CISCO SYSTEMS

Cisco ONS 15454 Installation and Operations Guide

Product and Documentation Release 3.1
November 2001

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
        800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7813453=
Text Part Number: 78-13453-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.
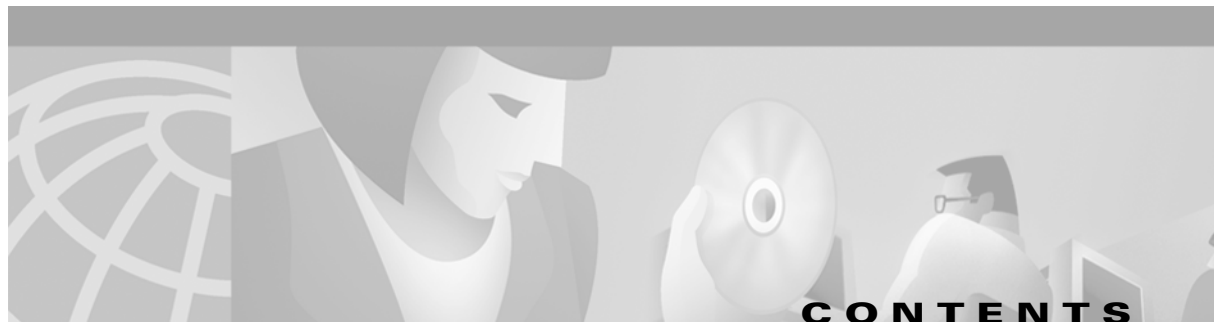
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Cisco ONS 15454 Installation and Operations Guide, Release 3.1
Copyright © 2001, Cisco Systems, Inc.
All rights reserved.

CONTENTS

CHAPTER 8   **Performance Monitoring**   8-1

F I G U R E S

T A B L E S

Hardware Installation

Alarm Monitoring and Management

SNMP

About This Manual

This section explains who should read the *Cisco ONS 15454 Installation and Operations Guide*, how the document is organized, related documentation, document conventions, how to order print and CD-ROM documentation, and how to obtain technical assistance.

Audience

This guide is for Cisco ONS 15454 administrators who are responsible for hardware installation, software installation, node setup, and node and network configuration. For troubleshooting, maintenance, and card detail reference information, see the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*. Users who require TL1 information should consult the *Cisco ONS 15454 TL1 Command Guide*.

Organization

Chapter Number and Title	Description
Chapter 1, "Hardware Installation"	Provides rack installation and power instructions for the ONS 15454, including component installation such as cards, cables, EIAs, and GBICs.
Chapter 2, "Software Installation"	Explains how to install the ONS 15454 software application and use its graphical user interface (GUI).
Chapter 3, "Node Setup"	Explains how to provision a node, including setting up timing, protection, and security and storing general node and network information.
Chapter 4, "IP Networking"	Explains how to set up ONS 15454s in internet protocol (IP) networks and provides scenarios showing nodes in common IP configurations. It explains how to create static routes and use the Open Shortest Path First (OSPF) protocol.
Chapter 5, "SONET Topologies"	Provides instructions for configuring UPSRs, BLSRs, subtending rings, linear 1+1 ADM protection, PPMNs, and DCC tunnels.

Chapter Number and Title	Description
Chapter 6, "Circuits and Tunnels"	Describes how to create standard STS and VT1.5 circuits as well as VT tunnels, multiple drop circuits, and monitor circuits. The chapter also explains how to edit UPSR circuits and create path traces to monitor traffic.
Chapter 7, "Card Provisioning"	Provides procedures for changing the default transmission parameters for ONS 15454 electrical and optical cards. The chapter also includes provisioning the Alarm Interface Controller card, enabling optical cards for SDH, and converting DS-1 and DS-3 cards from 1:1 to 1:N card protection.
Chapter 8, "Performance Monitoring"	Provides performance monitoring thresholds for ONS 15454 electrical and optical cards.
Chapter 9, "Ethernet Operation"	Explains how to use the Ethernet features of the ONS 15454, including transporting Ethernet traffic over SONET, creating and provisioning VLANs, protecting Ethernet traffic, provisioning Multicard and Single-card EtherSwitch, provisioning several types of Ethernet circuits, viewing Ethernet performance data, and creating Ethernet remote monitoring (RMON) alarm thresholds.
Chapter 10, "Alarm Monitoring and Management"	Explains how to view and manage alarms with CTC, which includes viewing current and historical alarm data, creating alarm profiles, and suppressing alarms. To find procedures for clearing CTC alarms, see the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting and Reference Guide*.
Chapter 11, "SNMP"	Explains how Simple Network Management Protocol (SNMP) is used with the ONS 15454.
Appendix A, "Circuit Routing"	Explains automated and manual circuit routing in detail.
Appendix B, "Regulatory and Compliance Requirements"	Provides customer, industry, and government requirements met by the ONS 15454. Installation warnings are also included.
Appendix C, "Acronyms"	Defines commonly-used acronyms.
Appendix D, "Glossary"	Defines commonly-used terms.

Related Documentation

Cisco ONS 15454 Troubleshooting and Maintenance Guide, Release 3.1

Cisco ONS 15454 TL1 Command Guide, Release 3.1

Cisco ONS 15454 Product Overview, Release 3.1

Release Notes for the Cisco ONS 15454, Release 3.1

Cisco Warranty Services for ONG Products

Cisco ONS 15454 Quick Configuration Guide

Cisco ONS 15454 Quick Installation Guide

Cisco ONS 15454 Quick Reference for TL1 Commands, Release 3.1

Related products:

Cisco ONS 15216 EDFA1 Operations Guide

Installing the Cisco ONS 15216 DWDM Filters

Installing Cisco ONS 15216 OADMS

Installing Cisco ONS 15216 Optical Performance Manager Operations Guide

Conventions

The following conventions are used throughout this publication:

Note Means reader take note. Notes contain helpful suggestions or useful background information.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means reader be careful. In this situation, you might do something that could result in harm to yourself or others.**

Tip Means the information might help you solve a problem.

Convention	Definition
Telcordia	Replaces all instances of Bellcore, the former name of Telcordia Technologies, Inc.
Cisco Transport Controller (CTC)	Replaces all instances of Cerent Management System (CMS)
Bold	Denotes icons, buttons, or tabs that the user must select
>	Used to separate consecutive actions; for example, "click the Maintenance>Protection>Ring tabs"
Procedure:	Precedes all procedures; a horizontal line indicates the end of each procedure

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Release 3.1 of the *Cisco ONS 15454 Installation and Operations Guide*, *Cisco ONS 15454 Troubleshooting and Reference Guide*, and the *Cisco ONS 15454 TL1 Command Guid*e, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM, a member of the Cisco Connection Family, is updated as required. Therefore, it might be more current than printed documentation. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www.europe.cisco.com.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation, including the *Optical Networking Product* CD-ROM, from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. The toll-free Optical Networking Assistance number is 1-877-323-7368.

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.

- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Hardware Installation

This chapter provides procedures for installing the Cisco ONS 15454. Chapter topics include:

- Installation equipment
- Rack installation
- Front door access
- Backplane covers
- Fan-tray assembly
- Power and ground installation
- Backplane pin connections (alarms, timing, LAN, and craft interface)
- Coaxial and DS-1 cable installation
- Card installation
- Fiber-optic cable installation
- Cable routing and management
- Ferrite installation
- Hardware specifications
- Hardware and software compatibility

Note The Cisco ONS 15454 assembly is intended for use with telecommunications equipment only.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Warning **This equipment must be installed and maintained by service personnel as defined by AS/NZS 3260. Incorrectly connecting this equipment to a general purpose outlet could be hazardous. The telecommunications lines must be disconnected 1) before unplugging the main power connector and/or 2) while the housing is open.**

⚠ **Warning**   **The ONS 15454 is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock, key, or other means of security. A restricted access area is controlled by the authority responsible for the location.**

⚠ **Warning**   **The ONS 15454 is suitable for mounting on concrete or other non-combustible surfaces only.**

⚠ **Caution**   Unused card slots should be filled with a blank faceplate (Cisco P/N 15454-BLANK). The blank faceplate ensures proper airflow when operating the ONS 15454 without the front door attached, although Cisco recommends that the front door remain attached.

✎ **Note**   The ONS 15454 is designed to comply with GR-1089-CORE Type 2 and Type 4. Install and operate the ONS 15454 only in environments that do not expose wiring or cabling to the outside plant. Acceptable applications include Central Office Environments (COEs), Electronic Equipment Enclosures (EEEs), Controlled Environment Vaults (CEVs), huts, and Customer Premise Environments (CPEs).

1.1 Installation Overview

When installed in an equipment rack, the ONS 15454 assembly is typically connected to a fuse and alarm panel to provide centralized alarm connection points and distributed power for the ONS 15454. Fuse and alarm panels are third-party equipment and are not described in this documentation. If you are unsure about the requirements or specifications for a fuse and alarm panel, consult the documentation for the related equipment. The front door of the ONS 15454 allows access to the shelf assembly, fan-tray assembly, and cable-management area. The backplanes provide access to alarm contacts, external interface contacts, power terminals, and BNC/SMB connectors.

⚠ **Warning**   **The ONS 15454 relies on the protective devices in the building installation to protect against short circuit, overcurrent, and grounding faults. Ensure that the protective devices are properly rated to protect the system, and that they comply with national and local codes.**

⚠ **Warning**   **Incorporate a readily-accessible, two-poled disconnect device in the fixed wiring.**

You can mount the ONS 15454 in a 19- or 23-inch rack. The shelf assembly weighs approximately 55 pounds with no cards installed and features a front door for added security, a fan tray module for cooling, and extensive cable-management space.

ONS 15454 optical cards have SC connectors on the card faceplate. Fiber optic cables are routed into the front of the destination cards. Electrical cards (DS-1, DS-3, DS3XM-6, and EC-1) require electrical interface assemblies (EIAs) to provide the cable connection points for the shelf assembly. In most cases, EIAs are ordered with the ONS 15454 and come pre-installed on the backplane. See the "Backplane Access" section on page 1-14 for more information about the EIAs.

The ONS 15454 is powered using -48V DC power. Negative, return, and ground power terminals are accessible on the backplane.

Table 1-1 lists the tasks required to install an ONS 15454.

Table 1-1   Installation Tasks

Task	Reference
Mount the ONS 15454 in the rack.	See the "Rack Installation" section on page 1-5.
Install the EIAs.	See the "Install a BNC, High-Density BNC, or SMB EIA" procedure on page 1-22.
Install the fan-tray assembly.	See the "Fan-Tray Assembly Installation" section on page 1-25.
Ground the equipment.	See the "Power and Ground Installation" section on page 1-28.
Run the power cables and fuse the power connections.	See the "Power and Ground Installation" section on page 1-28.
Connect the backplane pins.	See the "Alarm, Timing, LAN, and Craft Pin Connections" section on page 1-32.
Install the coaxial cable and DS-1 cable on the back of the unit.	See the "Coaxial Cable Installation" section on page 1-36 and the "DS-1 Cable Installation" section on page 1-39.
Install the cards.	See the "Card Installation" section on page 1-44.
Install the fiber-optic cables.	See the "Fiber-Optic Cable Installation" section on page 1-52.

Note   In this chapter, the terms "ONS 15454" and "shelf assembly" are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15454 refers to the entire system, both hardware and software.

Install the ONS 15454 in compliance with your local and national electrical codes:

- United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code
- Canada: Canadian Electrical Code, Part I, CSA C22.1
- Other countries: If local and national electrical codes, are not available, refer to IEC 364, Part 1 through Part 7.

Warning   **Read the installation instructions before you connect the system to its power source.**

Warning   **Dispose of this product according to all national laws and regulations.**

1.2 Installation Equipment

You will need the following tools and equipment to install and test the ONS 15454.

1.2.1 Included Materials

The following materials are required and are shipped with the ONS 15454. The number in parentheses gives the quantity of the item included in the package.

- #12-24 x 3/4 pan head phillips mounting screws (8)
- #12 -24 x 3/4 socket set screws (2)
- T-handle #12-24 hex tool for set screws (1)
- ESD wrist strap with 1.8 m (6 ft) coil cable (1)
- Tie wraps (10)
- Pinned Allen key for front door (1)
- Spacers (4)
- Spacer mounting brackets (2)
- Clear plastic rear cover (1)
- Bottom brackets for the fan-tray air filter

1.2.2 User-Supplied Materials

The following materials and tools are required but are not supplied with the ONS 15454.

- Equipment rack (22 inches total width for a 19-inch rack; 26 inches total width for a 23-inch rack)
- Fuse panel
- Power cable (from fuse and alarm panel to assembly), #10 AWG, copper conductors, 194°F [90°C])
- Ground cable #6 AWG stranded
- Alarm cable pairs for all alarm connections, #22 or #24 AWG, solid tinned
- Shielded Building Integrated Timing Supply (BITS) clock cable pair #22 or #24, solid tinned
- Single mode SC fiber jumpers with UPC polish (55 dB or better) for optical cards
- Shielded coaxial cable terminated with SMB or BNC connectors for DS-3 cards
- Shielded ABAM cable terminated with AMP Champ connectors or unterminated for DS-1 cards with #22 or #24 AWG ground wire (typically about two feet in length)
- Tie wraps and/or lacing cord
- Labels
- Listed pressure terminal connectors such as ring and fork types; connectors must be suitable for 10AWG copper conductors

1.2.2.1 Tools Needed

- #2 phillips screw driver
- Medium slot head screw driver
- Small slot head screw driver
- Wire wrapper
- Wire cutters

- Wire strippers

- Crimp tool

1.2.2.2 Test Equipment

- Volt meter

- Power meter (for use with fiber optics only)

- Bit Error Rate (BER) tester, DS-1 and DS-3

1.3 Rack Installation

Warning   **To prevent the equipment from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 131°F (55°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.**

The ONS 15454 is easily mounted in a 19- or 23-inch equipment rack. The shelf assembly projects five inches from the front of the rack. It mounts in both EIA-standard and Telcordia-standard racks. The shelf assembly is a total of 17 inches wide with no mounting ears attached. With the mounting ears attached, the shelf assembly is 19 inches wide. Ring runs are not provided by Cisco and may hinder side-by-side installation of shelves where space is limited.

The ONS 15454 measures 18.5 inches high, 19 or 23 inches wide (depending on which way the mounting ears are attached), and 12 inches deep (47 by 48.3 by 30.5 cm). You can install up to four ONS 15454s in a seven-foot equipment rack. The ONS 15454 must have 1 inch of airspace below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 is installed underneath the shelf assembly, the air ramp on top of the lower shelf assembly provides the air spacing needed and should not be modified in any way. Figure 1-1 shows the dimensions of the ONS 15454.

Note   The 10 Gbps compatible shelf assembly (15454-SA-10G) and fan-tray assembly (15454-FTA3) are required with the ONS 15454 XC10G, OC-192, and OC-48 any slot (AS) cards.

Warning   **The ONS 15454 should be installed in the lower rack position or mounted above another ONS 15454 shelf assembly.**

Warning   **The ONS 15454 must have 1 inch of airspace below the installed shelf assembly to allow air flow to the fan intake. The air ramp (the angled piece of sheet metal on top of the shelf assembly) provides this spacing and should not be modified in any way.**

Figure 1-1   Cisco ONS 15454 dimensions

Top View
22" total width

12"

19" or 23" between mounting screw holes

Side View
5"

18.5"

12"

Front View
22" total width

32099

19" or 23" between mounting screw holes
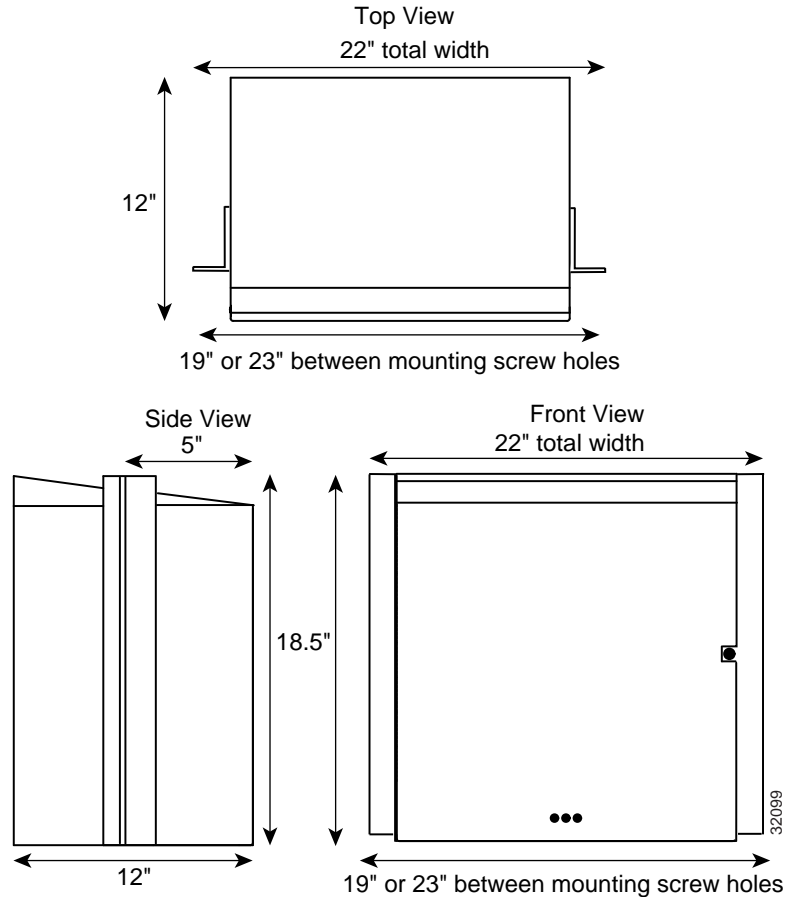
1.3.1 Reversible Mounting Bracket

⚠
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 non-conductive 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.

The shelf assembly comes preset for installation in a 23-inch rack, but you can reverse the mounting bracket to fit the smaller, 19-inch rack. The following steps describe how to reverse the shelf assembly mounting bracket to fit a 19-inch rack.

Procedure: Reverse the Mounting Bracket to Fit a 19-Inch Rack

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 1-2).

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 procedure for the mounting bracket on the opposite side.

Figure 1-2   Reversing the mounting brackets (23-inch position to 19-inch position)
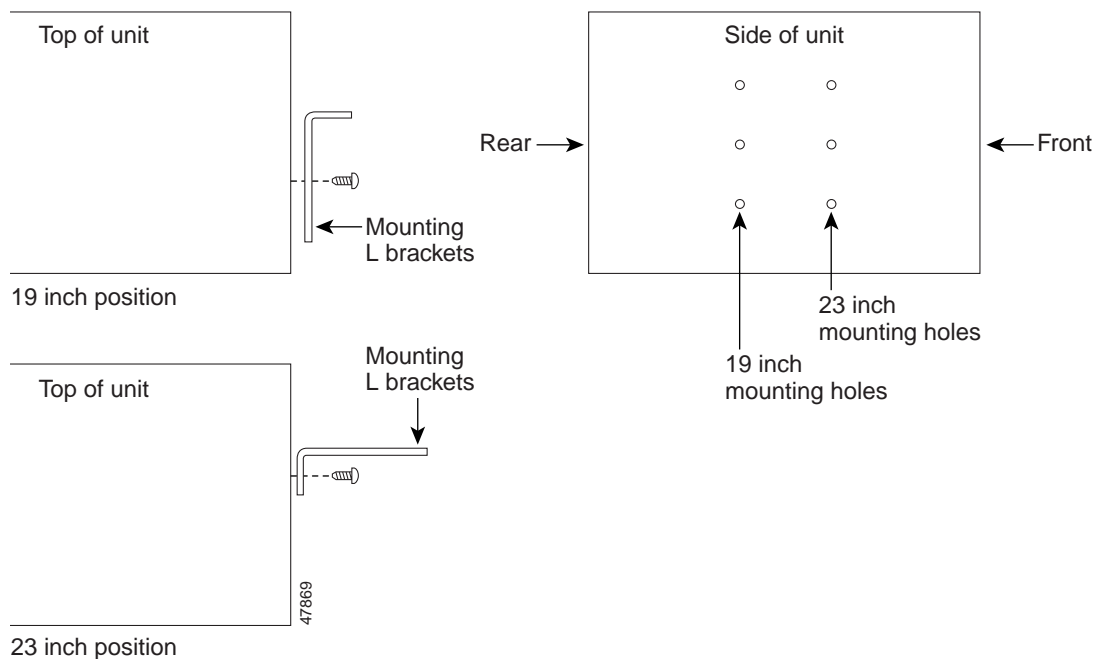
1.3.2 Mounting a Single Node

Mounting the ONS 15454 in a rack requires a minimum of 18.5 inches of vertical rack space (and one inch for air flow). To ensure the mounting is secure, use two to four #12-24 mounting screws for each side of the shelf assembly. Figure 1-3 shows the rack mounting position for the ONS 15454.

Figure 1-3   Mounting an ONS 15454 in a rack

Equipment rack

Universal
ear mounts
(reversible)
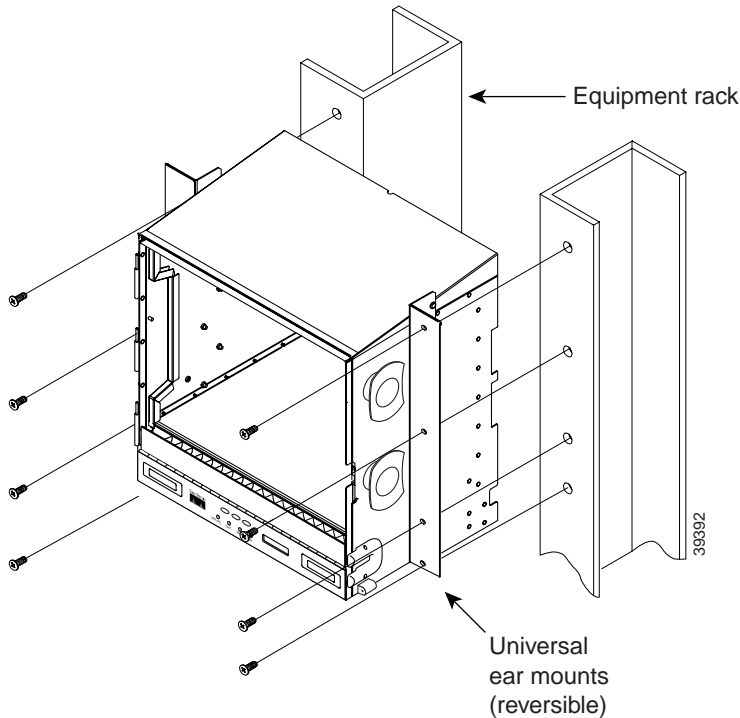
Two people should install the shelf assembly; however, one person can install it using the temporary set screws included. The shelf assembly should be empty for easier lifting. The front door can also be removed to lighten the shelf assembly (see the "Remove the Front Door" procedure on page 1-13).

Note   If you are installing the fan-tray air filter using the brackets provided, mount the brackets on the bottom of the shelf assembly before installing the ONS 15454 in a rack.

Procedure: Mount the Shelf Assembly in a Rack (One Person)

Step 1   Ensure that the shelf assembly is set for the desired rack size (either 19 or 23 inches).

Step 2   Using the hex tool that shipped with the assembly, install the set screws into the screw holes that will not be used to mount the shelf.

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

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

Step 5   Install one mounting screw in each side of the assembly.

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

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

Step 7   Remove the temporary set screws.

Procedure: Mount the Shelf Assembly in a Rack (Two People)

Step 1 Ensure that the shelf assembly is set for the desired rack size (either 19 or 23 inches).

Step 2 Lift the shelf assembly to the desired position in the rack.

Step 3 Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 4 While one person holds the shelf assembly in place, the other person can install one mounting screw in each side of the assembly.

Step 5 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 future slippage.

1.3.3 Mounting Multiple Nodes

Most standard seven-foot racks can hold four ONS 15454s and a fuse and alarm panel. However, unequal flange racks are limited to three ONS 15454s and a fuse and alarm panel or four ONS 15454s and a fuse and alarm panel from an adjacent rack.

If you are using the bottom brackets to install the fan-tray air filter, you can install three shelf assemblies in a standard seven-foot rack. If you are not using the bottom brackets, you can install four shelf assemblies in a rack. The advantage to using the bottom brackets is that you can replace the filter without removing the fan tray.

Procedure: Mount Multiple Shelf Assemblies in a Rack

✎

Note   The ONS 15454 must have one inch 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 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 Install the fuse and alarm panel in the top space.

Step 2 Mount the first ONS 15454 directly below the fuse and alarm panel.

Step 3 Repeat the procedure with the third and fourth ONS 15454s.

1.3.3.1 Four Node Configuration

You can link multiple ONS 15454s using their OC-N cards (i.e., create a fiber-optic bus) to accommodate more access traffic than a single ONS 15454 can support. For example, if you need to drop more than 112 DS-1s or 96 DS-3s (the maximum that can be aggregated in a single node), you can link the nodes

Cisco ONS 15454 Installation and Operations Guide ■

but not merge multiple nodes into a single ONS 15454. You can link nodes with OC-12 or OC-48 fiber spans as you would link any other two network nodes. The nodes can be co-located in a facility to aggregate more local traffic.

Figure 1-4 shows a four-shelf node setup. Each shelf assembly is reorganized as a separate node in the ONS 15454's software interface (Cisco Transport Controller [CTC]), and traffic is mapped using CTC cross-connect options. In the figure, each node uses redundant fiber-optic cards. Node 1 uses redundant OC-N transport and OC-N bus (connecting) cards for a total of four cards, with eight free slots remaining. Nodes 2 and 3 each use two redundant OC-N bus cards for a total of four cards, with eight free slots remaining. Node 4 uses redundant OC-12 bus cards for a total of two cards, with ten free slots remaining. The four node example presented here is one of many ways to set up a multiple-node configuration. See "Chapter 5, "SONET Topologies"" for more information about multiple-node configurations.

Figure 1-4   A four-shelf node configuration
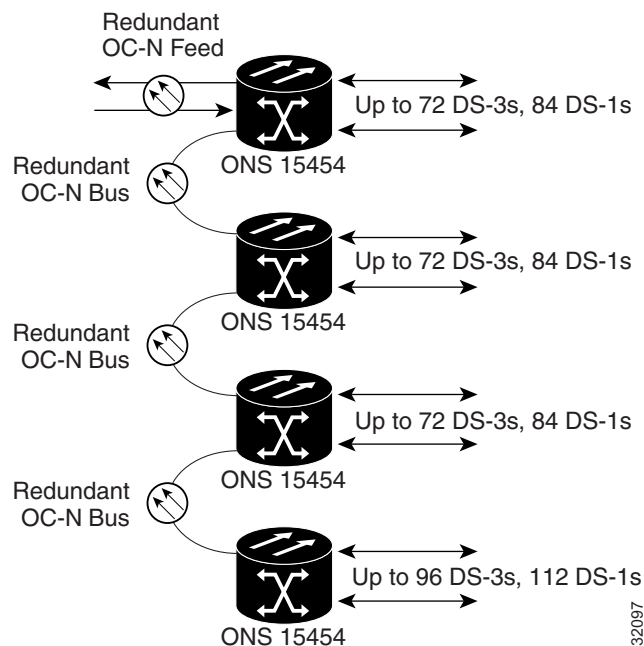
1.3.3.2 ONS 15454 Bay Assembly

The Cisco ONS 15454 Bay Assembly simplifies ordering and installing the ONS 15454 because it allows you to order shelf assemblies pre-installed in a seven-foot rack. The Bay Assembly is available in a three- or four-shelf configuration. The three-shelf configuration includes three ONS 15454 shelf assemblies, a pre-wired fuse and alarm panel, and two cable-management trays. Optional fiber channels can be ordered. The four-shelf configuration includes four ONS 15454 shelf assemblies and a pre-wired fuse and alarm panel. Optional fiber channels can be ordered. A four shelf ONS 15454 Bay Assembly is shown in Figure 1-5.

Figure 1-5   A four-shelf ONS 15454 Bay Assembly
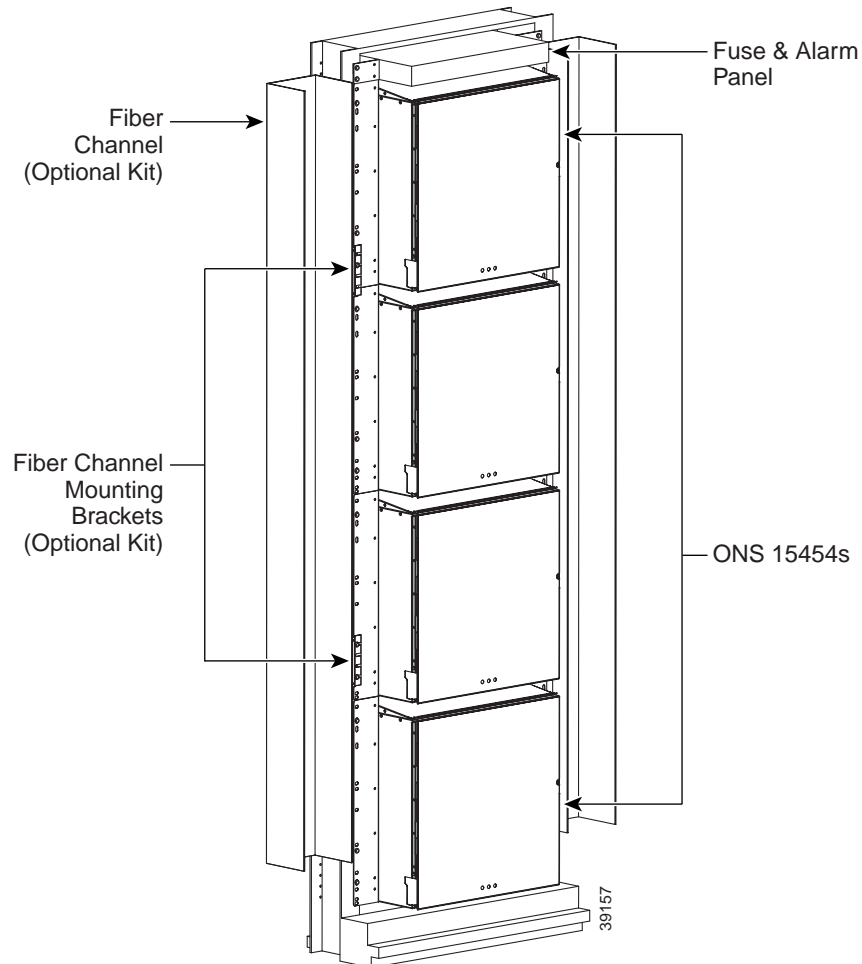
1.4 Front Door Access

The Critical, Major, and Minor alarm LEDs visible through the front door indicate whether a Critical, Major, or Minor alarm is present anywhere on the ONS 15454. These LEDs must be visible so technicians can quickly determine if any alarms are present. You can use the LCD to further isolate alarms. See Chapter 10, "Alarm Monitoring and Management" for more information.

This section tells you how to access ONS 15454 equipment in the front compartment. The ONS 15454 features a locked door to the front compartment. A pinned Allen key that unlocks the front door ships with the ONS 15454. A button on the right side of the shelf assembly releases the door. The front door provides access to the shelf assembly, cable-management tray, fan-tray assembly, and LCD screen (Figure 1-8).

You can remove the front door of the ONS 15454 to provide unrestricted access to the front of the shelf assembly. An erasable label (Figure 1-6) is pasted on the inside of the front door. You can use the label to record slot assignments, port assignments, card types, node ID, rack ID, and serial number for the ONS 15454.

Figure 1-6   The front-door erasable label

Note The front door label also includes the Class I and Class 1M laser warning shown in the laser warning on the front-door label (Figure 1-7).

Figure 1-7   The laser warning on the front-door label

Procedure: Open the Front Cabinet Compartment (Door)

Note 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.

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 1-8   The ONS 15454 front door
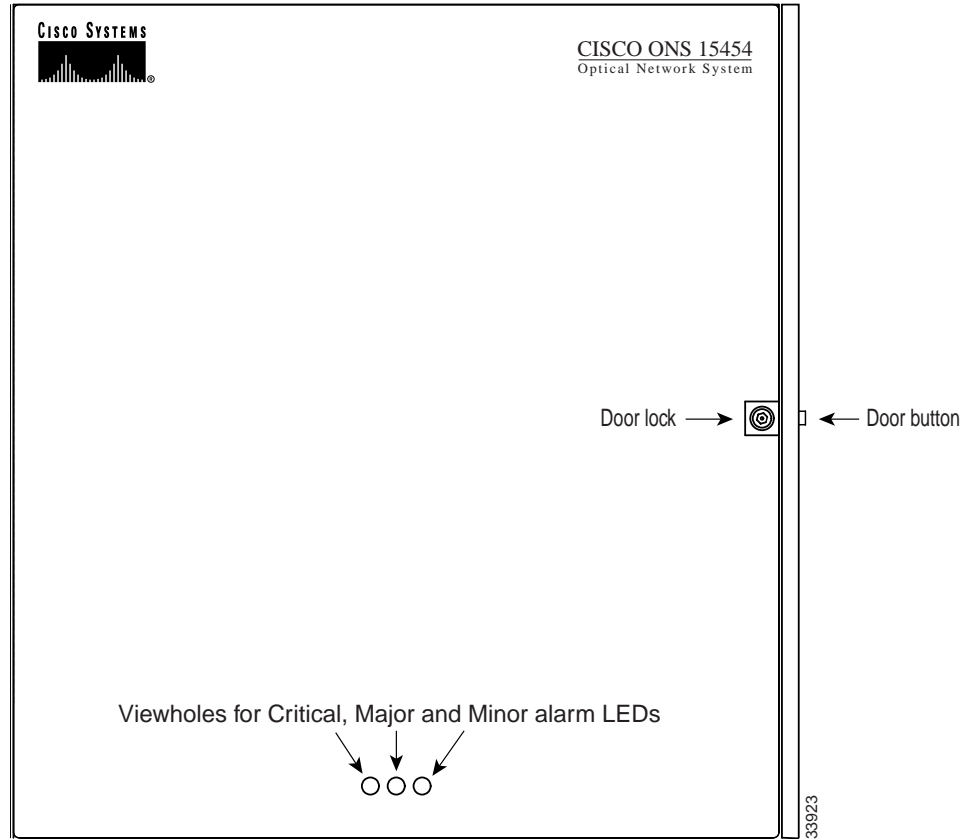
Procedure: Remove the Front Door

Step 1   Open the door.

Step 2   Lift the door from its hinges at the top left-hand corner of the door (Figure 1-9).

Figure 1-9   Removing the ONS 15454 front door

Translucent
circles
for LED
viewing

Door hinge

Assembly hinge pin

Assembly hinge
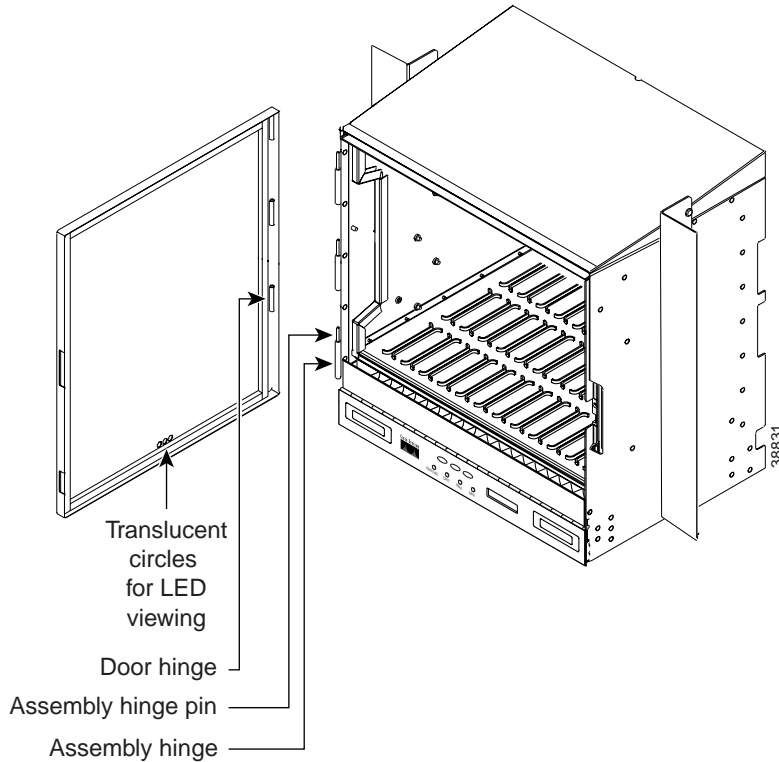
1.5 Backplane Access

To access the ONS 15454 backplane, remove the two standard sheet metal covers on each side of the backplane (Figure 1-10). Each sheet metal cover is held in place with nine 6-32 x 3/8 inch phillips screws.

Figure 1-10   Backplane sheet metal covers
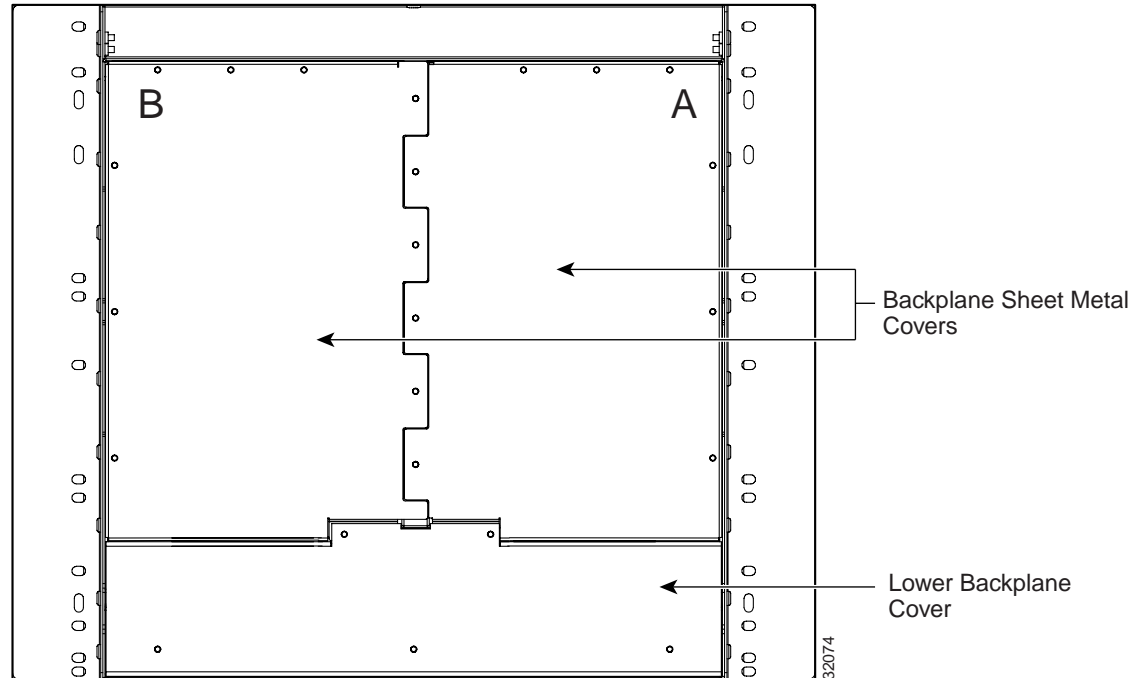
Procedure: Remove the Backplane Sheet Metal Covers

Step 1   To remove the lower backplane 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 sheet metal cover(s) whenever EIA(s) are not installed.

1.5.1 Lower Backplane Cover

The lower section of the ONS 15454 backplane is covered by a clear plastic protector, which is held in place by five 6-32 x 1/2 inch screws. Remove the lower backplane cover to access the alarm interface panel (AIP), alarm pin field, frame ground, and power terminals.

Figure 1-11   Removing the lower backplane cover
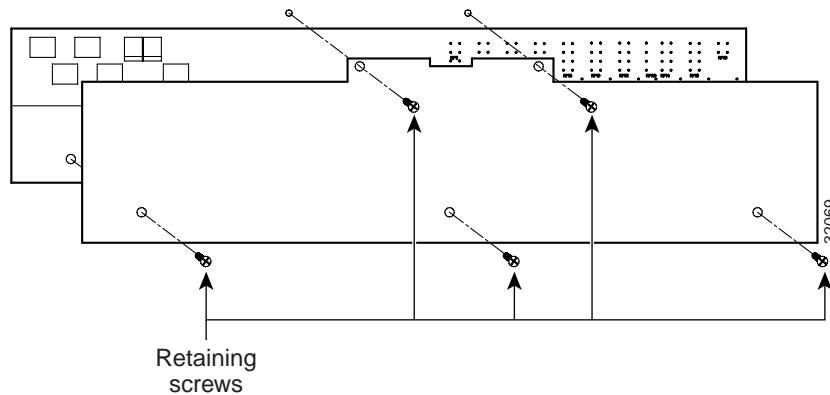
Retaining
screws

Procedure: Remove the Lower Backplane Cover

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

Step 2   Grasp the clear plastic cover at each side.

Step 3   Gently pull the cover away from the backplane (shown in Figure 1-11).

1.5.2 Alarm Interface Panel

The AIP is located above the alarm pin field on the lower section of the backplane. The AIP provides surge protection for the ONS 15454. It also provides an interface from the backplane to the fan-tray assembly and LCD. The AIP plugs into the backplane using a 96-pin DIN connector and is held in place with two retaining screws. The panel has a non-volatile memory chip that stores the unique node address (MAC address).

Note   The 5-amp AIP card (73-7665-XX) is required when installing the new fan-tray assembly (15454-FTA3). See the "Install the Fan-Tray Assembly" procedure on page 1-27.

The MAC address identifies the nodes that support circuits. It allows CTC to determine circuit sources, destinations, and spans. The Timing Communication and Control+ (TCC+) cards in the ONS 15454 also read the MAC address to store the node database. If the AIP fails, a MAC Fail alarm displays on the CTC Alarms menu and/or the LCD display on the fan tray will go blank.

Note   A blown fuse on the AIP board can cause the LCD display to go blank.

1.6 EIA Installation

Optional EIA backplane covers are typically pre-installed when ordered with the ONS 15454. EIAs must be ordered when using DS-1, DS-3, DS3XM-6, or EC-1 cards. A minimum amount of assembly may be required when EIAs are ordered separately from the ONS 15454. Four different EIA backplane covers are available for the ONS 15454: BNC, High-Density BNC, SMB, and AMP Champ. This section describes each EIA in detail.

EIAs are attached to the shelf assembly backplane to provide coaxial cable connections. EIAs are available with SMB and BNC connectors for DS-3 or EC-1 cards. EIAs are available with AMP Champ connectors for DS-1 cards. You must use SMB EIAs for DS-1 twisted-pair cable installation. You can install EIAs on one or both sides of the ONS 15454 backplane in any combination (in other words, AMP Champ on Side A and BNC on Side B or High-Density BNC on side A and SMB on side B, and so forth).

If you are installing EIAs after the shelf assembly is installed, plug the EIA into the backplane. The EIA has six electrical connectors that plug into six corresponding backplane connectors. The EIA backplane must replace the standard sheet metal cover to provide access to the coaxial cable connectors. The EIA sheet metal covers use the same screw holes as the solid backplane panels, but they have 12 additional 6-32 x 1/2 inch phillips screw holes so you can screw down the cover and the board using standoffs on the EIA board. This section describes each EIA and provides installation procedures.

For EIA replacement procedures, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*. For information about attaching ferrites to EIA connectors, see the "Ferrite Installation" section on page 1-61.

1.6.1 BNC EIA

The ONS 15454 BNC EIA supports 24 DS-3 circuits on each side of the ONS 15454 (24 transmit and 24 receive connectors). If you install BNC EIAs on both sides of the shelf assembly, the ONS 15454 hosts up to 48 circuits. The BNC connectors on the EIA supports Trompeter UCBJ224 (75 Ohm) 4 leg connectors (King or ITT are also compatible). You can use BNC EIAs for DS-3 (including the DS3XM-6) or EC-1 cards. Figure 1-39 shows the ONS 15454 with pre-installed BNC EIAs.

To install coaxial cable with BNC connectors, see the "BNC Connector Installation" section on page 1-36.

Figure 1-12   A BNC backplane for use in 1:1 protection schemes
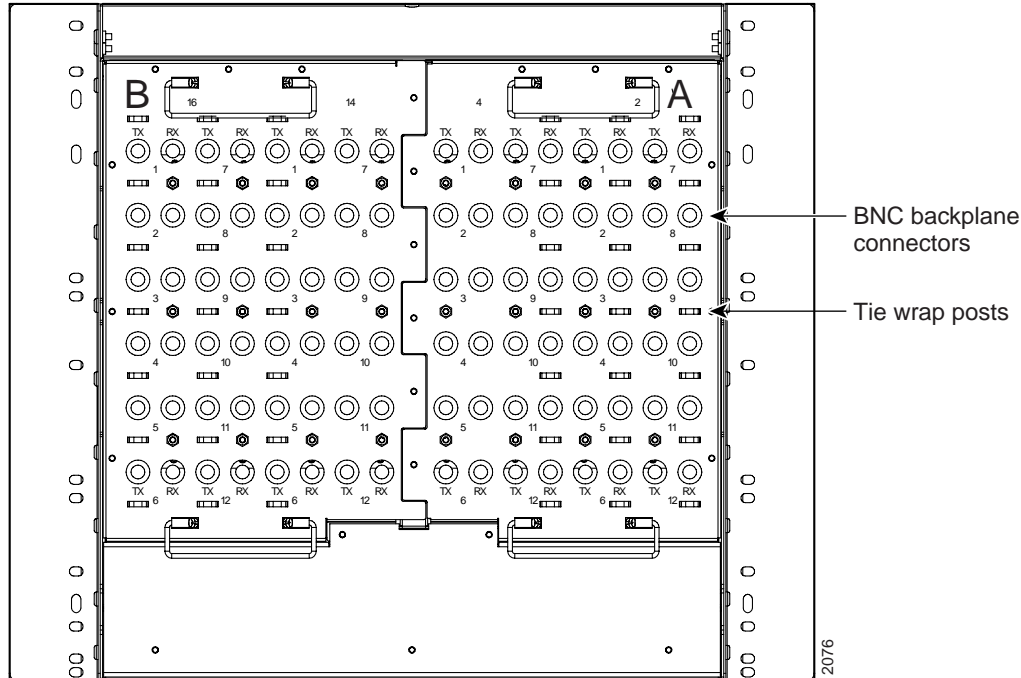
The EIA side marked "A" has 24 pairs of BNC connectors. The first 12 pairs of BNC connectors correspond to Ports 1 – 12 for a 12-port card and map to Slot 2 on the shelf assembly. The BNC connector pairs are marked "Tx" and "Rx" to indicate transmit and receive cables for each port. You can install an additional card in Slot 1 as a protect card for the card in Slot 2. The second 12 BNC connector pairs correspond to Ports 1 – 12 for a 12-port card and map to Slot 4 on the shelf assembly. You can install an additional card in Slot 3 as a protect card for the card in Slot 4. Slots 5 and 6 do not support DS-3 cards when BNC connectors are used.

The EIA side marked "B" provides an additional 24 pairs of BNC connectors. The first 12 BNC connector pairs correspond to Ports 1 – 12 for a 12-port card and map to Slot 14 on the shelf assembly. The BNC connector pairs are marked "Tx" and "Rx" to indicate transmit and receive cables for each port. You can install an additional card in Slot 15 as a protect card for the card in Slot 14. The second 12 BNC connector pairs correspond to Ports 1 – 12 for a 12-port card and map to Slot 16 on the shelf assembly. You can install an additional card in Slot 17 as a protect card for the card in Slot 16. Slots 12 and 13 do not support DS-3 cards when BNC connectors are used.

When BNC connectors are used with a DS3N-12 card in Slot 3 or 15, the 1:N card protection extends only to the two slots adjacent to the 1:N card due to BNC wiring constraints.

1.6.2 High-Density BNC EIA

The ONS 15454 High-Density BNC EIA supports 48 DS-3 circuits on each side of the ONS 15454 (48 transmit and 48 receive connectors). If you install BNC EIAs on both sides of the unit, the ONS 15454 hosts up to 96 circuits. The High-Density BNC EIA supports Trompeter UCBJ224 (75 Ohm) 4 leg connectors (King or ITT are also compatible). You can use High-Density BNC EIAs for DS-3 (including the DS3XM-6) or EC-1 cards. Figure 1-13 shows the ONS 15454 with pre-installed High-Density BNC EIAs.

To install coaxial cable with High-Density BNC connectors, see the "High-Density BNC Connector Installation" section on page 1-37.

Figure 1-13   A High-Density BNC backplane for use in 1:N protection schemes
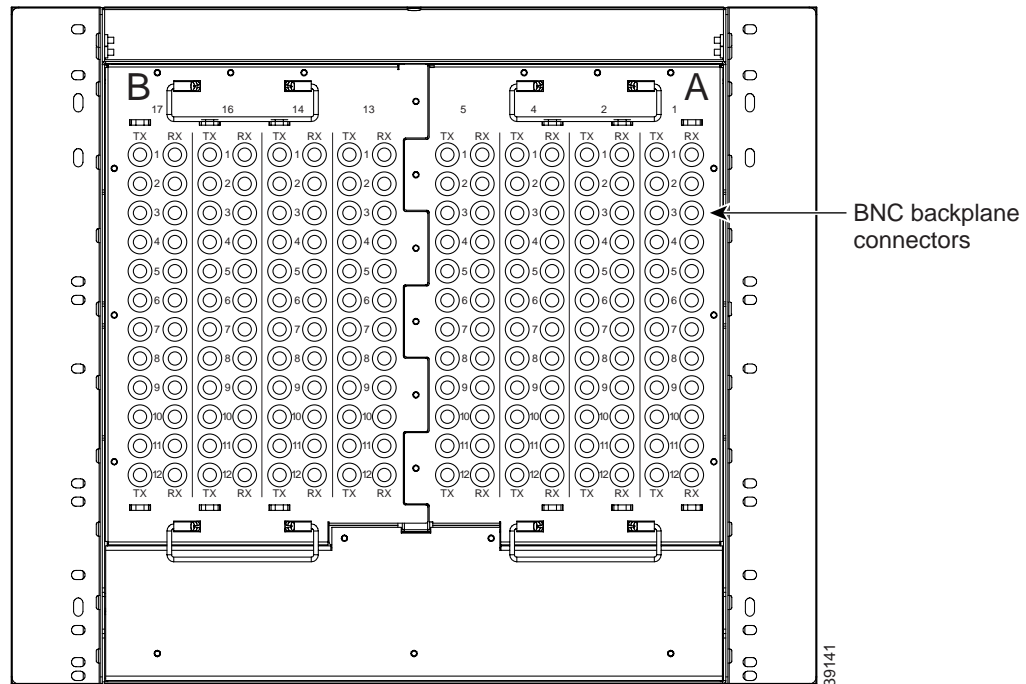
The EIA side marked "A" hosts 48 pairs of BNC connectors. Each column of connector pairs is numbered and corresponds to the slot of the same number. The first column (12 pairs) of BNC connectors corresponds to Slot 1 on the shelf assembly, the second column to Slot 2, the third column to Slot 4, and the fourth column to Slot 5. The rows of connectors correspond to Ports 1 – 12 of a 12-port card.

The EIA side marked "B" provides an additional 48 pairs of BNC connectors. The first column (12 pairs) of BNC connectors corresponds to Slot 13 on the shelf assembly, the second column to Slot 14, the third column to Slot 16, and the fourth column to Slot 17. The rows of connectors correspond to Ports 1 – 12 of a 12-port card. The BNC connector pairs are marked "Tx" and "Rx" to indicate transmit and receive cables for each port. The High-Density BNC EIA supports both 1:1 and 1:N protection across all slots.

1.6.3 SMB EIA

The ONS 15454 SMB EIA supports AMP 415484-1 75 Ohm 4 leg connectors. You can use SMB EIAs with DS-1, DS-3 (including the DS3XM-6), and EC-1 cards. If you use DS-1 cards, use the DS-1 electrical interface adapter to terminate the twisted pair DS-1 cable from the backplane.
Figure 1-14 shows the ONS 15454 with pre-installed SMB EIAs and the sheet metal cover and screw locations for the EIA.

To install SMB connectors, see the "SMB Connector Installation" section on page 1-38.

Figure 1-14   An SMB EIA backplane
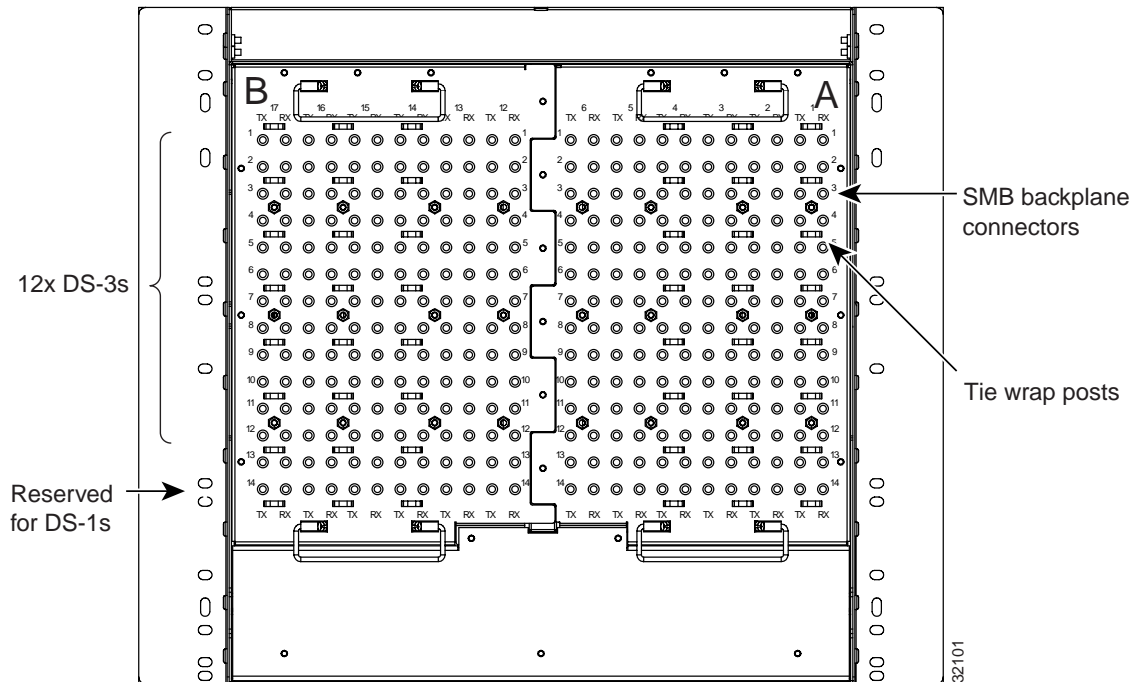
The SMB EIA has 84 transmit and 84 receive connectors on each side of the ONS 15454 for a total of 168 SMB connectors (84 circuits).

The EIA side marked "A" hosts 84 SMB connectors in six columns of 14 connectors. The "A" side columns are numbered 1 – 6 and correspond to Slots 1 – 6 on the shelf assembly. The EIA side marked "B" hosts an additional 84 SMB connectors in six columns of 14 connectors. The "B" side columns are numbered 12 – 17 and correspond to Slots 12 – 17 on the shelf assembly. The connector rows are numbered 1 – 14 and correspond to the 14 ports on a DS-1 card.

For DS-3 or EC-1, the EIA supports 72 transmit and 72 receive connectors, for a total of 144 SMB connectors (72 circuits). If you use a DS-3 or EC-1 card, only Ports 1 – 12 are active. If you use a DS3XM-6 card, only Ports 1 – 6 are active. The SMB connector pairs are marked "Tx" and "Rx" to identify transmit and receive cables for each port. If you use SMB connectors, you can install DS-1, DS-3, or EC-1 cards in any multispeed slot.

1.6.4 AMP Champ EIA

The ONS 15454 AMP Champ EIA supports 64-pin (32 pair) AMP Champ connectors for each slot on both sides of the shelf assembly where the EIA is installed. Cisco AMP Champ connectors are female AMP # 552246-1 with AMP # 552562-2 bail locks. Each AMP Champ connector supports 14 DS-1 ports. You can use AMP Champ EIAs with DS-1 cards only. Figure 1-15 shows the ONS 15454 with pre-installed AMP Champ EIAs and the corresponding sheet metal cover and screw locations for the EIA.

To install AMP Champ connector DS-1 cables, see the "AMP Champ Connector Installation" section on page 1-41.

For information about attaching ferrites to AMP Champ connectors, see the "Ferrite Installation" section on page 1-61.

For information about AMP champ cable management, see the "AMP Champ Cable Management" section on page 1-59.

Figure 1-15   An AMP EIA Champ backplane
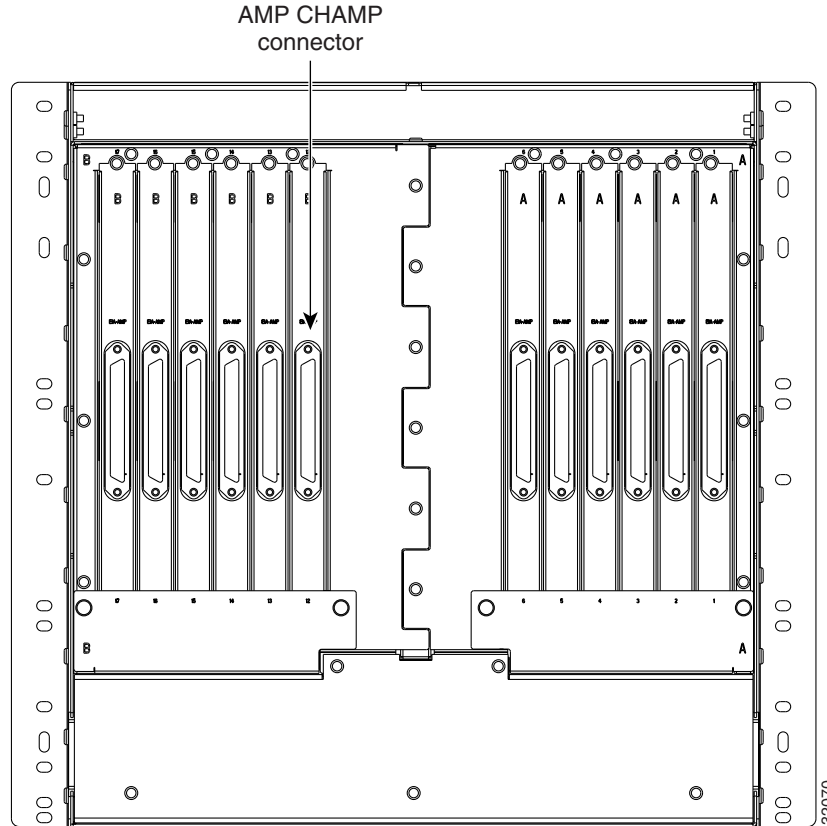
The EIA side marked "A" hosts six AMP Champ connectors. The connectors are numbered 1 – 6 for the corresponding slots on the shelf assembly. Each AMP Champ connector on the backplane supports 14 DS-1 ports for a DS1-14 card, and each connector features 28 live pairs—one transmit pair and one receive pair—for each DS-1 port.

The EIA side marked "B" hosts six AMP Champ connectors. The connectors are labeled 12–17 for the corresponding slots on the shelf assembly. Each AMP Champ connector on the backplane supports 14 DS-1 ports for a DS1-14 card, and each connector features 28 live pairs—one transmit pair and one receive pair—for each DS-1 port.

Note   EIAs are hot-swappable. You do not need to disconnect power to install or remove EIAs.

Caution   Always use an electrostatic discharge (ESD) wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Cisco ONS 15454 Installation and Operations Guide

Procedure: Install a BNC, High-Density BNC, or SMB EIA

See the "Install the AMP Champ EIA" procedure on page 1-24 if you are using an AMP Champ EIA.

Step 1   To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

Step 2   Remove the EIA 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 3   Place the metal EIA cover panel over the card.

Step 4   Insert and tighten the nine perimeter screws (P/N 48-0358) at 8-10 lbs to secure the cover panel to the backplane.

Step 5   Insert and tighten the twelve (BNC and SMB) or nine (High-Density BNC) inner screws (P/N 48-0004) at 8-10 lbs to secure the cover panel to the card and backplane.

Step 6   Replace the lower backplane cover, and insert and tighten the five screws to secure it.

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 1-16 shows a BNC EIA installation. Figure 1-17 shows High-Density BNC EIA installation. Figure 1-18 shows an SMB EIA installation.

Figure 1-16   Installing the BNC EIA
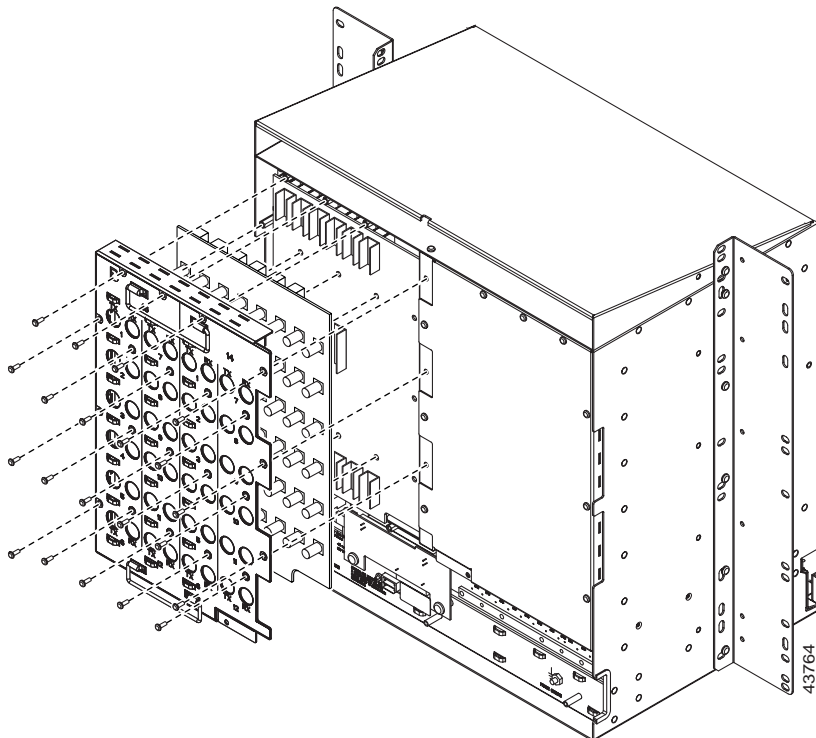
Figure 1-17   Installing the High-Density BNC EIA
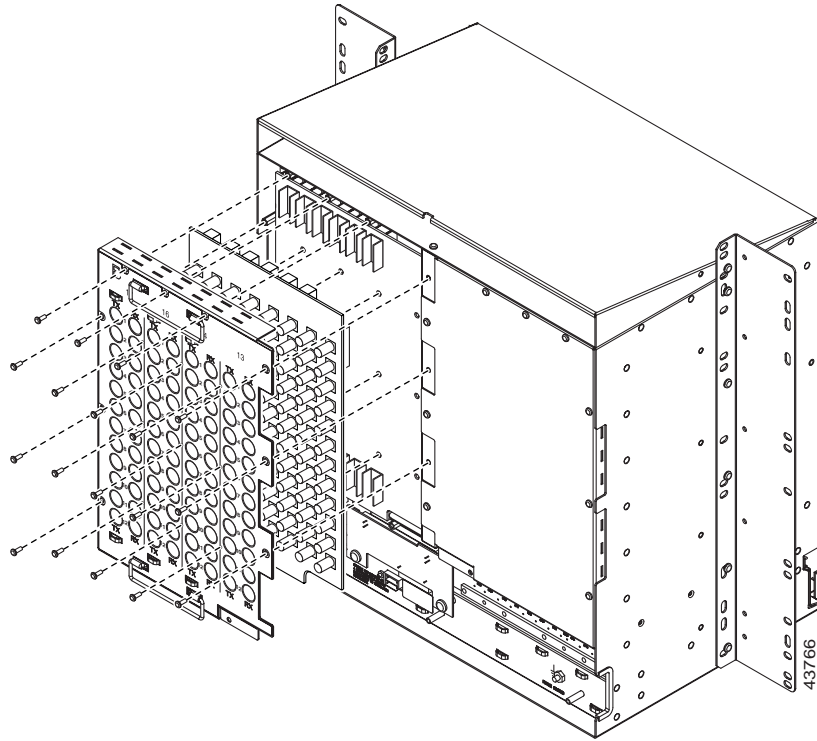
Figure 1-18   Installing the SMB EIA (use a balun for DS-1 connections)
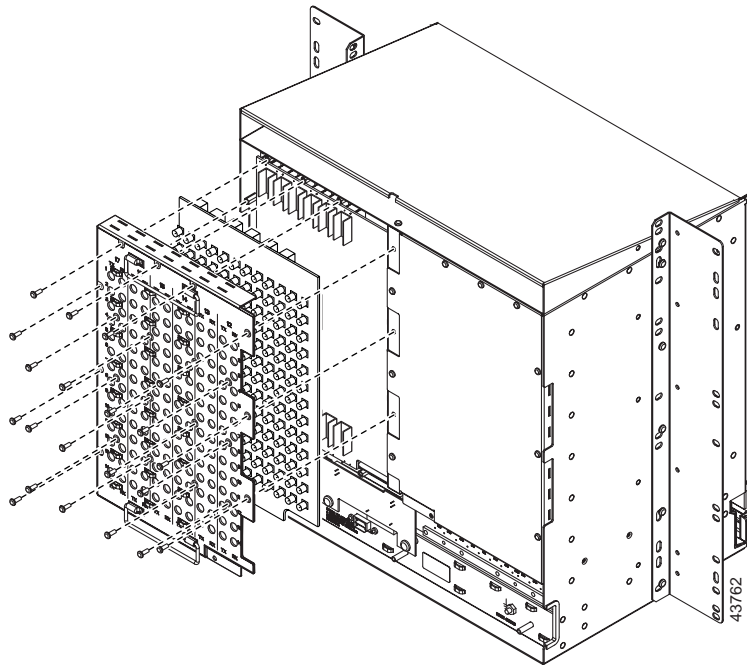
Procedure: Install the AMP Champ EIA

Step 1   To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

Step 2   Align the AMP Champ cover panel with the backplane and insert and tighten the nine perimeter screws (P/N 48-0358) at 8-10 lbs.

Step 3   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 4   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 8-10 lbs.

Step 5   Place the AMP Champ fastening plate along the bottom of the cover panel, and hand tighten the two thumbscrews.

Figure 1-19 shows an AMP Champ EIA installation.

Figure 1-19   Installing the AMP CHAMP EIA
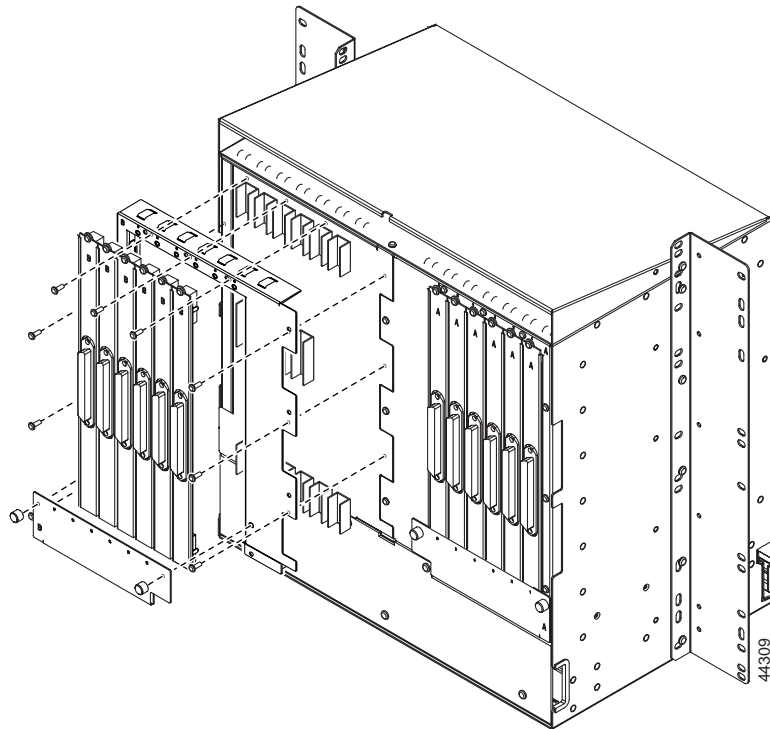
1.7 Fan-Tray Assembly Installation

The fan-tray assembly is located at the bottom of the ONS 15454 front compartment. The fan tray is a removable drawer that holds fans and fan-control circuitry for the ONS 15454. The front door can be left in place when removing or installing the fan tray but removal is recommended. After you install the fan tray, you should only need to access it if a fan failure occurs or you need to replace or clean the fan-tray air filter.

The front of the fan-tray assembly has an LCD screen that provides slot and port-level information for all ONS 15454 card slots, including the number of Critical, Major, and Minor alarms.

The fan-tray assembly features an air filter at the bottom of the tray that you can install and remove by hand. Remove and visually inspect this filter every 30 days and keep spare filters in stock. See the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for information about cleaning and maintaining the fan-tray air filter.

Note   The 10-Gbps compatible shelf assembly (15454-SA-ANSI, P/N: 800-19857) and fan-tray assembly (15454-FTA3) are required with the ONS 15454 XC10G, OC-192, and OC-48 any slot (AS) cards.

Caution   Do not operate an ONS 15454 without a fan-tray filter. A fan-tray filter is mandatory.

Caution   The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 Release 3.1 shelf assemblies (15454-SA-ANSI, 800-19857). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 Release 3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N 800-0714915454). Installing the 15454-FTA3 in a non-compliant shelf assembly may result in failure of the alarm interface panel (AIP), which in turn, will result in power loss to the fan-tray assembly.

Note   The ONS 15454 Release 3.1 fan-tray assembly (15454-FTA3) is not I-temp. To obtain an I-temp fan tray, install the 15454-FTA2 fan-tray assembly in an ONS 15454 Release 3.1 shelf assembly (P/N: 800-19857). However, do not install the ONS 15454 Release 3.1 XC10G, OC-192, and OC-48 any slot (AS) cards in the shelf assembly with the 15454-FTA2 fan-tray assembly.

If one or more fans fail on the fan-tray assembly, replace the entire assembly. You cannot replace individual fans. The red Fan Fail LED on the front of the fan tray illuminates when one or more fans fail. For fan tray replacement instructions, see the "Install the Fan-Tray Assembly" procedure on page 1-27. The red Fan Fail LED clears after you install a working fan tray.

Fan speed is controlled by TCC+ card temperature sensors. The sensors measure the input air temperature at the fan-tray assembly. Fan speed options are low, medium, and high. If the TCC+ card fails, the fans automatically shift to high speed. The temperature measured by the TCC+ sensors is displayed on the LCD screen.

Procedure: Install the Bottom Brackets and Air Filter

The shelf assembly ships with bottom brackets that you should use to install the air filter. The bottom brackets consist of two grooved metal pieces that attach to the bottom of the shelf assembly using three screws each. When you use the bottom bracket to install the fan-tray air filter, you do not need to remove the fan-tray assembly to access the air filter. Attach the brackets to the bottom of the shelf assembly before installing the rack.

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.

Note   If you choose not to install the bottom 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.

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

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 provided.

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 face-down during installation).

Figure 1-20 illustrates bottom bracket installation. If you do not use the bottom brackets, in the future you must remove the fan-tray assembly before removing the air filter. The bottom brackets enable you to clean and replace the air filter without removing the fan-tray assembly.

Figure 1-20   Installing the bottom brackets
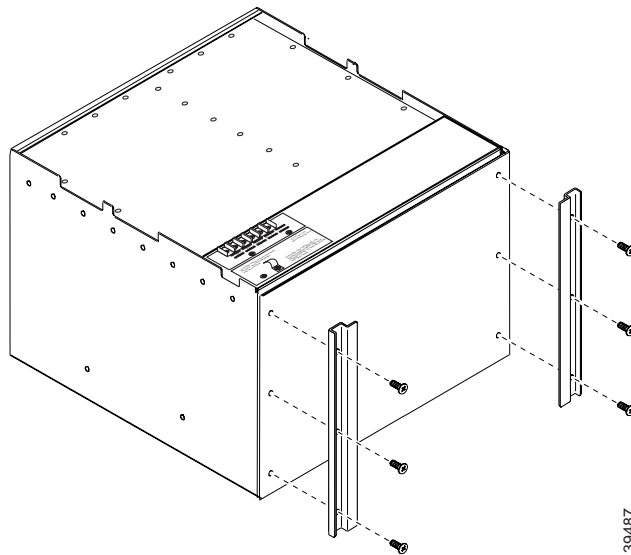
If you are using the bottom brackets to install the fan-tray air filter, you can install three shelf assemblies in a standard seven-foot rack. If you are not using the bottom brackets, you can install four shelf assemblies in a rack.

Step 4   Slide the air filter into the shelf assembly.

Procedure: Install the Fan-Tray Assembly

To install the fan-tray assembly, it is not necessary to move any of the cable-management facilities.

⚠

Caution   You must place the edge of the air filter flush against the front of the fan-tray assembly compartment when installing the fan tray on top of the filter. Failure to do so could result in damage to the filter, the fan tray, or both.

⚠

Caution   Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the back panel of the shelf assembly.

Step 1   Remove the front door of the shelf assembly.

Step 2   Slide the fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 3   To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Figure 1-21 shows the location of the fan tray.

Figure 1-21   Installing the fan-tray assembly

Fan tray
assembly
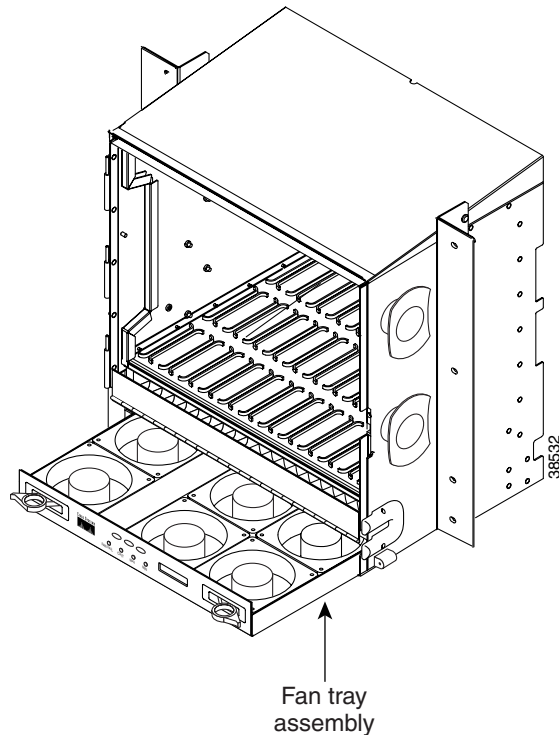
1.8 Power and Ground Installation

This section explains how to connect the ONS 15454 assembly to the power supply. Ground the equipment according to Telcordia standards or local practices.

Warning   **Shut off the power from the power source or turn off the breakers before beginning work.**

Warning   **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

Caution   Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Warning   **Do not mix conductors of dissimilar metals in a terminal or splicing connector where physical contact occurs (such as copper and aluminum, or copper and copper-clad aluminum), unless the device is suited for the purpose and conditions of use.**

Warning   **Connect the ONS 15454 only to a DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950-based safety standards.**

Warning   **The ONS 15454 relies on the protective devices in the building installation to protect against short circuit, overcurrent, and grounding faults. Ensure that the protective devices are properly rated to protect the system, and that they comply with national and local codes.**

Warning   **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.**

Cisco recommends the following wiring conventions, but customer conventions prevail:

- Red wire for battery connections (-48V DC)
- Black wire for battery return connections (0V DC)

The ONS 15454 has redundant -48V DC #8 power terminals on the shelf assembly backplane. The terminals are labeled BAT1, RET1, BAT2, and RET2 and are located on the lower section of the backplane behind a clear plastic cover. See the "Lower Backplane Cover" section on page 1-15 for information about accessing the power terminals.

To install redundant power feeds, use four power cables and one ground cable. For a single power feed, only two power cables (#10 AWG, copper conductor, 194°F [90°C]) and one ground cable (#6 AWG) are required. Use a conductor with low impedance to ensure circuit overcurrent protection. However, the conductor must have the capability to safely conduct any fault current that might be imposed.

The existing ground post is a #10-32 bolt. The nut provided for a field connection is also a #10, with an integral lock washer. The lug must be a dual-hole type and rated to accept the #6 AWG cable. Two posts are provided on the Cisco ONS 15454 to accommodate the dual-hole lug. Figure 1-22 shows the location of the ground posts.

Figure 1-22   Ground posts on the ONS 15454 backplane
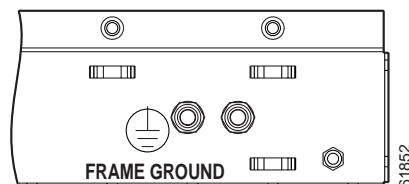
For information about attaching ferrites to power cabling, see the "Ferrite Installation" section on page 1-61.

Warning   **When installing redundant power feeds, do not use aluminum conductors.**

Warning   **If you use redundant power leads to power the ONS 15454, disconnecting one lead will not remove power from the node.**

Procedure: Install Redundant Power Feeds

Ground only one cable to ground the shelf assembly. Terminate the other end of the ground cable to ground according to local site practice. The ONS 15454 backplane also has a ground terminal on the right side of the backplane. Connect a ground terminal for the frame ground (FGND) terminal according to local site practice.

If the system loses power or both TCC+ cards are reset, 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 "Setting Up Basic Node Information" section on page 3-2.

Note   If you encounter problems with the power supply, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for possible causes.

Warning   **Do not apply power to the ONS 15454 until you complete all installation steps and check the continuity of the -48V DC and return.**

Step 1   Measure and cut the cables as needed to reach the ONS 15454 from the fuse panel. Figure 1-23 shows the ONS 15454 power terminals.

Step 2   Dress the power and ground cables according to local site practice.

Warning   **When installing the ONS 15454, the ground connection must always be made first and disconnected last.**

Figure 1-23   Power terminals
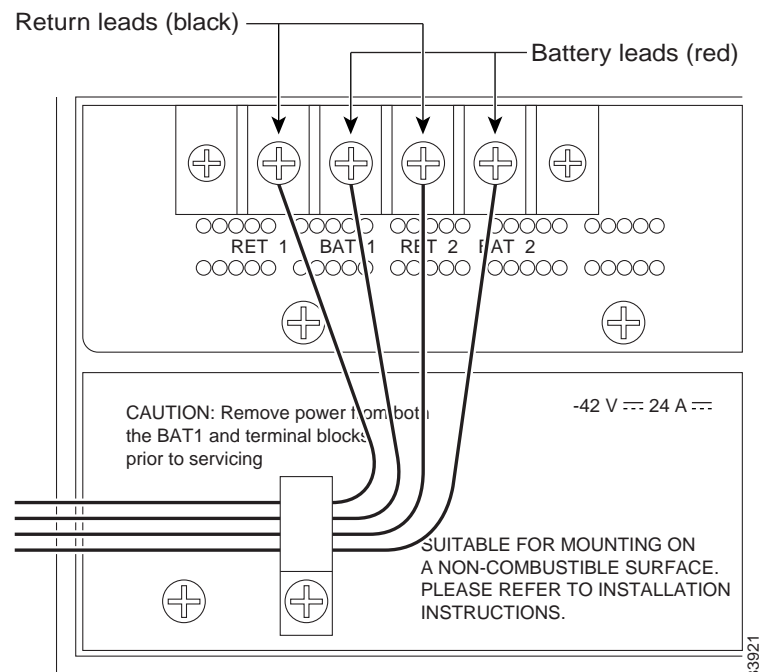
Step 3   Remove or loosen the #8 power terminal screws on the ONS 15454. To avoid confusion, label the cables connected to the BAT1/RET1 power terminals as 1, and the cables connected to the BAT2/RET2 power terminals as 2.

✎
Note   Use only pressure terminal connectors, such as ring and fork 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 4   Strip 1/2 inch of insulation from all power cables that you will use. Crimp the lugs onto the ends of all power leads.

✎
Note   When terminating battery and battery return connections as shown in Figure 1-23, follow a torque specification of 10 in-lbs. When terminating a frame ground, use the kep-nut provided with the ONS 15454 and tighten it to a torque specification of 31 in-lbs. The kep-nut provides a frame ground connection that minimizes the possibility of loosening caused by rotation during installation and maintenance activity. This type of prevention is inherently provided by the terminal block for battery and battery return connections.

Step 5   Terminate the return 1 lead to the RET1 backplane terminal. Use oxidation-prevention grease to keep connections non-corrosive.

⚠
Warning   **Do not secure multiple connectors with the same bolt assembly.**

Step 6   Terminate the negative 1 lead to the negative BAT1 backplane power terminal. Use oxidation prevention grease to keep connections non-corrosive.

Step 7   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 non-corrosive.

Route the cables out below the power terminals using the plastic cable clamp.

1.9 Alarm, Timing, LAN, and Craft Pin Connections

⚠️
Caution   Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

The ONS 15454 has a backplane pin field located at the bottom of the backplane. The backplane pin field provides 0.045 square inch wire-wrap pins for enabling external alarms, timing input and output, and craft interface terminals. This section describes the backplane pin field and the pin assignments for the field. Figure 1-24 shows the wire-wrap pins on the backplane pin field. Beneath each wire-wrap pin is a frame ground pin. Frame ground pins are labeled FG1, FG2, FG3, etc. Install the ground shield of the cables connected to the backplane to the ground pin that corresponds to the pin field used. Figure 1-24 shows pinouts for the ONS 15454.

Figure 1-24   Pinouts
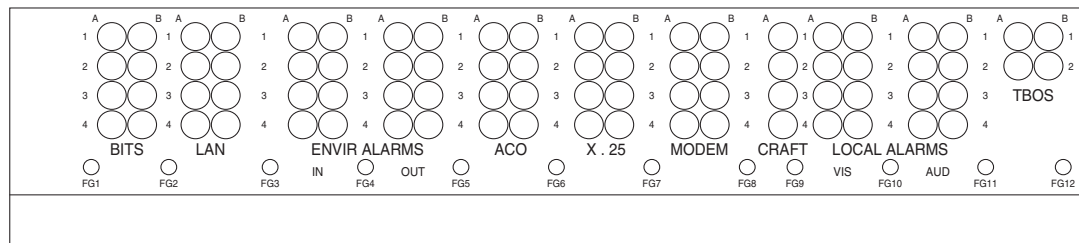
Field	Pin	Function	Field	Pin	Function
BITS	A1	BITS Output 2 negative (-)	ENVIR ALARMS OUT	A1	Normally open output pair number 1
	B1	BITS Output 2 positive (+)		B1	
	A2	BITS Input 2 negative (-)		A2	Normally open output pair number 2
	B2	BITS Input 2 positive (+)	N/O	B2	
	A3	BITS Output 1 negative (-)		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 1		Connecting to a Router, Hub, or Switch	ACO	A1	Normally open ACO pair
	A1	RJ-45 pin 6		B1	
	B1	RJ-45 pin 3	CRAFT	A1	Receive (PC pin #2)
	A2	RJ-45 pin 2		A2	Transmit (PC pin #3)
	B2	RJ-45 pin 1		A3	Ground (PC pin #5)
		Connecting to a PC or Workstation		A4	DTR (PC pin #4)
	A1	RJ-45 pin 2	LOCAL ALARMS AUD (Audible)	A1	Alarm output pair number 1: Remote audible alarm.
	B1	RJ-45 pin 1		B1	
	A2	RJ-45 pin 6		A2	Alarm output pair number 2: Critical audible alarm.
	B2	RJ-45 pin 3		B2	
LAN 2		Not Used	N/O	A3	Alarm output pair number 3: Major audible alarm.
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.		B3	
	B1			A4	Alarm output pair number 4: Minor audible alarm.
	A2	Alarm input pair number 2: Reports closure on connected wires.		B4	
	B2		LOCAL ALARMS VIS (Visual)	A1	Alarm output pair number 1: Remote visual alarm.
	A3	Alarm input pair number 3: Reports closure on connected wires.		B1	
	B3			A2	Alarm output pair number 2: Critical visual alarm.
	A4	Alarm input pair number 4: Reports closure on connected wires.	N/O	B2	
	B4			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.

1.9.1 Alarm Installation

The alarm pin field supports up to 17 alarm contacts, including four audible alarms, four visual alarms, one alarm cutoff (ACO), and four user-definable alarm input and output contacts.

Audible alarm contacts are in the LOCAL ALARM AUD pin field and visual contacts are in the LOCAL ALARM VIS pin field. Both of these alarms are in the LOCAL ALARMS category. User-definable contacts are in the ENVIR ALARM IN and ENVIR ALARM OUT pin fields. These alarms are in the ENVIR ALARMS category; you must have the AIC card installed to use the ENVIR ALARMS. Alarm contacts are Normally Open (N/O), meaning that the system closes the alarm contacts when the corresponding alarm conditions are present. Each alarm contact consists of two wire-wrap pins on the shelf assembly backplane. Visual and audible alarm contacts are classified as Critical, Major, Minor, and Remote. Figure 1-24 shows alarm pin assignments.

Visual and audible alarms are typically wired to trigger an alarm light at a central alarm collection point when the corresponding contacts are closed. You can use the Alarm Cutoff pins to activate a remote ACO for audible alarms. You can also activate the ACO function by pressing the ACO button on the TCC+ card faceplate. The ACO function clears all audible alarm indications. After clearing the audible alarm indication, the alarm is still present and viewable in the Alarms tab in CTC.

Procedure: Install Alarm Wires on the Backplane

Step 1 Use #22 or #24 AWG alarm wires.

Step 2 Wrap the alarm wires on the appropriate wire-wrap pins according to local site practice.

> **Note** For information about attaching ferrites to wire-wrap pin fields, see the "Ferrite Installation" section on page 1-61.

1.9.2 Timing Installation

The ONS 15454 backplane supports two Building Integrated Timing Supply (BITS) clock pin fields. The first four BITS pins, rows 3 and 4, support output and input from the first external timing device. The last four BITS pins, rows 1 and 2, perform the identical functions for the second external timing device. Table 1-2 lists the pin assignments for the BITS timing pin fields.

Table 1-2   External Timing Pin Assignments for BITS

External Device	Contact	Tip & Ring	Function
First external device	A3 (BITS 1 Out)	Primary ring (-)	Output to external device
	B3 (BITS 1 Out)	Primary tip (+)	Output to external device
	A4 (BITS 1 In)	Secondary ring (-)	Input from external device
	B4 (BITS 1 In)	Secondary tip (+)	Input from external device
Second external device	A1 (BITS 2 Out)	Primary ring (-)	Output to external device
	B1 (BITS 2 Out)	Primary tip (+)	Output to external device
	A2 (BITS 2 In)	Secondary ring (-)	Input from external device
	B2 (BITS 2 In	Secondary tip (+)	Input from external device

Note   Refer to Telcordia SR-NWT-002224 for rules about provisioning timing references

Procedure: Install Timing Wires on the Backplane

Step 1   Use #22 or #24 AWG wire.

Step 2   Wrap the clock wires on the appropriate wire-wrap pins according to local site practice.

Step 3   The BITS pin field (FG1) has a frame ground pin beneath it. Wrap the ground shield of the alarm cable to the frame ground pin.

Note   For more detailed information about timing, see the "Setting Up ONS 15454 Timing" section on page 3-12.

1.9.3 LAN Installation

Use the LAN pins on the ONS 15454 backplane to connect the ONS 15454 to a workstation or Ethernet LAN, or to a LAN modem for remote access to the node. You can also use the LAN port on the TCC+ faceplate to connect a workstation or to connect the ONS 15454 to the network. Table 1-3 shows the LAN pin assignments.

Before you can connect an ONS 15454 to other ONS 15454s or to a LAN, you must change the default IP address that is shipped with each ONS 15454 (192.1.0.2). See the "Change IP Address, Default Router, and Network Mask Using the LCD" procedure on page 3-4.

Table 1-3   LAN Pin Assignments

Pin Field	Backplane Pins	RJ-45 Pins
LAN 1 Connecting to data circuit-terminating equipment (DCE*) (a hub or switch)	B2	1
	A2	2
	B1	3
	A1	6
LAN 1 Connecting to data terminal equipment (DTE) (a PC/workstation or router)	B1	1
	A1	2
	B2	3
	A2	6

*The Cisco ONS 15454 is DCE.

Procedure: Install LAN Wires on the Backplane

Step 1   Use #22 or #24 AWG wire.

Step 2   Wrap the wires on the appropriate wire-wrap pins according to local site practice.

Step 3   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.

1.9.4 TL1 Craft Interface Installation

You can use the craft pins on the ONS 15454 backplane or the RS-232 port on the TCC+ faceplate to create a VT100 emulation window to serve as a TL1 craft interface to the ONS 15454. Use a straight-through cable to connect to the RS-232 port. Table 1-4 shows the pin assignments for the CRAFT pin field.

Note   You cannot use the craft backplane pins and the RS-232 port on the TCC+ card simultaneously.

Table 1-4   Craft Interface Pin Assignments

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

Procedure: Install Craft Interface Wires on the Backplane

Step 1   Use #22 or #24 AWG wire.

Step 2   Wrap the craft interface wires on the appropriate wire-wrap pins according to local site practice.

> ✎
>
> **Note**   For information about attaching ferrites to wire-wrap pin fields, see the "Ferrite Installation" section on page 1-61.

Step 3   Wrap the ground shield of the craft interface cable to the frame-ground pin.

Step 4   Wrap the ground wire of your computer cable to pin A3 on the craft pin field.

1.10 Coaxial Cable Installation

> ⚠
>
> **Caution**   Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

When using ONS 15454 DS-3 electrical cables, the cables must terminate on an EIA installed on the ONS 15454 backplane. EIAs are available with SMB and BNC connectors. All DS-3 cables connected to the ONS 15454 DS-3 card must terminate with coaxial cables using the desired connector type to connect to the specified EIA. For information about physically installing an EIA in the field, see the "Install a BNC, High-Density BNC, or SMB EIA" procedure on page 1-22. For information about coaxial cable management, see the "Coaxial Cable Management" section on page 1-57.

The electromagnetic compatibility (EMC) performance of the system depends on good-quality DS-3 coaxial cables, such as Shuner Type G 03233 D, or the equivalent.

1.10.1 BNC Connector Installation

For a description of BNC EIAs, see the "BNC EIA" section on page 1-17. The BNC connectors on the EIA supports Trompeter UCBJ224 (75 Ohm) 4 leg connectors. Right-angle mating connectors for the connecting cable are AMP 413588-2 (75 Ohm) connectors. If preferred, you can also use a straight connector of the same type. Use RG-59/U cable to connect to the ONS 15454 BNC EIA. These cables are recommended to connect to a patch panel and are designed for long runs of up to 450 feet.

Procedure: Install Coaxial Cable With BNC Connectors

Step 1   Place the BNC cable connector over the desired connection point on the backplane.

Figure 1-25 shows how to connect a coaxial cable to the BNC EIA using a right-angle BNC cable connector.

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 until the notch clicks 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.

Figure 1-25   Using a right-angle connector to install coaxial cable with BNC connectors
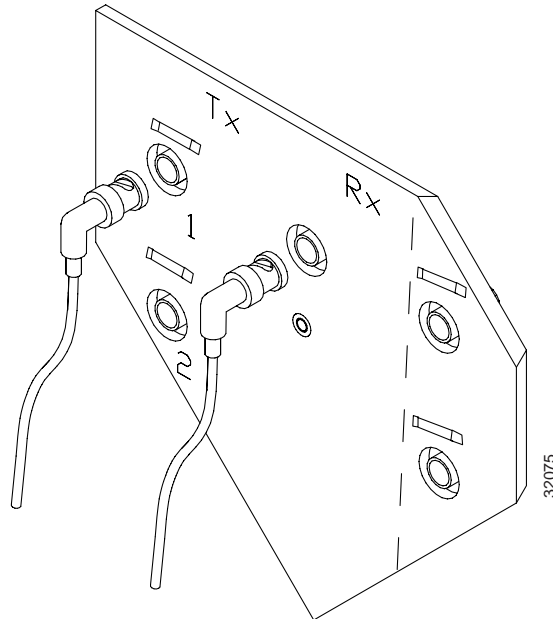
Note   Slots 1, 3, 15 and 17 are designated protection slots when BNC connectors are used. Slots 5, 6, 11, and 12 do not support DS3-12 cards when BNC connectors are used. A total of four DS3-12 cards can be used to carry traffic with BNC connectors.

Step 7   Label all cables at each end of the connection to avoid confusion with cables that are similar in appearance.

1.10.2 High-Density BNC Connector Installation

The High-Density BNC EIA supports Trompeter UCBJ224 (75 Ohm) 4 leg connectors. Use straight connectors on RG-59/U cable to connect to the High-Density BNC EIA. Cisco recommends these cables for connection to a patch panel; they are designed for long runs of up to 450 feet. For more detail, see the "High-Density BNC EIA" section on page 1-18.

Although not required, Cisco strongly recommends using the BNC insertion tool to connect cables to the EIA. Refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for more information about the insertion tool.

Procedure: Install Coaxial Cable With High-Density BNC Connectors

Step 1 Place the BNC cable connector over the desired connection point on the backplane.

Step 2 Using the insertions 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 until the notch clicks 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.

1.10.3 SMB Connector Installation

The SMB backplane cover is similar to the BNC cover. For further detail, see the "SMB EIA" section on page 1-19. The SMB connectors on the EIA are AMP 415504-3 (75 Ohm) 4 leg connectors. Right-angle mating connectors for the connecting cable are AMP 415484-2 (75 Ohm) connectors. Use RG-179/U cable to connect to the ONS 15454 EIA. Cisco recommends these cables for connection to a patch panel; they are not designed for long runs (over 50 feet). Range does not affect loopback testing.

For information about attaching ferrites to SMB/BNC connectors, see the "Ferrite Installation" section on page 1-61.

Procedure: Install Coaxial Cable with SMB Connectors

Refer to Figure 1-26 when performing the following steps.

Step 1 Place the SMB cable connector over the desired connection point on the backplane.

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.

Figure 1-26   Installing coaxial cable with SMB connectors
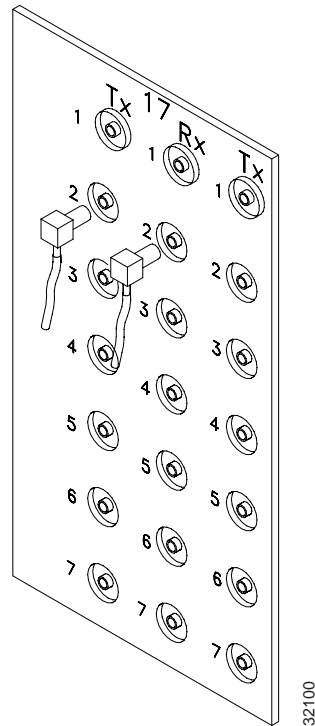
Warning   **Metallic interfaces for connection to outside plant lines (such as T1/E1/T3/E3, etc.) must be connected through a registered or approved device such as CSU/DSU or NT1.**

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.

1.11 DS-1 Cable Installation

DS-1s support both twisted pair wire-wrap cabling and AMP Champ connector cabling. Install the proper backplane EIA on the ONS 15454 for each cabling option. This section provides information about the DS-1 EIA options.

For information about DS-1 cable management, see the "DS-1 Twisted-Pair Cable Management" section on page 1-58.

1.11.1 Twisted Pair Wire-Wrap Installation

Installing twisted-pair, wire-wrap DS-1 cables requires separate pairs of grounded twisted-pair cables for receive (in) and transmit (out). Prepare four cables, two for receive and two for transmit, for each DS-1 facility to be installed.

⚠

Caution   Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

If you use DS-1 electrical twisted-pair cables, equip the ONS 15454 with an SMB EIA on each side of the backplane where DS-1 cables will terminate. You must install special DS-1 electrical interface adapters, commonly referred to as a balun, on every transmit and receive connector for each DS-1 termination.

✎

Note   DS-1 electrical interface adapters project an additional 1.72 inches from the ONS 15454 backplane.

If you install DS-1 cards in the ONS 15454, you must fit the corresponding transmit and receive SMB connectors on the EIA with a DS-1 electrical interface adapter. You can install the adapter on the SMB connector for the port. The adaptor has wire-wrap posts for DS-1 transmit and receive cables. Figure 1-27 shows the DS-1 electrical interface adapter.

Figure 1-27   DS-1 electrical interface adapter (balun)
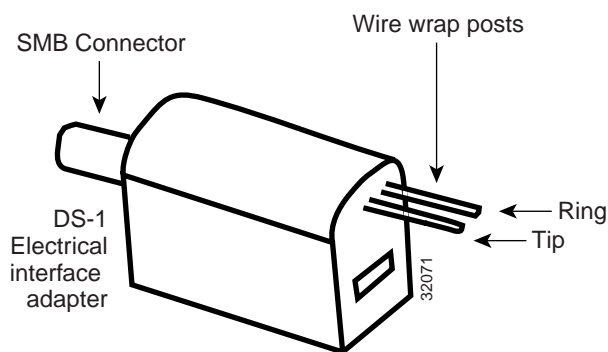
Each DS-1 electrical interface adapter has a female SMB connector on one end and a pair of .045 inch square wire-wrap posts on the other end. The wire-wrap posts are .200 inches apart.

Procedure: Install DS-1 Cables Using Electrical Interface Adapters (Balun)

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 beyond the SMB EIA.

Step 1   Attach the SMB connector on the 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.

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 1-28 shows a ONS 15454 backplane with an SMB EIA with DS-1 electrical interface adapters attached on both sides of the shelf assembly to create DS-1 twisted-pair termination points.

