PC for Craft Connection to an ONS 15454 Using Automatic Host Detection

Purpose	This task sets up your computer for local craft connection to the ONS 15454 when: <ul style="list-style-type: none"> • You will connect to the ONS 15454 Ethernet port or backplane LAN pins either directly or through a hub. • All nodes that you will access are running Software Release 3.3 or later. • You will connect to multiple ONS 15454s and do not want to reconfigure your IP address each time. • You do not need to access non-ONS 15454 applications such as ping and tracert (trace route).
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
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 Windows 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.
 - i. In the Subnet Mask field, type the same subnet mask as the ONS 15454. 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 [h](#). 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.
 - g. In the Subnet Mask field, type the same subnet mask as the ONS 15454. 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 node IP address.
- f. In the Subnet Mask field, type the same subnet mask as the ONS 15454. 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 to select it. Right-click and select **Properties**.
- c. From the Local Area Connection Properties dialog box, click on **Internet Protocol (TCP/IP)** to select it, then click **Properties**.
- d. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD of the ONS 15454. The default IP address is 192.1.0.2.
- e. In the Subnet Mask field, type the same subnet mask as the ONS 15454. 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-A54 Hard-Reset a CE-100T-8 Card Using CTC

Purpose	This task hard-resets the CE-100T-8 Ethernet card without requiring physical removal.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser only



Caution

A hard reset causes a traffic hit.



Note

The hard-reset option is enabled only when the card is in the OOS-MA, MT service state.

- Step 1** In node view click the **Inventory** tab. Locate the appropriate card in the inventory pane.
- Step 2** Click the **Admin State** drop-down menu and select **OOS-MT,MA**. Click **Apply**.
- Step 3** Click **Yes** in the “Action may be service affecting. Are you sure?” dialog box.
- Step 4** The service state of the card becomes Locked enabled, loopback & maintenance. The card’s faceplate appears blue in CTC and the SRV LED turns amber.
- Step 5** Right-click the card to reveal a pop-up menu.
- Step 6** Click **Hard-reset Card**.
- Step 7** Click **Yes** in the “Are you sure you want to hard-reset this card?” dialog box.
- Step 8** Return to your originating procedure (NTP).
-

DLP-A56 Disable Proxy Service Using Internet Explorer (Windows)

Purpose	This task disables proxy service for PCs running Internet Explorer.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	Required if your computer is connected to a network computer proxy server and your browser is Internet Explorer.
Onsite/Remote	Onsite or remote
Security Level	None

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



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

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

Step 3 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.
- Leave **Use a proxy server** selected and click **Advanced**. In the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15454 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 15454s on your network. Click **OK** to close each open dialog box.



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

Step 5 Return to your originating procedure (NTP).

DLP-A57 Disable Proxy Service Using Netscape (Windows and UNIX)

Purpose	This task disables proxy service for PCs and UNIX workstations running Netscape. You must perform this task if your computer is connected to a network computer proxy server and your browser is Netscape.
Tools/Equipment	None
Prerequisite Procedures	NTP-A260 Set Up Computer for CTC, page 3-1
Required/As Needed	As needed
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 15454 nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.



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

Step 5 Return to your originating procedure (NTP).

DLP-A60 Log into CTC

Purpose	This task logs a user into Cisco Transport Controller (CTC).
Tools/Equipment	None
Prerequisite Procedures	<p>NTP-A260 Set Up Computer for CTC, page 3-1</p> <p>One of the following procedures:</p> <ul style="list-style-type: none"> • NTP-A234 Set Up CTC Computer for Local Craft Connection to the ONS 15454, page 3-3 • NTP-A235 Set Up a CTC Computer for a Corporate LAN Connection to the ONS 15454, page 3-5 • NTP-A236 Set Up a Remote Access Connection to the ONS 15454, page 3-6
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Retrieve or higher



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

Step 1 From the computer connected to the ONS 15454, 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` or the `-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 15454 IP address. For initial setup, the default IP address is 192.1.0.2. (This IP address can appear on the LCD. You can suppress the LCD IP address display using CTC. For more information, see the [“DLP-A266 Change IP Settings” task on page 19-49.](#)) Press **Enter**.

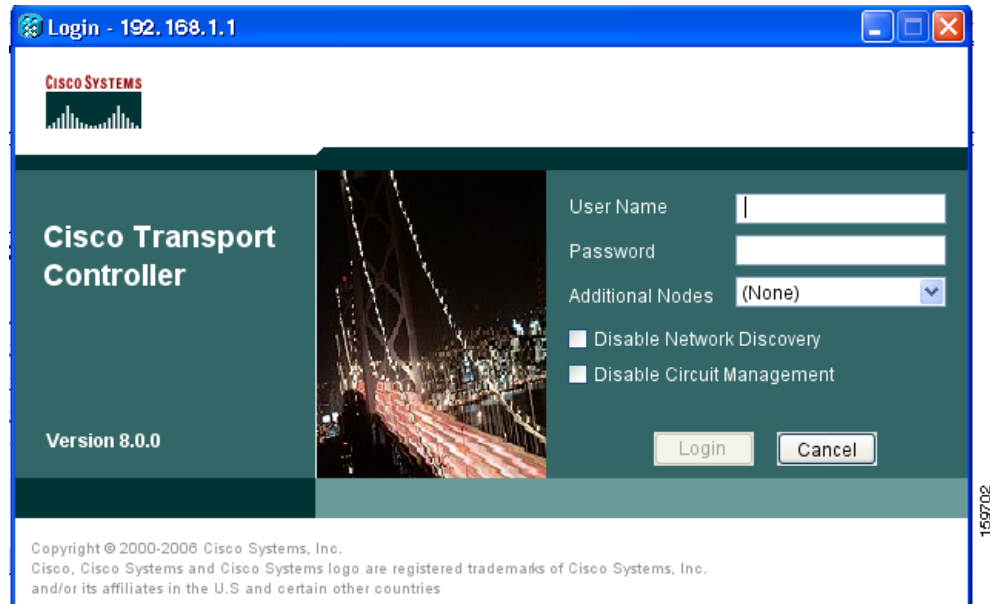
**Note**

If you are logging into ONS 15454 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 15454 software version for each node visible on the network view. If the node is not visible, the software version can be read from the LCD display. To resolve an alarm, refer to the *Cisco ONS 15454 Troubleshooting Guide*.

If a Java Plug-in Security Warning dialog box appears, complete the [“DLP-A418 Install Public-Key Security Certificate” task on page 21-5](#) 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 15454, this process can take several minutes. After the download, the CTC Login dialog box appears ([Figure 17-24](#)).