Figure 1-28   A backplane with SMB EIA for DS-1 cables
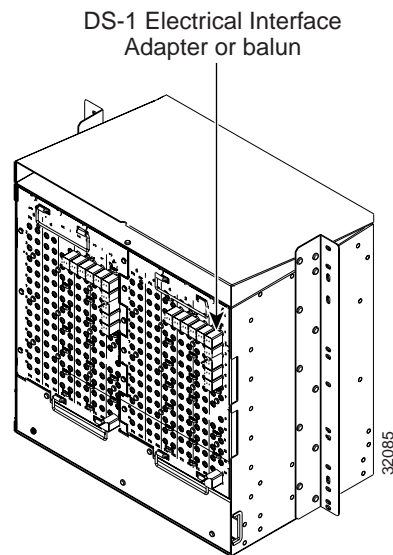
1.11.2 AMP Champ Connector Installation

To install AMP Champ connector DS-1 cables, you must use 64-pin bundled cable connectors with a 64-pin male AMP Champ connector. You need an AMP Champ connector #552276-1 for the receptacle side and #1-552496-1 (for cable diameter .475in.–.540in) or #2-552496-1 (for cable diameter .540in.–.605in.) for the right-angle shell housing (or their functional equivalent). The corresponding 64-pin female AMP Champ connector on the AMP Champ EIA supports one receive and one transmit for each DS-1 port for the corresponding card slot.

Because each DS1-14 card supports 14 DS-1 ports, only 56 pins (28 pairs) of the 64-pin connector are used. Prepare one 56-wire cable for each DS-1 facility installed. Table 1-5 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA. See the "AMP Champ EIA" section on page 1-20 for more information about the AMP Champ EIA.

Table 1-5   Pin Assignments for AMP Champ Connectors (Shaded Area Corresponds to White/Orange Binder Group)

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

Table 1-5   Pin Assignments for AMP Champ Connectors (Shaded Area Corresponds to White/Orange Binder Group) (continued)

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
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 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+ N/A	15	47	Tx Spare0- N/A	Rx Spare0+ N/A	31	63	Rx Spare0- N/A
Tx Spare1+ N/A	16	48	Tx Spare1- N/A	Rx Spare1+ N/A	32	64	Rx Spare1- N/A

Table 1-6 shows the pin assignments for the AMP Champ connectors on the ONS 15454 AMP Champ EIA for a shielded DS1 cable.

Table 1-6   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

Table 1-6   Pin Assignments for AMP Champ Connectors (shielded DS1 cable) (continued)

64-Pin Blue Bundle				64-Pin Orange Bundle			
Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
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

Caution   Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

When using DS-1 AMP Champ cables, you must equip the ONS 15454 with an AMP Champ connector EIA on each side of the backplane where DS-1 cables will terminate. Each AMP Champ connector on the EIA corresponds to a slot in the shelf assembly and is numbered accordingly. The AMP Champ connectors have screw-down tooling at each end of the connector. To install an AMP Champ backplane cover, see the "AMP Champ EIA" section on page 1-20.

Procedure: Install DS-1 AMP Champ Cables on the AMP Champ EIA

Step 1   Prepare a 56-wire cable for each DS-1 card you will install in the shelf assembly. See Table 1-5 on page 1-41 for the ONS 15454 AMP Champ connector pin assignments.

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.

Note To install optical cable, you must first install optical cards.

1.12 Card Installation

This section describes the how to install ONS 15454 cards. The procedure for installing ONS 15454 cards is nearly identical for each card. AIC card installation is slightly different from all other cards and is described in its own procedure. The XC/XCVT /XC10G and TCC+ installation procedures are virtually identical and are described in one procedure. Installation for all other cards is the same and is covered by one procedure.

The order in which you install cards is important. The proper sequence follows:

1. TCC+ cards
2. XC/XCVT/XC10G cards
3. Optical cards
4. Electrical cards
5. Ethernet cards
6. AIC card

Note Because all other cards boot from the active TCC+ card which houses the ONS 15454 software, you must install the TCC+ card before booting any other cards. See Chapter 2, "Software Installation" for information about the TCC+ card and software versions.

Note Before installing cards, verify that the power is turned on.

ONS 15454 cards have electrical plugs at the back that plug into electrical connectors on the shelf assembly backplane. When the ejectors are fully closed, the card plugs into the assembly backplane. Figure 1-29 shows card installation.

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Warning **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

⚠️

Warning   **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

⚠️

Warning   **The laser is active when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

Figure 1-29   Installing cards in the ONS 15454

Ejector   Guide rail
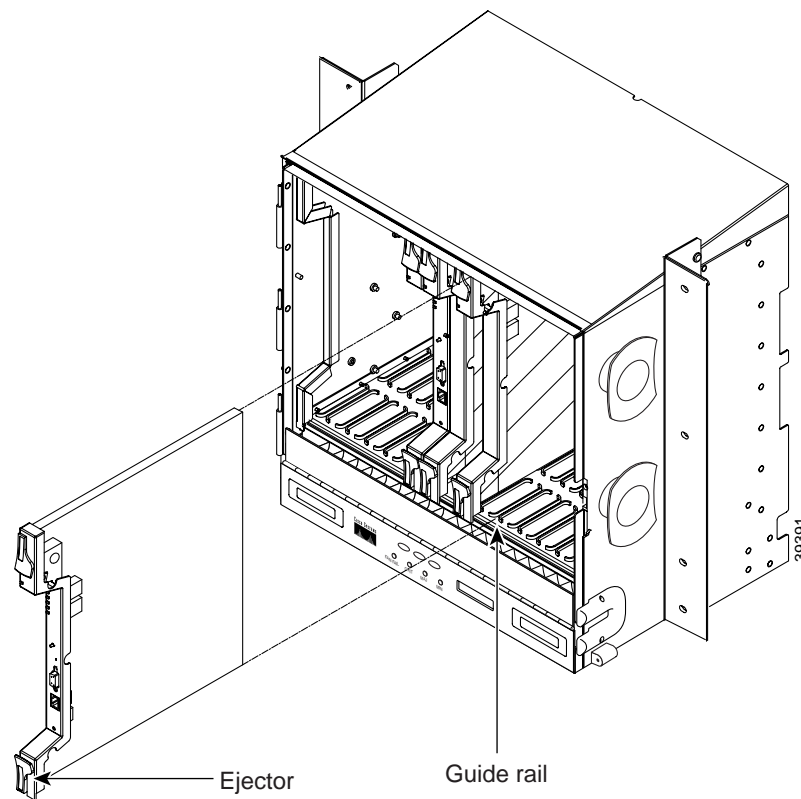
1.12.1 Slot Requirements

The ONS 15454 shelf assembly has 17 card slots numbered sequentially from left to right. Slots 1 – 4 and 14 – 17 are multispeed slots. They can host any ONS 15454 card, except the OC48IR 1310, OC48LR 1550, OC48ELR 1550, and OC192LR 1550 cards. Slots 5, 6, 12 and 13 are high-speed slots. They can host any ONS 15454 card, including the OC48IR 1310, OC48LR 1550, OC48ELR 1550, and OC192LR 1550 cards. You can install the OC48 IR/STM16 SH AS 1310 and the OC48 LR/STM16 LH AS 1550 cards in any multispeed or high-speed card slot.

Cisco ONS 15454 Installation and Operations Guide

Slots 7 and 11 are dedicated to TCC+ cards. Slots 8 and 10 are dedicated to cross-connect (XC, XCVT, XC10G) cards. Slot 9 is reserved for the optional Alarm Interface Controller (AIC) card. Slots 3 and 15 can also host DS1N-14 and DS3N-12 cards that are used in 1:N protection.

Caution   Do not operate the ONS 15454 with a single TCC+ card or a single XC/XCVT/XC10G card installed. Always operate the shelf assembly with one working and one protect card of the same type.

Shelf assembly slots have symbols indicating the type of cards that you can install in them. Each ONS 15454 card has a corresponding symbol. The symbol on the card must match the symbol on the slot.

Table 1-7 shows the slot and card symbol definitions.

Table 1-7   Slot and Card Symbols

Symbol	Color/Shape	Definition
●	Orange/Circle	Multispeed slot (all traffic cards except the OC48IR 1310, OC48LR 1550, and OC192 LR 1550 cards). Only install ONS 15454 cards with a circle symbol on the faceplate.
▲	Blue/Triangle	High-speed slot (all traffic cards including the OC48IR 1310, OC48LR 1550, and OC192LR 1550 cards). Only install ONS 15454 cards with circle or a triangle symbol on the faceplate.
■	Purple/Square	TCC+ slot. Only install ONS 15454 cards with a square symbol on the faceplate.
✚	Green/Cross	Cross-connect (XC/XCVT/XC10G) slot. Only install ONS 15454 cards with a cross symbol on the faceplate.
P	Red/P	Protection slot in 1:N protection schemes.
◆	Red/Diamond	AIC Slot. Only install ONS 15454 cards with a diamond symbol on the faceplate.
★	Gold/Star	Multispeed slot - future

Table 1-8 lists the number of ports, line rates, connector options, and connector locations for ONS 15454 optical and electrical cards.

Table 1-8   Card Ports, Line Rates, and Connectors

Card	Ports	Line Rate per Port	Connector Types	Connector Location
DS1-14	14	1.544 Mbps	SMB w/wire wrap adapter, AMP Champ Connector*	Backplane
DS1N-14	14	1.544 Mbps	SMB w/wire wrap adapter, AMP Champ Connector*	—
DS3-12	12	44.736 Mbps	SMB or BNC*	Backplane
DS3N-12	12	44.736 Mbps	SMB or BNC*	—
DS3-12E	12	44.736 Mbps	SMB or BNC*	Backplane

Table 1-8   Card Ports, Line Rates, and Connectors (continued)

Card	Ports	Line Rate per Port	Connector Types	Connector Location
DS3N-12E	12	44.736 Mbps	SMB or BNC*	—
DS3XM-6	6	44.736 Mbps	SMB or BNC*	Backplane
EC1-12	12	51.84 Mbps	SMB or BNC*	Backplane
E100T-12	12	100 Mbps	RJ-45	Faceplate
E1000-2	2	1000 Mbps	SC (GBIC)	Faceplate
E100T-G	12	100 Mbps	RJ-45	Faceplate
E1000-2-G	2	1000 Mbps	SC (GBIC)	Faceplate
OC-3 IR	4	155.52 Mbps (STS-3)	SC	Faceplate
OC-12 (IR/LR)	1	622.08 Mbps (STS-12)	SC	Faceplate
OC-48 (IR/LR/ELR)	1	2488.32 Mbps (STS-48)	SC	Faceplate
OC-48 any slot (IR/LR)	1	2488.32 Mbps (STS-48)	SC	Faceplate
OC-192 (LR)	1	9.95 Gbps (STS-192)	SC	Faceplate

*   When used as a protect card, the card does not have a physical external connection. The protect card connects to the working card(s) through the backplane and becomes active when the working card fails. The protect card then uses the physical connection of the failed card.

Procedure: Install the TCC+ and XC/XCVT/XC10G Cards

Although the installation procedure is the same for both TCC+ and XC/XCVT/XC10G cards, you must install the TCC+ card and let it initialize before installing the XC/XCVT/XC10G cards. The TCC+ card houses the ONS 15454 software. For a detailed explanation, see Chapter 2, "Software Installation."

Note   This is not the procedure to use when upgrading from XC to XCVT cards or from XCVT to XC10G cards. If you are performing an XC to XCVT upgrade, an XCVT to a XC10G upgrade, or a TCC to TCC+ upgrade, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.

Step 1   Open the card ejectors.

Step 2   Slide the card along the guide rails into the correct slot (Slot 8 or 10 for the XC/XCVT/XC10G and Slot 7 or 11 for the TCC+).

Step 3   Close the ejectors.

Step 4   Verify that power is applied to the shelf assembly.

Step 5   Verify the LED activity as described in Table 1-9.

Table 1-9   LED Activity during TCC+ and XC/XCVT/XC10G Card Installation

Card Type	LED Activity
TCC+	1. The red FAIL LED turns on and remains lit for 20 to 30 seconds.
	2. The red FAIL LED blinks for 35 to 45 seconds.
	3. The red FAIL LED remains lit for 5 to 10 seconds.
	4. All LEDs (including the CRIT, MAJ, MIN, REM, SYNC, and ACO LEDs) blink once and turn off for 5 to 10 seconds.
	5. The ACT/STBY LED turns on. (On the TCC+ card, the ACT/STBY LED may take several minutes to illuminate while the DCC processor boots.)
XC/XCVT/XC10G	1. The red LED turns on and remains lit for 20 to 30 seconds.
	2. The red LED blinks for 35 to 45 seconds.
	3. The red LED remains lit for 5 to 10 seconds.
	4. All LEDs blink once and turn on.
	5. The ACT/STBY LED turns on.

Note If the FAIL LED is lit continuously on the TCC+ card, see the tip below about the TCC+ automatic upload.

Step 6 Verify that the ACT/STBY LED is the correct color for the card (green for active, amber for standby). The IP address for the node, the temperature of the ONS 15454, and the time of day will be displayed on the LCD. The default time and date is 12:00 AM, January 1, 1970.

Tip When a TCC+ card installed in the shelf assembly has a different version of the ONS 15454 software installed than the version running on the active TCC+, the newly-installed TCC+ card automatically loads the software version running on the active TCC+. You do not need to do anything in this situation. However, the loading TCC+ card will not boot up in the normal manner. When the card is first inserted, the red FAIL LED stays on for a short period. The FAIL LED then blinks normally and all LEDs go dark. The FAIL LED and the ACT/STBY LED flash alternately every 30 to 45 seconds as the new software loads onto the new TCC+ card. After loading the new software for approximately 30 minutes, the TCC+ card becomes the standby card and the amber LED is illuminated.

Procedure: Install Optical, Electrical, and Ethernet Cards

Although the installation procedure is the same for optical, electrical, and Ethernet cards, you must install the optical cards before installing the electrical cards.

Warning **Before installing an OC-192 card, make sure the safety key on the faceplate is in off position (labeled 0). When in the on position (labeled 1), the laser is activated.**

Step 1 Open the card ejectors.

Step 2   Slide the card along the guide rails into the correct slot.

Step 3   Close the ejectors.

Step 4   Verify that power is applied to the shelf assembly.

Step 5   Verify the LED activity, as described in Table 1-10.

Table 1-10   LED Activity during Optical and Electrical Card Installation

Card Type	LED Activity
OC-3, OC-12, OC-48, OC-192	1. The red FAIL LED turns on and remains lit for 20 to 30 seconds. 2. The red FAIL LED blinks for 35 to 45 seconds. 3. All LEDs blink once and turn off for 5 to 10 seconds. 4. The ACT LED turns on.
DS-1, DS-3, EC-1	1. The red FAIL LED turns on and remains lit for 10 to 15 seconds. 2. The red FAIL LED blinks for 30 to 40 seconds. 3. All LEDs blink once and turn off for 1 to 5 seconds. 4. The ACT/STBY LED turns on.
Ethernet	1. The red FAIL LED turns on and remains lit for 20 to 30 seconds. 2. The red FAIL LED blinks for 35 to 45 seconds. 3. All LEDs blink once and turn off for 1 to 5 seconds. 4. The ACT LED turns on.

Step 6   Verify that the ACT or ACT/STBY LED is on. The signal fail (SF) LED can persist until all card ports connect to their far end counterparts and a signal is present.

Step 7   When you have displayed CTC on your workstation, verify that the card appears in the correct slot on the CTC node view. See Chapter 2, "Software Installation" for CTC information and setup instructions.

Procedure: Install the AIC Card

Step 1   Open the card ejectors.

Step 2   Slide the card along the guide rails into the correct slot.

Step 3   Close the ejectors.

Step 4   Verify that power is applied to the shelf assembly.

Step 5   Verify the that red FAIL LED remains lit for 1 second.

Step 6   Verify that the red FAIL LED blinks for 1 to 5 seconds.

Step 7   Verify that after 1 to 5 seconds, all LEDs blink once and turn off.

Step 8   Verify that the ACT LED is on.

1.12.2 Gigabit Interface Converter

GBICs are hot-swappable input/output devices that plug into a Gigabit Ethernet (E1000-2 or E1000-2-G) card to link the card with the fiber-optic network. Cisco provides two GBIC models: one for short reach applications (part number 15454-GBIC-SX) and one for long-reach applications (15454-GBIC-LX). The short reach, or "SX" model, connects to multimode fiber and the long reach, or "LX" model, requires single-mode fiber. Because the GBICs are very similar in appearance, check the label on the GBIC carefully before installing it.

For a description of GBICs and their capabilities, see Chapter 9, "Ethernet Operation."

Procedure: Install Gigabit Interface Converters

Step 1 Remove the GBIC from its protective packaging.

Step 2 Check the part number to verify that the GBIC is the correct type for your network.

Step 3 Grip the sides of the GBIC with your thumb and forefinger and insert it into the slot on the front panel of the Gigabit Ethernet card (shown in Figure 1-30).

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

Note GBICs are keyed to prevent incorrect installation.

Figure 1-30   Installing a GBIC on an E1000-2 card
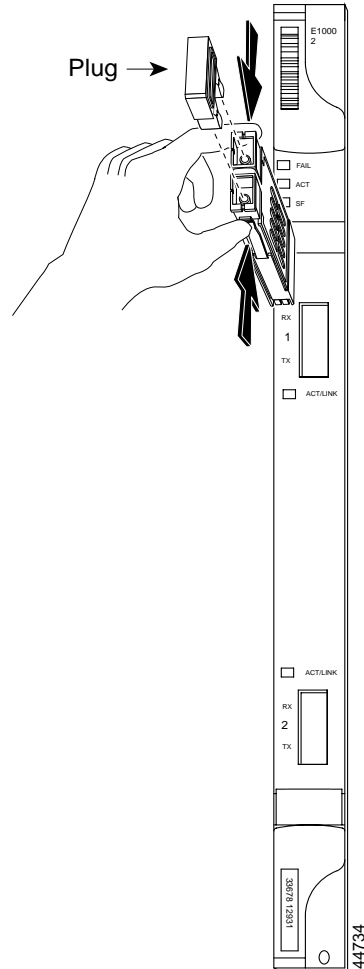
Step 4   Slide the GBIC through the cover flap until you hear a click.

The click indicates the GBIC is locked into the slot.

⚠️

Warning   **GBICs are Class I laser products. These products have been tested and comply with Class I limits.**

⚠️

Warning   **Invisible laser radiation may be emitted from the aperture ports of the single-mode fiber optic modules when no cable is connected. Avoid exposure and do not stare into open apertures.**

Step 5   When you are ready to attach the network interface fiber-optic cable, remove the plug from the GBIC and save the plug for future use.

Step 6   Install and route the cable. See the "Optical Cable Management" section on page 1-55 for routing instructions.

Cisco ONS 15454 Installation and Operations Guide

Procedure: Remove a Gigabit Interface Converter

Step 1   Disconnect the network fiber cable from the GBIC SC connector.

Step 2   Release the GBIC from the slot by simultaneously squeezing the two plastic tabs (one on each side of the GBIC).

Step 3   Slide the GBIC out of the Gigabit Ethernet module slot.

A flap closes over the GBIC slot to protect the connector on the Gigabit Ethernet card.

1.13 Fiber-Optic Cable Installation

This section explains how to install optical fibers on OC-N cards.

⚠
Caution   Always use the supplied ESD wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

ONS OC-N cards feature SC connectors. To install fiber-optic cables in the ONS 15454, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the ONS 15454 cards. On ONS 15454 optical card ports, the top connector is transmit and the bottom connector is receive. Cisco recommends that the transmit and receive and the working and protection fibers be labeled at each end of the fiber span to avoid confusion with cables that are similar in appearance.

For information about fiber cable management, see the "Optical Cable Management" section on page 1-55.

⚠
Warning   **Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**

⚠
Warning   **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**

⚠
Warning   **The laser is active when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**

⚠
Warning   **Follow all directions and warning labels when working with optical fibers. To prevent eye damage, never look directly into a fiber or connector.**

⚠

Caution   Do not user fiber loopbacks with the OC192 LR 1550 card unless you are using a 20 dB attentuator. Never connect a direct fiber loopback. Using fiber loopbacks causes irreparable damage to the OC-192 card.

Procedure: Install Fiber-Optic Cables on OC-N Cards

✎

Note   Clean all fiber connectors thoroughly. Dust particles can degrade performance. Put caps on any fiber connectors that are not used.

Step 1   Place the SC connector in front of the connection point on the card faceplate. Each card supports at least one transmit and one receive connector to create an optical carrier port. Figure 1-31 shows the cable location.

Figure 1-31   Installing fiber-optic cables
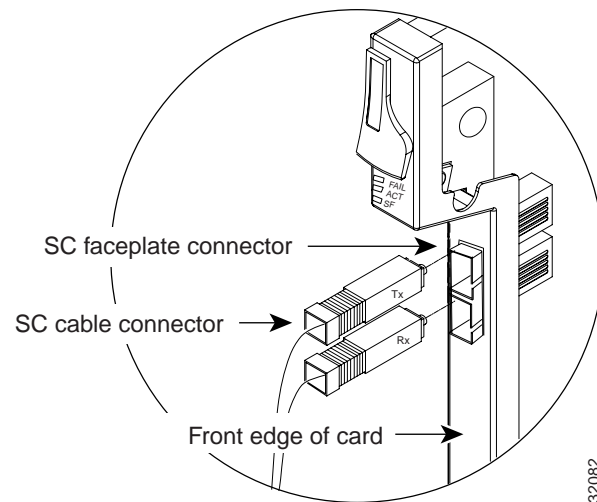
Step 2   Align the keyed ridge of the cable connector with the receiving slot on the faceplate connection point.

Step 3   Gently push the cable connector into the faceplate connection point until the connector snaps into place.

Procedure: Install the Fiber Boot

Cisco provides clear plastic fiber boots for the OC-3, OC-12, and OC-48 (except OC48 AS) cards. The boots prevent hanging fibers from bending too sharply, which may degrade performance. The boots also prevent the front door from interfering with hanging fibers. The fiber boots are not necessary for the OC-192 and the OC-48 AS cards because of the angled SC connector. Figure 1-32 shows the fiber boot attachment.

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

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.

Step 3   Twist the fiber boot to lock the fiber cable into the tail end of the fiber boot.

Slide the fiber boot forward along the fiber cable until the fiber boot fits snugly onto the end of the SC cable connector.

Figure 1-32   Attaching a fiber boot
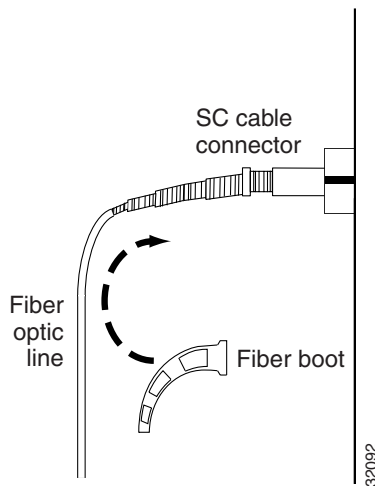
1.14 Cable Routing and Management

The ONS 15454 cable management facilities include the following:

- Cable management clips on optical card faceplates

- A cable-routing channel that runs the width of the shelf assembly

- Plastic horseshoe-shaped fiber guides at each side opening of the cable-routing channel that ensure the proper bend radius is maintained in the fibers

Note   You can remove the fiber guide if necessary to create a larger opening (if you need to route Cat-5 Ethernet cables out the side, for example). To remove the fiber guide, take out the three screws that anchor it to the side of the shelf assembly.

- A fold-down door that provides access to the cable-management tray

- Cable tie-wrap facilities on EIAs that secure cables to the cover panel

- Reversible jumper routing fins that enable you to route cables out either side by positioning the fins as desired

- Jumper slack storage reels (2) on each side panel that reduce the amount of slack in cables that are connected to other devices

> **Note**   To remove the reels, take out the screw in the center of each reel.

Figure 1-33 shows the cable management facilities that you can access through the fold-down front door, including the cable-routing channel and the jumper routing fins.

Figure 1-33   Managing cables on the front panel
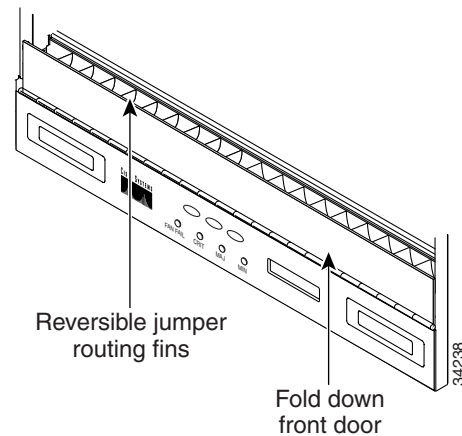
1.14.1 Optical Cable Management

Optical cables connect to the SC connectors which are located on the faceplate of the optical cards and on GBICs. Route optical cables down through the fiber management clips on the optical card faceplate (shown in Figure 1-34) or, if the optical cables are connected to GBICs, route them down through the jumper routing fins (Ethernet cards do not have fiber management clips).

Route optical cables into the cable management area of the shelf assembly, through a cutout in the nearest side of the assembly, and onto the side of the assembly. A hinged panel on the front of the shelf assembly folds down to provide access to the cable-management tray.

Figure 1-34   Routing fiber-optic cables on the optical-card faceplate
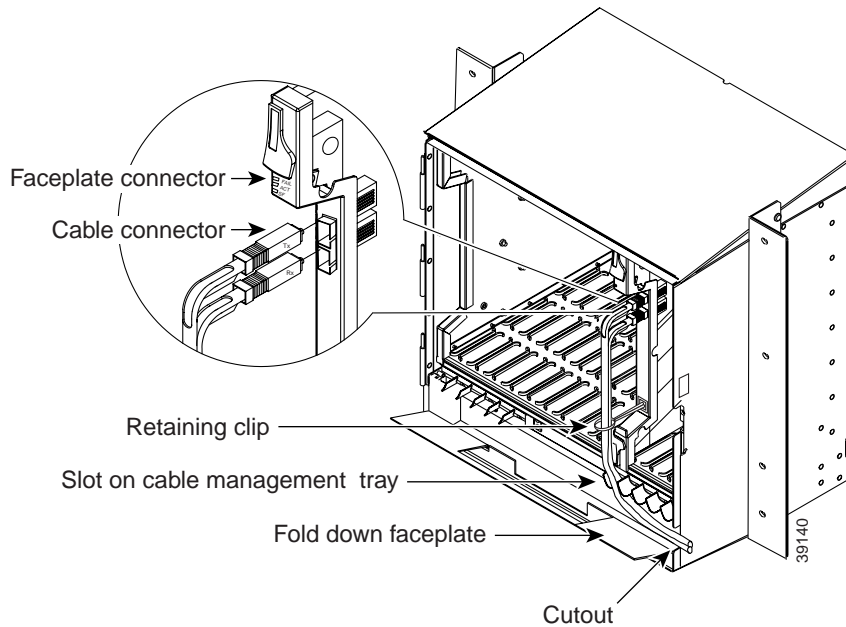
Procedure: Route Fiber-Optic Cables in the Shelf Assembly

Step 1   Open the fold-down front door on the cable-management tray.

Step 2   Route the cable on the card faceplate through the fiber clip on the faceplate.

GBICs do not have fiber clips; therefore, if you are routing optical cable from an E1000-2-G or E1000-2 card, skip to Step 3.

Step 3   Route the cables into the cable-management tray.

Step 4   Route the cables out either side of the cable-management tray through the cutouts on each side of the shelf assembly. Use the reversible fiber guides to route cables out the desired side.

Step 5   Close the fold-down front door when all cables in the front compartment are properly routed.

Figure 1-35 shows the fold-down front door of the shelf assembly open to display the cable routing channel.

Figure 1-35   Fold-down front door of the cable-management tray (displaying the cable routing channel)
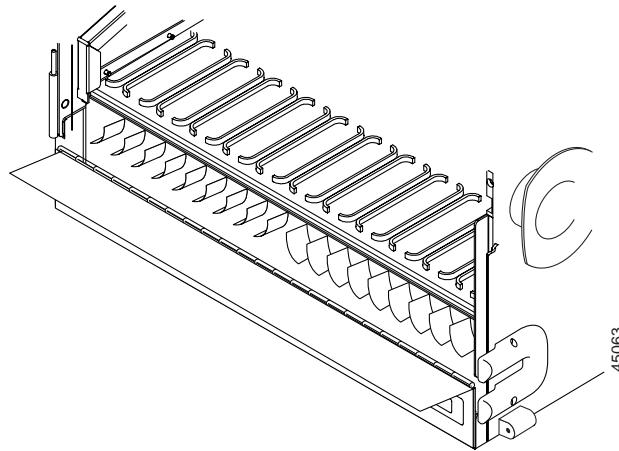
1.14.2 Coaxial Cable Management

Coaxial cables connect to EIAs on the ONS 15454 backplane using cable connectors. EIAs feature cable-management eyelets for tie wrapping or lacing cables to the cover panel.

Procedure: Route the Coaxial Cables

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.

Note   When using the RG179 cable with SMB connectors, remember that the maximum distance available with the RG179 cable is less than the maximum distance available with standard RG59 cable. If you only use the RG179, the maximum available distance is 50 feet versus the 450 feet available with the larger RG59 cable.

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

Step 3   Use standard RG59 connected to the RG179 for the remainder of the cable run. When using a 10-foot section of the RG179, you can attach a maximum length of 437 feet of RG59. When using a 30-foot section of RG179, you can attach a maximum length of 311 feet of RG59.

The shorter maximum distance available with the RG179 is due to a higher attenuation rate for the thinner cable. The attenuation rate for RG59 cable (based on testing with Belden 923, the equivalent of 328A cable) is ~1.0 dB/100 feet at 22 Mhz (DS-3 data rate). The attenuation rate of RG179 is 6.3 db/100 feet. Use a figure of 5.0 for total cable loss when making calculations. Figure 1-36 shows one side of the ONS 15454 backplane with SMB EIAs and the coaxial cables properly routed.

Figure 1-36   Routing coaxial cable through the SMB EIA backplane
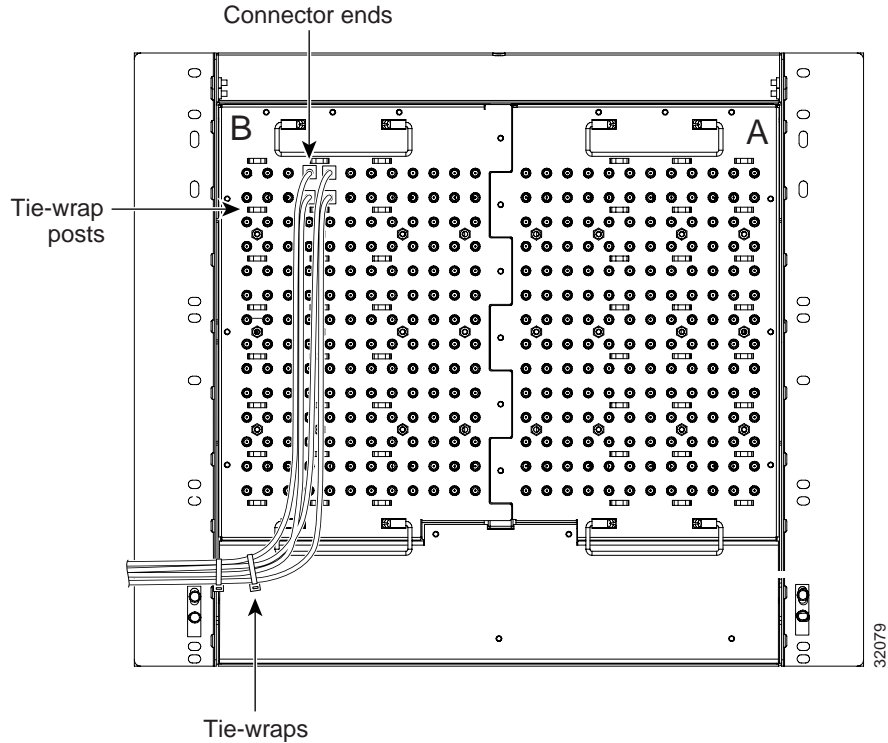
1.14.3 DS-1 Twisted-Pair Cable Management

Connect twisted pair/DS-1cables to SMB EIAs on the ONS 15454 backplane using cable connectors and DS-1 electrical interface adapters (balun).

Procedure: Route DS-1 Twisted-Pair Cables

When using DS-1 twisted-pair cables, the backplane cover has cutouts over the SMB cable connectors. SMB EIAs feature cable-management eyelets for tie wrapping or lacing cables to the cover panel.

Step 1   Install DS-1 electrical interface adapters on every transmit and receive connector for DS-1 ports.

Step 2   Use wire-wrap posts on the DS-1 electrical interface adapters to connect the terminated incoming cables.

Step 3   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.

1.14.4 AMP Champ Cable Management

EIAs have cable management eyelets to tiewrap or lace cables to the cover panel. Tie wrap or lace the AMP Champ cables according to local site practice and route the cables. If you configure the ONS 15454 for a 23-inch rack, two additional inches of cable management area is available on each side of the shelf assembly. See the"AMP Champ EIA" section on page 1-20 and the "AMP Champ Connector Installation" section on page 1-41 and the for more information.

1.14.5 BIC Rear Cover Installation

The ONS 15454 has an optional backplane interface connector (BIC) rear cover. This clear plastic cover provides additional protection for the cables and connectors on the backplane (Figure 1-37). You can also install the optional spacers if more space is needed between the cables and rear cover (Figure 1-38).

Figure 1-37   Clear BIC rear cover
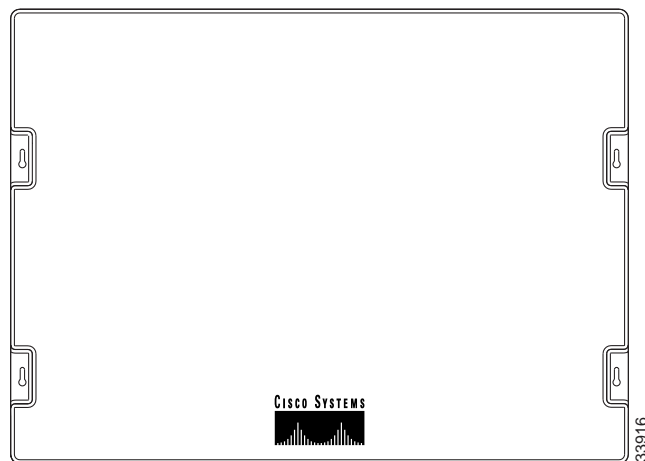
Procedure: Install the BIC Rear Cover

Step 1   Locate the three screws that run vertically along the edges of the backplane.

Only one pair of screws lines up with the screw slots on the mounting brackets, making them easy to locate.

Step 2   Loosen the top and bottom screws on one edge of the backplane to provide room to slide the mounting brackets into place using the u-shaped screw slots on each end.

Step 3   Slide one of the mounting brackets into place and tighten the screws.

Step 4   Repeat Steps 2 and 3 for the second mounting bracket.

Step 5   Attach the cover by hanging it from the mounting screws on the back of the mounting brackets and pulling it down until it fits snugly into place.

Figure 1-38   Backplane attachment for BIC cover

Screw locations
for attaching BIC
rear cover

32073
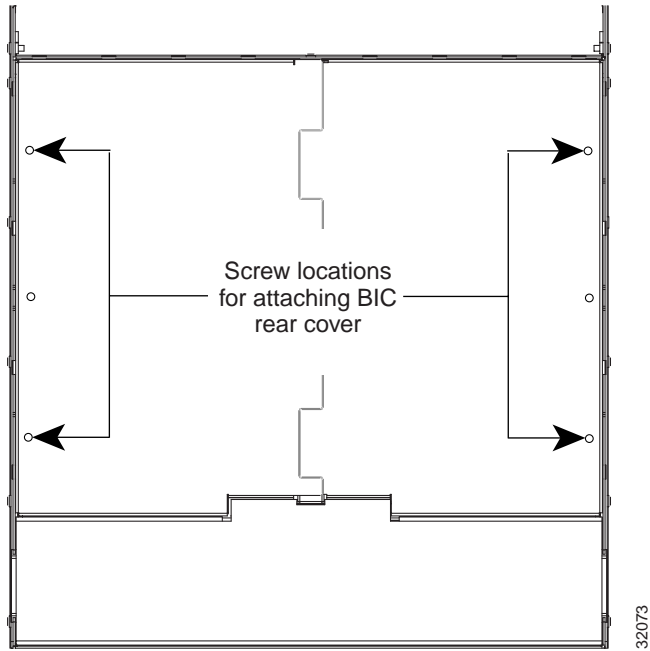
Figure 1-39   Installing the BIC rear cover with spacers

55374
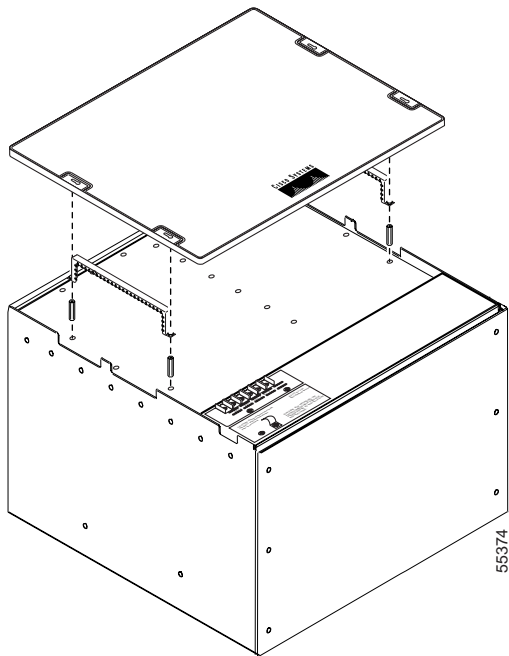
1.15 Ferrite Installation

Place third-party ferrites on certain cables to dampen electromagnetic interference (EMI) from the ONS 15454. Ferrites must be added to meet the requirements of GR 1089. Refer to the ferrite manufacturer documentation for proper use and installation of the ferrites. The following illustrations show possible ferrite placements on the ONS 15454 for power cables, AMP Champ connectors, baluns, BNC/SMB connectors, and the wire-wrap pin field.

Procedure: Attach Ferrites to Power Cabling

Use a single oval ferrite TDK ZCAT2035-0930 for both pairs of cables and a block ferrite Fair Rite 0443164151 for each pair of cables.

Step 1   Wrap the cables once around and through the block ferrites and pull the cable straight through the oval ferrites.

Step 2   Place the oval ferrite between the ONS 15454 and the block ferrite as shown in Figure 1-40.

Step 3   Place the oval ferrite as close to the power terminals as possible and place the block ferrite within 5 to 6 inches of the power terminals.

Figure 1-40   Attaching ferrites to power cabling
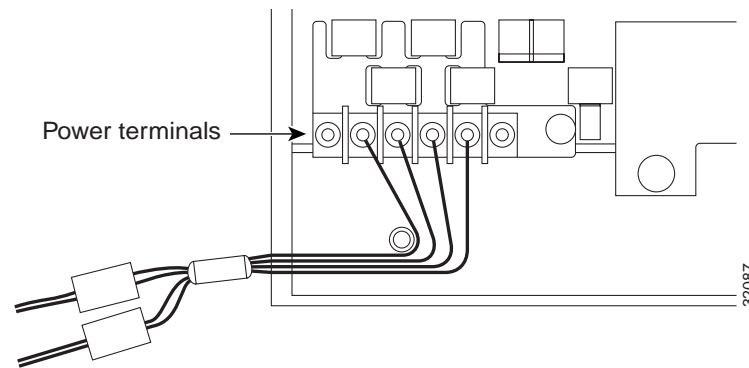
Figure 1-41 shows the suggested method for attaching the ferrites to AMP Champ connectors. Use a block ferrite Fair Rite 0443164151 for each cable.

Figure 1-41   Attaching ferrites to AMP Champ connectors
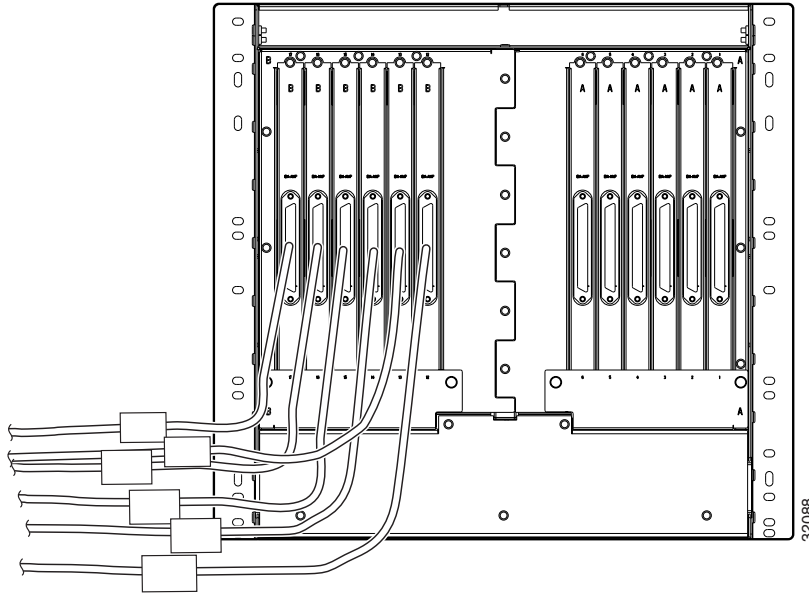
Figure 1-42 shows the suggested method for attaching ferrites to baluns. Use an oval ferrite TDK ZCAT 1730-0730 for each cable.

Figure 1-42   Attaching ferrites to electrical interface adapters (baluns)
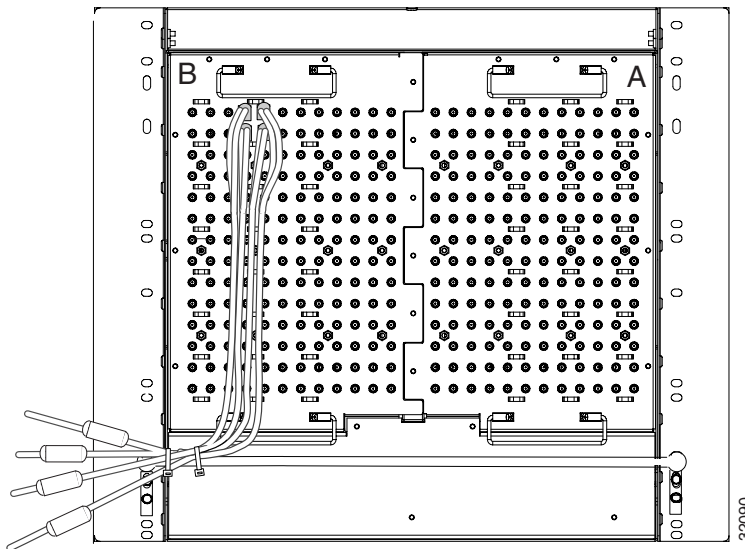
Figure 1-43 shows the suggested method for attaching ferrites to SMB/BNC connectors. Use an oval ferrite TDK ZCAT1730-0730 for each cable and place the ferrite as close to the connector as possible.

Figure 1-43   Attaching ferrites to SMB/BNC connectors
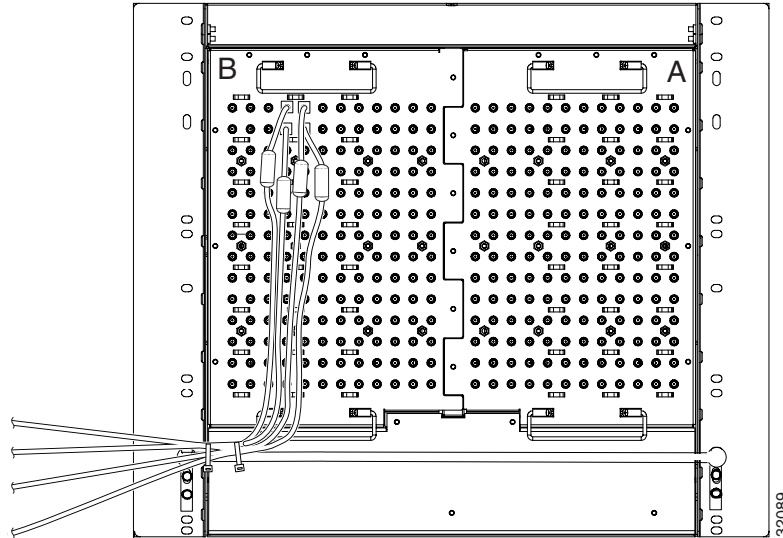
Procedure: Attach Ferrites to Wire-Wrap Pin Fields

Use an oval ferrite TDK ZCAT1730-0730 and block ferrite Fair Rite 0443164151 for each pair of cables.

Figure 1-44 shows the suggested method for attaching ferrites to wire-wrap pin fields.

Step 1   Wrap the cables once around and through the block ferrites and pull the cables straight through the oval ferrites.

Step 2   Place the oval ferrite as close to the wire-wrap pin field as possible and between the ONS 15454 and the block ferrite as shown. The block ferrite should be within 5 to 6 inches of the wire-wrap pin field.

Figure 1-44   Attaching ferrites to wire-wrap pin fields

Cisco ONS 15454 Installation and Operations Guide
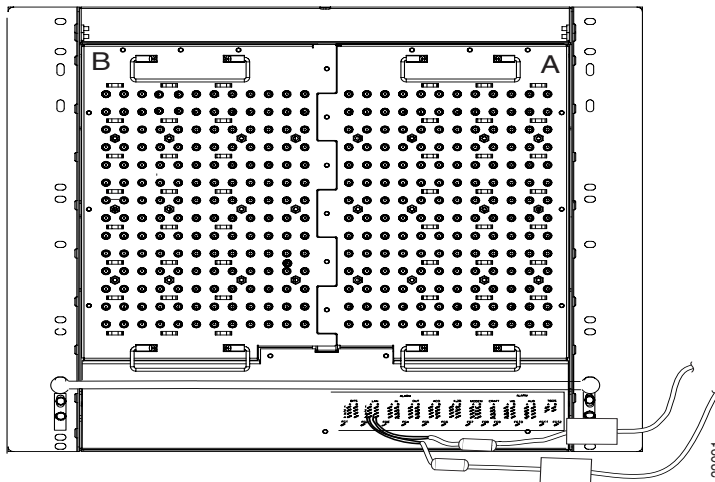
1.16 ONS 15454 Assembly Specifications

This section contains hardware and software specifications for the ONS 15454.

1.16.1 Bandwidth

- Total bandwidth: 240 Gbps
- Data plane bandwidth: 160 Gbps
- SONET plane bandwidth: 80 Gbps

1.16.2 Slot Assignments

- Total card slots: 17
- Multispeed slots (any traffic card except OC48 IR 1310, OC48 LR/ELR 1550, and OC192 LR 1550 cards): Slots 1 – 4, 14 – 17
- High-speed slots (any traffic card including OC48 IR 1310, OC48 LR/ELR 1550, and OC192 LR 1550 cards): Slots 5, 6, 12, 13
- TCC+ (Timing Communication and Control): Slots 7, 11
- XC/XCVT/XC10G (Cross Connect): Slots 8, 10
- AIC (Alarm Interface Card): Slot 9

1.16.3 Cards

- TCC+
- XC
- XCVT
- XC10G
- AIC
- EC1-12
- DS1-14
- DS1N-14
- DS3-12
- DS3N-12
- DS3-12E
- DS3N-12E
- DS3XM-6
- OC3 IR 4 1310
- OC12 IR 1310
- OC12 LR 1310

- OC12 LR 1550

- OC48 IR 1310

- OC48 LR 1550

- OC48 IR/STM16 SH AS 1310

- OC48 LR/STM16 LH AS 1550

- OC192 LR 1550

- OC48 ELR DWDM

- OC48 ELR 1550

- E100T-12

- E1000-2

- E100T-G

- E1000-2-G

Note   The OC-3, OC-12, OC-48, and E1000-2 cards are Class 1 laser products (IEC 60825-1 2001-01/Class I laser product (21CFR 1040.10 and 1040.11).

Note   The OC-192 card is a Class 1M laser product ((IEC 60825-1 2001-01)/Class I laser product (21CFR 1040.10 and 1040.11).

1.16.4 Configurations

- Two-fiber UPSR ring

- Path protected mesh network (PPMN)

- Two-fiber BLSR

- Four-fiber BLSR

- Add-drop multiplexer

- Terminal mode

- Regenerator mode

1.16.5 Cisco Transport Controller

- 10 Base-T

- TCC+ access: RJ-45 connector

- Backplane access: LAN pin field

1.16.6 External LAN Interface

- 10 Base-T Ethernet

Cisco ONS 15454 Installation and Operations Guide

- Backplane access: LAN pin field

1.16.7 TL1 Craft Interface

- Speed: 9600 bps
- TCC+ access: RS-232 DB-9 type connector
- Backplane access: CRAFT pin field

1.16.8 Modem Interface

- Hardware flow control
- TCC+: RS-232 DB-9 type connector

1.16.9 Alarm Interface

- Visual: Critical, Major, Minor, Remote
- Audible: Critical, Major, Minor, Remote
- Alarm contacts: 0.045mm, -48V, 50 mA
- Backplane access: Alarm pin fields

1.16.10 EIA Interface

- SMB: AMP #415504-3 75 Ohm 4 leg connectors
- BNC: Trompeter #UCBJ224 75 Ohm 4 leg connector (King or ITT are also compatible)
- AMP Champ: AMP#552246-1 with #552562-2 bail locks

1.16.11 Nonvolatile Memory

64 MB, 3.0V FLASH memory

1.16.12 BITS Interface

- 2 DS-1 BITS inputs
- 2 derived DS-1 outputs
- Backplane access: BITS pin field

1.16.13 System Timing

- Stratum 3 per Telcordia GR-253-CORE
- Free running accuracy: ± 4.6 ppm

Cisco ONS 15454 Installation and Operations Guide

- Holdover Stability: 3.7 x10^{-7}/day, including temperature (< 255 slips in first 24 hours)

- Reference: External BITS, line, internal

1.16.14 Power Specifications

- Input power: -48 VDC

- Power consumption: 55W (fan tray only); 650W (maximum draw w/cards)

- Power Requirements: -42 to -57 VDC

- Power terminals: #6 Lug

1.16.15 Environmental Specifications

- Operating Temperature: 0 to +55 degrees Celsius

- Operating Humidity: 5 - 95%, non-condensing

1.16.16 Dimensions

- Height: 18.5 inches (40.7 cm)

- Width: 19 or 23 inches (41.8 or 50.6 cm) with mounting ears attached

- Depth: 12 inches (26.4 cm) (5 inch projection from rack)

- Weight: 55 lbs. (empty)

1.17 Installation Checklist

This section provides a summary of the steps required to install the ONS 15454. The section assumes that individual cards are used with their default provisioning values or will be provisioned by local technicians as required by the site.

Table 1-11   Installation Checklist

Description	Check
The ONS 15454 is mounted securely in the rack.	
The ONS 15454 is grounded with the frame ground.	
Power runs to the ONS 15454.	
Visual and Audible alarm pins connect to central alarm collection equipment.	
If used, BITS, LAN, Alarm, ACO, and CRAFT pins connect to corresponding cables.	
If used, BITS, LAN, Alarm, ACO, and CRAFT cables are tiewrapped and routed under screw holes.	
The preferred EIAs are installed.	
Coaxial and/or DS-1 cables are installed on the backplane.	
Laced or tiewrapped coaxial cables run onto the sides of the ONS 15454.	

Cisco ONS 15454 Installation and Operations Guide

Table 1-11   Installation Checklist (continued)

Description	Check
Power connections are fused properly (15A recommended).	
-48V DC (tolerance -42 to -57V DC) power is present at DC A and DC B terminals (if used) when power is applied.	
The fan-tray air filter is installed in the fan tray with the flow direction arrow on the filter frame pointing up.	
The fan-tray assembly is installed. When installed, fans will run on high speed with no TCC+s installed.	
If used, Ethernet patchcords are connected to Ethernet cards.	
Fiber-optic and/or Ethernet patchcords route through the faceplate clips, into the cable-management tray, through the side cutout, and along the sides of the ONS 15454.	
The fan-tray assembly can be removed without disturbing fiber or Ethernet patchcords.	
The LCD is working. (Use LCD buttons to toggle through slots, ports and states of cards.)	
The door is mounted with hinges on hinge pins.	
Doors open and close without disturbing fiber or Ethernet patchcords.	

1.18   ONS 15454 Software and Hardware Compatibility Matrix

Table 1-12 provides a matrix showing software and hardware compatibility for ONS 15454 Releases 2.0, 2.1, 2.2.0, 3.0. and 3.1.

Table 1-12   ONS 15454 Software and Hardware Compatibility

Hardware	2.00.0x (2.0)	2.10.0x (2.1)	2.20.0x (2.2.0)	3.00.0x (3.0)	3.10.0x (3.1)
TCC	Required	Required	Fully Compatible	Not Supported	Not Supported
TCC+	Not Supported	Not Supported	Fully Compatible	Required	Required
XC	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
XCVT	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
XC10G	Not Supported	Not Supported	Not Supported	Not Supported	Fully Compatible
AIC	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
EC1-12	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
DS1-14	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
DS1N-14	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible

Table 1-12   ONS 15454 Software and Hardware Compatibility (continued)

Hardware	2.00.0x (2.0)	2.10.0x (2.1)	2.20.0x (2.2.0)	3.00.0x (3.0)	3.10.0x (3.1)
DS3-12	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
DS3N-12	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
DS3-12E	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
DS3N-12E	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
DS3XM-6	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC3 IR 4 1310	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC12 IR 1310	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC12 LR 1310	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC12 LR 1550	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC48 IR 1310	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC48 LR 1550	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC48 ELR DWDM	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
OC48 IR/STM16 SH AS 1310	See Note	See Note	See Note	See Note	Fully Compatible
OC48 LR/STM16 LH AS 1550	See Note	See Note	See Note	See Note	Fully Compatible

Note   Use the XC10G card, the TCC+ card, and Software R3.1 or higher to enable the any slot function on the OC48 IR/STM16 SH AS 1310 and OC48 LR/STM16 LH AS 1550 cards.

Hardware	2.00.0x (2.0)	2.10.0x (2.1)	2.20.0x (2.2.0)	3.00.0x (3.0)	3.10.0x (3.1)
OC192 LR/STM64 LH 1550	Not Supported	Not Supported	Not Supported	Not Supported	Fully Compatible
E100T-12	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
E1000-2	Not Supported	Not Supported	Fully Compatible	Fully Compatible	Fully Compatible

Cisco ONS 15454 Installation and Operations Guide

Table 1-12   ONS 15454 Software and Hardware Compatibility (continued)

Hardware	2.00.0x (2.0)	2.10.0x (2.1)	2.20.0x (2.2.0)	3.00.0x (3.0)	3.10.0x (3.1)
E100T-G	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible	Fully Compatible
E1000-2-G	Not Supported	Not Supported	Fully Compatible	Fully Compatible	Fully Compatible

If an upgrade is required for compatibility, call the Cisco Technical Assistance Center at 1-877-323-7368.

Software Installation

Cisco Transport Controller (CTC), the Cisco ONS 15454's software interface, is stored on the TCC+ card and download to your workstation each time you log into the ONS 15454. This chapter:

- Describes how Cisco Transport Controller (CTC) software is installed on PCs and Solaris workstations

- Tells you how to connect PCs and Solaris workstations to the Cisco ONS 15454, including direct connections, LAN connections, remote connections, and firewall-compliant connections

- Describes the CTC graphic user interface, including the three main CTC views, network, node, and card

- Explains how to create domains to manage multiple nodes, change the network view background color and image (map), and add a node to the network map

- Describes the different ways you can invoke commands within CTC

- Explains how to print and export CTC data

2.1 Installation Overview

ONS 15454 provisioning and administration is performed using the Cisco Transport Controller software. CTC is a Java application that is installed in two locations:

- ONS 15454 Timing Communications and Control card (TCC+)

- PCs and Solaris workstations that connect to the ONS 15454

CTC software is pre-installed on the TCC+. The only time you install software on the TCC+ is when you upgrade from one CTC release to another. To upgrade CTC on the TCC+, you must follow the upgrade procedures specific to the software release. These procedures can be downloaded from the Cisco website (www.cisco.com).

For PCs and Solaris workstations, CTC is downloaded from the TCC+ and installed on your computer automatically after you connect to the ONS 15454. To connect to an ONS 15454, you enter the ONS 15454 IP address in the URL field of a web browser, such as Netscape Navigator or Microsoft® Internet Explorer. After connecting to an ONS 15454, the following installation occurs automatically:

1. A CTC launcher applet is downloaded from the TCC+ to your computer's Temp directory. (If these files are deleted, they are reinstalled the next time you connect to the ONS 15454.)

2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15454 TCC+.

3. If the computer does not have CTC installed, or if the installed release is older than the TCC+ version, the launcher downloads the CTC program files from the TCC+.

4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. If you log into an ONS 15454 that is connected to ONS 15454s with older versions of CTC, or to Cisco ONS 15327s, CTC "element" files are downloaded automatically to enable you to interact with those nodes. You cannot interact with nodes on the network that have a software version later than the node that you are logged into. Therefore, always log into nodes having the latest software release.

Each ONS 15454 can handle up to four network-level CTC sessions (the login node and its DCC-connected nodes) and one node-level session (login node only) at one time. CTC performance may vary, depending upon the volume of activity in each session.

Note   You can also use TL1 commands to communicate with the Cisco ONS 15454 through VT100 terminals and VT100 emulation software, or you can Telnet to an ONS 15454 using TL1 port 3083. See the *Cisco* ONS 15454 *TL1 Command Guide* for a comprehensive list of TL1 commands.

2.2 Computer Requirements

To use CTC in ONS 15454 Release 3.1, your computer must have a web browser with the correct Java Runtime Environment (JRE) installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 ONS 15454 software CD. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 2-1 on page 2-2 shows JRE compatibility with ONS software releases.

Table 2-1   JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15327 Release 1.0	Yes	No
ONS 15327 Release 1.0.1	Yes	Yes
ONS 15454 Release 2.2.1 and earlier	Yes	No
ONS 15454 Release 2.2.2	Yes	Yes
ONS 15454 Release 3.0	Yes	Yes
ONS 15454 Release 3.1	Yes	Yes

Requirements for PCs and Solaris workstations are provided in Table 2-2. A modified java.policy file must also be installed. In addition to Netscape Communicator and the JRE, also included on the ONS 15454 software CD and the ONS 15454 documentation CD are the Java plug-in and modified java.policy file.

Table 2-2   Computer Requirements for CTC

Area	Requirements	Notes
Processor	Pentium II 300 MHz, UltraSPARC, or equivalent	300 Mhz is the recommended processor speed. You can use computers with less processor speed; however, you may experience longer response times and slower performance.
RAM	128 MB	
Hard drive	2 GB	CTC application files are downloaded from the TCC+ to your computer's Temp directory. These files occupy 3-5 MB of hard drive space.
Operating System	• PC: Windows 95, Windows 98, Windows NT 4.0, or Windows 2000 • Workstation: Solaris 2.6 or 2.7	
Web browser	• PC: Netscape Navigator 4.51 or higher, or Netscape Communicator 4.61 or higher, or Internet Explorer 4.0 (service pack 2) or higher • Workstation: Netscape Navigator 4.73 or higher	Netscape Communicator 4.73 (Windows) and 4.76 (Solaris) are installed by the CTC Setup Wizard included on the Cisco ONS 15454 software and documentation CDs.
Java Runtime Environment	JRE 1.2.2_05 with Java Plugin 1.2.2 minimum JRE 1.3.0_C (PC) recommended JRE 1.3.0_01 (Solaris) recommended	Use JRE 1.2.2_05 if you connect to ONS 15454s running CTC Release 2.2.1 or earlier. Use JRE 1.3.0 if all ONS 15454s that you connect to are running Release 2.2.2 or later. JRE 1.3.0 is installed by the CTC Setup Wizard included on the Cisco ONS 15454 software and documentation CDs.
Java.policy file	A java.policy file modified for CTC must be installed	A modified java.policy file is installed by the CTC Setup Wizard included on the Cisco ONS 15454 software and documentation CDs.
Cable	User-supplied Category 5 straight-through cable with RJ-45 connectors on each end to connect the computer to the ONS 15454 directly or though a LAN.	

✐
Note On PCs, the mouse pointer scheme should be set to Windows Standard (Windows 95/98) or None (Windows NT or Windows 2000). To check the settings, choose Settings and then Control Panel from the Windows Start menu. Double-click the Mouse option. From the Pointers tab of the Mouse Properties dialog box, select the Windows Standard (or "none" for NT or Windows 2000) mouse scheme. Click OK.

2.3 Running the CTC Setup Wizard

The ONS 15454 provides a setup wizard that installs the files needed to run CTC on PCs and Solaris workstations. You can run the setup wizard from the Cisco ONS 15454 software CD or from the Cisco ONS 15454 documentation CD. The wizard will install:

- Netscape Communicator 4.73 (Windows) or 4.76 (Solaris)
- JRE 1.3 (Windows) or JRE 1.3.0.01 (Solaris)
- Cisco ONS 15454 online documentation
- Modified java.policy file

For Solaris workstations, the JRE may require patches to run properly. You can find the patch tar file in the Jre/Solaris directory on the CD. For information about installing the patches, see the Jre/Solaris/Solaris.txt file on the CD. After installing the patches, if necessary, perform the "Set Up the Environment Variable (Solaris installations only)" procedure on page 2-4 and the "Reference the JRE (Solaris installations only)" procedure on page 2-5 to set up JRE on the workstation.

Procedure: Run the CTC Setup Wizard

Step 1 Insert the Cisco ONS 15454 Release 3.1 software or documentation CD into your computer CD drive. If the CD directory does not automatically open, open it.

Step 2 Double-click **setup.exe** (Windows) or **setup.bat** (Solaris).

Step 3 Follow the on-screen instructions. You can choose to install all components, or select the Custom option to install selected components.

Procedure: Set Up the Environment Variable (Solaris installations only)

Perform one of the following edit procedures. (*JRE* indicates the destination directory you selected for the JRE.)

- If you are using csh, edit the .cshrc file in your home directory by adding:

    setenv NPX_PLUGIN_PATH [*JRE*]/j2rel1_3_0_01/plugin/sparc/ns4

- If you are using ksh, edit the .kshrc file in your home directory by adding:

    export NPX_PLUGIN_PATH = [*JRE*]/j2rel1_3_0_01/plugin/sparc/ns4

Procedure: Reference the JRE (Solaris installations only)

Step 1   Run the Control Panel by typing:

[*JRE*]/j2rel1_3_0_01/bin/ControlPanel

Step 2   Click the **Advanced** tab.

Step 3   From the combo box, select **[*JRE*]/j2rel1_3_0_01**. If the JRE is not found, select **other** and enter the following in the Path text box:

[*JRE*]/j2rel1_3_0_01

Step 4   Click **Apply**.

2.4   Connecting PCs to the ONS 15454

You can connect a PC to the ONS 15454 using the RJ-45 LAN port on the TCC+ or the LAN 1 pins on the ONS 15454 backplane. For a list of LAN pin assignments, see Table 1-2 on page 1-34. Each ONS 15454 must have a unique IP address that you use to access the ONS 15454. The address is displayed on the front panel LCD. The initial IP address, 192.1.0.2, is the default address for ONS 15454 access and configuration. Each computer used to communicate with the ONS 15454 should have only one IP address.

✎
Note   Do not use dual network interface cards (NIC) or an enabled NIC card and dial-up adapter at the same time; this hampers communication between CTC and ONS 15454s.

2.4.1   Direct Connections to the ONS 15454

A direct PC to ONS 15454 connection means your computer is physically connected to the ONS 15454. This is most commonly done by connecting a CAT-5 straight-through cable from your PC NIC card to the RJ-45 port on the TCC+. However, direct connections include connections to switches or hubs to which the ONS 15454 is physically connected. To connect to the ONS 15454 with a direction connection, you must:

- Set up Windows on your PC for direct connections
- Attach cables from the PC to the ONS 15454
- Test your connection

Procedure: Creating a Direct Connection to an ONS 15454

Step 1   Attach a CAT-5 cable from the PC NIC card to one of the following:

- RJ-45 jack on the ONS 15454 TCC+ card
- RJ-45 jack on a hub or switch to which the ONS 15454 is physically connected

Step 2   Use the steps in Table 2-3 to set up Windows for direct connections to an ONS 15454 when:

- DHCP (Dynamic Host Configuration Protocol) is not enabled on the ONS 15454 or the ONS 15454 is not connected to a DHCP server. If DHCP is enabled, go to Step 2. (For information about DHCP, see the"Setting Up Network Information" section on page 3-2.)

- The ONS 15454 is not connected to a LAN.

Table 2-3   Setting Up Windows 95/98, Windows NT, and Windows 2000 PCs for Direct ONS 15454 Connections

Windows 95/98	Windows NT	Windows 2000
1. From the Windows Start menu, choose **Settings** > **Control Panel**.	1. From the Windows Start menu, choose **Settings** > **Control Panel**.	1. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.
2. On the Control Panel dialog box, click the **Network** icon.	2. On the Control Panel dialog box, click the **Network** icon.	2. On the Local Area Connection Status dialog box, click **Properties**.
3. In the Network dialog box select TCP/IP for your PC Ethernet card, then click **Properties**.	3. In the Network dialog box click the **Protocols** tab, choose **TCP/IP Protocol**, then click **Properties**.	3. On the General tab, choose **TCP/IP Protocol**, then click **Properties**.
4. On the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.	4. Click the **IP Address** tab.	4. Click **Use the following IP address**.
5. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.	5. In the IP Address window, click **Specify an IP address**.	5. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last three digits. The last three digits must be between 1 and 254.
6. Click the **IP Address** tab.	6. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last three digits. The last three digits must be between 1 and 254.	6. In the Subnet Mask field, type 255.255.255.0.
7. In the IP Address window, click **Specify an IP address**.	7. In the Subnet Mask field, type 255.255.255.0.	7. In the Default Gateway field, type the ONS 15454 IP address.
8. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address except for the last three digits. The last three digits must be between 1 and 254.	8. Click **OK**.	8. Click **OK**.
9. In the Subnet Mask field, type 255.255.255.0.	9. On the TCP/IP Properties dialog box, type the ONS 15454 IP address in the Default Gateway field.	
10. Click **OK**.	10. Click **Apply**.	
11. On the TCP/IP dialog box, click the **Gateway** tab.	11. In some cases, Windows NT will prompt you to reboot your PC. If you receive this prompt, click **Yes**.	
12. In the New Gateway field, type the ONS 15454 IP address. Click **Add**.		
13. Verify that the IP address displays in the Installed Gateways field, then click **OK**.		
14. When the prompt to restart your PC displays, click **Yes**.		

Step 3   Test the connection:

    a. Start Netscape Navigator or Internet Explorer.

   b. Enter the Cisco ONS 15454 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box display. If this occurs, go to Step 2 of the "Log into the ONS 15454" procedure on page 2-9 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

   c. From the Windows Start menu, choose the MS-DOS or command prompt.

   d. At the prompt, type:

```
ping [ONS 15454 IP address]
```

For example, you would type "ping 192.1.0.2" to connect to an ONS 15454 with default IP address 192.1.0.2. If your computer is connected to the ONS 15454, a "reply from [IP address]" message displays.

If your PC is not connected, a Request timed out message displays. If this occurs, check that the cables connecting the PC to the ONS 15454 are securely attached. Check the Link Status LED on the PC NIC card. Repeat the procedures provided in Table 2-3 while verifying IP and submask information.

2.4.2 Network Connections

When connecting the PC to the ONS 15454 through a LAN, the PC's IP address must be configured to be on the same subnet as the ONS 15454's LAN interface. The ONS 15454 IP address and netmask are visible on the LCD panel. If needed, change the IP address configuration on the PC or use the LCD panel on the ONS 15454.

Procedure: Access the ONS 15454 from a LAN

Step 1 Change the ONS 15454 IP address to an IP address that exists on the LAN. (See the "Change IP Address, Default Router, and Network Mask Using the LCD" procedure on page 3-4 for instructions.)

Step 2 Ensure that the ONS 15454 is physically connected to the LAN (typically using a cross-over cable to a hub or switch).

Step 3 If you changed the PC network settings for direct access to the ONS 15454, change the settings back to the LAN access settings. Usually this means setting the IP Address on the TCP/IP dialog box back to "Obtain an IP address automatically" (Windows 95/98) or "Obtain an IP address from a DHCP server" (Windows NT/2000). If your LAN requires that DNS or WINS be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 4 If your computer is connected to a proxy server, disable proxy service or add the ONS 15454 nodes as exceptions.

Step 5 Start your web browser and type the ONS 15454 IP address in the URL field.

Procedure: Disable Proxy Service Using Internet Explorer (Windows)

Complete these steps if your computer is connected to a proxy server and your browser is Internet Explorer.

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

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

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

Step 4   On the LAN Settings dialog box, either:

- Deselect **Use a proxy server** to disable the service

or

- Leave **Use a proxy server** selected and click **Advanced**. On 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.

Procedure: Disable Proxy Service Using Netscape (Windows and Solaris)

Complete these steps if your computer is connected to a proxy server and your browser is Netscape Navigator.

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, either:

- Choose **Direct connection to the Internet** to bypass the proxy server

or

- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. On 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.

2.4.3 Remote Access to the ONS 15454

You can use LAN modems to access ONS 15454s from remote sites. The LAN modem must be connected to the RJ-45 port on a TCC+ card or to the LAN pins on the ONS 15454 backplane. The LAN modem must be properly configured for use with the ONS 15454. When the modem is installed, dial-up access to the ONS 15454 is available using a PC or Solaris workstation modem.

2.4.4 TL1 Terminal Access to the ONS 15454

You can communicate with the ONS 15454 using TL1. To connect a TL1 terminal (or a PC running terminal emulation software) to the ONS 15454, you can:

- Use the DB-9 plug on the front panel of the TCC+ card or the CRAFT pins on the backplane. (For a list of CRAFT pin assignments, see Table 1-3 on page 1-35.)
- Telnet to port 3083 with a LAN connection.
- Start a TL1 session from CTC by selecting Open TL1 Session from the CTC Tools menu and selecting the node where you want to hold the TL1 session in the Select Node dialog box.

For information about using TL1 commands with the ONS 15454, see the *Cisco ONS 15454 TL1 Command Guide*.

2.5 Logging into the ONS 15454

After you set up the physical connections between the PC and ONS 15454 and change your PC network settings, you can log into CTC.

Note   If you encounter errors while logging in, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for possible causes.

Procedure: Log into the ONS 15454

Step 1   From the PC connected to the ONS 15454, start Netscape or Internet Explorer.

Step 2   In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15454 IP address. For initial setup, this is the default address, 192.1.0.2. Press **Enter**.

Note   If you are logging into ONS 15454 or ONS 15327 networks running different releases of CTC software, log into the node running the most recent release. If you log into a node with an older release, nodes running later releases display as grey icons on the network map, and the IP address will display instead of the node name. To check the software version of a node, select **About CTC** from the CTC Help menu.

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 display while CTC files are downloaded to your computer; then the CTC Login dialog box displays (Figure 2-1).

Figure 2-1   Logging into the ONS 15454
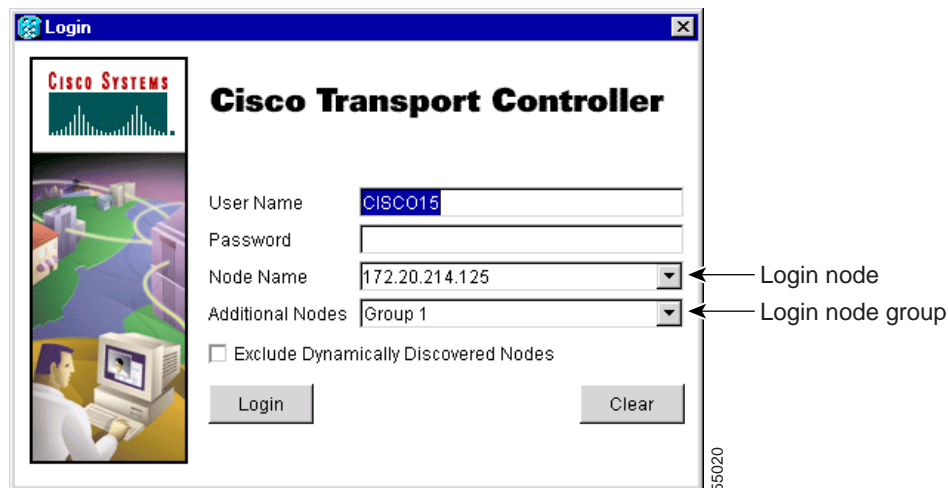
Step 3   Type a user name and password (both are case sensitive). For initial setup, type the user name "CISCO15" and click **Login** (no password is required).

> **Note** The CISCO15 user is provided with every ONS 15454. CISCO15 has superuser privileges, so you can create other users. CISCO15 is delivered without a password. To create one, click the **Provisioning** > **Security** tabs after you log in and change the CISCO15 password. (You cannot delete the CISCO15 user.) For more information about ONS 15454 security, see the "Creating Users and Setting Security" section on page 3-6.

Step 4   Set the following login options, as needed:

- *Node Name*—Displays the IP address entered in the web browser and a pull-down menu of previously-entered ONS 15454 IP addresses. You can select any ONS 15454 (or ONS 15327) on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.

- *Additional Nodes*—Displays a list of login node groups that were created. Login node groups allow you to display ONS 15454s and/or ONS 15327s that are not connected by the SONET Data Communications Channel (DCC) to the ONS 15454 in the Node Name field. (For instructions, see the "Creating Login Node Groups" section on page 2-10.)

> **Note** Topology hosts that were created in previous ONS 15454 releases by modifying the cms.ini file are displayed as a "Topology Host" group under Additional Nodes.

- *Exclude Dynamically Discovered Nodes*—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 the Node Name ONS 15454 through the DCC are not displayed.

Step 5   Click **Login**.

If login is successful, the CTC window displays. From here, you can navigate to other CTC views to provision and manage the ONS 15454.

2.5.1 Creating Login Node Groups

When you log into an ONS 15454 node, only ONS 15454s optically connected (i.e., with DCC connections) to the node will display in network view. However, you can create a login node group to view and manage ONS 15454s that only have an IP connection. For example, logging into Node 1 in Figure 2-2 displays Node 2 and Node 3 because they are optically connected to Node 1. Nodes 4, 5, and 6 do not display because DCC connections do not exist. To view all six nodes at once, you create a login node group with the IP addresses of Nodes 1, 4, and 5. Those nodes, and all nodes optically connected to them, display when you log into any node in the group.

Figure 2-2   A login node group

Laptop PC

IP Address
192.168.106.100

LAN/WAN (Ethernet)

Node 1
IP Address
192.168.106.143

Node 4
IP Address
192.168.105.119

Node 5
IP Address
192.168.104.109

Three node ring

Single

Two node ring

Node 2

Node 3

Node 6
IP Address
192.168.103.199

55029
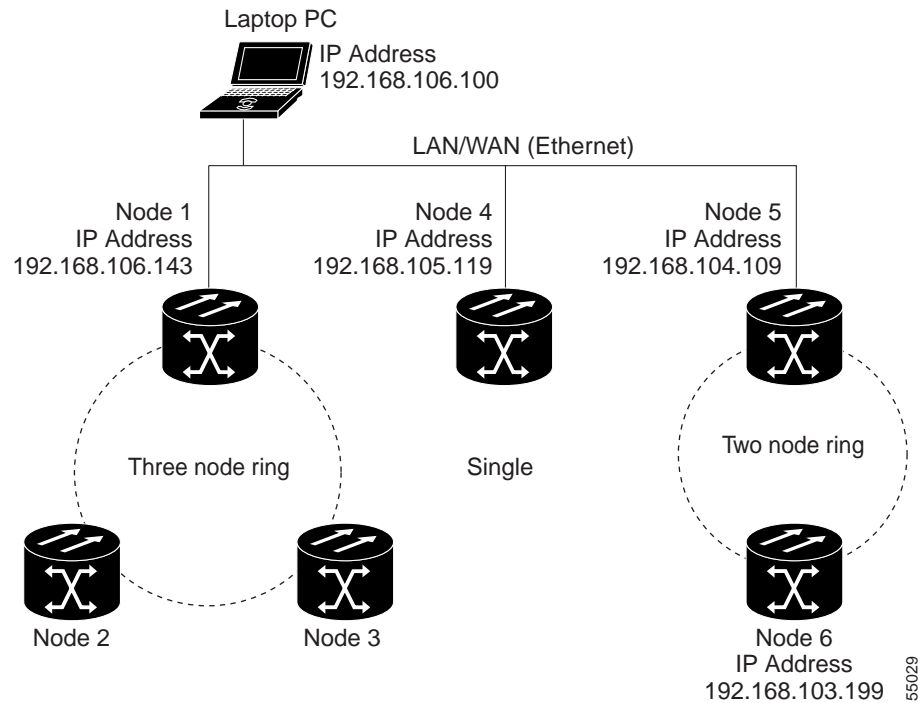
Procedure: Create a Login Node Group

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

Step 2   Click the **Login Node Group** tab and click **Create Group**.

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

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

Step 5   Click **OK**.

The next time you log into an ONS 15454, the login node group will be available in the Additional Nodes list of the Login dialog box. 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.

2.5.2 Accessing ONS 15454s Behind Firewalls

If an ONS 15454 or CTC computer resides behind a firewall that uses port filtering, you must receive an Internet Inter-ORB Protocol (IIOP) port from your network administrator and enable the IIOP port on the ONS 15454 and/or CTC computer, depending on whether one or both devices reside behind firewalls.

If the ONS 15454 is in a protected network and the CTC computer is in an external network, as shown in Figure 2-3, enable the IIOP listener port specified by the firewall administrator on the ONS 15454. The ONS 15454 sends the port number to the CTC computer during the initial contact between the devices using Hyper-Text Transfer Protocol (HTTP). After the CTC computer obtains the ONS 15454 IIOP port, the computer opens a direct session with the node using the specified IIOP port.

Figure 2-3   ONS 15454s residing behind a firewall
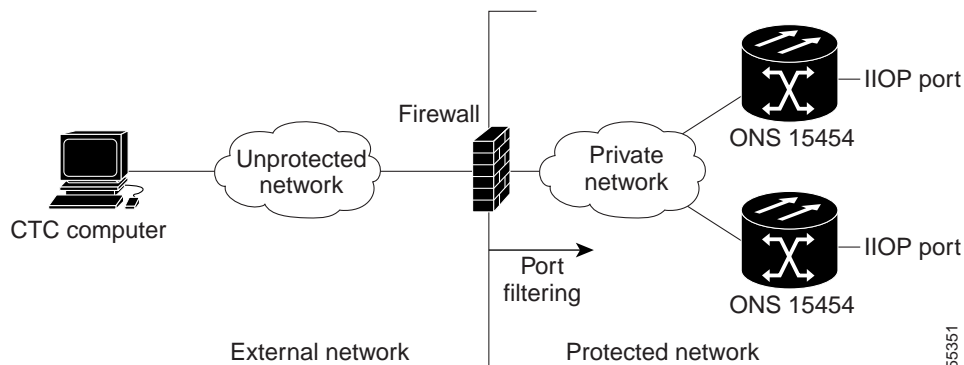
If the CTC computer and the ONS 15454 both reside behind firewalls (Figure 2-4), set the IIOP port on the CTC computer and on the ONS 15454. Each firewall can use a different IIOP port. For example, if the CTC computer firewall uses IIOP port 4000, and the ONS 15454 firewall uses IIOP port 5000, 4000 is the IIOP port set on the CTC computer and 5000 is the IIOP port set on the ONS 15454.

Figure 2-4   A CTC computer and ONS 15454s residing behind firewalls
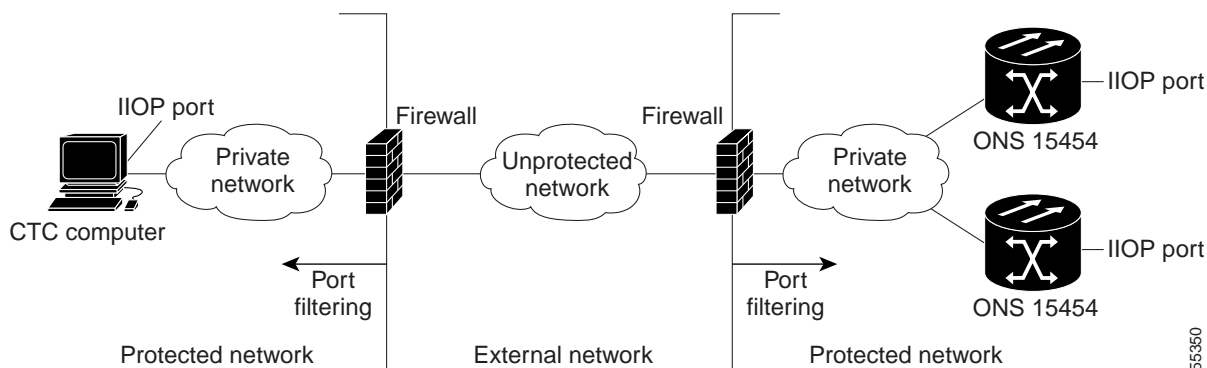
Procedure: Set the IIOP Listener Port on the ONS 15454

Step 1   Log into the ONS 15454 node from a CTC computer that is behind the firewall.

Step 2   In node view, select the **Provisioning** > **Network** tabs.

Step 3   On the **General** subtab under TCC+ CORBA (IIOP) Listener Port, select a listener port option:

- *Default - Variable*—Used to connect to ONS 15454s on the same side of the firewall or if no firewall is used

- *Standard Constant*—Uses port 683, the CORBA default port number

- *Other Constant*—Allows you to set an IIOP port specified by your firewall administrator

Step 4   Click **OK** to apply the change.

Step 5   When the Change Network Configuration? message displays, click **Yes**.

Both ONS 15454 TCC+s will reboot, one at a time.

Procedure: Set the IIOP Listener Port on CTC

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

Step 2   On the Preferences dialog box, select the **Firewall** tab.

Step 3   Under CTC CORBA (IIOP) Listener Port, set the listener port option:

- *Default - Variable*—Used to connect to ONS 15454s from within a firewall or if no firewall is used

- *Standard Constant*—Uses port 683, the CORBA default port number

- *Other Constant*—Allows you to specify an IIOP port defined by your administrator

Step 4   Click **OK** to apply the change and close the dialog box.

2.6 Working with the CTC Window

The CTC window (screen) displays after you log into an ONS 15454 (Figure 2-5). The window includes a menu bar, toolbar, and a top and bottom pane. The top pane displays status information about the selected objects and a graphic of the current view. The bottom pane displays tabs and subtabs, which you use to view ONS 15454 information and perform ONS 15454 provisioning and maintenance. From this window you can display three ONS 15454 views: network, node, and card.

Figure 2-5   CTC window elements in the node view (default login view)
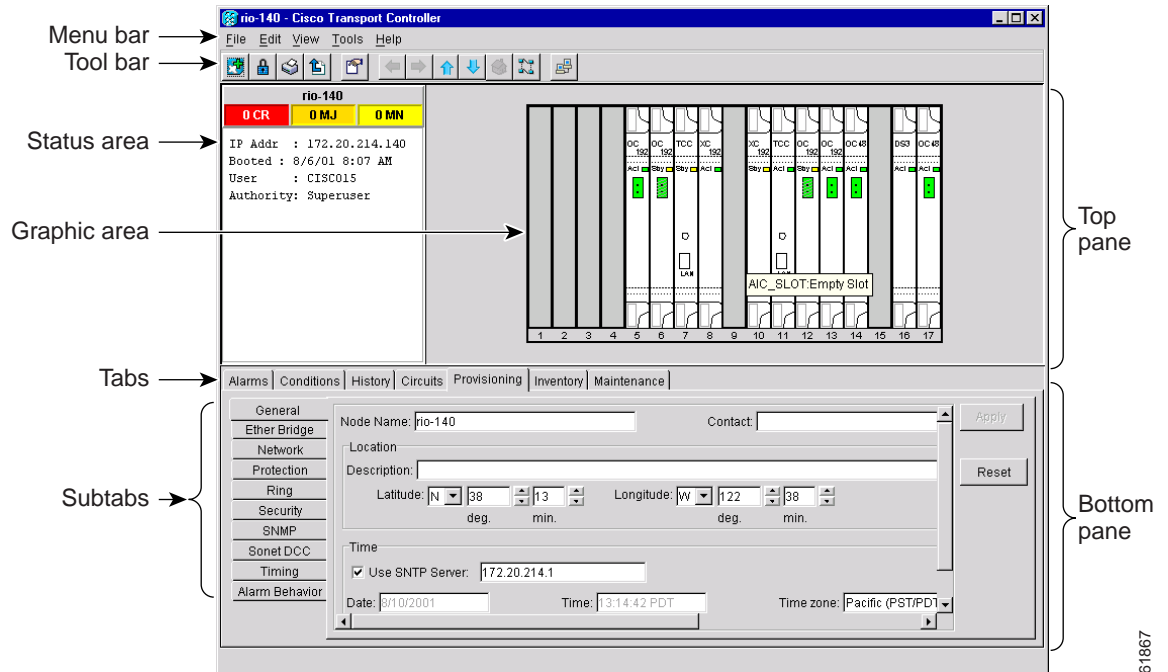
2.6.1 Node View

The CTC node view, shown in Figure 2-5, is the first view displayed after you log into an ONS 15454. The login node is the first node displayed, and it is the "home view" for the session. Node view allows you to view and manage one ONS 15454 node. The status area shows the node name, IP address, session boot date and time, number of critical (CR), major (MJ), and minor (MN) alarms, the name of the current logged-in user, and security level of the user.

2.6.1.1 CTC Card Colors

The graphic area of the CTC window depicts the ONS 15454 shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card and slot (Table 2-4).

Table 2-4   Node View Card Colors

Card Color	Status
Grey	Slot is not provisioned; no card is installed
Violet	Slot is provisioned; no card is installed
White	Slot is provisioned; a functioning card is installed
Yellow	Slot is provisioned; a minor alarm condition exists
Orange	Slot is provisioned; a major alarm condition exists
Red	Slot is provisioned; a critical alarm exists

2.6.1.2 Node View Card Shortcuts

If you move your mouse over cards in the graphic, tooltips display additional information about the card including the card type, card status (active or standby), the number of critical, major, and minor alarms (if any), and the alarm profile used by the card. Right-clicking a card reveals a shortcut menu, which you can use to open, reset, or delete a card. Right-click a slot (grey) to pre-provision a card (i.e., provision a slot before installing the card).

2.6.1.3 Node View Tabs

Use the node view tabs and subtabs, shown in Table 2-5, to provision and manage the ONS 15454.

Table 2-5   Node View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the node and updates them in real-time	none
Conditions	Displays a list of standing conditions on the node.	none
History	Provides a history of node alarms including date, type, and severity of each alarm. The Session subtab displays alarms and events for the current session. The Node subtab displays alarms and events retrieved from a fixed-size log on the node.	Session, Node
Circuits	Create, delete, edit, and map circuits	none
Provisioning	Provision the ONS 15454 node	General, Ether Bridge, Network, Protection, Ring, Security, SNMP, Sonet DCC, Timing, Alarming
Inventory	Provides inventory information (part number, serial number, CLEI codes) for cards installed in the node. Allows you to delete and reset cards.	none
Maintenance	Perform maintenance tasks for the node	Database, Ether Bridge, Protection, Ring, Software, XC cards, Diagnostic, Timing, Audit, Routing Table

2.6.2 Network View

Network view (Figure 2-6) allows you to view and manage ONS 15454s and ONS 15327s that have DCC connections to the node that you logged into and any login node groups you may have selected. (Nodes with DCC connections to the login node will not display if you selected Exclude Dynamically Discovered Nodes on the Login dialog box.) The graphic area displays a background image with colored ONS 15454 icons. The icon colors indicate the node status (Table 2-6). Green lines show DCC connections between the nodes. Selecting a node or span in the graphic area displays information about the node and span in the status area.

Figure 2-6   A four-node network displayed in CTC network view

Icon color
indicates
node status

Dots indicate
the selected
node

Bold letters
indicate login
node; asterisk
indicates
topology host
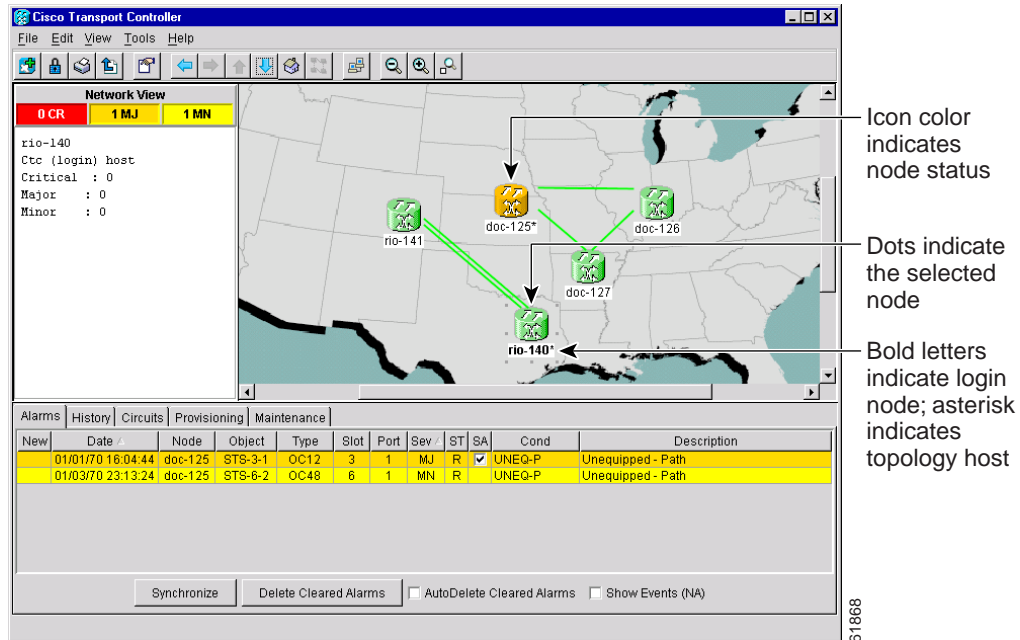
2.6.2.1 CTC Node Colors

The colors of nodes displayed in network view indicate the status of the node

Table 2-6   Node Status

Color	Alarm Status
Green	No alarms
Yellow	Minor alarms
Orange	Major alarms
Red	Critical alarms
Grey with node name	Node is initializing
Grey with IP address	Node is initializing, or a problem exists with IP routing from node to CTC

2.6.2.2 Network View Tasks

Right-click the network view graphic area or a node, span, or domain (domains are described in the "Creating Domains" section on page 2-17) to display shortcut menus. Table 2-7 lists the actions that are available from the network view.

Table 2-7   Performing Network Management Tasks in Network View

Action	Procedure
Open a node	Any of the following: • Double-click a node icon • Right-click a node icon, choose **Drill Down to Node** from the shortcut menu • Click a node and choose **Go to Selected Object View** from the CTC View menu • From the View menu, choose **Other Node**. Select a node from the Select Node dialog box • Double-click a node alarm or event in the Alarms or History tabs
Move a node icon	Press the **Ctrl** key and the left mouse button simultaneously and drag the node icon to a new location.
Reset node icon position	Right-click a node and choose **Reset Node Position** from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the Provisioning > General tabs in node view.
Provision a circuit	Right-click a node. From the shortcut menu, choose **Provision Circuit To** and select the node where you want to provision the circuit. For circuit creation procedures, see the "Create an Automatically Routed Circuit" section on page 6-2.
Update circuits with new node	Right-click a node and choose **Update Circuits With New Node** from the shortcut menu. Use this command when you add a new node and want to pass circuits through it.
Display a link end point	Right-click a span. On the shortcut menu, select **Go To [node/slot/port]** for the drop port you want to view. CTC displays the card in card view.
Display span properties	Any of the following: • Move mouse over a span; properties display above the span • Click a span; properties display in the upper left corner of the window • Right-click a span; properties display at the top of the shortcut menu
Perform a UPSR protection switch for an entire span	Right-click a network span and click **Circuits**. See the "Switch UPSR Traffic" section on page 5-32 for UPSR protection switch procedures.
Upgrade a span	Right-click a span and choose **Upgrade Span** from the shortcut menu. **Note** For detailed span upgrade information and instructions, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.

2.6.2.3 Creating Domains

Domains are icons where you can add a group of ONS 15454s or ONS 15327s. Adding domains to the network view map makes networks with many nodes easier to manage. After you create a domain, you can drag and drop ONS 15454 icons into it (Figure 2-7). The ONS 15454s are hidden until you open the domain. Figure 2-9 shows an example of an opened domain.

Figure 2-7   Adding nodes to a domain
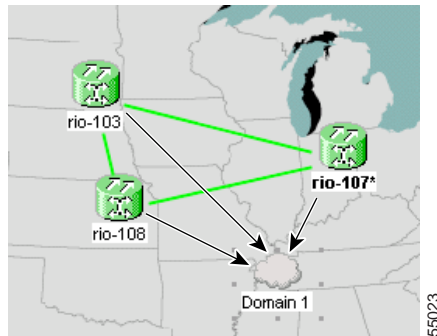
After you add a node to a domain, the span lines leading to nodes within the domain become thicker (Figure 2-8). The thick lines may represent multiple spans. For example, if the "rio-104" node in Figure 2-8 is connected to two nodes within domain-0, the thick line represents two spans. The thick line is green if all spans it represents are active and grey if any one span it represents is down. The domain icon color reflects the highest alarm severity of any node within it.

Figure 2-8   Outside nodes displayed within the domain
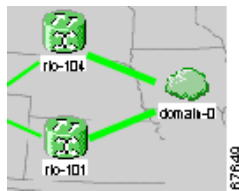
Within the domain, external nodes and domains that are directly connected to nodes inside the domain are displayed in a dimmed color (Figure 2-9). DCC links with one or two ends inside the domain are also displayed.

Figure 2-9   Nodes inside a domain
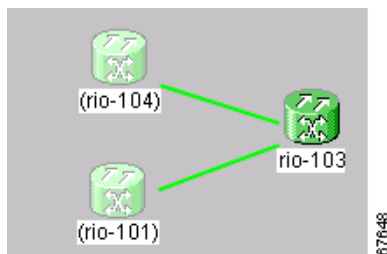
You manage ONS 15454s that reside within a domain the same way you manage ONS 15454s on the network map. Table 2-8 shows the domain actions.

Note   Domains you create will be seen by all users who log into the network.

Table 2-8   Managing Domains

Action	Procedure
Create a domain	Right-click the network map and choose **Create New Domain** from the shortcut menu. When the domain icon appears on the map, type the domain name.
Move a domain	Pressing **Ctrl**, drag the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose **Rename Domain** from the shortcut menu. Type the new name in the domain name field.
Add a node to a domain	Drag a node icon to the domain icon. Release the mouse button when the node icon is over the domain icon.
Move a node from a domain to the network map	Right-click a node.
Open a domain	• Double-click the domain icon. • Right-click the domain and choose **Drill Down to Domain**.
Return to network view	Right-click the domain view area and choose **Go to Parent View** from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose **Show Domain Overview**. The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, select **Show Domain Overview** again.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes residing in the domain are returned to the network map.

2.6.2.4 Changing the Network View Background Color

You can change the color of the network view background and the domain view background (the area displayed when you open a domain). If you modify background colors, the change is stored in your CTC user profile on the computer. The change does not affect other CTC users.

Procedure: Modify the Network or Domain Background Color

Step 1   Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.

Step 2   On the Choose Color dialog box, select a background color.

Step 3   Click **OK**.

2.6.2.5 Changing the Network View Background Image

You can replace the background map image displayed in network view with any JPEG or GIF image that is accessible on a local or network drive. If you want to position nodes on the map based on the node coordinates, you will need the longitudes and latitudes for the edges of the map. However, if you will use your mouse to position nodes, coordinates for the image edges are not necessary. The change does not affect other CTC users.

> **Note**   You can obtain the longitude and latitude for cities and Zip Codes from the U.S. Census Bureau U.S. Gazetteer website (http://www.census.gov/cgi-bin/gazetteer).

Procedure: Change the Network View Background Image

> ⚠ **Caution**   Before you begin this procedure, verify that the image file you want to use is located on your hard drive and is in JPEG or GIF format. CTC may stop responding if you link to a file that is not JPEG or GIF, or if you provide an incorrect path.

Step 1   In network view, choose **Edit > Preferences**. (You also right-click the network or domain map and select **Set Background Image**.)

Step 2   On the **General** tab of the Preferences dialog box (Figure 2-10), deselect **Use Default Map**.

Figure 2-10   Changing the CTC background image
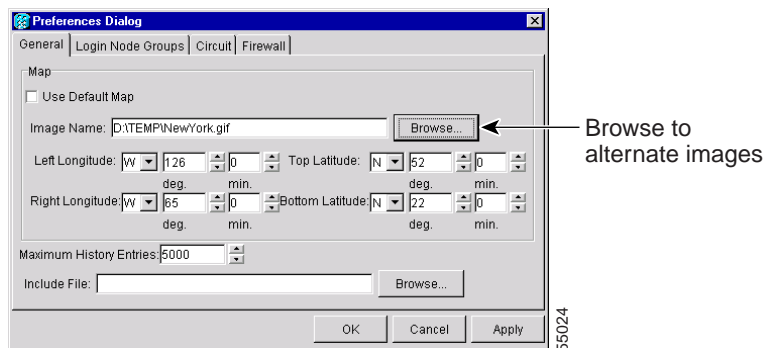
Step 3   Click **Browse**. Navigate to the graphic file you want to use as a background.

Step 4   Select the file. Click **Open**.

Step 5   (Optional) Enter the coordinates for the map image edges in the longitude and latitude fields on the Preferences dialog box. CTC uses the map's longitude and latitude to position the node icons based on the node coordinates entered for each node on the Provisioning > General tabs. Coordinates only need to be precise enough to place ONS node icons in approximate positions on the image. You can also drag and drop nodes to position them on the network view map.