Figure 17-24 Logging into CTC



- 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 15454. 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 15454 users and assign security, go to the [“NTP-A30 Create Users and Assign Security” procedure on page 4-4](#). Additional information about security is provided in the “Security” chapter in the *Cisco ONS 15454 Reference Manual*.

- Step 4** Each time you log into an ONS 15454, you can make selections on the following login options:
- **Node Name**—Displays the IP address entered in the web browser and a drop-down list of previously entered ONS 15454 IP addresses. You can select any ONS 15454 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 add additional groups, see the [“DLP-A61 Create Login Node Groups” task on page 17-64](#).
 - **Disable Network Discovery**—Check this box to view only the ONS 15454 (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 startup time in networks with many DCC-connected nodes, and reduce memory consumption.
 - **Disable Circuit Management**—Check this box to disable discovery of existing circuits. Using this option can decrease the CTC initialization time in networks with many existing circuits and reduce memory consumption. This option does not prevent the creation and management of new circuits.
- Step 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 15454. 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 15454 Troubleshooting Guide*.

Step 7 Return to your originating procedure (NTP).

DLP-A61 Create Login Node Groups

Purpose	This task creates a login node group to display ONS 15454s that have an IP connection but not a DCC connection to the login node.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 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**.

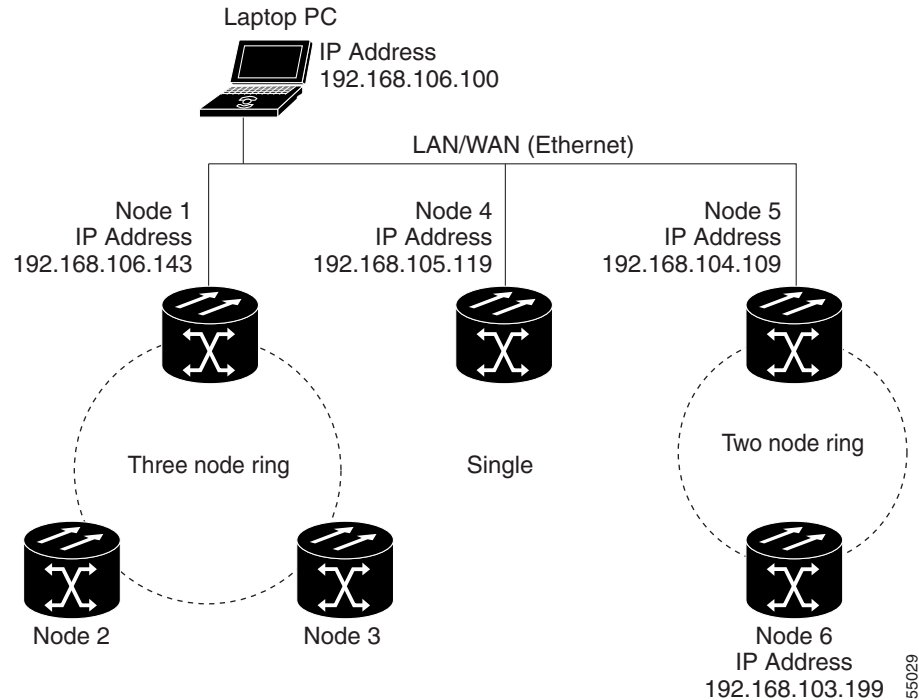
Step 4 In the Members area, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node that you want to add to the group.



Note If the ONS 15454 that you want to add to the login node group has TCC2P cards installed and the TCC2P secure mode option is enabled, enter the backplane LAN port IP address. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the “Management Network Connectivity” chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

Step 5 Click **OK**.

The next time you log into an ONS 15454, the login node group will be available in the Additional Nodes list of the Login dialog box. For example, in [Figure 17-25](#), 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, 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 17-25 Login Node Group

Step 6 Return to your originating procedure (NTP).

DLP-A62 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-A60 Log into CTC, page 17-61
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).

If the ONS 15454 that you want to add has TCC2P cards installed and the TCC2P secure mode option is enabled, enter the backplane LAN port IP address.



Note If the node is in secure mode, the backplane IP address display might be disabled. A Superuser can reenables the IP address display. If the node is in secure mode and the configuration has been locked, you will not be able to change the IP address unless the lock is disabled by Cisco Technical Support. See the “Management Network Connectivity” chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

- Step 3** If you want to add the node to the current login group, check **Add to current login node group**. Otherwise, leave it unchecked. 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-A64 Set the IP Address, Default Router, and Network Mask Using the LCD

Purpose	This task changes the ONS 15454 IP address, default router, and network mask using the LCD on the fan-tray assembly. Use this task if you cannot log into CTC.
Tools/Equipment	None
Prerequisite Procedures	DLP-A36 Install the TCC2/TCC2P Cards, page 17-39
Required/As Needed	As needed
Onsite/Remote	Onsite
Security Level	None

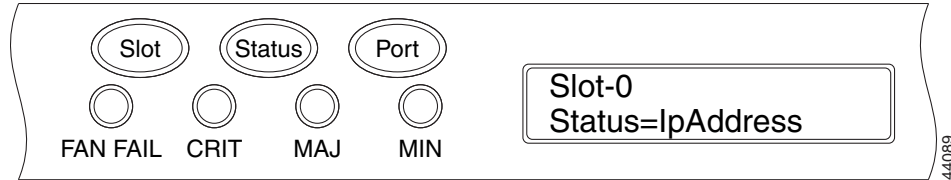


Note You cannot perform this task if the LCD IP Display on the node view Provisioning > Network tab is set to Display Only or Suppress Display. See “[DLP-A249 Provision IP Settings](#)” task on [page 19-30](#) to view or change the LCD IP Display field. If the node is locked in secure mode with the LCD display disabled, you will not be able to change this provisioning unless the lock is disabled by Cisco Technical Support. Refer to the “Management Network Connectivity” chapter in the *Cisco ONS 15454 Reference Manual* for more information about secure mode.

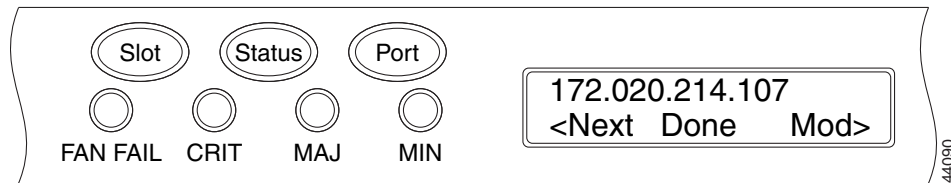


Note The LCD reverts to normal display mode after 5 seconds of button inactivity.