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

Figure 2-11   Network view with a custom map image
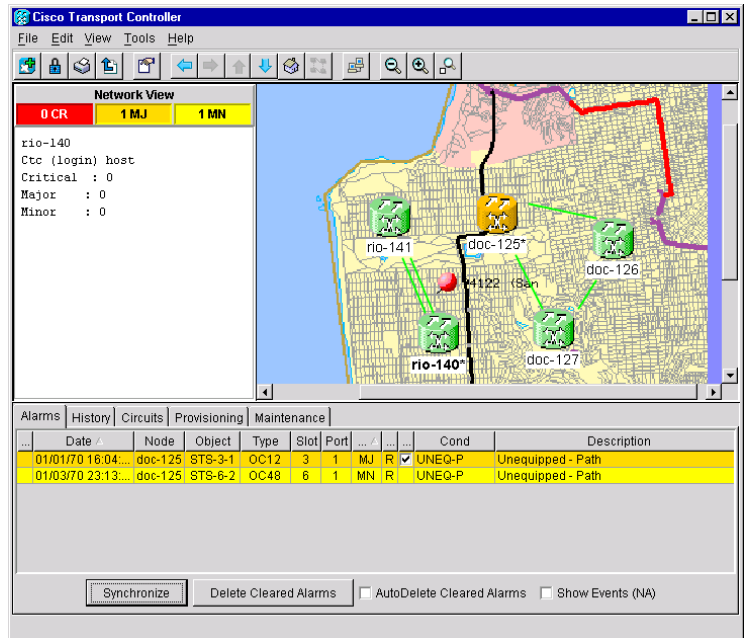
Step 7   At the network view, use the CTC toolbar Zoom buttons (or right-click the graphic area and select a Zoom command from the shortcut menu) to set the area of the image you can view.

Procedure: Add a Node to the Current Session

During a CTC session, you can add nodes that are not displayed in the session without having to log out of the session. When you add the node, you have the option to add it to the current login node group.

Step 1   From the CTC File menu, click **Add Node** (or click the Add Node button on the toolbar).

Step 2   On the Add Node dialog box, enter the node name (or IP address).

Step 3   If you want to add the node to the current login group, click **Add Node to Current Login Group**. Otherwise, leave it unchecked.

Step 4   Click **OK**.

After a few seconds, the new node will be displayed on the network view map.

2.6.3 Card View

Card view displays information about individual ONS 15454 cards and is the window where you perform card-specific maintenance and provisioning (Figure 2-12). A graphic of the selected card is shown in the graphic area. The status area displays the node name, slot, number of alarms, card type, equipment type, and either the card status (active or standby) or port status (IS [in service] or OOS [out of service]). The information that is displayed and the actions you can perform depend on the card.

Note   CTC displays a card view for all ONS 15454 cards except the TCC+, XC, XCVT, and XC10G cards.

Card view provides access to the following tabs: Alarms, History, Circuits, Provisioning, Maintenance, Performance, and Conditions. (The Performance tab is not displayed for the AIC card.) The subtabs, fields, and information displayed under each tab depend on the card type selected.

Figure 2-12   CTC card view showing an DS3N-12 card
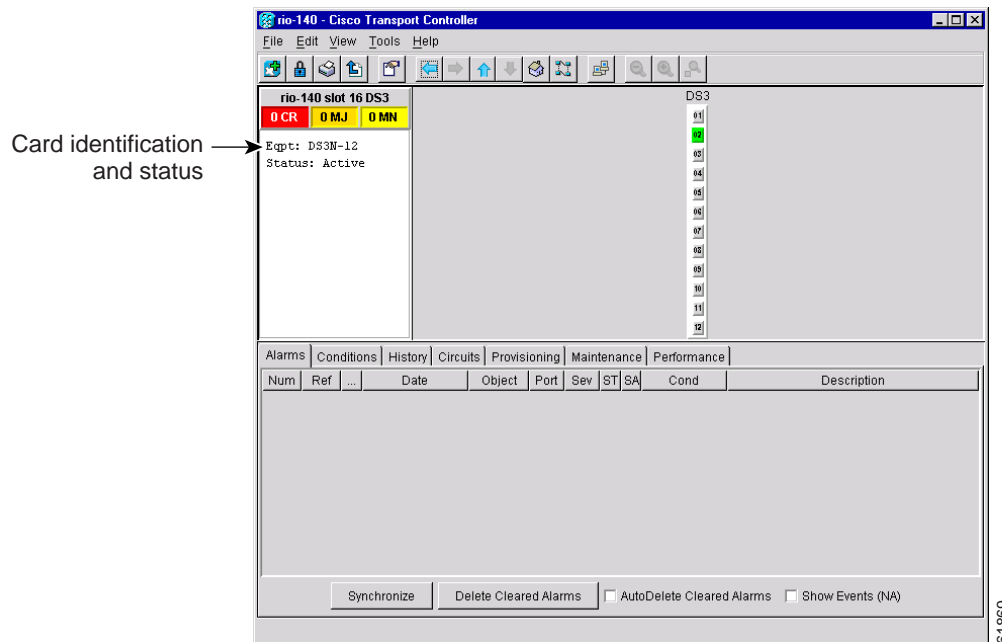
2.7 CTC Navigation

Different navigational methods are available within the CTC window to access views and perform management actions. Commands on the View menu and CTC toolbar allow you to quickly move between network, node, and card views. You can double-click and right-click objects in the graphic area and move the mouse over nodes, cards, and ports to view popup status information. Figure 2-13 shows an example.

Figure 2-13   CTC node view showing popup information
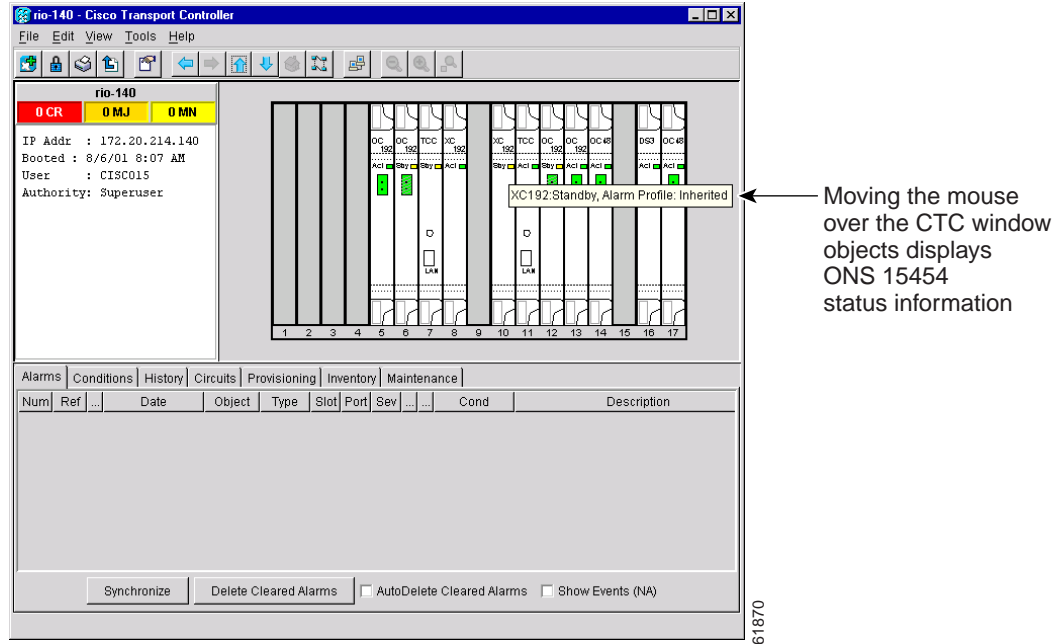
Table 2-9 describes different methods for navigating within the CTC window.

Table 2-9   CTC Window Navigation

Technique	Description
View menu and Toolbar	You can choose from: • The previous view (available after you navigate to two or more views) • The next view (available after you navigate to previous views) • The parent of the currently-selected view. Network is the parent of node view; node view is the parent of card view. • The currently selected object. For example, selecting a card on the node view graphic displays the card in card view; selecting a node on the network view map displays the node in node view. • The home view (the node you initially logged into) • The network view • The other node (View menu only) • Different zoom levels (toolbar only)
Double-Click	• A node in network view to display the node view • A card in node view to display the card view

Table 2-9   CTC Window Navigation (continued)

Technique	Description
Right-Click	• Network view graphic area—Displays a menu where you can create a new domain, change the position and zoom level of the graphic image, and change the background image and color. • Node in network view—Displays a menu where you can open the node, provision circuits, update circuits with a new node, and reset the node icon position to the longitude and latitude set on the Provisioning > General tabs. • Span in network view—Displays a menu where you can view information about the source and destination ports, the span's protection scheme, and the span's optical or electrical level. You can also display the Circuits on Span dialog box, which displays additional span information and allows you to perform UPSR protection switching. • Card in node view—Displays a menu where you can open, delete, reset, and change cards. The card that is selected determines the commands that are displayed.
Move Mouse Cursor	• Over node in network view—Displays a summary of node alarms and provides a warning if the node icon has been moved out of the map range. • Over span in network view—Displays circuit (node, slot, port) and protection information • Over card in node view—Displays card type and card status • Over card port in node view—Displays port number and port status

2.8 Viewing CTC Table Data

Much of the ONS 15454 data that CTC displays, such as alarms, alarm history, circuits, and inventory, is displayed in tables. You can change the way the CTC tables are displayed. For example, you can:

- Rearrange or hide table columns

- Sort tables by primary and secondary keys in descending or ascending order. (Sorting and hiding is available for all read-only tables.)

- Export CTC table data to spreadsheets and database management programs to perform additional data manipulation. To export table data, see the "Printing and Exporting CTC Data" section on page 2-26.

To change the display of a CTC table, left-click or right-click a column header in the table. Right-click a column header to display a shortcut menu that has table column display options (Figure 2-14).

Figure 2-14   Table shortcut menu that customizes table appearance
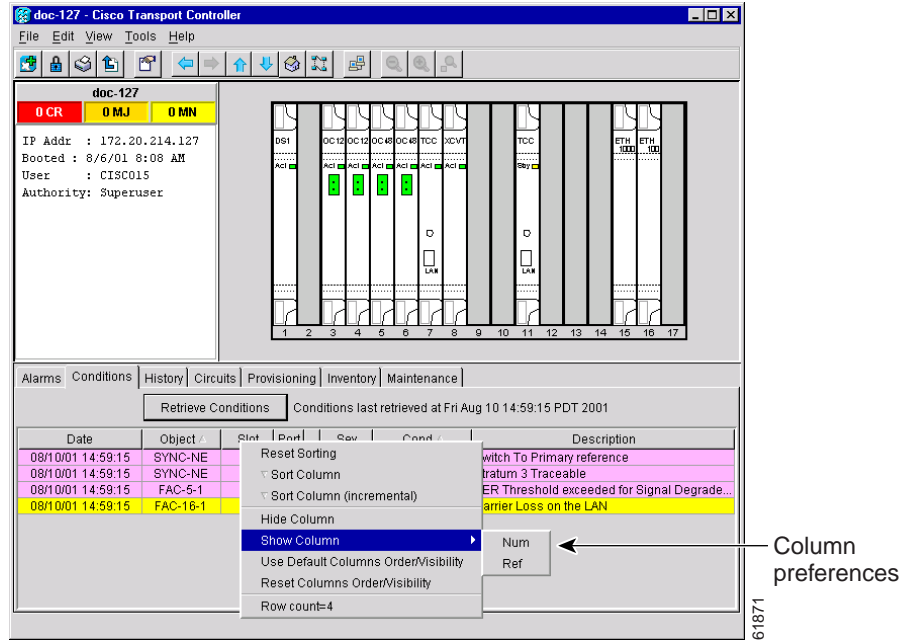
Table 2-10 lists the options that you can use to customize information that is displayed in CTC tables.

Table 2-10   Table Display Options

Task	Click	Right-Click Shortcut Menu
Resize column	Left click while dragging the header separator to the right or left	N/A
Rearrange column order	Left click while dragging the column header to the right or left	N/A
Reset column order	N/A	Choose Reset Columns Order/Visibility
Hide column	N/A	Choose Hide Column
Display a hidden column	N/A	Choose Show Column>[column name]
Display all hidden columns	N/A	Choose Reset Columns Order/Visibility
Sort table (primary)	Click a column header; each click changes sort order (ascending or descending)	Choose Sort Column
Sort table (secondary sorting keys)	Press the Shift key and simultaneously click the column header	Choose Sort Column (incremental)
Reset sorting	N/A	Choose Reset Sorting
View table row count	N/A	Choose Row count; it is the last item on the shortcut menu

2.9 Printing and Exporting CTC Data

You can print CTC windows and table data such as alarms and inventory. You can also export CTC table data for use by other applications such as spreadsheets, word processors, and database management applications. Table 2-11 shows CTC data that can be exported.

Table 2-11   Table Data with Export Capability

View or Card	Tab	Subtab(s)
Network	Alarms	
	History	
	Circuits	
	Provisioning	Alarm Profiles
	Maintenance	Software
Node	Alarms	
	Conditions	
	History	Session/Node
	Circuits	
	Provisioning	Ether Bridge (Spanning Trees/Thresholds)
		Network (General/Static Routes/OSPF)
		Ring
		Alarm Behavior
	Inventory	
	Maintenance	Ether Bridge (Spanning Trees/MAC Table/Trunk Utilization)
		Ring
		Software
		Audit
		Routing Table
		Test Access
OC-N Cards	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	Line/Threshold/STS/Alarm Behavior
	Maintenance	Loopback
	Performance	
DS-N Cards	Alarms	
	Conditions	
	History	Session/Card
	Circuits	

Table 2-11   Table Data with Export Capability (continued)

View or Card	Tab	Subtab(s)
	Provisioning	Line/Alarm Behavior
AIC Card	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	External Alarms/External Controls
	Maintenance	External Alarms/External Controls/Virtual Wires
EC1-12	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	Line/Threshold/STS/Alarm Behavior
	Maintenance	
	Performance	
DS3XM-6	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	Line/Alarm Behavior
	Maintenance	DS-1/DS-3/Performance
E100T-12/E1000-2/ E100T-12-G/E1000-2-G	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	Port/VLAN/Alarm Behavior
	Performance	Statistics/Utilization/History

Procedure: Print CTC Window and Table Data

Use the following procedure to print CTC windows and table data. Before you start, make sure your PC is connected to a printer.

Step 1   From the CTC File menu, click **Print**.

Step 2   In the Print dialog (Figure 2-15) choose an option:

- *Entire Frame*—Prints the entire CTC window
- *Tabbed View*—Prints the lower half of the CTC window

- *Table Contents*—Prints CTC data in table format; this option is only available for CTC table data (see the "Viewing CTC Table Data" section on page 2-24).

Figure 2-15   Selecting CTC data for print
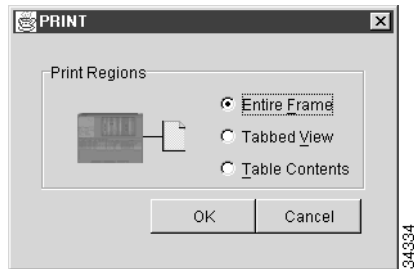
Step 3   Click **OK**.

Step 4   In the Windows Print dialog, choose a printer and click **Print**.

Procedure: Export CTC Data

Step 1   From the CTC File menu, click **Export**.

Step 2   In the Export dialog (Figure 2-16) choose a format for the data:

- *As HTML*—Saves the data as an HTML file. The file can be viewed with a web browser without running CTC.

- *As CSV*—Saves the CTC table values as text, separated by commas. You can import CSV data into spreadsheets and database management programs.

- *As TSV*—Saves the CTC table values as text, separated by tabs. You can import TSV data into spreadsheets and database management programs.

Figure 2-16   Selecting CTC data for export
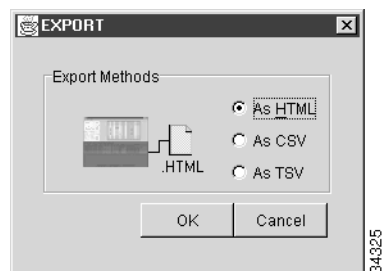
Step 3   Click **OK**.

Step 4   In the Save dialog, enter a file name in one of the following formats:

- *[filename].htm* for HTML files
- *[filename].csv* for CSV files
- *[filename].tsv* for TSV files

Step 5   Navigate to a directory where you want to store the file.

Step 6   Click **OK**.

2.10 Displaying CTC Data in Other Applications

CTC data exported in HTML format can be viewed with any web browser, such as Netscape Navigator or Microsoft Internet Explorer. To display the data, use the browser's File/Open command to open the CTC data file.

CTC data exported as comma separated values (CSV) or tab separated values (TSV) can be viewed in text editors, word processors, spreadsheets, and database management applications. Although procedures depend on the application, you typically can use File/Open to display the CTC data. Text editors and word processors display the data exactly as it is exported. Spreadsheet and database management applications display the data in cells. You can then format and manage the data using the spreadsheet or database management application tools.

In addition to the CTC exporting, CTC text information can be copied and pasted into other applications using the Windows Copy (Ctrl+C), Cut (Ctrl+X) and Paste (Ctrl+V) commands.

Cisco ONS 15454 Installation and Operations Guide

Node Setup

This chapter explains how to set up a Cisco ONS 15454 node using the Cisco Transport Controller (CTC). Topics include:

- Setting up general node information
- Preparing the ONS 15454 to connect to networks
- Changing the node IP address, default router, and subnet mask using the LCD
- Creating, editing, and deleting ONS 15454 users and assigning user security levels
- Setting the node timing references
- Creating card protection groups
- Viewing node inventory
- Viewing CTC software versions

Lastly, the chapter includes a node checklist to help you keep track of the procedures you have performed. See Chapter 2, "Software Installation" for general CTC information.

3.1 Before You Begin

Before you begin node setup, review the following checklist to ensure you have the perquisite information. Basic node information that you will provide need includes node name, contact, location, date, and time. If the ONS 15454 will be connected to a network, you will need:

- The IP address and subnet mask to assign to the node and
- The IP address of the default router.
- If Dynamic Host Configuration Protocol is used, you will need the IP address of the DHCP server.

If you are responsible for setting up IP networking for the ONS 15454 network, see Chapter 4, "IP Networking" for more information.

To create card protection groups, you will need to know:

- The card protection scheme that will be used and what cards will be included in it.
- The SONET protection topology that will be used for the node.

Note You must be able to log into the node to complete node provisioning. If you cannot log into the node, see "Connecting PCs to the ONS 15454" section on page 2-5.

3.2 Setting Up Basic Node Information

Setting basic information for each Cisco ONS 15454 node is one of the first provisioning tasks you perform. This information includes node name, location, contact, and timing. Completing the information for each node facilitates ONS 15454 management, particularly when the node is connected to a large ONS 15454 network.

Procedure: Add the Node Name, Contact, Location, Date, and Time

Step 1   Log into the ONS 15454 node. The CTC node view is displayed.

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

Step 3   Enter the following:

- *Node Name*—Type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric characters.

- *Contact*—Type the name of the node contact person and the phone number (optional).

- *Location*—Type the node location (optional) (such as a city name or specific office location).

- *Latitude*—Enter the node latitude: N (North) or S (South), degrees, and minutes.

- *Longitude*—Enter the node longitude: E (East) or W (West), degrees, and minutes.

  CTC uses the latitude and longitude to position node icons on the network view map. (You can also position nodes manually.) To convert a coordinate in degrees to degrees and minutes, multiply the number after the decimal by 60. For example, the latitude 38.250739 converts to 38 degrees, 15 minutes (.250739 x 60 = 15.0443, rounded to the nearest whole number).

- *Use SNTP Server*—When checked, CTC uses a Simple Network Time Protocol (SNTP) server to set the date and time of the node. Using an SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades. If you check *Use SNTP Server*, type the server's IP address in the next field. If you do not use an SNTP server, complete the *Date*, *Time,* and *Time Zone* fields. The ONS 15454 will use these fields for alarm dates and times. (CTC displays all alarms in the login node's time zone for cross network consistency.)

- *Date*—Type the current date.

- *Time*—Type the current time.

- *Time Zone*—Select the time zone.

Step 4   Click **Apply**.

3.3 Setting Up Network Information

ONS 15454s almost always operate in network environments. Before you connect an ONS 15454 to other ONS 15454s or to a LAN, you must change the default IP address that is shipped with each ONS 15454 (192.1.0.2). IP addresses are unique identifiers for devices—called hosts—that connect to TCP/IP networks. Every IP address includes a network number, which is assigned to an organization, and a host (device) number, which the organization's LAN administrator assigns to an individual network device.

Subnetting enables LAN administrators to create subnetworks that are transparent to the Internet. Within networks, ONS 15454s often exist as subnetworks, which are created by adding a subnet mask to the ONS 15454 IP address.

The following procedure tells you how to set up the essential ONS 15454 networking information. Additional ONS 15454 networking information and procedures, including IP addressing examples, static route scenarios and Open Shortest Path First (OSPF) protocol options are provided in Chapter 3, "IP Networking."

Procedure: Set Up Network Information

Step 1   From the CTC node view, click the **Provisioning** > **Network** tabs (Figure 3-1).

Step 2   Complete the following:

- *IP Address*—Type the IP address assigned to the ONS 15454 node.

- *Prevent LCD IP Config*—If checked, prevents the ONS 15454 IP address from being changed using the LCD. See the "Change IP Address, Default Router, and Network Mask Using the LCD" procedure on page 3-4.

- *Default Router*—If the ONS 15454 must communicate with a device on a network to which the ONS 15454 is not connected, the ONS 15454 forwards the packets to the default router. Type the IP address of the router in this field. If the ONS 15454 is not connected to a LAN, leave the field blank.

- *Subnet Mask Length*—If the ONS 15454 is part of a subnet, type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15454s in the same subnet.

Note   The MAC Address is read only. It displays the ONS 15454 address as it is identified on the IEEE 802 Media Access Control (MAC) layer.

- *Forward DHCP Request To*—When checked, forwards Dynamic Host Configuration Protocol requests to the IP address entered in the Request To field. DHCP is a TCP/IP protocol that enables CTC computers to get temporary IP addresses from a server. If you enable DHCP, CTC computers that are directly connected to an ONS 15454 node can obtain temporary IP addresses from the DHCP server.

- *TCC CORBA (IIOP) Listener Port*—Sets a listener port to allow communication with the ONS 15454 through firewalls. See the "Accessing ONS 15454s Behind Firewalls" section on page 2-12 for more information.

Figure 3-1   Setting up general network information
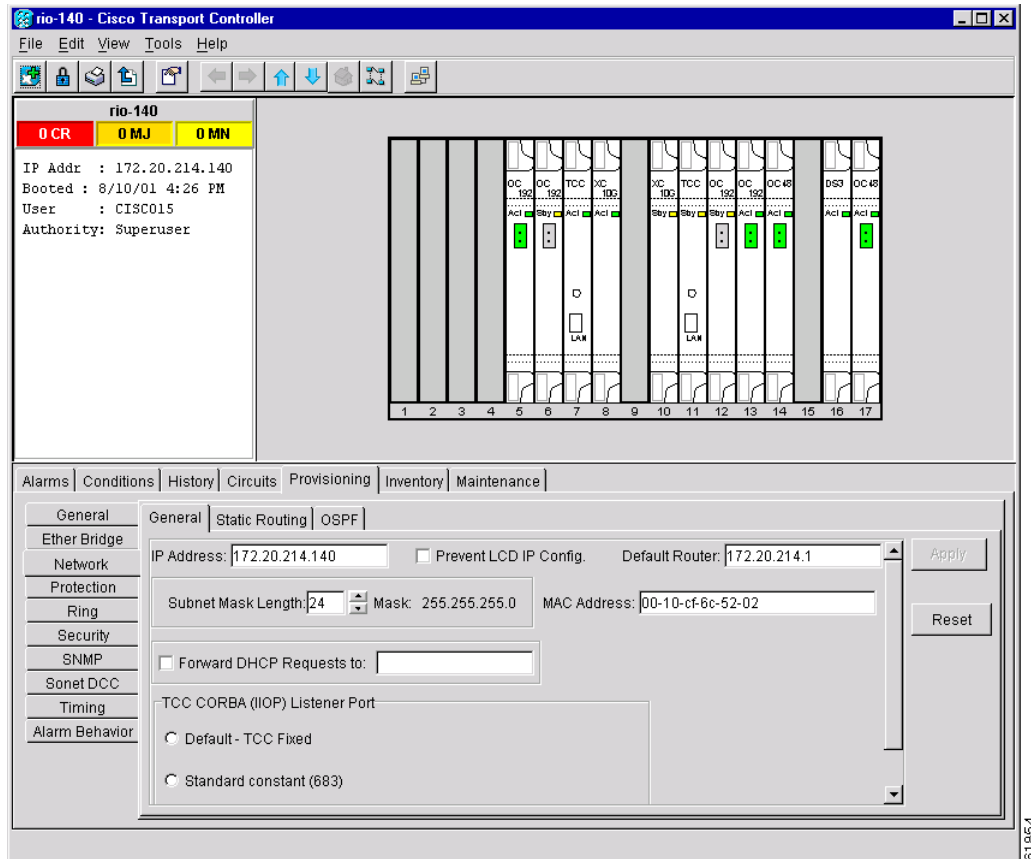
Step 3   Click **Apply**.

Step 4   Click **Yes** on the confirmation dialog box.

Both ONS 15454 TCC+ cards will reboot, one at a time.

Procedure: Change IP Address, Default Router, and Network Mask Using the LCD

You can change the ONS 15454 IP address, subnet mask, and default router address using the Slot, Status, and Port buttons on the front panel LCD.

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 3-2)
- To change the node network mask, Status=Net Mask
- To change the default router IP address, Status=Default Rtr

Figure 3-2   Selecting the IP address option

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

Slot-0
Status=IpAddress

44089
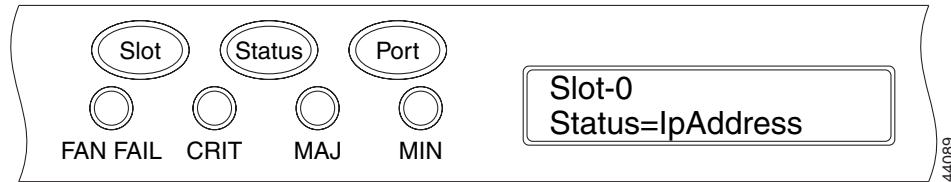
Step 3   Press the **Status** button to display the node IP address (Figure 3-3), the node subnet mask length, or default router IP address.

Figure 3-3   Changing the IP address

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

172.020.214.107
<Next   Done   Mod>

44090
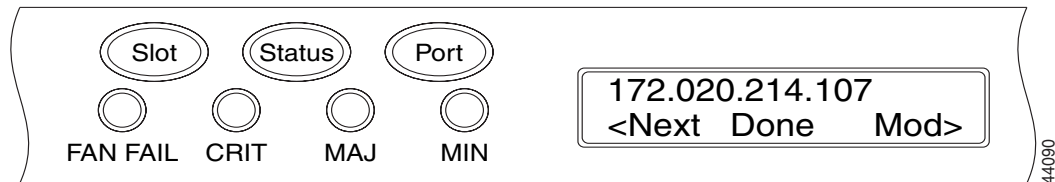
Step 4   Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.

Step 5   Press the **Port** button to cycle the IP address or subnet mask digit 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 3-4).

Figure 3-4   Selecting the Save Configuration option

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

Slot-0
Status=Save Cfg.

44091
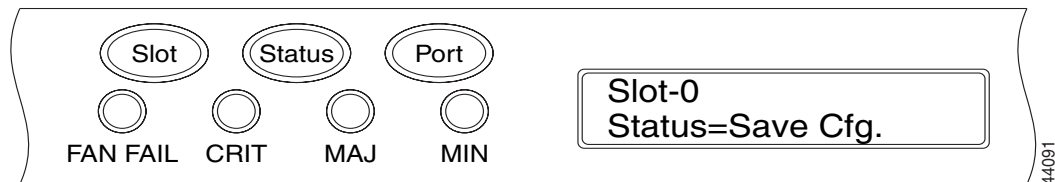
Step 8   Press the **Status** button to select the Save Configuration option.

A Save and REBOOT message appears (Figure 3-5).

Figure 3-5   Saving and rebooting the TCC+

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

Save and REBOOT?
<Apply   Revert>

44092
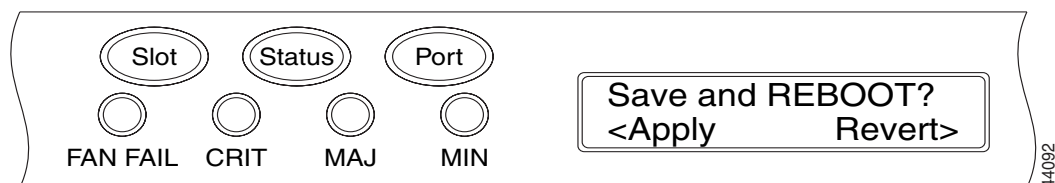
Step 9   Press the **Slot** button to save the new IP address configuration. (Or press **Port** to cancel the configuration.)

Saving the new configuration causes the TCC+ 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
TCC+ reboot is complete.

3.4 Creating Users and Setting Security

The CISCO15 user provided with each ONS 15454 can be used to set up other ONS 15454 users. You
can add up to 500 users to one ONS 15454. Each ONS 15454 user can be assigned one of the following
security levels:

- *Retrieve* users can retrieve and view CTC information but cannot set or modify parameters.
- *Maintenance* users can access only the ONS 15454 maintenance options.
- *Provisioning* users can access provisioning and maintenance options.
- *Superusers* can perform all of the functions of the other security levels as well as set names,
  passwords, and security levels for other users.

Table 3-1 shows the actions that each user can perform in node view.

Table 3-1   ONS 15454 Security Levels—Node View

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	n/a	Synchronize alarms	X	X	X	X
Conditions	n/a	Retrieve	X	X	X	X
History	Session	Read only				
	Node	Retrieve Alarms/Events	X	X	X	X
Circuits	n/a	Create/Delete/Edit/ Upgrade			X	X
		Path Selector Switching		X	X	X
		Search	X	X	X	X
		Switch retrieval	X	X	X	X
Provisioning	General	Edit				X
	EtherBridge	Spanning Trees: Edit			X	X
		Thresholds: Create/Delete			X	X
	Network	All				X
	Protection	Create/Delete/Edit			X	X
		Browse groups	X	X	X	X
	Ring	All (BLSR)			X	X
	Security	Create/Delete				X
		Change password	same user	same user	same user	all users
	SNMP	Create/Delete/Edit				X
		Browse trap destinations	X	X	X	X
	Sonet DCC	Create/Delete				X
	Timing	Edit			X	X

Table 3-1   ONS 15454 Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
	Alarming	Edit			X	X
Inventory	n/a	Delete			X	X
		Reset		X	X	X
Maintenance	Database	Backup/Restore				X
	EtherBridge	Spanning Tree Retrieve	X	X	X	X
		Spanning Tree Clear/Clear all		X	X	X
		MAC Table Retrieve	X	X	X	X
		MAC Table Clear/Clear all		X	X	X
		Trunk Utilization Refresh	X	X	X	X
	Protection	Switch/lock out operations		X	X	X
	Ring	BLSR maintenance		X	X	X
	Software	Download/Upgrade/ Activate/Revert				X
	XC Cards	Protection switches		X	X	X
	Diagnostic	Retrieve/Lamp test		X	X	X
	Timing	Edit		X	X	X
	Audit	Retrieve	X	X	X	X
	Routing Table	Read only				
	Test Access	Read only				

Each ONS 15454 user has a specified amount of time that he or she can leave the system idle before the CTC window is locked. The lockouts prevent unauthorized users from making changes. Higher-level users have shorter idle times, as shown in Table 3-2.

Table 3-2   ONS 15454 User Idle Times

Security Level	Idle Time
Superuser	15 minutes
Provisioning	30 minutes
Maintenance	60 minutes
Retrieve	Unlimited

You can perform ONS 15454 user management tasks from network or node view. In network view, you can add, edit, or delete users from multiple nodes at one time. If you perform user management tasks in node view, you can only add, edit, or delete users from that node.

Note   You must add the same user name and password to each node the user will access.

Procedure: Create New Users

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

Step 2   On the Security pane, click **Create**.

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

- *Name*—Type the user name.
- *Password*—Type the user password. The password must be a minimum of six and a maximum of ten alphanumeric (a-z, A-Z, 0-9) and special characters (+, #, %), where at least two characters are non-alphabetic and at least one character is a special character.
- *Confirm Password*—Type the password again to confirm it.
- *Security Level*—Select the user's security level.

Step 4   Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected by default).

Step 5   Click **OK**.

Procedure: Edit a User

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

Step 2   Click **Change**.

Step 3   On the Change User dialog box, edit the user information: name, password, password confirmation, and/or security level. (A Superuser does not need to enter an old password. Other users must enter their old password when changing their own passwords.)

> ✎
>
> **Note**   You cannot change the CISCO15 user name.

Step 4   If you do not want the user changes to apply to all network nodes, deselect the unchanged nodes in the Change Users dialog box.

Step 5   Click **OK**.

Changed user permissions and access levels do not take effect until the user logs out of CTC and logs back in.

Procedure: Delete a User

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

Step 2   Click **Delete**.

Step 3   On the Delete User dialog box, enter the name of the user you want to delete.

Step 4   If you do not want to delete the user from all network nodes, deselect the nodes.

Step 5   Click **OK** and click **Apply**.

3.5 Creating Protection Groups

The ONS 15454 provides several card protection methods. When you set up protection for ONS 15454 cards, you must choose between maximum protection and maximum slot availability. The highest protection reduces the number of available card slots; the highest slot availability reduces the protection. Table 3-3 shows the protection types that can be set up for ONS 15454 cards.

Table 3-3   Protection Types

Type	Cards	Description
1:1	DS-1 DS-3 EC-1-12 DS3XM-6	Pairs one working card with one protect card. Install the protect card in an odd-numbered slot and the working card in an even-numbered slot next to the protect slot towards the center, for example: protect in Slot 1, working in Slot 2; protect in Slot 3, working in Slot 4; protect in Slot 15, working in Slot 14.
1:N	DS-1 DS-3	Assigns one protect card for several working cards. The maximum is 1:5. Protect cards (DS1N-14, DS3N-12) must be installed in Slots 3 or 15 and the cards they protect must be on the same side of the shelf. Protect cards must match the cards they protect. For example, a DS1N-14 can only protect DS1-14 or DS1N-14 cards. If a failure clears, traffic reverts to the working card after the reversion time has elapsed.
1+1	Any optical	Pairs a working optical port with a protect optical port. Protect ports must match the working ports. For example, Port 1 of an OC-3 card can only be protected by Port 1 of another OC-3 card. Cards do not need to be in adjoining slots.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. However, because no card slots are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15454. Unprotected is the default protection type.

Procedure: Create Protection Groups

Step 1   From the CTC node view, click the **Provisioning** > **Protection** tabs.

Step 2   Under Protection Groups, click **Create**.

Step 3   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 alpha-numeric characters.

- *Type*—Choose the protection type: 1:1, 1:N, or 1+1. The protection selected determines the cards that are available to serve as protect and working cards. For example, if you choose 1:N protection, only DS-1N and DS-3N cards are displayed.

- *Protect Card or Port*—Choose the protect card (if using 1:1 or 1:N) or protect port (if using 1+1) from the list.

Based on these selections, a list of available working cards or ports is displayed under Available Cards or Available Ports. Figure 3-6 shows a 1+1 protection group.

Figure 3-6   Creating a 1+1 protection group
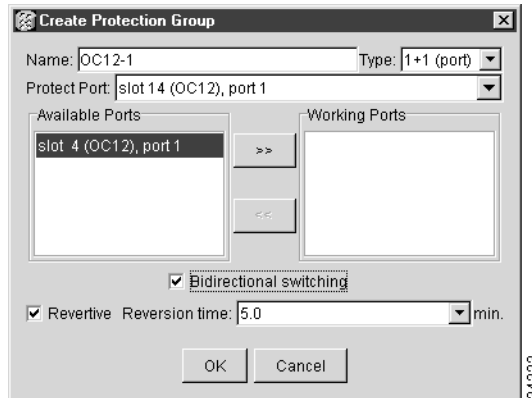
Step 4   From the Available Cards or Available Ports list, choose the card or port that you want to be the working card or port (the card(s) or port(s) that will be protected by the card or port selected in Protect Cards or Protect Ports). Click the top arrow button to move each card/port to the Working Cards or Working Ports list.

Step 5   Complete the remaining fields:

- *Bidirectional switching*—(optical cards only) click if you want both the transmit and the receive channels to switch if a failure occurs to one.

- *Revertive*—if checked, the ONS 15454 reverts traffic to the working card or port after failure conditions stay corrected for the amount of time entered in Reversion Time.

- *Reversion time*—if Revertive is checked, enter the amount of time following failure condition correction that the ONS 15454 should switch back to the working card or port.

Step 6   Click **OK**.

Note   To convert protection groups, see the "Converting DS-1 and DS-3 Cards From 1:1 to 1:N Protection" section on page 7-30.

Card protection does not take effect until you enable the ports on all the cards in the protection group. Because ports must be enabled before the cards carry traffic, you can enable the ports immediately after provisioning card protection, or wait until you are ready to send traffic on the cards.

Caution   Before running traffic on a card within a protection group, enable the ports of all protection group cards.

Procedure: Enable Ports

Step 1   Log into the node in CTC and display the card you want to enable in card view.

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

Step 3   Change the port status to In Service.

Step 4   Click **Apply**.

Procedure: Edit Protection Groups

Step 1   From the CTC node view, click the **Provisioning** > **Protection** tabs (Figure 3-7).

Figure 3-7   Editing protection groups
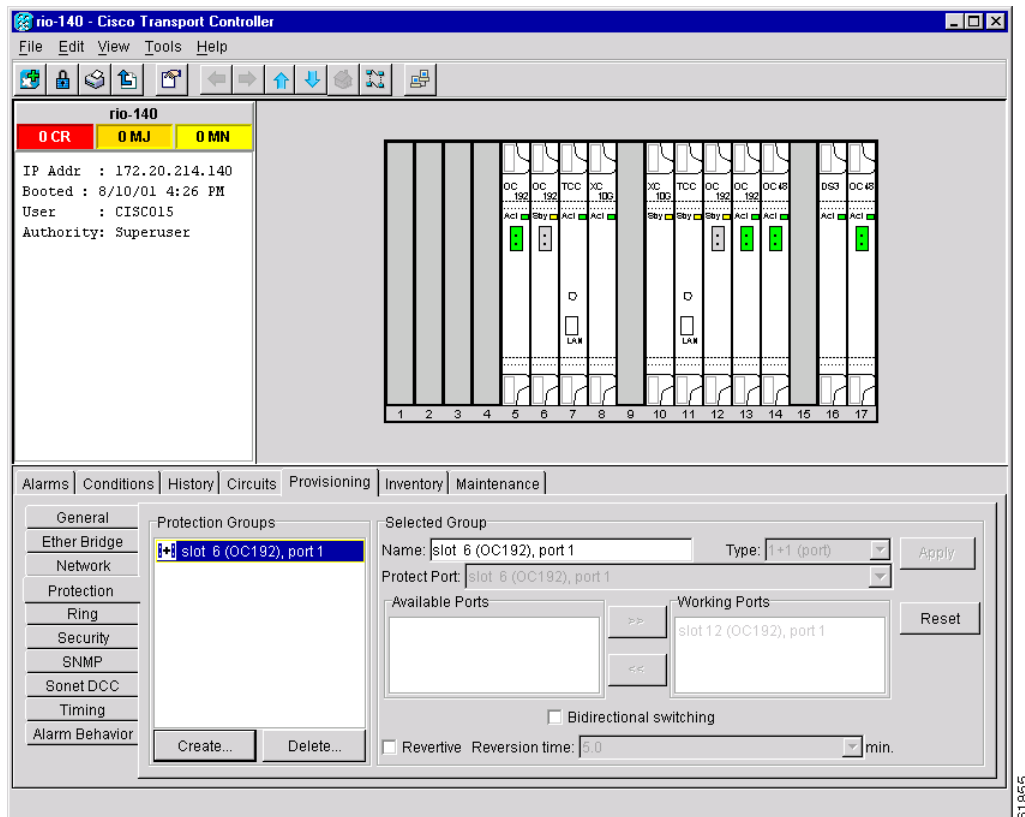
Step 2   In the Protection Groups section, choose a protection group.

Step 3   In the Selected Group section, edit the fields as appropriate. (For field descriptions, see the "Create Protection Groups" procedure on page 3-9.)

Step 4   Click **Apply**.

Procedure: Delete Protection Groups

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

Step 2   Verify that working traffic is not running on the protect card:

   a. In the Protection Groups section, choose the group you want to delete.

   b. In the Selected Group section, verify that the protect card is in standby mode. If it is in standby mode, continue with Step 3. If it is active, complete Step c.

   c. If the working card is in standby mode, manually switch traffic back to the working card. In the Selected Group pane, click the working card, then click **Manual**. Verify that the protect card switches to standby mode and the working card is active. If it does, continue with Step 3. If the protect card is still active, do not continue. Begin troubleshooting procedures or call technical support.

Step 3   From the node view, click the **Provisioning** > **Protection** tabs.

Step 4   In the Protection Groups section, click a protection group.

Step 5   Click **Delete**.

3.6 Setting Up ONS 15454 Timing

SONET timing parameters must be set for each ONS 15454. Each ONS 15454 independently accepts its timing reference from one of three sources:

- The BITS (Building Integrated Timing Supply) pins on the ONS 15454 backplane
- An OC-N card installed in the ONS 15454. The card is connected to a node that receives timing through a BITS source.
- The internal ST3 clock on the TCC+ card

You can set ONS 15454 timing to one of three modes: external, line, or mixed. If timing is coming from the BITS pins, set ONS 15454 timing to external. If the timing comes from an OC-N card, set the timing to line. In typical ONS 15454 networks:

- One node is set to external. The external node derives its timing from a BITS source wired to the BITS backplane pins. The BITS source, in turn, derives its timing from a Primary Reference Source (PRS) such as a Stratum 1 clock or GPS signal.
- The other nodes are set to line. The line nodes derive timing from the externally-timed node through the OC-N trunk cards.

You can set three timing references for each ONS 15454. The first two references are typically two BITS-level sources, or two line-level sources optically connected to a node with a BITS source. The third reference is the internal clock provided on every ONS 15454 TCC+ card. This clock is a Stratum 3 (ST3). If an ONS 15454 becomes isolated, timing is maintained at the ST3 level.

⚠
Caution   Mixed timing allows you to select both external and line timing sources. However, Cisco does not recommend its use because it can create timing loops. Use this mode with caution.

3.6.1 Network Timing Example

Figure 3-8 shows an ONS 15454 network timing setup example. Node 1 is set to external timing. Two timing references are set to BITS. These are Stratum 1 timing sources wired to the BITS input pins on the Node 1 backplane. The third reference is set to internal clock. The BITS output pins on the backplane of Node 3 are used to provide timing to outside equipment, such as a Digital Access Line Access Multiplexer.

In the example, Slots 5 and 6 contain the trunk cards. Timing at Nodes 2, 3, and 4 is set to line, and the timing references are set to the trunk cards based on distance from the BITS source. Reference 1 is set to the trunk card closest to the BITS source. At Node 2, Reference 1is Slot 5 because it is connected to Node 1. At Node 4, Reference 1 is set to Slot 6 because it is connected to Node 1. At Node 3, Reference 1 could be either trunk card because they are equal distance from Node 1.

Figure 3-8   An ONS 15454 timing example
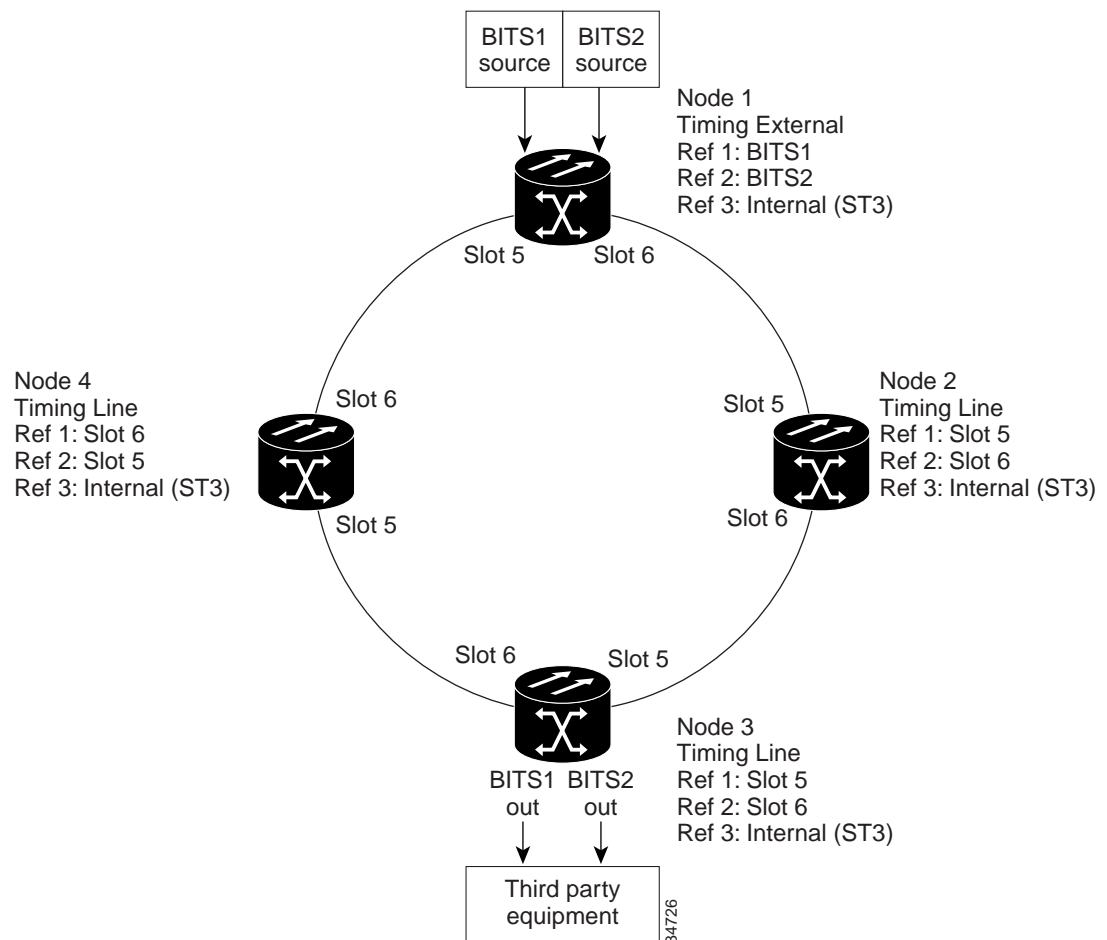
3.6.2 Synchronization Status Messaging

Synchronization Status Messaging (SSM) is a SONET protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SONET Line layer. They enable SONET devices to automatically select the highest quality timing reference and to avoid timing loops.

SSM messages are either Generation 1 or Generation 2. Generation 1 is the first and most widely deployed SSM message set. Generation 2 is a newer version. If you enable SSM for the ONS 15454, consult your timing reference documentation to determine which message set to use. Table 3-4 and Table 3-5 show the Generation 1 and Generation 2 message sets.

Table 3-4   SSM Generation 1 Message Set

Message	Quality	Description
PRS	1	Primary reference source – Stratum 1
STU	2	Sync traceability unknown
ST2	3	Stratum 2
ST3	4	Stratum 3
SMC	5	SONET minimum clock
ST4	6	Stratum 4
DUS	7	Do not use for timing synchronization
RES		Reserved; quality level set by user

Table 3-5   SSM Generation 2 Message Set

Message	Quality	Description
PRS	1	Primary reference source - Stratum 1
STU	2	Sync traceability unknown
ST2	3	Stratum 2
TNC	4	Transit node clock
ST3E	5	Stratum 3E
ST3	6	Stratum 3
SMC	7	SONET minimum clock
ST4	8	Stratum 4
DUS	9	Do not use for timing synchronization
RES		Reserved; quality level set by user

Procedure: Set up ONS 15454 Timing

Step 1   From the CTC node view, click the **Provisioning > Timing** tabs (Figure 3-9).

Step 2   In the General Timing section, complete the following information:

- *Timing Mode*—Set to External if the ONS 15454 derives its timing from a BITS source wired to the backplane pins; set to Line if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references. (Because Mixed timing may cause timing loops, Cisco does not recommend its use. Use this mode with care.)

- *SSM Message Set*—Choose the message set level supported by your network. If a Generation 1 node receives a Generation 2 message, the message will be mapped down to the next available Generation 1. For example, an ST3E message becomes an ST3.

- *Quality of RES*—If your timing source supports the reserved S1 byte, you 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. See Table 3-4 and Table 3-5 for more information.

- *Revertive*—If checked, the ONS 15454 reverts 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, indicate the amount of time the ONS 15454 will wait before reverting back to its primary timing source.

Step 3   In the BITS Facilities section, complete the following information:

✎
Note   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.

- *State*—Set the BITS reference to IS (In Service) or OOS (Out of Service). For nodes set to Line timing with no equipment timed through BITS Out, set State to OOS. For nodes using External timing or Line timing with equipment timed through BITS Out, set State to IS.

- *Coding*—Set to the coding used by your BITS reference, either B8ZS or AMI.

- *Framing*—Set to the framing used by your BITS reference, either ESF (Extended Super Frame, or SF (D4) (Super Frame). SSM is not available with Super Frame.

- *Sync Messaging*—Check to enable SSM.

- *AIS Threshold*—Sets the quality level where a node sends an Alarm Indication Signal (AIS) from the BITS 1 Out and BITS 2 Out backplane pins. When a node times at or below the AIS Threshold quality, AIS is sent (used when SSM is disabled or frame is SF).

Step 4   Under Reference Lists, complete the following information:

✎
Note   Reference lists 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, Ref3). The node uses Reference 1 unless a failure occurs to that reference, in which case, the node uses Reference 2. If that fails, the node uses Reference 3, which is typically set to Internal Clock. This is the Stratum 3 clock provided on the TCC+. The options displayed depend on the Timing Mode setting.

    - Timing Mode set to External—options are BITS1, BITS2, and Internal Clock.

- Timing Mode set to Line—options are the node's working optical cards and Internal Clock. Select the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, select Slot 5 as Reference 1.

- Timing Mode set to Mixed—both BITS and optical cards are available, allowing you to set a mixture of external BITS and optical trunk cards as timing references.

- *BITS 1 Out/BITS 2 Out*—Define the timing references for equipment wired to the BITS Out backplane pins. Normally, BITS Out is used with Line nodes, so the options displayed are the working optical cards. BITS 1 and BITS 2 Out are enabled as soon as BITS-1 and BITS-2 facilities are placed in service.

Figure 3-9   Setting Up ONS 15454 timing
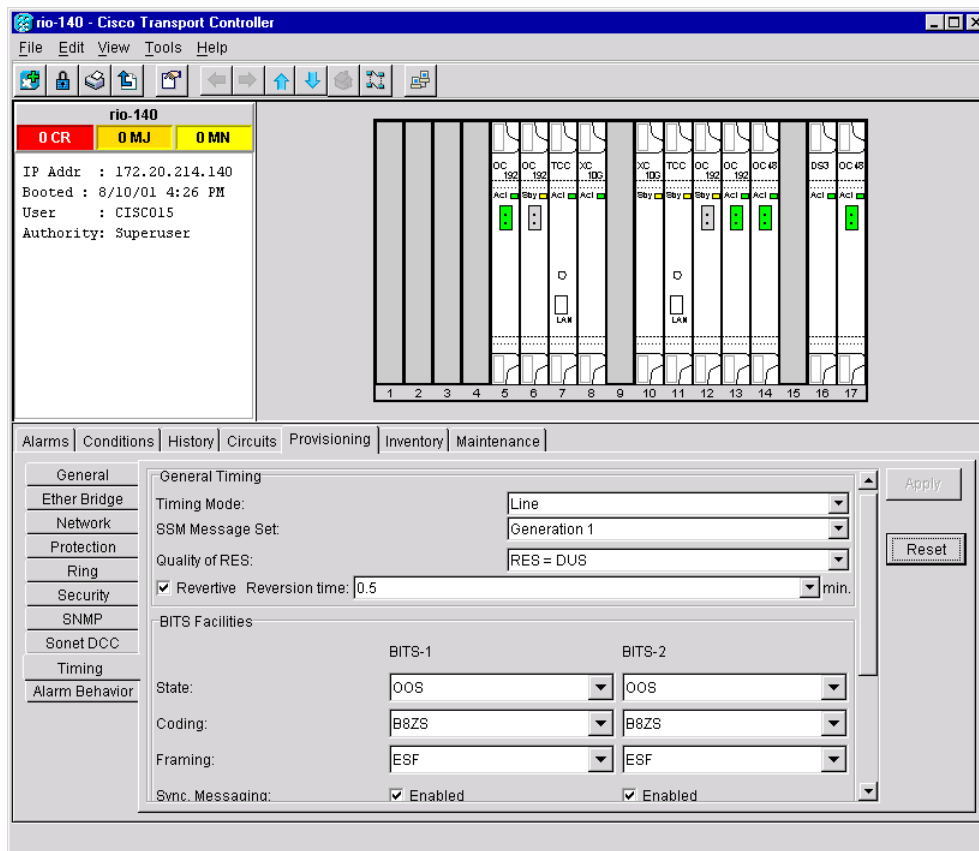
Step 5   Click **Apply**.

✎

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

Procedure: Set Up Internal Timing

If no BITS source is available, you can set up internal timing by timing all nodes in the ring from the internal clock of one node.

⚠
Caution   Internal timing is Stratum 3 and not intended for permanent use. All ONS 15454s should be timed to a Stratum 2 or better primary reference source.

Step 1   Log into the node that will serve as the timing source.

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

Step 3   In the General Timing section, enter the following:

- *Timing Mode*—Set to External.
- *SSM Message Set*—Set to Generation 1.
- *Quality of RES*—Set to DUS.
- *Revertive*—Is not relevant for internal timing; the default setting (checked) is sufficient.
- *Revertive Time*—The default setting (5 minutes) is sufficient.

Step 4   In the BITS Facilities section, enter the following information:

- *State*—Set BITS 1 and BITS 2 to OOS (Out of Service).
- *Coding*—Is not relevant for internal timing. The default (B8ZS) is sufficient.
- *Framing*—Is not relevant for internal timing. The default (ESF) is sufficient.
- *Sync Messaging*—Checked
- *AIS Threshold*—Is not available.

Step 5   In the Reference Lists section, enter the following information

- *NE Reference*
    - Ref1—Set to Internal Clock.
    - Ref2—Set to Internal Clock.
    - Ref3—Set to Internal Clock.
- *BITS 1 Out/BITS 2 Out*—Set to None

Step 6   Click **Apply**.

Step 7   Log into a node that will be timed from the node set up in Steps 1–4.

Step 8   In the CTC node view, click the **Provisioning > Timing** tabs.

Step 9   In the General Timing section, enter the same information as entered in Step 3, except for the following:

- *Timing Mode*—Set to Line.

Reference Lists

- *NE Reference*
    - Ref1—Set to the OC-N trunk card with the closest connection to the node in Step 3.
    - Ref2—Set to the OC-N trunk card with the next closest connection to the node in Step 3.
    - Ref3—Set to Internal Clock.

Step 10   Click **Apply**.

Step 11   Repeat Steps 7–10 at each node that will be timed by the node in Step 3.

3.7 Viewing ONS 15454 Inventory

The Inventory tab (Figure 3-10) displays information about cards installed in the ONS 15454 node including part numbers, serial numbers, hardware revisions, and equipment types. The tab provides a central location to obtain information and to determine applicability of ONS 15454 Product Change Notices (PCNs) and Field Service Bulletins (FSBs). Using the ONS 15454 export feature, you can export inventory data from ONS 15454 nodes into spreadsheet and database programs to consolidate ONS 15454 information for network inventory management and reporting.

Figure 3-10   Displaying ONS 15454 hardware information

The Inventory tab displays the following information about the cards installed in the ONS 15454:

• *Location*—The slot where the card is installed

• *Eqpt Type*—Equipment type the slot is provisioned for, for example, OC-12 or DS-1

• *Actual Eqpt Type*—The actual card that is installed in the slot, for example, OC12 IR 4 1310 or DS1N-14

Tip   You can pre-provision a slot before the card is installed by right-clicking the slot in node view and selecting a card type.

- *HW Part #*—Card part number; this number is printed on the top of the card
- *HW Rev*—Card revision number
- *Serial #*—Card serial number; this number is unique to each card
- *CLEI Code*—Common Language Equipment Identifier code
- *Firmware Rev*—Revision number of the software used by the ASIC chip installed on the card

3.8 Viewing CTC Software Versions

CTC software is pre-loaded on the ONS 15454 TCC+ cards; therefore, you do not need to install software on the TCC+. When a new CTC software version is released, you must follow procedures provided by the Cisco Technical Assistance Center (TAC) to upgrade the ONS 15454 software.

When you upgrade CTC software, the TCC+ stores the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. You can view the software versions that are installed on an ONS 15454 by selecting the Maintenance tab followed by the Software subtab. Select these tabs in node view to display the software installed on one node. Select the tabs in network view to display the software versions installed on all the network nodes.

4

IP Networking

This chapter explains how to set up Cisco ONS 15454s in internet protocol (IP) networks and includes:

- Scenarios showing Cisco ONS 15454s in common IP network configurations
- Procedures for creating static routes
- Procedures for using the Open Shortest Path First (OSPF) protocol

The chapter does not provide a comprehensive explanation of IP networking concepts and procedures.

Note To set up ONS 15454s within an IP network, you must work with a LAN administrator or other individual at your site who has IP networking training and experience. To learn more about IP networking, many outside resources are available. *IP Routing Fundamentals*, by Mark Sportack (Cisco Press, 1999), provides a comprehensive introduction to routing concepts and protocols in IP networks.

4.1 IP Networking Overview

ONS 15454s can be connected in many different ways within an IP environment:

- They can be connected to LANs through direct connections or a router.
- IP Subnetting can create ONS 15454 node groups, which allow you to provision non-DCC connected nodes in a network.
- Different IP functions and protocols can be used to achieve specific network goals. For example, Proxy Address Resolution Protocol (ARP) enables one LAN-connected ONS 15454 to serve as a gateway for ONS 15454s that are not connected to the LAN.
- You can create static routes to enable connections among multiple CTC sessions with ONS 15454s that reside on the same subnet but have different destination IP addresses.
- If ONS 15454s are connected to OSPF networks, ONS 15454 network information is automatically communicated across multiple LANs and WANs.

4.2 ONS 15454 IP Addressing Scenarios

ONS 15454 IP addressing generally has seven common scenarios or configurations. Use the scenarios as building blocks for more complex network configurations. Table 4-1 provides a general list of items to check when setting up ONS 15454s in IP networks. Additional procedures for troubleshooting Ethernet connections and IP networks are provided in Chapter 9, "Ethernet Operation."

Table 4-1   General ONS 15454 IP Networking Checklist

Item	What to check
PC/workstation	Each CTC computer must have the following: • Netscape 4.61 or Internet Explorer 5.0 or higher • JRE 1.3.0_C (PC) or JRE 1.3.0_01 (Solaris) for Releases 2.2.2 or higher; JRE 1.2.2_05 or higher (Windows), or 1.2.2_03 or higher (Solaris) for Releases 2.2.1 or earlier • Modified Java policy file See the "Computer Requirements" section on page 2-2 for additional information.
Link integrity	Link integrity exists between: • CTC computer and network hub/switch • ONS 15454s (backplane wire-wrap pins or RJ-45 port) and network hub/switch • Router ports and hub/switch ports
ONS 15454 hub/switch ports	Set the hub or switch port that is connected to the ONS 15454 to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15454s.
IP addresses/subnet masks	ONS 15454 IP addresses and subnet masks are set up correctly.
Optical connectivity	ONS 15454 optical trunk ports are in service; DCC is enabled on each trunk port

4.2.1 Scenario 1: CTC and ONS 15454s on Same Subnet

Scenario 1 shows a basic ONS 15454 LAN configuration (Figure 4-1). The ONS 15454s and CTC computer reside on the same subnet. All ONS 15454s connect to LAN A, and all ONS 15454s have DCC connections.

Note   Instructions for creating DCC connections are provided in Chapter 5, "SONET Topologies" within the BLSR, UPSR and linear ADM procedures.

Figure 4-1   Scenario 1: CTC and ONS 15454s on same subnet

CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = N/A
Host Routes = N/A

LAN A

ONS 15454 #2
IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

SONET RING

ONS 15454 #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15454 #3
IP Address 192.168.1.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A
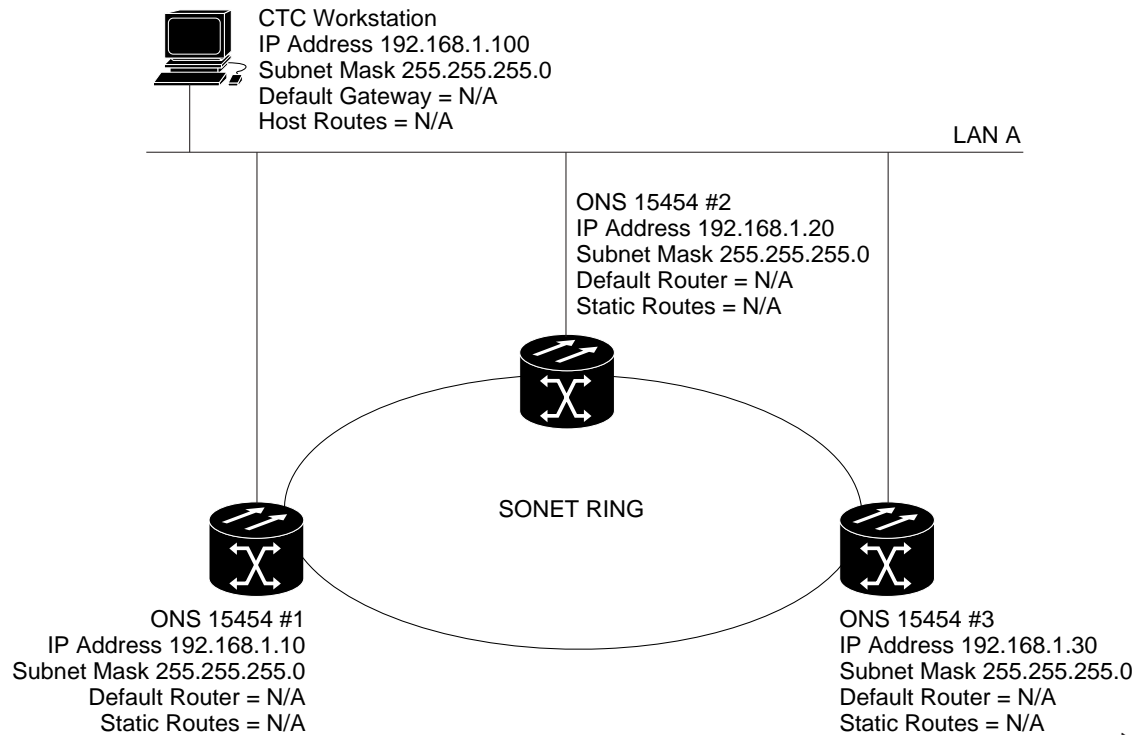
33157

4.2.2 Scenario 2: CTC and ONS 15454s Connected to Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 4-2). The ONS 15454s reside on a different subnet (192.168.2.0) and attach to LAN B. A router connects LAN A to LAN B. The IP address of router interface A is set to LAN A (192.168.1.1), and the IP address of router interface B is set to LAN B (192.168.2.1).

On the CTC computer, the default gateway is set to router interface A. If the LAN uses DHCP (Dynamic Host Configuration Protocol), the default gateway and IP address are assigned automatically. In the Figure 4-2 example, a DHCP server is not available.

Figure 4-2   Scenario 2: CTC and ONS 15454s connected to router

LAN A

Int "A"

Int "B" Router

CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A

Router
IP Address of interface "A" to LAN "A" 192.168.1.1
IP Address of interface "B" to LAN "B"   192.168.2.1
Subnet Mask 255.255.255.0
Default Router = N/A
Host Routes = N/A

LAN B

ONS 15454 #2
IP Address 192.168.2.20
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

SONET RING

ONS 15454 #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

ONS 15454 #3
IP Address 192.168.2.30
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

33158

4.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15454 Gateway

Scenario 3 is similar to Scenario 1, but only one ONS 15454 (node #1) connects to the LAN (Figure 4-3).
Two ONS 15454s (#2 and #3) connect to ONS 15454 #1 through the SONET DCC. Because all three
ONS 15454s are on the same subnet, Proxy ARP enables ONS 15454 #1 to serve as a gateway for ONS
15454s #2 and #3.

Figure 4-3   Scenario 3: Using Proxy ARP
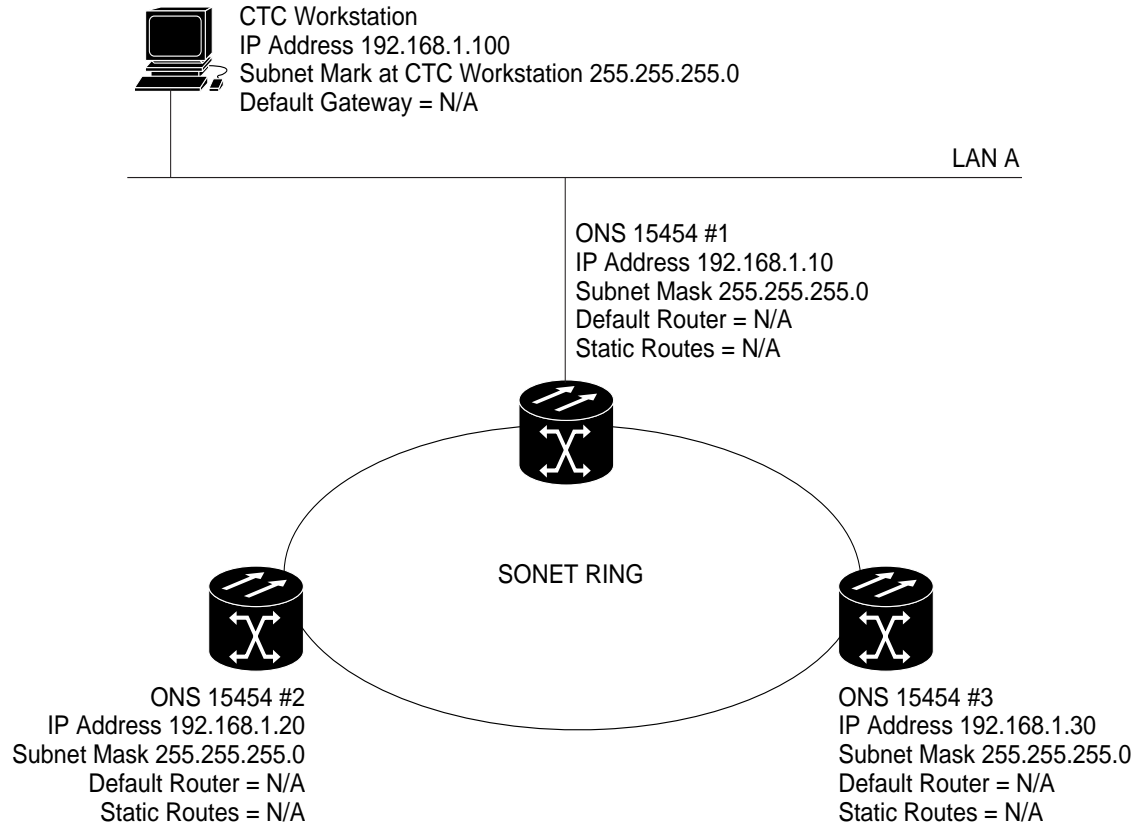
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of the machines on the network recognizes its own IP address in the request, it sends an ARP reply back to the requesting host. The reply contains the physical hardware address of the receiving host. The requesting host stores this address in its ARP cache so that all subsequent datagrams (packets) to this destination IP address can be translated to a physical address.

Proxy ARP enables one LAN-connected ONS 15454 to respond to the ARP request for ONS 15454s not connected to the LAN. (ONS 15454 Proxy ARP requires no user configuration.) For this to occur, the DCC-connected ONS 15454s must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15454 that is not connected to the LAN, the gateway ONS 15454 returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15454 to the MAC address of the proxy ONS 15454. The proxy ONS 15454 uses its routing table to forward the datagram to the non-LAN ONS 15454. The routing table is built using the OSPF IP routing protocol. (An OSPF example is presented in Scenario 6.)

Cisco ONS 15454 Installation and Operations Guide

4.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but nodes #2 and #3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 4-4). Node #1 and the CTC computer are on subnet 192.168.1.0. The network includes different subnets because Proxy ARP is not used. In order for the CTC computer to communicate with ONS 15454s #2 and #3, ONS 15454 #1 is entered as the default gateway on the CTC computer using the "Direct Connections to the ONS 15454" section on page 2-5.

Figure 4-4   Scenario 4: Default gateway on a CTC computer

CTC Workstation
IP Address 192.168.1.100
Subnet Mask at CTC Workstation 255.255.255.0
Default Gateway = 192.168.1.10
Host Routes = N/A

LAN A

ONS 15454 #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

SONET RING

ONS 15454 #2
IP Address 192.168.2.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15454 #3
IP Address 192.168.3.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

33160

4.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15454s to CTC sessions on one subnet connected by a router to ONS 15454s residing on another subnet. (These static routes are not needed if OSPF is enabled. Scenario 7 shows an OSPF example.)

- To enable multiple CTC sessions among ONS 15454s residing on the same subnet. (Scenario 6 shows an example.)

In Figure 4-5, one CTC residing on subnet 192.168.1.0 connects to a router through interface A. (The router is not set up with OSPF.) ONS 15454s residing on subnet 192.168.2.0 are connected through ONS 15454 #1 to the router through interface B. Proxy ARP enables ONS 15454 #1 as a gateway for ONS 15454s #2 and #3. To connect to CTC computers on LAN A, a static route is created on ONS 15454 #1.

Figure 4-5   Scenario 5: Static route with one CTC computer used as a destination
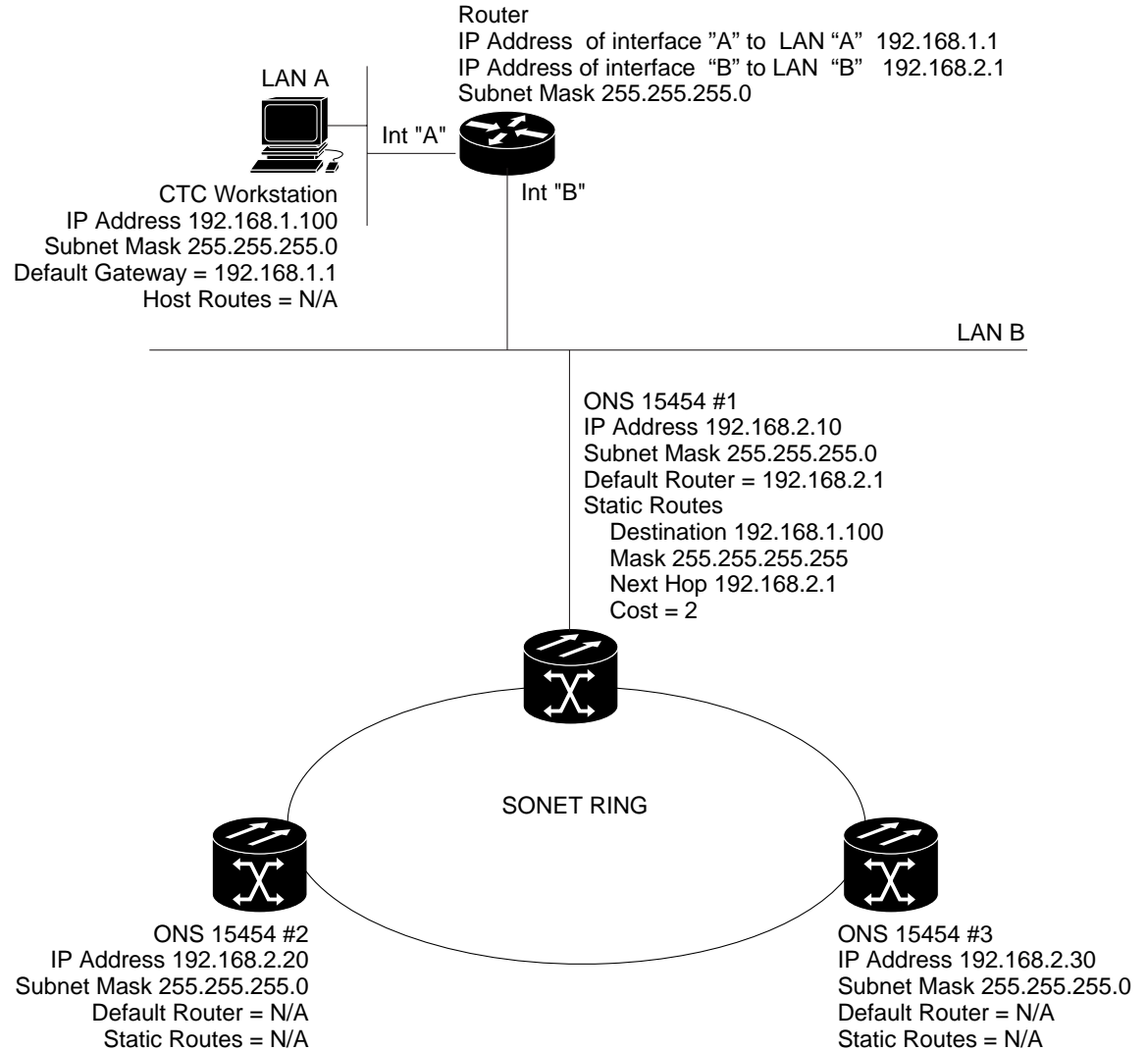
The destination and subnet mask entries control access to the ONS 15454s:

- If a single CTC computer is connected to router, enter the complete CTC "host route" IP address as the destination with a subnet mask of 255.255.255.255.

- If CTC computers on a subnet are connected to router, *e*nter the destination subnet (in this example, 192.168.1.0) and a subnet mask of 255.255.255.0.

- If all CTC computers are connected to router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 4-6 shows an example.

The IP address of router interface B is entered as the next hop, and the cost (number of hops from source to destination) is 2.

Figure 4-6   Scenario 5: Static route with multiple LAN destinations
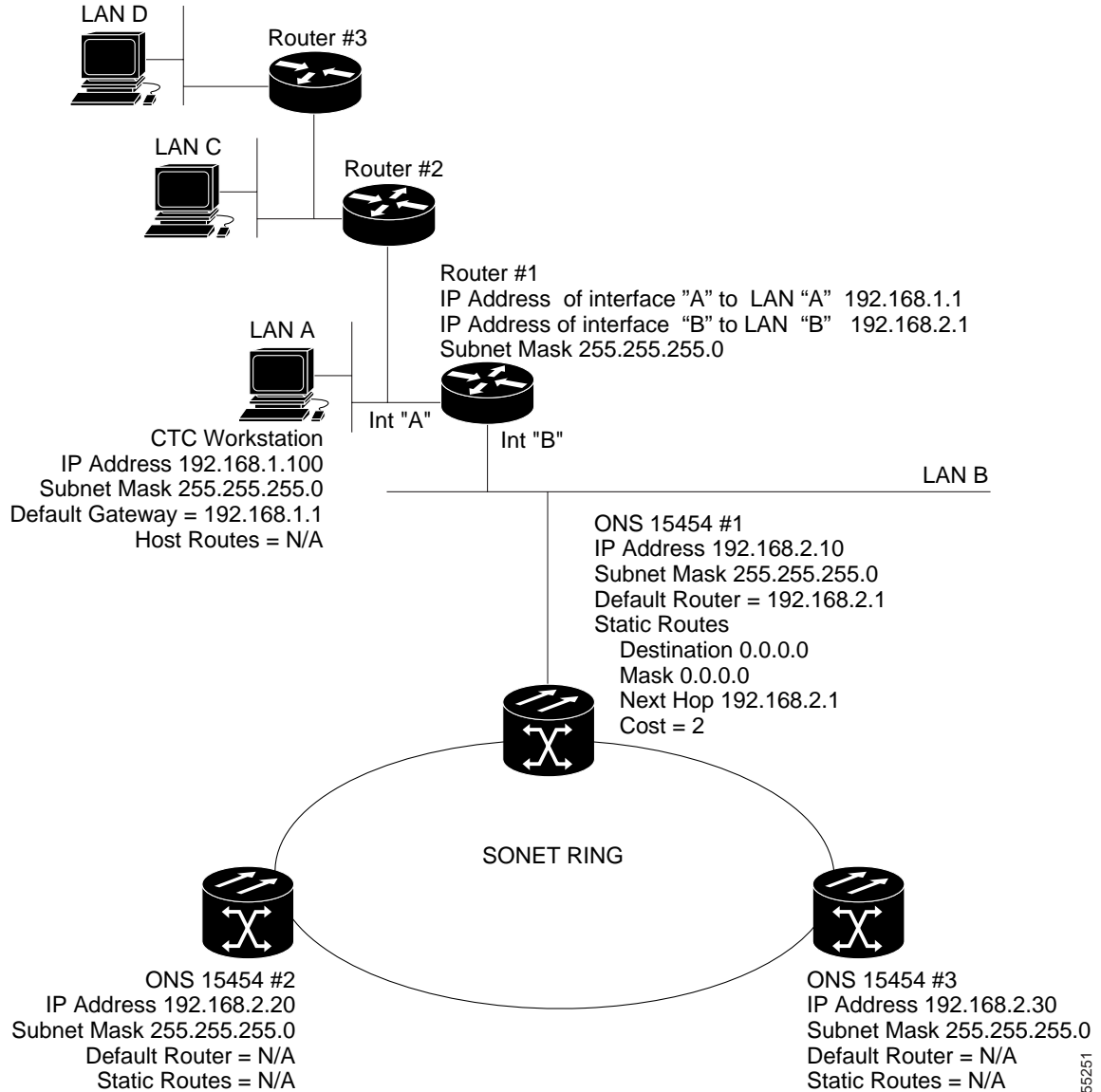
Procedure: Create a Static Route

Use the following steps to create a static route.

Step 1   Log into the ONS 15454 and select 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 (in the example, 192.168.1.100). 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 (i.e., 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, enter a subnet mask of 0.0.0.0 to provide access to all CTC computers.

- *Next Hop*—Enter the IP address of the router port (in this example, 192.168.90.1) 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. In this example, the cost is two, one hop from the ONS 15454 to the router and a second hop from the router to the CTC workstation.

Step 4   Click **OK**. Verify that the static route displays in the Static Route window, or ping the node.

4.2.6 Scenario 6: Static Route for Multiple CTCs

Scenario 6 shows a static route used when multiple CTC computers need to access ONS 15454s residing on the same subnet (Figure 4-7). In this scenario, CTC #1 and #2 and all ONS 15454s are on the same IP subnet; ONS 15454 #1 and CTC #1 are attached to LAN A. ONS 15454 #2 and CTC #2 are attached to LAN B. Static routes are added to ONS 15454 #1 pointing to CTC #1, and to ONS 15454 #2 pointing to CTC #2. The static route is entered from the node's perspective.

Figure 4-7   Scenario 6: Static route for multiple CTCs

CTC Workstation #1
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = N/A

LAN A

ONS 15454 #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes
    Destination 192.168.1.100
    Mask 255.255.255.255
    Next Hop 192.168.1.10
    Cost = 1

SONET RING

LAN B

ONS 15454 #2
IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes
    Destination 192.168.1.200
    Mask 255.255.255.255
    Next Hop 192.168.1.20
    Cost = 1

ONS 15454 #3
IP Address 192.168.1.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

CTC Workstation #2
IP Address 192.168.1.200
Subnet Mask 255.255.255.0
Default Gateway = N/A

33163

4.2.7 Scenario 7: Using OSPF

Open Shortest Path First (OSPF) is a link state Internet routing protocol. Link state protocols use a "hello protocol" to monitor their links with adjacent routers and to test the status of their links to their neighbors. Link state protocols advertise their directly-connected networks and their active links. Each link state router captures the link state "advertisements" and puts them together to create a topology of the entire network or area. From this database, the router calculates a routing table by constructing a shortest path tree. Routes are continuously recalculated to capture ongoing topology changes.

ONS 15454s use the OSPF protocol in internal ONS 15454 networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15454s so that the ONS 15454 topology is sent to OSPF routers on a LAN. Advertising the ONS 15454 network topology to LAN routers eliminates

the need to manually enter static routes for ONS 15454 subnetworks. Figure 4-7 shows the same network enabled for OSPF. Figure 4-9 shows the same network without OSPF. Static routes must be manually added to the router in order for CTC computers on LAN A to communicate with ONS 15454 #2 and #3 because these nodes reside on different subnets.

OSPF divides networks into smaller regions, called areas. An area is a collection of networked end systems, routers, and transmission facilities organized by traffic patterns. Each OSPF area has a unique ID number, known as the area ID, that can range from 0 to 4,294,967,295. Every OSPF network has one backbone area called "area 0." All other OSPF areas must connect to area 0.

When you enable ONS 15454 OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID to the ONS 15454 network. Coordinate the area ID number assignment with your LAN administrator. In general, all DCC-connected ONS 15454s are assigned the same OSPF area ID.

Figure 4-8   Scenario 7: OSPF enabled
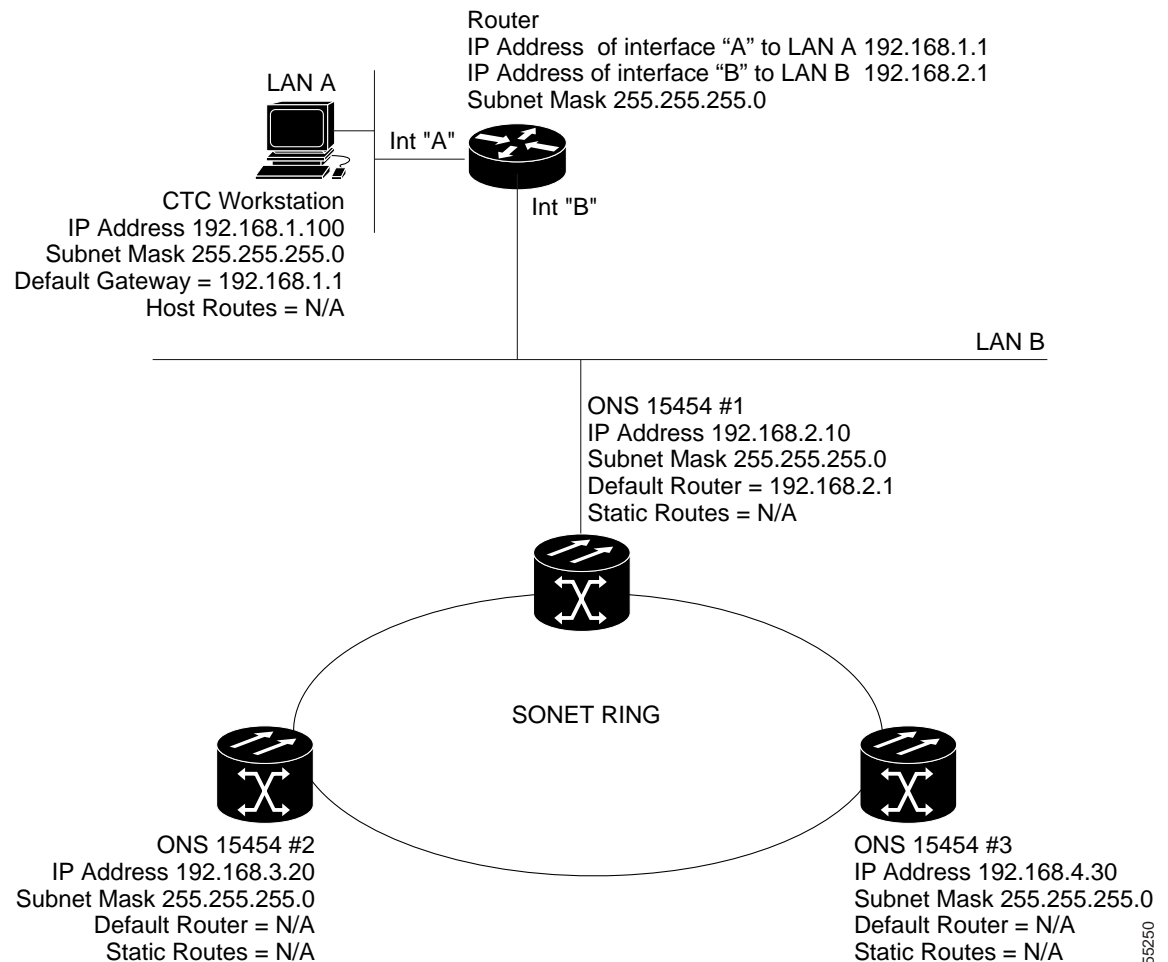
Figure 4-9   Scenario 7: OSPF not enabled
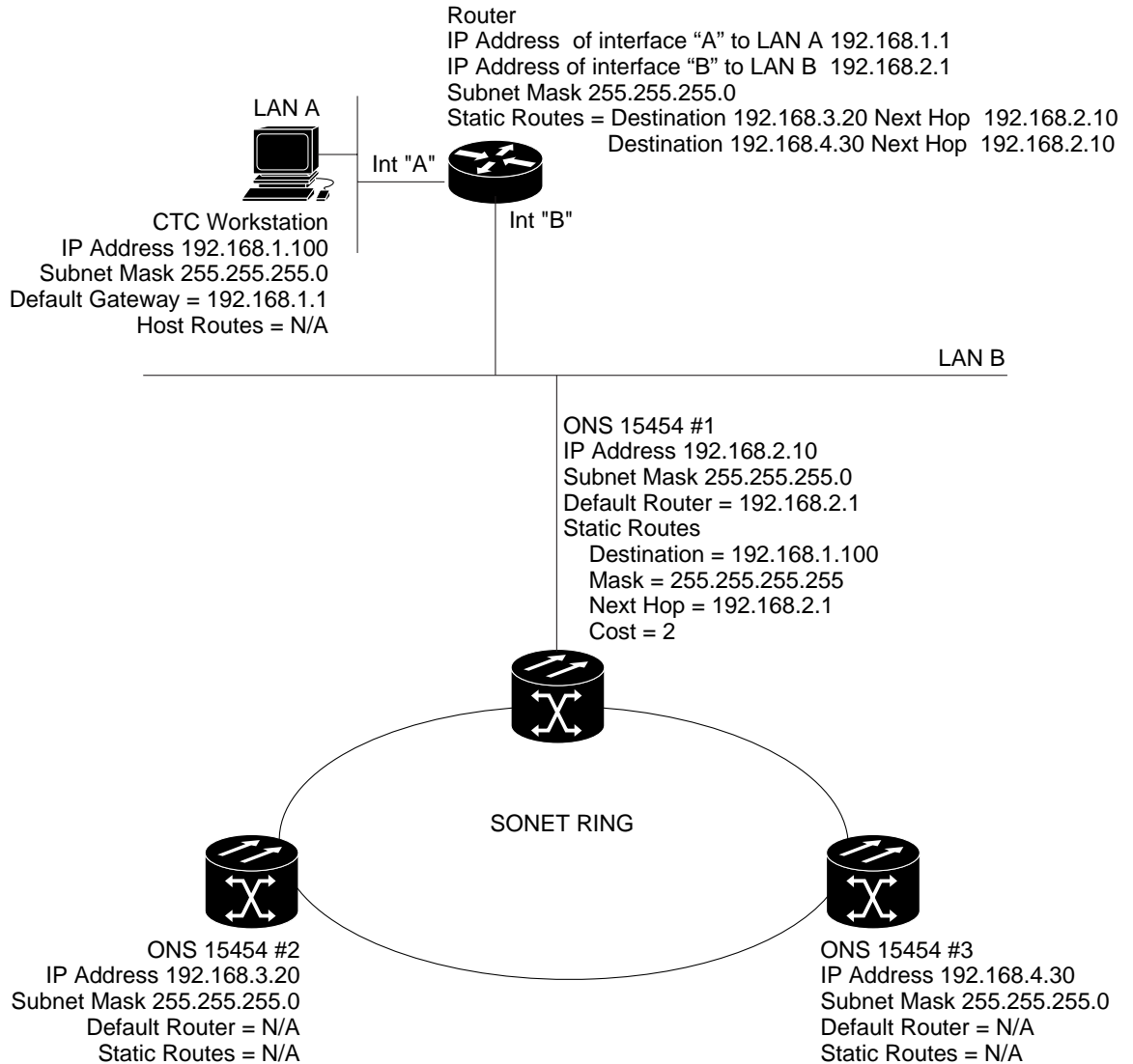
Use the following procedure to enable OSPF on each ONS 15454 node that you want included in the OSPF network topology. ONS 15454 OSPF settings must match the router OSPF settings, so you will need to get the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) from the router to which the ONS 15454 network is connected before enabling OSPF.

Procedure: Set up OSPF

Step 1   Log into the ONS 15454 node.

Step 2   In node view, select the **Provisioning** > **Network** > **OSPF** tabs. The OSPF pane has several options (Figure 4-10).

Figure 4-10   Enabling OSPF on the ONS 15454
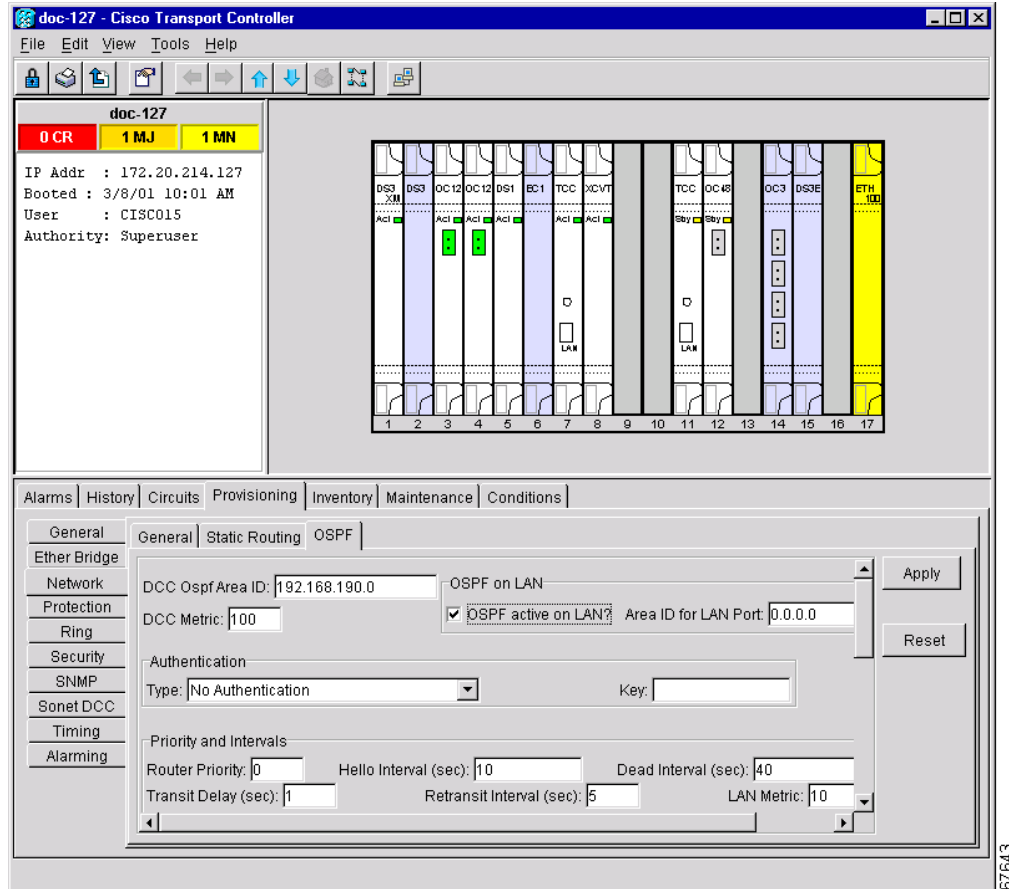
Step 3   On the top left side, complete the following:

- *DCC OSPF Area ID*—Enter the number that identifies the ONS 15454s as a unique OSPF area. The OSPF area number can be an integer between 0 and 4294967295, and it can take a form similar to an IP address. The number must be unique to the LAN OSPF area.

- *DCC Metric*—This value is normally unchanged. It sets a "cost" for sending packets across the DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default DCC metric is 100.

Step 4   In the OSPF on LAN area, complete the following:

- *OSPF active on LAN*—When checked, enables ONS 15454 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454s that directly connect to OSPF routers.

- *Area ID for LAN Port*—Enter the OSPF area ID for the router port where the ONS 15454 is connected. (This number is different from the DCC Area ID.)

Step 5   In the Authentication area, complete the following:

- *Type*—If the router where the ONS 15454 is connected uses authentication, select **Simple Password**. Otherwise, select **No Authentication**.

- *Key*—If authentication is enabled, enter the OSPF key (password).

Step 6   In the Priority and Intervals area, complete the following:

The OSPF priority and intervals default to values most commonly used by OSPF routers. In the Priority and Invervals area, verify that these values match those used by the OSPF router where the ONS 15454 is connected.

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

Step 7 In the OSPF Area Range Table area, complete the following:

Area range tables consolidate the information that is propagated outside an OSPF Area border. One ONS 15454 in the ONS 15454 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 OSPF area.

To create an area range table:

a. Under OSPF Area Range Table, click **Create**.

b. In the Create Area Range dialog box, enter the following:

- *Range Address*—Enter the area IP address for the ONS 15454s that reside within the OSPF area. For example, if the ONS 15454 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
- *Range Area ID*—Enter the OSPF area ID for the ONS 15454s. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.
- *Mask Length*—Enter the subnet mask length. In the Range Address example, this is 16.
- *Advertise*—Check if you want to advertise the OSPF range table.

c. Click **OK**.

Step 8 All OSPF areas must be connected to Area 0. If the ONS 15454 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

a. Under OSPF Virtual Link Table, click **Create**.

b. In the Create Virtual Link dialog box, complete the following fields (OSPF settings must match OSPF settings for the ONS 15454 OSPF area):

Neighbor—Enter the router ID of the Area 0 router.

Transit Delay (sec)—The service speed. One second is the default.

Hello Int (sec)—The number of seconds between OSPF "hello" packet advertisements sent by OSPF routers. Ten seconds is the default.

Auth Type—If the router where the ONS 15454 is connected uses authentication, select **Simple Password**. Otherwise, set it to **No Authentication**.

Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.

> *Dead Int (sec)*—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

c. Click **OK**.

Step 9 After entering ONS 15454 OSPF area data, click **Apply**.

If you changed the Area ID, the TCC+ cards will reset, one at a time.

4.3 Viewing the ONS 15454 Routing Table

ONS 15454 routing information is displayed on the Maintenance > Routing Table tabs (Figure 4-11). The routing table provides the following information:

- *Destination*—Displays the IP address of the destination network or host.
- *Mask*—Displays the subnet mask used to reach the destination host or network.
- *Gateway*—Displays the IP address of the gateway used to reach the destination network or host.
- *Usage*—Shows the number of times this route has been used.
- *Interface*—Shows the ONS 15454 interface used to access the destination. Values are:
  - cpm0—the ONS 15454 Ethernet interface, that is, the RJ-45 jack on the TCC+ and the LAN 1 pins on the backplane.
  - pdcc0—an SDCC interface, that is, an OC-N trunk card identified as the SDCC termination.
  - lo0—a loopback interface

Figure 4-11   Viewing the ONS 15454 routing table
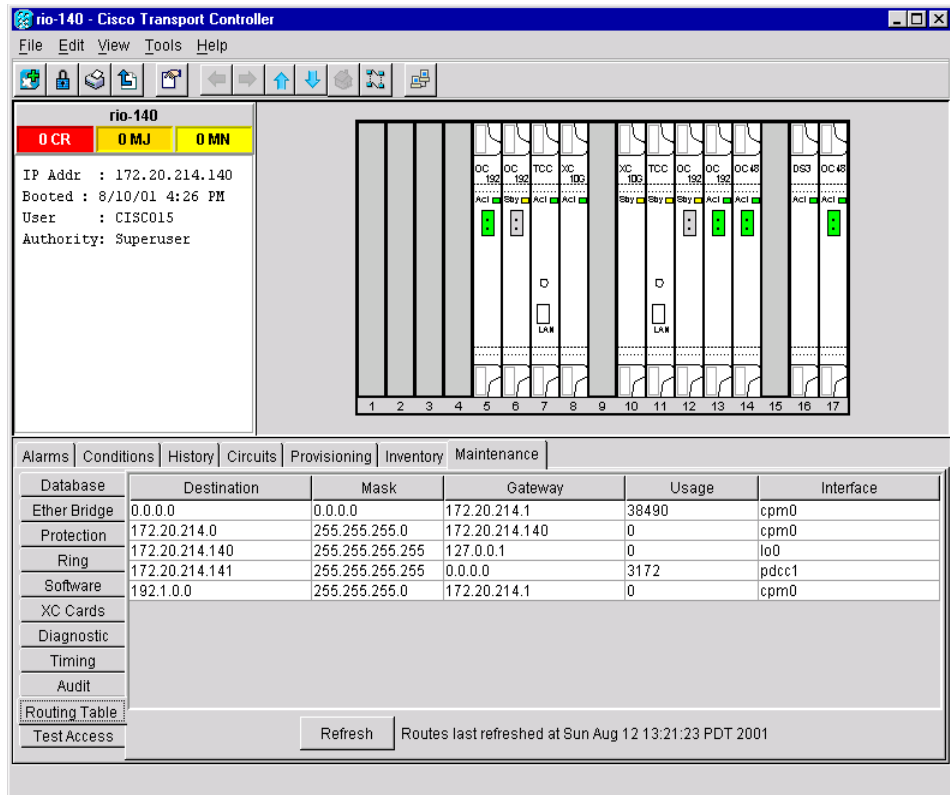
Table 4-2 shows sample routing entries for an ONS 15454.

Table 4-2   Sample Routing Table Entries

Entry	Destination	Mask	Gateway	Interface
1	0.0.0.0	0.0.0.0	172.20.214.1	cpm0
2	172.20.214.0	255.255.255.0	172.20.214.92	cpm0
3	172.20.214.92	255.255.255.255	127.0.0.1	lo0
4	172.20.214.93	255.255.255.255	0.0.0.0	pdcc0
5	172.20.214.94	255.255.255.255	172.20.214.93	pdcc0

Entry #1 shows the following:

- *Destination* (0.0.0.0) is the default route entry. All undefined destination network or host entries on this routing table will be mapped to the default route entry.

- *Mask* (0.0.0.0) is always 0 for the default route.

- *Gateway* (172.20.214.1) is the default gateway address. All outbound traffic that cannot be found in this routing table or is not on the node's local subnet will be sent to this gateway.

- *Interface* (cpm0) indicates that the ONS 15454 Ethernet interface is used to reach the gateway.