- Step 1** On the ONS 15454 front panel, repeatedly press the **Slot** button until Node appears on the LCD.
- Step 2** Repeatedly press the **Port** button until the following displays:
- To change the node IP address, Status=IpAddress ([Figure 17-26](#))
 - To change the node network mask, Status=Net Mask
 - To change the default router IP address, Status=Default Rtr

Figure 17-26 *Selecting the IP Address Option*

- Step 3** Press the **Status** button to display the node IP address (Figure 17-27), the node subnet mask length, and the default router IP address.

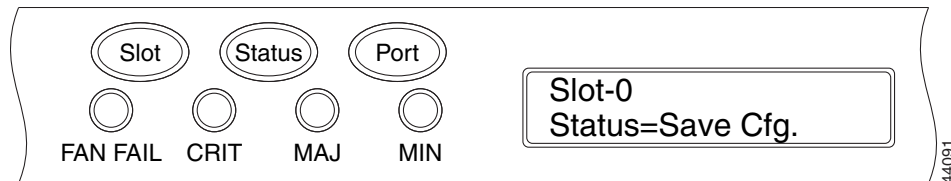
Figure 17-27 *Changing the IP Address*

- Step 4** Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.



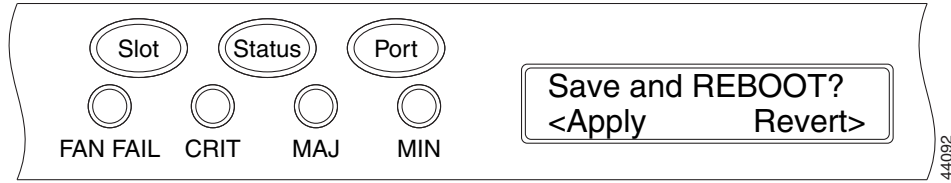
Tip The Slot, Status, and Port button positions correspond to the command position on the LCD. For example, in Figure 17-27, you press the Slot button to invoke the Next command and the Port button to invoke the Done command.

- Step 5** Press the **Port** button to cycle the IP address or subnet mask to the correct digit.
- Step 6** When the change is complete, press the **Status** button to return to the Node menu.
- Step 7** Repeatedly press the **Port** button until the Save Configuration option appears (Figure 17-28).

Figure 17-28 *Selecting the Save Configuration Option*

- Step 8** Press the **Status** button to choose the Save Configuration option. A Save and REBOOT message appears (Figure 17-29).

Figure 17-29 Saving and Rebooting the TCC2/TCC2P



- Step 9** Press the **Slot** button to apply the new IP address configuration or press **Port** to cancel the configuration. Saving the new configuration causes the TCC2/TCC2P cards to reboot. During the reboot, a “Saving Changes - TCC Reset” message displays on the LCD. The LCD returns to the normal alternating display after the TCC2/TCC2P reboot is complete.



Note The IP address and default router must be on the same subnet. If not, you cannot apply the configuration.

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

DLP-A65 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-A60 Log into CTC, page 17-61
Required/As Needed	Required if either of the following conditions is true: <ul style="list-style-type: none"> CTC computers on one subnet need to connect to ONS 15454s that are connected by a router to ONS 15454s residing on another subnet. OSPF is not enabled and the ENE gateway setting is not checked. You need to enable multiple CTC sessions among ONS 15454s residing on the same subnet and the ENE gateway setting is not enabled.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In node view, click the **Provisioning > Network** tabs.
- Step 2** Click the **Static Routing** tab. 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 15454 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 of the *Cisco ONS 15454 Reference Manual*.

Step 5 Return to your originating procedure (NTP).

DLP-A67 Provision the IIOP Listener Port on the ONS 15454

Purpose	This task sets the Internet Inter-ORB Protocol (IIOP) listener port on the ONS 15454, which enables you to access ONS 15454s that reside behind a firewall.
Tools/Equipment	IIOP listener port number provided by your LAN or firewall administrator
Prerequisite Procedures	DLP-A60 Log into CTC , page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Note If the Enable SOCKS Proxy Server on port 1080 check box is checked, CTC will use port 1080 and ignore the configured IIOP port setting. If Enable SOCKS 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 TCC CORBA (IIOP) Listener Port area, choose a listener port option:

- **Default - TCC Fixed**—Select this option if the ONS 15454s are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the ONS 15454 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 ONS 15454 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**.

Both ONS 15454 TCC2/TCC2P cards reboot, one at a time. The reboot takes approximately 15 minutes.

Step 5 Return to your originating procedure (NTP).

DLP-A68 Provision the IIOP Listener Port on the CTC Computer

Purpose	This task selects the IIOP listener port on CTC. You must perform this task if the computer running CTC resides behind a firewall.
Tools/Equipment	IIOP listener port number from LAN or firewall administrator.
Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-61
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 CTC CORBA (IIOP) Listener Port area, choose a listener port option:
- **Default - Variable**—Select this option if the ONS 15454s are on the same side of the firewall as the CTC computer or if no firewall is used (default). This option sets the CTC 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 defined by your administrator.
- Step 4** Click **Apply**. A warning appears telling you that the port change will apply during the next CTC login.
- Step 5** Click **OK**.
- Step 6** In the Preferences dialog box, click **OK**.
- Step 7** To access the ONS 15454 using the IIOP port, log out of CTC then log back in. (To log out, choose **Exit** from the File menu).
- Step 8** Return to your originating procedure (NTP).
-

DLP-A69 Set Up SONET External or Line Timing

Purpose	This task defines the SONET timing source (external or line) for the ONS 15454.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

Step 2 In the Timing Standard area, make sure that the Current Timing Standard is SONET. If it is not, continue with [Step 3](#). If the Current Timing Standard is SONET, skip to [Step 4](#).

Step 3 Click **Change** to switch the timing from SDH to SONET.



Note Changing the timing standard reinitializes the node and might affect traffic.

Step 4 In the General Timing area, complete the following information:

- **Timing Mode**—Choose **External** if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; choose **Line** if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set both external and line timing references.



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

- **SSM Message Set**—Choose a synchronization status messaging (SSM) message set. All ONS 15454s can translate Generation 2 message sets, so choose Generation 2 if the ONS 15454 is connected to other ONS 15454s. Choose Generation 1 only when the ONS 15454 is connected to equipment that does not support Generation 2. If a node that has its SSM message 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 (Stratum 3E) will become an ST3 (Stratum 3) clock.
- **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 of the *Cisco ONS 15454 Reference Manual* for more information about SSM, including definitions of the SONET timing levels.
- **Revertive**—Select this check box if you want the ONS 15454 to revert to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- **Revertive Time**—If Revertive is checked, choose the amount of time the ONS 15454 will wait before reverting to its primary timing source. Five minutes is the default.

Step 5 In the Reference Lists area, complete the following information:

**Note**

You can define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out pins on the backplane. If you attach equipment to BITS Out pins, you normally attach it to a node with Line mode because equipment near the external timing reference can be directly wired to the reference.

- NE Reference—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 TCC/TCC2P. The options displayed depend on the Timing Mode setting.
- If the Timing Mode is set to External, your options are BITS1, BITS2, and Internal Clock.
- If the Timing Mode is set to Line, your options are the node's working OC-N cards and Internal Clock. Choose the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk (span) cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, choose Slot 5 as Reference 1.
- If the Timing Mode is set to Mixed, both BITS and OC-N cards are available, allowing you to set a mixture of external BITS and OC-N trunk (span) cards as timing references.
- BITS-1 Out/BITS-2 Out—Define the timing references for equipment wired to the BITS Out pins on the backplane. BITS-1 Out and BITS-2 Out are enabled when BITS-1 and BITS-2 facilities are put in service. If Timing Mode is set to External, choose the OC-N card used to set the timing. If Timing Mode is set to Line, you can choose an OC-N card or choose NE Reference to have the BITS-1 Out and/or BITS-2 Out follow the same timing references as the NE.

Step 6 Click the **BITS Facilities** subtab.

The BITS Facilities section sets the parameters for your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer. If equipment is timed through BITS Out, you can set timing parameters to meet the requirements of the equipment.

Step 7 In the BITS In area, complete the following information:

- Facility Type—(TCC2P card only) Choose the BITS signal type supported by your BITS clock, either DS1 or 64Khz+8Khz.
- BITS In State—If Timing Mode is set to External or Mixed, set the BITS In State for BITS-1 and/or BITS-2 to **IS** (in service) depending whether one or both BITS input pin pairs on the MIC are connected to the external timing source. If Timing Mode is set to Line, set the BITS In State to **OOS** (out of service).

Step 8 If BITS In State is set to OOS, continue with [Step 9](#). If the BITS In 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.
- Admin SSM—If the Sync Messaging check box is not checked, you can choose the SSM Generation 2 type from the drop-down list.

- Step 9** In the BITS Out area, complete the following information, as needed:
- Facility Type—Choose the BITS Out signal type, either DS1 or 64 Khz.
 - BITS Out State—If equipment is connected to the node's BITS output pins on the backplane and you want to time the equipment from a node reference, set the BITS Out State for BITS-1 and/or BITS-2 to **IS**, depending on which BITS Out pins are used for the external equipment. If equipment is not attached to the BITS output pins, set the BITS Out State to **OOS**.
- Step 10** If the BITS Out State is set to OOS, continue with [Step 11](#). If BITS Out State is set to IS, complete the following information:
- Coding—Choose the coding used by your BITS reference, either B8ZS or AMI.
 - Framing—Choose the framing used by your BITS reference, either ESF or SF (D4).
 - 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 and BITS 2 Out backplane 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 15454. 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 11** Click **Apply**.



Note Refer to the *Cisco ONS 15454 Troubleshooting Guide* for timing-related alarms.

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



Note When provisioning a line timing reference for the node, you cannot select the protect port of a 1+1 protection group. If a traffic switch occurs on the working port of the 1+1 protection group, the timing reference of the node automatically switches to the protect port of the 1+1 protection group.

DLP-A70 Set Up Internal Timing

Purpose	This task sets up internal timing (Stratum 3) for an ONS 15454. Use only if a BITS source is not available.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454 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—Does not apply to internal timing.
 - Revertive—Does not apply to internal timing.
 - Revertive Time—Does not apply to internal timing.
- 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/BITS-2 Out—Set to **None**.
- Step 4** Click the **Provisioning > Timing > BITS Facilities** tabs.
- Step 5** In the BITS Facilities area, change the BITS In State and BITS Out State to **OOS**. Disregard the other BITS Facilities settings; they are not relevant to internal timing.
- Step 6** Click **Apply**.
- Step 7** Return to your originating procedure (NTP).
-

DLP-A71 Create a 1:1 Protection Group

Purpose	This task creates a 1:1 electrical card protection group.
Tools/Equipment	Redundant DS-1, DS-3, EC-1, or DS3XM cards should be installed in the shelf, or the ONS 15454 slots must be provisioned for two of these cards.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** Verify that the cards required for 1:1 protection are installed according to requirements specified in [Table 4-1 on page 4-13](#).
- Step 2** In node view, click the **Provisioning > Protection** tabs.
- Step 3** Click **Create**.
- Step 4** In the Create Protection Group dialog box, enter the following:
- Name—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (") characters.
 - Type—Choose **1:1** from the drop-down list.

- **Protect Card**—Choose the protect card from the drop-down list. The list displays cards available for 1:1 protection. If no cards are available, no cards appear in the list.

After you choose the protect card, the card available for protection appear in the Available Cards list, as shown in [Figure 17-30](#). If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the “[DLP-A330 Preprovision a Card Slot](#)” task on [page 20-20](#).

Figure 17-30 Creating a 1:1 Protection Group

- Step 5** From the Available Cards list, choose the card that will be protected by the card selected in the Protect Card drop-down list. Click the top arrow button to move each card to the Working Cards list.
- Step 6** Complete the remaining fields:
- **Bidirectional switching**—Not available for 1:1 protection.
 - **Revertive**—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.



Note When you perform a protection switch, do not change the protection group mode from nonrevertive to revertive or from revertive to nonrevertive.

- **Reversion time**—If Revertive is checked, choose the 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 card after conditions causing the switch are cleared. The reversion timer starts after conditions causing the switch are cleared.
- Step 7** Click **OK**, then click **Yes** in the confirmation dialog box.
- Step 8** Return to your originating procedure (NTP).

DLP-A72 Create a 1:N Protection Group

Purpose	This task creates a DS-1, DS-3, or SVC-RAN 1:N protection group.
Tools/Equipment	DS1N-14, DS3N-12, DS3N-12E, DS3/EC1-48, or DS1/E1-56 (protect cards); DS1-14, DS3-12, or DS3-12E (working cards).
Note	The DS1N-14, DS3N-12, DS3N-12E, DS3/EC1-48, or DS1/E1-56 protect cards must be installed in Slot 3 or Slot 15, and the cards they protect (DS1-14, DS3-12, DS3-12E) must be on the same side of the shelf.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to the 1:N requirements specified in [Table 4-1 on page 4-13](#).