Entry #2 shows the following:

- *Destination* (172.20.214.0) is the destination network IP address.

- *Mask* (255.255.255.0) is a 24-bit mask, meaning all addresses within the 172.20.214.0 subnet can be a destination.

- *Gateway* (172.20.214.92) is the gateway address. All outbound traffic belonging to this network is sent to this gateway.

- *Interface* (cpm0) indicates that the ONS 15454 Ethernet interface is used to reach the gateway.

Entry #3 shows the following:

- *Destination* (172.20.214.92) is the destination host IP address.

- *Mask* (255.255.255.255) is a 32 bit mask, meaning only the 172.20.214.92 address is a destination.

- *Gateway* (127.0.0.1) is a loopback address. The host directs network traffic to itself using this address.

- *Interface* (lo0) indicates that the local loopback interface is used to reach the gateway.

Entry #4 shows the following:

- *Destination* (172.20.214.93) is the destination host IP address.

- *Mask* (255.255.255.255) is a 32 bit mask, meaning only the 172.20.214.93 address is a destination.

- *Gateway* (0.0.0.0) means the destination host is directly attached to the node.

- *Interface* (pdcc0) indicates that a SONET SDCC interface is used to reach the destination host.

Entry #5 shows a DCC-connected node that is accessible through a node that is not directly connected:

- *Destination* (172.20.214.94) is the destination host IP address.

- *Mask* (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.94 address is a destination.

- *Gateway* (172.20.214.93) indicates that the destination host is accessed through a node with IP address 172.20.214.93.

- *Interface* (pdcc0) indicates that a SONET SDCC interface is used to reach the gateway.

SONET Topologies

This chapter explains how to set up the Cisco ONS 15454 in different SONET topologies, including:

- Two-fiber and four-fiber bidirectional line switched rings (BLSRs)
- Unidirectional path switched rings (UPSRs)
- Subtending rings
- Linear add/drop multiplexers (ADMs)
- Path-protected mesh networks (PPMNs)

5.1 Before You Begin

To avoid errors during network configuration, Cisco recommends that you draw the complete ONS 15454 SONET topology on paper (or electronically) before you begin the physical implementation. A sketch ensures that you have adequate slots, cards, and fibers to complete the topology.

Table 5-1 shows the SONET rings that can be created on each ONS 15454 node.

Table 5-1   ONS 15454 Rings

Ring Type	Maximum per node
All rings	5
BLSRs	2
2-Fiber BLSR	2
4-Fiber BLSR	1
UPSR	4

5.2 Bidirectional Line Switched Rings

The ONS 15454 can support two concurrent BLSRs in one of the following configurations:

- Two, two-fiber BLSRs, or
- One two-fiber and one four-fiber BLSR.

Each BLSR can have up to 16 ONS 15454s. Because the working and protect bandwidths must be equal, you can create only OC-12 (two-fiber only), OC-48, or OC-192 BLSRs.

> **Note** Two-fiber BLSRs can support up to 24 ONS 15454s, but switch times are slightly longer for rings containing more than 16 nodes. BLSRs with 16 or fewer nodes will meet the GR-1230 switch time requirement. Four-fiber BLSRs can only support 16 nodes.

5.2.1 Two-Fiber BLSRs

In two-fiber BLSRs, each fiber is divided into working and protect bandwidths. For example, in an OC-48 BLSR (Figure 5-1), STSs 1 – 24 carry the working traffic, and STSs 25 – 48 are reserved for protection. Working traffic (STSs 1 – 24) travels in one direction on one fiber and in the opposite direction on the second fiber. The Cisco Transport Controller (CTC) circuit routing routines calculate the "shortest path" for circuits based on many factors, including requirements set by the circuit provisioner, traffic patterns, and distance. For example, in Figure 5-1, circuits going from Node 0 to Node 1 typically will travel on Fiber 1, unless that fiber is full, in which case circuits will be routed on Fiber 2 through Node 3 and Node 2. Traffic from Node 0 to Node 2 (or Node 1 to Node 3), may be routed on either fiber, depending on circuit provisioning requirements and traffic loads.

Figure 5-1   A four-node, two-fiber BLSR
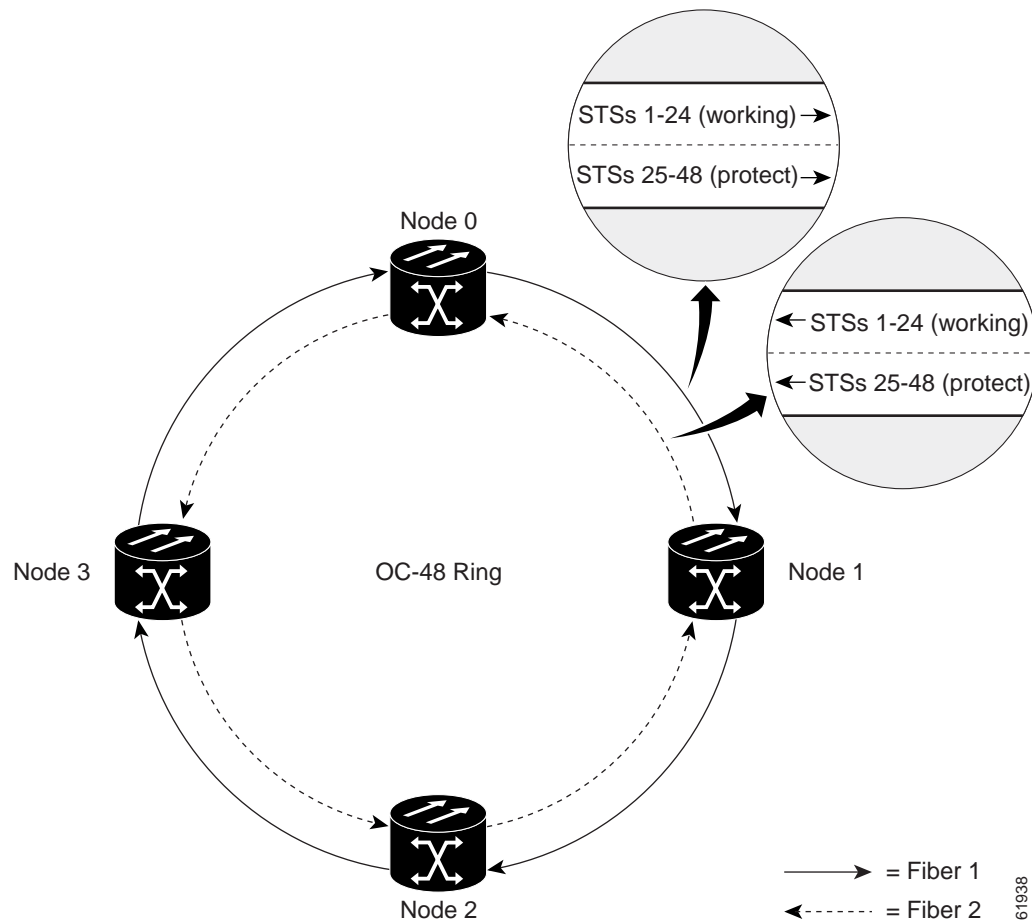
The SONET K1 and K2 bytes carry the information that governs BLSR protection switches. Each BLSR node monitors the K bytes to determine when to switch the SONET signal to an alternate physical path. The K bytes communicate failure conditions and actions taken between nodes in the ring.

If a break occurs on one fiber, working traffic targeted for a node beyond the break switches to the protect bandwidth on the second fiber. The traffic travels in reverse direction on the protect bandwidth until it reaches its destination node. At that point, traffic is switched back to the working bandwidth.

Figure 5-2 shows a sample traffic pattern on a four-node, two-fiber BLSR.

Figure 5-2   Four-node, two-fiber BLSR sample traffic pattern
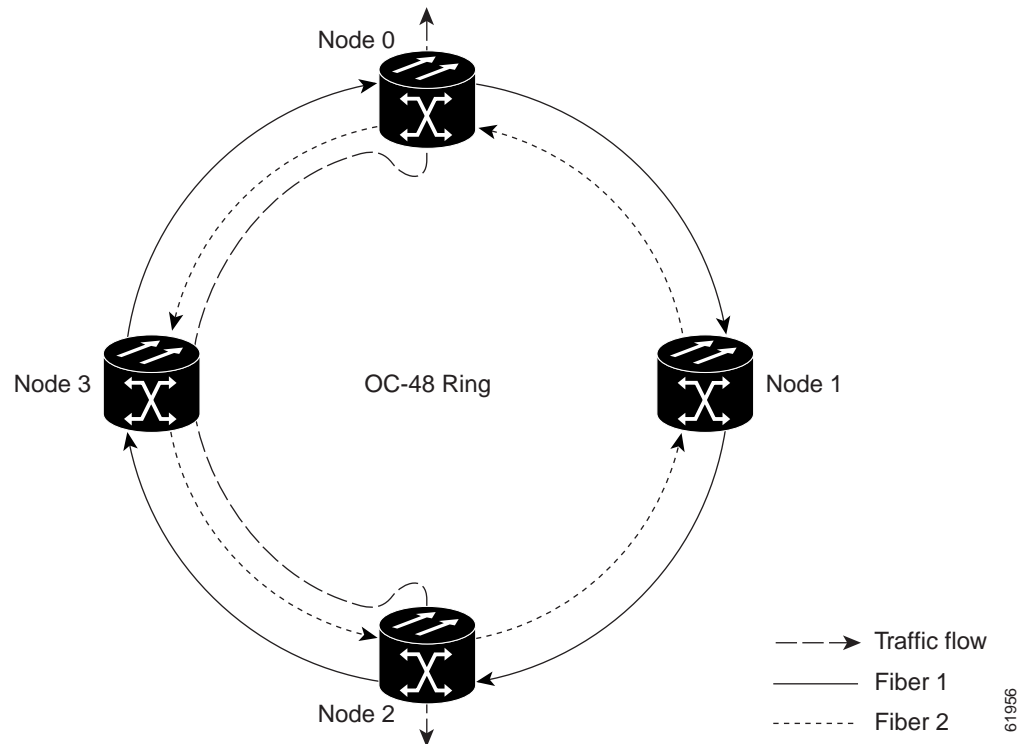
Figure 5-3 shows how traffic is rerouted following a line break between Node 0 and Node 3.

- All circuits originating on Node 0 carried to Node 2 on Fiber 2 are switched to the protect bandwidth of Fiber 1. For example, a circuit carried on STS-1 on Fiber 2 is switched to STS-25 on Fiber 1. A circuit carried on STS-2 on Fiber 2 is switched to STS-26 on Fiber 1. Fiber 1 carries the circuit to Node 3 (the original routing destination). Node 3 switches the circuit back to STS-1 on Fiber 2 where it is routed to Node 2 on STS-1.

- Circuits originating on Node 2 that were normally carried to Node 0 on Fiber 1 are switched to the protect bandwidth of Fiber 2 at Node 3. For example, a circuit carried on STS-2 on Fiber 1 is switched to STS-26 on Fiber 2. Fiber 2 carries the circuit to Node 0 where the circuit is switched back to STS-2 on Fiber 1 and then dropped to its destination.

Figure 5-3   Four-node, two-fiber BLSR traffic pattern following line break
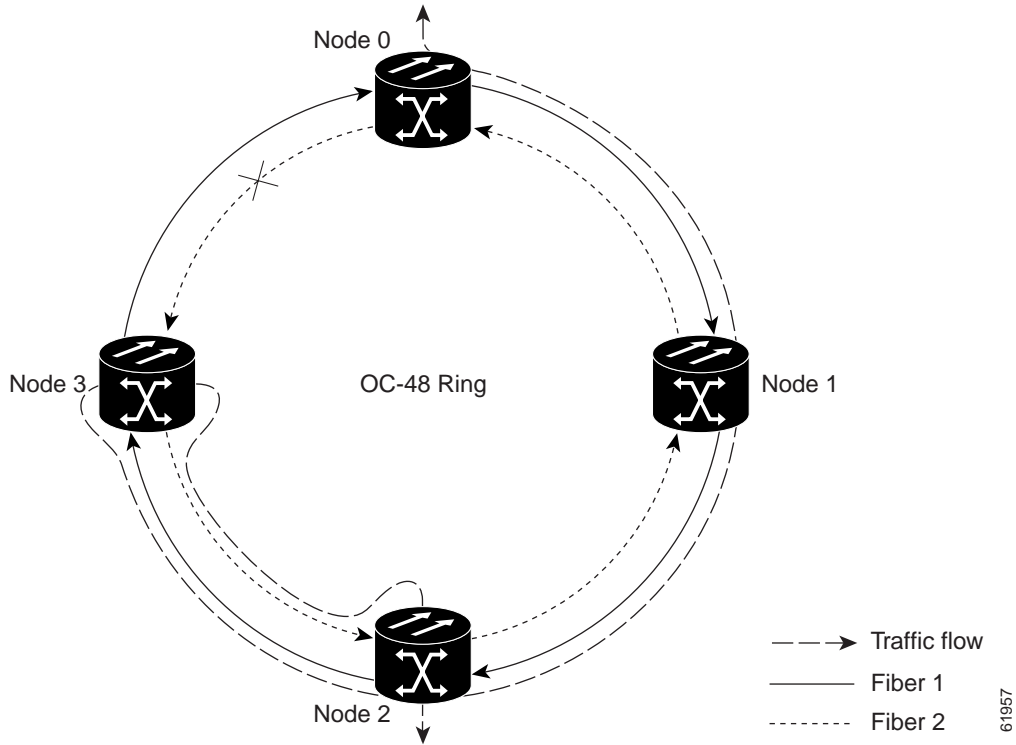
5.2.2 Four-Fiber BLSRs

Four-fiber BLSRs double the bandwidth of two-fiber BLSRs. Because they allow span switching as well as ring switching, four-fiber BLSRs increase the reliability and flexibility of traffic protection. Two fibers are allocated for working traffic and two fibers for protection, as shown in Figure 5-4. To implement a four-fiber BLSR, you must install four OC-48 or OC-48AS cards, or four OC-192 cards at each BLSR node.

Figure 5-4   A four-node, four-fiber BLSR
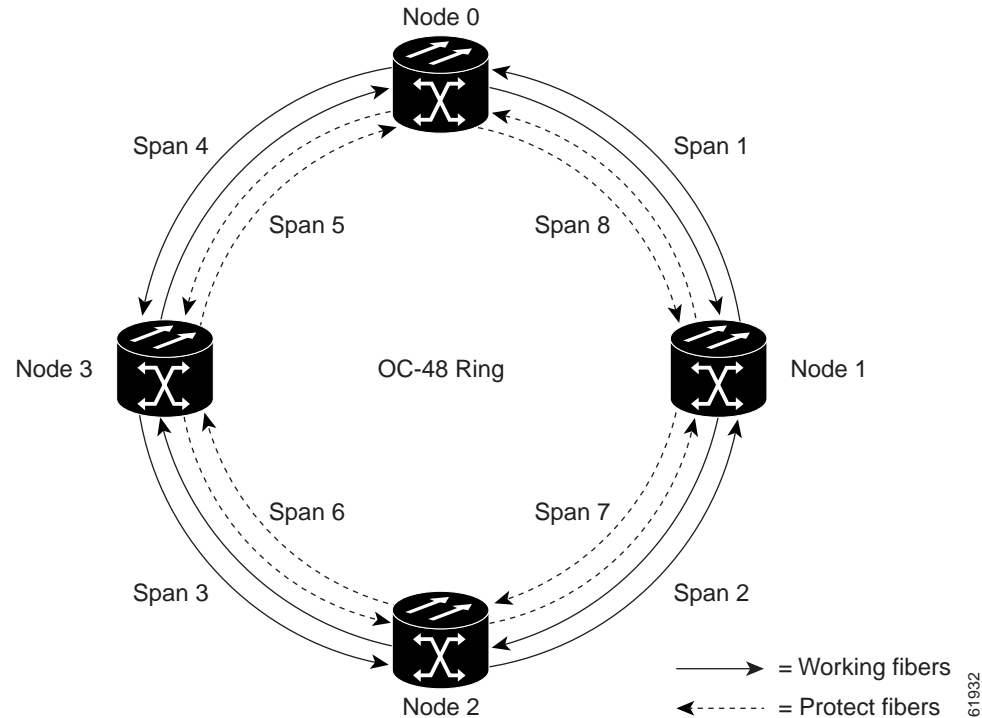
Four-fiber BLSRs provide span and ring switching:

- Span switching (Figure 5-5) occurs when a working span fails. Traffic switches to the protect fibers between the nodes (Node 0 and Node 1 in the Figure 5-5 example) and then returns to the working fibers. Multiple span switches can occur at the same time.

- Ring switching (Figure 5-6) occurs when a span switch cannot recover traffic, such as when both the working and protect fibers fail on the same span. In a ring switch, traffic is routed to the protect fibers throughout the full ring.

Figure 5-5   A four-fiber BLSR span switch

Node 0

Span 4

Span 5

Node 3

OC-48 Ring

Span 8

Span 1

Node 1

Span 6

Span 7

Span 3

Span 2

Node 2

= Working fibers

= Protect fibers

61959
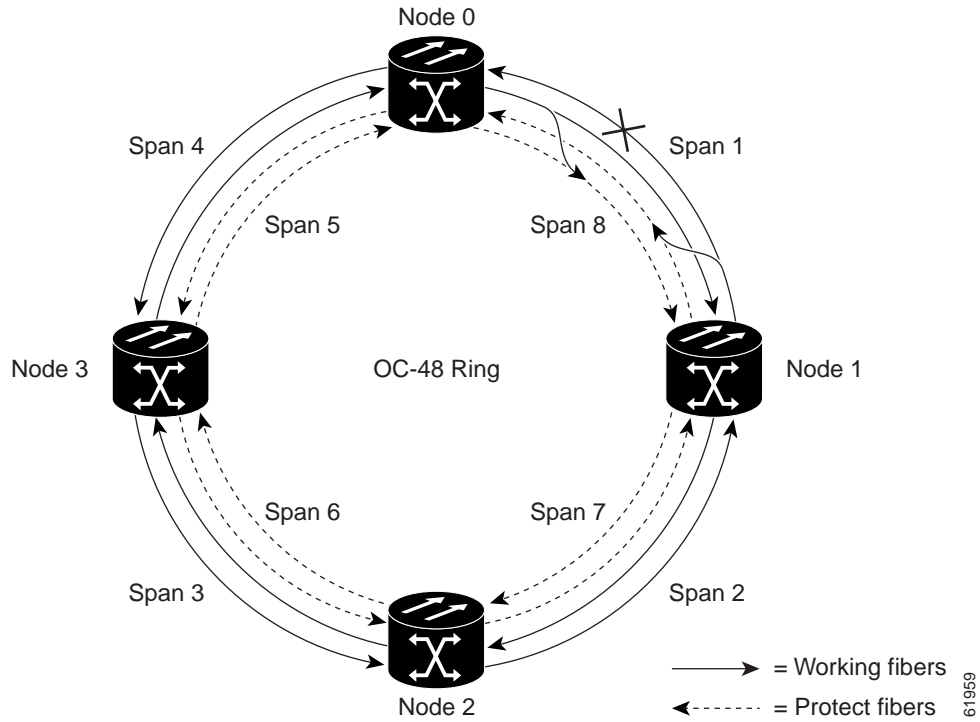
Figure 5-6   A four-fiber BLSR ring switch

Node 0

Span 4

Span 5

Node 3

OC-48 Ring

Span 8

Span 1

Node 1

Span 6

Span 7

Span 3

Span 2

Node 2

= Working fibers

= Protect fibers

61960

Cisco ONS 15454 Installation and Operations Guide
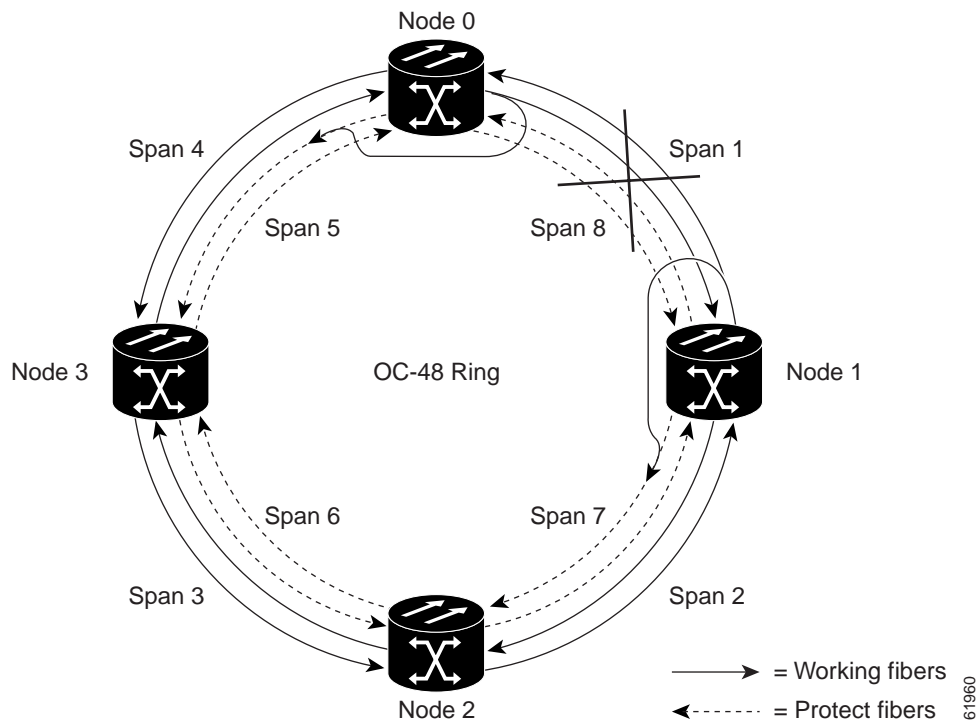
5.2.3 BLSR Bandwidth

BLSR nodes can terminate traffic that is fed from either side of the ring. Therefore, BLSRs are suited for distributed node-to-node traffic applications such as interoffice networks and access networks.

BLSRs allow bandwidth to be reused around the ring and can carry more traffic than a network with traffic flowing through one central hub. BLSRs can also carry more traffic than a UPSR operating at the same OC-N rate. Table 5-2 shows the bidirectional bandwidth capacities of two-fiber BLSRs. The capacity is the OC-N rate divided by two, multiplied by the number of nodes in the ring minus the number of pass-through STS-1 circuits. Table 5-3 shows the bidirectional bandwidth capacities of four-fiber BLSRs.

Table 5-2   Two-Fiber BLSR Capacity

OC Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
OC-12	STS1-6	STS 7-12	6 x N[1] - PT[2]
OC-48	STS 1-24	STS 25-48	24 x N - PT
OC-192	STS 1-96	STS 97-192	96 x N - PT

1. N equals the number of ONS 15454 nodes configured as BLSR nodes.

2. PT equals the number of STS-1 circuits passed through ONS 15454 nodes in the ring (capacity can vary depending on the traffic pattern).

Table 5-3   Four-Fiber BLSR Capacity

OC Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
OC-48	STS 1-48 (Fiber 1)	STS 1-48 (Fiber 2)	48 x N - PT
OC-192	STS 1-192 (Fiber 1)	STS 1-192 (Fiber 2)	192 x N - PT

Figure 5-7 shows an example of BLSR bandwidth reuse. The same STS carries three different traffic sets simultaneously on different spans on the ring: one set from Node 3 to Node 1, one from Node 1 to Node 2, and another from Node 2 to Node 3.

Figure 5-7   BLSR bandwidth reuse
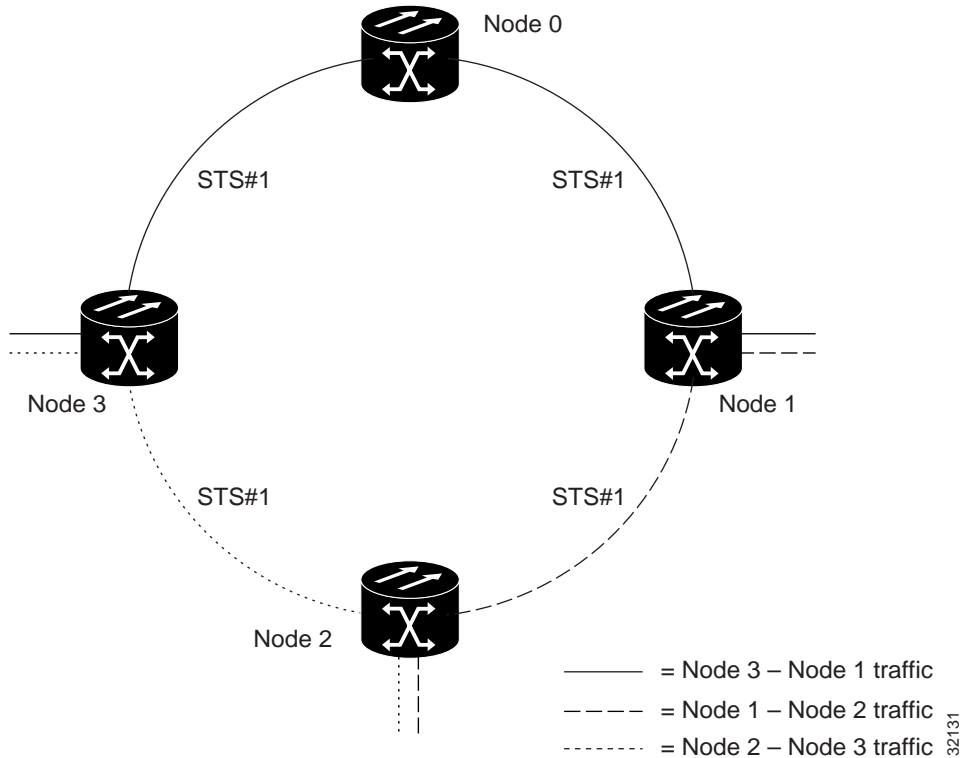
5.2.4 Sample BLSR Application

Figure 5-8 shows a sample two-fiber BLSR implementation. A regional long-distance network connects to other carriers at Node 0. Traffic is delivered to the service provider's major hubs.

- Carrier 1 delivers six DS-3s over two OC-3 spans to Node 0. Carrier 2 provides twelve DS-3s directly. Node 0 receives the signals and delivers them around the ring to the appropriate node.

- The ring also brings 14 DS-1s back from each remote site to Node 0. Intermediate nodes serve these shorter regional connections.

- The ONS 15454 OC-3 card supports a total of four OC-3 ports so that two additional OC-3 spans can be added at little cost.

Figure 5-8   A five-node BLSR
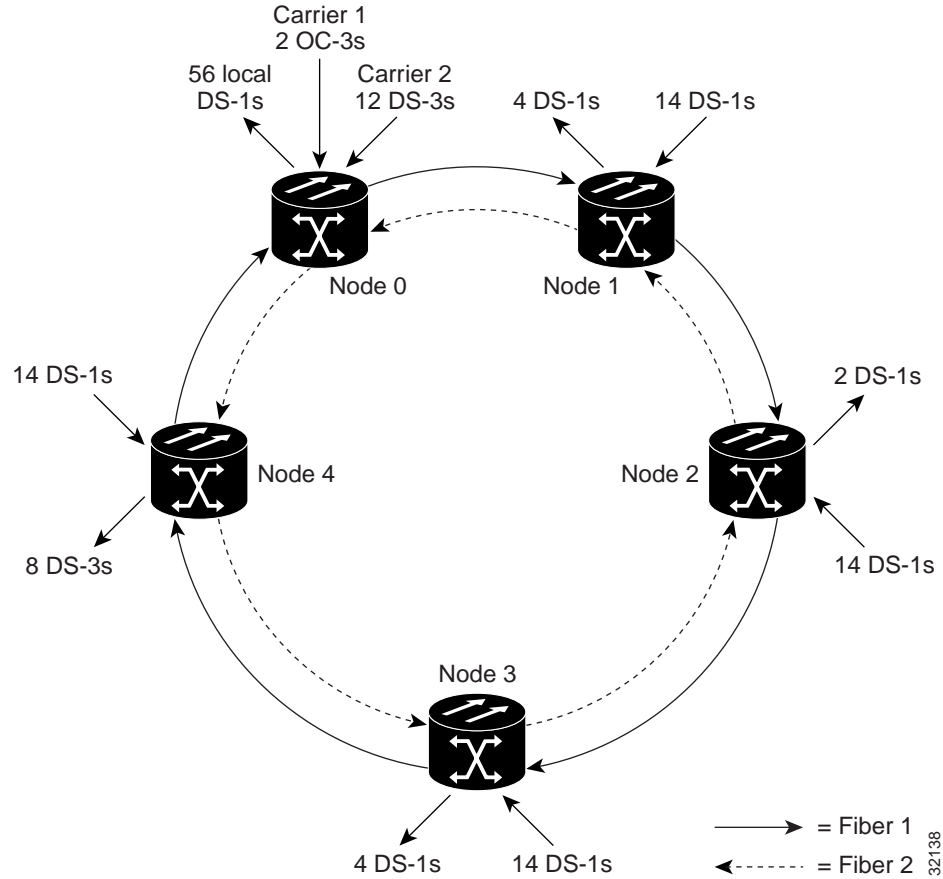
Figure 5-9 shows the shelf assembly layout for Node 0, which has one free slot. Figure 5-10 shows the shelf assembly layout for the remaining sites in the ring. In this BLSR configuration, an additional eight DS-3s at Node IDs 1 and 3 can be activated. An additional four DS-3s can be added at Node ID 4, and ten DS-3s can be added at Node ID 2. Each site has free slots for future traffic needs.

Figure 5-9   Shelf assembly layout for Node 0 in Figure 5-8
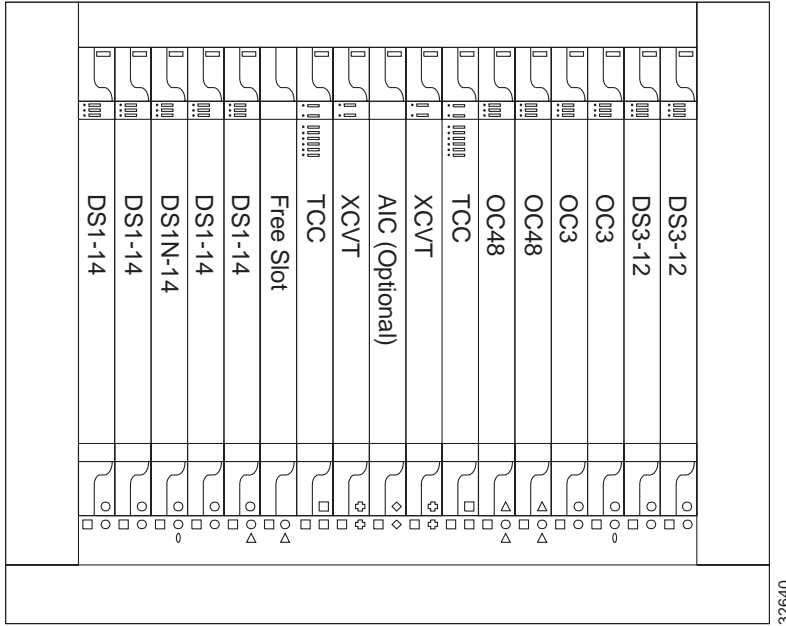
Figure 5-10   Shelf assembly layout for Nodes 1 – 4 in Figure 5-8
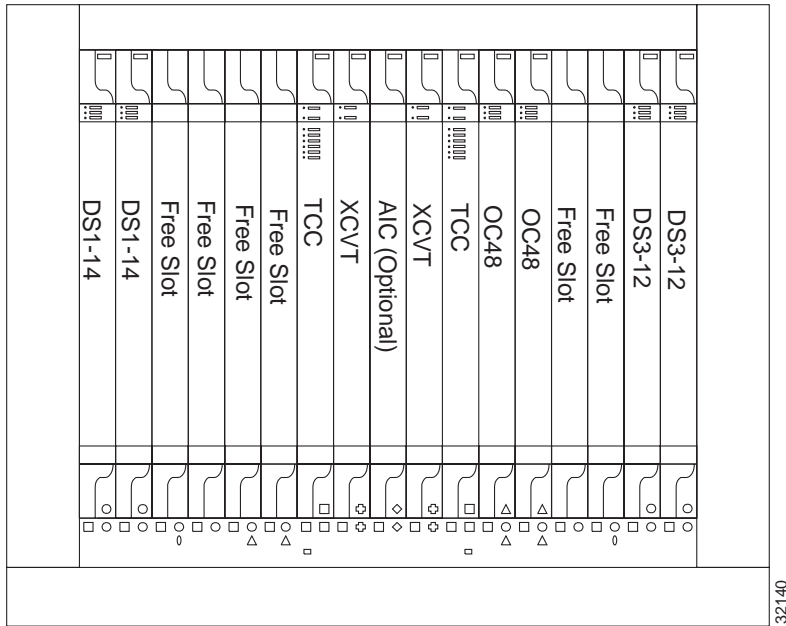
5.2.5 Setting Up BLSRs

To set up a BLSR on the ONS 15454, you perform five basic procedures:

- Install the BLSR trunk cards. See the "Install the BLSR Trunk Cards" procedure on page 5-11.

- Create the BLSR DCC terminations. See the "Create the BLSR DCC Terminations" procedure on page 5-13.
- Enable the BLSR ports. See the "Enable the BLSR Ports" procedure on page 5-13.
- Set up BLSR timing. See the "Set up ONS 15454 Timing" procedure on page 3-14.
- Provision the BLSR. See the "Provision the BLSR" procedure on page 5-14.

Procedure: Install the BLSR Trunk Cards

Step 1   Install the OC-12, OC-48, OC-48AS, or OC-192 cards that will serve as the BLSR trunk cards. You can install the OC-12 and OC-48AS cards in any slot, but you can install the OC-48 and OC-192 cards only in Slots 5, 6, 12, or 13.

Step 2   Allow the cards to boot.

Step 3   Attach the fiber to the east and west BLSR ports at each node.

Plan your fiber connections and use the same plan for all BLSR nodes. For example, make the east port the farthest slot to the right and the west port the farthest left. Plug fiber connected to an east port at one node into the west port on an adjacent node. Figure 5-11 shows fiber connections for a two-fiber BLSR with trunk cards in Slot 5 (west) and Slot 12 (east).

Note   Always plug the transmit (Tx) connector of an OC-N card at one node into the receive (Rx) connector of an OC-N card at the adjacent node. Cards will display an SF LED if Tx and Rx connections are mismatched.

For four-fiber BLSRs, use the same east - west connection pattern for the working and protect fibers. Do not mix working and protect card connections. The BLSR will not function if working and protect cards are interconnected. Figure 5-12 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 5-11   Connecting fiber to a four-node, two-fiber BLSR
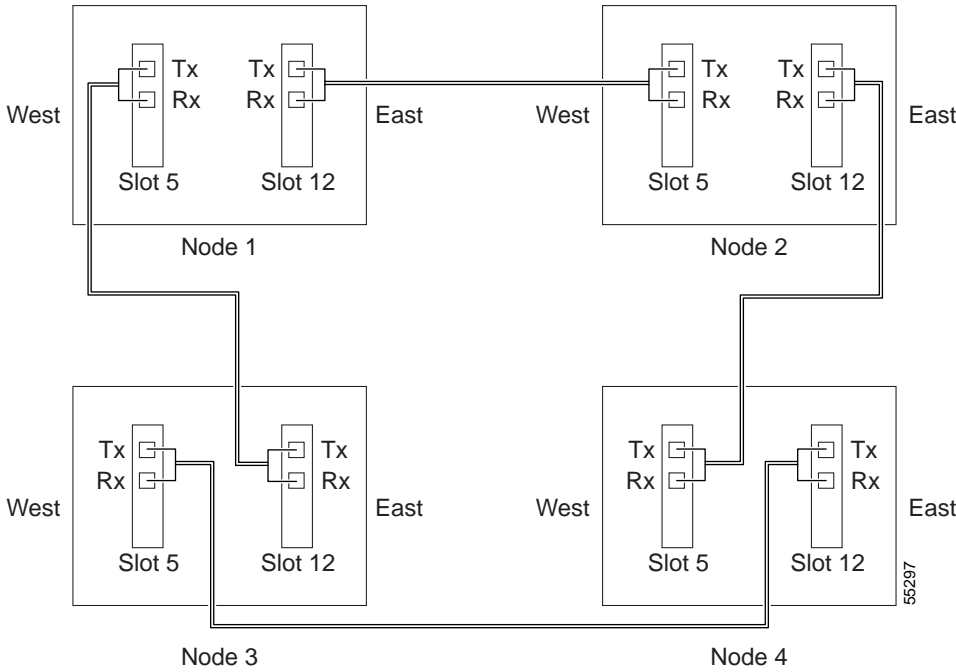
Figure 5-12   Connecting fiber to a four-node, four-fiber BLSR
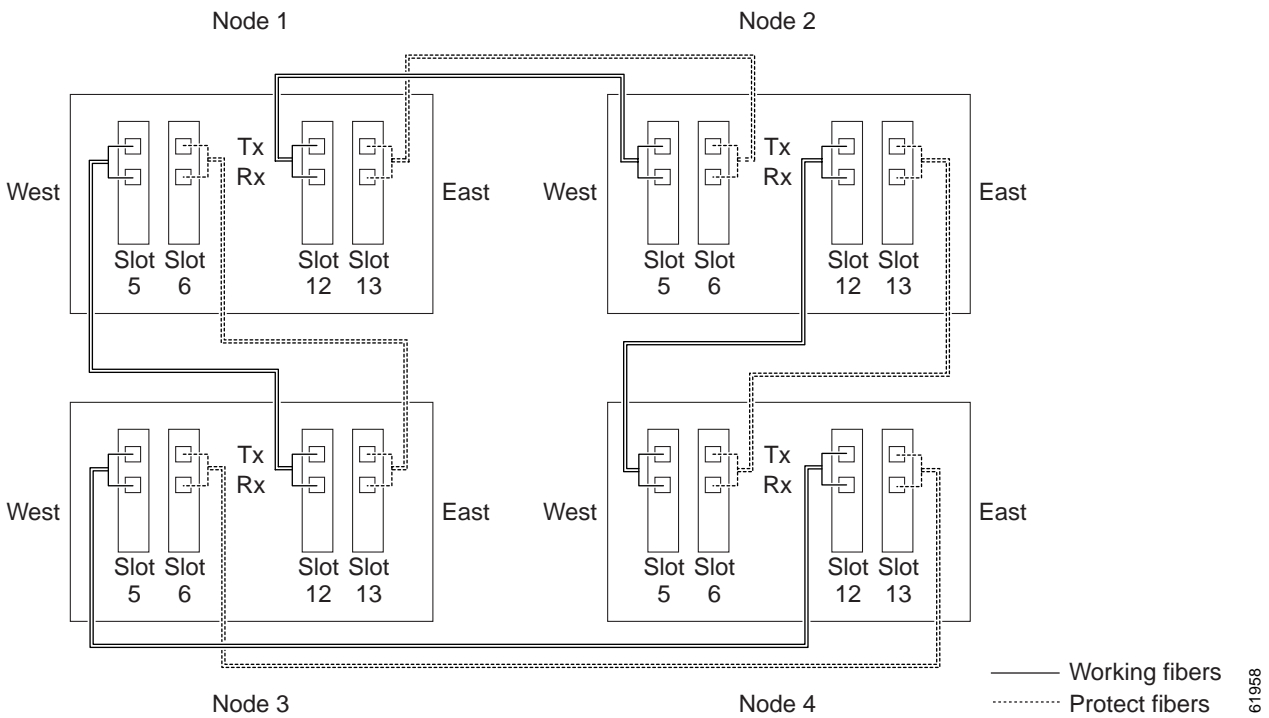
Procedure: Create the BLSR DCC Terminations

Step 1   Log into the first node that will be in the BLSR.

Step 2   Click the **Provisioning > Sonet DCC** tabs.

Step 3   In the SDCC Terminations section, click **Create**.

Step 4   On the Create SDCC Terminations dialog, press **Ctrl** and click the two slots/ports that will serve as the BLSR ports at the node. For example, Slot 5 (OC-48)/Port 1 and Slot 12 (OC-48)/ Port 1. For four-fiber BLSRs, provision the working cards, but not the protect cards, as DCC terminations.

Step 5   Click **OK**.

Step 6   The slots/ports appear in the SDCC Terminations list.

Step 7   Complete Steps 2 – 5 at each node that will be in the BLSR.

> **Note**   The ONS 15454 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs; therefore, the Line DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 networks. For more detail, see the "Creating DCC Tunnels" section on page 6-21.

Procedure: Enable the BLSR Ports

Step 1   Log into one of the nodes that will be in the BLSR.

Step 2   Double-click one of the OC-N cards that you configured as a DCC termination.

Step 3   Click the **Provisioning > Line** tabs.

Step 4   Click **Status** (Figure 5-13) and choose **In Service**.

Figure 5-13   Enabling an optical port
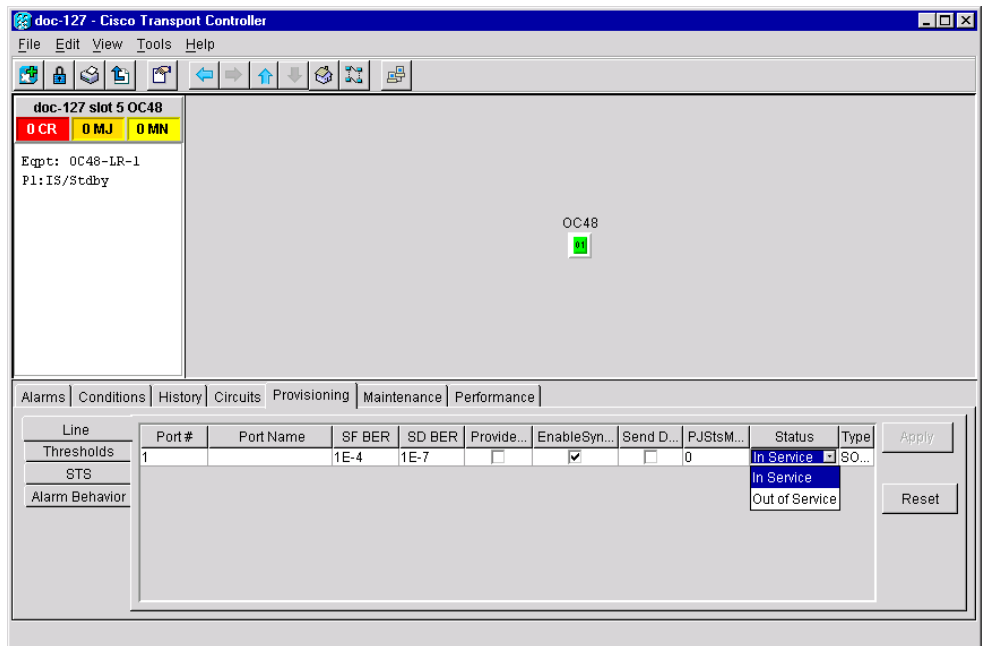
Step 5   Repeat Steps 2 – 4 for the other optical card configured as a DCC termination.

Step 6   (Four-fiber BLSR only) Repeat Steps 2 – 4 for each protect card.

Step 7   Repeat Steps 2 – 5 at each node that will be in the BLSR.

After configuring the SONET DCC, set the timing for the node. For procedures, see the "Setting Up ONS 15454 Timing" section on page 3-12. After you configure the timing you can provision the BLSR.

Procedure: Provision the BLSR

Step 1   Log into one BLSR node.

Step 2   Select the **Provisioning > Ring** tabs.

Step 3   Click **Create**.

Step 4   On the Create BLSR dialog box (Figure 5-14), set the BLSR properties:

- *Ring Type*—select the BLSR ring type, either two-fiber or four-fiber.

- *Ring ID*—Assign a ring ID (a number between 0 and 9999). Nodes in the same BLSR must have the same Ring ID.

- *Node ID*—Assign a Node ID. The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs.

- *Reversion time*—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR ring should have the same reversion time setting, particularly if "never" (i.e., non-revertive) is selected.

- *West Port*—Assign the west BLSR port for the node from the pull-down menu. (In Figure 5-11, this is Slot 5.)

- *East Port*—Assign the east BLSR port for the node from the pull-down menu. (In Figure 5-11, this is Slot 12.)

The east and west ports must match the fiber connections and DCC terminations set up in the "Install the BLSR Trunk Cards" procedure on page 5-11 and the "Create the BLSR DCC Terminations" procedure on page 5-13.

For four-fiber BLSRs, complete the following:

- *Span Reversion*—Set the amount of time that will pass before the traffic reverts to the original working path following a span reversion. The default is 5 minutes. Span reversions can be set to Never. If you set a reversion time, the times must be the same for both ends of the span. That is, if Node A's west fiber is connected to Node B's east port, the Node A west span reversion time must be the same as the Node B east span reversion time. To avoid reversion time mismatches, Cisco recommends that you use the same span reversion time throughout the ring.

- *West Protect*—Assign the west BLSR port that will connect to the west protect fiber from the pull-down menu. (In Figure 5-12, this is Slot 6.)

- *East Protect*—Assign the east BLSR port that will connect to the east protect fiber from the pull-down menu. (In Figure 5-12, this is Slot 13.)

Figure 5-14   Setting BLSR properties
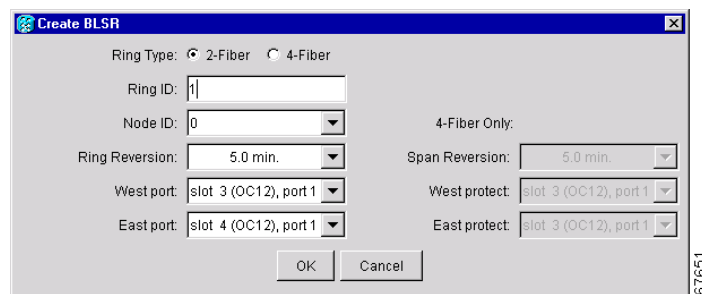
Step 5   Click **OK**.

> **Note**   Some or all of the following alarms display during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

Step 6   Complete Steps 2 – 5 at each node that you are adding to the BLSR.

Step 7   After you configure the last BLSR node, wait for the BLSR Ring Map Change dialog box to display (this can take 10 – 30 seconds).

> **Note**   The dialog box will not display if SDCC Termination alarms (e.g., EOC) or BLSR alarms (such as E-W MISMATCH and RING MISMATCH) are present. If an SDCC alarm is present, review the DCC provisioning at each node; use the "Create the BLSR DCC Terminations" procedure on page 5-13. If BLSR alarms have not cleared, repeat Steps 1 – 6 at each node, making sure each node is provisioned correctly. You can also following alarm troubleshooting procedures provided in the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.

Step 8   On the BLSR Ring Map Change dialog, click **Yes**.

Step 9   On the BLSR Ring Map dialog box, verify that the ring map contains all the nodes you provisioned in the expected order. If so, click **Accept**. If the nodes do not appear, or are not in the expected order, repeat Steps 1 – 8, making sure no errors are made.

Step 10   Switch to network view and verify the following:

- A green span line appears between all BLSR nodes
- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared.

Step 11   Test the BLSR using testing procedures normal for your site. Here are a few steps you can use:

   a.   Run test traffic through the ring.

   b.   Log into a node, click the **Maintenance > Ring** tabs, and choose **MANUAL RING** from the East Switch list. Click **Apply**.

   c.   In network view, click the **Conditions** tab and click **Retrieve**. You should see a Ring Switch West event, and the far-end node that responded to this request will report a Ring Switch East event.

   d.   Verify that traffic switches normally.

   e.   Choose **Clear** from the East Switch list and click **Apply**.

   f.   Repeat Steps a – d for the West Switch.

   g.   Disconnect the fibers at one node and verify that traffic switches normally.

5.2.6 Upgrading From Two-Fiber to Four-Fiber BLSRs

Two-fiber OC-48 or OC-192 BLSRs can be upgraded to four-fiber BLSRs. To upgrade, you install two OC-48 or OC-192 cards at each two-fiber BLSR node, then log into CTC and upgrade each node from two-fiber to four-fiber. The fibers that were divided into working and protect bandwidths for the two-fiber BLSR are now fully allocated for working BLSR traffic.

Procedure: Upgrade From a Two-Fiber to a Four-Fiber BLSR

Step 1   Log into one of the two-fiber BLSR nodes. In network view:

   a.   Verify that all spans between BLSR nodes on the network map are green.

   b.   Click the **Alarms** tab. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. In a BLSR, these facility conditions may be reported as minor alarms.

   c.   Click the **Conditions** tab, then click **Retrieve Conditions**. Verify that no ring switches are active.

If trouble is indicated, for example, a major alarm exists, resolve the problem before proceeding to Step 2. See the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for additional information.

Step 2   Install two OC-48 or OC-192 cards at each BLSR node. You must install the same OC-N card rate as the two fiber.

Step 3   Enable the ports for each new OC-N card:

   a.   Display the card in card view.

   b.   Click the **Provisioning > Line** tabs.

    c. Click **Status** and choose **In Service**.

    d. Click **Apply**.

    e. Repeat Steps a – d for each new OC-N card at each BLSR node.

Step 4 Connect the fiber to the new cards. Use the same east – west connection scheme that was used to create the two-fiber connections. Figure 5-12 shows an example.

Step 5 Test the new fiber connections using procedures standard for your site. For example, pull a Tx fiber for a protect card and verify that an LOS alarm displays for the appropriate Rx card. Do this fiber test for every span in the BLSR protect ring.

Step 6 Perform a span lockout at each BLSR node:

    a. At one of the BLSR nodes, switch to node view. Click the **Maintenance > Ring** tabs.

    b. Under West Switch for the two-fiber BLSR you will convert, select **LOCKOUT SPAN**. Click **Apply**

    c. Under East Switch, select **LOCKOUT SPAN**. Click **Apply**.

    d. Repeat Steps a – c at each node in the two-fiber BLSR.

Step 7 Upgrade each node from two-fiber to four-fiber BLSR:

    a. At one of the BLSR nodes, switch to node view. Click the **Provisioning > Ring** tabs.

    b. Select the two-fiber BLSR. Click **Upgrade**.

    c. On the Upgrade BLSR dialog box, complete the following:

        – *Span Reversion*—Set the amount of time that will pass before the traffic reverts to the original working path following a span reversion. The default is 5 minutes.

        – *West Protect*—Assign the east BLSR port that will connect to the east protect fiber from the pull-down menu. (In Figure 5-12, this is Slot 6.)

        – *East Protect*—Assign the east BLSR port that will connect to the east protect fiber from the pull-down menu. (In Figure 5-12, this is Slot 13.)

    d. Click **Ok**.

    e. Complete Steps a – d at each two-fiber BLSR node.

Step 8 Clear the span lockout:

    a. Display a BLSR node in node view. Click the **Maintenance > Ring** tabs.

    b. Under West Switch, select **CLEAR**. Click **Apply**

    c. Under East Switch, select **CLEAR**. Click **Apply**.

    d. Repeat Steps a – c at each node in the new four-fiber BLSR.

    e. Switch to network view. Verify that no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. If an alarm is present, resolve the problem using procedures in the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.

Step 9 Test the four-fiber BLSR using procedures in Step 11 in the "Provision the BLSR" procedure on page 5-14.

5.2.7 Adding and Removing BLSR Nodes

This section explains how to add and remove BLSR nodes. To add or remove a node, you force a protection switch to route traffic away from the span where you will add or remove the node. Figure 5-15 shows a three-node BLSR before the new node is added. To add Node 3, you would:

* Force a protection switch on the Node 1 (Slot 5, West) and Node 4 (Slot 12, East) span. The protection switch forces traffic away from the fibers that you will remove and reconnect to the added node.

* Remove fibers from Node 1/Slot 5 and Node 4/Slot 12, then, using additional fibers, connect Node 1 and Node 4 to Node 3.

* Remove the protection switch to route traffic through the added node.

Note   You can only add one node at a time to an ONS 15454 BLSR.

Figure 5-15   A three-node BLSR before adding a new node
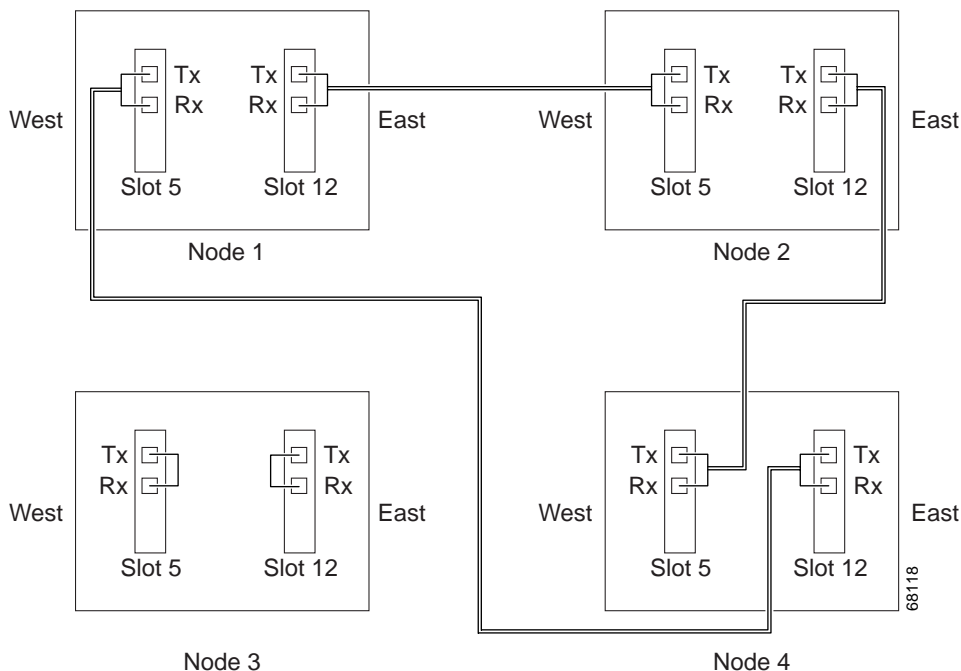
Procedure: Add a BLSR Node

Perform these steps on-site and not from a remote location.

Step 1   Draw a diagram, similar to Figure 5-15, for the BLSR installation where you will add the node. In the diagram, identify the nodes, cards (slots) and spans (east or west) that will connect to the new node. This information is essential to complete this procedure without error. For example, in Figure 5-15, you would circle Slot 5 (west) on Node 1, and Slot 12 (east) on Node 4.

Step 2   Log into CTC and display the BLSR nodes in network view. Verify the following:

- All BLSR spans on the network map are green.

- On the **Alarms** tab, no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. In a BLSR, these facility conditions may be reported as minor alarms.

- On the **Conditions** tab, no ring switches are active.

If trouble is indicated, for example, a major alarm exists, resolve the problem before proceeding.

Step 3   Install the OC-N cards in the ONS 15454 that you will add to the BLSR; use the "Install the BLSR Trunk Cards" procedure on page 5-11. Ensure fiber cables are available to connect to the cards. Run test traffic through the node to ensure the cards are functioning properly.

Step 4   Log into the new node and complete the BLSR setup.

- Provision the SONET DCC using the "Create the BLSR DCC Terminations" procedure on page 5-13.

- Configure the BLSR timing using the "Set up ONS 15454 Timing" procedure on page 3-14.

- Enable the BLSR ports using the "Enable the BLSR Ports" procedure on page 5-13.

- Provision the BLSR using the "Provision the BLSR" procedure on page 5-14

Step 5   Log into the node that will connect to the new node through its east port (Node 4 in the Figure 5-15 example).

Step 6   Switch protection on the east port:

a.   Click the **Maintenance > Ring** tabs.

b.   From the East Switch list, choose **FORCE RING**. Click **Apply**.

Performing a FORCE switch generates a manual switch request on an equipment (MANUAL-REQ) alarm. This is normal.

⚠

Caution   Traffic is unprotected during a protection switch.

Step 7   Log into the node that will connect to the new node through its west port (Node 1 in the Figure 5-15 example).

Step 8   Switch protection on the west port:

a.   Click the **Maintenance > Ring** tabs.

b.   From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 9   Following the diagram that you created in Step 1, remove the fiber connections from the two nodes that will connect directly to the new node.

a.   Remove the east fiber from the node that will connect to the west port of the new node. In the Figure 5-15 example, this is Node 4/Slot 12.

b.   Remove the west fiber from the node that will connect to the east port of the new node. In the Figure 5-15 example, this is Node 1/Slot 5.

Step 10   Replace the removed fibers with fibers that are connected to the new node. Connect the west port to the east port and the east port to the west port. Figure 5-16 shows the BLSR in the Figure 5-15 example after the node is connected.

Figure 5-16   A BLSR with a newly-added fourth node
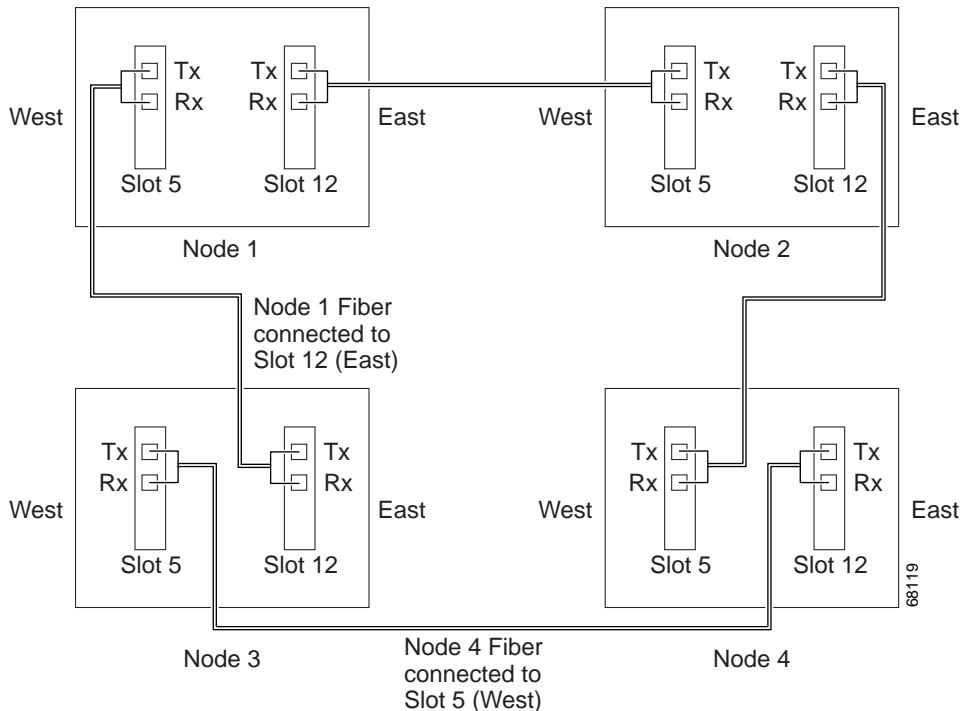
Step 11 Log out of CTC and then log back into any node in the BLSR.

Step 12 In node view, select the **Provisioning > Ring** tabs and click **Ring Map**.

Step 13 On the BLSR Map Ring Change dialog box, click **Yes**.

Step 14 On the BLSR Ring Map dialog box, verify that the new node is added. If it is, click **Accept**. If it does not appear, log into the new node. Verify that the BLSR is provisioned correctly according to the "Provision the BLSR" procedure on page 5-14, then repeat Steps 12 – 13. If the node still does not appear, repeat the steps in the procedure making sure that no errors were made.

Step 15 From the Go To menu, select **Network View**. Click the **Circuits** tab. Wait until all the circuits are discovered. The circuits that pass through the new node will be shown as incomplete.

Step 16 In network view, right-click the new node and select **Update Circuits With The New Node** from the shortcut menu. Verify that the number of updated circuits displayed in the dialog box is correct.

Step 17 Select the **Circuits** tab and verify that no incomplete circuits are present.

Step 18 Clear the protection switch for the node that is using its east port to connect to the new node, and for the node that is using its west port to connect to the new node.

   a. To clear the protection switch from the east port, display the **Maintenance > Ring** tabs. From the East Switch list choose **CLEAR**. Click **Apply**.

   b. To clear the protection switch from the west port, choose **CLEAR** from the West Switch list. Click **Apply**.

Procedure: Remove a BLSR Node

⚠

Caution   The following procedure minimizes traffic outages during node deletions, but traffic will be lost when you delete and recreate circuits that passed through the deleted node.

Step 1   Before you start this procedure, make sure you know the following:

- Which node is connected through its east port to the node that will be deleted. For example if you are deleting Node 1 in Figure 5-16, Node 3 is the node connected through its east port to Node 1.

- Which node is connected through its west port to the node that will be deleted. In Figure 5-16, Node 2 is connected to Node 1 through its west port.

Step 2   Log into a node on the same BLSR as the node you will remove. (Do not log into the node that you will remove.)

Step 3   Display the BLSR nodes in network view and verify the following:

- All BLSR spans on the network map are green.

- No critical or major alarms (LOF, LOS, ASP, ASL) are displayed on the **Alarms** tab.

- On the **Conditions** tab, no ring switches are active.

If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding.

Step 4   Display the node that you will remove in node view.

Step 5   Delete all the circuits that originate or terminate in that node. (If a circuit has multiple drops, delete only the drops that terminate on the node you want to delete.)

    a.   Click the **Circuits** tab. The circuits that use this node are displayed.

    b.   Select circuits that originate or terminate on the node. Click **Delete**.

    c.   Click **Yes** when prompted.

    d.   If a multidrop circuit has drops at the node that will be removed, select the circuit, click **Edit**, and remove the drops.

Step 6   Complete this step if circuits that were created using Cisco Transport Controller Release 2.x. pass through the node that will be deleted (i.e., circuits are displayed on the Circuits tab).

    a.   On the Circuits tab of the node that will be deleted, select a circuit and click **Edit**.

    b.   On the Edit Circuits window, check **Show Detailed Map**.

    c.   Verify that the circuits enter and exit the node on the same STS. For example, if a circuit enters on s5/p1/S1 (Slot 5, Port 1, STS1), verify that it exits on STS1. If a circuit enters/exits on different STSs, write down the name of the circuit. You will delete and recreate these circuits in Step e.

    d.   From the View menu select **Go to Network View**, then select the **Circuits** tab.

    e.   Delete and recreate each circuit recorded in Step c. To delete the circuit, select the circuit on the Circuits window and click the **Delete** button. To create the circuit, go to the "Create an Automatically Routed Circuit" procedure on page 6-2.

    f.   Repeat Steps a – e for each circuit displayed on the Circuits tab.

Cisco ONS 15454 Installation and Operations Guide ■

Step 7   Use information recorded in Step 1 to switch traffic away from the ports of neighboring nodes that will be disconnected when the node is removed:

⚠️

Caution   Traffic is unprotected during the protection switch.

    a.   Open the neighboring node that is connected through its east port to the removed node.

    b.   Click the **Maintenance > Ring** tabs.

    c.   From the East Switch list, choose **FORCE RING**. Click **Apply**.

    d.   Open the node that is connected through its west port to the removed node.

    e.   Click the **Maintenance > Ring** tabs.

    f.   From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 8   Remove all fiber connections between the node being removed and the two neighboring nodes.

Step 9   Reconnect the two neighboring nodes directly, west port to east port.

Step 10   Close CTC, then log into a node on the reduced ring.

Step 11   Wait for the BLSR Map Ring Change dialog box to display. (If the dialog box does not display after 10 – 15 seconds, select the **Provisioning > Ring** tabs and click **Ring Map**.) When the dialog box displays, click **Yes**.

Step 12   On the BLSR Ring Map dialog box, click **Accept**.

Step 13   Clear the protection switches on the neighboring nodes:

    a.   Open the node with the protection switch on its east port.

    b.   Click the **Maintenance > Ring** tabs and choose **CLEAR** from the East Switch list. Click **Apply**.

    c.   Open the node with the protection switch on its west port.

    d.   Click the **Maintenance > Ring** tabs and choose **CLEAR** from the West Switch list. Click **Apply**.

Step 14   If a BITS clock is not used at each node, check that the synchronization is set to one of the eastbound or westbound BLSR spans on the adjacent nodes. If the removed node was the BITS timing source, use a new node as the BITS source or select internal synchronization at one node where all other nodes will derive their timing. (For information about ONS 15454 timing, see the "Setting Up ONS 15454 Timing" section on page 3-12.)

5.2.8 Moving BLSR Trunk Cards

⚠️

Caution   Call the Technical Assistance Center (1-877-323-7368) before performing this procedure to ensure that circuit and provisioning data is preserved.

⚠️

Caution   To change BLSR trunk cards, you will drop one node at a time from the current BLSR. This procedure is service affecting during the time needed to complete the steps below. This applies to all BLSR nodes where cards will change slots. Review all the steps before you proceed.

Figure 5-17 shows a four node OC-48 BLSR using trunk cards in Slots 6 and 12 at all four nodes. Trunk cards will be moved at Node 4 from Slots 6 and 12 to Slots 5 and 6. To do this Node 4 is temporarily removed from the active BLSR while the trunk cards are switched.

Figure 5-17   A four-node BLSR before a trunk card switch
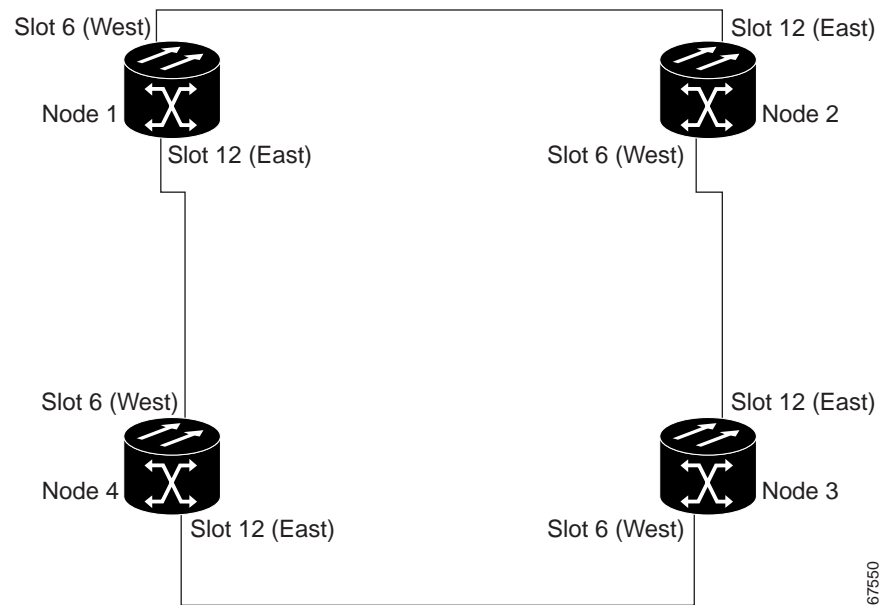
Figure 5-18 shows the BLSR after the cards are switched.

Figure 5-18   A four-node BLSR after the trunk cards are switched at one node
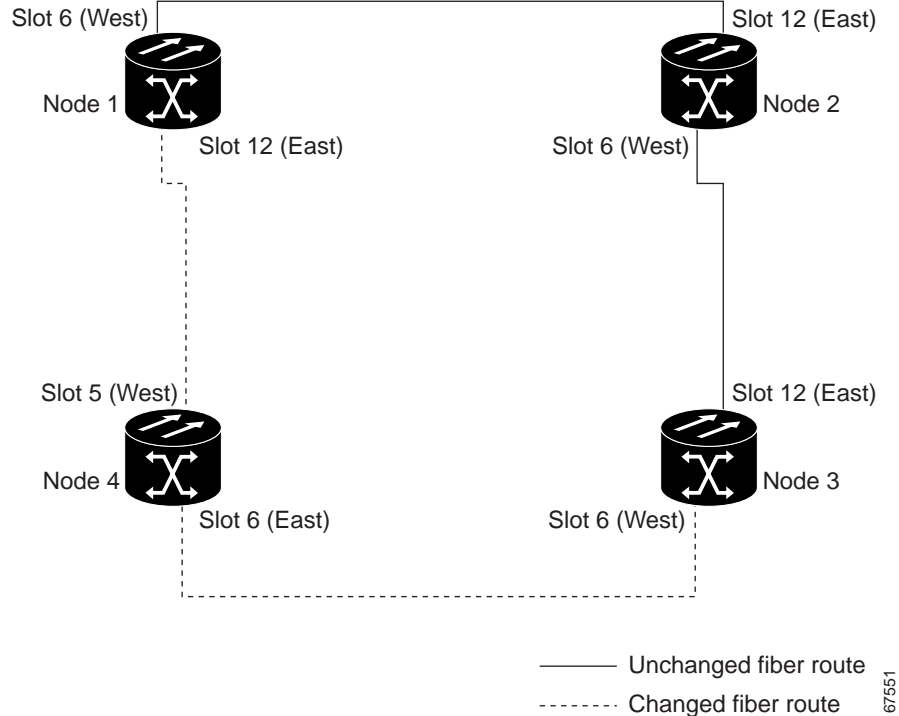
Procedure: Move a BLSR Trunk Card

Use the following steps to move one BLSR trunk card to a different slot. Use this procedure for each card you want to move. Although the procedure is for OC-48 BLSR trunk cards, you can use the same procedure for OC-12, OC-48AS, and OC-192 cards.

> **Note**   The ONS 15454 nodes must have CTC Release 2.0 or later and cannot have active alarms for the OC-48 or OC-12 cards or the BLSR configuration.

Step 1   Log into CTC and display the BLSR nodes in network view. Verify the following:

- All BLSR spans on the network map are green.
- On the **Alarms** tab, no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. In a BLSR, these facility conditions may be reported as minor alarms.
- On the **Conditions** tab, no ring switches are active.

If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding. Refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for alarm troubleshooting procedures.

Step 2   Switch traffic away from the node where the trunk card will be switched:

   a.   Log into the node that is connected through its east port to the node where the trunk card will be moved. (In the Figure 5-17 example, this is Node 1.) Click the **Maintenance > Ring** tabs.

   b.   From the East Switch list, choose **FORCE RING**. Click **Apply**.

When you perform a manual switch, a manual switch request equipment alarm (MANUAL-REA) is generated. This is normal.

⚠

Caution   Traffic is unprotected during a protection switch.

c. Log into the node that is connected through its west port to the node where the trunk card will be moved. (In the Figure 5-17 example, this is Node 3.) Click the **Maintenance > Ring** tabs.

d. From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 3   Log into the node where the trunk card you will move is installed.

Step 4   Click the **Circuits** tab (Figure 5-19). Write down the circuit information or, from the File menu, select **Print** or **Export** to print or export the information; you will need it to restore the circuits later. See the "Printing and Exporting CTC Data" section on page 2-26 for more information.

Figure 5-19   Deleting circuits from a BLSR trunk card
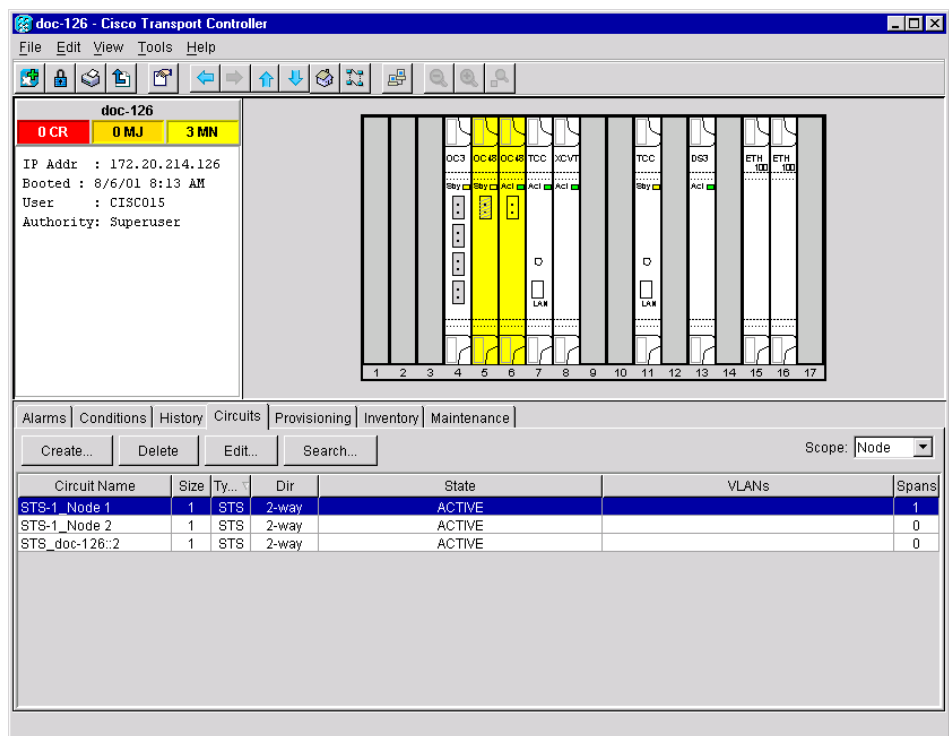
Step 5   Delete the circuits on the card you are removing:

a. Highlight the circuit(s). To select multiple circuits, press the Shift or Ctrl key.

b. Click **Delete**.

c. On the Delete Circuit dialog box, click **Yes**.

Step 6   Delete the SONET DCC termination on the card you are removing:

a. Click the **Provisioning > Sonet DCC** tabs.

b. From the SDCC Terminations list, click the SONET DCC you need to delete and click **Delete**.

Step 7   Disable the ring on the current node:

    a.   Click the **Provisioning > Ring** tabs.

    b.   Highlight the ring and click **Delete**.

    c.   On the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 8   If an OC-N card is a timing source, select the **Provisioning > Timing** tabs and set timing to Internal.

Step 9   Place the ports on the card out of service:

    a.   Double-click the card.

    b.   On the **Provisioning > Line** tabs in the Status section, choose **Out of Service** for each port.

Step 10   Physically remove the card.

Step 11   Insert the card into its new slot and wait for the card to boot.

Step 12   To delete the card from its former slot, right-click the card in node view and select **Delete** from the list of options.

Step 13   Place the port(s) back in service:

    a.   To open the card, double-click or right-click the card and select **Open**.

    b.   Click the **Provisioning** tab.

    c.   From Status choose **In Service**.

    d.   Click **Apply**.

Step 14   Follow the steps described in the "Setting Up BLSRs" section on page 5-10 to reenable the ring using the same cards (in their new slots) and ports for east and west. Use the same BLSR Ring ID and Node ID that was used before the trunk card was moved.

Step 15   Recreate the circuits that were deleted. See the "Create an Automatically Routed Circuit" procedure on page 6-2 for instructions.

Step 16   If you use line timing and the card you are moving is a timing reference, reenable the timing parameters on the card. See the "Set up ONS 15454 Timing" procedure on page 3-14 for instructions.

5.3 Unidirectional Path Switched Rings

UPSRs provide duplicate fiber paths around the ring. Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs in the working traffic path, the receiving node switches to the path coming from the opposite direction.

CTC automates ring configuration. UPSR traffic is defined within the ONS 15454 on a circuit-by-circuit basis. If a path-protected circuit is not defined within a 1+1 or BLSR line protection scheme and path protection is available and specified, CTC uses UPSR as the default.

Figure 5-20 shows a basic UPSR configuration. If Node ID 0 sends a signal to Node ID 2, the working signal travels on the working traffic path through Node ID 1. The same signal is also sent on the protect traffic path through Node ID 3. If a fiber break occurs (Figure 5-21), Node ID 2 switches its active receiver to the protect signal coming through Node ID 3.

Because each traffic path is transported around the entire ring, UPSRs are best suited for networks where traffic concentrates at one or two locations and is not widely distributed. UPSR capacity is equal to its bit rate. Services can originate and terminate on the same UPSR, or they can be passed to an adjacent access or interoffice ring for transport to the service-terminating location.

Figure 5-20   A basic four-node UPSR
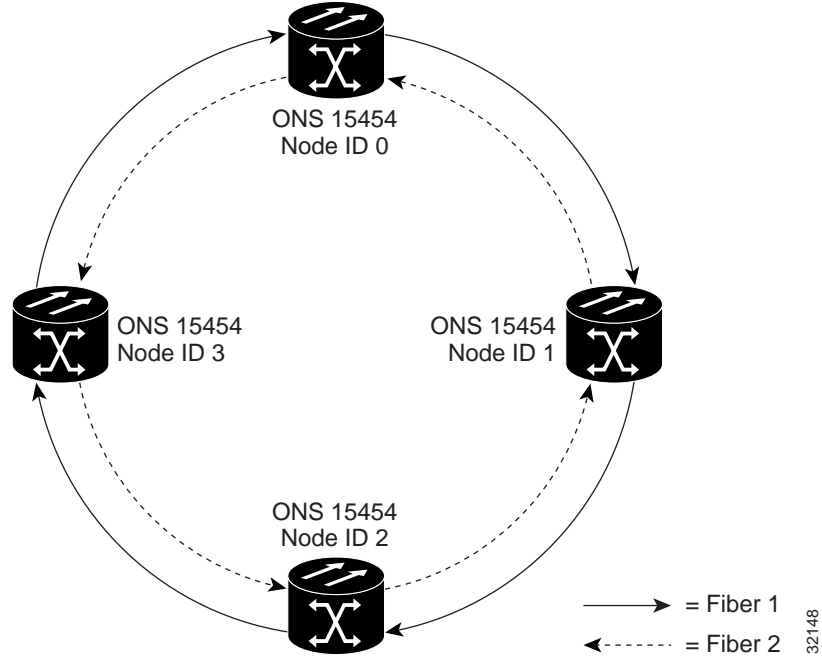
Figure 5-21   A UPSR with a fiber break
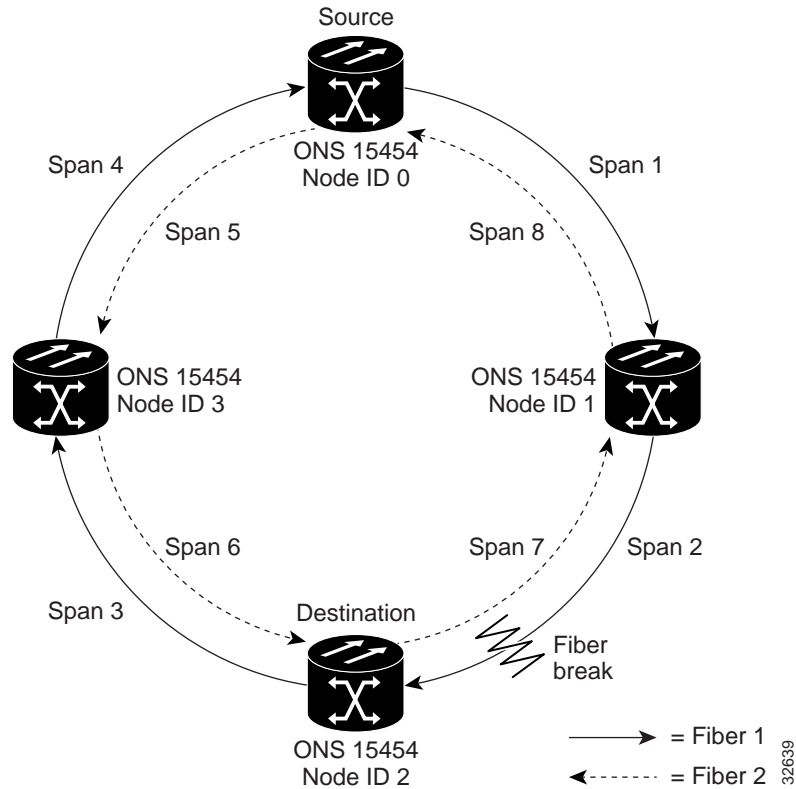
5.3.1 Example UPSR Application

Figure 5-22 shows a common UPSR application. OC-3 optics provide remote switch connectivity to a host TR-303 switch. In the example, each remote switch requires eight DS-1s to return to the host switch. Figure 5-23 and Figure 5-24 show the shelf layout for each site.

Figure 5-22   An OC-3 UPSR
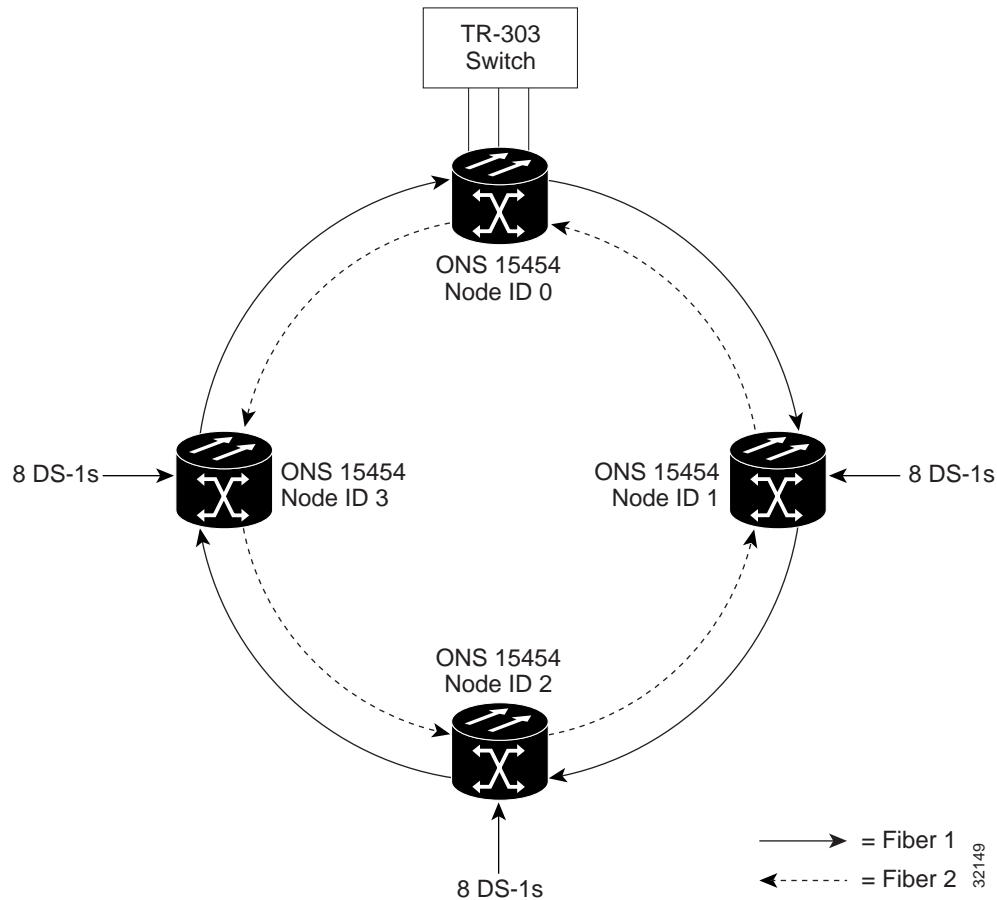
Node ID 0 has four DS1-14 cards to provide 56 active DS-1 ports. The other sites only require two DS1-14 cards to handle the eight DS-1s to and from the remote switch. You can use the other half of each ONS 15454 shelf assembly to provide support for a second or third ring to other existing or planned remote sites.

In this sample OC-3 UPSR, Node ID 0 contains four DS1-14 cards and two OC3 IR 4 1310 cards. Six free slots also exist in this setup and can be provisioned with cards or left empty. Figure 5-23 shows the shelf setup for these cards.

Figure 5-23   Layout of Node ID 0 in the OC-3 UPSR example (Figure 5-15)
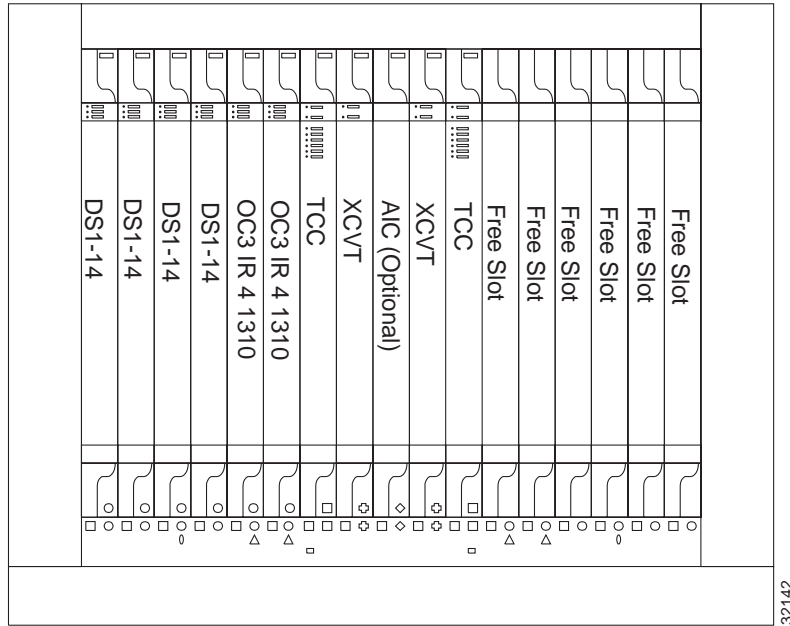
In the Figure 5-22 on page 5-28 example, Nodes IDs 1 - 3 each contain two DS1-14 cards and two OC3 4 IR 1310 cards. Eight free slots exist. They can be provisioned with other cards or left empty. Figure 5-24 shows the shelf assembly setup for this configuration sample.

Figure 5-24   Layout of Node IDs 1 – 3 in the OC-3 UPSR example (Figure 5-15)
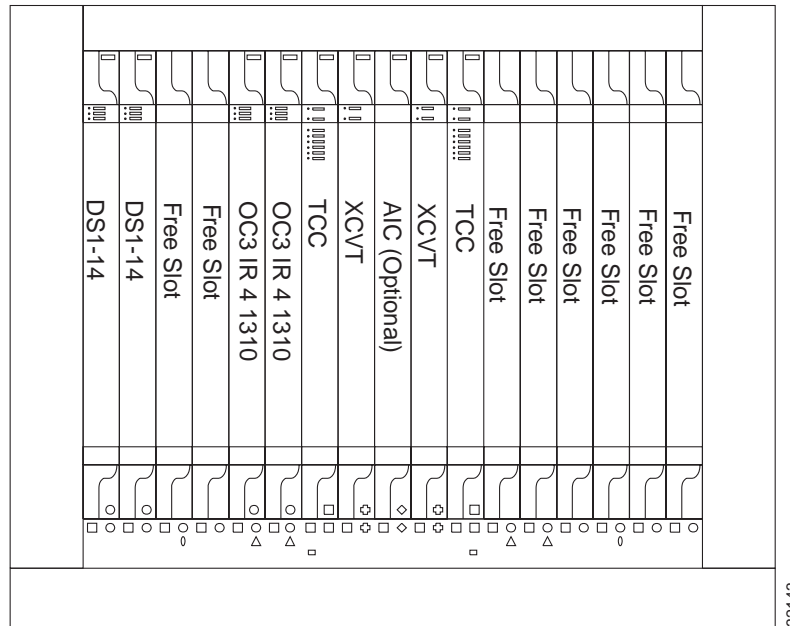
5.3.2 Setting Up a UPSR

To set up a UPSR, you perform four basic procedures:

- Install the UPSR trunk cards. Use the "Install the UPSR Trunk Cards" procedure on page 5-30
- Create the DCC terminations. Use the "Configure the UPSR DCC Terminations" procedure on page 5-31.
- Configure the timing. Use the "Setting Up ONS 15454 Timing" section on page 3-12.
- Enable the ports. Use the "Enable the UPSR Ports" procedure on page 5-32.

After you enable the ports, you set up the UPSR circuits. UPSR signal thresholds—the levels that determine when the UPSR path is switched—are set at the circuit level. To create UPSR circuits, see the "Circuits Overview" section on page 6-1.

Procedure: Install the UPSR Trunk Cards

Step 1 Install the OC-N cards that will serve as the UPSR trunk cards. You can install the OC-3, OC-12, and OC-48AS cards in any slot, but the OC-48 and OC-192 cards can only be installed in Slots 5, 6, 12, or 13.

Step 2 Allow the cards to boot.

Step 3 Attach the fiber to the east and west UPSR ports at each node.

To avoid errors, make the east port the farthest slot to the right and the west port the farthest left. Fiber connected to an east port at one node must plug into the west port on an adjacent node. Figure 5-25 shows fiber connections for a four-node UPSR with trunk cards in Slot 5 (west) and Slot 12 (east).

Always plug the fiber plugged into the transmit (Tx) connector of an OC-N card at one node into the receive (Rx) connector of an OC-N card at the adjacent node. The card will display an SF LED if Tx and Rx fibers are mismatched.

Figure 5-25   Connecting fiber to a four-node UPSR
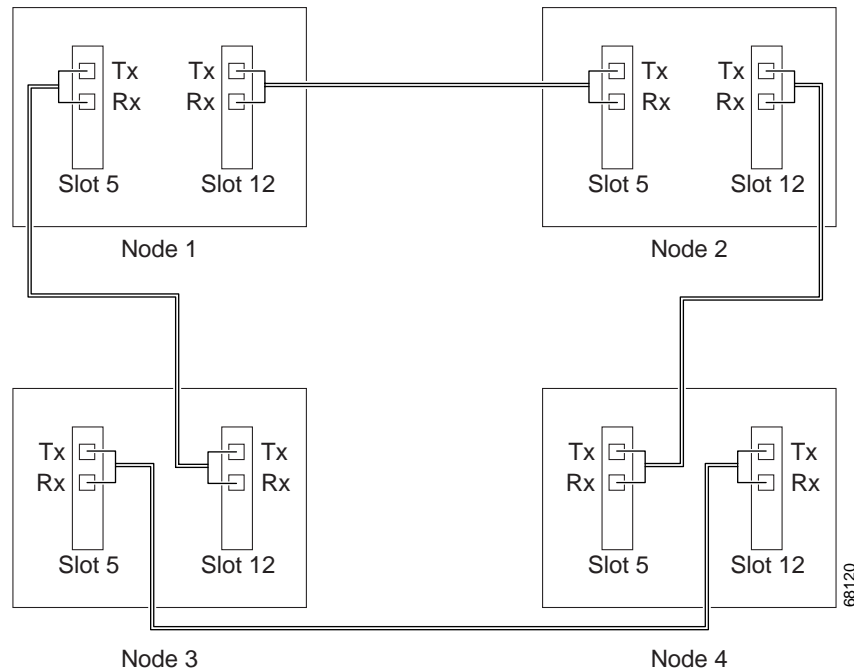
Procedure: Configure the UPSR DCC Terminations

Step 1   Log into the first node that will be in the UPSR.

Step 2   Click the **Provisioning > Sonet DCC** tabs.

Step 3   In the SDCC Terminations section, click **Create**.

Step 4   On the Create SDCC Terminations dialog box, press Control and click the two slots/ports that will serve as the UPSR ports at the node. For example, Slot 6 (OC-48)/Port 1 and Slot 12 (OC-48)/Port 1.

> ✎
>
> **Note**   The ONS 15454 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs. Line DCCs can be used to tunnel DCCs from third party equipment across ONS 15454 networks. For procedures, see the "Creating DCC Tunnels" section on page 6-21.

Step 5   Click **OK**.

The slots/ports display in the SDCC Terminations section.

Step 6   Complete Steps 2 – 5 at each node that will be in the UPSR.

After configuring the SONET DCC, set the timing for the node. For procedures, see the "Setting Up ONS 15454 Timing" section on page 3-12. After configuring the timing, enable the UPSR ports as described in the following procedure.

Procedure: Enable the UPSR Ports

Step 1   Log into the first UPSR node.

Step 2   Double-click one of the cards that you configured as an SDCC termination.

Step 3   Click the **Provisioning > Line** tabs.

Step 4   Under Status, select **In Service** for each port that you want enabled.

Step 5   Repeat Steps 2 - 4 for the second card.

Step 6   Click **Apply**.

You configured a UPSR for one node. Use the same procedures to configure the additional nodes. To create path-protected mesh networks, see the "Path-Protected Mesh Networks" section on page 5-50. To create circuits, see the "Circuits Overview" section on page 6-1.

5.3.3 Adding and Removing UPSR Nodes

This section explains how to add and remove nodes in an ONS 15454 UPSR configuration. To add or remove a node, you switch traffic on the affected spans to route traffic away from the area of the ring where service will be performed. Use the span selector switch option to switch traffic from a UPSR span at different protection levels. The span selector switch option is useful when you need to reroute traffic from a UPSR span temporarily to add or drop nodes, perform maintenance, or perform other operations.

Procedure: Switch UPSR Traffic

Step 1   Display the network view.

Step 2   Right-click the span that will be cut to add or delete a node and select **Circuits** from the shortcut menu (Figure 5-26).

Figure 5-26   Using the span shortcut menu to display circuits
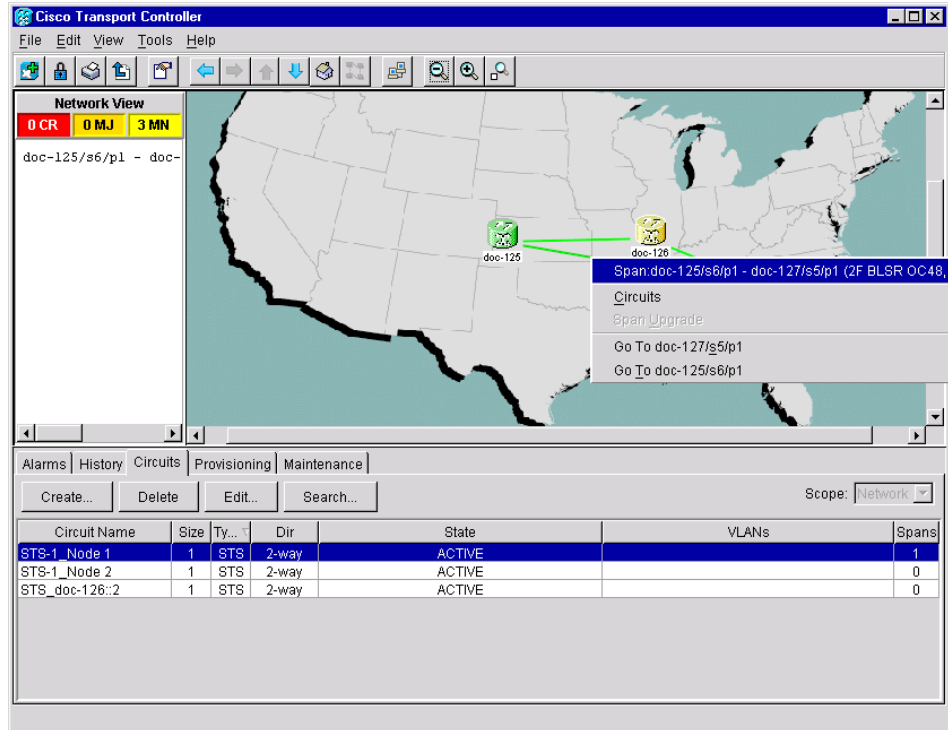
Step 3   On the Circuits on Span dialog box (Figure 5-27), select the protection from the **Switch all UPSR circuits away** menu:

- CLEAR removes a previously-set switch command.

- MANUAL switches the span if the new span is error free.

- FORCE forces the span to switch, regardless of whether the new span is error free.

- LOCKOUT locks out or prevents switching to a highlighted span. (LOCKOUT is only available when Revertive traffic is enabled.)

⚠

Caution   FORCE and LOCKOUT commands override normal protective switching mechanisms. Applying these commands incorrectly can cause traffic outages.

Figure 5-27   Switching UPSR circuits
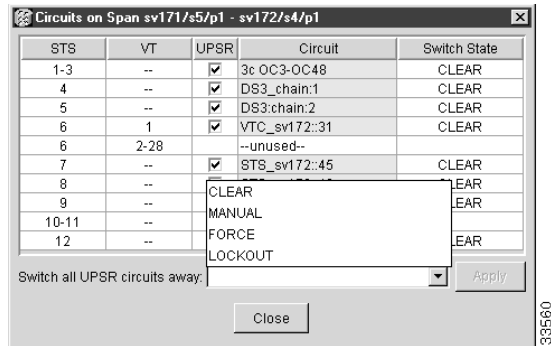
Step 4   Click Apply.

Step 5   When the confirmation dialog box appears, click **OK** to confirm the protection switching. The column under **Switch State** changes to your chosen level of protection.

Step 6   Click **Close** after **Switch State** changes.

Procedure: Add a UPSR Node

Note   You can add only one node at a time. Perform these steps onsite and not from a remote location.

Step 1   Log into CTC and display the UPSR nodes in network view. Verify the following:

- All UPSR spans on the network map are green.
- No critical or major alarms (LOF, LOS, ASP, ASL) are displayed on the **Alarms** tab.
- On the **Conditions** tab, no UPSR switches are active.
- At each physical UPSR node, all fibers are securely connected to the appropriate ports.

If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding.

Step 2   At the node that will be added to the UPSR:

- Verify that the OC-N cards are installed and fiber is available to connect to the other nodes.
- Run test traffic through the cards that will connect to the UPSR.
- Use the "Setting Up a UPSR" section on page 5-30 to provision the new node.

Step 3   Log into a node that will directly connect to the new node.

Step 4   Use the "Switch UPSR Traffic" procedure on page 5-32 to initiate a FORCE switch to switch traffic away from the span that will connect to the new node.

Caution   Traffic is not protected during a protection switch.

Step 5   Two nodes will connect directly to the new node; remove their fiber connections:

    a.   Remove the east fiber connection from the node that will connect to the west port of the new node.

b. Remove the west fiber connection from the node that will connect to the east port of the new node.

Step 6 Replace the removed fiber connections with connections from the new node.

✎

Note Perform this step on site at the new node.

Step 7 Log out of CTC and then log back in.

Step 8 Display the network view. The new node should appear in the network map. Wait for a few minutes to allow all the nodes to appear.

Step 9 Click the **Circuits** tab and wait for all the circuits to appear, including spans. The affected circuit will display as "incomplete."

Step 10 In the network view, right-click the new node and select **Update Circuits With New Node** from the list of options. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits displayed in the dialog box is correct.

Step 11 Select the **Circuits** tab and verify that no incomplete circuits are displayed. If incomplete circuits are displayed, repeat Step 9.

Step 12 Use the "Switch UPSR Traffic" procedure on page 5-32 to clear the protection switch.

Procedure: Remove a UPSR Node

⚠

Caution The following procedure is designed to minimize traffic outages while nodes are removed, but traffic will be lost when you delete and recreate circuits that passed through the removed node.