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

Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- **Name**—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (") characters.
- **Type**—Choose **1:N** from the drop-down list.
- **Protect Card**—Choose the protect card from the drop-down list. The list displays DS1N-14, DS3N-12, DS3/EC1-48, DS3N-12E, or DS1/E1-56 cards (installed in Slots 3 or 15). If these cards are not installed, no cards appear in the drop-down list.

After you choose the protect card, a list of cards available for protection appear in the Available Cards list. If no cards are available, no cards appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the [“DLP-A330 Preprovision a Card Slot” task on page 20-20](#).

Step 5 From the Available Cards list, choose the cards that will be protected by the card selected in the Protect Card drop-down list. Click the top arrow button to move each card to the Working Cards list.

Step 6 Complete the remaining fields:

- **Bidirectional switching**—Not available for 1:N protection.
- **Revertive**—Always enabled for 1:N protection groups.



Note When you perform a protection switch, do not change the protection group mode from nonrevertive to revertive or from revertive to nonrevertive.

- **Reversion time**—Click **Reversion time** and select 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 card after conditions causing the switch are cleared. The reversion timer starts after conditions causing the switch are cleared.

Step 7 Click **OK**, then click **Yes** in the confirmation dialog box.

Step 8 Return to your originating procedure (NTP).

DLP-A73 Create a 1+1 Protection Group

Purpose	This task creates a 1+1 protection group for any OC-N card/port (OC-3, OC3-8, OC-12, OC12-4, OC-48, OC-48 AS, OC-192, MRC-12, MRC-2.5G-4, OC192SR1/STM64IO Short Reach, and OC192/STM64 Any Reach cards).
Tools/Equipment	Installed OC-N cards or preprovisioned slots
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Step 1 Verify that the cards are installed according to 1+1 requirements specified in [Table 4-1 on page 4-13](#).

Step 2 In node view, click the **Provisioning > Protection** tabs.

Step 3 In the Protection Groups area, click **Create**.

Step 4 In the Create Protection Group dialog box, enter the following:

- **Name**—Type a name for the protection group. The name can have up to 32 alphanumeric (a-z, A-Z, 0-9) characters. Special characters are permitted. For TL1 compatibility, do not use question marks (?), backslash (\), or double quote (") characters.
- **Type**—Choose **1+1** from the drop-down list.
- **Protect Port**—Choose the protect port from the drop-down list. The list displays the available OC-N ports, as shown in [Figure 17-31 on page 17-78](#). If OC-N cards are not installed, no ports appear in the drop-down list.

After you choose the protect port, a list of ports available for protection appear in the Available Ports list, as shown in [Figure 17-31](#). If no cards are available, no ports appear. If this occurs, you can not complete this task until you install the physical cards or preprovision the ONS 15454 slots using the [“DLP-A330 Preprovision a Card Slot” task on page 20-20](#).

Figure 17-31 Creating a 1+1 Protection Group

Step 5 From the Available Ports list, choose the port that will be protected by the port you selected in the Protect Port field. Click the top arrow button to move each port to the Working Ports list.

Step 6 Complete the remaining fields:

- Bidirectional switching—Check this check box if you want both Tx and Rx signals to switch to the protect port when a failure occurs to one signal. Leave unchecked if you want only the failed signal to switch to the protect port.
- Revertive—Check this check box if you want traffic to revert to the working card after failure conditions remain corrected for the amount of time entered in the Reversion Time field.



Note When you perform a protection switch, do not change the protection group mode from nonrevertive to revertive or from revertive to nonrevertive.

- Reversion time—If Revertive is checked, choose a reversion time from the drop-down list. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. Reversion time is the amount of time that will elapse before the traffic reverts to the working card after conditions causing the switch are cleared. The reversion timer starts after conditions causing the switch are cleared.

Step 7 Click **OK**.

Step 8 Return to your originating procedure (NTP).



Note When provisioning a line timing reference for the node, you cannot select the protect port of a 1+1 protection group. If a traffic switch occurs on the working port of the 1+1 protection group, the timing reference of the node automatically switches to the protect port of the 1+1 protection group.

DLP-A74 Create a New User on a Single Node

Purpose	This task creates a new user for one ONS 15454 node.
Tools/Equipment	None

Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
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 Users window, click **Create**.

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

- **Name**—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be 6 to 10 characters.
- **Password**—Type the user password. The password length, by default, is set to a minimum of six and a maximum of 20. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #, %) characters, where at least two characters are nonalphabetic and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
- **Confirm Password**—Type the password again to confirm it.
- **Security Level**—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the “Security” chapter in the *Cisco ONS 15454 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 the password must be reentered. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the “[NTP-A205 Modify Users and Change Security](#)” procedure on page 11-7.

Step 4 Click **OK**.

Step 5 Return to your originating procedure (NTP).

DLP-A75 Create a New User on Multiple Nodes

Purpose	This task adds a new user to multiple ONS 15454 nodes.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
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 Users window, click **Create**.
- Step 4** In the Create User dialog box, enter the following:
- **Name**—Type the user name. The name must be a minimum of six and a maximum of 20 alphanumeric (a-z, A-Z, 0-9) characters. For TL1 compatibility, the user name must be 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. You can configure the default values in node view through Provisioning > NE Defaults > Node > security > passwordComplexity. The minimum length can be set to eight, ten or twelve characters, and the maximum length to 80 characters. The password must be a combination of alphanumeric (a-z, A-Z, 0-9) and special (+, #, %) characters, where at least two characters are nonalphanumeric and at least one character is a special character. For TL1 compatibility, the password must be 6 to 10 characters. The password must not contain the user name.
 - **Confirm Password**—Type the password again to confirm it.
 - **Security Level**—Choose a security level for the user: RETRIEVE, MAINTENANCE, PROVISIONING, or SUPERUSER. Refer to the “Security” chapter in the *Cisco ONS 15454 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. The defaults are: Retrieve user = unlimited, Maintenance user = 60 minutes, Provisioning user = 30 minutes, and Superuser = 15 minutes. To change the idle times, refer to the “[NTP-A205 Modify Users and Change Security](#)” procedure on page 11-7.

- 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, verify that the user was added to all the nodes chosen in [Step 5](#). If not, click **OK** and repeat Steps 2 through 6. If the user was added to all nodes, click **OK** and continue with the next step.
- Step 8** Return to your originating procedure (NTP).
-

DLP-A83 Provision Orderwire

Purpose	This task provisions orderwire on the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9. OC-N cards must be installed.