Step 1 Log into CTC and display the UPSR nodes in network view. Verify the following:

- All UPSR spans on the network map are green.
- No critical or major alarms (LOF, LOS, ASP, ASL) are displayed on the **Alarms** tab.
- On the **Conditions** tab, no UPSR switches are active.
- At each physical UPSR node, all fibers are securely connected to the appropriate ports.

If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding.

Step 2 Use the "Switch UPSR Traffic" procedure on page 5-32 to initiate a FORCE switch to switch traffic away from the node you are removing. Initiate a FORCE switch on all spans connected to the node you are removing.

⚠

Caution Traffic is not protected during a forced protection switch.

Step 3 In the node that will be removed, delete circuits that originate or terminate in that node. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.)

a. Click the **Circuits** tab.

b. Select the circuit(s) to delete. To select multiple circuits, press the Shift or Ctrl key.

c. Click **Delete**.

   d. Click **Yes** when prompted.

Step 4   From the node that will be deleted, remove the east and west span fibers. At this point, the node should no longer be a part of the ring.

Step 5   Reconnect the span fibers of the nodes remaining in the ring.

Step 6   Open the Alarms tab of each newly-connected node and verify that the span cards are free of alarms. Resolve any alarms before proceeding.

Step 7   One circuit at a time, delete and recreate each circuit that passed through the deleted node on different STSs.

> **Note**   If the removed node was the BITS timing source, select a new node as the BITS source or select another node as the master timing node.

Step 8   Use the "Switch UPSR Traffic" procedure on page 5-32 to clear the protection switch.

5.4 Subtending Rings

The ONS 15454 supports up to ten SONET DCCs. Therefore, one ONS 15454 node can terminate and groom any one of the following ring combinations:

- 5 UPSRs, or
- 4 UPSRs and 1 BLSR, or
- 3 UPSRs and 2 BLSRs

Subtending rings from an ONS 15454 reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling. Figure 5-28 shows an ONS 15454 with multiple subtending rings.

Figure 5-28   An ONS 15454 with multiple subtending rings
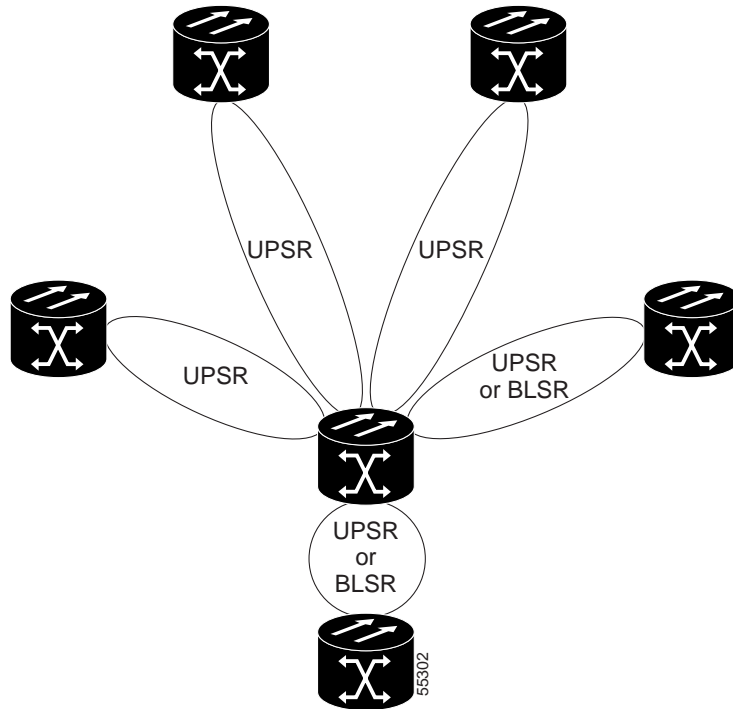
Figure 5-29 shows a UPSR subtending from a BLSR. In this example, Node 3 is the only node serving both the BLSR and UPSR. OC-N cards in Slots 5 and 12 serve the BLSR, and OC-N cards in Slots 6 and 13 serve the UPSR.

Figure 5-29   A UPSR subtending from a BLSR
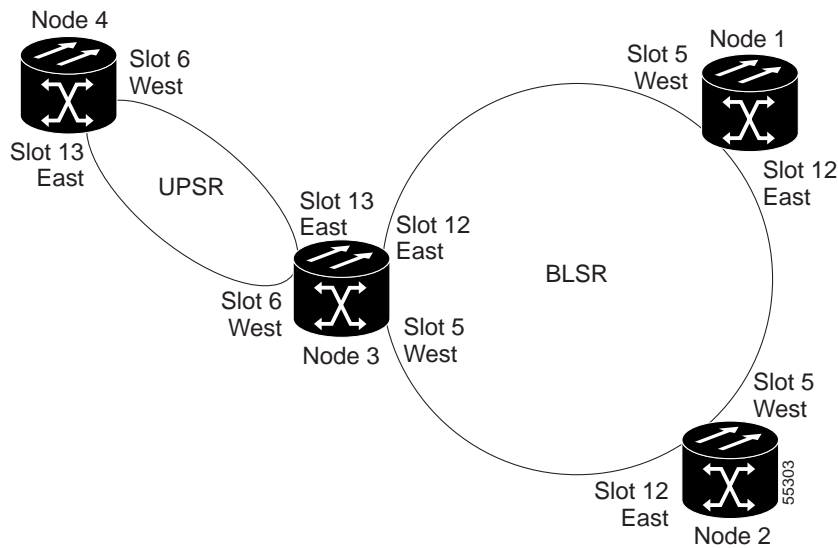
Procedure: Subtend a UPSR from a BLSR

This procedure requires an established BLSR and one BLSR node with OC-N cards and fibers to carry the UPSR. The procedure also assumes you can set up a UPSR. (For UPSR setup procedures, see the "Setting Up a UPSR" section on page 5-30.)

Step 1   In the node that will subtend the UPSR (Node 3 in Figure 5-29), install the OC-N cards that will serve as the UPSR trunk cards (Node 3, Slots 6 and 13).

Step 2   Attach fibers from these cards to the UPSR trunk cards on the UPSR nodes. In Figure 5-29, Slot 6 Node 3 connects to Slot 13/Node 5, and Slot 13 connects to Slot 6/Node 6.

Step 3   From the node view, click the **Provisioning > Sonet DCC** tabs.

Step 4   Click **Create**.

Step 5   In the Create SDCC Terminations dialog box, click the slot and port that will carry the UPSR.

Step 6   Click **OK**.

The selected slots/ports are displayed in the SDCC Terminations section.

Step 7   Put the ports that you will use for the UPSR in service:

   a.   In the node view, double-click UPSR trunk card.

   b.   Select the **Provisioning > Line** tabs. Under Status, choose **In Service**.

   c.   Click **Apply**.

   d.   Repeat steps a - c for the second UPSR trunk card.

Step 8   Follow Steps 1 – 7 for the other nodes you will use for the UPSR.

Step 9   Go to the network view to view the subtending ring.

Procedure: Subtend a BLSR from a UPSR

This procedure requires an established UPSR and one UPSR node with OC-N cards and fibers to connect to the BLSR. The procedure also assumes you can set up a BLSR. (For BLSR setup procedures, see the "Setting Up BLSRs" section on page 5-10.)

Step 1   In the node that will subtend the BLSR (Node 3 in the Figure 5-29 example), install the OC-N cards that will serve as the BLSR trunk cards (in Figure 5-29, Node 3, Slots 6 and 13).

Step 2   Attach fibers from these cards to the BLSR trunk cards on the BLSR nodes. In Figure 5-29, Slot 6/Node 3 connects to Slot 13/Node 5, and Slot 13 connects to Slot 6/Node 6.

Step 3   From the node view, click the **Provisioning > Sonet DCC** tabs.

Step 4   Click **Create**.

Step 5   In the Create SDCC Terminations dialog box, click the slot and port that will carry the BLSR.

Step 6   Click **OK**.

Step 7   The selected slots/ports are displayed under SDCC Terminations.

Step 8   Put the ports that you will use for the BLSR in service:

   a.   In the node view, double-click the BLSR trunk card.

   b.   Select the **Provisioning > Line** tabs. Under Status, choose **In Service**.

    c. Click **Apply**.

    d. Repeat steps a – c for the second BLSR trunk card.

Step 9   Use the "Provision the BLSR" procedure on page 5-14 to configure the BLSR.

Step 10   Follow Steps 1– 8 for the other nodes that will be in the BLSR.

Step 11   Go to the network view to see the subtending ring.

The ONS 15454 can support two BLSRs on the same node. This capability allows you to deploy an ONS 15454 in applications requiring SONET DCSs (digital cross connect systems) or multiple SONET ADMs (add/drop multiplexers).

Figure 5-30 shows two BLSRs shared by one ONS 15454. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7. Two BLSR rings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 5 and 12, and Ring 2 uses cards in Slots 6 and 13.

Note   Although different node IDs are used for the two BLSRs shown in Figure 5-30, nodes in different BLSRs can use the same node ID.

Figure 5-30 A BLSR subtending from a BLSR
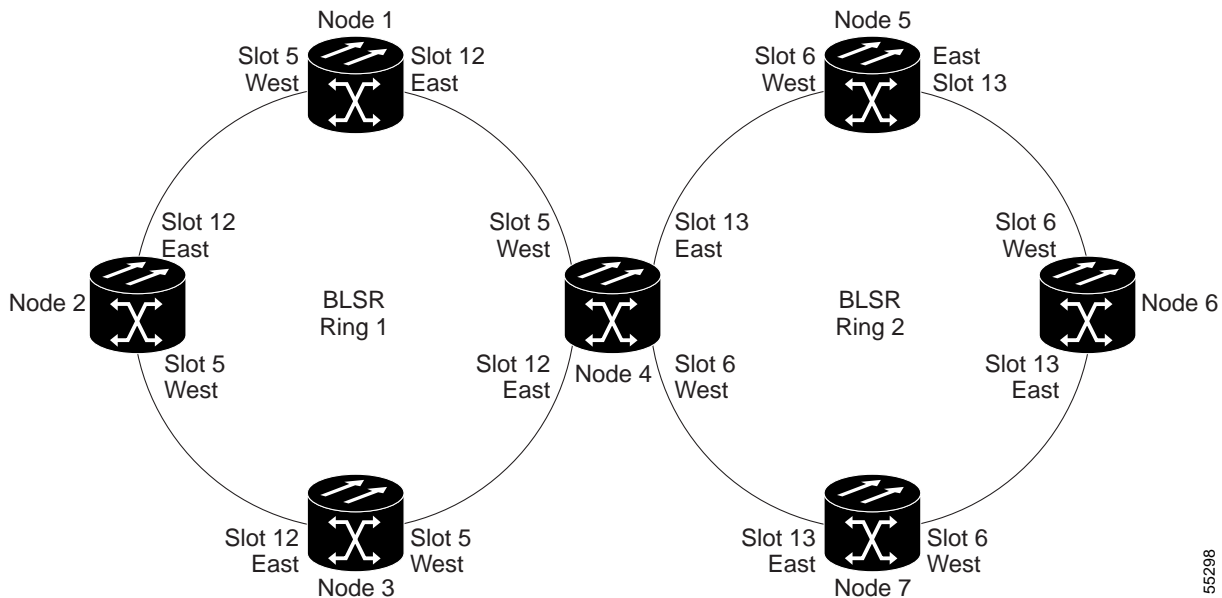
After subtending two BLSRs, you can route circuits from nodes in one ring to nodes in the second ring. For example in Figure 5-30, you can route a circuit from Node 1 to Node 7. The circuit would normally travel from Node 1 to Node 4 to Node 7. If fiber breaks occur, for example between Nodes 1 and 4 and Nodes 4 and 7, traffic is rerouted around each ring: in this example, Nodes 2 and 3 in Ring 1 and Nodes 5 and 6 in Ring 2.

Procedure: Subtend a BLSR from a BLSR

This procedure requires an established BLSR and one BLSR node with OC-N cards and fibers to carry the BLSR. The procedure also assumes you know how to set up a BLSR. For BLSR setup procedures, see the "Setting Up BLSRs" section on page 5-10.

Step 1   In the node that will subtend the BLSR (Node 4 in Figure 5-30), install the OC-N cards that will serve as the BLSR trunk cards (Node 4, Slots 6 and 13).

Step 2   Attach fibers from these cards to the BLSR trunk cards on the BLSR nodes. In Figure 5-30, Node 4/Slot 6 connects to Node 7/Slot 13, and Slot 13 connects to Node 5/Slot 6.

Step 3   From the node view, click the **Provisioning > Sonet DCC** tabs.

Step 4   Click **Create**.

Step 5   In the Create SDCC Terminations dialog box, click the slot and port that will carry the BLSR.

Step 6   Click **OK**.

Step 7   The selected slots/ports are displayed in the SDCC Terminations section.

Step 8   Put the ports that you will use for the BLSR in service:

    a.   In the node view, double-click the BLSR trunk card.

    b.   Select the **Provisioning > Line** tabs. Under Status, choose **In Service**.

    c.   Click **Apply**.

    d.   Repeat steps a – c for the second BLSR trunk card.

Step 9   To configure the BLSR, use the "Provision the BLSR" procedure on page 5-14. The subtending BLSR must have a ring ID that differs from the ring ID of the first BLSR.

Step 10   Follow Steps 1 – 8 for the other nodes that will be in the subtending BLSR.

Step 11   Display the network view to see the subtending ring.

Figure 5-31 shows an example of two subtending BLSRs.

Figure 5-31   Viewing subtending BLSRs on the network map
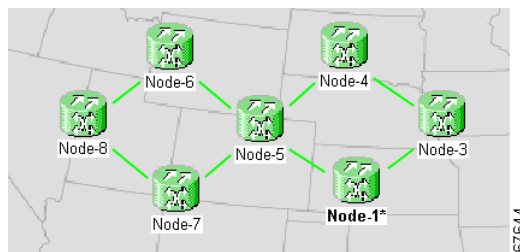
Figure 5-32 shows the Ring subtab for Node 5, which is the node that carries the two rings.

Figure 5-32   Configuring two BLSRs on the same node
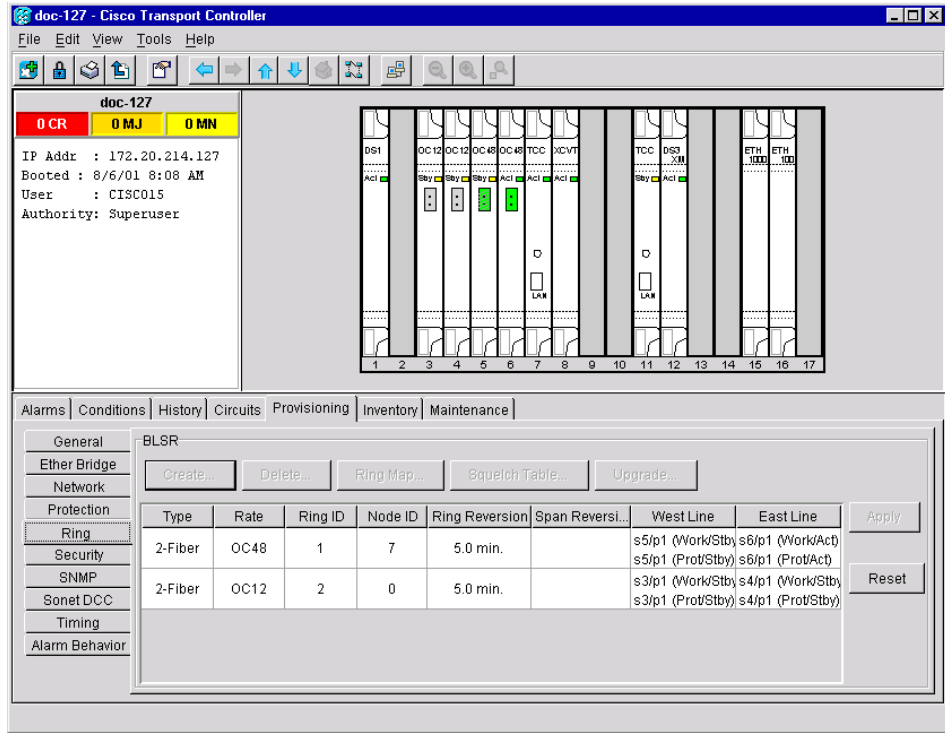
5.5 Linear ADM Configurations

You can configure ONS 15454s as a line of add/drop multiplexers (ADMs) by configuring one set of OC-N cards as the working path and a second set as the protect path. Unlike rings, linear (point-to-point) ADMs require that the OC-N cards at each node be in 1+1 protection to ensure that a break to the working line is automatically routed to the protect line.

Figure 5-33 shows three ONS 15454s in a linear ADM configuration. Working traffic flows from Slot 6/Node 1 to Slot 6/Node 2, and from Slot 12/Node 2 to Slot 12/Node 3. You create the protect path by placing Slot 6 in 1+1 protection with Slot 5 at Nodes 1 and 2, and Slot 12 in 1+1 protection with Slot 13 at Nodes 2 and 3.

Figure 5-33   A linear (point-to-point) ADM configuration
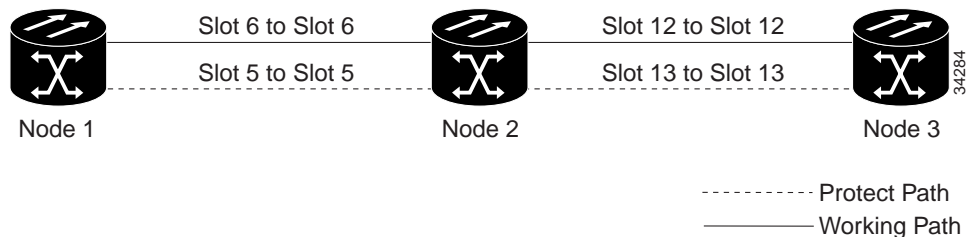
Procedure: Create a Linear ADM

Complete the following steps for each node that will be included in the linear ADM.

Step 1   Complete the general setup information for the node. For procedures, see the "Setting Up Basic Node Information" section on page 3-2.

Step 2   Set up the network information for the node. For procedures, see the "Setting Up Network Information" section on page 3-2.

Step 3   Set up 1+1 protection for the OC-N cards in the ADM. In Figure 5-33, Slots 6 and 12 are the working ports and Slots 5 and 13 are the protect ports. In this example, you would set up one protection group for Node 1 (Slots 5 and 6), two for Node 2 (Slots 5 and 6, and 12 and 13) and one for Node 3 (Slots 12 and 13). To create protection groups, see the "Creating Protection Groups" section on page 3-9.

Step 4   For OC-N ports connecting ONS 15454s, set the SONET DCC terminations:

    a.   Log into a linear ADM node and select the **Provisioning > Sonet DCC** tabs.

    b.   In the SDCC Terminations section, click **Create**.

    c.   On the Create SDCC Terminations dialog box, select the working port. Click **OK**.

> **Note**   Terminating nodes (Nodes 1 and 3 in Figure 5-33) will have one SDCC, and intermediate nodes (Node 2 in Figure 5-33) will have two SDCCs.

Step 5   Use the "Setting Up ONS 15454 Timing" section on page 3-12 to set up the node timing. If a node is using line timing, set the working OC-N card as the timing source.

Step 6   Place the OC-N ports in service:

    a.   Open an OC-N card that is connected to the linear ADM.

    b.   On the **Provisioning > Line** tabs under Status, select **In Service**.

    c.   Click **Apply**.

Repeat Step 6 for each OC-N card connected to the linear ADM.

Procedure: Convert a Linear ADM to UPSR

The following procedures describe how to convert a three-node linear ADM to a UPSR. You will need a SONET test set to monitor traffic while you perform these procedures.

> **Caution**   This procedure is service affecting.

> **Caution**   Always wear an authorized electrostatic discharge wrist band when removing or installing ONS 15454 cards.

Step 1   Start CTC and log into one of the nodes that you want to convert from linear to ring.

Step 2   Click the **Maintenance > Protection** tabs (Figure 5-34).

Figure 5-34   Verifying working slots in a protection group
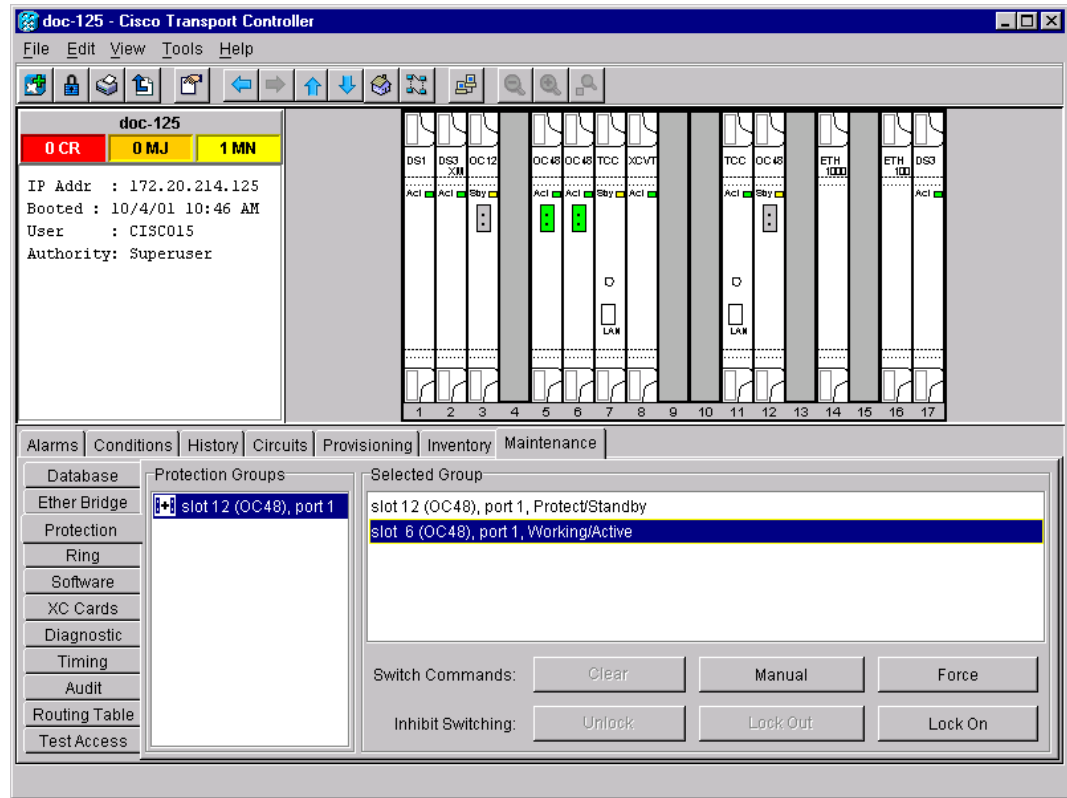
Step 3   Under Protection Groups, select the 1+1 protection group (that is, the group supporting the 1+1 span cards).

Step 4   Under Selected Group, verify that the working slot/port is shown as "Working/Active." If yes, go to Step 5. If the working slot says "Working/Standby" and the protect slot says "Protect/Active," switch traffic to the working slot:

- **a.**   Under Selected Group, select the protect slot, that is, the slot that says "Protect/Active."

- **a.**   From the Switch Commands, select **Manual**.

- **b.**   Click **Yes** on the confirmation dialog box.

- **c.**   Under Selected Group, verify that the working slot/port says "Working/Active." If so, continue to Step (d). If not, clear the conditions that prevent the card from carrying working traffic before proceeding.

- **d.**   From the Switch Commands, select **Clear**. A Confirm Clear Operation dialog is displayed.

- **e.**   Click **Yes** on the confirmation dialog box.

Step 5   Repeat Step 4 for each group in the 1+1 Protection Groups list at all nodes that will be converted.

Step 6   For each node, delete the 1+1 OC-N protection group that supports the linear ADM span:

> ✎
>
> **Note**   Deleting a 1+1 protection group may cause unequipped path (UNEQ-P) alarms to occur.

- **a.**   Click the **Provisioning > Protection** tabs (Figure 5-35).

- **b.**   From the Protection Groups list, choose the 1+1 group you want to delete. Click **Delete**.

c. Click **Yes** on the confirmation dialog box.

d. Verify that no traffic disruptions are indicated on the test set. If disruptions occur, do not proceed. Recreate the protection group and isolate the cause of the disruption.

e. Continue deleting 1+1 protection groups while monitoring the existing traffic with the test set.

Figure 5-35   Deleting a protection group
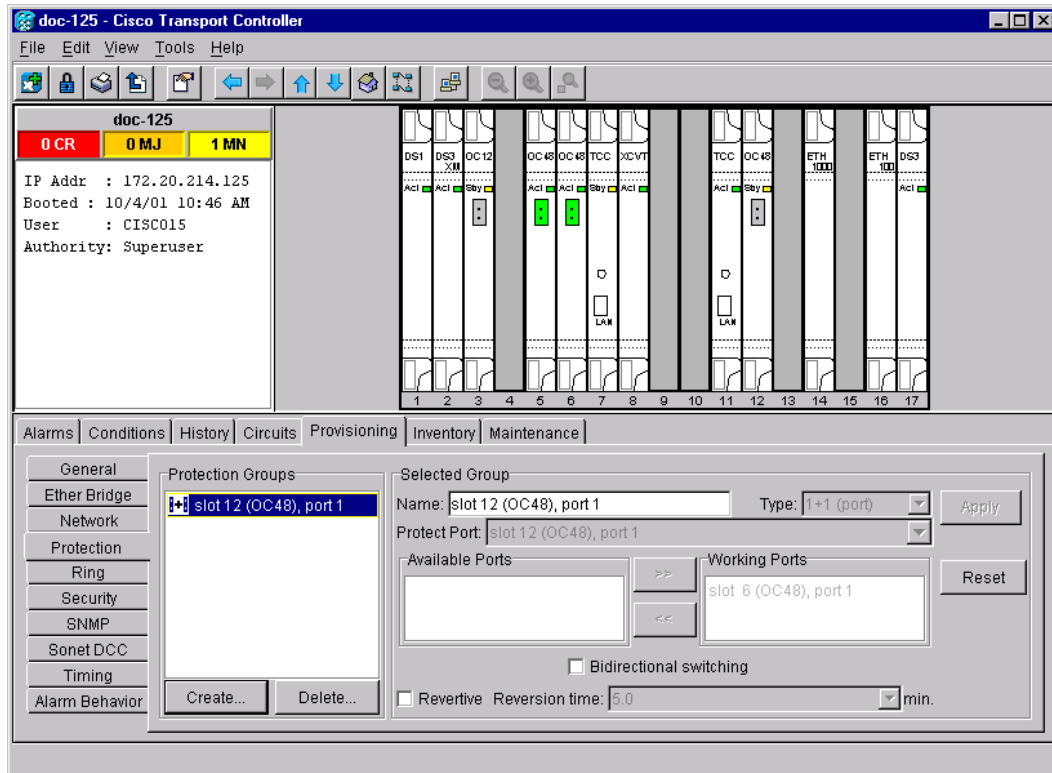
Step 7   Physically remove one of the protect fibers running between the middle and end nodes. For example, in the Figure 5-36, the fiber from Node 2/Slot 13 to Node 3/Slot 13 is removed. The corresponding OC-48 card will go into an LOS condition for that fiber and port.

Figure 5-36   Converting a linear ADM to a UPSR
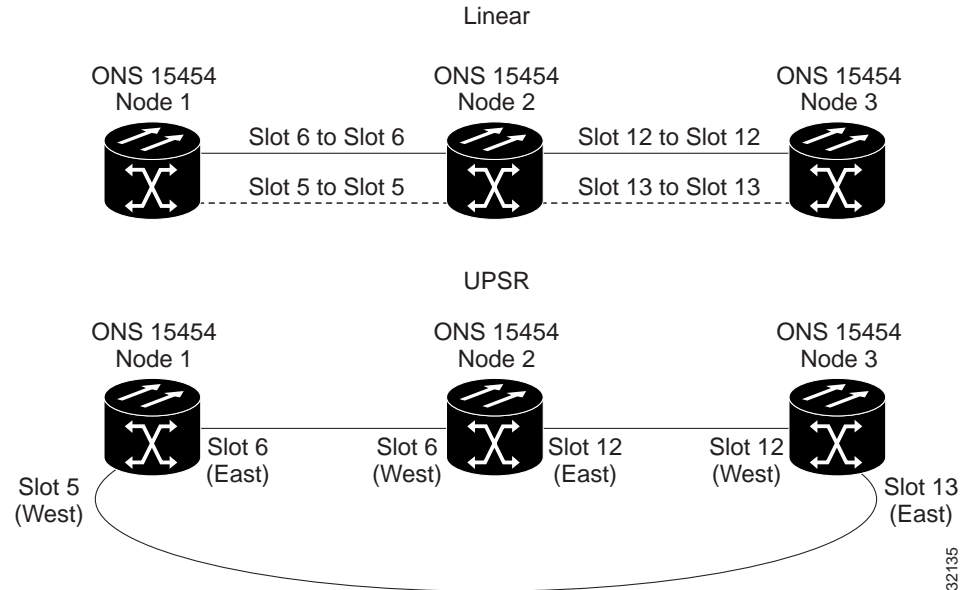
Step 8   Physically reroute the other protect fiber to connect the two end nodes. In the Figure 5-36 example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 is rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

If you are leaving the OC-N cards in place, go to Step 13. If you are removing the cards, complete Steps 9 – 12. (In this example, cards in Node 2/Slots 5 and 13 are removed.)

Step 9   In the middle node, place the cards in Slots 5 and 13 out of service:

  a.   Display the first card in card view and select the **Provisioning > Line** tabs.

  b.   Under Status, select **Out of Service**. Click **Apply**.

  c.   Repeat Steps a and b for the second card.

Step 10   Delete the equipment records for the cards:

  a.   Display the node view. (In card view, click the Up arrow on the toolbar.)

  b.   Right-click the card you just took out of service (e.g. Slot 5) and select **Delete Card**. (You can also go to the **Inventory** tab, select the card, and click **Delete**.)

  c.   Click **Yes** on the confirmation dialog box.

  d.   Repeat (a) through (c) for the second card (e.g. Slot 13).

Step 11   Save all circuit information.

  a.   In node view, select the **Provisioning > Circuits** tab.

  b.   Record the circuit information using one of the following procedures:

    –   From the File menu, select **Print** to print the circuits table, or,

    –   From the File menu, select **Export** to export the circuit data in HTML, CSV (comma separated values), or TSV (tab separated values). Click **Ok** and save the file in a temporary directory.

    See the "Printing and Exporting CTC Data" section on page 2-26 for more information.

Step 12   Remove the OC-N cards that are no longer connected to the end nodes (Slots 5 and 13, in the example).

Step 13   Display one of the end nodes (Node 1 or Node 3 in the example).

Step 14   Click the **Provisioning > Sonet DCC** tabs.

Cisco ONS 15454 Installation and Operations Guide

Step 15   In the SDCC Terminations section, click **Create**.

Step 16   In the Create SDCC Terminations dialog box, select the slot/port that had been the protect slot in the linear ADM, for example, for Node 1, this would be Slot 5/Port 1 (OC-48).

Step 17   Click **OK**.

An EOC SDCC alarm will occur until an SDCC termination is created on the adjacent node.

Step 18   Go to the node on the opposite end (Node 3 in the Figure 5-36 example) and repeat Steps 14 – 17.

Step 19   Delete and reenter the circuits one at a time. (See the "Creating Circuits and VT Tunnels" section on page 6-2.)

> ✎
> **Note**   Deleting circuits is traffic affecting.

You can create the circuits automatically or manually. However, circuits must be protected. When they were built in the linear ADM, they were protected by the protect path on Node 1/Slot 5 to Node 2/Slot 5 to Node 3/Slot 13. With the new UPSR, circuits should also be created with protection.

Deleting the first circuit and recreating it to the same card/port should restore the circuit immediately.

Step 20   Monitor your SONET test set to verify that the circuit was deleted and restored.

Step 21   You should also verify that the new circuit path for the clockwise (CW) fiber from Node 1 to Node 3 is working. To do this, switch to network view and move your cursor to the green span between Node 1 and 3.

Although the cursor only shows the first circuit created, do not become alarmed that the other circuits are not present. Verify with the SONET test set that the original circuits and the new circuits are operational. The original circuits were created on the counter clockwise linear path.

Step 22   Go to the network map to view the newly-created ring (Figure 5-37).

Figure 5-37   A UPSR displayed in network view

Procedure: Convert a Linear ADM to a BLSR

The following procedures describe how to convert a three-node linear ADM to a BLSR. You will need a SONET test set to monitor traffic while you perform these procedures.

⚠️
Caution   This procedure is service affecting.

⚠️
Caution   Always wear an authorized electrostatic discharge wrist band when removing or installing ONS 15454 cards.

Step 1   Start CTC and log into one of the nodes that you want to convert from linear to ring.

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

Step 3   Under Protection Groups, select the 1+1 protection group (that is, the group supporting the 1+1 span cards).

Step 4   Under Selected Group, verify that the working slot/port is shown as "Working/Active." If yes, go to Step 5. If the working slot says "Working/Standby" and the protect slot says "Protect/Active," switch traffic to the working slot:

   a.   Under Selected Group, select the protect slot, that is, the slot that says "Protect/Active."

   a.   From the Switch Commands, select **Manual**.

   b.   Click **Yes** on the confirmation dialog box.

     c. Verify that the working slot is carrying traffic. If it is, continue to Step (d). If not, clear the conditions that prevent the card from carrying working traffic before proceeding.

     d. From the Switch Commands, select **Clear**. A Confirm Clear Operation dialog is displayed.

     e. Click **Yes** on the confirmation dialog box.

Step 5 Repeat Step 4 for each group in the 1+1 Protection Groups list at all nodes that will be converted.

Step 6 For each node, delete the 1+1 OC-N protection group that supports the linear ADM span:

     a. Click the **Provisioning > Protection** tabs.

     b. From the Protection Groups list, choose the group you want to delete. Click **Delete**.

     c. Click **Yes** on the confirmation dialog box.

     d. Verify that no traffic disruptions are indicated on the SONET test set. If disruptions occur, do not proceed. Add the protection group and begin troubleshooting procedures to find out the cause of the disruption.

> **Note** Deleting a 1+1 protection group may cause unequipped path (UNEQ-P) alarms to occur.

Step 7 Physically remove one of the protect fibers running between the middle and end nodes. In the Figure 5-38 example, the fiber running from Slot 13/Node 2 to Slot 13/Node 3 is removed. The corresponding end-node trunk card will display an LOS alarm.

Figure 5-38   Converting a linear ADM to a BLSR
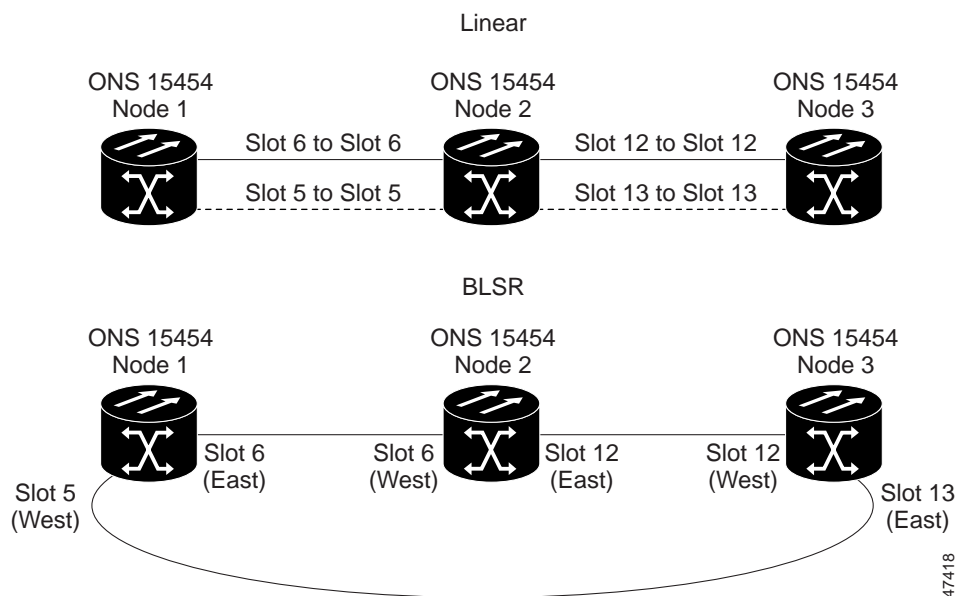
Step 8 Physically reroute the other protect fiber so it connects the two end nodes. In the Figure 5-38 example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 is rerouted to connect Node 1/Slot 5 to Node 3/Slot/ 13.

If you are leaving the OC-N cards in place, go to Step 13. If you are removing the cards, complete Steps 9 – 12. (In this example, cards in Node 2/Slots 5 and 13 are removed.)

Step 9   In the middle node, place the cards in Slots 5 and 13 out of service:

 a. Display the first card in card view, then select the **Provisioning > Line** tabs.

 b. Under Status, select **Out of Service**. Click **Apply**.

 c. Repeat Steps a and b for the second card.

Step 10   Delete the equipment records for the cards:

 a. From the View menu, choose **Node View**.

 b. Right-click the card you just took out of service (e.g. Slot 5) and select **Delete Card**. (You can also go to the **Inventory** tab, select the card, and click **Delete**.)

 c. Click **Yes** on the confirmation dialog box.

 d. Repeat (a) through (c) for the second card (e.g. Slot 13).

Step 11   Save all circuit information:

 a. In node view, select the **Provisioning > Circuits** tab.

 b. Record the circuit information using one of the following procedures:

 –   From the File menu, select **Print** to print the circuits table, or,

 –   From the File menu, select **Export** to export the circuit data in HTML, CSV (comma separated values), or TSV (tab separated values). Click **Ok** and save the file in a temporary directory.

   See the "Printing and Exporting CTC Data" section on page 2-26 for more information.

Step 12   Remove the OC-N cards that are no longer connected to the end nodes (Slots 5 and 13, in the example).

Step 13   Log into an end node. In node view, click the **Provisioning > Sonet DCC** tabs.

Step 14   In the SDCC Terminations section, click **Create**.

Step 15   Highlight the slot that is not already in the SDCC Terminations list (in this example, Port 1 of Slot 5 (OC-48) on Node 1.

Step 16   Click **OK**. (An EOC SDCC alarm will occur until the DCC is created on the other node; in the example, Node 3/Slot 13.

Step 17   Display the node on the opposite end (Node 3 in Figure 5-38) and repeat Steps 13 – 16.

Step 18   For circuits running on a BLSR protect STS (STSs 7 – 12 for an OC-12 BLSR, STSs 25 – 48 for an OC-48 BLSR), delete and recreate the circuit:

 a. Delete the first circuit.

 b. Recreate the circuit on STSs 1 – 6 (for an OC-12 BLSR) or 1 – 24 (for an OC-48 BLSR) on the fiber that served as the protect fiber in the linear ADM. During circuit creation, deselect "Route Automatically" and "Fully Protected Path" on the Circuit Creation dialog box so you can manually route the circuit on the appropriate STSs. See the "Create a Unidirectional Circuit with Multiple Drops" procedure on page 6-8 for more information.

 c. Repeat Steps (a) and (b) for each circuit residing on a BLSR protect STS.

✎
Note   Deleting circuits is traffic affecting.

Step 19   Follow all procedures in the "Setting Up BLSRs" section on page 5-10 to configure the BLSR. The ring should have an East/West logical connection. While it may not physically be possible to connect the OC-N cards in an East/West pattern, it is strongly recommended. If the network ring that is already passing traffic does not provide the opportunity to connect fiber in this manner, logical provisioning can be performed to satisfy this requirement.

Be sure to assign the same Ring ID and different node IDs to all nodes in the BLSR. Do not accept the BLSR ring map until all nodes are provisioned.

✎

Note   E-W Mismatch alarms will occur until all nodes are provisioned.

Step 20   Display the network map to view the newly-created ring.

5.6 Path-Protected Mesh Networks

In addition to single BLSRs, UPSRs and ADMs, you can extend ONS 15454 traffic protection by creating path-protected mesh networks (PPMNs). PPMNs include multiple ONS 15454 SONET topologies and extend the protection provided by a single UPSR to the meshed architecture of several interconnecting rings. In a PPMN, circuits travel diverse paths through a network of single or multiple meshed rings. When you create circuits, you can have CTC automatically route circuits across the PPMN, or you can manually route them. You can also choose levels of circuit protection. For example, if you choose full protection, CTC creates an alternate route for the circuit in addition to the main route. The second route follows a unique path through the network between the source and destination and sets up a second set of cross-connections.

For example, in Figure 5-39, a circuit is created from Node 3 to Node 9. CTC determines that the shortest route between the two nodes passes through Node 8 and Node 7, shown by the dotted line, and automatically creates cross-connections at Nodes, 3, 8, 7, and 9 to provide the primary circuit path.

If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 which, in this example, passes through Nodes 2, 1, and 11. Cross-connections are automatically created at Nodes, 3, 2, 1, 11, and 9, shown by the dashed line. If a failure occurs on the primary path, traffic switches to the second circuit path. In this example, Node 9 switches from the traffic coming in from Node 7 to the traffic coming in from Node 11 and service resumes. The switch occurs within 50 ms.

Figure 5-39   A path-protected mesh network
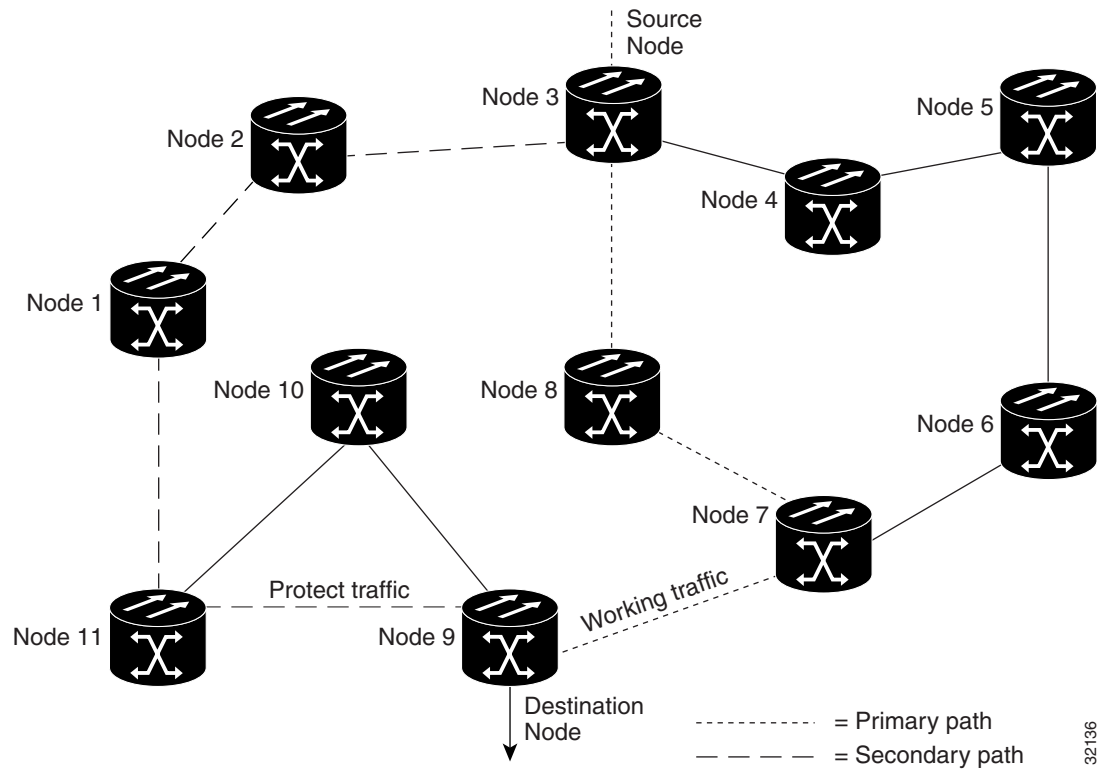
PPMN also allows spans of different SONET line rates to be mixed together in "virtual rings." Figure 5-40 shows Nodes 1, 2, 3, and 4 in a standard OC-48 ring. Nodes 5, 6, 7, and 8 link to the backbone ring through OC-12 fiber. The "virtual ring" formed by Nodes 5, 6, 7, and 8 uses both OC-48 and OC-12.

Figure 5-40   A PPMN virtual ring
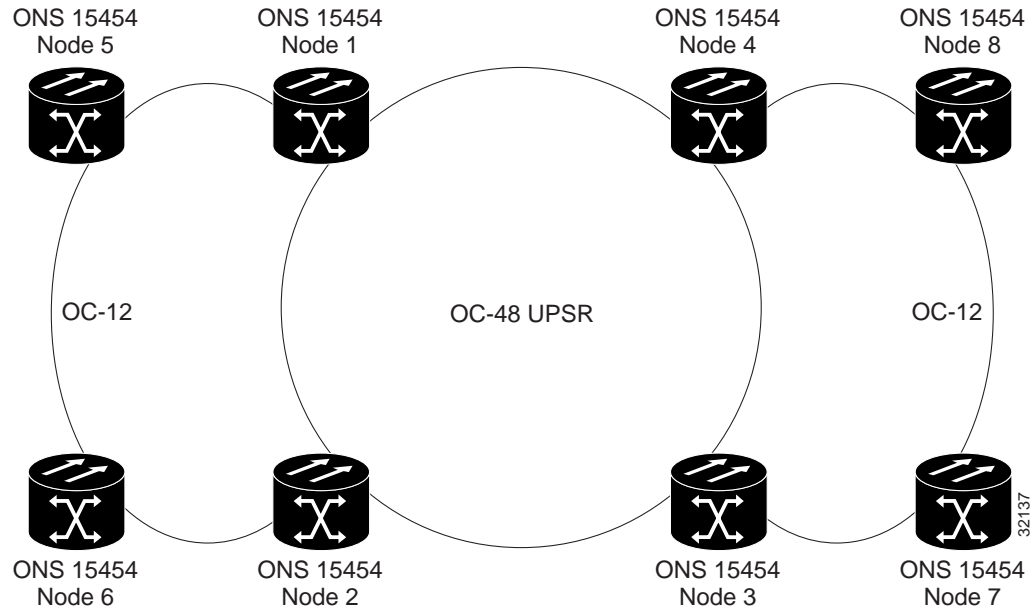
Circuits and Tunnels

This chapter explains how to create and administer Cisco ONS 15454 circuits and tunnels, which includes:

- Creating standard STS and VT1.5 circuits
- Creating VT tunnels
- Creating multiple drop circuits
- Creating monitor circuits
- Editing UPSR circuits
- Creating path traces to monitor traffic
- Reviewing ONS 15454 cross-connect card capacities
- Creating DCC tunnels to tunnel third-party equipment through ONS 15454 networks

6.1 Circuits Overview

You can create STS and VT1.5 circuits across and within ONS 15454 nodes and assign different attributes to circuits, for example:

- Create one-way, two-way, or broadcast circuits.
- Assign user-defined names to circuits.
- Assign different circuit sizes. STS circuits can be STS-1, STS-3c, STS-12c, STS-48c, or STS-192c. Ethernet circuits can be STS-1, STS-3c, STS-6c, or STS-12c. (To create Ethernet circuits see the "Provision a Shared Packet Ring" procedure on page 9-10.)
- Route circuits automatically or manually.
- Automatically create multiple circuits.
- Require the circuit path to be fully protected.
- Require protected source and destination cards and ports.
- Define a secondary circuit source or destination that allows you to interoperate an ONS 15454 unidirectional path switched ring (UPSR) with third-party equipment UPSRs.

> **Note** In this chapter, "cross-connect" and "circuit" have the following meanings: Cross-connect refers to the connections that occur within a single ONS 15454 to allow a circuit to enter and exit an ONS 15454. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15454 network) to the drop or destination (where traffic exits an ONS 15454 network).

6.2 Creating Circuits and VT Tunnels

This section explains how to create STS and VT1.5 circuits and VT tunnels. For an explanation and examples of circuits and VT tunnels, see the "Cross-Connect Card Capacities" section on page 6-15. You can create unidirectional or bidirectional, revertive or non-revertive circuits. You can have circuits routed automatically or you can manually route them. The auto range feature eliminates the need to individually build circuits of the same type; CTC can create additional sequential circuits if you specify the number of circuits you need and build the first circuit.

You can provision circuits at any of the following points:

- Before cards are installed. The ONS 15454 allows you to provision slots and circuits before installing the traffic cards. (To provision an empty slot, right-click it and select a card from the shortcut menu.) However, circuits will not carry traffic until you install the cards and place their ports in service. For procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-48 and the "Enable Ports" procedure on page 3-10.

- Cards are installed; ports are out of service. You must place the ports in service before circuits will carry traffic.

- Cards are installed, and their ports are in service. Circuits will carry traffic as soon as the signal is received.

Procedure: Create an Automatically Routed Circuit

> **Note** If you want to route circuits on protected drops, create the card protection groups before creating circuits. See the "Create Protection Groups" procedure on page 3-9.

Step 1 Log into an ONS 15454 and click the **Circuits** tab.

> **Tip** You can also right-click a source node in network view, select **Provision Circuit To**, and choose the circuit destination node from the menu.

Step 2 Click **Create**.

Step 3 In the Circuit Creation dialog box (Figure 6-1), complete the following fields:

- *Name*—(optional) Assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.

- *Type*—Select the type of circuit you want to create: STS, VT (VT1.5), or VT tunnel. The circuit type determines the circuit-provisioning options that are displayed. See the "VT1.5 Cross-Connects" section on page 6-16 and the "VT Tunnels" section on page 6-19 for more information.

- *Size*—Select the circuit size (STS circuits only). The "c" indicates concatenated STSs.

- *Bidirectional*—Check this box to create a two-way circuit; uncheck it to create a one-way circuit (STS and VT circuits only; VT tunnels are bidirectional).

- *Number of circuits*—Type the number of circuits you want to create. If you enter more than 1, you can use auto-ranging to create the additional circuits automatically. Otherwise, CTC returns to the Circuit Source page after you create each circuit until you finish creating the number of circuits specified here.

- *Auto Ranged*—If selected, and you select the source and destination of one circuit, CTC automatically determines the source and destination for the remaining *Number of circuits* and creates the circuits. To determine the source and destination, CTC increments the most specific part of the end points. An end point can be a port, an STS, or a VT/DS-1. If CTC runs out of choices, or selects an end point that is already in use, CTC stops and allows you to either select a valid end point or cancel. If you select a valid end point and continue, auto-ranging begins after you click **Finish** for the current circuit.

- *Protected Drops*—If this box is checked, CTC only displays protected cards and ports (1:1, 1:N, 1+1 or BLSR protection) as choices for the circuit source and destination.

Figure 6-1   Creating a circuit

Step 4   (UPSR circuits only) Set the UPSR Selector Defaults:

- *Revertive*—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If Revertive is not chosen, traffic remains on the protect path after the switch.

- *Reversion time*—If *Revertive* is checked, set the reversion time. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared (the default reversion time is 5 minutes).

- *SF threshold*—Set the UPSR path-level signal failure bit error rate (BER) thresholds (STS circuits only).

- *SD threshold*—Set the UPSR path-level signal degrade BER thresholds (STS circuits only).

- *Switch on PDI-P*—Check this box if you want traffic to switch when an STS payload defect indicator is received (STS circuits only).

Step 5   Click **Next**.

Step 6   In the Circuit Source dialog box, set the circuit source.

Options include node, slot, port, STS, and VT/DS-1. The options that display depend on the circuit type and circuit properties you selected in Step 3 and the cards installed in the node. For example, if you are creating a VT circuit or tunnel, only nodes with XCVT and XC10G cards are displayed. For Ethergroups, see the "Ethernet Circuit Configurations" section on page 9-6.

Click **Use Secondary Source** if you need to create a UPSR bridge/selector circuit entry point in a multivendor UPSR.

Step 7 Click **Next**.

Step 8 In the Circuit Destination dialog box, enter the appropriate information for the circuit destination. If the circuit is bidirectional, you can click **Use Secondary Destination** if you need to create a UPSR bridge/selector circuit destination point in a multivendor UPSR. (To add secondary destinations to unidirectional circuits, see "Create a Unidirectional Circuit with Multiple Drops" procedure on page 6-8.)

Step 9 Click **Next**.

Step 10 Under Circuit Routing Preferences (Figure 6-2), select **Route Automatically**. The following options (described in detail in the next step) are available:

- *Using Required Nodes/Spans*—If selected, you can specify nodes and spans to include or exclude in the CTC-generated circuit route.

- *Review Route Before Creation*—If selected, you can review and edit the circuit route before the circuit is created.

Step 11 If you want the circuit routed on a protected path, select **Fully Protected Path**. Otherwise, go to Step 12. CTC creates a primary and alternate circuit route (virtual UPSR) based on the nodal diversity option you select:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse. (For information about PPMN, see the "Path-Protected Mesh Networks" section on page 5-50.)

- *Nodal Diversity Desired*—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.

- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Figure 6-2   Setting circuit routing preferences
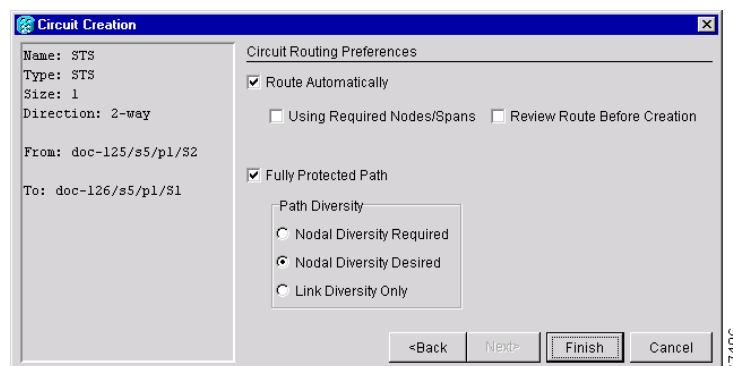
Step 12 Click **Finish** or **Next** depending on whether you selected **Using Required Nodes/Spans** and/or **Review Route Before Creation**:

- *Using Required Nodes/Spans*—If selected, click **Next** to display the Circuit Route Constraints panel (Figure 6-3). On the circuit map, click a node or span and click **Include** (to include the node or span in the circuit) or **Exclude** (to exclude the node/span from the circuit). The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction. After you add the spans and nodes, you can use the Up and Down buttons to change their order, or click **Remove** to remove a node or span. When you are finished, click **Finish** or **Next**, depending on whether you selected **Review Route Before Creation**.

Figure 6-3   Specifying circuit constraints
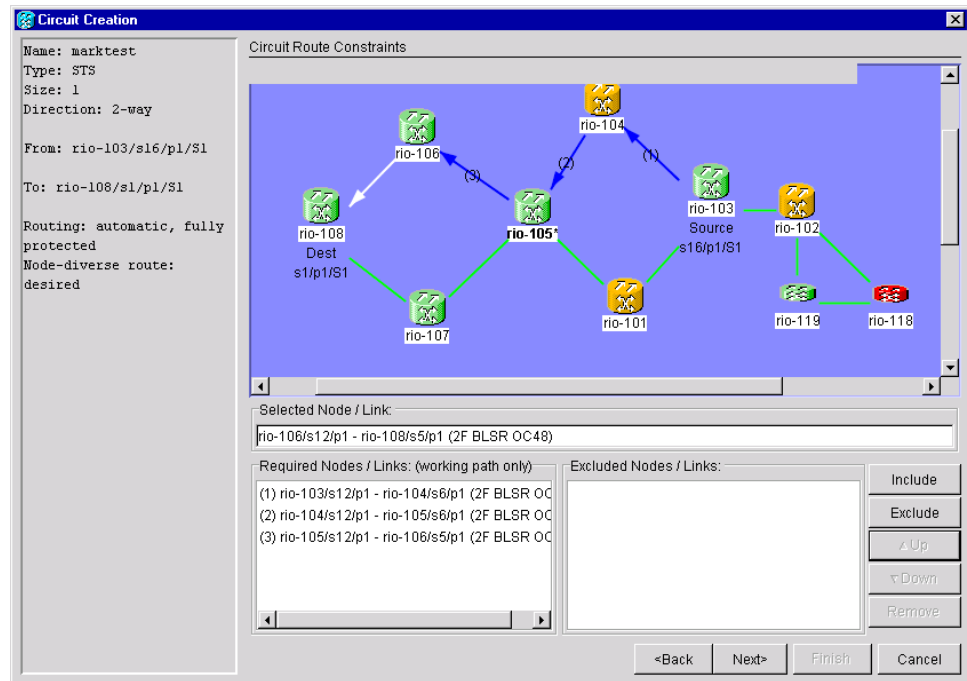
- *Review Route Before Creation*—If selected, click **Next** to display the route for you to review. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

When you click **Finish**, CTC creates the circuit and returns to the Circuits window. If you entered more than 1 in *Number of Circuits* in the Circuit Attributes dialog box in Step 3, the Circuit Source dialog box is displayed so you can create the remaining circuits. If Auto Ranged is checked, CTC automatically creates the number of sequential circuits that you entered in *Number of Circuits*. Otherwise, go on to Step 13.

Step 13   If you are provisioning circuits before installing the traffic cards and enabling their ports, you must install the cards and enable the ports before circuits will carry traffic. For procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-48 and the "Enable Ports" procedure on page 3-10.

Procedure: Create a Manually Routed Circuit

Note   If you want to route circuits on protected drops, create the card protection groups before creating circuits. See the "Create Protection Groups" procedure on page 3-9.

Step 1   Log into an ONS 15454 and click the **Circuits** tab.

Tip   You can also right-click a source node in network view, select **Provision Circuit To**, and choose the circuit destination node from the menu.

Step 2   Click **Create**.

Step 3   In the Circuit Creation dialog box (Figure 6-1), complete the following fields:

- *Name*—(optional) Assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.

- *Type*—Select the type of circuit you want to create: STS, VT (VT1.5), or VT tunnel. The circuit type determines the circuit-provisioning options that are displayed. "VT1.5 Cross-Connects" section on page 6-16 and the "VT Tunnels" section on page 6-19 for more information.

- *Size*—Select the circuit size (STS circuits only). The "c" indicates concatenated STSs.

- *Bidirectional*—Check this box to create a two-way circuit; uncheck it to create a one-way circuit (STS and VT circuits only; VT tunnels are bidirectional).

- *Number of circuits*—Type the number of circuits you want to create. CTC returns to the Circuit Source page after you create each circuit until you finish creating the number of circuits specified here.

- *Auto Ranged*—This option is not available with manual circuit routing.

- *Protected Drops*—If this box is checked, CTC only displays protected cards and ports (1:1, 1:N, 1+1 or BLSR protection) as choices for the circuit source and destination.

Figure 6-4   Creating a circuit

Step 4   (UPSR circuits only) Set the UPSR Selector Defaults:

- *Revertive*—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If Revertive is not chosen, traffic remains on the protect path after the switch.

- *Reversion time*—If Revertive is checked, set the reversion time. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared (the default reversion time is 5 minutes).

- *SF threshold*—Set the UPSR path-level signal failure bit error rate (BER) thresholds (STS circuits only).

- *SD threshold*—Set the UPSR path-level signal degrade BER thresholds (STS circuits only).

- *Switch on PDI-P*—Check this box if you want traffic to switch when an STS payload defect indicator is received (STS circuits only).

Step 5   Click **Next**.

Step 6   In the Circuit Source dialog box, set the circuit source.

Options include node, slot, port, STS, and VT/DS-1. The options that display depend on the circuit type and circuit properties you selected in Step 3 and the cards installed in the node. For example, if you are creating a VT circuit or tunnel, only nodes with XCVT and XC10G cards are displayed. For Ethergroups, see the "Ethernet Circuit Configurations" section on page 9-6.

Click **Use Secondary Source** if you need to create a UPSR bridge/selector circuit entry point in a multivendor UPSR.

Step 7   Click **Next**.

Step 8   In the Circuit Destination dialog box, enter the appropriate information for the circuit destination. If the circuit is bidirectional, you can click **Use Secondary Destination** if you need to create a UPSR bridge/selector circuit destination point in a multivendor UPSR. (To add secondary destinations to unidirectional circuits, see "Create a Unidirectional Circuit with Multiple Drops" procedure on page 6-8.)

Step 9   Click **Next**.

Step 10   Under Circuit Routing Preferences (Figure 6-2), de-select **Route Automatically**.

Step 11   If you want the circuit routed on a protected path, select **Fully Protected Path**. Otherwise, go to Step 12. CTC creates a primary and alternate circuit route (virtual UPSR) based on the nodal diversity option you select:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse. (For information about PPMN, see the "Path-Protected Mesh Networks" section on page 5-50.)

- *Nodal Diversity Desired*—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.

- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

Step 12   Click **Next**. The Route Review and Edit panel is displayed for you to manually route the circuit. The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.

Step 13   Set the circuit route:

a.   Click the arrowhead of the span you want the circuit to travel.

b.   If you want to change the source STS or VT, change it in the Source STS or Source VT fields.

c. Click **Add Span**.

The span is added to the Included Spans list and the span arrow turns blue.

Step 14 Repeat Step 13 until the circuit is provisioned from the source to the destination node.

When provisioning a protected circuit, you only need to select one path of BLSR or 1+1 spans from the source to the drop. If you select unprotected spans as part of the path, select two different paths for the unprotected segment of the path.

Step 15 When the circuit is provisioned, click **Finish**.

If you entered more than 1 in *Number of Circuits* in the Circuit Attributes dialog box in Step 3, the Circuit Source dialog box is displayed so you can create the remaining circuits.

Step 16 If you are provisioning circuits before installing the traffic cards and enabling their ports, you must install the cards and enable the ports before circuits will carry traffic. For procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-48 and the "Enable Ports" procedure on page 3-10.

6.3 Creating Multiple Drops for Unidirectional Circuits

Unidirectional circuits can have multiple drops for use in broadcast circuit schemes. In broadcast scenarios, one source transmits traffic to multiple destinations, but traffic is not returned back to the source.

When you create a unidirectional circuit, the card that does not have its backplane Rx input terminated with a valid input signal generates a loss of service (LOS) alarm. To mask the alarm, create an alarm profile suppressing the LOS alarm and apply it to the port that does not have its Rx input terminated. See the "Creating and Modifying Alarm Profiles" section on page 10-9 for information.

Procedure: Create a Unidirectional Circuit with Multiple Drops

Step 1 Use the "Create an Automatically Routed Circuit" procedure on page 6-2 to create a circuit. To make it unidirectional, clear the Bidirectional check box on the Circuit Creation dialog box.

Step 2 After the unidirectional circuit is created, in node or network view select the **Circuits** tab.

Step 3 Select the unidirectional circuit and click **Edit** (or double-click the circuit).

Step 4 On the **Drops** tab of the Edit Circuits dialog box, click **Create** or, if Show Detailed Map is selected, right-click a node on the circuit map and select **Add Drop**.

Step 5 On the Define New Drop dialog box, complete the appropriate fields to define the new circuit drop: *Node, Slot, Port, STS, VT* (if applicable).

Step 6 Click **OK**.

Step 7 If you need to create additional drops, repeat Steps 4 – 6. If not, click **Close**.

Step 8 Verify the new drops on the Edit Circuit map:

- If Show Detailed Map is selected: a "D" enclosed by circles appears on each side of the node graphic.
- If Show Detailed Map is not selected: "Drop #1, Drop #2" appear under the node graphic.

6.4 Creating Monitor Circuits

You can set up secondary circuits to monitor traffic on primary bidirectional circuits. Figure 6-5 shows an example of a monitor circuit. At Node 1, a VT1.5 is dropped from Port 1 of an EC1-12 card. To monitor the VT1.5 traffic, test equipment is plugged into Port 2 of the EC1-12 card and a monitor circuit to Port 2 is provisioned in CTC. Circuit monitors are one-way. The monitor circuit in Figure 6-5 is used to monitor VT1.5 traffic received by Port 1 of the EC1-12 card.

Note Monitor circuits cannot be used with EtherSwitch circuits.

Note For unidirectional circuits, create a drop to the port where the test equipment is attached.

Figure 6-5   A VT1.5 monitor circuit received at an EC1-12 port
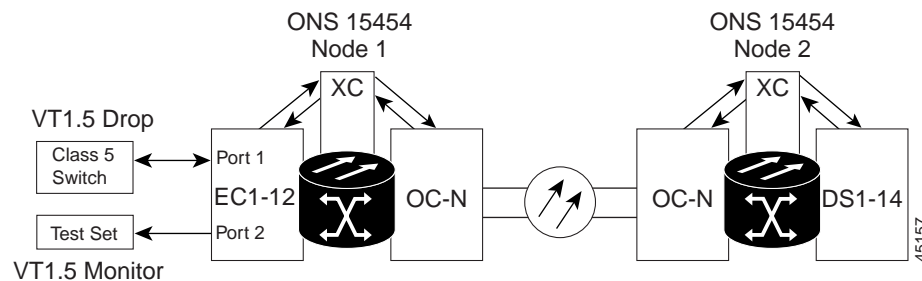
Procedure: Create a Monitor Circuit

Step 1   Log into CTC.

Step 2   In node view, select the **Circuits** tab.

Step 3   Select the bidirectional circuit that you want to monitor. Click **Edit**.

Step 4   On the Edit Circuit dialog box, click the **Monitors** tab.

Step 5   The Monitors tab displays ports that you can use to monitor the circuit selected in Step 3.

Step 6   On the Monitors tab, select a port. The monitor circuit displays traffic coming into the node at the card/port you select. In Figure 6-5, you would select either the DS1-14 card (to test circuit traffic entering Node 2 on the DS1-14) or the OC-N card at Node 1 (to test circuit traffic entering Node 1 on the OC-N card).

Step 7   Click **Create Monitor Circuit**.

Step 8   On the Circuit Creation dialog box, select the destination node, slot, port, and STS for the monitored circuit. In the Figure 6-5 example, this is Port 2 on the EC1-12 card. Click **Next**.

Step 9   On the Circuit Creation dialog box confirmation, review the monitor circuit information. Click **Finish**.

Step 10   On the Edit Circuit dialog box, click **Close**. The new monitor circuit displays on the Circuits tab.

6.5 Searching for Circuits

CTC provides the ability to search for ONS 15454 circuits based on circuit name. Searches can be conducted at the network, node, and card level. You can search for whole words and include capitalization as a search parameter.

Procedure: Search for ONS 15454 Circuits

Step 1   Log into CTC.

Step 2   Switch to the appropriate CTC view:

- Network view to conduct searches at the network level
- Node view to conduct searches at the network or node level
- Card view to conduct searches at the card, node, or network level

Step 3   Click the **Circuits** tab.

Step 4   If you are in Node or Card view, select the scope for the search in the Scope field.

Step 5   Click Search.

Step 6   In the Circuit Name Search dialog box, complete the following:

- *Find What*—Enter the text of the circuit name you want to find.
- *Match Whole Word Only*—If checked, CTC selects circuits only if the entire word matches the text in the Find What field.
- *Match Case*—If checked, CTC selects circuits only when the capitalization matches the capitalization entered in the Find What field.
- *Direction*—Select the direction for the search. Searches are conducted up or down from the currently selected circuit.

Step 7   Click **Find Next**.

Step 8   Repeat Steps 6 and 7 until you are finished, then click **Cancel**.

6.6 Editing UPSR Circuits

Use the Edit Circuits window to change UPSR selectors and switch protection paths (Figure 6-6). In this window, you can:

- View the UPSR circuit's working and protection paths
- Edit the reversion time
- Edit the Signal Fail/Signal Degrade thresholds
- Change PDI-P settings, perform maintenance switches on the circuit selector, and view switch counts for the selectors
- Display a map of the UPSR circuits to better see circuit flow between nodes

Figure 6-6   Editing UPSR selectors
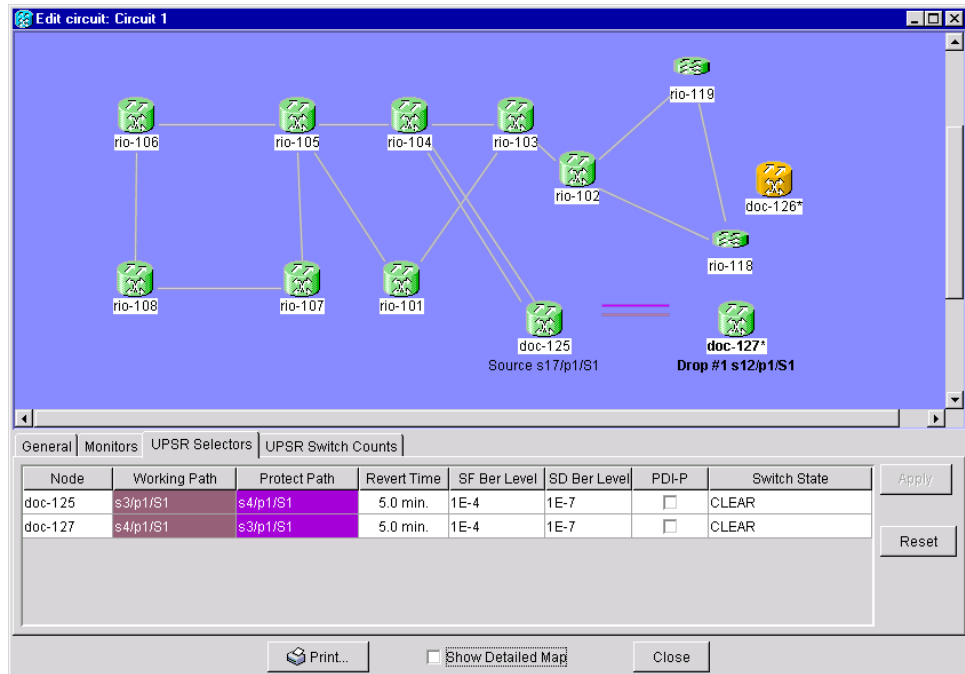
Procedure: Edit a UPSR Circuit

Step 1   Log into the source or drop node of the UPSR circuit.

Step 2   Click the **Circuits** tab.

Step 3   Click the circuit you want to edit, then click **Edit**.

Step 4   On the Edit Circuit window, click the **UPSR** tab.

Step 5   Edit the UPSR selectors:

- *Reversion Time*—Controls whether traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If you select Never, traffic does not revert. Selecting a time sets the amount of time that will elapse before traffic reverts to the working path.

- *SF Ber Level*—Sets the UPSR signal failure BER threshold (STS circuits only).

- *SD Ber Level*—Sets the UPSR signal degrade BER threshold (STS circuits only).

- *PDI-P*—When checked, traffic switches if an STS payload defect indication is received (STS circuits only).

- *Switch State*—Switches circuit traffic between the working and protect paths. The color of the Working Path and Protect Path fields indicates the active path. Normally, the Working Path is green and the Protect Path is purple. If the Protect Path is green, working traffic has switched to the Protect Path.

  CLEAR—Removes a previously-set switch command.

  LOCKOUT OF PROTECT—Prevents traffic from switching to the protect circuit path.

  FORCE TO WORKING—Forces traffic to switch to the working circuit path, regardless of whether the path is error free.

Cisco ONS 15454 Installation and Operations Guide

FORCE TO PROTECT—Forces traffic to switch to the protect circuit path, regardless of whether the path is error free.

MANUAL TO WORKING—Switches traffic to the working circuit path when the working path is error free.

MANUAL TO PROTECT—Switches traffic to the protect circuit path when the protect path is error free.

⚠

Caution   The FORCE and LOCKOUT commands override normal protection switching mechanisms. Applying these commands incorrectly can cause traffic outages.

Step 6   Click **Apply**, then check that the selector switches as you expect.

6.7 Creating a Path Trace

The SONET J1 Path Trace is a repeated, fixed-length string comprised of 64 consecutive J1 bytes. You can use the string to monitor interruptions or changes to circuit traffic. Table 6-1 shows the ONS 15454 cards that support path trace. DS-1 and DS-3 cards can transmit and receive the J1 field, while the EC-1, OC-3, OC-48AS, and OC-192 can only receive it. Cards not listed in the table do not support the J1 byte.

Table 6-1   ONS 15454 Cards Supporting J1 Path Trace

Card	Receive	Transmit
DS1-14	X	X
DS1N-14	X	X
DS3-12E	X	X
DS3N-12E	X	X
DS3XM-6X	X	X
EC1-12	X	
OC3 IR 4 1310	X	
OC48 IR/STM16 SH AS 1310	X	
OC48 LR/STM16 LH AS 1550	X	
OC192 LR/STM64 LH 1550	X	

The J1 path trace transmits a repeated, fixed-length string. If the string received at a circuit drop port does not match the string the port expects to receive, an alarm is raised. Two path trace modes are available:

- *Automatic*—The receiving port assumes the first J1 string it receives is the baseline J1 string.

- *Manual*—The receiving port uses a string that you manually enter as the baseline J1 string.

Table 6-2 shows the general flow for setting up the J1 path trace. To set up a path trace on an ONS 15454 circuit, follow the steps in the "Create a J1 Path Trace" procedure on page 6-13.

Table 6-2   Path Trace Source and Drop Provisioning

Step	Port	Action	Notes
1	Source	Edit the path-trace transmit string.	If not edited, an empty string is transmitted.
2	Drop	Edit the path-trace transmit string.	If not edited, an empty string is transmitted.
3	Source	Edit the path-trace expected string.	Only if Path Trace mode is set to Manual, and only on DS-1, DS3E, and DS3XM cards.
4	Drop	Edit the path-trace expected string	Only Path Trace mode is set to Manual, and only on DS-1, DS3E, and DS3XM cards.
5	Drop	Change Path Trace Mode	Automatic or Manual.
6	Source	Change Path Trace Mode	Automatic or Manual.

Procedure: Create a J1 Path Trace

To perform this procedure, you must have an STS circuit using a DS-1, DS3E, or DS3XM card at the circuit source and drop ports, or an STS circuit passing through an EC-1, OC-3, OC-48AS, or OC-192 card.

Step 1   Log into the circuit source node and select the **Circuits** tab.

Step 2   Select the circuit you want to trace, then click **Edit**.

Step 3   On the Edit Circuit window, click **Show Detailed Map** at the bottom of the window.

Step 4   On the detailed circuit map, right-click the source port for the circuit and select **Edit Path Trace** from the shortcut menu. Figure 6-7 shows an example.

Figure 6-7   Selecting the Edit Path Trace option
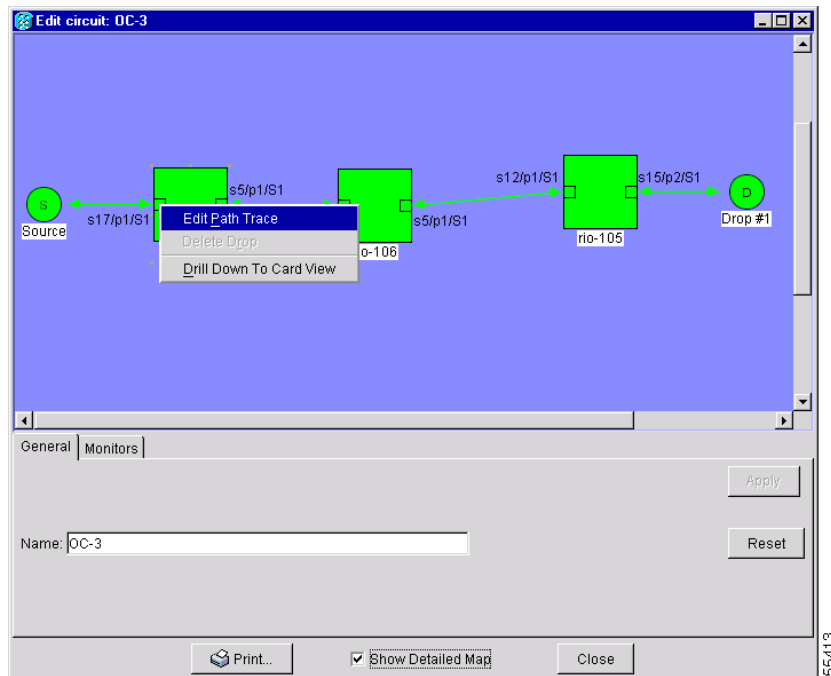
Step 5   On the Circuit Path Trace window (Figure 6-8) in the New Transmit String field (this field is available only on DS-1, DS3E, and DS3XM cards), enter the string that you want the source port to transmit. For example, you could enter the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits an empty string.

Figure 6-8   Setting up a path trace
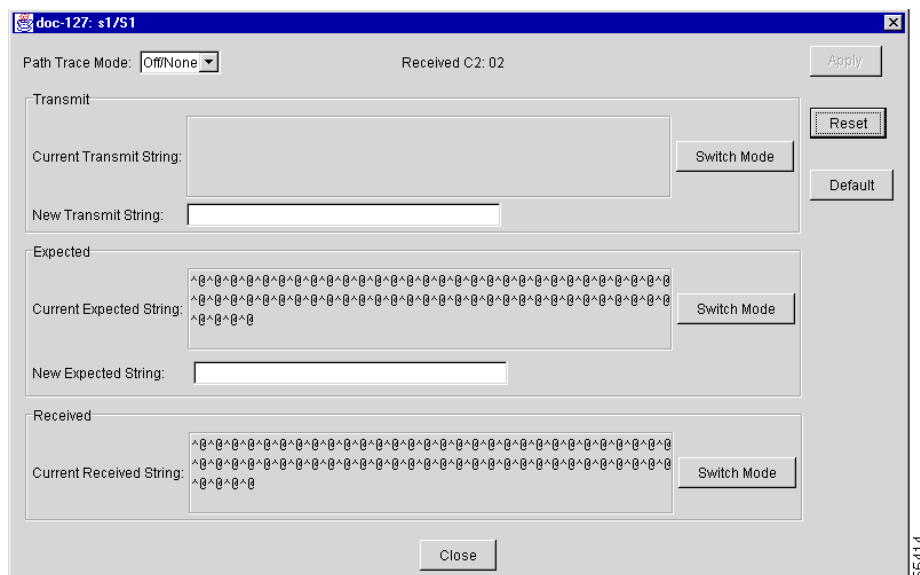
Step 6   Click **Apply** but do not close the window.

Step 7   Return to the Edit Circuit window (Figure 6-7).

Step 8   On the circuit map, right-click the drop port for the circuit and select **Edit Path Trace** from the shortcut menu.

Step 9   On the Circuit Path Trace window (Figure 6-8) in the New Transmit String field (this field is available only on DS-1, DS3E, and DS3XM cards), enter the string that you want the drop port to transmit. If the field is left blank, the J1 transmits an empty string.

Step 10   If you will set Path Trace Mode to Manual in Step 11, enter the string that the drop port should expect to receive in the New Expected String field. This string must match the New Transmit String entered for the source port in Step 5. (When you click **Apply** in Step 12, this string becomes the Current Expected String.)

Step 11   In the Path Trace Mode field, select one of the following options:

- *Auto*—Assumes the first string received from the source port is the baseline string. An alarm is raised when a string that differs from the baseline is received.

- *Manual*—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 12   Click **Apply** and then click **Close**.

Step 13   Display the Circuit Path Trace window for the source port from Step 5.

Step 14   If you will set the Path Trace Mode to Manual in Step 15, enter the string the source port should expect to receive in the New Expected String field. This string must match the New Transmit String entered for the source port in Step 9.

Step 15   In the Path Trace Mode field, select one of the following options:

- *Auto*—Assumes that the first string received from the drop port is the baseline string. An alarm is raised when a string that differs from the baseline is received.

- *Manual*—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 16   Click **Apply** and click **Close**.

After you set up the path trace, the received string is displayed in the Received box on the path trace setup window (Figure 6-8). Click **Switch Mode** to toggle between ASCII and hexadecimal display. Click the **Reset** button to reread values from the port. Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

6.8 Cross-Connect Card Capacities

The ONS 15454 XC, XCVT, and XC10G cards perform port-to-port time-division multiplexing (TDM).

- XCs perform STS switching

- XCVTs and XC10Gs perform STS and VT1.5 switching

XCs and XCVTs have capacity to terminate 288 STSs, or 144 STS cross-connections (each STS cross-connection uses two STS ports on the cross-connect card STS matrix). XC10Gs have capacity for 1152 STSs, or 576 STS cross-connections. Table 6-3 shows STS capacities for the XC, XCVT, and XC10G cards.

Note   The *Cisco ONS 15454 Troubleshooting and Maintenance Guide* contains detailed specifications of the XC, XCVT, and XC10G cards.

Table 6-3   XC, XCVT, and XC10G Card STS Cross-Connect Capacities

Card	Total STSs	STS Cross-connects
XC	288	144
XCVT	288	144
XC10G	1152	576

6.8.1 VT1.5 Cross-Connects

XCVTs and XC10Gs can map up to 24 STSs for VT1.5 traffic. Because one STS can carry 28 VT1.5s, the XCVT and XC10G cards can terminate up to 672 VT1.5s, or 336 VT1.5 cross-connects. However, to terminate 336 VT1.5 cross-connects:

- Each STS mapped for VT1.5 traffic must carry 28 VT1.5 circuits. If you assign each VT1.5 circuit to a different STS, the XCVT and XC10G VT1.5 cross-connect capacity will be reached after you create 12 VT1.5 circuits.

- ONS 15454s must be in a bidirectional line switched ring (BLSR). Source and drop nodes in UPSR or 1+1 (linear) protection have capacity for only 224 VT1.5 cross-connects because an additional STS is used for the protect path.

Table 6-4 shows the VT1.5 capacities for ONS 15454 cross-connect cards. All capacities assume each VT1.5-mapped STS carries 28 VT1.5 circuits.

Table 6-4   XC, XCVT, and XC10G VT1.5 Capacities

Card	Total VT1.5s (BLSR)	VT1.5 Cross-Connect Capacity (BLSR)	VT1.5 Cross-Connect Capacity (UPSR or 1+1)
XC	0	0	0
XCVT	672	336	224
XC10G	672	336	224

Figure 6-9 shows the logical flow of a VT1.5 circuit through the XCVT/XC10G STS and VT matrices at a BLSR node. The circuit source is an EC-1 card using STS-1. After the circuit is created:

- Two of the 24 XCVT or XC10G STSs available for VT1.5 traffic are used (one STS for VT1.5 input into the VT matrix; one STS for VT1.5 output).

- 22 STSs are available for VT1.5 circuits.

- The STS-1 from the EC-1 card has capacity for 27 more VT1.5 circuits.

Figure 6-9   Example #1: A VT1.5 circuit in a BLSR

VT1.5 circuit #1 on STS-1
1 VT1.5 used on STS-1
27 VT1.5s available on STS-1

XCVT-XC10G Matrices

Source

STS Matrix

Drop

EC-1

2 STSs total used
22 STSs available

OC-12

VT1.5 Matrix

STS
VT1.5

61846
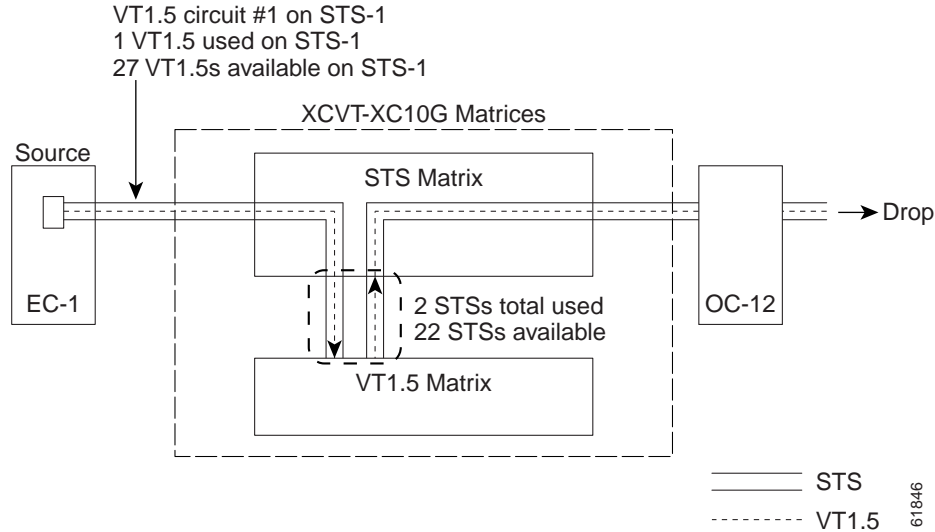
In Figure 6-10, a second VT1.5 circuit is created from the EC-1 card. In this example, the circuit is assigned to STS-2:

- Two more of the 24 STSs available for VT1.5 traffic are used.
- 20 STSs are available on the XCVT or XC10G for VT1.5 circuits.
- STS-2 can carry 27 additional VT1.5 circuits.

Figure 6-10   Example #2: Two VT1.5 circuits in a BLSR

VT1.5 circuit #1

XCVT-XC10G Matrices

Source

STS Matrix

Drop

EC-1

4 STSs total used
20 STSs available

OC-12

VT1.5 circuit #2 on STS-2
1 VT1.5 used on STS-2
27 VT1.5s available on STS-2

STS
VT1.5

61847
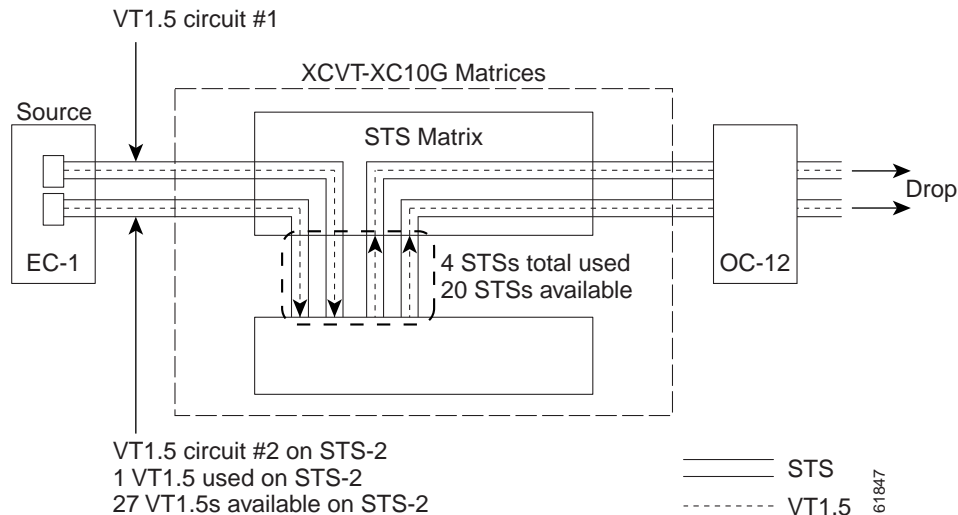
If you create VT1.5 circuits on nodes in UPSR or 1+1 protection, an additional STS is used for the protect path at the source and drop nodes. Figure 6-11 shows a VT1.5 circuit at a UPSR source node. When the circuit is completed:

- Three of the 24 STSs available for VT1.5 mapping on the XCVT or XC10G are used (one input and two outputs, one output for the working path and one output for the protect path).

Cisco ONS 15454 Installation and Operations Guide

• 21 STSs are available for VT1.5 circuits.

Figure 6-11   Example #3: VT1.5 circuit in a UPSR or 1+1 protection scheme
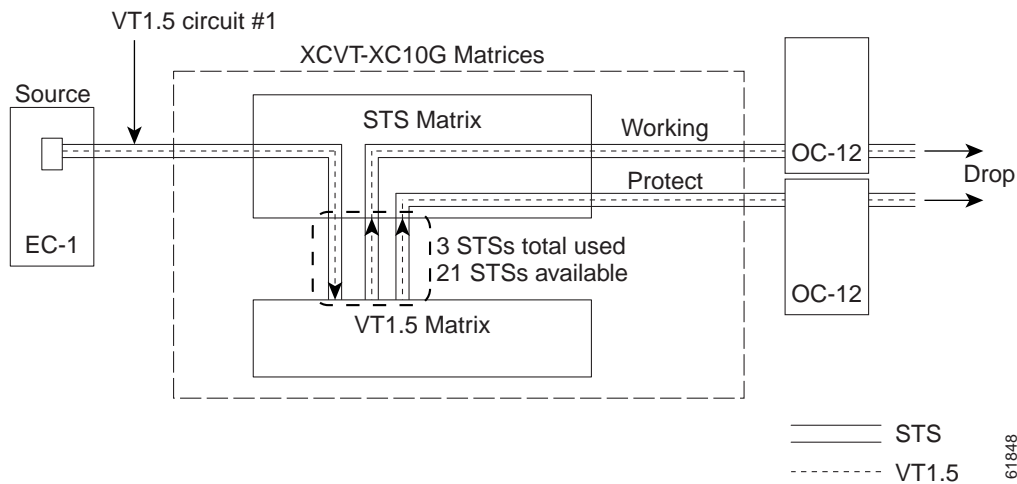
Figure 6-12 shows a second VT1.5 circuit that was created using STS-2. When the second VT1.5 circuit is created:

• Three more VT1.5-mapped STSs are used.

• 18 STSs are available on the XCVT or XC10G for VT1.5 circuits.

Figure 6-12   Example #4: Two VT1.5 circuits in UPSR or 1+1 protection scheme
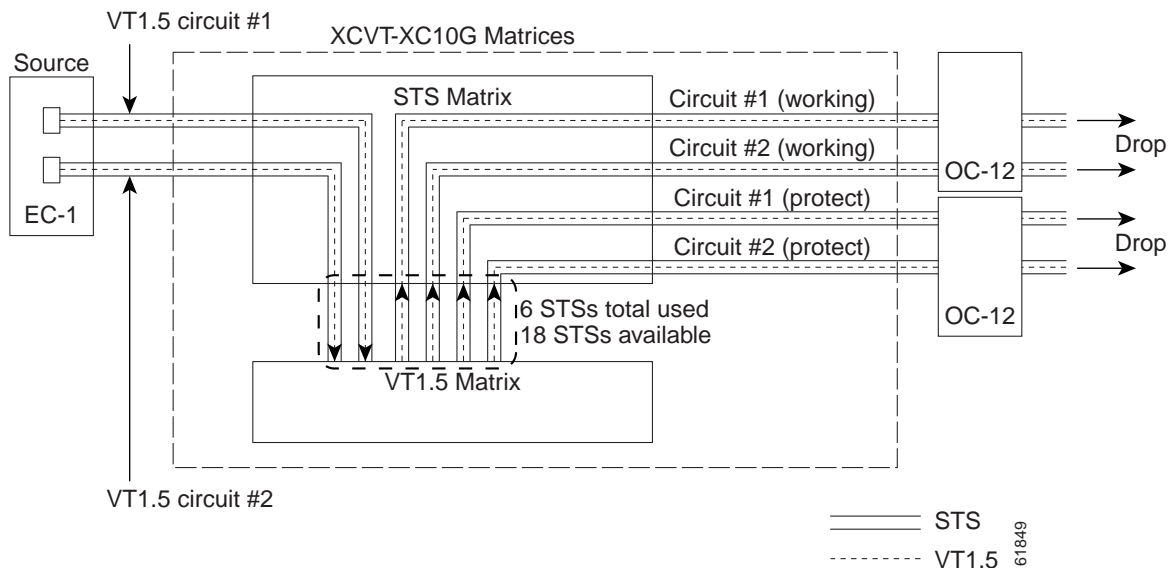
Unless you create VT tunnels (see the "VT Tunnels" section on page 6-19), VT1.5 circuits use STSs on the XCVT/XC10G VT matrix at each node through which the circuit passes.

• Two STSs are used at each node in the Figure 6-9 example, and three STSs are used at each node in the Figure 6-11 example.

- In the Figure 6-10 example, three STSs are used at the source and drop nodes and four STSs are used at pass-through nodes. In Figure 6-12, six STSs are used at the source and drop nodes and four STSs at the pass-through nodes.

6.8.2 VT Tunnels

To maximize VT matrix resources, you can tunnel VT1.5 circuits through ONS 15454 pass-through nodes (nodes that are not a circuit source or drop). VT1.5 tunnels provide two benefits:

- They allow you to route VT1.5 circuits through ONS 15454s that have XC cards. (VT1.5 circuits require XCVT or XC10G cards at circuit source and drop nodes.)

- When tunneled through nodes with XCVT or XC10G cards, VT1.5 tunnels do not use VT matrix capacity, thereby freeing the VT matrix resources for other VT1.5 circuits.

Figure 6-13 shows a VT tunnel through the XCVT and XC10G matrices. No VT1.5-mapped STSs are used by the tunnel, which can carry 28 VT1.5s. However, the tunnel does use two STS matrix ports on each node through which it passes.

Figure 6-13   A VT1.5 tunnel
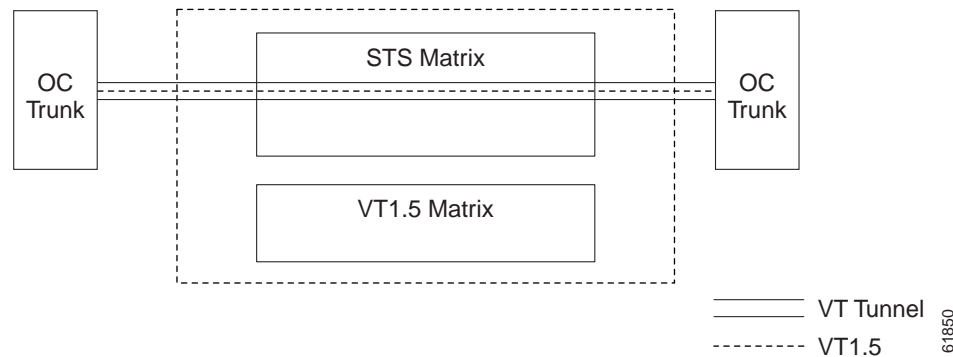
Figure 6-14 shows a six-node ONS 15454 ring with two VT tunnels. One tunnel carries VT1.5 circuits from Node 1 to Node 3. The second tunnel carries VT1.5 circuits from Node 1 to Node 4. Table 6-5 shows the VT1.5-mapped STS usage at each node in a ring based on protection scheme and use of VT tunnels. In the Figure 6-14 example, the circuit travels west through Nodes 2, 3, and 4. Subsequently, VT-mapped STS usage at these nodes is greater than at Nodes 5 and 6.

Figure 6-14   A six-node ring with two VT1.5 tunnels
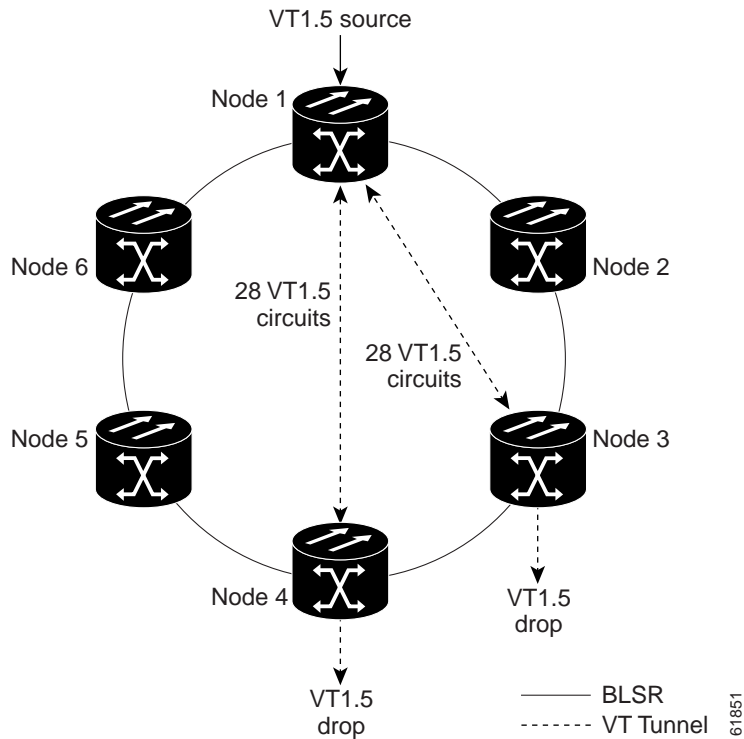
Table 6-5   VT1.5-Mapped STS Use in Figure 6-6

Node	VT Tunnel (BLSR)	VT Tunnel (UPSR, 1+1)	No VT Tunnel (BLSR)	No VT Tunnel (UPSR)	No VT Tunnel (1+1)
1	4	6	4	6	6
2	0	0	4	3	8
3	2	3	4	3	6
4	2	3	2	3	3
5	0	0	0	2	0
6	0	0	0	2	0

When planning VT1.5 circuits, weigh the benefits of using tunnels with the need to maximize STS capacity. For example, a VT1.5 tunnel between Node 1 and Node 4 passing (transparently) through Nodes 2 and Node 3 is advantageous if a full STS is used for Node 1 – Node 4 VT1.5 traffic (that is, the number of VT1.5 circuits between these nodes is close to 28). A VT tunnel is required if:

• Node 2 or Node 3 have XC cards, or

• All VT1.5-mappable STSs at Node 2 and Node 3 are in use.

However, if the Node 1 – Node 4 tunnel will carry few VT1.5 circuits, creating a regular VT1.5 circuit between Nodes 1, 2, 3, and 4 might maximize STS capacity.

When you create a VT1.5 circuit, CTC determines whether a tunnel already exists between source and drop nodes. If a tunnel exists, CTC checks the tunnel capacity. If the capacity is sufficient, CTC routes the circuit on the existing tunnel. If a tunnel does not exist, or if an existing tunnel does not have

sufficient capacity, CTC displays a dialog box asking whether you want to create a tunnel. Before you create the tunnel, review the existing tunnel availability, keeping in mind future bandwidth needs. In some cases, you may want to manually route a circuit rather than create a new tunnel.

6.9 Creating DCC Tunnels

SONET provides four data communications channels (DCCs) for network element operations, administration, maintenance, and provisioning: one on the SONET Section layer and three on the SONET Line layer. The ONS 15454 uses the Section DCC (SDCC) for ONS 15454 management and provisioning.

You can use the Line DCCs (LDCCs) and the SDCC (when the SDCC is not used for ONS 15454 DCC terminations) to tunnel third-party SONET equipment across ONS 15454 networks. A DCC tunnel end-point is defined by Slot, Port, and DCC, where DCC can be either the SDCC, Tunnel 1, Tunnel 2, or Tunnel 3 (LDCCs). You can link an SDCC to an LDCC (Tunnel 1, Tunnel 2, or Tunnel 3), and an LDCC to an SDCC. You can also link LDCCs to LDCCs and link SDCCs to SDCCs. To create a DCC tunnel, you connect the tunnel end points from one ONS 15454 optical port to another.

Each ONS 15454 can support up to 32 DCC tunnel connections. Table 6-6 shows the DCC tunnels that you can create.

Table 6-6   DCC Tunnels

DCC	SONET Layer	SONET Bytes	OC-3 (all ports)	OC-12, OC-48
SDCC	Section	D1 - D3	Yes	Yes
Tunnel 1	Line	D4 - D6	No	Yes
Tunnel 2	Line	D7 - D9	No	Yes
Tunnel 3	Line	D10 - D12	No	Yes

Figure 6-15 shows a DCC tunnel example. Third-party equipment is connected to OC-3 cards at Node 1/Slot 3/Port 1 and Node 3/Slot 3/Port 1. Each ONS 15454 node is connected by OC-48 trunk cards. In the example, three tunnel connections are created, one at Node 1 (OC-3 to OC-48), one at Node 2 (OC-48 to OC-48), and one at Node 3 (OC-48 to OC-3).

Figure 6-15   A DCC tunnel

Link 1		Link 2		Link 3	
From (A)	To (B)	From (A)	To (B)	From (A)	To (B)
Slot3 (OC3)	Slot13 (OC48)	Slot12 (OC48)	Slot13 (OC48)	Slot12 (OC48)	Slot3 (OC3)
port 1, SDCC	port 1, Tunnel 1	port 1, Tunnel 1	port 1, Tunnel 1	port 1, Tunnel 1	port 1, SDCC
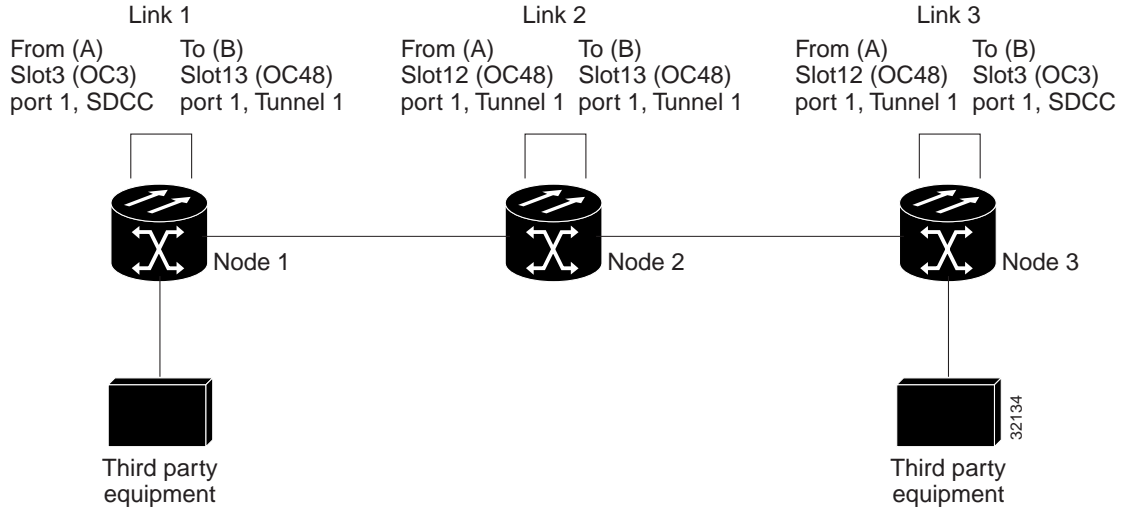
When you create DCC tunnels, keep the following guidelines in mind:

- Each ONS 15454 can have up to 32 DCC tunnel connections.
- Each ONS 15454 can have up to 10 SDCC terminations.
- An SDCC that is terminated cannot be used as a DCC tunnel end-point.
- An SDCC that is used as an DCC tunnel end-point cannot be terminated.
- All DCC tunnel connections are bidirectional.

Procedure: Provision a DCC Tunnel

Step 1   Log into an ONS 15454 that is connected to the non-ONS 15454 network.

Step 2   Click the **Provisioning > Sonet DCC** tabs.

Step 3   Beneath the DCC Tunnel Connections area (bottom right of the screen), click **Create**.

Step 4   In the Create DCC Tunnel Connection dialog box (Figure 6-16), select the tunnel end points from the *From (A)* and *To (B)* lists.

Note   You cannot use the SDCC listed under SDCC Terminations (left side of the window) for tunnel connections. These are used for ONS 15454 optical connections.

Figure 6-16   Selecting DCC tunnel end points
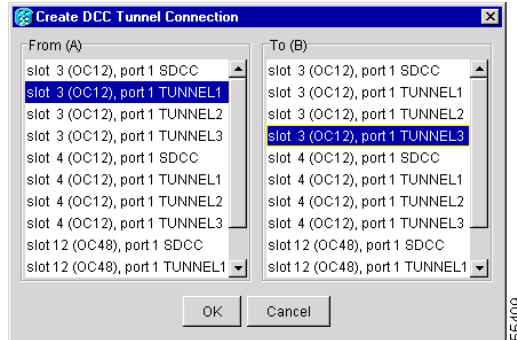
Step 5   Click **OK**.

Step 6   Put the ports hosting the DCC tunnel in service:

   a. Double-click the card hosting the DCC in the shelf graphic or right-click the card on the shelf graphic and select **Open**.

   b. Click the **Provisioning > Line** tabs.

   c. Under Status, select **In Service**.

   d. Click **Apply**.

DCC provisioning is now complete for one node. Repeat these steps for all slots/ports that are part of the DCC tunnel, including any intermediate nodes that will pass traffic from third party equipment. The procedure is confirmed when the third-party network elements successfully communicate over the newly-established DCC tunnel.

Card Provisioning

This chapter provides Cisco ONS 15454 procedures for:

- Changing the default transmission parameters for electrical (EC-1, DS-N) and optical (OC-N) cards, including provisioning OC-N cards for SDH
- Setting performance monitoring (PM) thresholds, including intermediate path performance monitoring
- Provisioning the Alarm Interface Controller card
- Converting the DS1-14 and DS3-12 cards from 1:1 to 1:N protection

Note Ethernet card provisioning is described in Chapter 9, "Ethernet Operation."

Because much of the electrical and optical card provisioning involves PM thresholds, see Chapter 8, "Performance Monitoring," for definitions and general information about ONS 15454 performance monitoring parameters. In addition, refer to the Telcordia GR-1230-CORE, GR-820-CORE, and GR-253-CORE documents. The default thresholds delivered with ONS 15454 cards are based on specifications contained in those documents.

Note For information about creating protection groups, see the "Creating Protection Groups" section on page 3-9. For circuit creation procedures, see Chapter 6, "Circuits and Tunnels."

7.1 Performance Monitoring Thresholds

ONS 15454 card default thresholds are based on GR-253-CORE and GR-820-CORE. If you change their settings, the following rules apply:

- The minimum threshold that you can set is 1.
- If you set a threshold to 0, no threshold crossing alert (TCA) is issued.
- You can set thresholds to any DS-N or OC-N maximum. However, CTC does not perform range checking. Setting a threshold to a value greater than what is logically possible is the same as setting the threshold to zero. No TCA will be issued.

7.2 Provisioning Electrical Cards

The ONS 15454 electrical cards (DS1-14, DS1N-14, DS3-12, DS3N-12, DS3E1-12, DS3EN-12, DS3XM-6, and EC1-12) are pre-provisioned with settings that you can modify to manage transmission quality. When you open a card in CTC and select the Provisioning tab, the following subtabs are commonly displayed:

- *Line*—Sets line setup parameters, such as line coding and line length. This is also where you put ports in and out of service.
- *Line Threshold*—Sets the line-level PM thresholds.
- *Elect Path Threshold*—Sets the path-level PM thresholds for electrical (DS-3/DS-1) traffic.
- *SONET Threshold*—Sets the path-level PM thresholds for (STS/VT1.5) traffic.
- *Alarming*—Sets alarm profiles for individual ports and suppresses alarms. See Chapter 10, "Alarm Monitoring and Management," for information about alarm profiles and alarm suppression.

Table 7-1 provides an overview of DS-1, DS-3, DS3E, and DS3XM parameters (an X means the item is available for the card). EC1-12 card parameters are shown in Table 7-6 on page 7-15.

Table 7-1   DS-N Card Provisioning Overview

Subtab	Provisioning Item	DS1-14/ DS1N-14	DS3-12/ DS3N-12	DS3E1-12/ DS3EN-12	DS3XM-6
Line	Port #	X	X	X	X
	Port Name	X	X	X	X
	Line Type	X		X	X
	Detected Line Type			X	
	Line Coding	X		X	X
	Line Length	X	X	X	X
	Status	X	X	X	X
Line Threshold	Port	X	X	X	X
	CV	X	X	X	X
	ES	X	X	X	X
	SES	X	X	X	X
	LOSS		X	X	X
Elect Path	Port	X		X	X
	CV			X	X
	ES	X		X	X
	SES	X		X	X
	SAS	X		X	X
	AIS	X		X	X
	UAS	X		X	X

Table 7-1   *DS-N Card Provisioning Overview (continued)*

| Subtab	Provisioning Item	DS1-14/ DS1N-14	DS3-12/ DS3N-12	DS3E1-12/ DS3EN-12	DS3XM-6
SONET Threshold	Port	X	X	X	X
	CV	X	X	X	X
	ES	X	X	X	X
	FC	X	X	X	X
	SES	X	X	X	X
	UAS	X	X	X	X
Alarming	Port	X	X	X	X
	Profile	X	X	X	X
	Suppress Alarms	X	X	X	X

7.2.1 DS-1 Card Parameters

The ONS 15454 DS-1 cards (DS1-14 and DS1N-14) provide 14 DS-1 ports. Each port operates at 1.544 Mbps. Default thresholds are based on recommendations in GR-820-CORE, Sections 4.0.

Procedure: Modify Line and Threshold Settings for the DS-1 Card

Step 1   Display the DS1-14 or DS1N-14 in CTC card view.

Step 2   Click the **Provisioning** tab (Figure 7-1).

Figure 7-1   *Provisioning line parameters on the DS1-14 card*
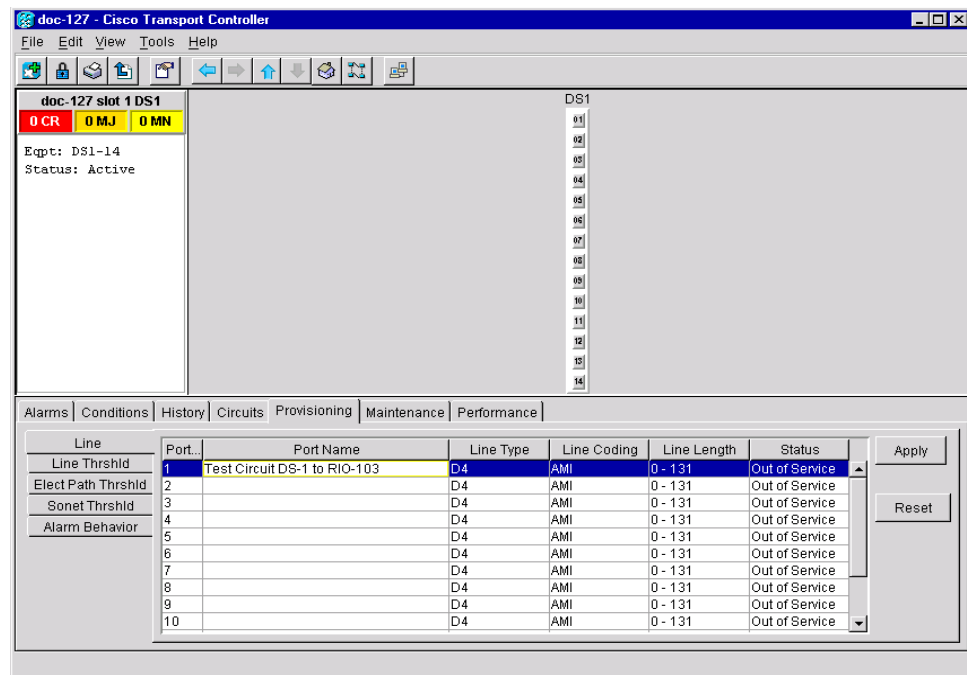
Step 3   Depending on the setting you need to modify, click the **Line**, **Line Thrshld**, **Elect Path**, or **Sonet Thrshld** subtab.

> ✎
> **Note**   See Chapter 10, "Alarm Monitoring and Management" for information about the Alarm Behavior tab.

Step 4   Modify the settings shown in Table 7-2 on page 7-4. For drop-down lists, select an item from the list. For numerics, double-click the field and type the new number.

Table 7-2   DS-1 Card Parameters

Subtab	Parameter	Description	Options
Line	Port #	Port number	1 - 14
	Port	Port name	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	Line Type	Defines the line framing type	• D4 (default) • ESF - Extended Super Frame • Unframed
	Line Coding	Defines the DS-1 transmission coding type	• AMI - Alternate Mark Inversion (default) • B8ZS - Bipolar 8 Zero Substitution
	Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 131 (default) • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655
	Status	Places port in or out of service	• Out of Service (default) • In Service
Line Thrshold	CV	Coding violations	Numeric. Defaults: • 13340 (15 min) • 133400 (1 day)
	ES	Errored seconds	Numeric. Defaults: • 65 (15 min) • 648 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 10 (15 minutes) • 100 (1 day)

Table 7-2   DS-1 Card Parameters (continued)

Subtab	Parameter	Description	Options
Elect Path Thrshld	ES	Errored seconds	Numeric. Defaults: • 65 (15 minutes) • 648 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 10 (15 minutes) • 100 (1 day)
	SAS	Severely errored frame/alarm indication signal	Numeric. Defaults: • 2 (15 minutes) • 17 (1 day)
	AIS	Alarm indication signal	Numeric. Defaults: • 10 (15 minutes) • 10 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults: • 10 (15 minutes) • 10 (1 day)
SONET Threshold	CV	Coding violations	Numeric. Defaults: • 15 (15 minutes) • 125 (1 day)
	ES	Errored seconds	Numeric. Defaults: • 12 (15 minutes) • 100 (1 day)
	FC	Failure count	Numeric. Defaults (VT termination): • 10 (15 minutes) • 10 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 3 (15 minutes) • 7 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults: • 10 (15 minutes) • 10 (1 day)

Table 7-2   DS-1 Card Parameters (continued)

Subtab	Parameter	Description	Options
Alarming	Port	Port number	1 - 14
	Profile	Sets the alarm profile for the port	• Default • Inherited • Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port	• Unselected (default) • Selected

Step 5   Click **Apply**.

Step 6   Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.2.2 DS-3 Card Parameters

The ONS 15454 DS-3 cards (DS3-12 and DS3N-12) provide 12 DS-1 ports. Each port operates at 44.736 Mbps. Default thresholds are based on recommendations in GR-820-CORE, Section 5.0.

Procedure: Modify Line and Threshold Settings for the DS-3 Card

Step 1   Display the DS3-12 or DS3N-12 in CTC card view.

Step 2   Click the **Provisioning** tab.

Step 3   Depending on the setting you need to modify, click the **Line**, **Line Thrshld**, or **Sonet Thrshld** subtab.

Note   See Chapter 10, "Alarm Monitoring and Management" for information about the Alarm Behavior tab.

Step 4   Modify the settings shown in Table 7-3. For drop-down lists, select an item from the list. For numerics, double-click the field and type the new number.

Table 7-3   DS-3 Card Parameters

Subtab	Parameter	Description	Options
Line	Port #	Port number	1 - 12
	Port	Port name	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 225 (default) • 226 - 450
	Status	Places port in or out of service	• Out of Service (default) • In Service
Line Thrshold	CV	Coding violations	Numeric. Defaults: • 387 (15 minutes) • 3865 (1 day)
	ES	Errored seconds	Numeric. Defaults: • 25 (15 minutes) • 250 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 4 (15 minutes) • 40 (1 day)
	LOSS	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Defaults: • 10 (15 minutes) • 10 (1 day)

Table 7-3   DS-3 Card Parameters (continued)

Subtab	Parameter	Description	Options
SONET Thrshold	CV	Coding violations	Numeric. Defaults (Near End, STS termination): • 15 (15 minutes) • 125 (1 day)
	ES	Errored seconds	Numeric. Defaults (Near End, STS termination): • 12 (15 minutes) • 100 (1 day)
	FC	Failure count	Numeric. Defaults (Near End, STS termination: • 10 (15 minutes) • 10 (1 day)
	SES	Severely errored seconds	Numeric. Defaults (Near End, STS termination): • 3 (15 minutes) • 7 (1 day)
	UAS	Unavailable seconds	Numeric. Default (Near End, STS termination): • 10 (15 minutes) • 10 (1 day)
Alarming	Port	Port number	1 - 12
	Profile	Sets the alarm profile for the port.	• Default • Inherited • Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port.	• Unselected (default) • Selected

Step 5   Click **Apply**.

Step 6   Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.2.3 DS3E Card Parameters

The DS3E-12 and DS3EN-12 cards provide 12 DS-3 ports. Each port operates at 44.736 Mbps. The DS3E uses B3ZS error monitoring and enhanced performance monitoring, including P-Bit and CP-Bit monitoring. Default thresholds are based on recommendations in GR-820-CORE, Section 5.0.

> ✎
> **Note**   If the DS3E is installed in an ONS 15454 slot that is provisioned for a DS-3 card, the DS3E enhanced
> performance monitoring parameters are not available. If this occurs, remove the DS3E from the ONS
> 15454, delete the DS-3 card in CTC, and provision the slot for the DS3E.

Procedure: Modify Line and Threshold Settings for the DS3E Card

Step 1   Display the DS3E-12 or DS3EN-12 in CTC card view.

Step 2   Click the **Provisioning** tab.

Step 3   Depending on the setting you need to modify, click the **Line**, **Line Thrshld**, **Elect Path**, or **Sonet Thrshld** subtab.

> ✎
> **Note**   See Chapter 10, "Alarm Monitoring and Management" for information about the Alarm
> Behavior tab.

Step 4   Modify the settings shown in Table 7-4 on page 7-9. For drop-down lists, select an item from the list.
For numerics, double-click the field and type the new number.

Table 7-4   DS3E Card Parameters

Subtab	Parameter	Description	Options
Line	Port #	Port number	• 1 - 12
	Port	Port name	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	Line Type	Defines the line framing type	• M23 • C Bit • Auto Provisioned
	Detected Line Type	Displays the detected line type	Read-only
	Line Coding	Defines the DS3E transmission coding type	• B3ZS
	Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 225 (default) • 226 - 450
	Status	Places port in or out of service	Out of Service (default) In Service

Table 7-4   DS3E Card Parameters (continued)

Subtab	Parameter	Description	Options
Line Thrshold	CV	Coding violations	Numeric. Defaults: • 387 (15 minutes) • 3865 (1 day)
	ES	Errored seconds	Numeric. Defaults: • 25 (15 minutes) • 250 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 4 (15 minutes) • 40 (1 day)
	LOSS	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Defaults: • 10 (15 minutes) • 10 (1 day)
Elect Path Thrshld	CV	Coding violations	Numeric. Defaults (DS3 Pbit, Near End only; DS3 CPbit, Near and Far End): • 382 (15 minutes) • 3820 (1 day)
	ES	Errored seconds	Numeric. Defaults (DS3 Pbit, Near End only; DS3 CPbit, Near and Far End): • 25 (15 minutes) • 250 (1 day)
	SES	Severely errored seconds	Numeric. Defaults (DS3 Pbit, Near End only; DS3 CPbit, Near and Far End): • 4 (15 minutes) • 40 (1 day)
	SAS	Severely errored frame/Alarm indication signal	Numeric. Defaults (DS3 Pbit, Near End only; DS3 CPbit, Near and Far End): • 2 (15 minutes) • 8 (1 day)
	AIS	Alarm indication signal	Numeric. Defaults (DS3 Pbit, Near End only; DS3 CPbit, Near and Far End): • 10 (15 minutes) • 10 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults (DS3 Pbit, Near End only; DS3 CPbit, Near and Far End): • 10 (15 minutes) • 10 (1 day)

Table 7-4   DS3E Card Parameters (continued)

Subtab	Parameter	Description	Options
Sonet Thrshld	CV	Coding violations	Numeric. Defaults (Near End STS termination): • 15 (15 minutes) • 125 (1 day)
	ES	Errored seconds	Numeric. Defaults (Near End STS termination): • 12 (15 minutes) • 100 (1 day)
	FC	Failure count	Numeric. Defaults (Near End STS termination): • 10 (15 minutes) • 10 (1 day)
	SES	Severely errored seconds	Numeric. Defaults (Near End STS termination): • 3 (15 minutes) • 7 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults (Near End STS termination): • 10 (15 minutes) • 10 (1 day)
Alarming	Port	Port number	1 - 12
	Profile	Sets the alarm profile for the port.	• Default • Inherited • Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port.	• Unselected (default) • Selected

Step 5   Click **Apply**.

Step 6   Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.2.4 DS3XM-6 Card Parameters

The DS3XM-6 transmux card can accept up to six DS-3 signals and convert each signal to 28 VT1.5s. Conversely, the card can take 28 T-1s and multiplex them into a channeled C-bit or M23 framed DS-3. Unlike the DS3-12 and DS3N-12 cards, the DS3XM-6 allows circuit mapping at the VT level. Table 7-5 on page 7-12 shows parameters that you can provision for each port.

Procedure: Modify Line and Threshold Settings for the DS3XM-6 Card

Step 1   Display the DS3XM-6 in CTC card view.

Step 2   Click the **Provisioning** tab.

Step 3   Depending on the setting you need to modify, click the **Line**, **Line Thrshld**, **Elect Path**, or **Sonet Thrshld** subtab.

> **Note**   See Chapter 10, "Alarm Monitoring and Management" for information about the Alarm Behavior tab.

Step 4   Modify the settings shown in Table 7-5. For drop-down lists, select an item from the list. For numerics, double-click the field and type the new number.

Table 7-5   DS3XM-6 Parameters

Subtab	Parameter	Description	Options
Line	Port #	Port number	1 - 6
	Port	Port name	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	Line Type	Defines the line framing type	• M23 - default • C BIT
	Line Coding	Defines the DS-1 transmission coding type that is used	• B3ZS
	Line Length	Defines the distance (in feet) from backplane connection to the next termination point	• 0 - 225 (default) • 226 - 450
	Status	Places port in or out of service	• Out of Service (default) • In Service
Line Thrshld	CV	Coding violations	Numeric. Defaults: • 387 (15 minutes) • 3865 (1 day)
	ES	Errored seconds	Numeric. Defaults: • 25 (15 minutes) • 250 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 4 (15 minutes) • 40 (1 day)
	Loss	Loss of signal	Numeric. Defaults: • 10 (15 minutes) • 10 (1 day)

Table 7-5   DS3XM-6 Parameters (continued)

Subtab	Parameter	Description	Options
Elect Path Thrshld	CV	Coding violations	Numeric. Defaults (DS3, Pbit Near End only; DS3 CPbit, Near and Far End): • 382 (15 minutes) • 3820 (1 day)
	ES	Errored seconds	Numeric. Defaults (15 min/1 day): • 25/250 (DS3 Pbit Near End only; DS3 CPbit, Near and Far End) • 65/648 (DS1, Near End only)
	SES	Severely errored seconds	Numeric. Defaults (15 min/1 day): • 4/40 (DS3 Pbit Near End only; DS3 CPbit, Near and Far End) • 10/100 (DS1, Near End only)
	SAS	Severely errored frame/alarm indication Signal	Numeric. Defaults (15 min/1 day): • 2/8 (DS3 Pbit Near End only; DS3 CPbit, Near and Far End) • 2/17 (DS1, Near End only)
	AIS	Alarm indication signal	Numeric. Defaults (15 min/1 day): • 10/10 DS1, Near End; DS3, Near & Far End • 0/0 DS1 Far End
	UAS	Unavailable seconds	Numeric. Defaults (15 min/1 day): • 10/10 (DS3 Pbit Near End only; DS3 CPbit, Near and Far End) • 10/10 (DS1, Near End only)

Table 7-5   DS3XM-6 Parameters (continued)

Subtab	Parameter	Description	Options
Sonet Thrshld	CV	Coding violations	Numeric. Defaults (Near/Far End): • 15 (15 minutes, STS and VT Term) • 125 (1 day, STS and VT Term)
	ES	Errored seconds	Numeric. Defaults (Near/Far End): • 12 (15 minutes, STS and VT Term) • 100 (1 day, STS and VT Term)
	FC	Failure count	Numeric. Defaults (Near/Far End): • 10 (15 minutes, STS Term) • 10 (1 day, STS Term)
	SES	Severely errored seconds	Numeric. Defaults (Near/Far End): • 3 (15 minutes, STS and VT Term) • 7 (1 day, STS and VT Term)
	UAS	Unavailable seconds	Numeric. Defaults (Near/Far End): • 10 (15 minutes, STS and VT Term) • 10 (1 day, STS and VT Term)
Alarming	Port	Port number	1 - 6
	Profile	Sets the alarm profile for the port	• Default • Inherited • Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port	• Unselected (default) • Selected

Step 5   Click **Apply**.

Step 6   Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.2.5 EC1-12 Card Parameters

The EC1-12 provides 12 STS-1 electrical ports. Each port operates at 51.840 Mbps. Table 7-6 shows the parameters for the EC1-12 card.

Procedure: Modify Line and Threshold Settings for the EC-1 Card

Step 1   Display the EC1-12 in CTC card view.

Step 2   Click the **Provisioning** tab.

Step 3   Depending on the setting you need to modify, click the **Line**, **Thresholds,** or **STS** subtab.

> ✎
> **Note**   See Chapter 10, "Alarm Monitoring and Management" for information about the Alarm Behavior tab.

Step 4   Modify the settings shown in Table 7-6. For drop-down lists, select an item from the list. For numerics, double-click the field and type the new number.

Table 7-6   EC1-12 Card Parameters

Subtab	Parameter	Description	Options
Line	Port #	EC-1 card port #	1 - 12
	Port Name	Name assigned to the port (optional)	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	PJStsMon#	Sets the STS that will be used for pointer justification. If set to zero, no STS is used. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	• 0 (default) • 1
	Line Buildout	Defines the distance (in feet) from backplane to next termination point	• 0 - 225 (default) • 226 - 450
	Rx Equalization	For early EC1-12 card versions, equalization can be turned off if the line length is short or the environment is extremely cold; Rx Equalization should normally be set to On	• On (checked, default) • Off (unchecked)
	Status	Places the port in or out of service	• Out of Service (default) • In Service

Table 7-6   EC1-12 Card Parameters (continued)

Subtab	Parameter	Description	Options
Thresholds - Line	CV	Coding violations	Numeric. Defaults: • 1312 (15 minutes) • 13120 (1 day)
	ES	Errored seconds	Numeric. Defaults: • 87 (15 minutes) • 864 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: • 1 (15 minutes) • 4 (1 day)
	FC	Failure count	Numeric. Defaults: • 10 (15 minutes) • 0 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults: • 3 (15 minutes) • 10 (1 day)
	PPJC-Pdet	Positive Pointer Justification Count, STS Path Detected. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults (near end): • 60 (15 minutes) • 5760 (1 day)
	NPJC-Pdet	Negative Pointer Justification Count, STS Path Detected. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults • 0 (15 minutes) • 0 (1 day)
	PPJC-Pgen	Positive Pointer Justification Count, STS Path Generated. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults: • 0 (15 minutes) • 0 (1 day)
	NPJC-Pgen	Negative Pointer Justification Count, STS Path Generated. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults: • 0 (15 minutes) • 0 (1 day)

Table 7-6   EC1-12 Card Parameters (continued)

Subtab	Parameter	Description	Options
Thresholds - Section	CV	Coding violations	Numeric. Defaults (Near End only): 10000 (15 minutes) 100000 (1 day)
	ES	Errored seconds	500 (15 minutes) 5000 (1 day)
	SES	Severely errored seconds	500 (15 minutes) 5000 (1 day)
	SEFS	Severely errored framing seconds	500 (15 minutes) 5000 (1 day)
Thresholds - Path	CV	Coding violations	Numeric. Defaults (Near and Far End): 15 (15 minutes) 125 (1 day)
	ES	Errored seconds	12 (15 minutes) 100 (1 day)
	FC	Failure count	10 (15 minutes) 10 (1 day)
	SES	Severely errored seconds	3 (15 minutes) 7 (1 day)
	UAS	Unavailable seconds	10 (15 minutes) 10 (1 day)
STS	STS #	EC-1 port (Line #) and STS # available for Intermediate Path Performance Monitoring.	
	Enable IPPM	Enables IPPM for the EC-1 port and STS #	Unchecked (default); IPPM not enabled Checked; IPPM is enabled
Alarming	Port	Port number	1 - 12
	Profile	Sets the alarm profile for the port.	Default Inherited Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port.	Unselected (default) Selected

Step 5   Click **Apply**.

Step 6   Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.3 Provisioning Optical Cards

This section explains how to modify transmission quality by provisioning line and threshold settings for OC-N cards and how to provision OC-N cards for SDH.

7.3.1 Modifying Transmission Quality

The OC-3, OC-12, OC-48, and OC-192 cards are pre-provisioned with settings that you can modify to manage transmission quality. Depending on the optical card, you can specify thresholds for near and far end nodes at the Line, Section, and Path levels for 15-minute and one day intervals.

Procedure: Provision Line Transmission Settings for OC-N Cards

Step 1   Display the OC-N card in CTC card view.

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

Step 3   Modify the settings shown in Table 7-7.

Table 7-7   OC-N Card Line Settings on the Provisioning > Line Tab

Heading	Description	Options
#	Port number	• 1 (OC-12, OC-48, OC-192) • 1-4 (OC-3)
SF BER Level	Sets the signal fail bit error rate	• 1E-3 • 1E-4 (default) • 1E-5
SD BER Level	Sets the signal degrade bit error rate	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Provides Synch	If checked, the card is provisioned as a network element timing reference on the Provisioning > Timing tabs	Read-only • Yes (checked) • No (unchecked)
Enable Synch Messages	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source	• Yes (checked, default) • No (unchecked)

Table 7-7   OC-N Card Line Settings on the Provisioning > Line Tab (continued)

Heading	Description	Options
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte	• Yes (checked) • No (unchecked; default)
PJ Sts Mon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	• 0 (default) - 3 (OC-3, per port) • 0 (default) - 12 (OC-12) • 0 (default) - 48 (OC-48) • 0 (default) - 192 (OC-192)
Status	Places port in or out of service	• Out of Service (default • In Service
Type	Defines the port as SONET or SDH. See the "Provisioning OC-N Cards for SDH" section on page 7-23.	• Sonet • SDH

Step 4   Click **Apply**.

Procedure: Provision Threshold Settings for OC-N Cards

Step 1   Display the OC-N card in CTC card view (Figure 7-2 on page 7-19).

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

Figure 7-2   Provisioning thresholds for the OC48 IR 1310 card
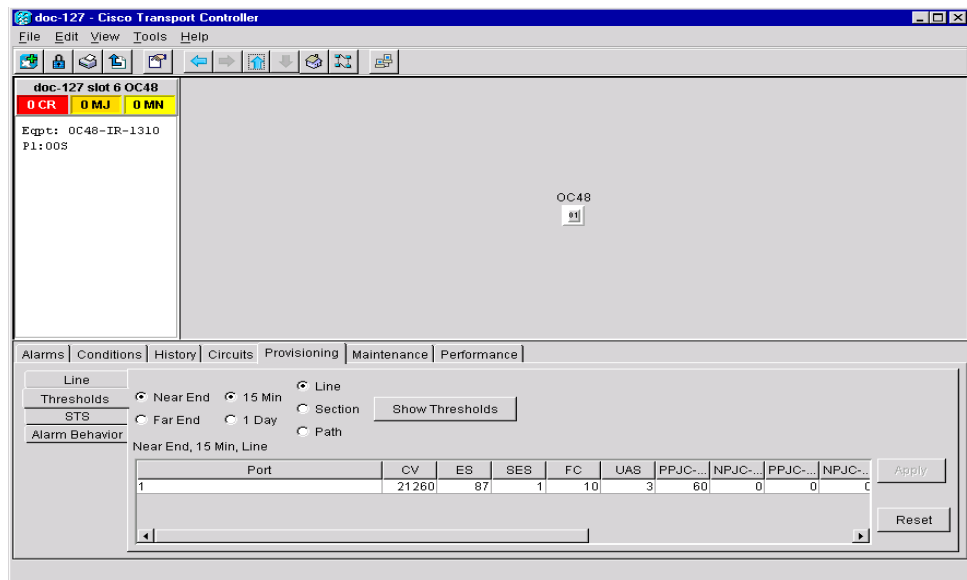
Step 3   Modify the settings shown in Table 7-8 on page 7-20.

Default thresholds apply to all optical cards unless otherwise specified.

Table 7-8   OC-N Card Threshold Settings on the Provisioning > Thresholds Tab

Heading	Description	Options
Port	Port number	• 1, 2, 3, or 4 (OC-3) • 1 (OC-12, OC-48, OC-192)
CV	Coding violations	Numeric. Defaults (15 min/1 day): Line • 1312/13,120 (OC-3 Near & Far End) • 5315/53150 (OC-12 Near & Far End) • 21260/212600 (OC-48 Near & Far End) • 85040/850400 (OC-192 Near & Far End) Section • 10000/100000 (Near End) 0/0 (Far End) • 10000/500 (OC-192 Near & Far End) Path • 15/125 (OC-12, OC-48, OC-192 Near & Far End)
ES	Errored seconds	Numeric. Default (15 min/1 day): Line • 87/864 (Near & Far End) Section • 500/5000 (Near End); 0/0 (Far End) Path • 12/100 (OC-48 & OC-192 Near & Far End)
SES	Severely errored seconds	Numeric. Defaults (15 min/1 day): Line • 1/4 (Near and Far End) Section • 500/5000 (Near End); 0/0 (Far End) Path • 3/7 (OC-48 & OC-192 Near & Far End)
SEFS	Severely errored framing seconds	Numeric. Defaults (15 min/1 day): Section • 500/5000 (Near End); 0/0 (Far End)

Table 7-8   OC-N Card Threshold Settings on the Provisioning > Thresholds Tab (continued)

Heading	Description	Options
FC	Failure count	Numeric. Defaults (15 min/1 day): Line • 10/0 (OC-3, Near and Far End) • 10/40 (OC-12, OC-48, OC-192 Near and Far End) Path • 10/10 (OC-12, OC-48, OC-192 Near and Far End)
UAS	Unavailable seconds	Numeric. Defaults (15 min/1 day): Line • 3/3 (OC-3, Near & Far End • 3/10 (OC-12, OC-48, OC-192 Near and Far End) Path • 10/10 (Near and Far End)
PPJC-Pdet	Positive Pointer Justification Count, STS Path detected. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults (15 min/1 day): Line • 60/5760 Near End • 0/0 Far End
NPJC-Pdet	Negative Pointer Justification Count, STS Path detected. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults (Near and Far End): Line • 0 (15 minutes) • 0 (1 day)
PPJC-Pgen	Positive Pointer Justification Count, STS Path generated. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults (15 min/1 day): Line • 0/0 (Near and Far End)
NPJC-Pgen	Negative Pointer Justification Count, STS Path generated. See the "Pointer Justification Count Parameters" section on page 8-12 for more information.	Numeric. Defaults (15 min/1 day): Line • 0/0 (Near and Far End)
PSC	Protection Switching Count (Line)	Numeric. Defaults (15 min/1 day): Line • 1/5 (Near End) • 0/0 (Far End)

Table 7-8   OC-N Card Threshold Settings on the Provisioning > Thresholds Tab (continued)

Heading	Description	Options
PSD	Protection Switch Duration (Line)	Numeric. Defaults (15 min/1 day): Line • 300/600 (Near End) • 0/0 (all OC-N cards, Far End)
PSC-W	Protection Switching Count - Working line BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line • 0/0 (all OC-N cards except OC-3, Near and Far End)
PSD-W	Protection Switching Duration - Working line BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line • 0/0 (all OC-N cards except OC-3, Near and Far End)
PSC-S	Protection Switching Duration - Span BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line • 0/0 (all OC-N cards except OC-3, Near and Far End)
PSD-S	Protection Switching Duration - Span BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line • 0/0 (all OC-N cards except OC-3, Near and Far End)
PSC-R	Protection Switching Duration - Ring BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line • 0/0 (all OC-N cards except OC-3, Near and Far End)
PSD-R	Protection Switching Duration - Ring BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line • 0/0 (all OC-N cards except OC-3, Near and Far End)

Click **Apply**.

7.3.2 Provisioning OC-N Cards for SDH

You can provision the ONS 15454 OC-3, OC-12, and OC-48 cards to support either SONET or SDH over SONET signals. When provisioned for SDH, each OC-N port drops and inserts STM traffic in unprotected or 1+1 protection mode. Each STM-1 signal is mapped as a 155 Mbps concatenated signal (STS-3c) for transparent transport over a SONET network. The original STM-1 traffic may be handed off as an STM-1 or OC-3.

Because SDH and SONET frame format and size are nearly identical, their line speeds meet, starting at 155 Mbps. For example, at the STM-1/OC-3 level, the ONS 15454 performs section and line overhead conversions and maps the 261x9 byte VC-4 into an STS-3c for transparent transport across the SONET domain. At the far end, the STS-3c carrying the original VC-4 is remapped into an STM-1 for handoff to an SDH network element (node). Table 7-9 shows the SDH over SONET mapping for the ONS 15454 OC-N cards.

Table 7-9   OC-N – SDH Over SONET Mapping

Card	SDH	SDH over SONET
OC-3	STM-1	STS-3c
OC-12	STM-4	STS-12c
OC-48	STM-16	STS-48c
OC-192	STM-64	STS-192c

The ONS 15454 performs section, line overhead, and pointer conversions between SDH and SONET. However, to ensure operability, the following requirements must be met:

- The embedded payload must be compatible on both sides and require no conversion of any kind. Examples of such payloads include concatenated ATM or Packet over SONET/SDH signals.

- The path overhead (POH) must be compatible on both sides and require no conversion of any kind. Each overhead byte must be processed identically or simultaneously ignored. Key POH bytes to consider are the J1 (path indicator) and C2 (payload format).

- You cannot enable intermediate path protection monitoring (IPPM) on OC-12 and OC-48 ports that are enabled for SDH.

Most SONET and SDH routers and ATM switches can be configured to meet these requirements.

Procedure: Provision an OC-N Card for SDH

Step 1   Log into the node and double-click the OC-N card.

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

Step 3   Under **Type**, choose SDH.

Step 4   Click **Apply**.

7.4 Provisioning IPPM

Intermediate-Path Performance Monitoring (IPPM) allows you to transparently monitor traffic originating on DS-1, DS-3, DS3E and DS3XM cards (Path Terminating Equipment) as it passes through EC-1, OC-3, OC-12, OC-48, and OC-192 cards (Line Terminating Equipment). To use IPPM, you create the STS circuit on the DS-N cards, then enable IPPM on the EC-1 or OC-N cards that carry the circuit.

Note For Release 3.0 and later, IPPM is enabled for near-end (originating) traffic only. Far-end (terminating) IPPM will be enabled in a future release.

For example, suppose you have an STS circuit that originates and terminates on DS-N cards at Nodes 1 and 4. You want to monitor the circuit as it passes through OC-N cards at Nodes 2 and 3. To do this, you enable IPPM on the OC-N card by selecting the appropriate STS, in this example, STS 1 (Figure 7-3).

Figure 7-3   IPPM provisioned for STS 1 on an OC-12 card
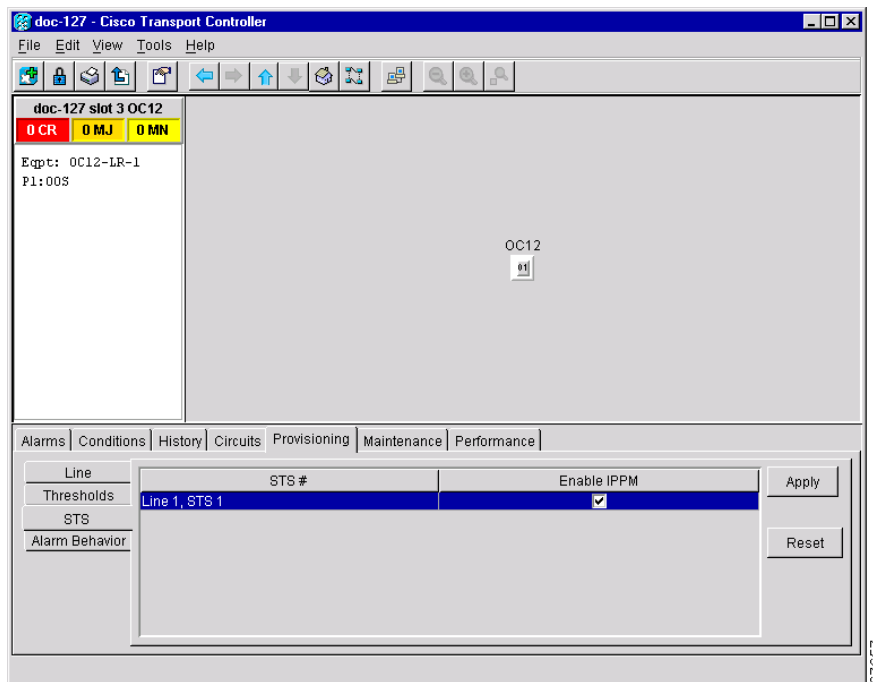
After enabling IPPM, performance is displayed on the Performance tab for the OC-48 card. IPPM enables per-path statistics for STS CV-P (coding violations), STS ES-P (errored seconds), STS FC-P (failure count), STS SES-P (severely errored seconds), and STS UAS-P (unavailable seconds). Only one STS per port can be monitored at one time. See Chapter 8, "Performance Monitoring" for a definition of every parameter.

Procedure: Enable Intermediate-Path Performance Monitoring

Step 1 If the STS circuit does not exist, create the circuit. (The circuit must pass through the EC-1 or OC-N card before you can enable IPPM on the circuit.)

Step 2 In CTC, open the card view of an EC-1 or OC-N card that carries the circuit.

Step 3 Select the **Provisioning > STS** tabs.

Step 4 Click **Enable IPPM** for the STS you want to monitor.

Step 5 Click **Apply**.

7.5 Provisioning the Alarm Interface Controller

The Alarm Interface Controller (AIC) card can be provisioned to receive input from, or send output to, external devices wired to the ONS 15454 backplane. (For detailed specifications about the AIC, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.) You can provision the AIC to:

- Generate CTC alarms based on events such as heating or cooling equipment failure, fire alarms, smoke detection, and other environmental changes that can damage ONS 15454 equipment. These are called external alarms.

- Turn external devices on or off based on a CTC alarm. For example, you can provision the AIC to turn on an audio or visual device, such as a bell or light, when a critical ONS 15454 alarm occurs. These triggers are called external controls.

Figure 7-4 shows the flow to and from external devices provisioned through the AIC.

Figure 7-4   AIC alarm input and output
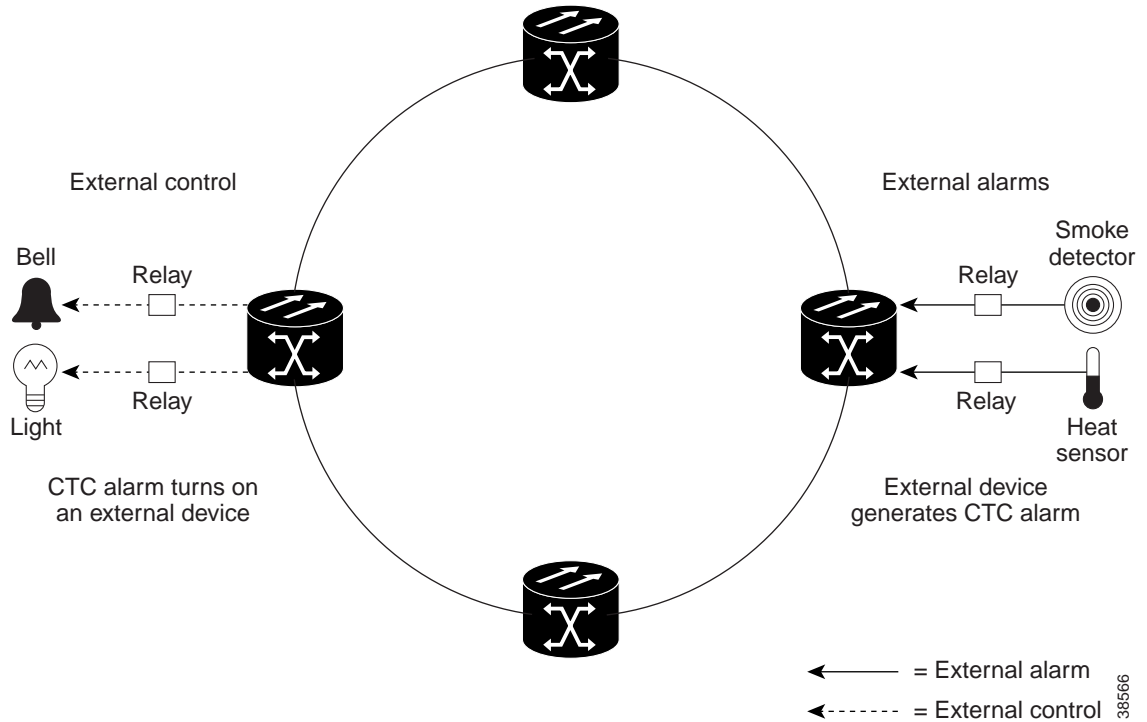
7.5.1 Using Virtual Wires

Provisioning the AIC card provides a "virtual wires" option used to route external alarms and controls from different nodes to one or more alarm collection centers. In Figure 7-5, smoke detectors at Nodes 1, 2, 3, and 4 are assigned to Virtual Wire #1, and Virtual Wire #1 is provisioned as the trigger for an external bell at Node 1.

Figure 7-5   External alarms and controls using a virtual wire
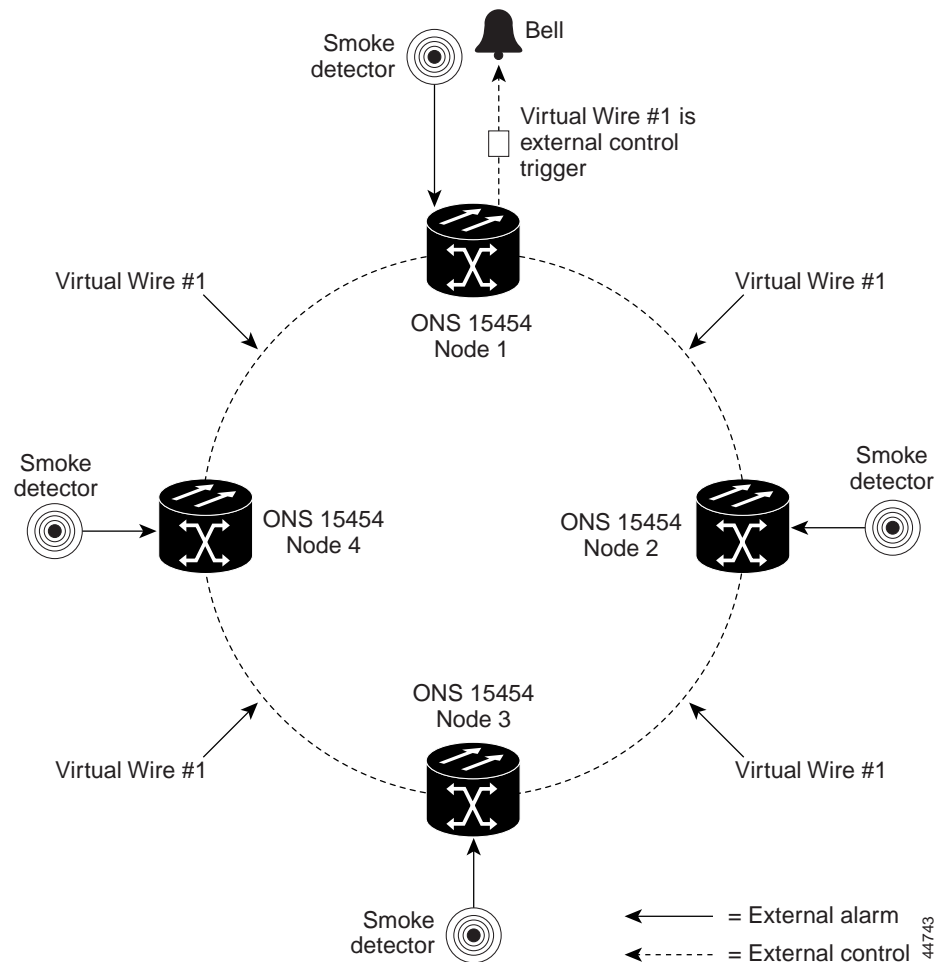
When using AIC virtual wires, you can:

- Assign different external devices to the same virtual wire.
- Assign virtual wires as the trigger type for different external controls.

Procedure: Provision External Alarms

Step 1   Wire the external-device relays to the ENVIR ALARMS IN backplane pins. See the "Alarm, Timing, LAN, and Craft Pin Connections" section on page 1-32 for more information.

Step 2   Log into the node in CTC and display the AIC in card view.

Step 3   Click the **Provisioning > External Alarms** tabs (Figure 7-6 on page 7-28).

Step 4   Complete the following fields for each external device wired to the ONS 15454 backplane:

- *Enabled*—Click to activate the fields for the alarm input number.
- *Alarm Type*—Select an alarm type from the provided list.

Cisco ONS 15454 Installation and Operations Guide

- *Severity*—Select a severity. The severity determines how the alarm is displayed in the CTC Alarms and History tabs and whether the LEDs are activated. Critical, Major, and Minor activate the appropriate LEDs. Not Alarmed and Not Reported do not activate LEDs, but do report the information in CTC.

- *Virtual Wire*—To assign the external device to a virtual wire, select the virtual wire. Otherwise, do not change the None default.

- *Raised When*—Select the contact condition (open or closed) that will trigger the alarm in CTC.

- *Description*—Default descriptions are provided for each alarm type; change the description as necessary.

Figure 7-6   Provisioning external alarms on the AIC card
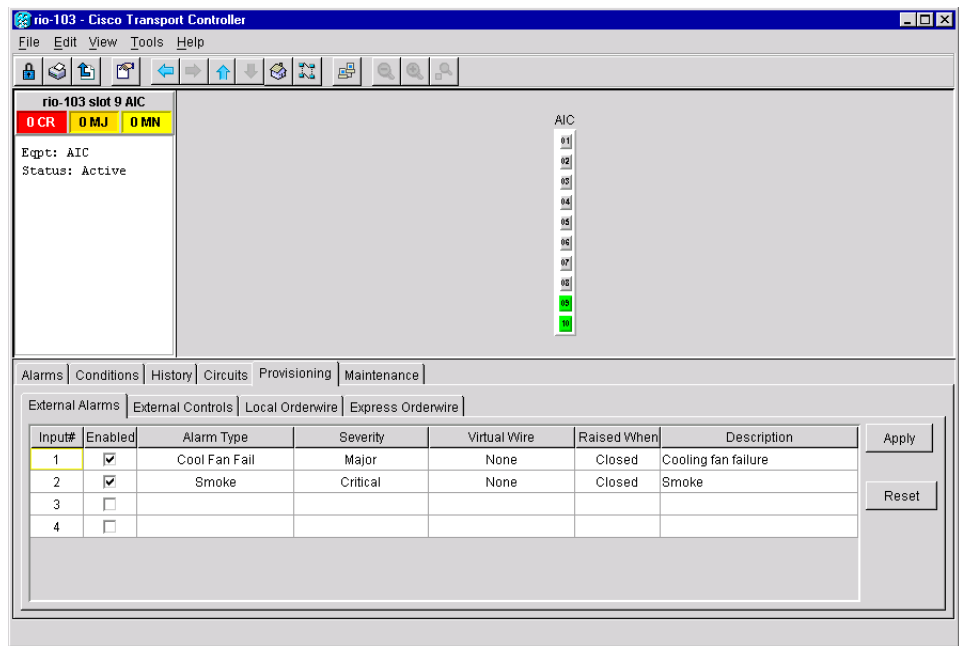
Step 5   To provision additional devices, complete Step 4 for each additional device.

Step 6   Click **Apply**.

Procedure: Provision External Controls

Step 1   Wire the external control relays to the ENVIR ALARMS OUT backplane pins. See the "Alarm, Timing, LAN, and Craft Pin Connections" section on page 1-32 for more information.

Step 2   In CTC, log into the node and display the AIC in card view.

Step 3   On the **External Controls** subtab, complete the following fields for each external control wired to the ONS 15454 backplane:

- *Enabled*—Click to activate the fields for the alarm input number.

- *Trigger Type*—Select a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.

- *Description*—Enter a description.

Step 4   To provision additional controls, complete Step 3 for each additional device.

Step 5   Click **Apply**.

7.5.2 Provisioning AIC Orderwire

The AIC provides RJ-11 jacks to allow onsite personnel to communicate with one another using standard phone sets. The AIC Local and Express orderwire channels are carried on the SONET Orderwire overhead:

- Local orderwire is carried on the SONET Section layer E1 byte. Regenerators between ONS 15454 nodes terminate the channel.

- Express orderwire is carried on the E2 byte of the SONET Line layer.

If regenerators are not used between ONS 15454 nodes, local or express AIC orderwire channels can be used. If regenerators exist, use the Express orderwire channel. You can provision up to four ONS 15454 OC-N ports for each orderwire path.

⚠

Caution   When provisioning orderwire for ONS 15454s 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.

Procedure: Provision AIC Orderwire

🔍

Tip   Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

Step 1   In CTC, open the AIC card view.

Step 2   Select the orderwire subtab, **Local Orderwire** or **Express Orderwire**, appropriate to the orderwire path that you want to create.

The Local Orderwire subtab is shown in Figure 7-7 on page 7-30. Provisioning procedures are the same for both types of orderwire.

Figure 7-7   Provisioning local orderwire
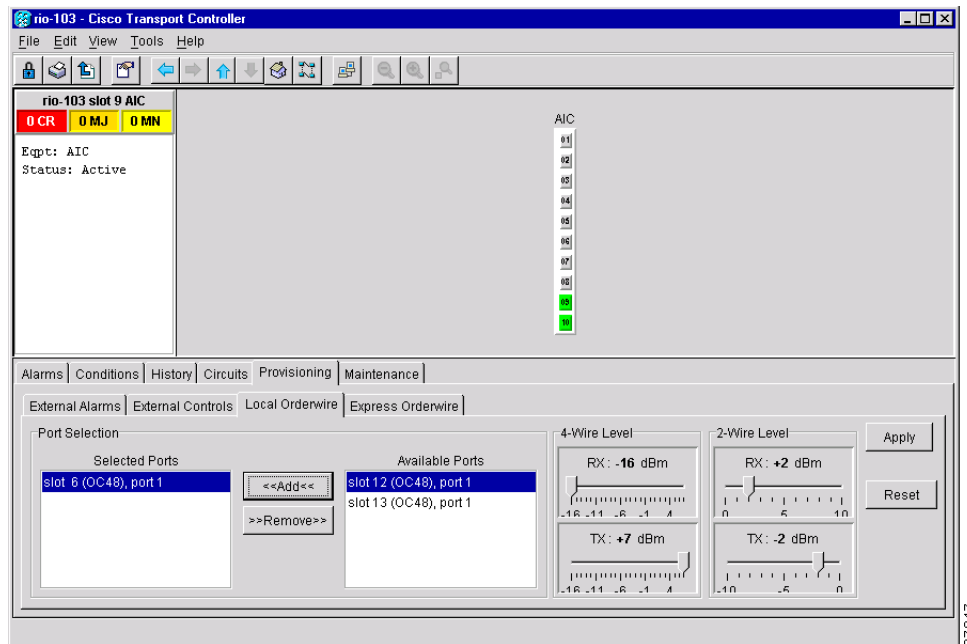
Step 3   In the Available Ports list, select each port that you want to use for the orderwire channel and click **Add** to move them to the Selected Ports column.

Step 4   If needed, adjust the Tx and Rx dBm by moving the slider to the right or left for the headset type (four-wire or two-wire) that you will use. In general, you should not need to adjust the dBm.

Step 5   Click **Apply**.

7.5.3 Using the AIC Orderwire

The AIC orderwire channels function as a party line. Anyone plugging a phone set into an AIC orderwire channel can communicate with all participants on the connected orderwire. The AIC does not provide private, point-to-point connections. To alert participants, press the AIC Call button to activate a buzzer and illuminate the RING LED on AICs at all connected nodes.

7.6 Converting DS-1 and DS-3 Cards From 1:1 to 1:N Protection

The ONS 15454 provides three protection options for DS1-14 and DS3-12 cards: unprotected, 1:1, and 1:N (N=5 or less). Changing protection from 1:1 to 1:N increases the available bandwidth because two of the three cards used for protection in the 1:1 protection group become working cards in the 1:N group.

When setting up 1:N protection, install the DS1N-14 or DS3N-12 card in Slot 3 or 15 on the same side of the ONS 15454 as the cards it protects. Slot 3 protects cards in Slots 1 - 2 and 4 - 6. Slot 15 protects Slots 12 - 14 and 16 - 17. A DS1N-14 or DS3N-12 card installed in Slot 3 or 15 can protect up to five DS1-14 or DS3-12 cards. If you install a DS3N-12 or DS1N-14 card in another slot, it behaves like a normal DS-1 or DS-3 card.

To create 1:1 protection for DS-1 and DS-3 cards, see the "Creating Protection Groups" section on page 3-9.

Procedure: Convert DS1-14 Cards From 1:1 to 1:N Protection

Note   This procedure assumes DS1-14 cards are installed in Slots 1 through 6 and/or Slots 12 through 17. The DS1-14 cards in Slots 3 and 15, which are the protection slots, will be replaced with DS1N-14 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS1N-14 card and a protection group with DS1-14 cards.

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

Step 2   Click the protection group that contains Slot 3 or Slot 15 (where you will install the DS1N-14 card).

Step 3   Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby (shown in Figure 7-8 on page 7-32) and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to switch traffic to the working card:

    a.   Under Selected Group, click the protect card.

    b.   Next to Switch Commands, click **Switch**.

        The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they do not change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

    c.   Next to Switch Commands, select **Clear**.

Cisco ONS 15454 Installation and Operations Guide ■

Figure 7-8   Viewing slot protection status
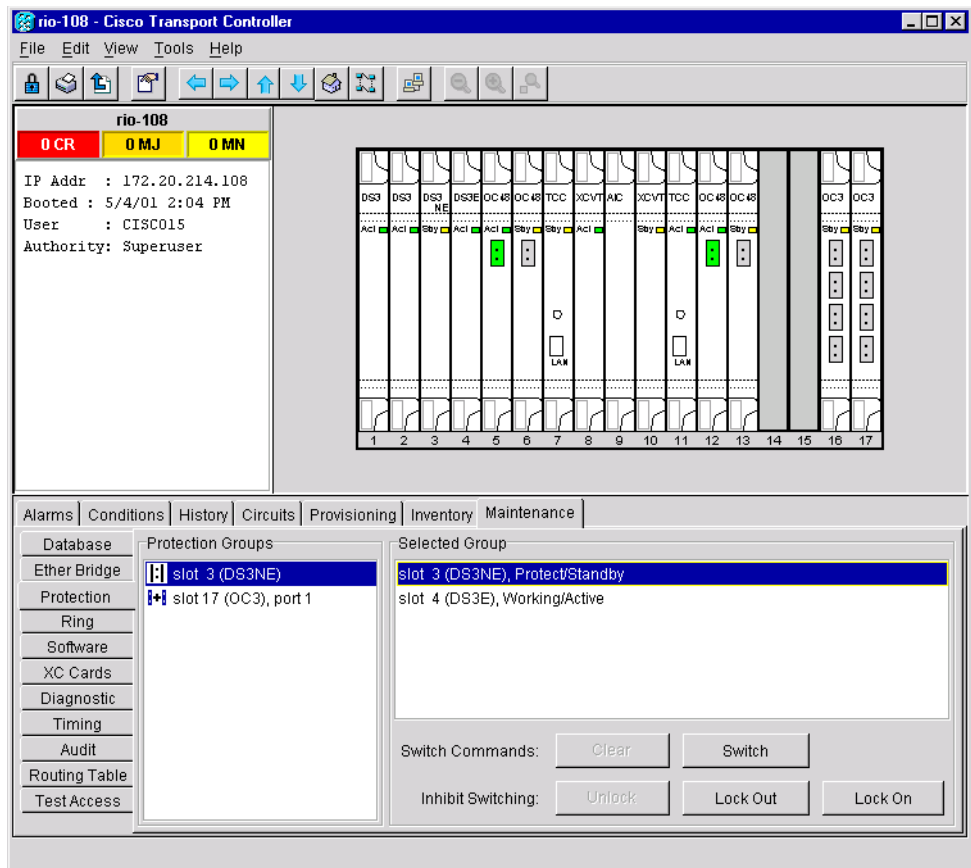
Step 4 Repeat Steps 1 – 3 for each protection group that you need to convert.

Step 5 Verify that no standing alarms exist for any of the DS1-14 cards that you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6 Click the **Provisioning** > **Protection** tabs.

Step 7 Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog displays, click **Yes**.

Note Deleting the 1:1 protection groups does not disrupt service. However, no protection bandwidth exists for the working circuits until you complete the 1:N protection procedure. Therefore, complete this procedure as quickly as possible.

Step 10 If needed, repeat Steps 7– 9 for other protection groups.

Step 11 On the node view, right-click the DS1-14 card in Slot 3 or Slot 15 and select **Delete** from the shortcut menu.

Step 12 Physically remove the DS1-14 card from Slot 3 or Slot 15. This raises an improper removal alarm.

Step 13 In node view, right-click the slot that held the removed card and select delete from the pull-down menu. Wait for the card to disappear from the node view.

Step 14   Physically insert a DS1N-14 card into the same slot.

Step 15   Verify that the card boots up properly.

Step 16   Click the **Inventory** tab and verify that the new card appears as a DS1N-14.

Step 17   Click the **Provisioning** > **Protection** tabs.

Step 18   Click **Create**. The Create Protection Group dialog opens with the protect card in the Protect Card field and the available cards in the Available Cards field.

Step 19   Type a name for the protection group in the Name field (optional).

Step 20   Click **Type** and choose **1:N (card)** from the pull-down menu.

Step 21   Verify that the DS1N-14 card appears in the Protect Card field.

Step 22   Under Available Cards, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 23   Click **OK**. The protection group appears in the Protection Groups list on the Protection subtab.

Procedure: Convert DS3-12 Cards From 1:1 to 1:N Protection

Note   This procedure assumes that DS3-12 cards are installed in Slots 1 - 6 and/or Slots 12 - 17. The DS3-12 cards in Slots 3 and 15, which are the protection slots, will be replaced with DS3N-12 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS3N-12 card and a protection group with DS3-12 cards.

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

Step 2   Click the protection group containing Slot 13 or Slot 15 (where you will install the DS3N-12 card).

Step 3   Make sure the slot you are upgrading is not carrying working traffic. In the Selected Group list, the protect slot must say Protect/Standby as shown in Figure 7-8 on page 7-32, and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to switch traffic to the working card:

   a.   Under Selected Group, click the protect card.

   b.   Next to Switch Commands, click **Switch**.

   The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

   c.   Next to Switch Commands, click **Clear**.

Step 4   Repeat Steps 2 and 3 for each protection group that you need to convert.

Step 5   Verify that no standing alarms exist for any of the DS3-12 cards you are converting. If alarms exist and you have difficulty clearing them, contact your next level of support.

Step 6   Click the **Provisioning** > **Protection** tabs.

Step 7   Click the 1:1 protection group that contains the cards that you will move into the new protection group.

Step 8   Click **Delete**.

Step 9   When the confirmation dialog displays, click **Yes**.

> ✎
> **Note**   Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Do not delay when completing this procedure.

Step 10   If you are deleting more than one protection group, repeat Steps 7–9 for each group.

Step 11   On the node view, right-click the DS3-12 card in Slot 3 or Slot 15 and choose **Delete** from the shortcut menu.

Step 12   Physically remove the DS3-12 card from Slot 3 or Slot 15. This raises an improper removal alarm.

Step 13   In node view, right-click the slot that held the removed card and choose **Delete** from the pull-down menu. Wait for the card to disappear from the node view.

Step 14   Physically insert a DS3N-12 card into the same slot.

Step 15   Verify that the card boots up properly.

Step 16   Click the **Inventory** tab and verify that the new card appears as a DS3N-12.

Step 17   Click the **Provisioning** > **Protection** tabs.

Step 18   Click **Create**.

The Create Protection Group dialog shows the protect card in the Protect Card field and the available cards in the Available Cards field.

Step 19   Type a name for the protection group in the Name field (optional).

Step 20   Click **Type** and choose **1:N (card)** from the pull-down menu.

Step 21   Verify that the DS3N-12 card appears in the Protect Card field.

Step 22   In the Available Cards list, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 23   Click **OK**.

The protection group should appear in the Protection Groups list on the Protection subtab.

CHAPTER

8

Performance Monitoring

Performance monitoring parameters (PMs) are used by service providers to gather, store, threshold, and report performance data for early detection of problems. PM terms are defined for both electrical cards and optical cards.

This chapter provides the:

- "Using the Performance Monitoring Screen" section on page 8-1
- "Changing Thresholds" section on page 8-9
- "Enabling Intermediate-Path Performance Monitoring" section on page 8-10
- "Pointer Justification Count Parameters" section on page 8-12
- "Performance Monitoring for Electrical Cards" section on page 8-14
- "Performance Monitoring for Optical Cards" section on page 8-33

For information about:

- Ethernet PMs, see Chapter 9, "Ethernet Operation"
- Troubleshooting UPSR switch counts, see the alarm troubleshooting information in the *Cisco ONS 15454 Troubleshooting and Reference Guide, Release 3.1*
- Editing UPSR circuits, see Chapter 6, "Circuits and Tunnels."
- Digital transmission surveillance, see Telcordia's GR-1230-CORE, GR-820-CORE, and GR-253-CORE documents and the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*

8.1 Using the Performance Monitoring Screen

The following sections describe how to use basic screen elements such as tabs, menus, and informational columns. Figure 8-1 shows the Performance tab of Cisco Transport Controller (CTC) card-level view.

Figure 8-1   Viewing performance monitoring information

8.1.1 Viewing PMs

Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For information about circuit creation and card provisioning, see the Cisco ONS 15454 Installation and Operations Guide.

Procedure: View PMs

Step 1 Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2 From the card view, click the **Performance** tab.

Step 3 View the PM parameter names that appear on the left portion of the screen in the Param column. The parameter numbers appear on the right portion of the screen in the Curr (current), and Prev (previous) columns.

8.1.2 Changing the Screen Intervals

Changing the screen view allows you to view PMs in 15-minute intervals or 24-hour periods. Figure 8-2 shows the time interval buttons on the Performance Monitoring screen.

Figure 8-2   Time interval buttons on the card view Performance tab

Fifteen-minute and twenty-four hour intervals

Procedure: Select Fifteen-Minute PM Intervals on the Performance Monitoring Screen

Step 1   Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2   From the card view, click the **Performance** tab.

Step 3   Click the **15 min** button.

Step 4   Click the **Refresh** button. Performance monitoring parameters display in 15-minute intervals synchronized with the time of day.

Step 5   View the Current column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) will be raised. The value represents the counter for each specific performance monitoring parameter.

Step 6   View the Prev-N columns to find PM counts for the preceding 15-minute intervals.

Note If a complete 15-minute interval count is not possible, the value displays with a yellow background. An incomplete or incorrect count can be caused by changing node timing settings, changing the time zone settings on CTC, replacing a card, resetting a card, changing port states, or by using the Baseline button. When a complete count occurs, the subsequent 15-minute interval appears with a white background.

Procedure: Select Twenty-Four Hour PM Intervals on the Performance Monitoring Screen

Step 1 Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2 From the card view, click the **Performance** tab.

Step 3 Click the **1 day** button.

Step 4 Click the **Refresh** button. Performance monitoring displays in 24-hour periods synchronized with the time of day.

Step 5 View the Current column to find PM counts for the current 24-hour period.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 24-hour period, a threshold crossing alert (TCA) will be raised. The value represents the counter for each specific performance monitoring parameter.

Step 6 View the Prev columns to find PM counts for the preceding 24-hour period.

Note If a complete count over a 24-hour period is not possible, the value displays with a yellow background. An incomplete or incorrect count can be caused by changing node timing settings, changing the time zone settings on CTC, replacing a card, resetting a card, changing port states, or by using the Baseline button. When a complete count occurs, the subsequent 24-hour period appears with a white background.

8.1.3 Viewing Near End and Far End PMs

Select the Near End or Far End button depending on the PMs you wish to view. Only cards that allow both near-end and far-end monitoring have these buttons as an option. Figure 8-3 on page 8-5 shows the Near End and Far End buttons on the Performance Monitoring screen.

Figure 8-3   Near End and Far End buttons on the card view Performance tab

Near End and Far End buttons

Procedure: Select Near End PMs on the Performance Monitoring Screen

Step 1   Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2   From the card view, click the **Performance** tab.

Step 3   Click the **Near End** button.

Step 4   Click the **Refresh** button. All PMs occurring for the selected card on the incoming signal are displayed.

Procedure: Select Far End PMs on the Performance Monitoring Screen

Step 1   Open the electrical or optical card of choice. To do so, double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2   From the card view, click the **Performance** tab.

Step 3   Click the **Far End** button.

Step 4   Click the **Refresh** button. All PMs recorded by the far-end node for the selected card on the outgoing signal are displayed.

8.1.4 Using the Signal-Type Menu

Use the signal-type menus to monitor PMs for near-end or far-end signals on a selected port. Different signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path, OCn section, line) appear based on the card. For example, the DS3XM has DS3, DS1, VT path, and STS path PMs. Figure 8-4 shows the signal-type menus on the Performance Monitoring screen for a DS3XM-6 card.

Figure 8-4   Signal-type menus for a DS3XM-6 card

Procedure: Select Signal-Type Menus on the Performance Monitoring Screen

Step 1 Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2 From the card view, click the **Performance** tab.

Step 3 Click the signal-type menu. (For example, the DS3XM card has menus labeled DS3, DS1, VT, and STS.)

Step 4 Select a port using the signal-type menu.

8.1.5 Using the Baseline Button

In Software R3.0 and higher, the Baseline button located on the far right of the screen clears the PM count displayed in the Current column, but does not clear the PM count on the card. When the current 15-minute or 24-hour time interval expires or the screen view changes, the total number of PM counts on the card and on the screen appear in the appropriate column.

The baseline values are discarded if you change views to a different screen and then return to the Performance Monitoring screen. The Baseline button enables you to easily see how quickly PM counts are rising without having to perform calculations. Figure 8-5 shows the Baseline button on the Performance Monitoring screen.

Figure 8-5   Baseline button for clearing displayed PM counts

Procedure: Use the Baseline Button on the Performance Monitoring Screen

Step 1 Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2 From the card view, click the **Performance** tab.

Step 3 Click the **Baseline** button.

8.1.6 Using the Clear Button

The Clear button located on the far right of the Performance Monitoring screen clears certain PM counts depending on the option selected. Figure 8-6 shows the Clear button on the Performance Monitoring screen.

⚠

Caution Pressing the Clear button can potentially mask problems if used incorrectly. This button is commonly used for testing purposes.

Figure 8-6   Clear button for clearing PM counts

Procedure: Use the Clear Button on the Performance Monitoring Screen

Step 1 Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2 From the card view, click the **Performance** tab.

Step 3 Click the **Clear** button.

Step 4 From the Clear Statistics menu, choose one of three options:

- **Selected Interfaces**: Clearing selected interfaces erases all PM counts associated with the selected radio buttons. For example, if the 15 min and the Near End buttons are selected and you click the Clear button, all near-end PM counts in the current 15-minute interval are erased from the card and the screen display.

- **All interfaces on port x**: Clearing all interfaces on port x erases from the card and the screen display all PM counts associated with all combinations of the radio buttons on the selected port. This means the 15-minute near-end and far-end counts are cleared, and 24-hour near-end and far-end counts are cleared from the card and the screen display.

- **All interfaces on card**: Clearing all interfaces on the card erases from the card and the screen display all PM counts for data and ports on all interfaces.

Step 5   From the Zero Data menu, click **Yes** to clear the selected statistics.

Note   The Ethernet cards are the only cards without the **Clear** button option.

8.2 Changing Thresholds

Thresholds are used to set error levels for each PM. You can program PM threshold ranges from the Provisioning > Threshold tabs on the card view. For procedures on provisioning card thresholds, such as line, path, and SONET thresholds, see Chapter 7, "Card Provisioning."

During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and sent to CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the performance monitoring parameter is disabled. Figure 8-7 shows the Provisioning > Threshold tabs for an OC-48 card.

Figure 8-7   Threshold tab for setting threshold values
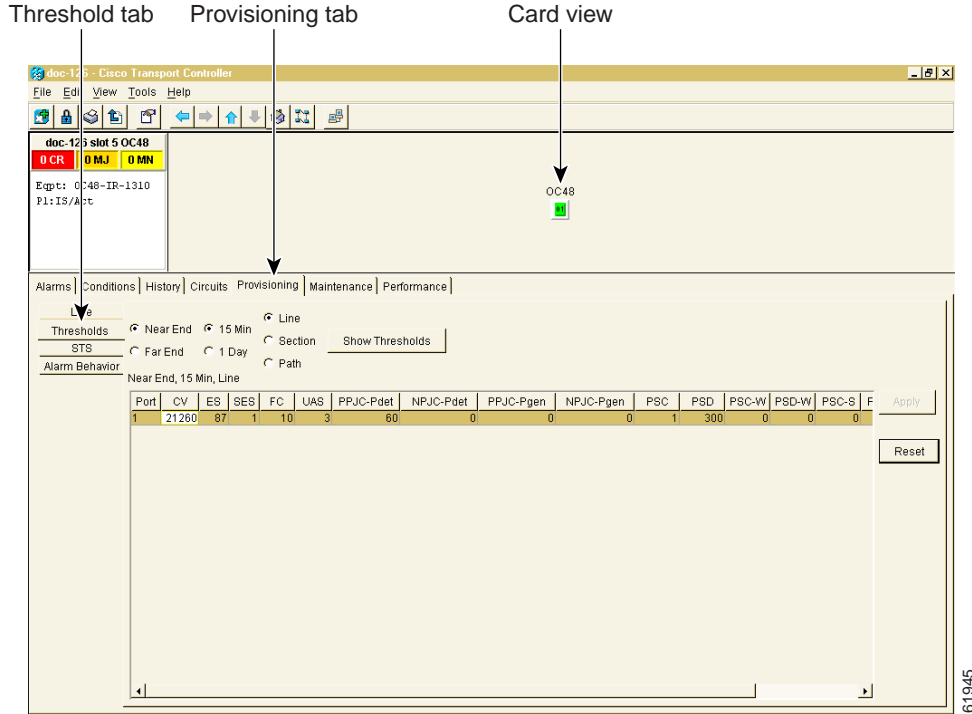
Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical DS1 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

8.3 Enabling Intermediate-Path Performance Monitoring

Intermediate-path performance monitoring (IPPM) allows transparent monitoring of a constituent channel of an incoming transmission signal by a node that does not terminate that channel. Many large ONS 15454 networks only use line terminating equipment (LTE) not path terminating equipment (PTE). Table 8-1 shows ONS 15454 cards that are considered LTEs. Figure 8-8 shows the Provisioning > STS tabs for an OC-3 card.

Table 8-1   Traffic Cards That Terminate the Line, Called LTEs

Line Terminating Equipment	
EC1-12	OC3 IR 4/STM1 SH 1310
OC12 IR/STM4 SH 1310	OC12 LR/STM4 LH 1310
OC12 LR/STM4 LH 1550	OC48 IR 1310
OC48 LR 1550	OC48 IR/STM16 SH AS 1310
OC48 LR/STM16 LH AS 1550	OC48 ELR/STM16 EH 100 GHz
OC48 ELR/STM16 EH 200 GHz	OC192 LR/STM64 LH 1550

Figure 8-8   STS tab for enabling IPPM
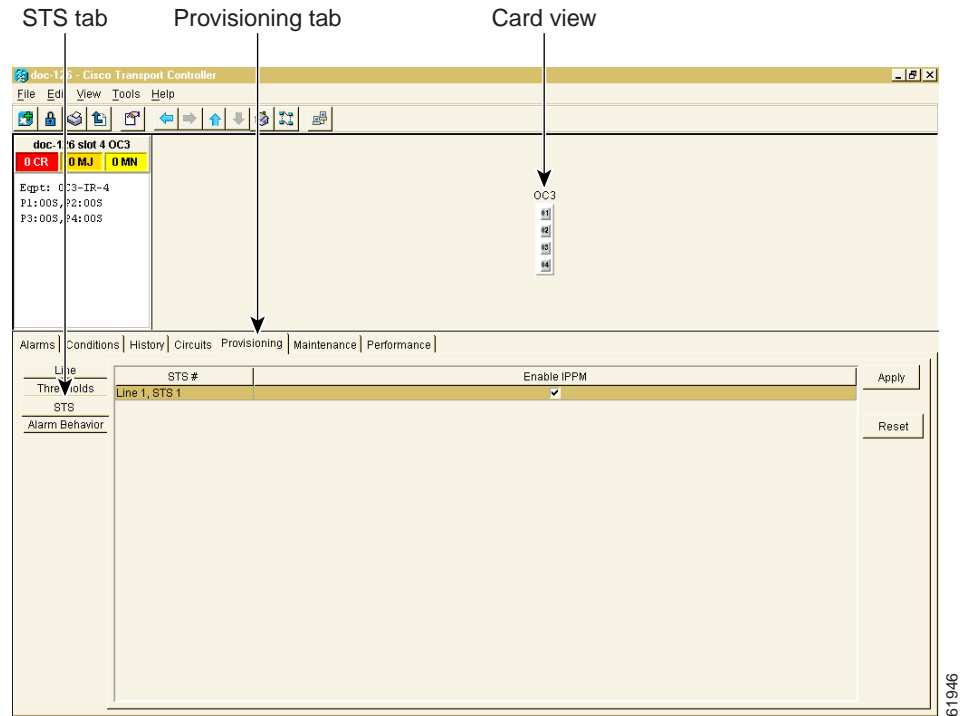
Software R3.0 and higher allows LTE cards to monitor near-end PM data on individual STS payloads by enabling IPPM. After enabling IPPM provisioning on the line card, service providers can monitor large amounts of STS traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on STS paths which have IPPM enabled, and TCAs are raised only for PM parameters on the selected IPPM paths. The monitored IPPMs are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. For detailed information about provisioning cards and the procedure for enabling IPPM, see Chapter 7, "Card Provisioning."

> **Note**   The far-end IPPM feature is not supported in Software R3.1. However, SONET path PMs can be monitored by logging into the far-end node directly.

The ONS 15454 performs IPPM by examining the overhead in the monitored path and by reading all of the near-end path PMs in the incoming direction of transmission. The IPPM process allows the path signal to pass bidirectionally through the node completely unaltered.

For detailed information about specific PMs, locate the card name in the following sections and review the appropriate definition.

8.4 Pointer Justification Count Parameters

Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks. There are positive (PPJC) and negative (NPJC) pointer justification count parameters. PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications depending on the specific PM name.

Figure 8-9 shows pointer justification count parameters on the Performance Monitoring screen. You can enable PPJC and NPJC performance monitoring parameters for LTE cards. See Table 8-1 on page 8-10 for a list of Cisco ONS 15454 LTE cards.

For pointer justification count definitions, see the "EC1 Card Performance Monitoring Parameters" section on page 8-14, the "OC-3 Card Performance Monitoring Parameters" section on page 8-33, or the "OC-12, OC-48, and OC-192 Card Performance Monitoring Parameters" section on page 8-37 depending on the cards in use.

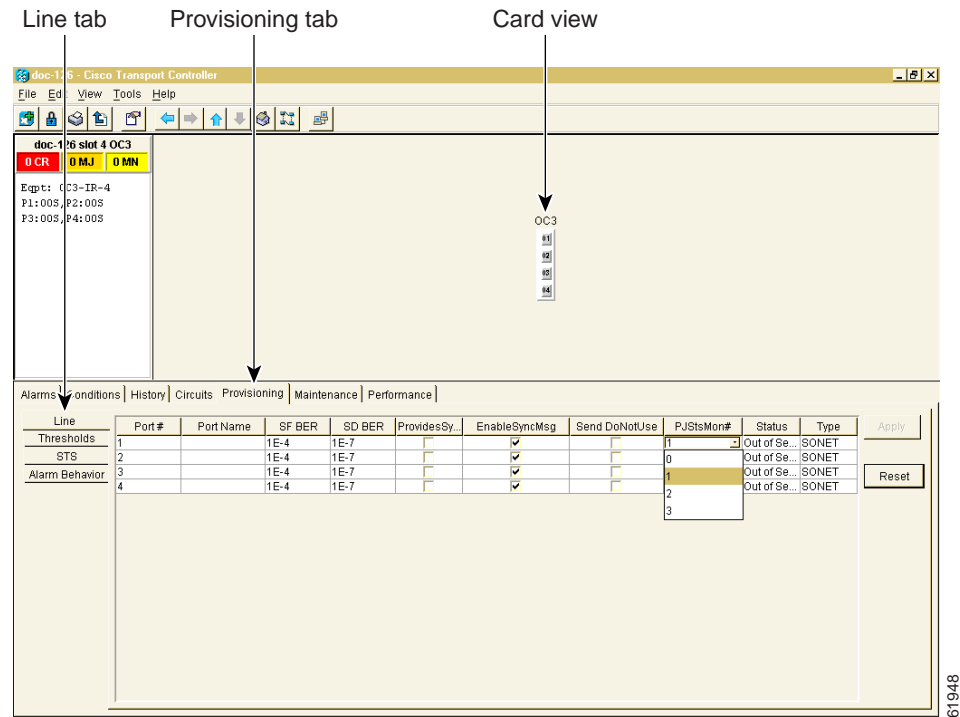*Figure 8-9   Viewing pointer justification count parameters*
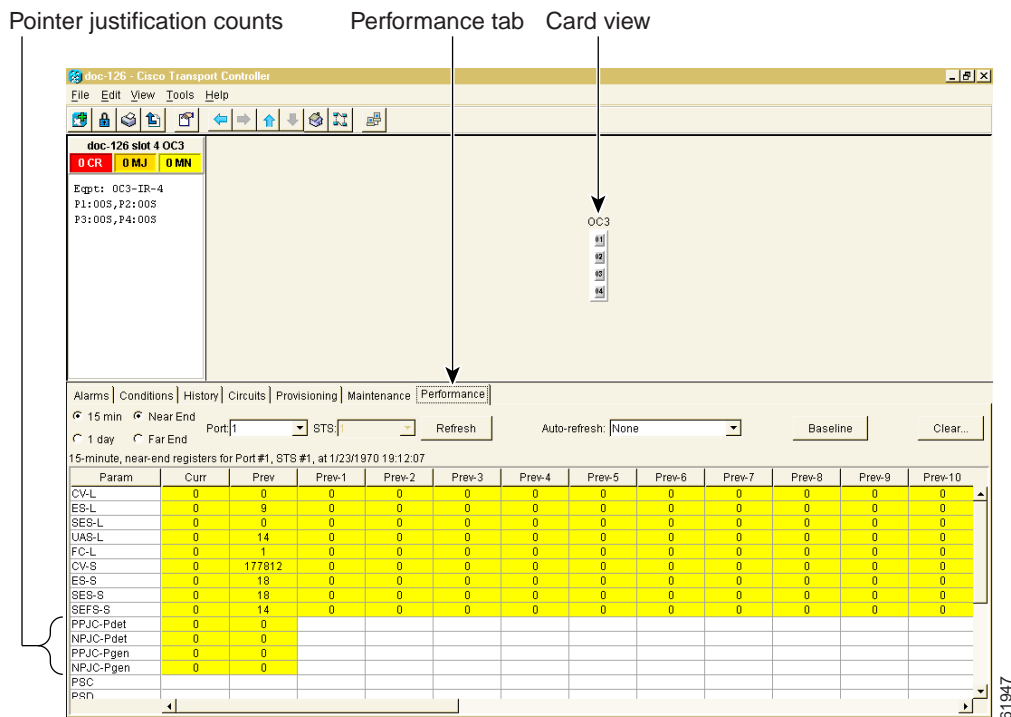
Pointers provide a way to align the phase variations in STS and VT payloads. The STS payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the STS synchronous payload envelope (SPE) called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

A consistent pointer justification count indicates clock synchronization problems between nodes. Detected and generated counts should be equal. A difference between the counts means the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count. Positive pointer adjustments occur when the frame rate of the SPE is too slow in relation to the rate of the STS 1.

On CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. Figure 8-10 shows the PJStsMon# menu on the Provisioning screen.

Figure 8-10   Line tab for enabling pointer justification count parameters

Procedure: Enable Pointer Justification Count Performance Monitoring

Step 1   Open the electrical or optical card of choice. Double-click the card's graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)

Step 2   From the card view, click the **Provisioning > Line** tabs.

Step 3   Click the **PJStsMon#** menu and select a number.

- The value of 0 means pointer justification monitoring is disabled.

- The values 1-N are the STS numbers on one port. One STS per port can be enabled from the **PJStsMon#** menu.

  EC1 PJStsMon# card menu: 0 or 1 can be selected on a total of 12 ports.

  OC-3 PJStsMon# card menu: 1, 2, or 3 can be selected on a total of 4 ports.

  OC-12 PJStsMon# card menu: 1 or any number through 12 can be selected on 1 port.

  OC-48 PJStsMon# card menu: 1 or any number through 48 can be selected on 1 port.

  OC-192 PJStsMon# card menu: 1 or any number through 192 can be selected on 1 port.

Step 4   Click **Apply** and return to the **Performance** tab to view PM parameters.

8.5 Performance Monitoring for Electrical Cards

The following sections define performance monitoring parameters for the EC1, DS1, DS1N, DS3, DS3N, DS3-12E, DS3N-12E, and DS3XM electrical cards.

8.5.1 EC1 Card Performance Monitoring Parameters

Figure 8-11 shows signal types that support far-end PMs. Far-end performance monitoring is not reported for EC1. Figure 8-12 shows where overhead bytes detected on the application specific integrated circuits (ASICs) produce performance monitoring parameters for the EC1 card.

Figure 8-11   Monitored signal types for the EC1 card
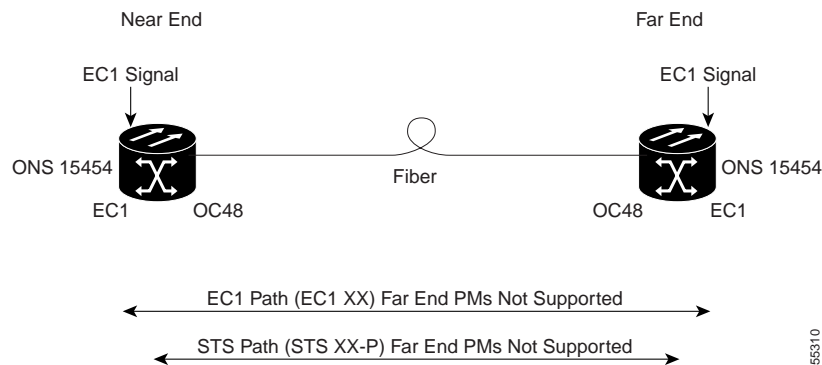
> **Note**   The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-12   PM read points on the EC1 card
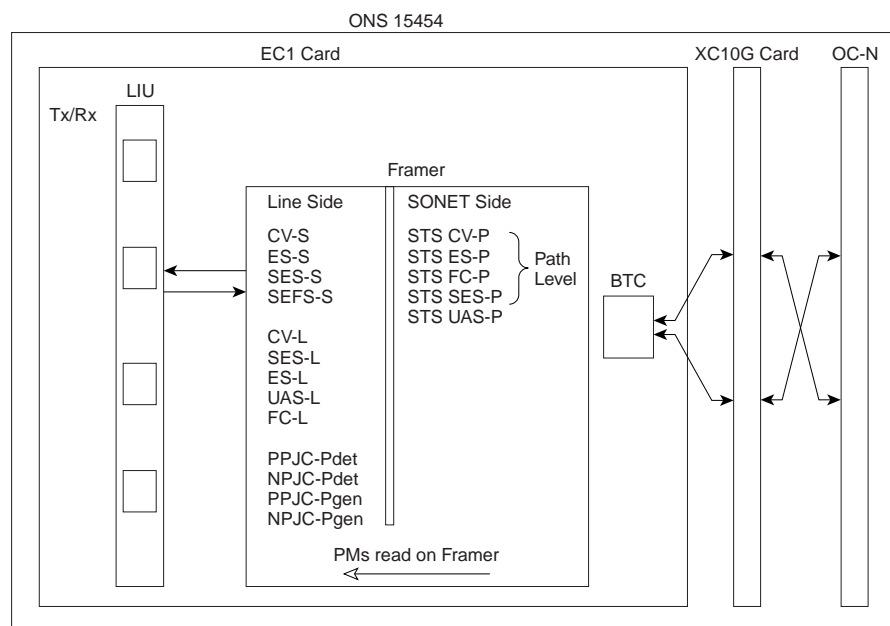
Note   SONET path PMs will not count unless IPPM is enabled. For additional information, see the "Enable Intermediate-Path Performance Monitoring" procedure on page 7-25. The far-end IPPM feature is not supported in Software R3.1. However, SONET path PMs can be monitored by logging into the far-end node directly.

Table 8-2   Near-End Section PMs for the EC1 Card

Parameter	Definition
CV-S	Section Coding Violation (CV-S) is a count of BIP errors detected at the section-layer (i.e. using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.
ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or loss of signal (LOS) defect was present.
SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see GR-253-CORE for value) or more section-layer BIP errors were detected or a severely errored frame (SEF) or LOS defect was present.
SEFS-S	Section Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected during most seconds where an LOS or loss of frame (LOF) defect is present. However, there may be situations when that is not the case, and the SEFS-S parameter is only incremented based on the presence of the SEF defect.

Table 8-3   Near-End Line Layer PMs for the EC1 Card

Parameter	Definition
CV-L	Near-End Line Code Violation (CV-L) is a count of BIP errors detected at the line-layer (i.e. using the B2 bytes in the incoming SONET signal). Up to 8 x N BIP errors can be detected per STS-N frame, with each error incrementing the current CV-L second register.
ES-L	Near-End Line Errored Seconds (ES-L) is a count of the seconds when at least one line-layer BIP error was detected or an alarm indication signal-line (AIS-L) defect was present.
SES-L	Near-End Line Severely Errored Seconds (SES-L) is a count of the seconds when K (see GR-253 for values) or more line-layer BIP errors were detected or an AIS-L defect was present.

Table 8-3   Near-End Line Layer PMs for the EC1 Card (continued)

Parameter	Definition
UAS-L	Near-End Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and the line continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls.
FC-L	Near-End Line Failure Count (FC-L) is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure or a lower-layer, traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.

Table 8-4   Near-End SONET Path PMs for the EC1 Card

Parameter	Definition
Note	SONET path PMs will not count unless IPPM is enabled. For additional information, see the "Enable Intermediate-Path Performance Monitoring" procedure on page 7-25. The far-end IPPM feature is not supported in Software R3.1. However, SONET path PMs can be monitored by logging into the far-end node directly.
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. STS ES-P can also be caused by an AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a unequipped path (UNEQ-P) or a trace identifier mismatch (TIM-P) failure is declared. A failure event also begins if the STS PTE monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. STS SES-P can also be caused by an AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

Table 8-5   Near-End SONET Path BIP PMs for the EC1 Card

Parameter	Definition
PPJC-Pdet	Positive Pointer Justification Count, STS Path Detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path in an incoming SONET signal.
NPJC-Pdet	Negative Pointer Justification Count, STS Path Detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path in an incoming SONET signal.
PPJC-Pgen	Positive Pointer Justification Count, STS Path Generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	Negative Pointer Justification Count, STS Path Generated (NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the synchronous payload envelope (SPE) with the local clock.

Table 8-6   Far-End Line Layer PMs for the EC-1 Card

Parameter	Definition
CV-L	Far-End Line Code Violation (CV-L) is a count of BIP errors detected by the far-end line terminating equipment (LTE) and reported back to the near-end LTE using the REI-L indication in the line overhead. For SONET signals at rates below OC-48, up to 8 x N BIP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 BIP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each BIP error indicated by the incoming REI-L.
ES-L	Far-End Line Errored Seconds (ES-L) is a count of the seconds when at least one line-layer BIP error was reported by the far-end LTE or an RDI-L defect was present.
SES-L	Far-End Line Severely Errored Seconds (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer BIP errors were reported by the far-end LTE or an RDI-L defect was present.
UAS-L	Far-End Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable at the far end. A line becomes unavailable at the far end when ten consecutive seconds occur that qualify as SES-LFEs and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-LFEs.
FC-L	Far-End Line Failure Count (FC-L) is a count of the number of far-end line failure events. A failure event begins when RFI-L failure is declared, and it ends when the RFI-L failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

8.5.2 DS1 and DS1N Card Performance Monitoring Parameters

Figure 8-13 shows the signal types that support far-end PMs. Far-end VT and STS path performance monitoring is supported for the DS1 card. Far-end DS1 path performance monitoring is not supported for the DS1 card. Figure 8-14 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS1 and DS1N cards.

Figure 8-13   Monitored signal types for the DS1 and DS1N cards
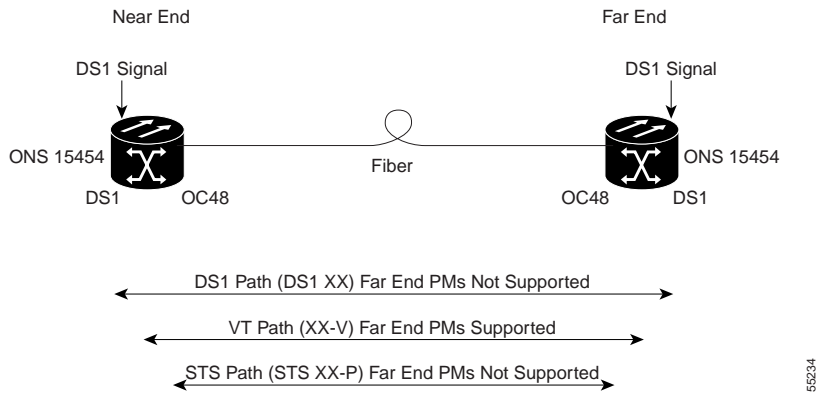
Note   The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-14   PM read points on the DS1 and DS1N cards
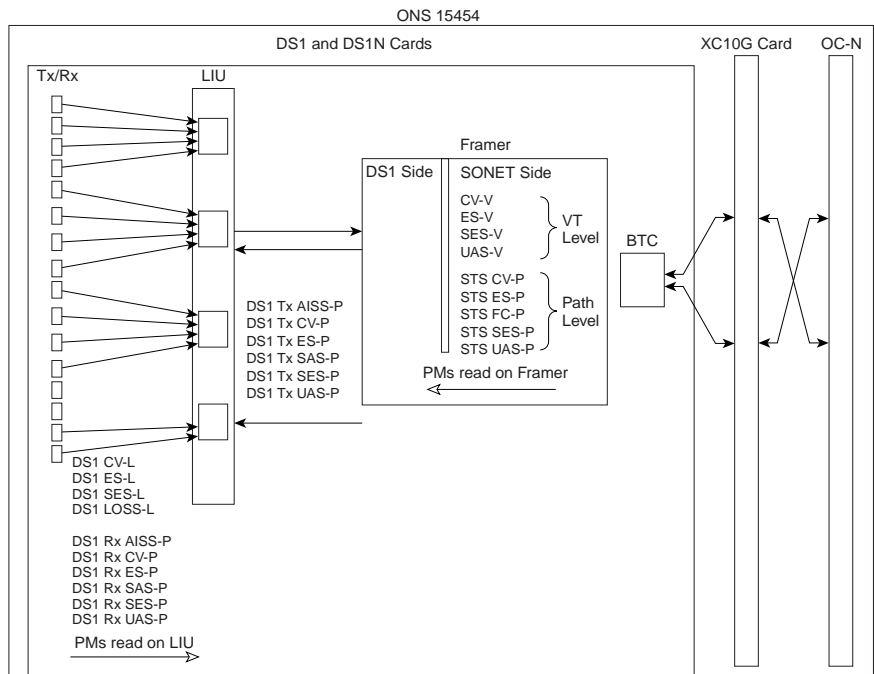
Table 8-7   DS1 Line PMs for the DS1 and DS1N Cards

Parameter	Definition
DS1 CV-L	Code Violation Line (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
DS1 ES-L	Errored Seconds Line (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (loss of signal) on the line.
DS1 SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 1544) and/or defects on the line.
DS1 LOSS-L	Loss of Signal Seconds Line (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Table 8-8   DS1 Receive Path PMs for the DS1 and DS1N Cards

Parameter	Definition
DS1 Rx AISS-P	Receive Path Alarm Indication Signal (Rx AIS-P) means an alarm indication signal occurred on the receive end of the path. This parameter is a count of seconds containing one or more AIS defects.
DS1 Rx CV-P	Receive Path Code Violation (Rx CV-P) means a coding violation occurred on the receive end of the path. For DS1-ESF paths, this parameter is a count of detected CRC-6 errors. For the DS1-SF paths, the Rx CV-P parameter is a count of detected frame bit errors (FE).
DS1 Rx ES-P	Receive Path Errored Seconds (Rx ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths on the receive end of the signal. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more SEF or AIS defects. For DS1-SF paths, the Rx ES-P parameter is a count of one-second intervals containing one or more FE events, or one or more CS events, or one or more SEF or AIS defects.
DS1 Rx SAS-P	Receive Path Severely Errored Seconds Frame/Alarm Indication Signal (Rx SAS-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the receive end of the signal.
DS1 Rx SES-P	Receive Path Severely Errored Seconds (Rx SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths on the receive end of the signal. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more SEF or AIS defects occurred. For DS1-SF paths, an SES is a second containing either the occurrence of four FEs or one or more SEF or AIS defects.
DS1 Rx UAS-P	Receive Path Unavailable Seconds (Rx UAS-P) is a count of one-second intervals when the DS1 path is unavailable on the receive end of the signal. The DS1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. Once unavailable, the DS1 path becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time.