Prerequisite Procedures	NTP-A323 Verify Card Installation, page 4-2 DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

-
- Step 1** In the 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).
 - **Circuit Type**—Choose either **Local Orderwire** or **Express Orderwire** depending on the orderwire path that you want to create. If regenerators are not used between ONS 15454 nodes, you can use either local or express orderwire channels. If regenerators exist, use the express orderwire channel. You can provision up to four ONS 15454 OC-N ports for each orderwire path.
 - **PCM**—Choose the Pulse Code Modulation voice coding and companding standard, either **Mu_Law** (North America, Japan) or **A_Law** (Europe). The provisioning procedures are the same for both types of orderwire.

**Caution**

When provisioning orderwire for ONS 15454 nodes residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops, provision two orderwire ports (east and west) at all but one of the ring nodes.

-
- 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-A88 Optical 1+1 Protection Test

Purpose	This task verifies that a 1+1 protection group will switch traffic properly. You must perform this procedure if you have created a 1+1 protection group.
Tools/Equipment	The test set specified by the acceptance test procedure.
Prerequisite Procedures	DLP-A60 Log into CTC , page 17-61; a test circuit created as part of the topology acceptance test.
Required/As Needed	As needed
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.
- Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on [page 19-18](#) as necessary.
 - Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 3** Click the **Conditions** tab. Verify that no unexplained conditions appear on the network. If unexplained conditions appear, resolve them before continuing. Refer to the *Cisco ONS 15454 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 it in node view.
- Step 5** Click the **Maintenance > Protection** tabs.
- Step 6** Initiate a Force switch on the working port:
- In the Protection Groups area, click the 1+1 protection group.
 - Click the working port. Next to Switch Commands, click **Force**.
 - In the Confirm Force Operation dialog box, click **Yes**.
 - 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:
- Next to Switch Commands, click **Clear**.
 - In the Confirm Clear Operation dialog box, click **Yes**.
- Step 9** Initiate a Force switch on the protect port:
- In the Selected Group area, click the protect port. Next to Switch Commands, click **Force**.
 - In the Confirm Force Operation dialog box, click **Yes**.
 - 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
 - Working port: Working/Active
- Step 12** Return to your originating procedure (NTP).

DLP-A89 Remap the K3 Byte

Purpose	This task provisions the K3 byte. Do not remap the K3 byte unless specifically required to run an ONS 15454 BLSR through third-party equipment. This task is unnecessary for most users.
Tools/Equipment	OC48 AS cards must be installed on the BLSR span that you remap.
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher



Caution

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

- Step 1** In node view, double-click the OC48 AS card that connects to the third-party equipment.
- Step 2** Click the **Provisioning > Line** tabs.
- Step 3** Click **BLSR Ext Byte** and choose the alternate byte: Z2, E2, or F1.
- Step 4** Click **Apply**.
- Step 5** (Four-fiber BLSRs only) Repeat Steps [2](#) through [4](#) for each protect card.
- Step 6** Repeat this task at the node and card on the other end of the BLSR span.



Note

The extension byte chosen in [Step 3](#) should match at both ends of the span.

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

DLP-A91 BLSR Switch Test

Purpose	This task verifies that protection switching is working correctly in a BLSR.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

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

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

Step 3 Click the row of the BLSR you will switch, then click **Edit**.

Step 4 Initiate a Force Ring switch the west port:

- a. Right-click any BLSR node west port and choose **Set West Protection Operation**. [Figure 19-2 on page 19-11](#) shows an example. (To move a graphic icon, click it, then press **Ctrl** while you drag and drop it to a new location.)



Note For two fiber BLSRs, the squares on the node icons represent the BLSR working and protect channels. You can right-click either channel. For four-fiber BLSRs, the squares represent ports. Right-click either working or protect port.

- b. In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Ring switch. The BLSR span lines turn purple where the switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the West port:
 - **FORCED-REQ-RING**—A Force Switch Request On Ring condition is reported against the span's working slot on the west side of the node.
 - **RING-SW-EAST**—A Ring Switch Active on the east side condition is reported against the working span on the east side of the node.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

- d. Verify that the following conditions are reported on the node that is connected to the West line of the node where you performed the switch:

- FE-FRCDWKSWPR-RING—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the east side of the node.
 - RING-SW-WEST—A Ring Switch Active on the west side condition is reported against the working span on the west side of the node.
- Step 6** (Optional) If you remapped the K3 byte to run an ONS 15454 BLSR through third-party equipment, check the following condition. Verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.
- Step 7** Verify the BLSR line status on each node:
- a. From the View menu choose **Go to Node View**.
 - b. Click the **Maintenance > BLSR** tabs.
 - c. Verify the following:
 - The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node where you invoked the Force Ring switch.
 - The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node that is connected to the west line of the node where you invoked the Force Ring switch.
 - The line states are shown as Act/Act on both East and west sides of the remaining nodes in the ring.
- Step 8** From the View menu, choose **Go to Network View**.
- Step 9** Click the **Alarms** tab.
- a. Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on [page 19-18](#) as necessary.
 - b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 10** Display the BLSR window where you invoked the Force Ring switch (the window might be hidden by the CTC window).
- Step 11** Clear the switch on the west port:
- a. Right-click the west port of the BLSR node where you invoked the Force Ring switch and choose **Set West Protection Operation**.
 - b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.
 - c. Click **OK**.
 - d. Click **Yes** in the Confirm BLSR Operation dialog box.
- On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.
- Step 12** From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.
- Step 13** Verify the BLSR line status on each node:
- a. From the View menu, choose **Go to Node View**.
 - a. Click the **Maintenance > BLSR** tabs.
 - b. Verify that the line states are shown as Act/Stby on both the east and west sides of each node in the ring.

Step 14 Initiate a Force Ring switch on the east port:

- a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **FORCE RING** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the working BLSR channel where you invoked the Force Ring switch. The BLSR span lines are purple where the Force Ring switch was invoked, and all span lines between other BLSR nodes are green. The span lines might take a few moments to change color.

Step 15 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that the following conditions are reported on the node where you invoked the Force Ring switch on the East port:
 - **FORCED-REQ-RING**—A Force Switch Request On Ring condition is reported against the span's working slot on the east side of the node.
 - **RING-SW-WEST**—A Ring Switch Active on the west side condition is reported against the working span on the east side of the node.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

- d. Verify that the following conditions are reported on the node that is connected to the East line of the node where you performed the switch:
 - **FE-FRCDWKSWPR-RING**—A Far-End Working Facility Forced to Switch to Protection condition is reported against the working span on the west side of the node.
 - **RING-SW-EAST**—A Ring Switch Active on the east side condition is reported against the working span on the west side of the node.