Cisco ONS 15454 Installation and Operations Guide

Table 8-9   DS1 Transmit Path PMs for the DS1 and DS1N Cards

Parameter	Definition
DS1 Tx AISS-P	Transmit Path Alarm Indication Signal (Tx AIS-P) means an alarm indication signal occurred on the transmit end of the path. This parameter is a count of seconds containing one or more AIS defects.
DS1 Tx CV-P	Transmit Path Code Violation (Tx CV-P) means a coding violation occurred on the transmit end of the path. For DS1-ESF paths, this parameter is a count of detected CRC-6 errors. For the DS1-SF paths, the Tx CV-P parameter is a count of detected FEs.
DS1 Tx ES-P	Transmit Path Errored Seconds (Tx ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths on the transmit end of the signal. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more SEF or AIS defects. For DS1-SF paths, the Tx ES-P parameter is a count of one-second intervals containing one or more FE events, or one or more CS events, or one or more SEF or AIS defects.
DS1 Tx SAS-P	Transmit Path Severely Errored Seconds Frame/Alarm Indication Signal (Tx SAS-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the receive end of the signal.
DS1 Tx SES-P	Transmit Path Severely Errored Seconds (Tx SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths on the transmit end of the signal. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more SEF or AIS defects occurred. For DS1-SF paths, an SES is a second containing either the occurrence of four FEs or one or more SEF or AIS defects.
DS1 Tx UAS-P	Transmit Path Unavailable Seconds (Tx UAS-P) is a count of one-second intervals when the DS1 path is unavailable on the transmit end of the signal. The DS1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. Once unavailable, the DS1 path becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time.

Table 8-10   VT Path PMs for the DS1 and DS1N Cards

Parameter	Definition
CV-V	Code Violation VT Layer (CV-V) is a count of the BIP errors detected at the VT path layer. Up to two BIP errors can be detected per VT superframe, with each error incrementing the current CV-V second register.
ES-V	Errored Seconds VT Layer (ES-V) is a count of the seconds when at least one VT Path BIP error was detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause an ES-V.

Table 8-10   VT Path PMs for the DS1 and DS1N Cards (continued)

Parameter	Definition
SES-V	Severely Errored Seconds VT Layer (SES-V) is a count of seconds when K (600) or more VT Path BIP errors were detected. SES-V can also be caused by an AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect.
UAS-V	Unavailable Second VT Layer (UAS-V) is a count of the seconds when the VT path was unavailable. A VT path becomes unavailable when ten consecutive seconds occur that qualify as SES-Vs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Vs.

Table 8-11   SONET Path PMs for the DS1 and DS1N Cards

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame, with each error incrementing the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

Table 8-12   Far-End VT Path PMs for the DS1 Card

Parameter	Definition
CV-V	Far-End VT Path Coding Violations (CV-VFE) is a count of the number of BIP errors detected by the far-end VT path terminating equipment (PTE) and reported back to the near-end VT PTE using the REI-V indication in the VT path overhead. Only one BIP error can be indicated per VT superframe using the REI-V bit. The current CV-VFE second register is incremented for each BIP error indicated by the incoming REI-V.
ES-V	Far-End VT Path Errored Seconds (ES-VFE) is a count of the seconds when at least one VT path BIP error was reported by the far-end VT PTE, or a one-bit RDI-V defect was present.
SES-V	Far-End VT Path Severely Errored Seconds (SES-VFE) is a count of the seconds when K (600) or more VT path BIP errors were reported by the far-end VT PTE or a one-bit RDI-V defect was present.
UAS-V	Far-End VT Path Unavailable Seconds (UAS-VFE) is a count of the seconds when the VT path is unavailable at the far-end. A VT path is unavailable at the far-end when ten consecutive seconds occur that qualify as SES-VFEs.

8.5.3 DS3 and DS3N Card Performance Monitoring Parameters

Figure 8-15 shows the signal types that support far-end PMs. Figure 8-16 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3 and DS3N cards.

Figure 8-15   Monitored signal types for the DS3 and DS3N cards
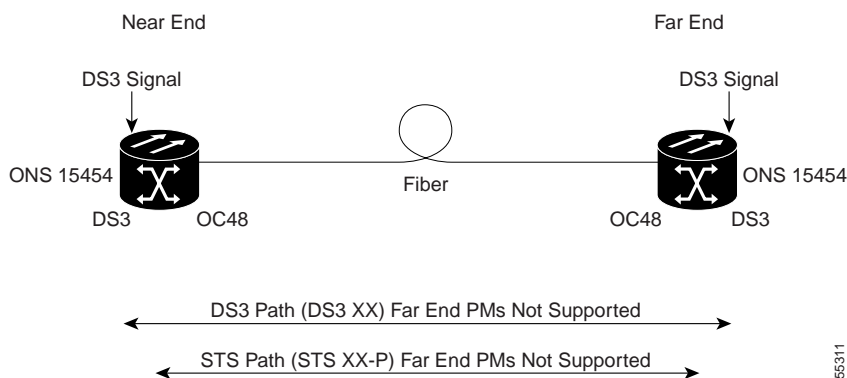
Note   The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.
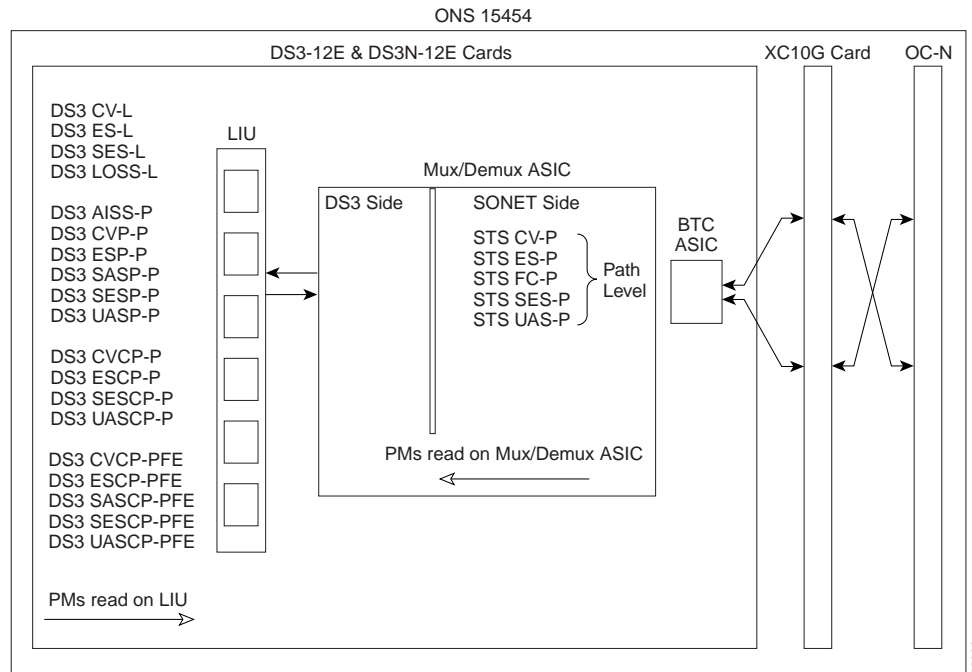
Figure 8-16   PM read points on the DS3 and DS3N cards
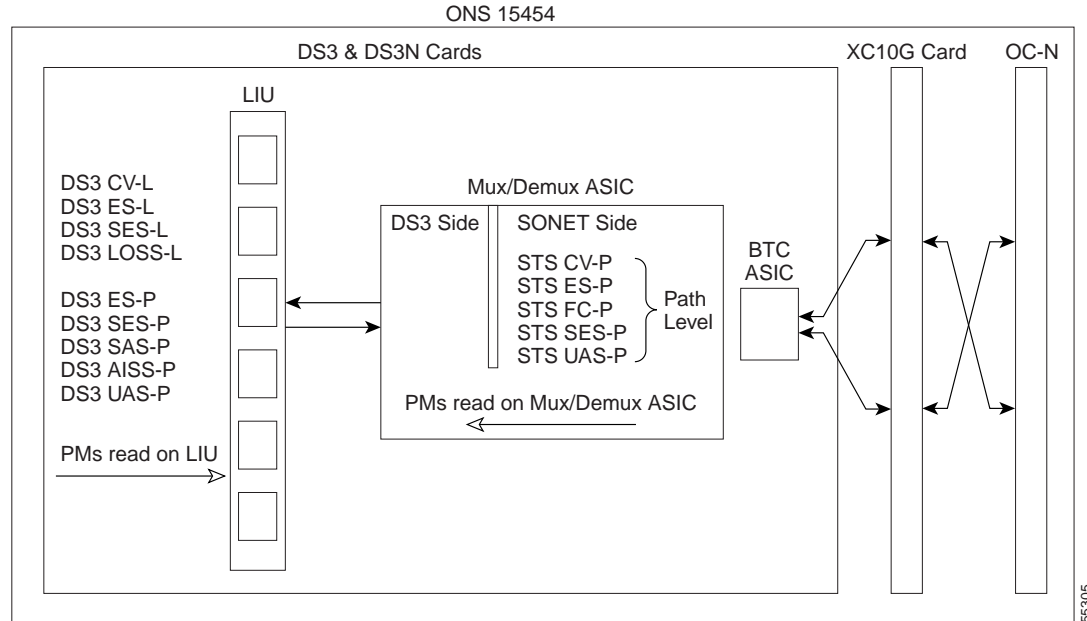
Table 8-13   Near-End DS3 Line PMs for the DS3 and DS3N Cards

Parameter	Definition
DS3 CV-L	Code Violation Line (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
DS3 ES-L	Errored Seconds Line (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (loss of signal) on the line.
DS3 SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
DS3 LOSS-L	Line Loss of Signal (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Table 8-14   Near-End DS3 Path PMs for the DS3 and DS3N Cards

Parameter	Definition
DS3 ES-P	Errored Seconds-Path (ES-P) is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more SEF or AIS defects.
DS3 SES-P	Severely Errored Seconds-Path (SES-P) is a count of seconds where 320 or more CRC-6 errors occur or one or more SEF or AIS defects occur.
DS3 SAS-P	Severely Errored Frame/Alarm Indication Signal-Path (SAS-P) is a count of seconds containing one or more SEFs or one or more AIS defects.

Cisco ONS 15454 Installation and Operations Guide

Table 8-14   Near-End DS3 Path PMs for the DS3 and DS3N Cards (continued)

Parameter	Definition
DS3 AISS-P	Alarm Indication Signal Seconds-Path (AISS-P) is a count of seconds containing one or more AIS defects.
DS3 UAS-P	Unavailable Seconds-Path (UAS-P) is a count of one-second intervals during which the DS3 path is unavailable.

Table 8-15   Near-End SONET Path PMs for the DS3 and DS3N Cards

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

8.5.4 DS3-12E and DS3N-12E Card Performance Monitoring Parameters

Figure 8-17 shows the signal types that support far-end PMs. Figure 8-18 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3-12E and DS3N-12E cards.

Figure 8-17   Monitored signal types for the DS3-12E and DS3N-12E cards
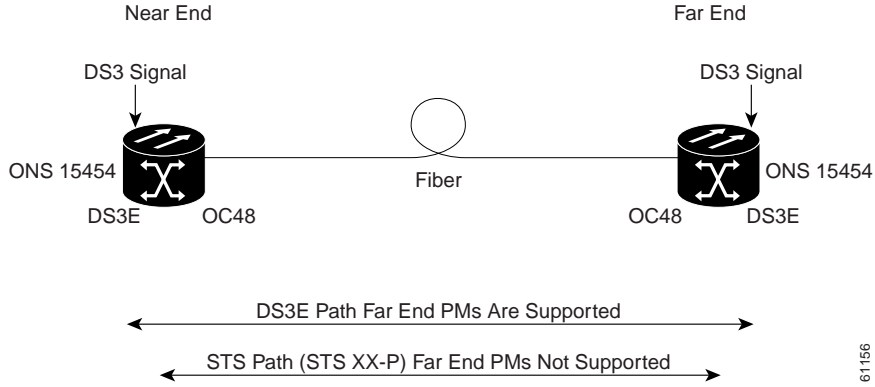
Note   The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-18   PM read points on the DS3-12E and DS3N-12E cards

Table 8-16   Near-End DS3 Line PMs for the DS3-12E and DS3N-12E Cards

Parameter	Definition
DS3 CV-L	Code Violation Line (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
DS3 ES-L	Errored Seconds Line (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (i.e. loss of signal) on the line.
DS3 SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
DS3 LOSS-L	Line Loss of Signal (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Table 8-17   Near-End DS3 Path PMs for the DS3-12E and DS3N-12E Cards

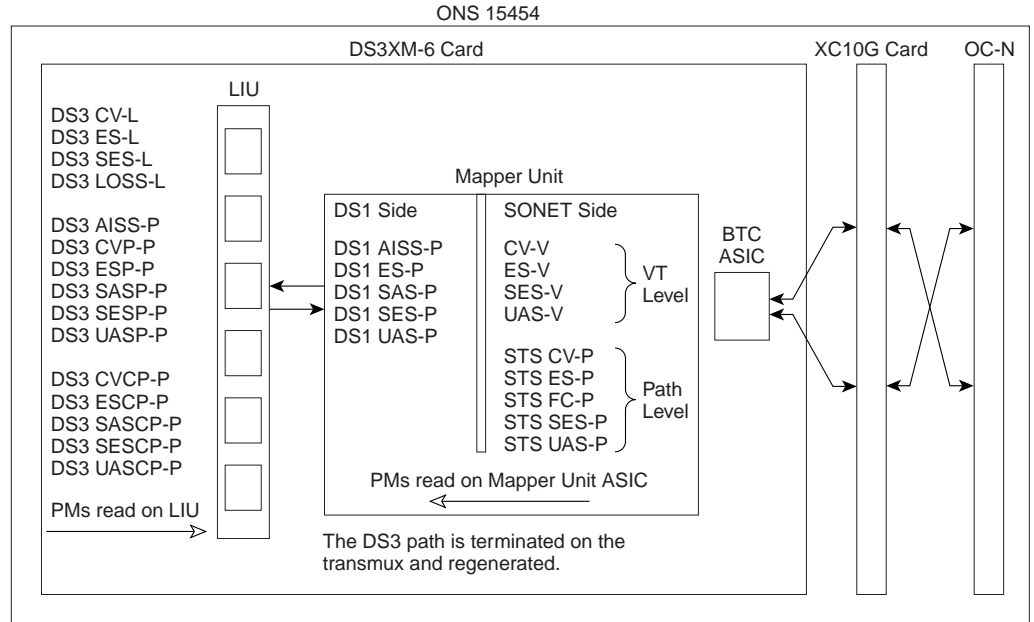| Parameter	Definition
DS3 AISS-P	AIS Seconds Path (AISS-P) is a count of one-second intervals containing one or more AIS defects.
DS3 CVP-P	Code Violation Path (CVP-P) is a code violation parameter for M23 applications. CVP-P is a count of P-bit parity errors occurring in the accumulation period.
DS3 ESP-P	Errored Second Path (ESP-P) is a count of seconds containing one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
DS3 SASP-P	SEF/AIS Seconds Path (SASP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
DS3 SESP-P	Severely Errored Seconds Path (DS3 SESP-P) is a count of seconds containing more than 44 P-bit parity violations, one or more SEF defects, or one or more AIS defects.
DS3 UASP-P	Unavailable Second Path (DS3 UASP-P) is a count of one-second intervals when the DS3 path is unavailable. A DS3 path becomes unavailable when ten consecutive SESP-Ps occur. The ten SESP-Ps are included in unavailable time. Once unavailable, the DS3 path becomes available when ten consecutive seconds with no SESP-Ps occur. The ten seconds with no SESP-Ps are excluded from unavailable time.

Table 8-18   Near-End CP-bit Path PMs for the DS3-12E and DS3N-12E Cards

Parameter	Definition
DS3 CVCP-P	Code Violation Path (CVCP-P) is a count of CP-bit parity errors occurring in the accumulation period.
DS3 ESCP-P	Errored Second Path (ESCP-P) is a count of seconds containing one or more CP-bit parity errors, one or more SEF defects, or one or more AIS defects. ESCP-P is defined for the C-bit parity application.

Table 8-18   Near-End CP-bit Path PMs for the DS3-12E and DS3N-12E Cards (continued)

Parameter	Definition
DS3 SESCP-P	Severely Errored Seconds Path (SESCP-P) is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
DS3 UASCP-P	Unavailable Second Path (UASCP-P) is a count of one-second intervals when the DS3 path is unavailable. A DS3 path becomes unavailable when ten consecutive SESCP-Ps occur. The ten SESCP-Ps are included in unavailable time. Once unavailable, the DS3 path becomes available when ten consecutive seconds with no SESCP-Ps occur. The ten seconds with no SESCP-Ps are excluded from unavailable time.

Table 8-19   Near-End SONET Path PMs for the DS3-12E and DS3N-12E Cards

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

Table 8-20   Far-End CP-bit Path PMs for the DS3-12E and DS3N-12E Cards

Parameter	Definition
DS3 CVCP-P	Code Violation (CVCP-PFE) is a parameter that is counted when the three far-end block error (FEBE) bits in a M-frame are not all collectively set to 1.
DS3 ESCP-P	Errored Second (ESCP-PFE) is a count of one-second intervals containing one or more M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
DS3 SASCP-P	SEF/AIS Second (SASCP-PFE) is a count of one-second intervals containing one or more far-end SEF/AIS defects.
DS3 SESCP-P	Severely Errored Second (SESCP-PFE) is a count of one-second intervals containing one or more 44 M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
DS3 UASCP-P	Unavailable Second (UASCP-PFE) is a count of one-second intervals when the DS3 path becomes unavailable. A DS3 path becomes unavailable when ten consecutive far-end CP-bit SESs occur. The ten CP-bit SESs are included in unavailable time. Once unavailable, the DS3 path becomes available when ten consecutive seconds occur with no CP-bit SESs. The ten seconds with no CP-bit SESs are excluded from unavailable time.

8.5.5 DS3XM-6 Card Performance Monitoring Parameters

Figure 8-19 shows the signal types that support far-end PMs. Figure 8-20 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3XM-6 card.

Figure 8-19   Monitored signal types for the DS3XM-6 card
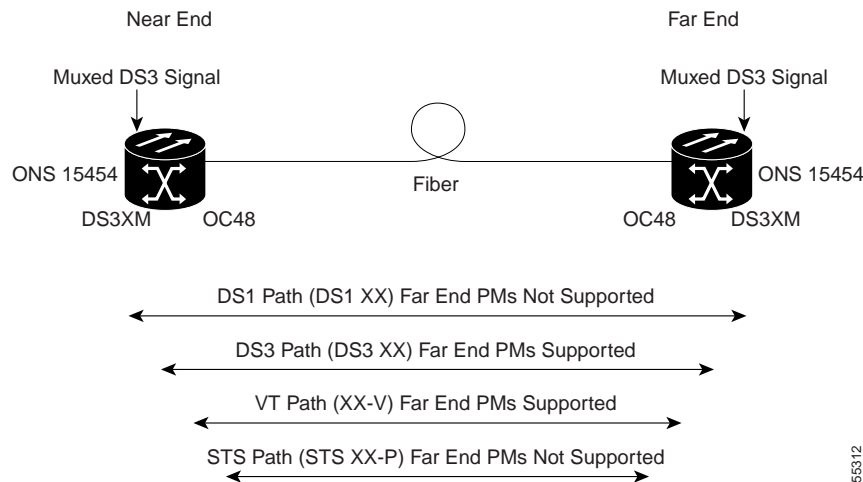
Note The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-20   PM read points on the DS3XM-6 card

Table 8-21   Near-End DS3 Line PMs for the DS3XM-6 Card

Parameter	Definition
DS3 CV-L	Code Violation Line (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
DS3 ES-L	Errored Seconds Line (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (i.e. LOS) on the line.
DS3 SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
DS3 LOSS-L	Line Loss of Signal (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Cisco ONS 15454 Installation and Operations Guide

Table 8-22   Near-End DS3 Path PMs for the DS3XM-6 Card

Parameter	Definition
DS3 AISS-P	AIS Seconds Path (AISS-P) is a count of one-second intervals containing one or more AIS defects.
DS3 CVP-P	Code Violation Path (CVP-P) is a code violation parameter for M23 applications. CVP-P is a count of P-bit parity errors occurring in the accumulation period.
DS3 ESP-P	Errored Second Path (ESP-P) is a count of seconds containing one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
DS3 SASP-P	SEF/AIS Seconds Path (SASP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
DS3 SESP-P	Severely Errored Seconds Path (SESP-P) is a count of seconds containing more than 44 P-bit parity violations, one or more SEF defects, or one or more AIS defects.
DS3 UASP-P	Unavailable Second Path (UASP-P) is a count of one-second intervals when the DS3 path is unavailable. A DS3 path becomes unavailable when ten consecutive SESP-Ps occur. The ten SESP-Ps are included in unavailable time. Once unavailable, the DS3 path becomes available when ten consecutive seconds with no SESP-Ps occur. The ten seconds with no SESP-Ps are excluded from unavailable time.

Table 8-23   Near-End CP-bit Path PMs for the DS3XM-6 Card

Parameter	Definition
DS3 CVCP-P	Code Violation Path (CVCP-P) is a count of CP-bit parity errors occurring in the accumulation period.
DS3 ESCP-P	Errored Second Path (ESCP-P) is a count of seconds containing one or more CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
DS3 SESCP-P	Severely Errored Seconds Path (SESCP-P) is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
DS3 UASCP-P	Unavailable Seconds Path (DS3 UASCP-P) is a count of one-second intervals when the DS3 path is unavailable. A DS3 path becomes unavailable when ten consecutive SESCP-Ps occur. The ten SESCP-Ps are included in unavailable time. Once unavailable, the DS3 path becomes available when ten consecutive seconds with no SESCP-Ps occur. The ten seconds with no SESCP-Ps are excluded from unavailable time.

Table 8-24   Near-End DS1 Path PMs for the DS3XM-6 Card

Parameter	Definition
DS1 AISS-P	Alarm Indication Signal Path (AIS-P) means an AIS occurred on the path. This parameter is a count of seconds containing one or more AIS defects.
DS1 ES-P	Errored Seconds Path (ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more SEF or AIS defects. For DS1-SF paths, the ES-P parameter is a count of one-second intervals containing one or more FE events, or one or more CS events, or one or more SEF or AIS defects.
DS1 SAS-P	Severely Errored Seconds Path Frame/Alarm Indication Signal (SAS-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects.
DS1 SES-P	Severely Errored Seconds Path (SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more SEF or AIS defects occurs. For DS1-SF paths, an SES is a second containing either the occurrence of eight FEs, four FEs, or one or more SEF or AIS defects.
DS1 UAS-P	Unavailable Seconds Path (UAS-P) is a count of one-second intervals when the DS1 path is unavailable. The DS1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. Once unavailable, the DS1 path becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time.

Table 8-25   Near-End VT PMs for the DS3XM-6 Card

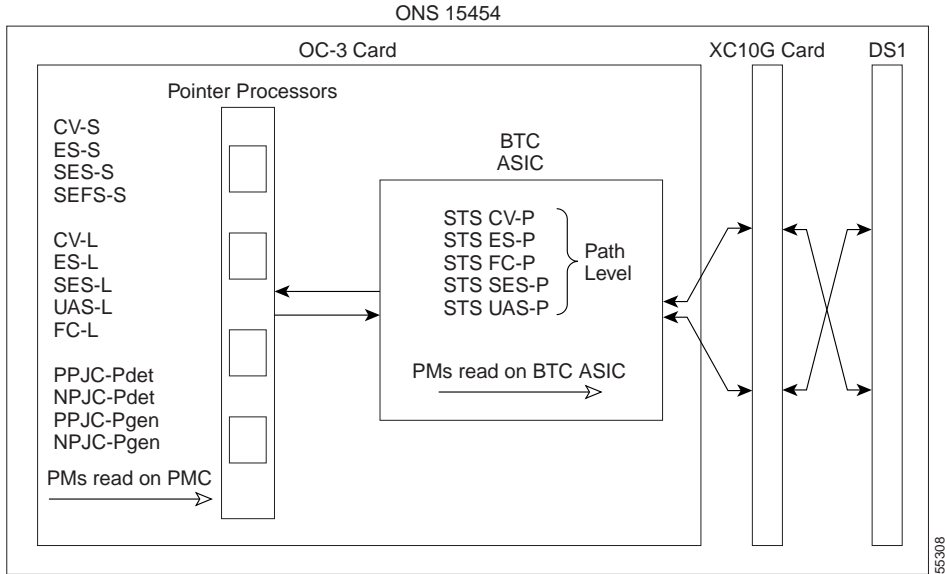| Parameter	Definition
CV-V	Code Violation VT Layer (CV-V) is a count of the BIP errors detected at the VT path layer. Up to two BIP errors can be detected per VT superframe; each error increments the current CV-V second register.
ES-V	Errored Seconds VT Layer (ES-V) is a count of the seconds when at least one VT Path BIP error was detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause ES-V.
SES-V	Severely Errored Seconds VT Layer (SES-V) is a count of seconds when K (600) or more VT Path BIP errors were detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause SES-V.
UAS-V	Unavailable Seconds VT Layer (UAS-V) is a count of the seconds when the VT path was unavailable. A VT path becomes unavailable when ten consecutive seconds occur that qualify as SES-Vs and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Vs.

Table 8-26   Near-End SONET Path PMs for the DS3XM-6 Card

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

Table 8-27   Far-End CP-bit Path PMs for the DS3XM-6 Card

Parameter	Definition
DS3 CVCP-P	Code Violation (CVCP-PFE) is a parameter that is counted when the three FEBE bits in a M-frame are not all collectively set to 1.
DS3 ESCP-P	Errored Second (ESCP-PFE) is a count of one-second intervals containing one or more M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
DS3 SASCP-P	SEF/AIS Second (SASCP-PFE) is a count of one-second intervals containing one or more far-end SEF/AIS defects.
DS3 SESCP-P	Severely Errored Second (SESCP-PFE) is a count of one-second intervals containing one or more 44 M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
DS3 UASCP-P	Unavailable Second (UASCP-PFE) is a count of one-second intervals when the DS3 path becomes unavailable. A DS3 path becomes unavailable when ten consecutive far-end CP-bit SESs occur. The ten CP-bit SESs are included in unavailable time. Once unavailable, the DS3 path becomes available when ten consecutive seconds with no CP-bit SESs occur. The ten seconds with no CP-bit SESs are excluded from unavailable time.

Table 8-28   Far-End VT PMs for the DS3XM-6 Card

Parameter	Definition
CV-V	Code Violation VT Layer (CV-V) is a count of the BIP errors detected at the VT path layer. Up to two BIP errors can be detected per VT superframe; each error increments the current CV-V second register.
ES-V	Errored Seconds VT Layer (ES-V) is a count of the seconds when at least one VT Path BIP error was detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause an ES-V.
SES-V	Severely Errored Seconds VT Layer (SES-V) is a count of seconds when K (600) or more VT Path BIP errors were detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause an SES-V.
UAS-V	Unavailable Second VT Layer (UAS-V) is a count of the seconds when the VT path was unavailable. A VT path becomes unavailable when ten consecutive seconds occur that qualify as SES-Vs and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Vs.

8.6 Performance Monitoring for Optical Cards

The following sections define performance monitoring parameters and definitions for the OC-3, OC-12, OC-48, and OC-192.

8.6.1 OC-3 Card Performance Monitoring Parameters

Figure 8-21 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-3 card.

Figure 8-21   PM read points on the OC-3 card

⬥

Note   For PM locations relating to protection switch counts, see the GR-253-CORE document.

Table 8-29   Near-End Section PMs for the OC-3 Card

Parameter	Definition
CV-S	Section Coding Violation (CV-S) is a count of BIP errors detected at the section-layer (i.e. using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame, with each error incrementing the current CV-S second register.
ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or LOS defect was present.
SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see GR-253 for value) or more section-layer BIP errors were detected or an SEF or LOS defect was present.
SEFS-S	Section Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected to be present during most seconds when an LOS or LOF defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect.

Table 8-30   Near-End Line Layer PMs for the OC-3 Card

Parameter	Definition
CV-L	Near-End Line Code Violation (CV-L) is a count of BIP errors detected at the line-layer (i.e. using the B2 bytes in the incoming SONET signal). Up to 8 x N BIP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	Near-End Line Errored Seconds (ES-L) is a count of the seconds when at least one line-layer BIP error was detected or an AIS-L defect was present.
SES-L	Near-End Line Severely Errored Seconds (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer BIP errors were detected or an AIS-L defect was present.
UAS-L	Near-End Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls.
FC-L	Near-End Line Failure Count (FC-L) is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure is declared or when a lower-layer traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.

Table 8-31   Near-End Line Layer PMs for the OC-3 Cards

Parameter	Definition
PSC (1+1 protection)	In a 1 + 1 protection scheme for a working card, Protection Switching Count (PSC) is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card.
	For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM is only applicable if revertive line-level protection switching is used.
	Note BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.
PSD	Protection Switching Duration (PSD) applies to the length of time, in seconds, that service is carried on another line. For a working line, PSD is a count of the number of seconds that service was carried on the protection line.
	For the protection line, PSD is a count of the seconds that the line was used to carry service. The PSD PM is only applicable if revertive line-level protection switching is used.
	Note BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.

Table 8-32   Near-End SONET Path H-byte PMs for the OC-3 Card

Parameter	Definition
PPJC-Pdet	Positive Pointer Justification Count, STS Path Detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	Negative Pointer Justification Count, STS Path Detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	Positive Pointer Justification Count, STS Path Generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	Negative Pointer Justification Count, STS Path Generated (NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the synchronous payload envelope (SPE) with the local clock.

Table 8-33   Near-End SONET Path PMs for the OC-3 Card

Parameter	Definition
Note	SONET path PMs will not count unless IPPM is enabled. For additional information, see the "Enable Intermediate-Path Performance Monitoring" procedure on page 7-25. The far-end IPPM feature is not supported in Software R3.1. However, SONET path PMs can be monitored by logging into the far-end node directly.
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when one or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

Table 8-34   Far-End Line Layer PMs for the OC-3 Card

Parameter	Definition
CV-L	Far-End Line Code Violation (CV-L) is a count of BIP errors detected by the far-end line terminating equipment (LTE) and reported back to the near-end LTE using the REI-L indication in the line overhead. For SONET signals at rates below OC-48, up to 8 x N BIP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 BIP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each BIP error indicated by the incoming REI-L.
ES-L	Far-End Line Errored Seconds (ES-L) is a count of the seconds when at least one line-layer BIP error was reported by the far-end LTE or an RDI-L defect was present.
SES-L	Far-End Line Severely Errored Seconds (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer BIP errors were reported by the far-end LTE or an RDI-L defect was present.
UAS-L	Far-End Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable at the far end. A line becomes unavailable at the far end when ten consecutive seconds occur that qualify as SES-LFEs and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-LFEs.
FC-L	Far-End Line Failure Count (FC-L) is a count of the number of far-end line failure events. A failure event begins when RFI-L failure is declared, and it ends when the RFI-L failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

8.6.2 OC-12, OC-48, and OC-192 Card Performance Monitoring Parameters

Figure 8-22 shows the signal types that support far-end PMs. Figure 8-23 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-12, OC-48, and OC-192 cards.

Figure 8-22   Monitored signal types for the OC-12, OC-48, and OC-192 cards
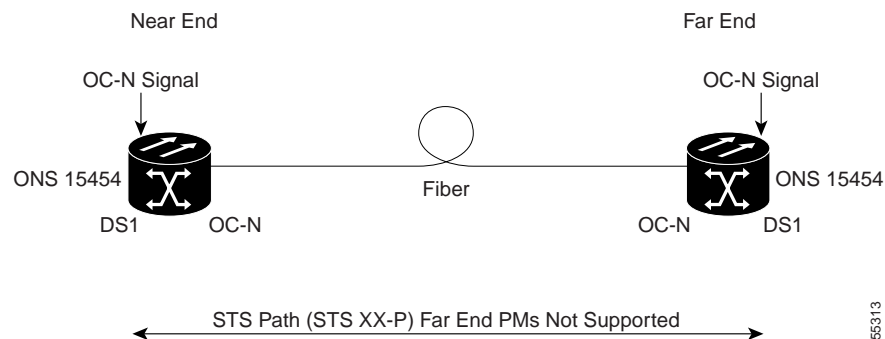
Note   PMs on the protect STS are not supported for BLSR. The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-23   PM read points on the OC-12, OC-48, and OC-192 cards
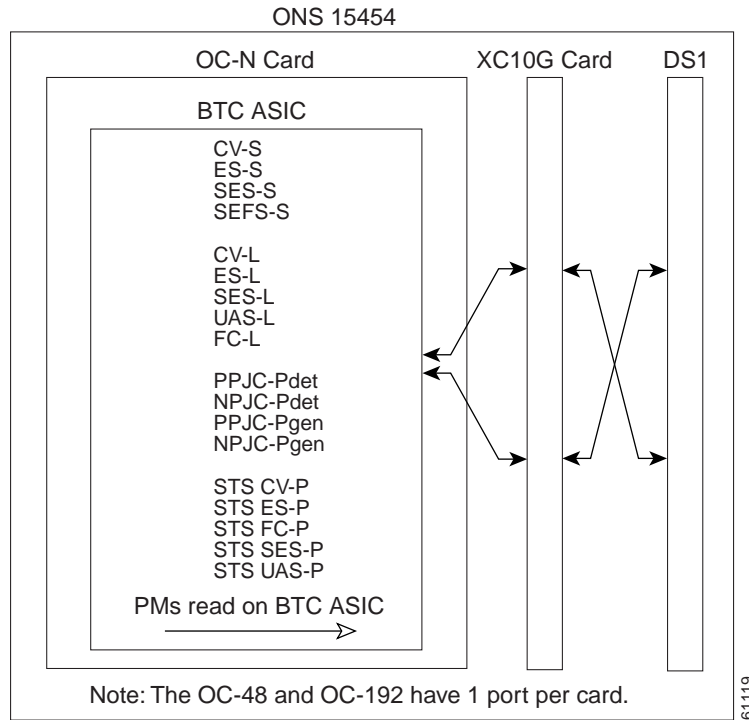
Note   For PM locations relating to protection switch counts, see the GR-1230-CORE document.

Table 8-35   Near-End Section PMs for the OC-12, OC-48, and OC-192 Cards

Parameter	Definition
CV-S	Section Coding Violation (CV-S) is a count of BIP errors detected at the section-layer (i.e. using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.
ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or LOS defect was present.

Table 8-35   Near-End Section PMs for the OC-12, OC-48, and OC-192 Cards (continued)

Parameter	Definition
SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see GR-253 for value) or more section-layer BIP errors were detected or an SEF or LOS defect was present.
SEFS-S	Section Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected to be present during most seconds when an LOS or LOF defect is present. However, there may be situations when the SEFS-S parameter is only incremented based on the presence of an SEF defect.

Table 8-36   Near-End Line Layer PMs for the OC-12, OC-48, and OC-192 Cards

Parameter	Definition
CV-L	Near-End Line Code Violation (CV-L) is a count of BIP errors detected at the line-layer (i.e. using the B2 bytes in the incoming SONET signal). Up to 8 x N BIP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	Near-End Line Errored Seconds (ES-L) is a count of the seconds when at least one line-layer BIP error was detected or an AIS-L defect was present.
SES-L	Near-End Line Severely Errored Seconds (SES-L) is a count of the seconds when K (see GR-253 for values) or more line-layer BIP errors were detected or an AIS-L defect was present.
UAS-L	Near-End Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls.
FC-L	Near-End Line Failure Count (FC-L) is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure or a lower-layer traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.

Table 8-37   Near-End SONET Path H-byte PMs for the OC-12, OC-48, and OC-192 Cards

Parameter	Definition
PPJC-Pdet	Positive Pointer Justification Count, STS Path Detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	Negative Pointer Justification Count, STS Path Detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.

Table 8-37   Near-End SONET Path H-byte PMs for the OC-12, OC-48, and OC-192 Cards (continued)

Parameter	Definition
PPJC-Pgen	Positive Pointer Justification Count, STS Path Generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	Negative Pointer Justification Count, STS Path Generated (PPJC-Pgen) is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the synchronous payload envelope (SPE) with the local clock.

Table 8-38   Near-End Line Layer PMs for the OC-12, OC-48, and OC-192 Cards

Parameter	Definition
PSC (BLSR)	For a protect line in a 2-fiber ring, Protection Switching Count (PSC) refers to the number of times a protection switch has occurred either to a particular span's line protection or away from a particular span's line protection. Therefore, if a protection switch occurs on a 2-fiber BLSR, the PSC of the protection span to which the traffic is switched will increment, and when the switched traffic returns to its original working span from the protect span, the PSC of the protect span will increment again.
PSC (1+1 protection)	In a 1 + 1 protection scheme for a working card, Protection Switching Count (PSC) is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM is only applicable if revertive line-level protection switching is used.
PSD	For an active protection line in a 2-fiber BLSR, Protection Switching Duration (PSD) is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. PSD increments on the active protect line and PSD-W increments on the failed working line.
PSC-W	For a working line in a 2-fiber BLSR, Protection Switching Count-Working (PSC-W) is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line and PSC increments on the active protect line. For a working line in a 4-fiber BLSR, PSC-W is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. PSC-W increments on the failed line and PSC-R or PSC-S increments on the active protect line.
PSD-W	For a working line in a 2-fiber BLSR, Protection Switching Duration-Working (PSD-W) is a count of the number of seconds that service was carried on the protection line. PSD-W increments on the failed working line and PSD increments on the active protect line.

Table 8-38   Near-End Line Layer PMs for the OC-12, OC-48, and OC-192 Cards (continued)

Parameter	Definition
PSC-S	In a 4-fiber BLSR, Protection Switching Count-Span (PSC-S) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. A count is only incremented if span switching is used.
PSD-S	In a 4-fiber BLSR, Protection Switching Duration-Span (PSD-S) is a count of the seconds that the protection line was used to carry service. A count is only incremented if span switching is used.
PSC-R	In a 4-fiber BLSR, Protection Switching Count-Ring (PSC-R) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to a working line. A count is only incremented if ring switching is used.
PSD-R	In a 4-fiber BLSR, Protection Switching Duration-Ring (PSD-R) is a count of the seconds that the protection line was used to carry service. A count is only incremented if ring switching is used.

Table 8-39   Near-End SONET Path PMs for the OC-12, OC-48, and OC-192 Cards

Parameter	Definition
Note	SONET path PMs will not count unless IPPM is enabled. For additional information, see the "Enable Intermediate-Path Performance Monitoring" procedure on page 7-25. The far-end IPPM feature is not supported in Software R3.1. However, SONET path PMs can be monitored by logging into the far-end node directly.
STS CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.

Table 8-40   Far-End Line Layer PMs for the OC-12, OC-48, and OC-192 Cards

Parameter	Definition
CV-L	Far-End Line Code Violation (CV-L) is a count of BIP errors detected by the far-end line terminating equipment (LTE) and reported back to the near-end LTE using the REI-L indication in the line overhead. For SONET signals at rates below OC-48, up to 8 x N BIP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 BIP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each BIP error indicated by the incoming REI-L.
ES-L	Far-End Line Errored Seconds (ES-L) is a count of the seconds when at least one line-layer BIP error was reported by the far-end LTE or an RDI-L defect was present.
SES-L	Far-End Line Severely Errored Seconds (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer BIP errors were reported by the far-end LTE or an RDI-L defect was present.
UAS-L	Far-End Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable at the far end. A line becomes unavailable at the far end when ten consecutive seconds occur that qualify as SES-LFEs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-LFEs.
FC-L	Far-End Line Failure Count (FC-L) is a count of the number of far-end line failure events. A failure event begins when RFI-L failure is declared and ends when the RFI-L failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

Ethernet Operation

The Cisco ONS 15454 integrates Ethernet into a SONET time-division multiplexing (TDM) platform. Unlike traditional transport products, which map Ethernet frames directly over dedicated TDM bandwidth, the ONS 15454 incorporates layer 2 switching to allow more efficient data transport over the existing SONET backbone.

This chapter describes the Ethernet capabilities of the ONS 15454, including:

- Ethernet cards

- Multicard and Single-card Etherswitch

- Ethernet circuit combinations and configurations

- VLAN and IEEE 802.1Q support

- Spanning tree and IEEE 802.1D support

- Ethernet performance and maintenance screens

- Ethernet alarm thresholds (RMON)

9.1 Ethernet Cards

The ONS 15454 shelf assembly holds up to ten Ethernet cards in any multispeed slot. Ethernet cards include the E100T-12, E100T-G, E1000-2 and E1000-2-G. The E100T-12 is the functional equivalent of the E100T-G, and the E1000-2 is the functional equivalent of the E1000-2-G. An ONS 15454 using XC10G cards requires the G versions of the Ethernet cards.

Ethernet card faceplates have two card-level LEDs and a pair of port-level LEDs next to each port.

Table 9-1   Card-level LEDS

LED State	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready or a catastrophic software failure occurred on the Ethernet card. As part of the boot sequence, the FAIL LED is turned on until the software deems the card operational.
Green ACT LED	A green ACT LED provides the operational status of the E100T-G. When the ACT LED is green it indicates that the Ethernet card is active and the software is operational.

Table 9-2   Port-level LEDs

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Green Light Off	Inactive Connection or Unidirectional Traffic

9.1.1 E100T-12/E100T-G

E100T-12/E100T-G cards provide twelve switched, IEEE 802.3-compliant 10/100 Base-T Ethernet ports. Ports detect the speed of an attached device by auto-negotiation and automatically connect at the appropriate speed and duplex mode, either half or full duplex, and determine whether to enable or disable flow control. An E100T-12/E100T-G card consumes 55 W, 1.46 AMPS, and 188 BTU/Hr.

9.1.2 E1000-2/E1000-2-G

E1000-2/E1000-2-G cards provides two switched, IEEE 802.3-compliant Gigabit Ethernet (1000 Mbps) ports that support full duplex operation. An E100T-12/E100T-G card consumes 60 W, 1.25 AMPS, and 205 BTU/Hr.

Gigabit interface converters (GBICs) are hot-swappable input/output devices that plug into a Gigabit Ethernet (E1000-2 or E1000-2-G) card to link the port with the fiber-optic network and determine the maximum distance that the Ethernet traffic will travel from the E1000-2/E1000-2-G card to the next network device.

E1000-2/E1000-2-G cards support two types of standard Cisco GBICs: the IEEE 1000Base-SX compliant 850 nm "short reach" and the IEEE 1000Base-LX compliant 1300 nm "long reach." The 850 nm SX optics are designed for multimode fiber and distances up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300 nm LX optics are designed for single-mode fiber and distances up to 5 kilometers.

Figure 9-1   A gigabit interface converter

Receiver   Transmitter
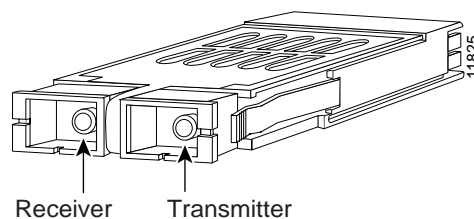
Table 9-3 shows the available GBICs.

Table 9-3   Available GBICs

GBIC	Product Number
Short wavelength (1000BaseSX)	15454-GBIC-SX
Long wavelength/long haul (1000BaseLX)	15454-GBIC-LX

For GBIC installation and cabling instructions, see the "Fiber-Optic Cable Installation" section on page 1-52.

⚠

Caution   E1000-2/E1000-2-G cards lose traffic for approximately 30 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm will appear and clear during this period.

For detailed specifications of the Ethernet cards, refer to the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.

9.1.3 Port Provisioning for Ethernet Cards

This section explains how to provision Ethernet ports on an Ethernet card. Most provisioning requires filling in two fields: Enabled and Mode. However, you can also map incoming traffic to a low priority or a high priority queue using the Priority column, and you can enable spanning tree with the Stp Enabled column. For more information about spanning tree, see the "Spanning Tree (IEEE 802.1D)" section on page 9-26. The Status column displays information about the port's current operating mode, and the Stp State column provides the current spanning tree status.

Procedure: Provision Ethernet Ports

Step 1   Display CTC and double-click the card graphic to open the Ethernet card.

Step 2   Choose the **Provisioning** > **Port** tabs.

Figure 9-2 shows the Provisioning tab with the Port function subtab selected.

Figure 9-2   Provisioning Ethernet ports

Step 3 From the Port screen, choose the appropriate mode for each Ethernet port. Valid choices for the E100T-12/E100T-G card are Auto, 10 Half, 10 Full, 100 Half, or 100 Full. Valid choices for the E1000-2/E1000-2-G card are 1000 Full or Auto.

Both 1000 Full and Auto mode set the E1000-2 port to the 1000 Mbps and Full duplex operating mode; however, flow control is disabled when 1000 Full is selected. Choosing Auto mode enables the E1000-2 card to autonegotiate flow control. Flow control is a mechanism that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. The E1000-2 port handshakes with the connected network device to determine if that device supports flow control.

Step 4 Click the **Enabled** checkbox(s) to activate the corresponding Ethernet port(s).

Step 5 Click **Apply**.

Your Ethernet ports are now provisioned and ready to be configured for VLAN membership.

Step 6 Repeat this procedure for all other cards that will be in the VLAN.

9.2 Multicard and Single-Card EtherSwitch

The ONS 15454 enables multicard and single-card EtherSwitch modes. At the Ethernet card view in CTC, click the **Provisioning** > **Card** tabs to reveal the Card Mode option.

9.2.1 Multicard EtherSwitch

Multicard EtherSwitch provisions two or more Ethernet cards to act as a single layer 2 switch. It supports one STS-6c shared packet ring, two STS-3c shared packet rings, or six STS-1 shared packet rings. The bandwidth of the single switch formed by the Ethernet cards matches the bandwidth of the provisioned Ethernet circuit up to STS-6c worth of bandwidth.

Figure 9-3   A Multicard EtherSwitch configuration

⚠️
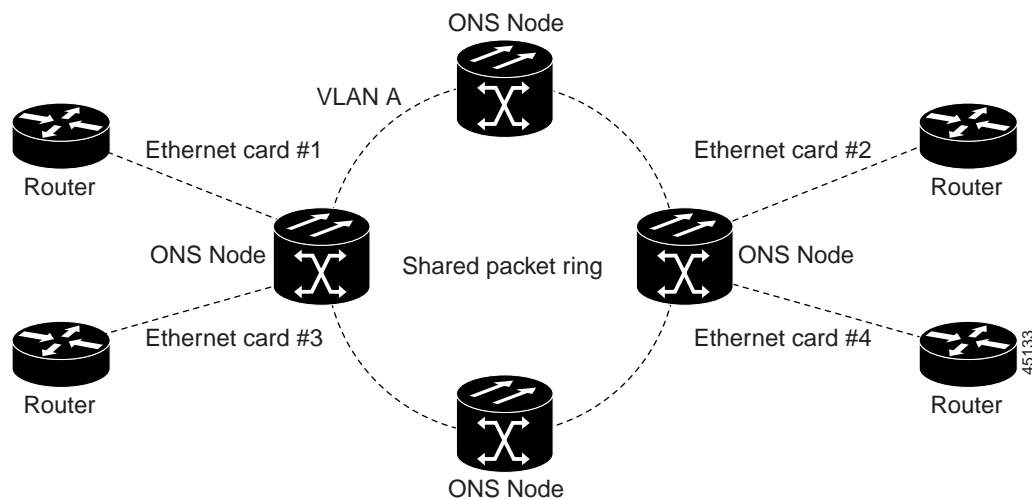
Caution Whenever you drop two STS-3c multicard EtherSwitch circuits onto an Ethernet card and delete only the first circuit, you should not provision STS-1 circuits to the card without first deleting the remaining STS-3c circuit. If you attempt to create a STS-1 circuit after deleting the first STS-3c circuit, the STS-1 circuit will not work and no alarms will indicate this condition. To avoid this condition, delete the second STS-3c prior to creating the STS-1 circuit.

9.2.2 Single-Card EtherSwitch

Single-card EtherSwitch allows each Ethernet card to remain a single switching entity within the ONS 15454 shelf. This option allows a full STS-12c worth of bandwidth between two Ethernet circuit points. Figure 9-4 illustrates a single-card EtherSwitch configuration.

Figure 9-4   A Single-card EtherSwitch configuration
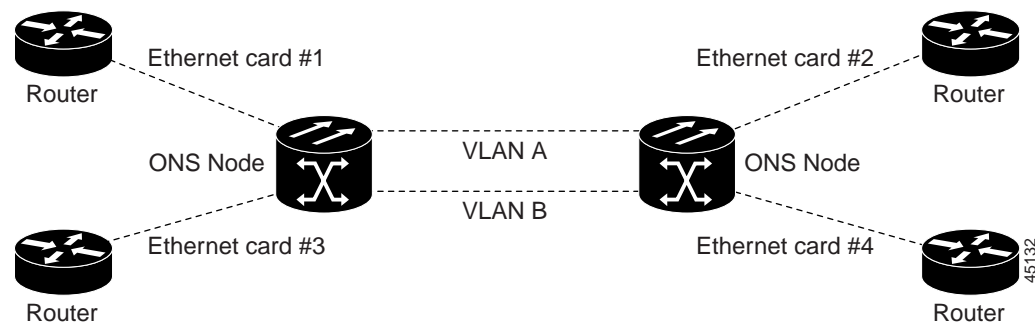
Seven scenarios exist for provisioning single-card EtherSwitch bandwidth:

1. STS 12c
2. STS 6c + STS 6c
3. STS 6c + STS 3c + STS 3c
4. STS 6c + 6 STS-1s
5. STS 3c + STS 3c +STS 3c +STS 3c
6. STS 3c +STS 3c + 6 STS-1s
7. 12 STS-1s

✎

Note When configuring scenario 3, the STS 6c must be provisioned before either of the STS 3c circuits.

9.2.3 ONS 15454 and ONS 15327 EtherSwitch Circuit Combinations

The following table shows the Ethernet circuit combinations available in ONS 15454s and ONS 15327s

Cisco ONS 15454 Installation and Operations Guide

.

Table 9-4   ONS 15454 and ONS 15327 Ethernet Circuit Combinations

15327 Single-Card	15327 Multicard	15454 Single-Card	15454 Multicard
six STS-1s	three STS-1s	one STS 12c	six STS-1s
two STS 3cs	one STS 3c	two STS 6cs	two STS 3cs
one STS 6c		one STS 6c and two STS 3cs	one STS 6c
one STS 12c		one STS 6c and six STS-1s	
		four STS 3cs	
		two STS 3cs and six STS-1s	
		twelve STS-1s	

9.3 Ethernet Circuit Configurations

Ethernet circuits can link ONS nodes through point-to-point, shared packet ring, or hub and spoke configurations. Two nodes usually connect with a point-to-point configuration. More than two nodes usually connect with a shared packet ring configuration or a hub and spoke configuration. This section includes procedures for creating these configurations and also explains how to create Ethernet manual cross-connects. Ethernet manual cross-connects allow you to cross connect individual Ethernet circuits to an STS channel on the ONS 15454 optical interface and also to bridge non-ONS SONET network segments.

Note   Before making Ethernet connections, choose a circuit size from STS-1, STS-3c, STS-6c, or STS-12c.

Note   When making an STS-12c Ethernet circuit, Ethernet cards must be configured as single-card EtherSwitch. Multi-card mode does not support STS-12c Ethernet circuits.

9.3.1 Point-to-Point Ethernet Circuits

The ONS 15454 can set up a point-to-point (straight) Ethernet circuit as Single-card or Multicard. Multicard EtherSwitch limits bandwidth to STS-6c of bandwidth between two Ethernet circuit points, but allows adding nodes and cards and making a shared packet ring. Single-card EtherSwitch allows a full STS-12c of bandwidth between two Ethernet circuit points.

Figure 9-5   A Multicard EtherSwitch point-to-point circuit
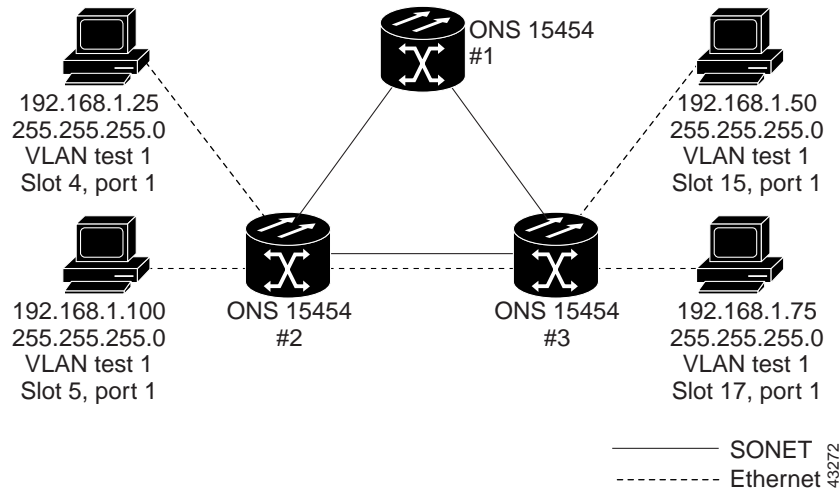
Figure 9-6   A Single-card Etherswitch point-to-point circuit
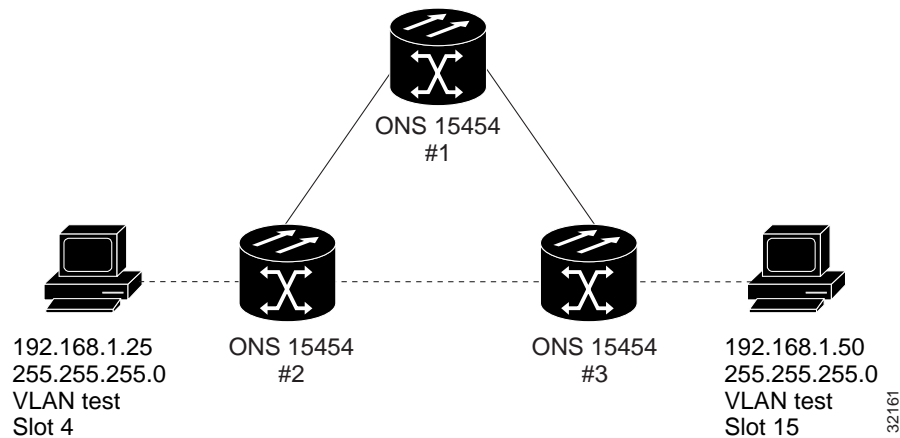
Procedure: Provision an EtherSwitch Point-to-Point Circuit (Multicard or Single-Card)

Step 1   Display CTC for one of the ONS 15454 Ethernet circuit endpoint nodes.

Step 2   Double-click one of the Ethernet cards that will carry the circuit.

Step 3   Click the **Provisioning** > **Card** tabs.

Step 4   If you are building a Multicard Etherswitch point-to-point circuit:

    a.   Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.

    b.   If **Multi-card EtherSwitch Group** is not checked, check it and click **Apply**.

    c.   Repeat Steps 2 – 4 for all other Ethernet cards in the ONS 15454 that will carry the circuit.

If you are building a Single-card Etherswitch circuit:

    d.   Under Card Mode, verify that **Single-card EtherSwitch** is checked.

    e.   If **Single-card EtherSwitch** is not checked, check it and click **Apply**.

Cisco ONS 15454 Installation and Operations Guide

Step 5   Navigate to the other ONS 15454 Ethernet circuit endpoint.

Step 6   Repeat Steps 2 – 5.

Step 7   Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens (Figure 9-7).

Figure 9-7   Provisioning an Ethernet circuit
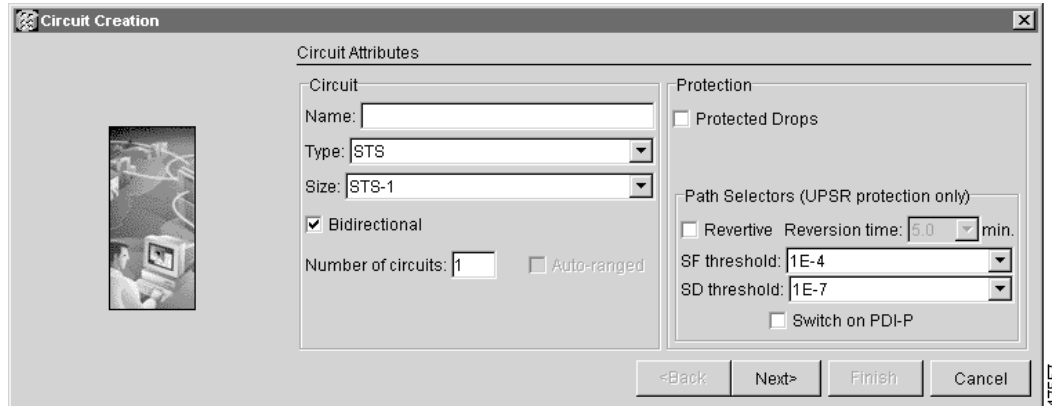
Step 8   In the Name field, type a name for the circuit.

Step 9   From the Type pull-down menu, choose **STS**.

Step 10   The VT and VT Tunnel types do not apply to Ethernet circuits.

Step 11   Choose the size of the circuit from the Size pull-down menu.

The valid circuit sizes for an Ethernet Multicard circuit are STS-1, STS-3c and STS6c.

The valid circuit sizes for an Ethernet Single-card circuit are STS-1, STS-3c, STS6c and STS12c.

Step 12   Verify that the **Bidirectional** checkbox is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box opens (Figure 9-8).

Figure 9-8   Choosing a circuit source
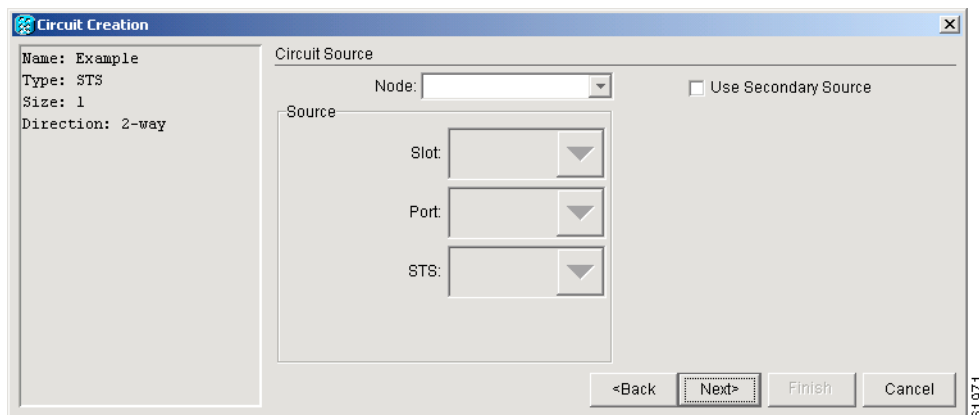
Step 13   Choose the circuit source from the Node menu. Either end node can be the circuit source.

Step 14   If you are building a Multicard EtherSwitch circuit, choose **Ethergroup** from the Slot menu and click **Next**.

Step 15   If you are building a Single-card EtherSwitch circuit, from the Slot menu choose the Ethernet card where you enabled the single-card Etherswitch and click **Next**.

The Circuit Creation (Destination) dialog box opens.

Step 16   Choose the circuit destination from the Node menu, in this example Node 2. Choose the node that is not the source.

Step 17   If you are building a Multicard EtherSwitch circuit choose **Ethergroup** from the Slot menu and click **Next**.

Step 18   If you are building a **Single-card EtherSwitch** circuit, from the Slot menu choose the Ethernet card for which you enabled the Single-card Etherswitch and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box opens.

Step 19   Create the VLAN:

   a.   Click the **New VLAN** tab.

   b.   Assign an easily-identifiable name to your VLAN.

   c.   Assign a VLAN ID.

   d.   The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

   e.   Click **OK**.

   f.   Highlight the VLAN name and click the arrow >> tab to move the available VLAN(s) to the Circuit VLANs column.

Step 20   Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 21   Confirm that the following information about the point-to-point circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs on the circuit
- ONS 15454 nodes included in the circuit

Step 22   Click **Finish**.

Step 23   You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the "Provision Ethernet Ports" procedure on page 9-3. For assigning ports to VLANs, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-24. For information about manually provisioning circuits, see the "Ethernet Manual Cross-Connects" procedure on page 9-16.

9.3.2 Shared Packet Ring Ethernet Circuits

This section provides steps for creating a shared packet ring (Figure 9-9). Your network architecture may differ from the example.

Figure 9-9   A shared packet ring Ethernet circuit
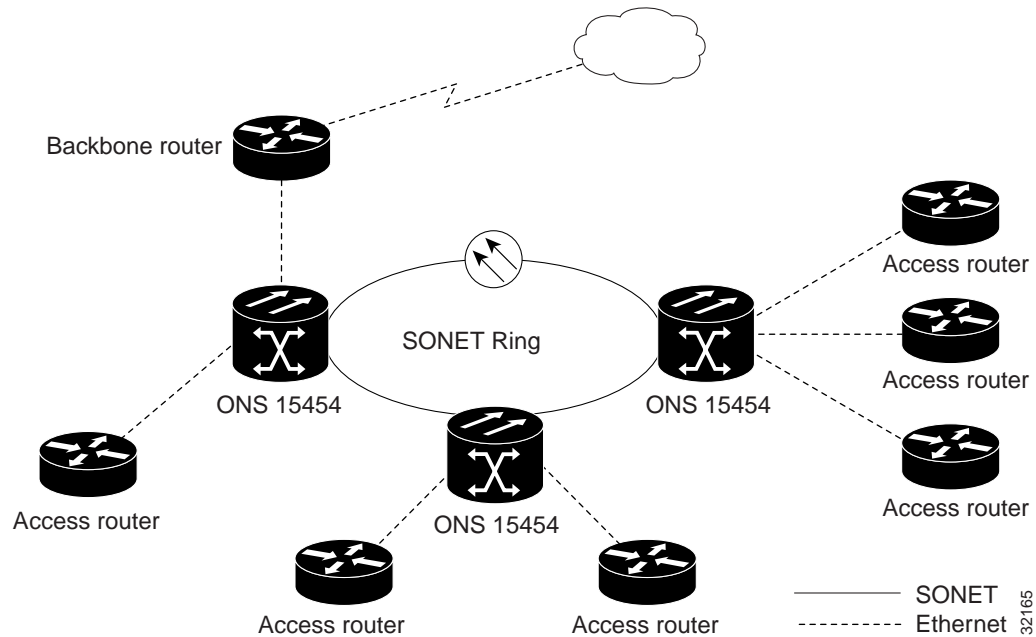
Procedure: Provision a Shared Packet Ring

Step 1   Display CTC for one of the ONS 15454 Ethernet circuit endpoints.

Step 2   Double-click one of the Ethernet cards that will carry the circuit.

Step 3   Click the **Provisioning** > **Card** tabs.

Step 4   Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.

Step 5   If **Multi-card EtherSwitch Group** is not checked, check it and click **Apply**.

Step 6   Display the node view.

Step 7   Repeat Steps 2 – 6 for all other Ethernet cards in the ONS 15454 that will carry the shared packet ring.

Step 8   Navigate to the other ONS 15454 endpoint.

Step 9   Repeat Steps 2 – 7.

Step 10 Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens.

Step 11 In the Name field, type a name for the circuit.

Step 12 From the Type pull-down menu, choose **STS**. The VT and VT Tunnel types do not apply to Ethernet circuits.

Step 13 From the Size pull-down menu, choose the size of the circuit.

For shared packet ring Ethernet, valid circuit sizes are STS-1, STS-3C and STS-6c.

Step 14   Verify that the **Bidirectional** checkbox is checked.

✎

Note   You must manually provision the circuits if you are building a shared packet ring configuration.

Step 15   Click **Next**.

The Circuit Creation (Circuit Source) dialog box opens.

Step 16   From the Node menu, choose the circuit source.

Any shared packet ring node can serve as the circuit source.

Step 17   Choose **Ethergroup** from the Slot menu and click **Next**.

The Circuit Creation (Circuit Destination) dialog box opens.

Step 18   Choose the circuit destination from the Node menu.

Step 19   Except for the source node, any shared packet ring node can serve as the circuit destination.

**Step 20**   Choose **Ethergroup** from the Slot menu and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box opens.

Step 21   Create the VLAN:

  a.   Click the **New VLAN** tab.

The Circuit Creation (Define New VLAN) dialog box opens (Figure 9-10).

Figure 9-10   Choosing a VLAN name and ID
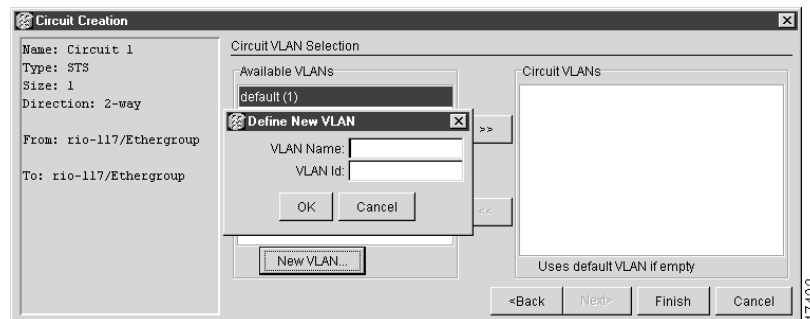
  b.   Assign an easily-identifiable name to your VLAN.

  c.   Assign a VLAN ID.

This VLAN ID number must be unique. It is usually the next available number not already assigned to an existing VLAN (between 2 and 4093). Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

  d.   Click **OK**.

Figure 9-11   Selecting VLANs
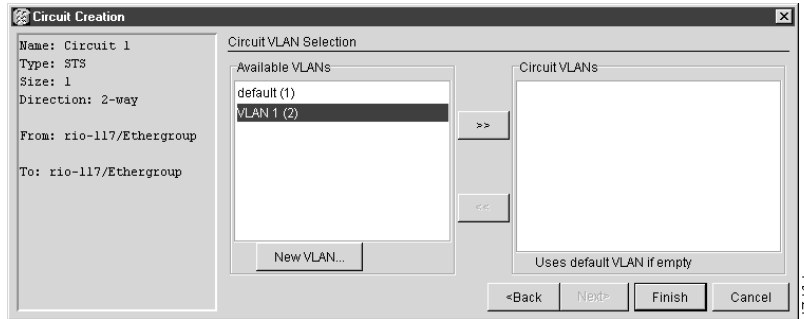
e. Highlight the VLAN name and click the >> tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-11).

By moving the VLAN from the Available VLANs column to the Circuit VLANs column, all the VLAN traffic is forced to use the shared packet ring circuit you created.

Step 22   Click **Next**.

Step 23   Uncheck the **Route Automatically** checkbox and click **Next**.

Figure 9-12   Adding a span
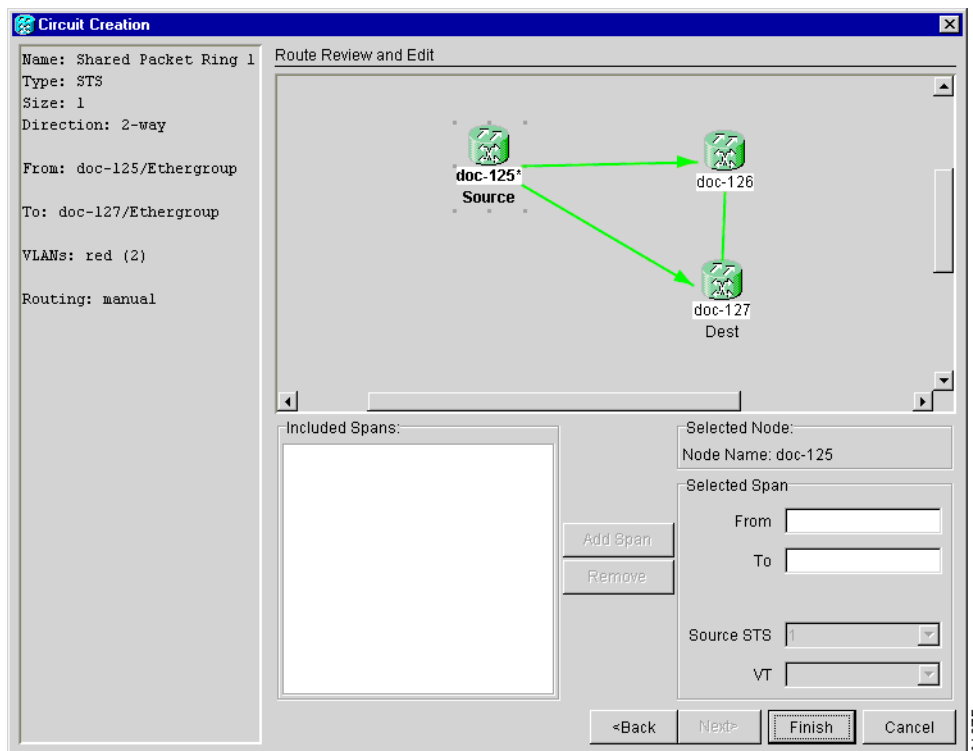
Step 24   Click either span (green arrow) leading from the source node (Figure 9-12).

The span turns white.

Step 25   Click **Add Span**.

The span turns blue and adds the span to the Included Spans field.

Step 26   Click the node at the end of the blue span.

Step 27 Click the green span leading to the next node.

The span turns white.

Step 28 Click **Add Span**.

The span turns blue.

Step 29 Repeat Steps 24 – 27 for every node remaining in the ring. Figure 9-13 shows the Circuit Path Selection dialog box with all the spans selected.

Figure 9-13   Viewing a span
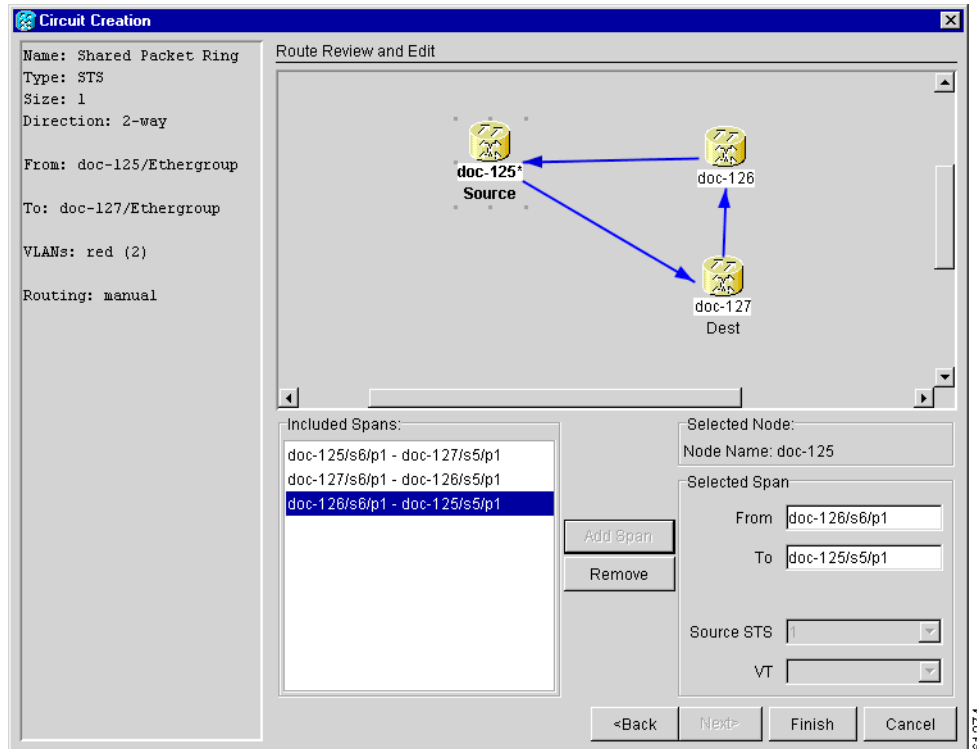
Step 30 Verify that the new circuit is correctly configured.

Note If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information. You can also click **Finish**, delete the completed circuit, and begin the procedure again.

Step 31 Click **Finish**.

Step 32 You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the "Provision Ethernet Ports" procedure on page 9-3. For assigning ports to VLANs, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-24.

9.3.3 Hub and Spoke Ethernet Circuit Provisioning

This section provides steps for creating a hub and spoke Ethernet circuit configuration. The hub and spoke configuration connects point-to-point circuits (the spokes) to an aggregation point (the hub). In many cases, the hub links to a high-speed connection and the spokes are Ethernet cards. Figure 9-14 illustrates a sample hub and spoke ring. Your network architecture may differ from the example.

Figure 9-14   A Hub and Spoke Ethernet circuit
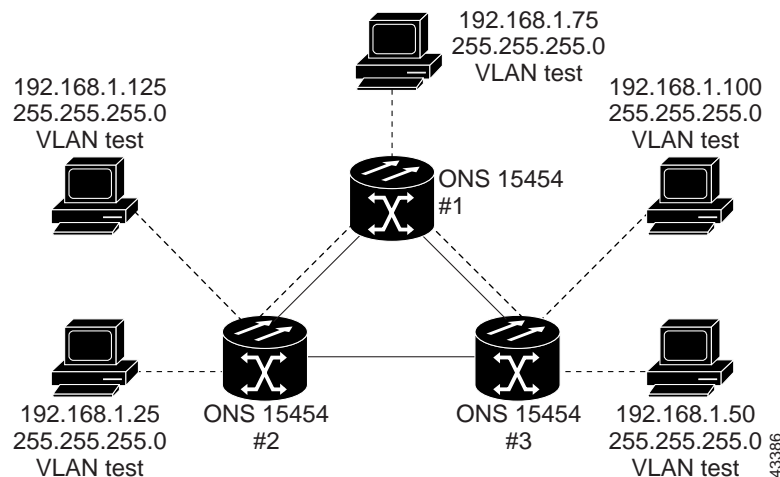
Procedure: Provision a Hub and Spoke Ethernet Circuit

Step 1   Display CTC for one of the ONS 15454 Ethernet circuit endpoints.

Step 2   Double-click the Ethernet card that will create the circuit.

Step 3   Click the **Provisioning** > **Card** tabs.

Step 4   Under Card Mode, check the **Single-card EtherSwitch** checkbox.

If **Single-card EtherSwitch** is not checked, check it and click **Apply**.

Step 5   Navigate to the other ONS 15454 endpoint and repeat Steps 2 – 4.

Step 6   Display the node view or network view.

Step 7   Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens (Figure 9-7 on page 9-8).

Step 8   In the Name field, type a name for the circuit.

Step 9   From the Type pull-down menu, choose **STS**.

> ✎
>
> **Note**   The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 10   Choose the size of the circuit from the Size pull-down menu.

Step 11   Verify that the **Bidirectional** checkbox is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box opens.

Step 12   From the Node menu, choose the circuit source.

Either end node can be the circuit source.

Step 13   From the Slot menu, choose the Ethernet card where you enabled the single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit Destination) dialog box opens.

Step 14   Choose the circuit destination from the Node menu.

Choose the node that is not the source.

Step 15   From the Slot menu, choose the Ethernet card where you enabled the single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box opens (Figure 9-8 on page 9-8).

Step 16   Create the VLAN:

   a.   Click the **New VLAN** tab.

     The Circuit Creation (Define New VLAN) dialog box opens (Figure 9-10 on page 9-11).

   b.   Assign an easily-identifiable name to your VLAN.

   c.   Assign a VLAN ID.

     This should be the next available number (between 2 and 4093) not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

   d.   Click **OK**.

   e.   Highlight the VLAN name and click the >> tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-11 on page 9-12).

Step 17   Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 18   Confirm that the following information about the point-to-point circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs that will be transported across this circuit
- ONS 15454 nodes included in this circuit

Note   If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information. You can also click **Finish**, delete the completed circuit, and start the procedure from the beginning.

Step 19   Click **Finish**. You must now provision the second circuit and attach it to the already-created VLAN.

Step 20   Log into the ONS 15454 Ethernet circuit endpoint for the second circuit.

Step 21   Double-click the Ethernet card that will create the circuit. The CTC card view displays.

Step 22   Click the **Provisioning > Card** tabs.

Step 23   Under Card Mode, check **Single-card EtherSwitch**.

If the **Single-card EtherSwitch** checkbox is not checked, check it and click **Apply**.

Step 24   Log into the other ONS 15454 endpoint for the second circuit and repeat Steps 21 – 23.

Step 25   Display the CTC node view.

Step 26   Click the **Circuits** tab and click **Create**.

Step 27   Choose **STS** from the Type pull-down menu.

> ✎
> **Note**   The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 28   Choose the size of the circuit from the Size pull-down menu.

Step 29   Verify that the **Bidirectional** checkbox is checked and click **Next**.

Step 30   Choose the circuit source from the Node menu and click **Next**.

Either end node can be the circuit source.

Step 31   Choose the circuit destination from the Node menu.

Choose the node that is not the source.

Step 32   From the Slot menu, choose the Ethernet card where you enabled the single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box is displayed.

Step 33   Highlight the VLAN that you created for the first circuit and click the >> tab to move the VLAN(s) from the Available VLANs column to the Selected VLANs column.

Step 34   Click **Next** and click **Finish**.

Step 35   You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the "Provision Ethernet Ports" procedure on page 9-3. For assigning ports to VLANs, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-24.

9.3.4 Ethernet Manual Cross-Connects

ONS 15454s require end-to-end CTC visibility between nodes for normal provisioning of Ethernet circuits. When other vendors' equipment sits between ONS 15454s, OSI/TARP- based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent this lack of continuous DCC, the Ethernet circuit must be manually cross connected to an STS channel riding through the non-ONS network. This allows an Ethernet circuit to run from ONS node to ONS node utilizing the non-ONS network.

> ✎
> **Note**   Provisioning manual cross-connects for *Multicard* Etherswitch circuits is a separate procedure from provisioning manual cross-connects for *Single-card* Etherswitch circuits. Both procedures are listed below.

Figure 9-15   Ethernet manual cross-connects

———— SONET
---------- Ethernet
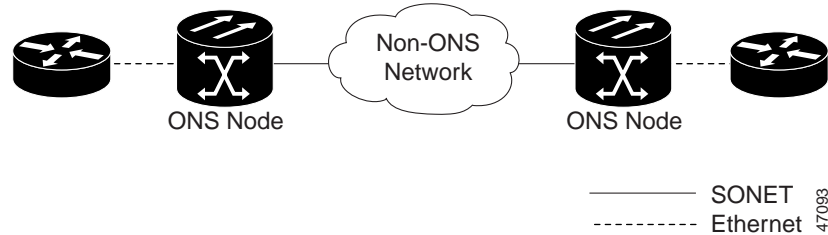
Procedure: Provision a Single-card EtherSwitch Manual Cross-Connect

Step 1   Display CTC for one of the ONS 15454 Ethernet circuit endpoints.

Step 2   Double-click one of the Ethernet cards that will carry the circuit.

Step 3   Click the **Provisioning** > **Card** tabs.

Step 4   Under Card Mode, verify that **Single-card EtherSwitch** is checked.

If the **Single-card EtherSwitch** is not checked, check it and click **Apply**.

Step 5   Display the node view.

Step 6   Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens (Figure 9-16).

Figure 9-16   Creating an Ethernet circuit
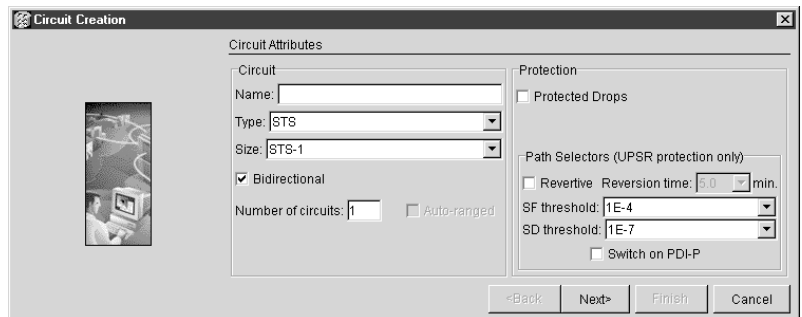
Step 7   In the Name field, type a name for the circuit.

Step 8   From the Type pull-down menu, choose **STS**.

Note   The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 9   Choose the size of the circuit from the Size pull-down menu.

The valid circuit sizes for an Ethernet Multicard circuit are STS-1, STS-3c and STS-6c.

Step 10   Verify that the **Bidirectional** checkbox is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box opens.

Step 11   From the Node menu, choose the current node as the circuit source.

Step 12   From the Slot menu, choose the Ethernet card that will carry the circuit and click **Next**.

The Circuit Creation (Circuit Destination) dialog box opens.

Step 13 From the Node menu, choose the current node as the circuit destination.

Step 14 From the Slot menu, choose the optical card that will carry the circuit.

Step 15 Choose the STS that will carry the circuit from the STS menu and click **Next**.

> ✎
>
> **Note** For Ethernet manual cross-connects, the same node serves as both source and destination.

The Circuit Creation (Circuit VLAN Selection) dialog box opens (Figure 9-11 on page 9-12).

Step 16 Create the VLAN:

a. Click the **New VLAN** tab.

The Circuit Creation (Define New VLAN) dialog box opens (Figure 9-10 on page 9-11).

b. Assign an easily-identifiable name to your VLAN.

c. Assign a VLAN ID.

The VLAN ID should be the next available number (between 2 and 4093) that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

d. Click **OK**.

Figure 9-17   Selecting VLANs
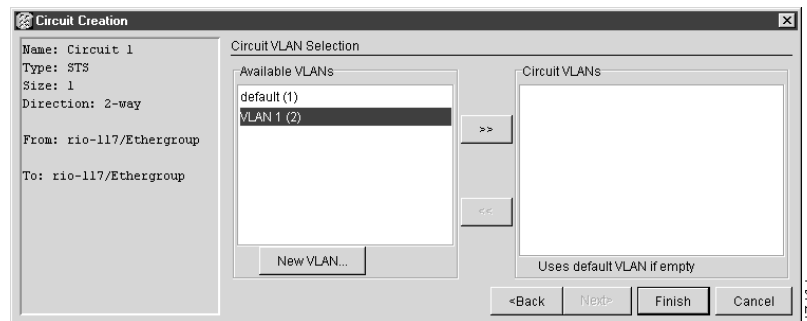
e. Highlight the VLAN name and click the arrow >> tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-17).

Step 17 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 18 Confirm that the following information is correct:

• Circuit name

• Circuit type

• Circuit size

• VLANs on this circuit

• ONS 15454 nodes included in this circuit

Note   If the circuit information is not correct use the Back button, then redo the procedure with the correct information. Alternately, you can click Finish, then delete the completed circuit and start the procedure from the beginning.

Step 19   Click **Finish**.

Step 20   You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the "Provision Ethernet Ports" procedure on page 9-3. For assigning ports to VLANs, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-24.

Step 21   After assigning the ports to the VLANs, repeat Steps 1 – 19 at the second ONS 15454 Ethernet manual cross-connect endpoint.

Note   The appropriate STS circuit must exist in the non-ONS 15454 equipment to connect the two STSs from the ONS 15454 Ethernet manual cross-connect endpoints.

Procedure: Provision a Multicard EtherSwitch Manual Cross-Connect

Step 1   Display CTC for one of the ONS 15454 Ethernet circuit endpoints.

Step 2   Double-click one of the Ethernet cards that will carry the circuit.

Step 3   Click the **Provisioning** > **Card** tabs.

Step 4   Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.

If the **Multicard-card EtherSwitch Group** is not checked, check it and click **Apply**.

Step 5   Display the node view.

Step 6   Repeat Steps 2 – 5 for any other Ethernet cards in the ONS 15454 that will carry the circuit.

Step 7   Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens (Figure 9-18).

Figure 9-18   Creating an Ethernet circuit
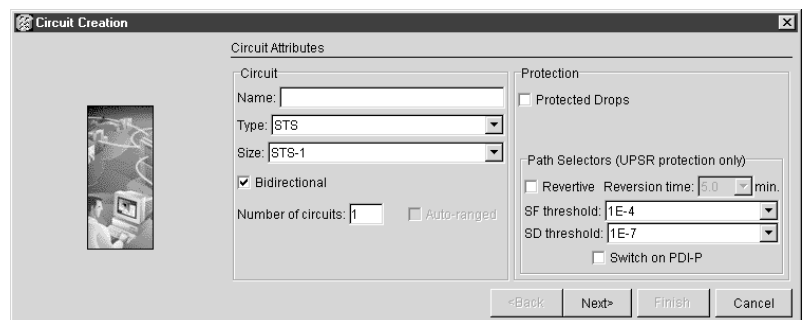
Step 8   In the Name field, type a name for the circuit.

Step 9   From the Type pull-down menu, choose **STS**.

✎

Note The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 10 Choose the size of the circuit from the Size pull-down menu.

The valid circuit sizes for an Ethernet Multicard circuit are STS-1, STS-3c and STS-6c.

Step 11 Verify that the **Bidirectional** checkbox is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box opens.

Step 12 From the Node menu, choose the current node as the circuit source.

Step 13 Choose **Ethergroup** from the Slot menu and click **Next**.

The Circuit Creation (Circuit Destination) dialog box opens.

Step 14 From the Node menu, choose the current node as the circuit destination.

Step 15 Choose the Ethernet card that will carry the circuit from the Slot menu and click **Next**.

✎

Note For the Ethernet manual cross-connect, the destination and source should be the same node.

The Circuit Creation (Circuit VLAN Selection) dialog box opens (Figure 9-11 on page 9-12).

Step 16 Create the VLAN:

a. Click the **New VLAN** tab.

The Circuit Creation (Define New VLAN) dialog box opens (Figure 9-10 on page 9-11).

b. Assign an easily-identifiable name to your VLAN.

c. Assign a VLAN ID.

The VLAN ID should be the next available number (between 2 and 4093) that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

d. Click **OK**.

Figure 9-19   Selecting VLANs
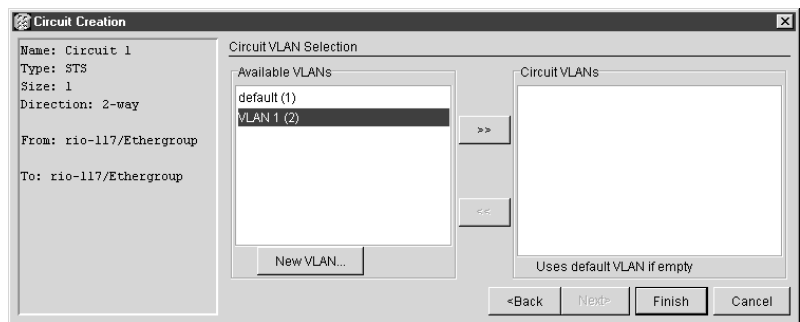
e. Highlight the VLAN name and click the arrow >> tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-19).

Step 17 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 18 Confirm that the following information is correct:

- Circuit name

- Circuit type

- Circuit size

- VLANs on this circuit

- ONS 15454 nodes included in this circuit

✎
Note   If the circuit information is not correct use the Back button, then redo the procedure with the correct information. Alternately, you can click Finish, then delete the completed circuit and start the procedure from the beginning.

Step 19   Click **Finish**.

You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the "Provision Ethernet Ports" procedure on page 9-3. For assigning ports to VLANs, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-24. Return to the following step after assigning the ports to VLANs.

Step 20   Highlight the circuit and click **Edit**.

The Edit Circuit dialog box opens.

Step 21   Click **Drops** and click **Create**.

The Define New Drop dialog box opens.

Step 22   From the Slot menu, choose the optical card that links the ONS 15454 to the non-ONS 15454 equipment.

Step 23   From the Port menu, choose the appropriate port.

Step 24   From the STS menu, choose the STS that matches the STS of the connecting non-ONS 15454 equipment.

Step 25   Click **OK**.

The Edit Circuit dialog box opens.

Step 26   Confirm the circuit information that displays in the Circuit Information dialog box and click **Close**.

Step 27   Repeat Steps 1 – 26 at the second ONS 15454 Ethernet manual cross-connect endpoint.

✎
Note   The appropriate STS circuit must exist in the non-ONS 15454 equipment to connect the two ONS 15454 Ethernet manual cross-connect endpoints.

9.4 VLAN Support

Users can provision up to 509 VLANs with the CTC software. Specific sets of ports define the broadcast domain for the ONS 15454. The definition of VLAN ports includes all Ethernet and packet-switched SONET port types. All VLAN IP address discovery, flooding, and forwarding is limited to these ports.

The ONS 15454 802.1Q-based VLAN mechanism provides logical isolation of subscriber LAN traffic over a common SONET transport infrastructure. Each subscriber has an Ethernet port at each site, and each subscriber is assigned to a VLAN. Although the subscriber's VLAN data flows over shared circuits, the service appears to the subscriber as a private data transport.

9.4.1 Q-Tagging (IEEE 802.1Q)

IEEE 802.1Q allows the same physical port to host multiple 802.1Q VLANs. Each 802.1Q VLAN represents a different logical network.

The ONS 15454 works with Ethernet devices that support IEEE 802.1Q and those that do not support IEEE 802.1Q. If a device attached to an ONS 15454 Ethernet port does not support IEEE 802.1Q, the ONS 15454 only uses Q-tags internally. The ONS 15454 associates these Q-tags with specific ports.

With Ethernet devices that do not support IEEE 802.1Q, the ONS 15454 takes non-tagged Ethernet frames that enter the ONS network and uses a Q-tag to assign the packet to the VLAN associated with the ONS network's ingress port. The receiving ONS node removes the Q-tag when the frame leaves the ONS network (to prevent older Ethernet equipment from incorrectly identifying the 8021.Q packet as an illegal frame). The ingress and egress ports on the ONS network must be set to Untag for the process to occur. Untag is the default setting for ONS ports. Example #1 in Figure 9-20 illustrates Q-tag use only within an ONS network.

With Ethernet devices that support IEEE 802.1Q, the ONS 15454 uses the Q-tag attached by the external Ethernet devices. Packets enter the ONS network with an existing Q-tag; the ONS 15454 uses this same Q-tag to forward the packet within the ONS network and leaves the Q-tag attached when the packet leaves the ONS network. Set both entry and egress ports on the ONS network to Tagged for this process to occur. Example #2 in Figure 9-20 illustrates the handling of packets that both enter and exit the ONS network with a Q-tag.

For more information about setting ports to Tagged and Untag, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-24.

Figure 9-20   A Q-tag moving through a VLAN

Data Flow

No tag   ONS 15454   Q-tag   ONS 15454   No tag

1. The ONS 15454 uses a Q-tag internally to deliver the frame to a specific VLAN.

The receiving ONS 15454 removes the Q-tag and forwards the frame to the specific VLAN.

Q-tag   ONS 15454   Q-tag   ONS 15454   Q-tag

2. The ONS 15454 receives a frame with a Q-tag and passes it on.

The receiving ONS 15454 receives a frame with a Q-tag and passes it on.

61075

9.4.2 Priority Queuing (IEEE 802.1Q)

Note   IEEE 802.1Q was formerly IEEE 802.1P.

Networks without priority queuing handle all packets on a first-in-first-out basis. Priority queuing reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. The ONS 15454 supports priority queuing. The ONS 15454 takes the eight priorities specified in IEEE 802.1Q and maps them to two queues (Table 9-5). Q-tags carry priority queuing information through the network.

The ONS 15454 uses a "leaky bucket" algorithm to establish a weighted priority (not a strict priority). A weighted priority gives high-priority packets greater access to bandwidth, but does not totally preempt low-priority packets. During periods of network congestion, roughly 70% of bandwidth goes to the high-priority queue and the remaining 30% goes to the low-priority queue. A network that is too congested will drop packets.

Table 9-5   Priority Queuing

User Priority	Queue	Allocated Bandwidth
0,1,2,3	Low	30%
4,5,6,7	High	70%

Figure 9-21   The priority queuing process

Data Flow

No priority — ONS 15454 — Priority — ONS 15454 — Priority tag removed

ONS 15454 maps a frame with port-based priority using a Q-tag.

The receiving ONS 15454 removes the Q-tag and forwards the frame.

Priority — ONS 15454 — Same priority — ONS 15454 — Priority

ONS 15454 uses a Q-tag to map a frame with priority and forwards it on.

The receiving ONS 15454 receives the frame with a Q-tag and forwards it.

9.4.3 VLAN Membership

This section explains how to provision Ethernet ports for VLAN membership. For initial port provisioning (prior to provisioning VLAN membership) see the "Port Provisioning for Ethernet Cards" section on page 9-3.

Procedure: Provision Ethernet Ports for VLAN Membership

The ONS 15454 allows you to configure the VLAN membership and Q-tag handling of individual Ethernet ports.

Step 1   Display the CTC card view for the Ethernet card.

Step 2   Click the **Provisioning > VLAN** tabs (Figure 9-22).

Figure 9-22   Configuring VLAN membership for individual Ethernet ports
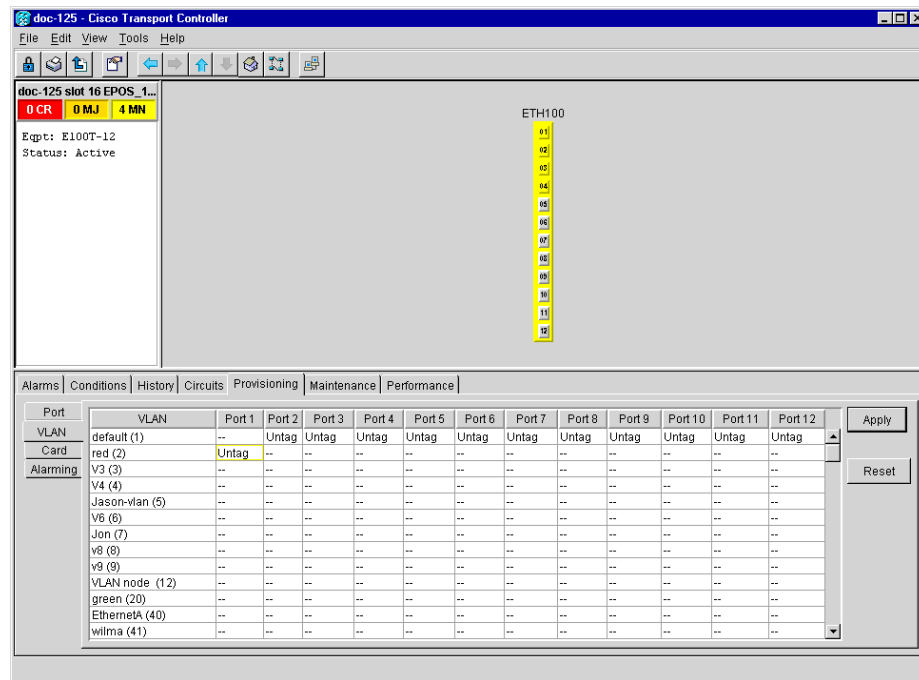
Step 3   To put a port in a VLAN, click the port and choose either Tagged or Untag. Figure 9-22 on page 9-25 shows Port 1 in the red VLAN and Port 2 through Port 12 in the default VLAN. Table 9-6 shows valid port settings.

If a port is a member of only one VLAN, go to that VLAN's row and choose **Untag** from the Port column. Choose **--** for all the other VLAN rows in that Port column. The VLAN with **Untag** selected can connect to the port, but other VLANs cannot access that port.

If a port is a trunk port, it connects multiple VLANs to an external device, such as a switch, which also supports trunking. A trunk port must have tagging (802.1Q) enabled for all the VLANs that connect to that external device. Choose **Tagged** at all VLAN rows that need to be trunked. Choose **Untag** at one or more VLAN rows in the trunk port's column that do not need to be trunked, for example, the default VLAN. Each Ethernet port must attached to at least one untagged VLAN.

Step 4   After each port is in the appropriate VLAN, click **Apply**.

Table 9-6   Port Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15454 will tag ingress frames and strip tags from egress frames.
Tagged	The ONS 15454 will handle ingress frames according to VLAN ID; egress frames will not have their tags removed.

Note   If Tagged is chosen, the attached external devices must recognize IEEE 802.1Q VLANs.

Note   Both ports on individual E1000-2/E1000-2-G cards cannot be members of the same VLAN.

9.5 Spanning Tree (IEEE 802.1D)

The Cisco ONS 15454 operates spanning tree protocol (STP) according to IEEE 802.1D when an Ethernet card is installed. STP operates over all packet-switched ports including Ethernet and SONET ports. On Ethernet ports, STP is disabled by default but may be enabled with a check box under the **Provisioning** > **Port** tabs at the card-level view. On SONET interface ports, STP activates by default and cannot be disabled.

The Ethernet card can enable STP on the Ethernet ports to allow redundant paths to the attached Ethernet equipment. STP spans cards so that both equipment and facilities are protected against failure.

STP detects and eliminates network loops. When STP detects multiple paths between any two network hosts, STP blocks ports until only one path exists between any two network hosts (Figure 9-23). The single path eliminates possible bridge loops. This is crucial for shared packet rings, which naturally include a loop.

Figure 9-23   An STP blocked path
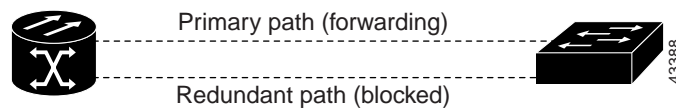
To remove loops, STP defines a tree that spans all the switches in an extended network. STP forces certain redundant data paths into a standby (blocked) state. If one network segment in the STP becomes unreachable, the spanning-tree algorithm reconfigures the spanning-tree topology and reactivates the blocked path to reestablish the link. STP operation is transparent to end stations, which do not discriminate between connections to a single LAN segment or to a switched LAN with multiple segments. The ONS 15454 supports one STP instance per circuit and a maximum of eight STP instances per ONS 15454.

9.5.1 Multi-Instance Spanning Tree and VLANs

The ONS 15454 can operate multiple instances of STP to support VLANs in a looped topology. You can dedicate separate circuits across the SONET ring for different VLAN groups (i.e., one for private TLS services and one for Internet access). Each circuit runs its own STP to maintain VLAN connectivity in a multi-ring environment.

Procedure: Enable Spanning Tree on Ethernet Ports

Step 1   Display the CTC card view.

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

Step 3   In the left-hand column, find the applicable port number and check the **Stp Enabled** checkbox to enable STP for that port.

Step 4   Click **Apply**.

9.5.2 Spanning Tree Parameters

Default spanning tree parameters are appropriate for most situations. Contact the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 before you change the default STP parameters.

At the node view, click the **Maintenance** > **Etherbridge > Spanning Trees** tabs to view spanning tree parameters.