Step 16 (Optional) If you remapped the K3 byte to run an ONS 15454 BLSR through third-party equipment, verify a FULLPASSTHR-BI condition reported on other nodes that are not connected to the west side of the node where you invoked the Force Ring switch.

Step 17 Verify the BLSR line status on each node:

- a. From the View menu, choose **Go to Node View**.
- b. Click the **Maintenance > BLSR** tabs.
 - Verify the following:
 - The line states are shown as Stby/Stby on the east side of the node and Act/Act on the west side of the node where you invoked the Force Ring switch.
 - The line states are shown as Stby/Stby on the west side of the node and Act/Act on the east side of the node that is connected to the east line of the node where you invoked the Force Ring switch.
 - The line states are shown as Act/Act on both East and West sides of the remaining nodes in the ring.

Step 18 From the View menu, choose **Go to Network View**.

- Step 19** Click the **Alarms** tab.
- Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on [page 19-18](#) as necessary.
 - Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 20** Display the BLSR window where you invoked the Force Ring switch (the window might be hidden by the CTC window).
- Step 21** Clear the switch on the east port:
- Right-click the east port of the BLSR node where you invoked the Force Ring switch and choose **Set East Protection Operation**.
 - In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.
 - Click **OK**.
 - Click **Yes** in the Confirm BLSR Operation dialog box.
- On the network view graphic, the Force Ring switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.
- Step 22** From network view, click the **Conditions** tab. Verify that all conditions raised in this procedure are cleared from the network. If unexplained conditions appear, resolve them before continuing.
- Step 23** Verify the BLSR line status on each node:
- From the View menu, choose **Go to Node View**.
 - Click the **Maintenance > BLSR** tabs.
 - Verify that the line states are shown as Act/Stby on both the East and west sides of each node in the ring.
- Step 24** From the File menu, choose **Close** to close the BLSR window.
- Step 25** Return to your originating procedure (NTP).

DLP-A92 Four-Fiber BLSR Exercise Span Test

Purpose	This task exercises a four-fiber BLSR span. Ring exercise conditions (including the K-byte pass-through) are reported and cleared within 10 to 15 seconds.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC , page 17-61
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 **Provisioning > BLSR** tabs.
- Step 3** Click the BLSR you will exercise, then click **Edit**.

Step 4 Exercise the west span:

- a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. (To move a graphic icon, press **Ctrl** while you drag and drop it to a new location.)



Note The squares on the network map represent ports. Right-click a working port.

- b. In the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.
- c. Click **OK**. In the Confirm BLSR Operation dialog box, click **Yes**.
On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 5 Verify the conditions:

- a. Click the **Conditions** tab, then click **Retrieve**.
- b. Verify the following conditions:
 - EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
 - FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the east span of the node connected to the west side of the node where you exercised the span.
 - KB-PASSTHR—If applicable, a K Byte Pass Though Active condition is reported.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the [“DLP-A227 Disable Alarm Filtering” task on page 19-18](#) as necessary.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 7 Exercise the east span:

- a. Right-click the east port of the four-fiber BLSR node that you want to exercise and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.
- c. Click **OK**.
- d. In the Confirm BLSR Operation dialog box, click **Yes**.
On the network view graphic, an E appears on the BLSR channel where you invoked the exercise. The E will appear for 10 to 15 seconds, then disappear.

Step 8 From the File menu, choose **Close**.**Step 9** Verify the conditions:

- a. Click the **Conditions** tab, then click **Retrieve**.
- b. Verify the following conditions:

- EXERCISING-SPAN—An Exercise Ring Successful condition is reported on the node where the span was exercised.
- FE-EX-SPAN—A Far-End Exercise Span Request condition is reported against the east span of the node connected to the west side of the node where you exercised the span.
- KB-PASSTHR—If applicable, a K Byte Pass Through Active condition is reported.



Note Make sure the Filter button in the lower right corner of the window is off. Click the Node column to sort conditions by node.

- Step 10** Click the **Alarms** tab.
- a. Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on [page 19-18](#) as necessary.
 - b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 11** From the File menu, choose **Close** to close the BLSR window.
- Step 12** Return to your originating procedure (NTP).

DLP-A93 Four-Fiber BLSR Span Switching Test

Purpose	This task verifies that traffic will switch from working to protect fibers on a four-fiber BLSR span.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC , page 17-61
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 **Provisioning > BLSR** tabs.
- Step 3** Click **Edit**. A BLSR window appears containing a graphic of the BLSR.



Note If the node icons are stacked on the BLSR graphic, press Ctrl while you drag and drop each one to a new location so you can see the BLSR port information clearly.

- Step 4** Switch the west span:
- a. Right-click the west port of the four-fiber BLSR node that you want to exercise and choose **Set West Protection Operation**. [Figure 19-2 on page 19-11](#) shows an example.



Note The squares on the network map represent ports. Right-click a working port.

- b. In the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the protection switch. The BLSR span lines turn purple where the Force Span switch was invoked, and all span lines between other BLSR nodes turn green.

Step 5 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.
- c. Verify that a SPAN-SW-WEST (Span Switch West) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-EAST (Span Switch East) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off. Click the Node column to sort conditions by node.

Step 6 Click the **Alarms** tab.

- a. Verify that the alarm filter is not on. See the [“DLP-A227 Disable Alarm Filtering” task on page 19-18](#) as necessary.
- b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.

Step 7 Display the BLSR window where you invoked the Force Span switch (the window might be hidden by the CTC window).

Step 8 Clear the west switch:

- a. Right-click the west port of the BLSR node where you invoked the Force Span switch and choose **Set West Protection Operation**.
- b. In the Set West Protection Operation dialog box, choose **CLEAR** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the Confirm BLSR Operation dialog box.

On the network view graphic, the Force Span switch is removed, the F disappears, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.

Step 9 Switch the east span:

- a. Right-click the east port of BLSR node and choose **Set East Protection Operation**.
- b. In the Set East Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.
- c. Click **OK**.
- d. Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

On the network view graphic, an F appears on the BLSR channel where you invoked the Force Span switch. The BLSR span lines are purple where the Force Span switch was invoked, and all span lines between other BLSR nodes are green. The span lines might take a few moments to change color.

Step 10 Verify the conditions:

- a. Click the **Conditions** tab.
- b. Click **Retrieve**.

- c. Verify that a SPAN-SW-EAST (Span Switch East) condition is reported on the node where you invoked the Force Span switch, and a SPAN-SW-WEST (Span Switch West) condition is reported on the node connected to the west line of the node where you performed the switch. Make sure the Filter button in the lower right corner of window is off.
- Step 11** Click the **Alarms** tab.
- a. Verify that the alarm filter is not on. See the “[DLP-A227 Disable Alarm Filtering](#)” task on [page 19-18](#) as necessary.
 - b. Verify that no unexplained alarms appear on the network. If unexplained alarms appear, resolve them before continuing. Refer to the *Cisco ONS 15454 Troubleshooting Guide* if necessary.
- Step 12** Display the BLSR window where you invoked the Force Span switch (the window might be hidden by the CTC window).
- Step 13** Clear the east switch:
- a. Right-click the east port of the BLSR node where you invoked the Force Span switch and choose **Set East Protection Operation**.
 - b. In the Set East Protection Operation dialog box, choose **CLEAR** from the drop-down list.
 - c. Click **OK**.
 - d. Click **Yes** in the Confirm BLSR Operation dialog box.
- On the network view graphic, the Force Span switch is removed, the F indicating the switch is removed, and the span lines between BLSR nodes will be purple and green. The span lines might take a few moments to change color.
- Step 14** From the File menu, choose **Close** to close the BLSR window.
- Step 15** Return to your originating procedure (NTP).

DLP-A94 Path Protection Configuration Protection Switching Test

Purpose	This task verifies that a path protection span is switching correctly.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
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 the Network View**.
- Step 2** Right-click a network span and choose **Circuits**.
- The Circuits on Span dialog box shows 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 for all circuits on the span:
- Click the **Perform Path Protection span switching** field.
 - Choose **FORCE SWITCH AWAY** from the drop-down list.
 - Click **Apply**.
 - In the Confirm Path Protection Switch dialog box, click **Yes**.
 - 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:
- Click the **Perform Path Protection span switching** field.
 - Choose **CLEAR** from the drop-down list.
 - Click **Apply**.
 - In the Confirm Path Protection Switch dialog box, click **Yes**.
 - 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-A95 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-A60 Log into CTC, page 17-61
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 containing the DS1-14, DS1N-14, DS1/E1-56, DS3XM-6, or DS3XM-12 card where the circuit will originate.



Note

A VT circuit source or destination can be on the STS grooming endpoint of a portless aggregation circuit.

- Step 3** If you chose DS3XM-6 or DS3XM-12 as the card, choose the port from the Port drop-down list.
- Step 4** From the DS-1 drop-down list, choose the source DS-1.

- 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. The destination is typically a DS-1 card. You can also choose an OC-N card to map the DS-1 to a VT1.5 for OC-N transport.
- Step 9** Depending on the destination card, choose the destination port, STS, VT, or DS1 from the drop-down lists that appear based on the card selected in Step 8. See Table 6-2 on page 6-3 for a list of valid options. CTC does not display ports, STSs, VTs, or DS1s already used by other circuits. If you and another user who is working on the same network choose the same port, STS, VT, port, or DS1 simultaneously, one of you receives a Path in Use error and is unable to complete the circuit. The user with the partial 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-A96 Provision a DS-1 or DS-3 Circuit Route

Purpose	This task provisions the circuit route for manually routed DS-1 or DS-3 circuits.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In the Route Review/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 yellow. In the Selected Span area, the From and To fields provide span information. The source STS and VT (DS-1 circuit only) appear.
- 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 for DS-1 circuits, adjust the Source VT field; otherwise, continue with Step 5.



Note VT is gray (unavailable) for DS-3 circuits.

- Step 5** Click **Add Span**. The span is added to the Included Spans list and the span arrow turns blue.
- Step 6** If the Fully Protect Path check box is checked in the Circuit Routing Preferences panel, you must:
- 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 BLSR or 1+1 portions of route from the source to the destination.
 - For circuits routed on path protection DRI topologies, provision the working and protect paths as well as spans between the DRI nodes.
- Step 7** Repeat Steps 2 through 6 until the circuit is provisioned from the source to the destination node through all intermediary nodes.
- Step 8** Return to your originating procedure (NTP).
-

DLP-A97 Provision an OC-N Circuit Source and Destination

Purpose	This task provisions an OC-N circuit source and destination.
Tools/Equipment	None
Prerequisite Procedures	DLP-A60 Log into CTC, page 17-61
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 and destination.

- 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 OC-N card where the circuit originates. (If card 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 lists. The Port list is only available if the card has multiple ports. STSs do not appear if they are already in use by other circuits.



Note The STSs that appear depend on the card, circuit size, and protection scheme. For example, if you create an STS-3c circuit on an OC-12 card in a path protection configuration, only four STSs are available. If you create an STS-3c circuit on an OC-12 card in a BLSR, two STSs are available because of the BLSR protection characteristics.

- Step 4** 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 3 to define the secondary source.
- Step 5** Click **Next**.
- Step 6** From the Node drop-down list, choose the destination node.

- Step 7** From the Slot drop-down list, choose the slot containing the OC-N 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 8** Depending on the card selected in [Step 2](#), choose the destination port and/or STS from the Port and STS drop-down lists. The Port drop-down list is available only if the card has multiple ports. The STSs that appear depend on the card, circuit size, and protection scheme.
- Step 9** 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 [6](#) through [8](#) to define the secondary destination.
- Step 10** Click **Next**.
- Step 11** Return to your originating procedure (NTP).
-

DLP-A99 Determine Available VLANs

Purpose	This task verifies that the network has the capacity to support the additional new VLANs required for the creation E-Series circuits. It does not apply to E-Series cards in port-mapped mode.
Tools/Equipment	E-Series Ethernet cards (E100T-12/E100T-G, E1000-2/E1000-2-G) must be installed at each end of the Ethernet circuit.
Prerequisite Procedures	NTP-A127 Verify Network Turn Up, page 6-5 DLP-A60 Log into CTC, page 17-61
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

- Step 1** In any CTC view, click the **Circuits** tab.
- Step 2** Click any existing Ethernet circuit.
- Step 3** Click **Edit**, then click the **VLANs** tab.
The Edit Circuit dialog box shows the number of VLANs used by circuits and the total number of VLANs available for use.
- Step 4** Determine that the number of available VLANs listed is sufficient for the number of E-Series Ethernet circuits that you will create.



Caution Multiple E-Series Ethernet circuits with spanning tree enabled block each other if the circuits traverse the same E-Series Ethernet card and use the same VLAN.

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