Table 9-7   Spanning Tree Parameters

BridgeID	ONS 15454 unique identifier that transmits the configuration bridge protocol data unit (BPDU); the bridge ID is a combination of the bridge priority and the ONS 15454 MAC address
TopoAge	Amount of time in seconds since the last topology change
TopoChanges	Number of times the spanning tree topology has been changed since the node booted up
DesignatedRoot	Identifies the spanning tree's designated root for a particular spanning tree instance
RootCost	Identifies the total path cost to the designated root
RootPort	Port used to reach the root
MaxAge	Maximum time that received-protocol information is retained before it is discarded
HelloTime	Time interval, in seconds, between the transmission of configuration BPDUs by a bridge that is the spanning tree root or is attempting to become the spanning tree root
HoldTime	Minimum time period, in seconds, that elapses during the transmission of configuration information on a given port
ForwardDelay	Time spent by a port in the listening state and the learning state

9.5.3 Spanning Tree Configuration

To view the spanning tree configuration, at the node view click the **Provisioning** tab and **Etherbridge** subtab.

Table 9-8   Spanning Tree Configuration

Column	Default Value	Value Range
Priority	32768	0 - 65535
Bridge max age	20 seconds	6 - 40 seconds
Bridge Hello Time	2 seconds	1 - 10 seconds
Bridge Forward Delay	15 seconds	4 - 30 seconds

9.5.4 Spanning Tree Map

The Circuit screen shows forwarding spans and blocked spans on the spanning tree map.

Procedure: View the Spanning Tree Map

Step 1   On the circuit screen (Figure 9-24), double-click an Ethernet circuit.

Figure 9-24   The spanning tree map on the circuit screen
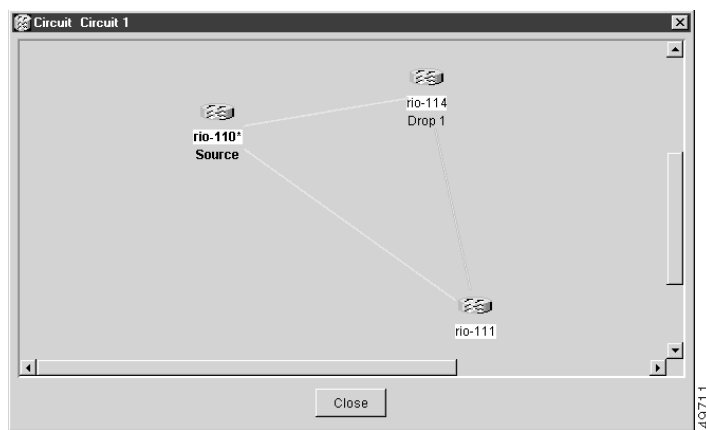
Note   Green represents forwarding spans and purple represents blocked (protect) spans. If you have a packet ring configuration, at least one span should be purple.

9.6 Ethernet Performance and Maintenance Screens

CTC provides Ethernet performance information, including line-level parameters, the amount of port bandwidth used, and historical Ethernet statistics. CTC also includes spanning tree information, MAC address information, and the amount of circuit bandwidth used. To view spanning tree information, see the "Spanning Tree Parameters" section on page 9-27.

9.6.1 Statistics Screen

The Ethernet statistics screen lists Ethernet parameters at the line level. Table 9-9 defines the parameters. Display the CTC card view for the Ethernet card and click the **Performance** > **Statistics** tabs to display the screen.

Table 9-9   Ethernet Parameters

Parameter	Meaning
Link Status	Indicates whether link integrity is present; up means present, and down means not present
RX Packets	Number of packets received since the last counter reset
RX Bytes	Number of bytes received since the last counter reset
TX Packets	Number of packets transmitted since the last counter reset
TX Bytes	Number of bytes transmitted since the last counter reset
RX Total Errors	Total number of receive errors
RX FCS	Number of packets with a Frame Check Sequence (FCS) error. FCS errors indicate Frame corruption during transmission
RX Alignment	Number of packets with alignment errors; alignment errors are received incomplete frames
RX Runts	Number of packets received that are less than 64 bytes in length
RX Giants	Number of packets received that are greater than 1518 bytes in length for untagged interfaces and 1522 bytes for tagged interfaces
TX Collisions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions
TX Excessive	Number of consecutive collisions
TX Deferred	Number of packets deferred

9.6.2 Line Utilization Screen

The Line Utilization screen shows the percentage of line, or port, bandwidth used and the percentage used in the past. Display the CTC card view and click the **Performance** and **Utilization** tabs to display the screen. From the Interval menu, choose a time segment interval. Valid intervals are 1 minute, 15 minutes, 1 hour, and 1 day. Press **Refresh** to update the data.

Note   Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

9.6.3 History Screen

The Ethernet History screen lists past Ethernet statistics. At the CTC card view, click the **Performance** tab and **History** subtab to view the screen. Choose the appropriate port from the Line menu and the appropriate interval from the Interval menu. Press **Refresh** to update the data. Table 9-9 defines the listed parameters.

9.6.4 MAC Table Screen

A MAC address is a hardware address that physically identifies a network device. The ONS 15454 MAC table, also known as the MAC forwarding table, will allow you to see all the MAC addresses attached to the enabled ports of an Ethernet card or an Ethernet Group. This includes the MAC address of the network device attached directly to the port and any MAC addresses on the network linked to the port. The MAC addresses table lists the MAC addresses stored by the ONS 15454 and the VLAN, Slot/Port/STS, and circuit that links the ONS 15454 to each MAC address (Figure 9-25).

Figure 9-25   MAC addresses recorded in the MAC table
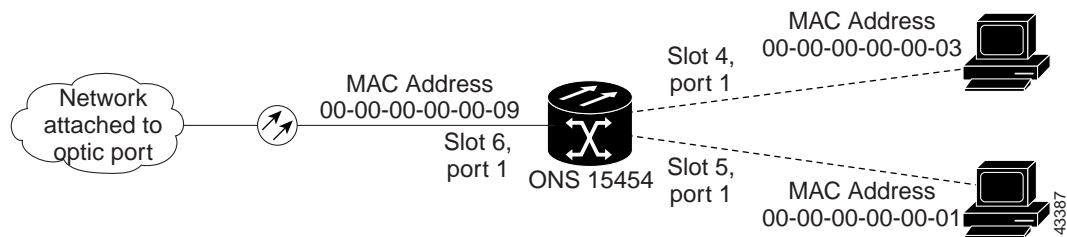
Procedure: Retrieve the MAC Table Information

Step 1   Click the **Maintenance > EtherBridge** > **MAC Table** tabs.

Step 2   Select the appropriate Ethernet card or Ethergroup from the Layer 2 Domain pull-down menu.

Step 3   Click **Retrieve** for the ONS 15454 to retrieve and display the current MAC IDs.

Note   Click **Clear** to clear the highlighted rows and click **Clear All** to clear all displayed rows.

9.6.5 Trunk Utilization Screen

The Trunk Utilization screen is similar to the Line Utilization screen, but Trunk Utilization shows the percentage of circuit bandwidth used rather than the percentage of line bandwidth used. Click the **Maintenance > Ether Bridge > Trunk Utilization** tabs to view the screen. Choose a time segment interval from the Interval menu.

Note   The percentage shown is the average of ingress and egress traffic.

9.7 Remote Monitoring Specification Alarm Thresholds

The ONS 15454 features Remote Monitoring (RMON) that allows network operators to monitor the health of the network with a Network Management System (NMS). For a detailed description of the ONS SNMP implementation, see Chapter 11, "SNMP."

One of the ONS 15454's RMON MIBs is the Alarm group. The alarm group consists of the alarmTable. An NMS uses the alarmTable to find the alarm-causing thresholds for network performance. The thresholds apply to the current 15-minute interval and the current 24-hour interval. RMON monitors several variables, such as Ethernet collisions, and triggers an event when the variable crosses a threshold during that time interval. For example, if a threshold is set at 1000 collisions and 1001 collisions occur during the 15-minute interval, an event triggers. CTC allows you to provision these thresholds for Ethernet statistics.

Note   You can find performance monitoring specifications for all other cards in the *Cisco ONS 15454 Troubleshooting and Maintenance Guide.*

Note   The following tables define the variables you can provision in CTC. For example, to set the collision threshold, choose **etherStatsCollisions** from the Variable menu.

Table 9-10   Ethernet Threshold Variables (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
dot3statsAlignmentErrors	Number of frames with an alignment error, i.e., the length is not an integral number of octets and the frame cannot pass the Frame Check Sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, i.e., there is an integral number of octets, but an incorrect Frame Check Sequence (FCS)
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrame	Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	Number of times the first transmission was delayed because the medium was busy
dot3StatsLateCollision	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsExcessiveCollision	Number of frames where transmissions failed because of excessive collisions
etherStatsJabbers	Total number of Octets of data (including bad packets) received on the network

Table 9-10   Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 – 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 – 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 – 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 – 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 – 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length

Procedure: Creating Ethernet RMON Alarm Thresholds

Step 1   Display the CTC node view.

Step 2   Click the **Provisioning** > **Etherbridge > Thresholds** tabs.

Step 3   Click **Create**.

The Create Ether Threshold dialog box opens.

Figure 9-26   Creating RMON thresholds

Step 4   From the Slot menu, choose the appropriate Ethernet card.

Step 5   From the Port menu, choose the Port on the Ethernet card.

Step 6   From the Variable menu, choose the variable. Table 9-10 lists and defines the Ethernet Threshold Variables available in this field.

Step 7   From Alarm Type, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8   From the Sample Type pull-down menu, choose either **Relative** or **Absolute**. **Relative** restricts the threshold to use the number of occurrences in the user-set sample period. **Absolute** sets the threshold to use the total number of occurrences, regardless of any time period.

Step 9   Type in an appropriate number of seconds for the Sample Period.

Step 10   Type in the appropriate number of occurrences for the Rising Threshold.

> **Note**   For a rising type of alarm to fire, the measured value must shoot from below the falling threshold to above the rising threshold. For example, if a network is running below a falling threshold of 400 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, these occurrences fire an alarm.

Step 11   Type in the appropriate number of occurrences for the Falling Threshold. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15 minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 12   Click the **OK** button to complete the procedure.

Alarm Monitoring and Management

This chapter explains how to manage alarms with Cisco Transport Controller (CTC), which includes

- Viewing alarms
- Viewing history
- Viewing conditions
- Viewing alarm counts on the front-panel LCD
- Creating and managing alarm profiles
- Suppressing alarms

To troubleshoot specific alarms, see the *Cisco ONS 15454 Troubleshooting and Maintenance Guide.*

10.1 Overview

The Cisco Transport Controller (CTC) detects and reports SONET alarms generated by the Cisco ONS 15454 and the larger SONET network. You can use CTC to monitor and manage alarms at a card, node, or network levels and view alarm counts on the LCD front panel. Default alarm severities conform to the Telcordia GR-253 standard, but you can reset severities to customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard Telcordia categories employed by ONS nodes, see the *Cisco ONS 15454 Troubleshooting and Maintenance Guide.*

✎ **Note** ONS 15454 alarms can also be monitored and managed through TL1 or a network management system (NMS).

10.2 Viewing ONS 15454 Alarms

At the card, node, or network-level CTC view, click the Alarms tab to display the alarms for that card, node or network. Table 10-1 lists the tab's column headings and the information recorded in each column.

Table 10-1   Alarms Column Descriptions

Column	Information Recorded
New	Indicates a new alarm. To change this status check either the **Synchronize Alarms** or **Delete Cleared Alarms** checkbox, or reset the active TCC+ card.
Date	Date and time of the alarm
Node	Node where the alarm occurred (displays in network view only)
Object	TL1 access identifier (AID) for the alarmed object
Type	Card type in this slot
Slot	Slot where the alarm occurred (displays in network and node view only)
Port	Port where the alarm occurred
Sev	Severity level: CR (critical), MJ (major), MN (minor), NA (not alarmed), NR (not reported)
ST	Status: R (raised), C (clear), T (transient)
SA	When checked, indicates a service-affecting alarm
Cond	The error message/alarm name. These are defined alphabetically in the alarm chapter of the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.
Description	Description of the alarm
Num	A count of incrementing alarm messages (this column is hidden by default)
Ref	The reference number assigned to a cleared alarm (this column is hidden by default).

Figure 10-1   Viewing alarms in the CTC node view

Alarms display in one of five background colors, listed in Table 10-2, to quickly communicate the alarm severity. Events, conditions, and cleared alarms are also color coded. Conditions and events display in the History or Conditions tab.

Table 10-2   Color Codes for Alarms, Conditions, and Events

Color	Description
Red	Critical Alarm (CR)
Orange	Major Alarm (MJ)
Yellow	Minor Alarm (MN)
Magenta	Event (NA)
Blue	Condition (NR)
White	Cleared alarm or event (CL)

10.2.1 Controlling Alarm Display

You can control the display of the alarms on the Alarms tab. Table 10-3 shows the actions you can perform from the Alarms tab.

Table 10-3   Alarm Display

Button	Action
Synchronize Alarms	Updates the alarm display; although CTC displays alarms in real time, the Synchronize Alarms button allows you to verify the alarm display. This is particularly useful during provisioning or troubleshooting.
Delete Cleared Alarms	Deletes alarms that have been cleared
AutoDelete Cleared Alarms	If checked, CTC automatically deletes cleared alarms
Show Events (NA)	If checked, CTC shows alarms and not alarmed (NA) events or Conditions. Not-alarmed events do not require action and normally display only under the Conditions tab.

10.2.2 Viewing Alarm-Affected Circuits

User can view which ONS 15454 circuits are affected by a specific alarm. Figure 10-6 illustrates the Select Affected Circuits option.

Figure 10-2   Selecting the Affected Circuits option
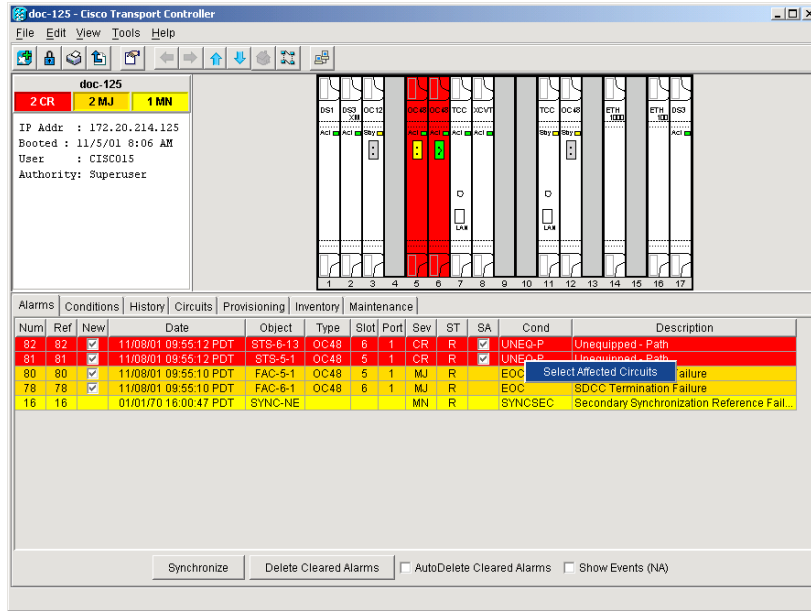
Procedure: View Affected Circuits for a Specific Alarm

Step 1   Under the Alarm tab, right-click the Cond column of an active alarm.

The Select Affected Circuit dialog appears.

Step 2   Left-click **Select Affected Circuits**.

The Circuits screen appears with affected circuits highlighted (Figure 10-3.)

Figure 10-3   Highlighted circuit appears
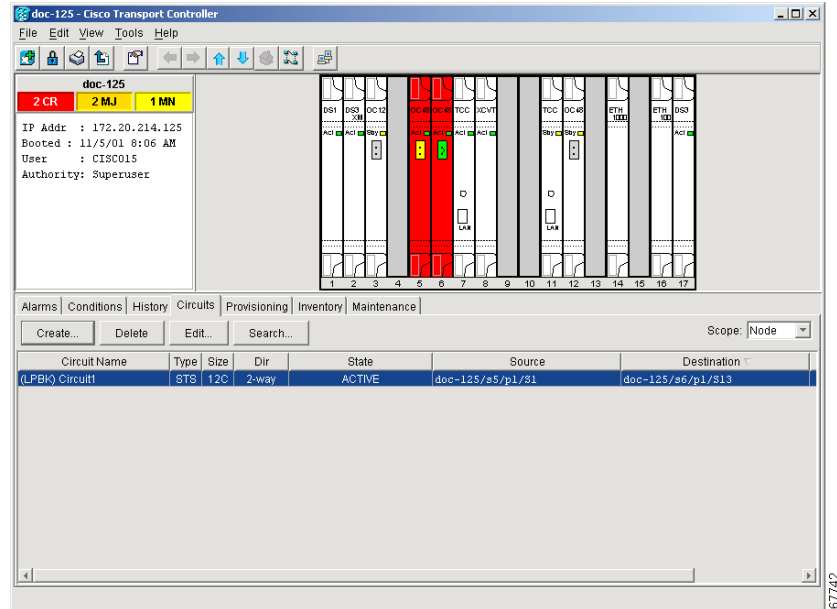
10.2.3 Conditions Tab

The Conditions tab displays retrieved fault conditions. A fault is a problem detected by ONS 15454 hardware or software. When a fault occurs and continues for a minimum time period, it raises a fault condition, which is a flag showing whether this particular fault currently exists on the ONS 15454. Fault conditions include all existing conditions, whether the severity is that of an alarm (Critical, Major or Minor) or a condition (Not Reported or Non Alarmed.) See the trouble notifications information in the *Cisco ONS 15454 Troubleshooting and Maintenance Guide* for more information on the classifications for alarms and conditions.

Displaying all existing fault conditions is helpful while troubleshooting the ONS 15454. The Conditions tab does not adhere to Telcordia guidelines for reporting alarms, events, and conditions. Alarm reporting under the Alarms tab is Telcordia-compliant.

10.2.3.1 Retrieve and Display Conditions

At the node view, click the Conditions tab and the Retrieve Condition**s** button to retrieve the current set of all existing fault conditions from the ONS 15454, as maintained by the alarm manager. Users can perform the same operation at the card view for the card level and at the network view for the network level.

Figure 10-4   Viewing fault conditions retrieved under the Conditions tabs
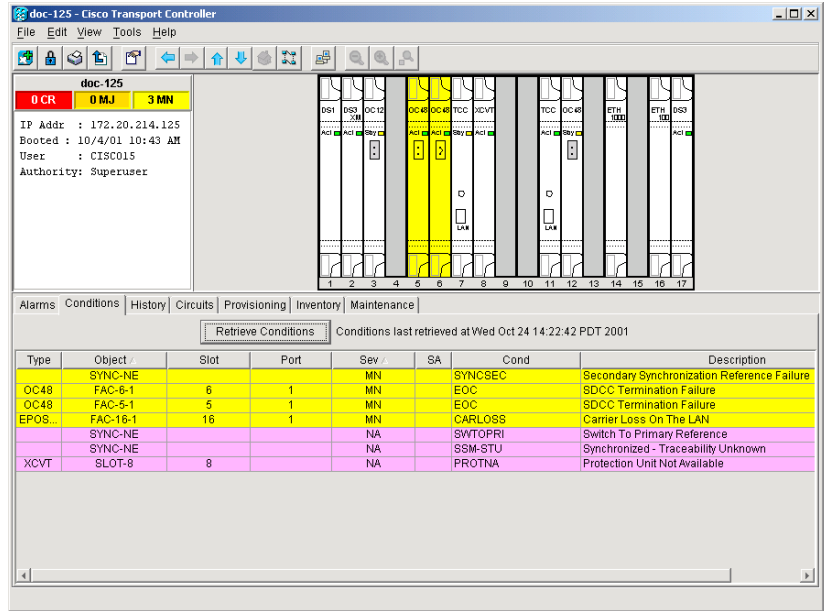
10.2.3.2 Conditions Column Descriptions

Table 10-4 lists the tab's column headings and the information recorded in each column.

Table 10-4   Conditions Columns Description

Column	Information Recorded
Node	Node where the condition occurred (displays in network view only)
Object	TL1 access identifier (AID) for the alarmed object
Type	Card type in this slot
Slot	Slot where the condition occurred (displays in network and node view only)
Port	Port where the condition occurred
Sev	Severity level: CR (critical), MJ (major), MN (minor), NA (not alarmed), NR (not reported)
SA	When checked, indicates a service-affecting alarm
Cond	The condition name
Description	Description of the condition

10.2.4 Viewing History

The History tab displays historical alarm data. It also displays events, which are non-alarmed activities such as timing changes and threshold crossings. For example, protection switching events or performance monitoring threshold crossings appear here. The History tab presents two alarm history views:

- The Session subtab (Figure 10-5) presents alarms and events that have occurred during the current CTC session.

- The Node subtab shows the alarms and events that occurred at the node since the CTC software installation. The ONS 15454 can store up to 640 critical alarms, 640 major alarms, 640 minor alarms, and 256 events. When the limit is reached, the ONS 15454 discards the oldest alarms and events.

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

Figure 10-5   Viewing all alarms reported for the current session

10.2.5 Viewing Alarms on the LCD

The Critical, Major and Minor alarm LEDs on the fan-tray assembly front panel indicate whether a critical, major, or minor alarm is present anywhere on the ONS 15454. These LEDs are viewable through the front door so that you can quickly determine if any alarms are present on the node. These LEDs are independent of the Card, Port, and Status indicators on the LCD.

When you press the Slot, Status, or Port buttons on the LCD to toggle to a certain slot or port, the LCD displays the Critical, Major, or Minor alarm count for the selected slot and port. Figure 10-6 illustrates the LCD panel.

Figure 10-6   The LCD panel
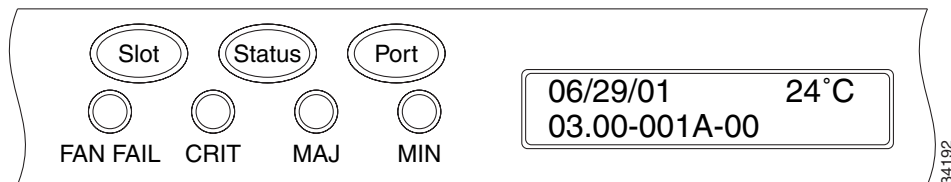
Procedure: View Alarm Counts on a Specific Slot and Port

Step 1 Use the Slot button to toggle to the desired slot number.

Set the slot number to Node to see a summary of alarms for the node.

Step 2 Use the Port button to toggle to the port.

Step 3 Press the Status button to display the slot and port.

Figure 10-6 shows the LCD panel.

Note A blank LCD results when the fuse on the AIP board is blown. If this occurs, call Cisco TAC at 1-877-323-7368.

10.3 Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15454 nodes. A profile you create can be applied to any node on the network. Alarm profiles must be stored on a node before they can be applied to a node, card, or port. CTC can store up to ten alarm profiles; eight are available for custom use and two are reserved. CTC can load an unlimited number of alarm profiles that have been stored on a node, server, or CTC workstation.

The two reserved profiles include the default profile, which sets severities to standard Telcordia GR-253 settings, and the Inherited profile, which sets all alarm severities to transparent (TR). If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm's severity at the next level. For example, a card with an Inherited alarm profile copies the severities used by the node that contains the card. The Inherited profile is not available at the node level.

10.3.1 Creating and Modifying Alarm Profiles

Alarm profiles are created at the network view using the Provisioning > Alarm Profiles tabs
(Figure 10-7.) A default alarm profile (in the Default column) is pre-provisioned for every alarm. After
loading the Default profile on the node, you can use the Clone feature to create new profiles based on
the default alarm profile. After the new profile is created, the Alarm Profiles tab shows the default profile
and the new profile.

Figure 10-7   Alarm profiles screen showing the default profiles of the listed alarms
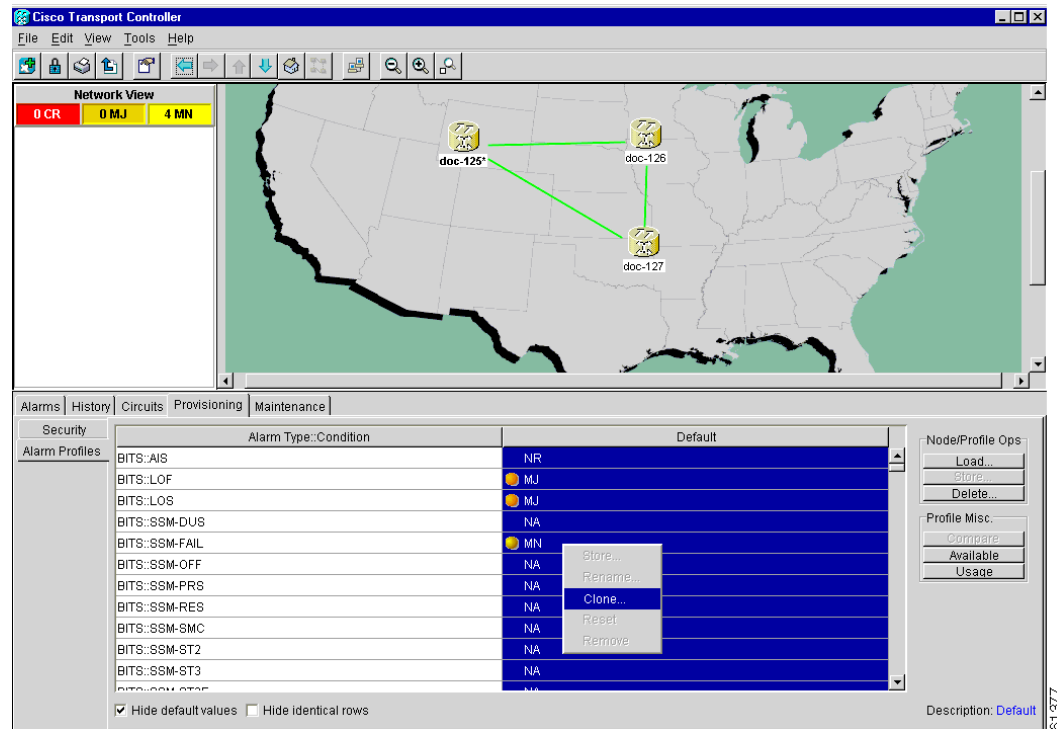
Procedure: Create an Alarm Profile

Step 1   Display the CTC network view.

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

Step 3   Click **Load**.

Step 4   Highlight the node name you are logged into under *Node Names* and highlight **Default** under *Profile Names*.

Step 5   Click **OK**.

Step 6   Right-click anywhere in the Default column to display the Profile Editing menu.

Step 7   Choose **Clone** from the menu. (You can also clone any other profiles that appear under the Available button, except Inherited.)

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

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

Step 9 Click **OK**.

A new alarm profile (named in Step 5) is created. This profile duplicates the severities of the default profile and is added as a new column on the far right-hand side.

Step 10 Modify (customize) the alarm profile:

a. In the new alarm profile column, click in a row that contains the alarm severity you want to change.

b. From the menu, select the desired severity.

c. Repeat Steps a and b for each alarm that needs to be changed.

d. After you have assigned the properties to your new alarm profile, click the new alarm profile to highlight it and click the **Store** button.

e. In the Store Profile(s) dialog box, select a node or nodes where the profile will be stored and/or specify a file on the workstation.

f. Click **OK**.

Note You can also clone alarm profiles shown under the Available tab.

10.3.1.1 Alarm Profile Menus

The Alarm Profiles tab displays two menus on the right-hand side, Node/Profile Ops and Profile Misc, which include six alarm profile buttons. Table 10-5 lists and describes each of the alarm profile buttons.

Table 10-5 Alarm Profile Buttons

Heading	Button	Description
Node Profile Ops	Load	Loads a profile to either a node or a file
	Store	Saves profiles on a node (or nodes) or in a file
	Delete	Deletes profiles from a node
Profile Misc.	Compare	Displays differences between alarm profiles (i.e. individual alarms that are not configured equivalently between profiles)
	Available	Displays all of the profiles available on each node
	Usage	Displays all of the entities present in the network and which profile(s) each is using

10.3.1.2 Alarm Profile Editing

Table 10-6 lists and describes the five profile editing options available when you right-click in an alarm profile column.

Table 10-6   Alarm Profile Editing Options

Button	Description
Store	Saves a profile in either a node or a file
Rename	Changes a profile name
Clone	Creates a new profile that contains the same alarm severity settings as the highlighted profile (the profile being cloned)
Reset	Restores a profile to the state of that profile before it was last applied or to the state when it was first loaded, if it has not yet been applied
Remove	Removes a profile from the table editor

10.3.1.3 Alarm Severity Option

You change or assign alarm severity using a menu. To view this menu, right-click the alarm you want to change in its alarm profile column. Seven severity levels appear for the alarm:

- CR: Critical
- MJ: Major
- MN: Minor
- NR: Not reported
- NA: Not alarmed
- TR: Transparent
- UNSET: Unset/Unknown (not normally used)

Transparent and Unset only appear in alarm profiles; they do not appear when you view alarms, history, or conditions.

10.3.1.4 Row Display Options

In addition to the alarm profile tabs, the Alarm Behavior tab displays two checkboxes at the bottom of the screen: *Hide default values* and *Hide identical rows*. The *Hide default values* checkbox highlights alarms with non-default severities by clearing alarm cells with default severities. The *Hide identical rows* checkbox hides rows of alarms that contain the same severity for each profile.

10.3.2 Applying Alarm Profiles

In CTC card view, the Alarm Behavior subtab displays the alarm profiles of the selected card. In node view, the Alarm Behavior subtab displays alarm profiles for the node. Alarms form a hierarchy. A node-level alarm profile applies to all cards in the node, except those that have their own profiles. A card-level alarm profile applies to all ports on the card, except those that have their own profiles.

At the node level, you may apply profile changes on a card-by-card basis or set a profile for the entire node. Figure 10-8 shows the profile of a DS-1 card being changed to Inherited at the node view.

Figure 10-8   Node view of a DS1 alarm profile

At the card level, you can apply profile changes on a port-by-port basis or set all ports on that card at once. Figure 10-9 shows the affected DS-1 card; notice the CTC shows Parent Card Profile: Inherited.

Figure 10-9   Card view of a DS1 alarm profile

Procedure: Apply an Alarm Profile at the Card View

Step 1   In CTC, display the card view of the desired card.

Step 2   Click the **Provisioning** > **Alarm Behavior** tabs.

Step 3   To apply profiles on a port-to-port basis:

   a. Click the appropriate row under the **Profile** column for the port desired.

   b. Choose the appropriate Profile.

   c. Click **Apply**. (Multiple port profiles can be selected before clicking **Apply**.)

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

   a. Click the **Force all ports to profile** menu arrow at the bottom of the screen.

   b. Choose the appropriate Profile.

   c. Click **Force (still need to "Apply")**

   d. Click **Apply**.

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

Procedure: Apply an Alarm Profile at the Node View

Step 1   In CTC, display the node view.

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

Step 3   To apply profiles on a card basis:

   a. Click the **Profile** column for the card desired.

   b. Choose the appropriate Profile.

   c. Click **Apply**. (Multiple card profiles can be selected before clicking **Apply**.)

Step 4   To apply the profile to an entire node:

   a. Click the **Node Profile** menu arrow.

   b. Choose the appropriate Profile.

   c. Click **Apply**.

Note   The Port Overrides column at the node view reads true when additional profiles are available and false when only the inherited profile is available.

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

10.4 Suppressing Alarms

Suppressing alarms causes alarms to appear under the Conditions tab instead of the Alarms tab. It prevents alarms from appearing on CTC Alarm or History tabs or in any other clients. The suppressed alarms behave like conditions, which have their own non-reporting (NR) severities. Under the Conditions tab, the suppressed alarms appear with their alarm severity, color code, and service-affecting status.

Note   Use alarm suppression with caution. If multiple CTC/TL1 sessions are open, you will suppress the alarms in all other open sessions.

Procedure: Suppressing Alarms

Step 1   At either the card view or node view, click the **Provisioning** > **Alarm Behavior** tabs.

At the card level, you can suppress alarms on a port-by-port basis. At the node level, you can suppress alarms on a card-by-card basis or the entire node.

Step 2   Check the **Suppress Alarms** box for the card or port you want to suppress. Figure 10-10 shows the Suppress Alarms box.

Figure 10-10 The suppress alarms checkbox

Step 3   Click the **Apply** button.

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

Note   When you uncheck the Suppress Alarms checkbox and click Apply, the node sends out autonomous messages to raise any actively suppressed alarms.

■ Suppressing Alarms

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454.

11.1 SNMP Overview

SNMP is an application-layer communication protocol that allows network devices to exchange management information. SNMP enables network administrators to manage network performance, find and solve network problems, and plan network growth.

The ONS 15454 uses SNMP to provide asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) MIBs to convey node-level inventory, fault, and performance management information for generic read-only management of DS-1, DS-3, SONET, and Ethernet technologies. SNMP allows limited management of the ONS 15454 by a generic SNMP manager, for example HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert.

The Cisco ONS 15454 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both versions share many features, but SNMPv2c includes additional protocol operations. This chapter describes both versions and explains how to configure SNMP on the ONS 15454. Figure 11-1 illustrates a basic network managed by SNMP.

Figure 11-1   A basic network managed by SNMP
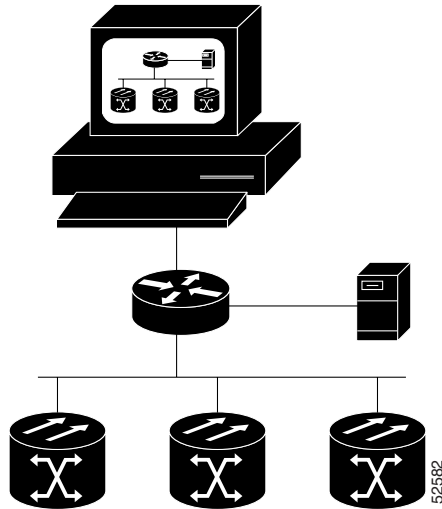
11.2 SNMP Basic Components

An SNMP-managed network consists of three primary components: managed devices, agents, and management systems. A managed device is a network node that contains an SNMP agent and resides on an SNMP-managed network. Managed devices collect and store management information and use SNMP to make this information available to management systems that use SNMP. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and network elements such as an ONS 15454.

An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the MIB, which is the repository for device parameter and network data. The agent can also send traps, or notification of certain events, to the manager. Figure 11-2 illustrates these SNMP operations.

Figure 11-2   An SNMP agent gathering data from an MIB and sending traps to the manager
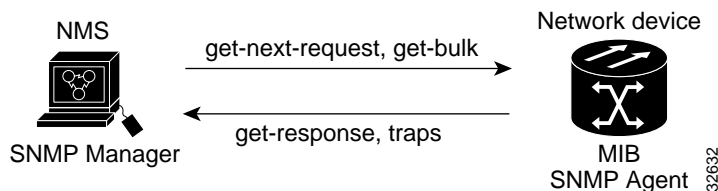
A management system such as HP OpenView executes applications that monitor and control managed devices. Management systems provide the bulk of the processing and memory resources required for network management. One or more management systems must exist on any managed network. Figure 11-3 illustrates the relationship between the three key SNMP components.

Figure 11-3   Example of the primary SNMP components

Managed Devices
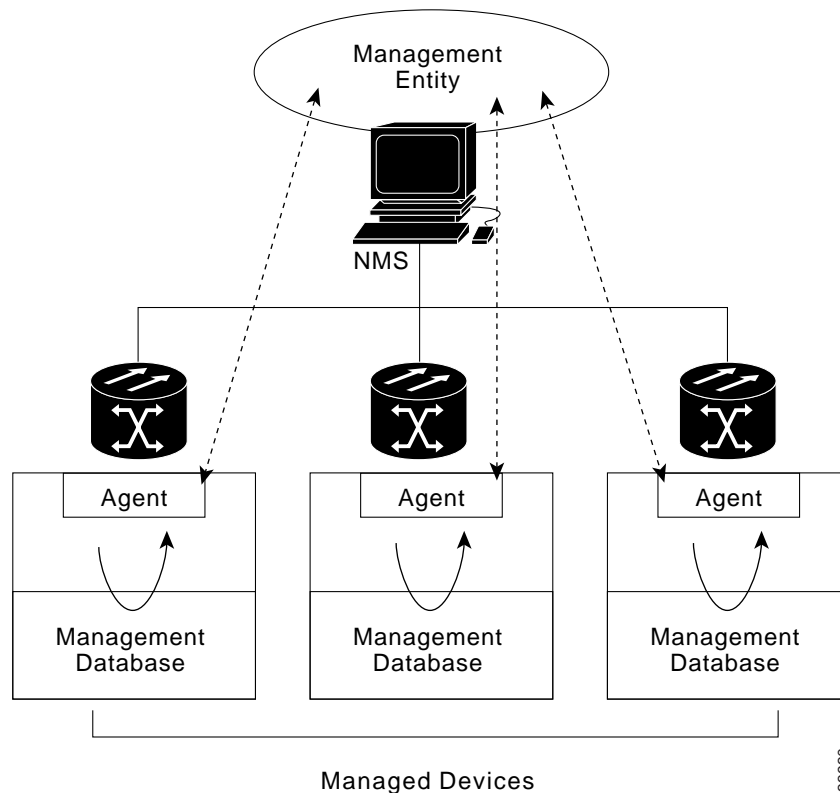
11.3 SNMP Support

The ONS 15454 supports SNMP v1 and v2c traps and get requests. The SNMP MIBs in the ONS 15454 define alarms, traps, and status. Through SNMP, NMS applications can query a management agent using a supported MIB. The functional entities include Ethernet switches and SONET multiplexers.

Procedure: Set Up SNMP Support

Step 1   Display the CTC node view.

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

Step 3   Click **Create** at the bottom of the screen.

The Create SNMP Trap Destination dialog box opens (Figure 11-4).

For a description of SNMP traps, see the "SNMP Traps" section on page 11-6.

Figure 11-4   Setting up SNMP

Step 4   Type the IP address of your NMS in the IP Address field.

Step 5   Type the SNMP community name in the Community Name field.

For a description of SNMP community names, see the "SNMP Community Names" section on page 11-8.

Note   The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the NMS.

Note   The default UDP port for SNMP is 162.

Step 6   Set the Trap Version field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

Step 7   Set your maximum traps per second in the Max Traps per Second field.

Note   The Max Traps per Second is the maximum number of traps per second that will be sent to the SNMP manager. If the field is set to 0, there is no maximum and all traps are sent.

Step 8   Click **OK**.

SNMP settings are now configured. To view SNMP information for each node, highlight the node IP address in the Trap Destinations area of the Trap Destinations screen (Figure 11-5).

Figure 11-5   Viewing trap destinations
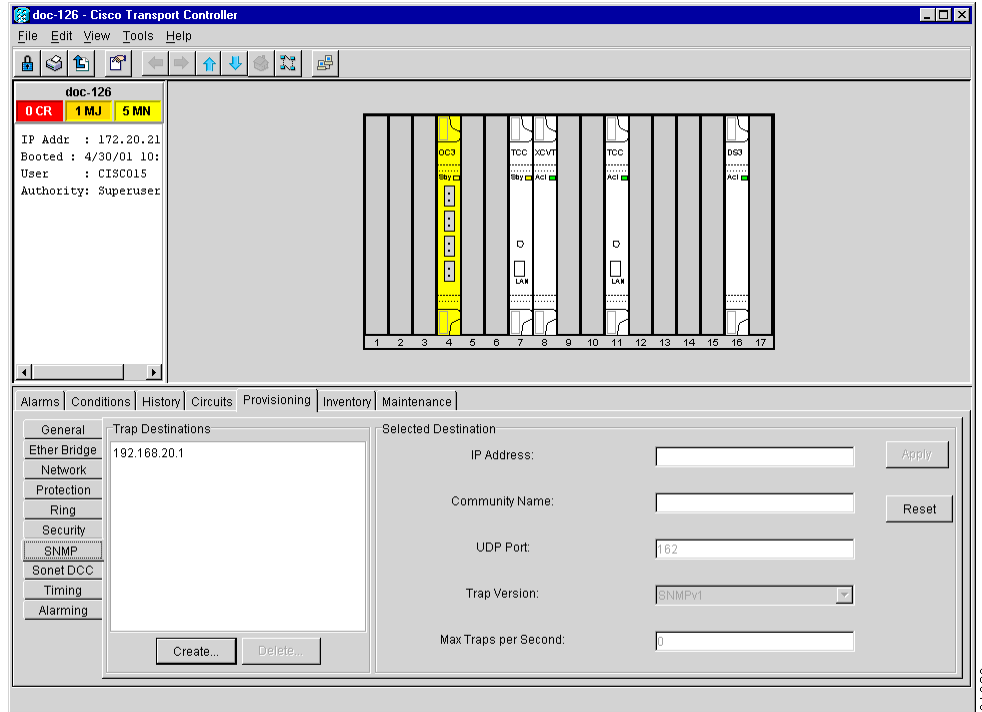
11.4 SNMP Management Information Bases

A management information base (MIB) is a hierarchically-organized collection of information.
Network-management protocols, such as SNMP, gain access to MIBs. MIBs consist of managed objects
and are identified by object identifiers.

The ONS 15454 SNMP agent communicates with an SNMP management application using SNMP
messages. Table 11-1 describes these messages.

Table 11-1   SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	The reply to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS

Table 11-1   SNMP Message Types

Operation	Description
get-bulk-request	Similar to a get-next-request, but this operation fills the get-response with up to the max-repetition number of get-next interactions
trap	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that an event has occurred

A managed object (sometimes called a MIB object) is one of any specific characteristics of a managed device. Managed objects consist of one or more object instances (variables).

The ONS 15454 MIBs are included on the software CD that ships with the ONS 15454. Compile these MIBs in the following order. If you do not follow the order, one or more MIB files might not compile.

1. CERENT-GLOBAL-REGISTRY.mib

2. CERENT-TC.mib

3. CERENT-454.mib

4. CERENT-GENERIC.mib

If you cannot compile the ONS 15454 MIBs, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Table 11-2   IETF Standard MIBs Implemented in the ONS 15454 SNMP Agent

RFC#	Module Name	Title/Comments
1213 +1907	RFC1213-MIB, SNMPV2-MIB	MIB-II from RFC1213 with enhancement from RFC1907 for v2
1493	BRIDGE-MIB	Bridge/Spanning Tree (SNMPv1 MIB)
1757	RMON-MIB	Remote monitoring (RMON) Ethernet
2737	ENTITY-MIB	Entity MIB using SMI v2 (version II)
2233	IF-MIB	Interface evolution (enhances MIB-II)
2358	Etherlike-MIB	Ethernet-like interface (SNMPv2 MIB)
2495	DS1-MIB	DS-1/E1
2496	DS3-MIB	DS-3/E3
2558	SONET-MIB	SONET
2674	P-BRIDGE-MIB, Q-BRIDGE-MIB	P-Bridge and Q-Bridge MIB

11.5 SNMP Traps

The ONS 15454 can receive SNMP requests from a number of SNMP managers and send traps to ten trap receivers. The ONS 15454 generates all alarms and events as SNMP traps.

The ONS 15454 generates traps containing an object ID that uniquely identifies the alarm. An entity identifier uniquely identifies the entity that generated the alarm (slot, port, STS, VT, BLSR, STP, etc.). The traps give the severity of the alarm (critical, major, minor, event, etc.) and indicate whether the alarm

is service affecting or non-service affecting. The traps also contain a date/time stamp that shows the date and time the alarm occurred. The ONS 15454 also generates a trap for each alarm when the alarm condition clears.

Each SNMP trap contains ten variable bindings listed in Table 11-4.

Table 11-3   SNMP Trap Variable Bindings

Number	Name	Description
1	cerentGenericAlarmTable	This table holds all the currently-raised alarms. When an alarm is raised, it appears as a new entry in the table. When an alarm is cleared, it is removed from the table and all the subsequent entries move up by one row.
2	cerentGenericAlarmIndex	This variable uniquely identifies each entry in an alarm table. When an alarm in the alarm table clears, the alarm indexes change for each alarm located subsequent to the cleared alarm.
3	cerentGenericAlarmObjectType	This variable provides the entity type that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
4	cerentGenericAlarmSlotNumber	This variable indicates the slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
5	cerentGenericAlarmPortNumber	This variable provides the port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
6	cerentGenericAlarmLineNumber	This variable provides the object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
7	cerentGenericAlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of the objects in each table; if the alarm is interface related, this is the index of the interfaces in the interface table.
8	cerentGenericAlarmType	This variable provides the exact alarm type.
9	cerentGenericAlarmState	This variable specifies alarm severity and service-affecting status. Severities are minor, major and critical. Service- affecting statuses are service-affecting and non-service affecting.
10	cerentGenericAlarmTimeStamp	This variable gives the time when the alarm occurred. The value is the number of the ticks that has lapsed since 1/1/1970.

The ONS 15454 supports the generic and IETF traps listed in Table 11-4.

Table 11-4   Traps Supported in the ONS 15454

Trap	From RFC#	Description
ColdStart	RFC1213-MIB	Agent up, cold start
WarmStart	RFC1213-MIB	Agent up, warm start
AuthenticationFailure	RFC1213-MIB	Community string does not match
NewRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree
TopologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking
EntConfigChange	RFC2037/ ENTITY-MIB	The entLastChangeTime value has changed
ds1xLineStatusChange	RFC2495/ DS1-MIB	A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (ex. DS-3), no traps for the DS-1 are sent.
dsx3LineStatusChange	RFC2496/ DS3-MIB	A dsx3LineStatusLastChange trap is sent when the value of an instance of dsx3LineStatus changes. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (ex. DS-1), no traps for the lower-level are sent.
risingAlarm	RFC1757/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC1757/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

11.6 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination dialog box in CTC (see the "SNMP Support" section on page 11-3). In effect, SNMP considers any request valid that uses a community name matching a community name on the list of provisioned SNMP trap destinations. Otherwise, SNMP considers the request invalid and drops it.

If an SNMP request contains an invalid community name, the request silently drops and the MIB variable (snmpInBadCommunityNames) increments. All MIB variables managed by the agent grant access to all SNMP requests containing a validated community name.

11.7 SNMP Remote Network Monitoring

The ONS 15454 incorporates Remote Network Monitoring (RMON) to allow network operators to monitor the ONS 15454 E10/100-4 cards. For more information on Ethernet RMONs, see "Remote Monitoring Specification Alarm Thresholds" section on page 9-30. This feature is not apparent to the

typical CTC user, because RMON interoperates with an NMS. However, with CTC you can provision the RMON alarm thresholds (see the "SNMP Remote Network Monitoring" section on page 11-8). CTC also monitors the five RMON groups implemented by the ONS 15454.

ONS 15454 RMON implementation is based on the IETF-standard MIB Request for Comment (RFC)1757. The ONS 15454 implements five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

11.7.1 Ethernet Statistics Group

The Ethernet Statistics group contains the basic statistics for each monitored subnetwork in a single table named etherstats.

11.7.2 History Control Group

The History Control group defines sampling functions for one or more monitor interfaces. RFC 1757 defines the historyControlTable.

11.7.3 Ethernet History Group

The ONS 15454 implements the etherHistoryTable as defined in RFC 1757, within the bounds of the historyControlTable.

11.7.4 Alarm Group

The Alarm group consists of a single alarm table. This table provides the network performance alarm thresholds for the network management application. With CTC, you can provision the thresholds in the table.

11.7.5 Event Group

The Event group consists of two tables, eventTable and logTable. The eventTable is read-only. The ONS 15454 implements the logTable as specified in RFC 1757.

Circuit Routing

This appendix provides an in-depth explanation of ONS 15454 circuit routing and VT tunneling in mixed protection or meshed environments, such as the one shown in Figure A-1. For circuit creation and provisioning procedures, see Chapter 6, "Circuits and Tunnels."

Figure A-1   Multiple protection domains
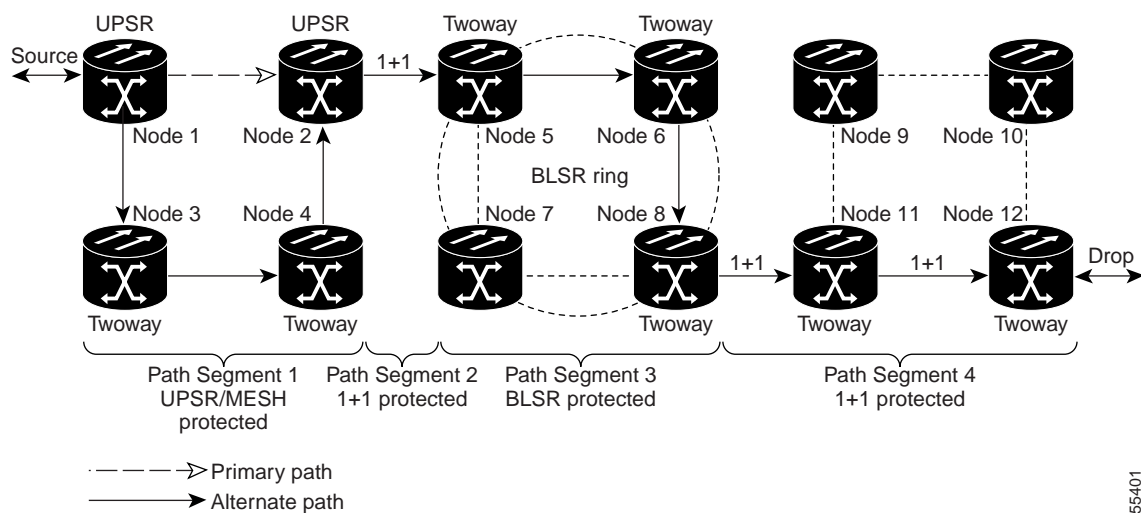
Automatic Circuit Routing

If you select automatic routing during circuit creation, Cisco Transport Controller (CTC) routes the circuit by dividing the entire circuit route into segments based on protection domains. For unprotected segments of protected circuits, CTC finds an alternate route to protect the segment in a virtual UPSR fashion. Each path segment is a separate protection domain, and each protection domain is protected in a specific fashion (virtual UPSR, BLSR, or 1+1).

Cisco ONS 15454 Installation and Operations Guide

Circuit Routing Characteristics

The following list provides principles and charactistics of automatic circuit routing:

- Circuit routing tries to use the shortest path within the user-specified or network-specified constraints. VT tunnels are preferable for VT circuits because VT tunnels are considered shortcuts when CTC calculates a circuit path in path-protected mesh networks.

- If you do not choose Fully Path Protected during circuit creation, circuits may still contain protected segments. Because circuit routing always selects the shortest path, one or more links and/or segments may have some protection. CTC does not look at link protection while computing a path for unprotected circuits.

- Circuit routing will not use links that are down. If you want all links to be considered for routing, do not create circuits when a link is down.

- Circuit routing computes the shortest path when you add a new drop to an existing circuit. It tries to find a shortest path from the new drop to any nodes on the existing circuit.

- If the network has a mixture of VT-capable nodes and nodes that are not VT capable, depending on the route found, CTC will automatically force creation of a VT tunnel. Otherwise, CTC asks you whether a VT tunnel is needed.

Bandwidth Allocation and Routing

Within a given network, CTC will route circuits on the shortest possible path between source and destination based on the circuit attributes, such as protection and type. CTC will consider using a link for the circuit only if the link meets the following requirements:

- The link has sufficient bandwidth to support the circuit

- The link does not change the protection characteristics of the path

- The link has the required time slots to enforce the same time slot restrictions for BLSR

If CTC cannot find a link that meets these requirements, it displays an error

The same logic applies to VT circuits on VT tunnels. Circuit routing typically favors VT tunnels because, based on topology maintained by circuit routing, VT tunnels are shortcuts between a given source and destination. If the VT tunnel in the route is full (no more bandwidth), CTC asks whether you want to create an additional VT tunnel.

Secondary Sources and Drops

CTC supports secondary sources and drops. Secondary sources and drops typically interconnect two "foreign" networks, as shown in Figure A-2. Traffic is protected while it goes through a network of ONS 15454s.

Figure A-2   Secondary sources and drops
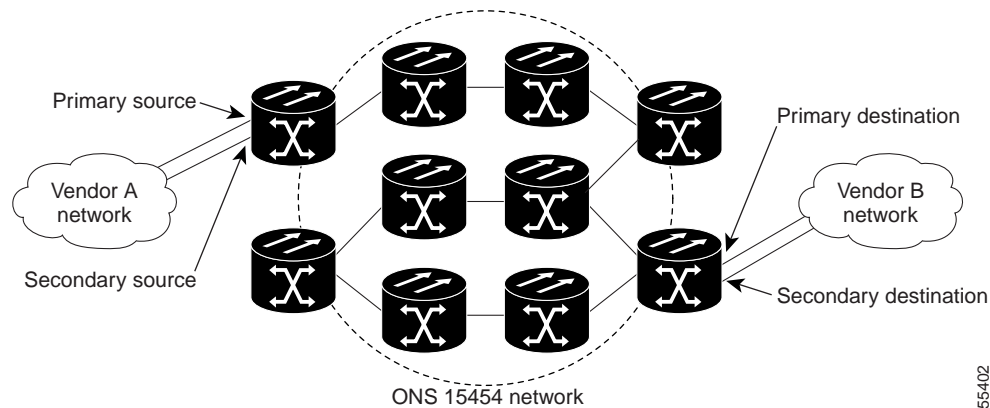
Several rules apply to secondary sources and drops:

- CTC does not allow a secondary destination for unidirectional circuits because you can always specify additional destinations (drops) after you create the circuit

- Primary and secondary sources should be on the same node

- Primary and secondary destinations should be on the same node

- The sources and drops cannot be DS-3, DS3XM, or DS-1 based STS-1s or VTs

- Secondary sources and destinations are permitted only for regular STS/VT connections (not for VT tunnels and multicard EtherSwitch circuits)

- For point-to-point (straight) Ethernet circuits, only SONET STS endpoints can be specified as multiple sources or drops

For bidirectional circuits, CTC creates a UPSR connection at the source node that allows traffic to be selected from one of the two sources on the ONS 15454 network. If you check the Fully Path Protected option during circuit creation, traffic is protected within the ONS 15454 network. At the destination, another UPSR connection is created to bridge traffic from the ONS 15454 network to the two destinations. A similar but opposite path exists for the reverse traffic flowing from the destinations to the sources.

For unidirectional circuits, a UPSR drop-and-continue connection is created at the source node.

Manual Circuit Routing

Routing circuits manually allows you to:

- Choose a specific path, not just the shortest path chosen by automatic routing

- Choose a specific STS/VT on each link along the route

- Create a shared packet ring for Multicard EtherSwitch circuits

- Choose a protected path for Multicard EtherSwitch circuits, allowing virtual UPSR segments

CTC imposes the following rules on manual routes:

- All circuits, except Multicard EtherSwitch circuits in a shared packet ring, should have links with a direction that flows from source to destination. This is true for Multicard EtherSwitch circuits that are not in a shared packet ring (see Figure A-1).

- If you enabled Fully Path Protected, choose a diverse protect (alternate) path for every unprotected segment (see Figure A-3).

Figure A-3   Alternate paths for virtual UPSR segments
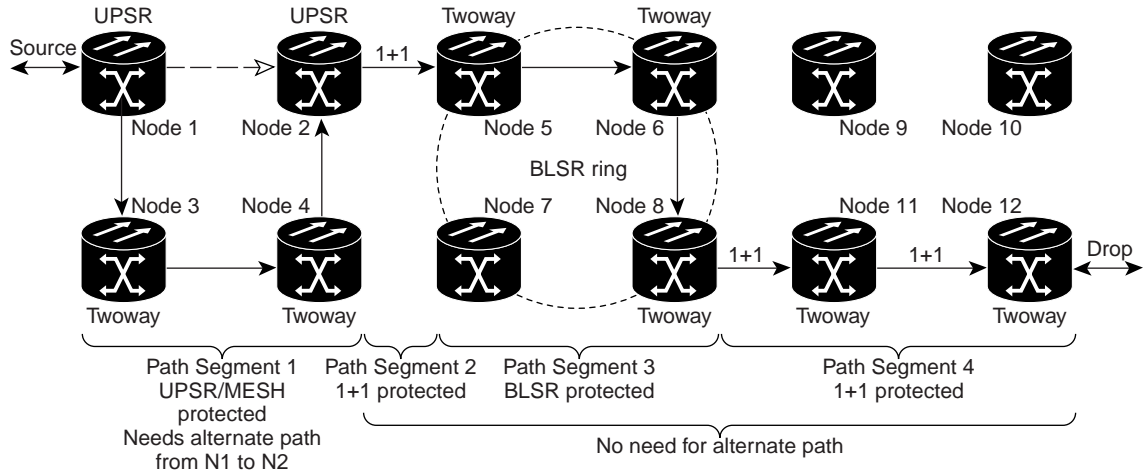
- For Multicard EtherSwitch circuits, the Fully Path Protected option is ignored.
- For a node that has a UPSR selector based on the links chosen, the input links to the UPSR selectors cannot be 1+1 or BLSR protected (see Figure A-4). The same rule applies at the UPSR bridge.

Figure A-4   Mixing 1+1 or BLSR protected links with a UPSR
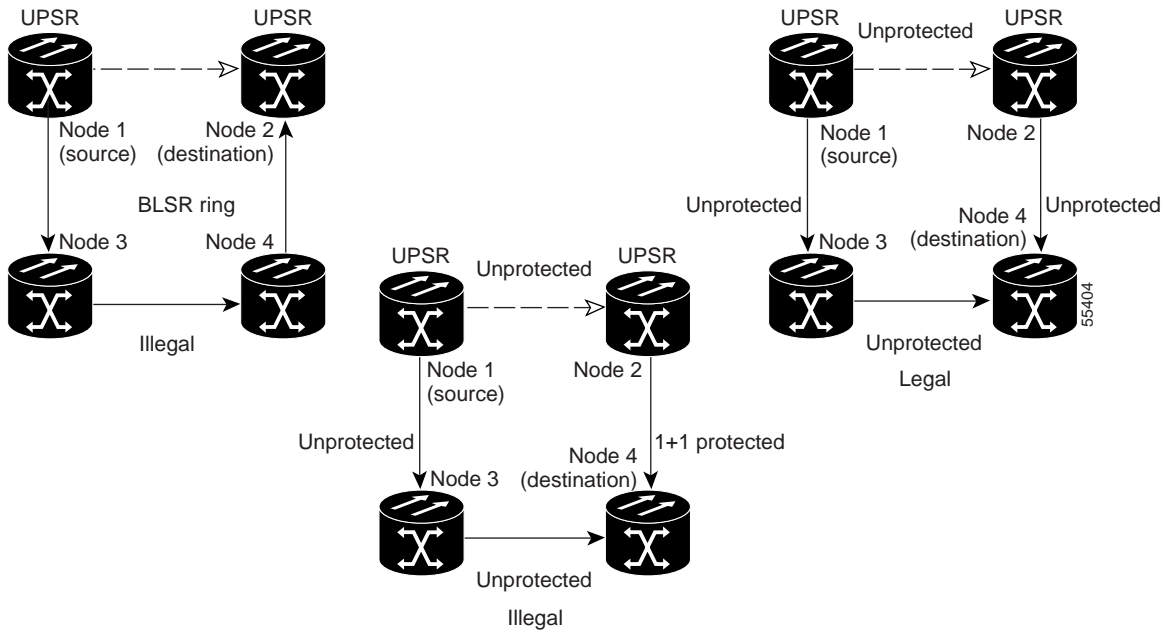
- Choose the links of Multicard EtherSwitch circuits in a shared packet ring to route from source to destination back to source (see Figure A-5). Otherwise, a route (set of links) chosen with loops is invalid.

Figure A-5   Ethernet shared packet ring routing
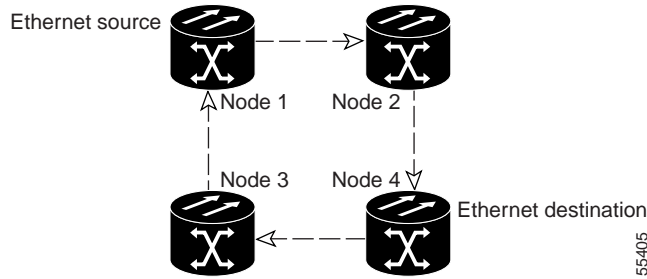
- Multicard EtherSwitch circuits can have virtual UPSR segments if the source or destination is not in the UPSR domain. This restriction also applies after circuit creation; therefore if you create a circuit with UPSR segments, Ethernet node drops cannot exist anywhere on the UPSR segment (see Figure A-6).

Figure A-6   Ethernet and UPSR
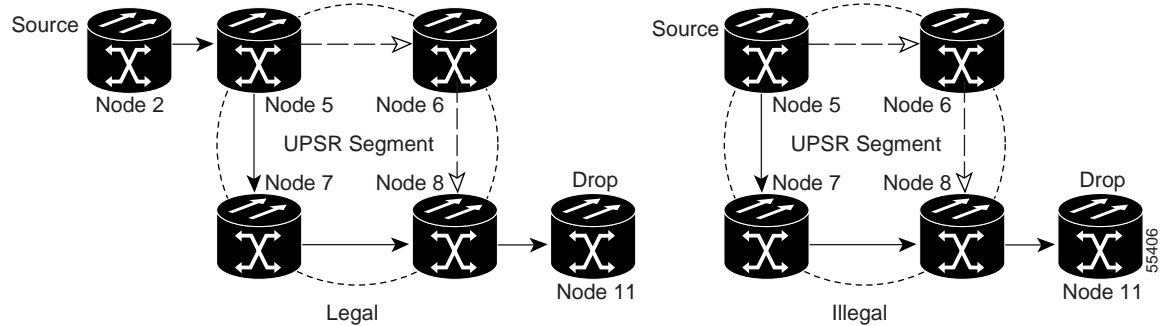
- VT Tunnels cannot be an endpoint of a UPSR segment. A UPSR segment endpoint is where the UPSR selector resides.

If Fully Path Protected is chosen, CTC verifies that the route selection is protected at all segments. A route can have multiple protection domains with each domain protected by a different mechanism.

The following tables summarize the available node connections. Any other combination is invalid and will generate an error.

Table A-1   Bidirectional STS/VT/Regular Multicard EtherSwitch/Point-to-Point (straight) Ethernet Circuits

# of Inbound Links	# of Outbound Links	# of Sources	# of Drops	Connection Type
-	2	1	-	UPSR
2	-	-	1	UPSR
2	1	-	-	UPSR
1	2	-	-	UPSR
1	-	-	2	UPSR
-	1	2	-	UPSR
2	2	-	-	Double UPSR
2	-	-	2	Double UPSR

Table A-1   Bidirectional STS/VT/Regular Multicard EtherSwitch/Point-to-Point (straight) Ethernet Circuits (continued)

# of Inbound Links	# of Outbound Links	# of Sources	# of Drops	Connection Type
-	2	2	-	Double UPSR
1	1	-	-	Two Way
0 or 1	0 or 1	Ethernet Node Source	-	Ethernet
0 or 1	0 or 1	-	Ethernet Node Drop	Ethernet

Table A-2   Unidirectional STS/VT Circuit

# of Inbound Links	# of Outbound Links	# of Sources	# of Drops	Connection Type
1	1	-	-	One way
1	2	-	-	UPSR Head End
-	2	1	-	UPSR Head End
2	-	-	1+	UPSR drop and continue

Table A-3   Multicard Group Ethernet Shared Packet Ring Circuit

# of Inbound Links	# of Outbound Links	# of Sources	# of Drops	Connection Type
At intermediate nodes only				
2	1	-	-	UPSR
1	2	-	-	UPSR
2	2	-	-	Double UPSR
1	1	-	-	Two way
At source or destination nodes only				
1	1	-	-	Ethernet

Table A-4   Bidirectional VT Tunnels

# of Inbound Links	# of Outbound Links	# of Sources	# of Drops	Connection Type
At intermediate nodes only				
2	1	-	-	UPSR
1	2	-	-	UPSR
2	2	-	-	Double UPSR
1	1	-	-	Two way
At source nodes only				
-	1	-	-	VT tunnel end point

Table A-4   Bidirectional VT Tunnels (continued)

# of Inbound Links	# of Outbound Links	# of Sources	# of Drops	Connection Type
At destination nodes only				
1	-	-	-	VT tunnel end point

Although virtual UPSR segments are possible in VT Tunnels, VT tunnels are still considered unprotected. If you need to protect VT circuits either use two independent VT tunnels that are diversely routed or use a VT tunnel that is routed over only 1+1 or BLSR (or a mix) links.

Constraint-Based Circuit Routing

When you create circuits, you can choose Fully Protected Path to protect the circuit from source to destination. The protection mechanism used depends on the path CTC calculates for the circuit. If the network is comprised entirely of BLSR and/or 1+1 links, or the path between source and destination can be entirely protected using 1+1 and/or BLSR links, no PPMN (virtual UPSR) protection is used.

If virtual UPSR (PPMN) protection is needed to protect the path, set the level of node diversity for the PPMN portions of the complete path on the Circuit Creation dialog box:

- Required—Ensures that the primary and alternate paths of each PPMN domain in the complete path have a diverse set of nodes.

- Desired—CTC looks for a node diverse path; if a node diverse path is not available, CTC finds a link diverse path for each PPMN domain in the complete path.

- Don't Care—Creates only a link diverse path for each PPMN domain

When you choose automatic circuit routing during circuit creation, you have the option to require and/or exclude nodes and links in the calculated route. You can use this option to:

- Simplify manual routing, especially if the network is large and selecting every span is tedious. You can select a general route from source to destination and allow CTC to fill in the route details.

- Balance network traffic; by default CTC chooses the shortest path, which can load traffic on certain links while other links are either free or less used. By selecting a required node and/or a link, you force the CTC to use (or not use) an element, resulting in more effecent use of network resources.

CTC considers required nodes and links to be an ordered set of elements. CTC treats the source nodes of every required link as required nodes. When CTC calculates the path, it makes sure the computed path traverses the required set of nodes and links and does not traverse excluded nodes and links.

The required nodes and links constraint is only used during the primary path computation and only for PPMN domains/segments. The alternate path is computed normally; CTC uses excluded nodes/links when finding all primary and alternate paths on PPMNs.

Cisco ONS 15454 Installation and Operations Guide

Regulatory and Compliance Requirements

This appendix lists customer, industry, and government requirements met by the Cisco ONS 15454. Installation warnings are also included.

Regulatory Compliance

Table B-1   Standards

Discipline	Country	Specification
EMC Emissions	Canada	ICES-003 Issue 3, 1997
		Telcordia GR-1089-CORE
	USA	Telcordia GR-1089-CORE
		FCC Part 15 Class A
	EU & Asia	EN55022 Class A-readiness
EMC Immunity	Canada	Telcordia GR-1089-CORE
	USA	Telcordia GR-1089-CORE
	Global	Telcordia GR-1089-CORE
		WorldCom Electrostatic Discharge immunity
		EN61000-4-2 Electrostatic Discharge immunity
		EN61000-4-3 Radiated immunity
		EN61000-4-4 Electrical fast transient/burst immunity
		EN61000-4-6 Conducted immunity
Safety	Canada	CAN/CSA-C22.2 No. 950-95
		Telcordia GR-1089-CORE
		Telcordia GR-63-CORE
	USA	UL 1950
		Telcordia GR-1089-CORE
		Telcordia GR-63-CORE
	EU & Asia	EN60950-readiness

Table B-1   Standards (continued)

Discipline	Country	Specification
Environmental	Canada	Telcordia GR-63-CORE NEBS
	USA	Cisco Mechanical Environmental Design and Qualification Guideline ENG-3396
Structural Dynamics (Mechanical)	Canada	Telcordia GR-63-CORE NEBS
	USA	Bell Atlantic NEBS Requirements, RNSA-NEB-95-0003, Rev 8
		AT&T Network Equipment Development Standards (NEDS) Generic Requirements, AT&T 801-900-160
		Pacific Bell/Nevada Bell, Detailed Method of Procedure Number 1 (13.01), Section 8
Power & Grounding	Global	SBC Local Exchange Carriers, Network Equipment Power, Grounding, Environmental, and Physical Design Requirements, TP76200MP

Japan Approvals

Table B-2   Card Approvals

Card	Certificate Number
OC3-4IR 1310	L00-0265
OC12IR 1310	L00-0266
OC48IR 1310	L00-267
DS3N-12	L00-0285

Label Information
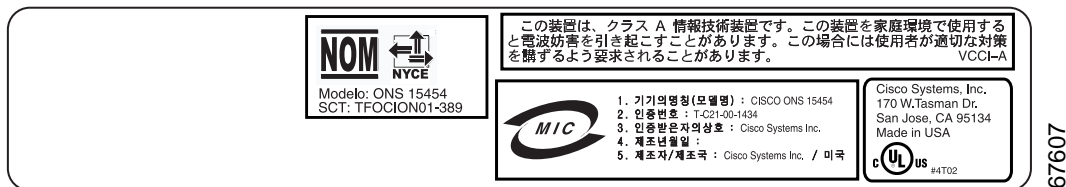
Class A Notice

⚠️

Warning   **This is a Class A Information Product. When used in residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.**

警告使用者   這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，
在這種情況下，使用者會被要求採取某些適當的對策。

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。

Installation Warnings

Install the ONS 15454 in compliance with your local and national electrical codes:

- United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code
- Canada: Canadian Electrical Code, Part I, CSA C22.1
- Other countries: If local and national electrical codes are not available, refer to IEC 364, Part 1 through Part 7.

⚠️

Warning   **Read the installation instructions before you connect the system to its power source.**

Waarschuwing   **Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.**

Varoitus   **Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.**

Attention   **Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.**

Warnung   **Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.**

Avvertenza   **Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.**

Advarsel   **Les installasjonsinstruksjonene før systemet kobles til strømkilden.**

Aviso   **Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.**

¡Advertencia!   **Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.**

Varning!   **Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.**

警告   システムを電源に接続する前に、インストレーションについての説明書を必ずお読みください。

DC Power Disconnection Warning

Warning   **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

Waarschuwing   **Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.**

Varoitus   **Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.**

Attention   **Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.**

Warnung   **Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.**

Avvertenza   **Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata (OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.**

Advarsel   **Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.**

Aviso   **Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.**

¡Advertencia!   **Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).**

Varning!   **Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.**

DC Power Connection Warning

Warning   **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.**

Waarschuwing **Nadat de bedrading van de gelijkstroom voeding aangebracht is, verwijdert u het plakband van de schakelaarhendel van de stroomverbreker en schakelt de stroom weer in door de hendel van de stroomverbreker naar de AAN positie te draaien.**

Varoitus   **Yhdistettyäsi tasavirtalähteen johdon avulla poista teippi suojakytkimen varresta ja kytke virta uudestaan kääntämällä suojakytkimen varsi KYTKETTY-asentoon.**

Attention   **Une fois l'alimentation connectée, retirer le ruban adhésif servant à bloquer la poignée du disjoncteur et rétablir l'alimentation en plaçant cette poignée en position de marche (ON).**

Warnung   **Nach Verdrahtung des Gleichstrom-Netzgeräts entfernen Sie das Klebeband vom Schaltergriff des Unterbrechers und schalten den Strom erneut ein, indem Sie den Griff des Unterbrechers auf EIN stellen.**

Avvertenza   **Dopo aver eseguito il cablaggio dell'alimentatore CC, togliere il nastro adesivo dall'interruttore automatico e ristabilire l'alimentazione spostando all'interruttore automatico in posizione ON.**

Advarsel   **Etter at likestrømsenheten er tilkoblet, fjernes teipen fra håndtaket på strømbryteren, og deretter aktiveres strømmen ved å dreie håndtaket på strømbryteren til PÅ-stilling.**

Aviso   **Depois de ligar o sistema de fornecimento de corrente contínua, retire a fita isoladora da manivela do disjuntor, e volte a ligar a corrente ao deslocar a manivela para a posição ON (Ligado).**

■ **Installation Warnings**

¡Advertencia!   **Después de cablear la fuente de alimentación de corriente continua, retirar la cinta de la palanca del interruptor automático, y restablecer la alimentación cambiando la palanca a la posición de Encendido (ON).**

Varning!   **När du har kopplat ledningarna till strömförsörjningsenheten för inmatad likström tar du bort tejpen från överspänningsskyddets omkopplare och slår på strömmen igen genom att ställa överspänningsskyddets omkopplare i TILL-läget.**

Power Supply Disconnection Warning

⚠

Warning   **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.**

Waarschuwing   **Voordat u aan een frame of in de nabijheid van voedingen werkt, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen; voor gelijkstroom toestellen dient u de stroom uit te schakelen bij de stroomverbreker.**

Varoitus   **Kytke irti vaihtovirtalaitteiden virtajohto ja katkaise tasavirtalaitteiden virta suojakytkimellä, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.**

Attention   **Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif ; couper l'alimentation des unités en courant continu au niveau du disjoncteur.**

Warnung   **Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw. schalten Sie bei Gleichstromeinheiten den Strom am Unterbrecher ab.**

Avvertenza   **Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all'interruttore automatico sulle unità CC.**

Advarsel   **Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut på vekselstrømsenheter og strømmen kobles fra ved strømbryteren på likestrømsenheter.**

Aviso   **Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada; desligue a corrente no disjuntor nas unidades de corrente contínua.**

¡Advertencia!   **Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA); cortar la alimentación desde el interruptor automático en los equipos de corriente continua (CC).**

Varning!   **Innan du arbetar med ett chassi eller nära strömförsörjningsenheter skall du för växelströmsenheter dra ur nätsladden och för likströmsenheter bryta strömmen vid överspänningsskyddet.**

Cisco ONS 15454 Installation and Operations Guide

警告 シャーシの取り扱いや電源まわりの作業を行う前に、AC装置の電源コードを抜いて
ください。DC装置では遮断器の電源を切り離してください。

Outside Line Connection Warning

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.**
Waarschuwing	**Metaalhoudende interfaces bestemd voor aansluiting op fabrieksleidingen buiten (zoals T1/E1/T3/E3 etc.) dienen aangesloten te worden m.b.v. een geregistreerd of goedgekeurd apparaat zoals CSU/DSU of NT1.**
Varoitus	**Laitoksen ulkopuolisten linjojen (T1/E1/T3/E3 jne.) kytkentään tarkoitetut metalliset rajapinnat on kytkettävä rekisteröidyn tai hyväksytyn laitteen, kuten CSU/DSU tai NT1, kautta.**
Attention	**Les interfaces métalliques destinées à une connexion à des lignes extérieures au site (par exemple : T1/E1/T3/E3, etc.) doivent être raccordées sur un appareil homologué ou approuvé tel que CSU/DSU ou NT1.**
Warnung	**Metallische Schnittstellen für die Verbindung mit Leitungen außerhalb der Anlagen (wie z.B. T1/E1/T3/E3 usw.) müssen durch ein registriertes oder zugelassenes Gerät wie CSU/DSU oder NT1 angeschlossen werden.**
Avvertenza	**Le interfacce metalliche per la connessione a linee di impianti esterni (come T1/E1/T3/E3 ecc.) devono essere connesse mediante un dispositivo registrato o approvato, come per esempio CSU/DSU (Channel Service Unit/Data Service Unit) o NT1 (Network Terminator).**
Advarsel	**Metallgrensesnitt for kopling til eksterne anleggslinjer (for eksempel T1/E1/T3/E3 osv.) skal koples gjennom en registrert eller godkjent enhet, for eksempel CSU/DSU eller NT1.**
Aviso	**As interfaces metálicas para conexão com as linhas externas (como T1/E1/T3/E3 etc) devem ser conectadas através de um dispositivo aprovado ou certificado como CSU/DSU ou NT1.**
¡Advertencia!	**Las interfaces metálicas destinadas a las conexiones de líneas exteriores (por ejemplo, T1/E1/T3/E3, etc.) deben conectarse mediante un dispositivo registrado o aprobado como, por ejemplo, CSU/DSU o NT1.**
Varning!	**Metallkontakter för anslutning till utomhusledningar (t.ex. T1/E1/T3/E3 m.fl.) måste anslutas via en registrerad eller godkänd enhet, t.ex. CSU/DSU eller NT1.**

Class 1 Laser Product Warning

Warning	**Class 1 laser product.**
Waarschuwing	**Klasse-1 laser produkt.**
Varoitus	**Luokan 1 lasertuote.**
Attention	**Produit laser de classe 1.**
Warnung	**Laserprodukt der Klasse 1.**
Avvertenza	**Prodotto laser di Classe 1.**
Advarsel	**Laserprodukt av klasse 1.**
Aviso	**Produto laser de classe 1.**
¡Advertencia!	**Producto láser Clase I.**
Varning!	**Laserprodukt av klass 1.**

警告　第１種レーザー製品

경고　1급 레이저 제품.

Class I and Class 1M Laser Warning

Warning	**Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products.**
Waarschuwing	**Laserproducten van Klasse I (21 CFR 1040.10 en 1040.11) en Klasse 1M (IEC 60825-1 2001-01).**
Varoitus	**Luokan I (21 CFR 1040.10 ja 1040.11) ja luokan 1M (IEC 60825-1 2001-01) lasertuotteita.**
Attention	**Produits laser catégorie I (21 CFR 1040.10 et 1040.11) et catégorie 1M (IEC 60825-1 2001-01).**

Warnung	**Laserprodukte der Klasse I (21 CFR 1040.10 und 1040.11) und Klasse 1M (IEC 60825-1 2001-01).**
Avvertenza	**Prodotti laser di Classe I (21 CFR 1040.10 e 1040.11) e Classe 1M (IEC 60825-1 2001-01).**
Advarsel	**Klasse I (21 CFR 1040.10 og 1040.11) og klasse 1M (IEC 60825-1 2001-01) laserprodukter.**
Aviso	**Produtos laser Classe I (21 CFR 1040.10 e 1040.11) e Classe 1M (IEC 60825-1 2001-01).**
¡Advertencia!	**Productos láser de Clase I (21 CFR 1040.10 y 1040.11) y Clase 1M (IEC 60825-1 2001-01).**
Varning!	**Laserprodukter av Klass I (21 CFR 1040.10 och 1040.11) och Klass 1M (IEC 60825-1 2001-01).**

Restricted Area Warning

Warning	**This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.**
Waarschuwing	**Dit toestel is bedoeld voor installatie op plaatsen met beperkte toegang. Een plaats met beperkte toegang is een plaats waar toegang slechts door servicepersoneel verkregen kan worden door middel van een speciaal instrument, een slot en sleutel, of een ander veiligheidsmiddel, en welke beheerd wordt door de overheidsinstantie die verantwoordelijk is voor de locatie.**
Varoitus	**Tämä laite on tarkoitettu asennettavaksi paikkaan, johon pääsy on rajoitettua. Paikka, johon pääsy on rajoitettua, tarkoittaa paikkaa, johon vain huoltohenkilöstö pääsee jonkin erikoistyökalun, lukkoon sopivan avaimen tai jonkin muun turvalaitteen avulla ja joka on paikasta vastuussa olevien toimivaltaisten henkilöiden valvoma.**
Attention	**Cet appareil est à installer dans des zones d'accès réservé. Ces dernières sont des zones auxquelles seul le personnel de service peut accéder en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité. L'accès aux zones de sécurité est sous le contrôle de l'autorité responsable de l'emplacement.**
Warnung	**Diese Einheit ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Ein Bereich mit beschränktem Zutritt ist ein Bereich, zu dem nur Wartungspersonal mit einem Spezialwerkzeugs, Schloß und Schlüssel oder anderer Sicherheitsvorkehrungen Zugang hat, und der von dem für die Anlage zuständigen Gremium kontrolliert wird.**
Avvertenza	**Questa unità deve essere installata in un'area ad accesso limitato. Un'area ad accesso limitato è un'area accessibile solo a personale di assistenza tramite un'attrezzo speciale, lucchetto, o altri dispositivi di sicurezza, ed è controllata dall'autorità responsabile della zona.**

Advarsel **Denne enheten er laget for installasjon i områder med begrenset adgang. Et område med begrenset adgang gir kun adgang til servicepersonale som bruker et spesielt verktøy, lås og nøkkel, eller en annen sikkerhetsanordning, og det kontrolleres av den autoriteten som er ansvarlig for området.**

Aviso **Esta unidade foi concebida para instalação em áreas de acesso restrito. Uma área de acesso restrito é uma área à qual apenas tem acesso o pessoal de serviço autorizado, que possua uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.**

¡Advertencia! **Esta unidad ha sido diseñada para instalarse en áreas de acceso restringido. Área de acceso restringido significa un área a la que solamente tiene acceso el personal de servicio mediante la utilización de una herramienta especial, cerradura con llave, o algún otro medio de seguridad, y que está bajo el control de la autoridad responsable del local.**

Varning! **Denna enhet är avsedd för installation i områden med begränsat tillträde. Ett område med begränsat tillträde får endast tillträdas av servicepersonal med ett speciellt verktyg, lås och nyckel, eller annan säkerhetsanordning, och kontrolleras av den auktoritet som ansvarar för området.**

Ground Connection Warning

Warning **When installing the unit, always make the ground connection first and disconnect it last.**

Waarschuwing **Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.**

Varoitus **Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.**

Attention **Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.**

Warnung **Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.**

Avvertenza **In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.**

Advarsel **Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.**

Aviso **Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.**

¡Advertencia!	**Al instalar el equipo, conectar la tierra la primera y desconectarla la última.**
Varning!	**Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.**

Qualified Personnel Warning

⚠ **Warning**	**Only trained and qualified personnel should be allowed to install or replace this equipment.**
Waarschuwing	**Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.**
Varoitus	**Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.**
Avertissement	**Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.**
Achtung	**Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.**
Avvertenza	**Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.**
Advarsel	**Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.**
Aviso	**Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.**
¡Atención!	**Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.**
Varning	**Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.**

Invisible Laser Radiation Warning (other versions available)

⚠ **Warning**	**Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.**
Waarschuwing	**Omdat er onzichtbare laserstraling uit de opening van de poort geëmitteerd kan worden wanneer er geen kabel aangesloten is, dient men om blootstelling aan laserstraling te vermijden niet in de open openingen te kijken.**

Varoitus	**Kun porttiin ei ole kytketty kaapelia, portin aukosta voi vuotaa näkymätöntä lasersäteilyä. Älä katso avoimiin aukkoihin, jotta et altistu säteilylle.**
Attention	**Etant donné qu'un rayonnement laser invisible peut être émis par l'ouverture du port quand aucun câble n'est connecté, ne pas regarder dans les ouvertures béantes afin d'éviter tout risque d'exposition au rayonnement laser.**
Warnung	**Aus der Öffnung des Ports kann unsichtbare Laserstrahlung austreten, wenn kein Kabel angeschlossen ist. Kontakt mit Laserstrahlung vermeiden und nicht in offene Öffnungen blicken.**
Avvertenza	**Poiché quando nessun cavo è collegato alla porta, da quest'ultima potrebbe essere emessa radiazione laser invisibile, evitare l'esposizione a tale radiazione e non fissare con gli occhi porte a cui non siano collegati cavi.**
Advarsel	**Usynlige laserstråler kan sendes ut fra åpningen på utgangen når ingen kabel er tilkoblet. Unngå utsettelse for laserstråling og se ikke inn i åpninger som ikke er tildekket.**
Aviso	**Evite uma exposição à radiação laser e não olhe através de aberturas expostas, porque poderá ocorrer emissão de radiação laser invisível a partir da abertura da porta, quando não estiver qualquer cabo conectado.**
¡Advertencia!	**Cuando no esté conectado ningún cable, pueden emitirse radiaciones láser invisibles por el orificio del puerto. Evitar la exposición a radiaciones láser y no mirar fijamente los orificios abiertos.**
Varning!	**Osynliga laserstrålar kan sändas ut från öppningen i porten när ingen kabel är ansluten. Undvik exponering för laserstrålning och titta inte in i ej täckta öppningar.**

More Than One Power Supply

⚠ Warning	**This unit has more than one power supply connection; all connections must be removed completely to completely remove power from the unit.**
Waarschuwing	**Deze eenheid heeft meer dan één stroomtoevoerverbinding; alle verbindingen moeten volledig worden verwijderd om de stroom van deze eenheid volledig te verwijderen.**
Varoitus	**Tässä laitteessa on useampia virtalähdekytkentöjä. Kaikki kytkennät on irrotettava kokonaan, jotta virta poistettaisiin täysin laitteesta.**
Attention	**Cette unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.**
Warnung	**Diese Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.**

Avvertenza	**Questa unità ha più di una connessione per alimentatore elettrico; tutte le connessioni devono essere completamente rimosse per togliere l'elettricità dall'unità.**
Advarsel	**Denne enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.**
Aviso	**Este dispositivo possui mais do que uma conexão de fonte de alimentação de energia; para poder remover a fonte de alimentação de energia, deverão ser desconectadas todas as conexões existentes.**
¡Advertencia!	**Esta unidad tiene más de una conexión de suministros de alimentación; para eliminar la alimentación por completo, deben desconectarse completamente todas las conexiones.**
Varning!	**Denna enhet har mer än en strömförsörjningsanslutning; alla anslutningar måste vara helt avlägsnade innan strömtillförseln till enheten är fullständigt bruten.**

Unterminated Fiber Warning

⚠ **Warning**	**Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam or view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified may result in hazardous radiation exposure.**
Waarschuwing	**Er kunnen onzichtbare laserstralen worden uitgezonden vanuit het uiteinde van de onafgebroken vezelkabel of connector. Niet in de straal kijken of deze rechtstreeks bekijken met optische instrumenten. Als u de laseruitvoer met bepaalde optische instrumenten bekijkt (zoals bijv. een oogloep, vergrootgras of microscoop) binnen een afstand van 100 mm kan dit gevaar voor uw ogen opleveren. Het gebruik van regelaars of bijstellingen of het uitvoeren van procedures anders dan opgegeven kan leiden tot blootstelling aan gevaarlijke straling.**
Varoitus	**Päättämättömän kuitukaapelin tai -liittimen päästä voi tulla näkymätöntä lasersäteilyä. Älä tuijota sädettä tai katso sitä suoraan optisilla välineillä. Lasersäteen katsominen tietyillä optisilla välineillä (esim. suurennuslasilla tai mikroskoopilla) 10 cm:n päästä tai sitä lähempää voi olla vaarallista silmille. Säätimien tai säätöjen käyttö ja toimenpiteiden suorittaminen ohjeista poikkeavalla tavalla voi altistaa vaaralliselle säteilylle.**
Attention	**Des émissions de radiations laser invisibles peuvent se produire à l'extrémité d'un câble en fibre ou d'un raccord sans terminaison. Ne pas fixer du regard le rayon ou l'observer directement avec des instruments optiques. L'observation du laser à l'aide certains instruments optiques (loupes et microscopes) à une distance inférieure à 100 mm peut poser des risques pour les yeux. L'utilisation de commandes, de réglages ou de procédures autres que ceux spécifiés peut entraîner une exposition dangereuse à des radiations.**

Cisco ONS 15454 Installation and Operations Guide ■

Warnung   **Eine unsichtbare Laserstrahlung kann vom Ende des nicht angeschlossenen Glasfaserkabels oder Steckers ausgestrahlt werden. Nicht in den Laserstrahl schauen oder diesen mit einem optischen Instrument direkt ansehen. Ein Betrachten des Laserstrahls mit bestimmten optischen Instrumenten, wie z.B. Augenlupen, Vergrößerungsgläsern und Mikroskopen innerhalb eines Abstands von 100 mm kann für das Auge gefährlich sein. Die Verwendung von nicht spezifizierten Steuerelementen, Einstellungen oder Verfahrensweisen kann eine gefährliche Strahlenexposition zur Folge haben.**

Avvertenza   **L'estremità del connettore o del cavo ottico senza terminazione può emettere radiazioni laser invisibili. Non fissare il raggio od osservarlo in modo diretto con strumenti ottici. L'osservazione del fascio laser con determinati strumenti ottici (come lupette, lenti di ingrandimento o microscopi) entro una distanza di 100 mm può provocare danni agli occhi. L'adozione di controlli, regolazioni o procedure diverse da quelle specificate può comportare il pericolo di esposizione a radiazioni.**

Advarsel   **Usynlig laserstråling kan emittere fra enden av den ikke-terminerte fiberkabelen eller koblingen. Ikke se inn i strålen og se heller ikke direkte på strålen med optiske instrumenter. Observering av laserutgang med visse optiske instrumenter (for eksempel øyelupe, forstørrelsesglass eller mikroskoper) innenfor en avstand på 100 mm kan være farlig for øynene. Bruk av kontroller eller justeringer eller utførelse av prosedyrer som ikke er spesifiserte, kan resultere i farlig strålingseksponering.**

Aviso   **Radiação laser invisível pode ser emitida pela ponta de um conector ou cabo de fibra não terminado. Não olhe fixa ou diretamente para o feixe ou com instrumentos ópticos. Visualizar a emissão do laser com certos instrumentos ópticos (por exemplo, lupas, lentes de aumento ou microscópios) a uma distância de 100 mm pode causar riscos à visão. O uso de controles, ajustes ou desempenho de procedimentos diferentes dos especificados pode resultar em exposição prejudicial de radiação.**

¡Advertencia!   **El extremo de un cable o conector de fibra sin terminación puede emitir radiación láser invisible. No se acerque al radio de acción ni lo mire directamente con instrumentos ópticos. La exposición del ojo a una salida de láser con determinados instrumentos ópticos (por ejemplo, lupas y microscopios) a una distancia de 100 mm puede comportar lesiones oculares. La aplicación de controles, ajustes y procedimientos distintos a los especificados puede comportar una exposición peligrosa a la radiación.**

Varning!   **Osynlig laserstrålning kan komma från änden på en oavslutad fiberkabel eller -anslutning. Titta inte rakt in i strålen eller direkt på den med optiska instrument. Att titta på laserstrålen med vissa optiska instrument (t.ex. lupper, förstoringsglas och mikroskop) från ett avstånd på 100 mm kan skada ögonen. Om andra kontroller eller justeringar än de angivna används, eller om andra processer än de angivna genomförs, kan skadlig strålning avges.**

Laser Activation Warning

Warning	**The laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).**
Waarschuwing	**De laser is aan zodra de kaart is opgestart en de veiligheidssleutel in de AAN-positie is (gelabeld 1). De poort hoeft niet in dienst te zijn om de laser aan te zetten. De laser is uit wanneer de veiligheidssleutel uit is (gelabeld 0).**
Varoitus	**Laser on päällä, kun kortti käynnistetään ja turva-avain on päällä (1) -asennossa. Laser voi olla päällä, vaikka portti ei olekaan käytössä. Laser on pois päältä, kun turva-avain on pois (0) -asennossa.**
Attention	**Le laser est allumé dès le démarrage de la carte et lorsque la clé de sûreté est en position allumée (ou 1). Il n'est pas nécessaire que le port soit en service pour que le laser soit allumé. Le laser est éteint lorsque la clé de sûreté est en position éteinte (ou 0).**
Warnung	**Der Laser ist eingeschaltet, wenn die Karte geladen wurde und der Sicherheitsschlüssel eingeschaltet ist (mit 1 bezeichnete Stellung). Der Port muss nicht in Betrieb sein, wenn der Laser eingeschaltet ist. Der Laser ist ausgeschaltet, wenn sich der Sicherheitsschlüssel in der Aus-Stellung (mit 0 bezeichnet) befindet.**
Avvertenza	**Il laser è attivato quando la scheda è inserita e la chiave di sicurezza è in posizione ON (indicata con I). Per l'attivazione del laser non è necessario che la porta sia in funzione. Il laser è disattivato quando la chiave di sicurezza è su OFF (indicata con 0).**
Advarsel	**Laseren er aktivert når kortet er på plass og sikkerhetstasten er i på-stilling (merket 1). Porten trenger ikke å være aktiv selv om laseren er på. Laseren er av når sikkerhetstasten er i av-stilling (merket 0).**
Aviso	**O laser está ativado quando a placa é reiniciada e a chave de segurança está na posição on (ou 1). A porta não precisa estar em atividade para o acionamento do laser. O laser está desativado quando a chave de segurança está na posição off (ou 0).**
¡Advertencia!	**El láser está encendido cuando la tarjeta ha arrancado y la llave de seguridad se encuentra en la posición ON (etiquetada 1). No es necesario que el puerto esté en funcionamiento para que el láser pueda funcionar. El láser está apagado cuando la llave de seguridad se encuentra en la posición OFF (etiquetada 0).**
Varning!	**Lasern är på när kortet är igångsatt och säkerhetsnyckeln är i läget På (markerat med 1). Porten behöver inte vara igång för att lasern ska vara på. Lasern är av när säkerhetsnyckeln är i läget Av (markerat med 0).**

Acronyms

Numerics

10BaseT
standard 10 megabit per second local area network over unshielded twisted pair copper wire

100BaseT

standard 100 megabit per second ethernet network

100BaseTX

specification of 100BaseT that supports full duplex operation

A

ACO

Alarm Cutoff

ACT/STBY

Active/Standby

ADM

Add-Drop Multiplexer

AIC
Alarm Interface Controller

AID

Access Identifier

AIP

Alarm Interface Panel

AIS

Alarm Indication Signal

AIS-L

Line Alarm Indication Signal

AMI

Alternate Mark Inversion

ANSI

American National Standards Institute

APS

Automatic Protection Switching

ARP

Address Resolution Protocol

ATAG

Autonomous Message Tag

ATM

Asynchronous Transfer Mode

AWG

American Wire Gauge

B

B8ZS

Bipolar 8 Zero Substitution

BER

Bit Error Rate

BIC

Backplane Interface Connector

BIP

Bit Interleaved Parity

BITS

Building Integrated Timing Supply

BLSR

Bidirectional line switched ring

BNC

Bayonet Neill-Concelman (coaxial cable bayonet locking connector)

BPDU

Bridge Protocol Data Unit

C

CAT 5

Category 5 (cabling)

CCITT

Consultative Committee International Telegraph and Telephone (France)

CEO

Central Office Environment

CEV

Controlled Environment Vaults

CLEI

Common Language Equipment Identifier code

CLNP

Correctionless Network Protocol

CMIP

Common Management Information Protocol

cm

centimeter

COE

Central Office Environment

CORBA

Common Object Request Broker Architecture

CPE

Customer Premise Environments

CTAG

Correlation Tag

Cisco ONS 15454 Installation and Operations Guide

CTC

Cisco Transport Controller

D

DCC

Data Communications Channel

DCN

Data Communications Network

DCS

Distributed Communications System

DRAM

Dynamic Random Access Memory

DS-1

Digital Signal Level One

DS-3

Digital Signal Level Three

DS1-14

Digital Signal Level One (14 ports)

DS1N-14

Digital Signal Level One (N-14 ports)

DS3-12

Digital Signal Level Three (12 ports)

DS3N-12

Digital Signal Level Three (N-12 ports)

DS3XM-6

Digital Service, level 3 Trans Multiplexer 6 ports

DSX

Digital Signal Cross Connect frame

E

EDFA

Erbium Doped Fiber Amplifier

EFT

Electrical Fast Transient/Burst

EIA

Electrical Interface Assemblies

ELR

Extended Long Reach

EMI

Electromagnetic interface

EML

Element Management Layer

EMS

Element Management System

EOW

Express Orderwire

ERDI

Enhanced Remote Defect Indicator

ES

Errored Seconds

ESD

Electrostatic Discharge

ESF

Extended Super Frame

ETSI

European Telecommunications Standards Institute

F

FC

Failure Count

FDDI

Fiber Distributed Data Interface

FE

Frame Bit Errors

FG1

Frame Ground #1(pins are labeled "FG1," "FG2," etc.)

FSB

Field Service Bulletin

G

Gbps

Gigabits per second

GBIC

Gigabit Interface Converter

GR-253-CORE

General Requirements #253 Council Of Registrars

GR-1089

General Requirements #1089

GUI

Graphical User Interface

H

HDLC

High-Level Data Link Control

I

IEC

InterExchange Carrier

IEEE

Institute of Electrical and Electronics Engineers

IETF

Internet Engineering Task Force

IP

Internet Protocol

IPPM

Intermediate-Path Performance Monitoring

I/O

Input/Output

ITU-T

The International Telecommunication Union- Telecommunication Standards Sector

J

JRE

Java Runtime Environment

L

LAN

Local Area Network

LCD

Liquid Crystal Display

LDCC

Line Data Communications Channel

LOP

Loss of Pointer

LOS

Loss of Signal

LOF

Loss of Frame

Cisco ONS 15454 Installation and Operations Guide

LOW

Local Orderwire

LTE

Line Terminating Equipment

LVDS

Low Voltage Differential Signal

M

MAC

Media Access Control

Mbps

Million bits per second, or Million bytes per second

Mhz

Megahertz

MIB

Management Information Bases

MIME

Multipurpose Internet Mail Extensions

Mux/Demux

Multiplexer/Demultiplexer

N

NE

Network Element

NEL

Network Element Layer

NEBS

Network Equipment-Building Systems

NML

Network Management Layer

Cisco ONS 15454 Installation and Operations Guide

NMS

Network Management System

O

OAM&P

Operations, Administration, Maintenance, and Provisioning

OC

Optical carrier

OOS AS

Out of Service Assigned

OSI

Open Systems Interconnection

OSPF

Open Shortest Path First

OSS

Operations Support System

OSS/NMS

Operations Support System/Network Management System

P

PCM

Pulse Code Modulation

PCMCIA

Personal Computer Memory Card International Association

PCN

Product Change Notices

PDI-P

STS Payload Defect Indication-Path

POP

Point of Presence

PM

Performance Monitoring

PPMN

Path-Protected Mesh Network

PSC

Protection Switching Count

PSD

Protection Switching Duration

PTE

Path Terminating Equipment

R

RAM

Random Access Memory

RDI-L

Remote Defect Indication Line

RES

Reserved

RJ45

Registered Jack #45 (8 pin)

RMA

Return Material Authorization

RMON

Remote Network Monitoring

RS232

Recommended Standard #232 (ANSI Electrical Interface for Serial Communication

Rx

Receive

S

SCI

Serial Communication Interface

SCL

System Communications Link

SDCC

Section Data Communications Channel

SDH/SONET

Synchronous Digital Hierarchy/Synchronous Optical Network

SEF

Severely Errored Frame

SELV

Safety Extra Low Voltage

SES

Severely Errored Seconds

SF

Super Frame

SML

Service Management Layer

SMF

Single Mode Fiber

SNMP

Simple Network Management Protocol

SNTP

Simple Network Time Protocol

SONET

Synchronous Optical Network

SPE

Synchronous Payload Envelope

SSM

Synchronous Status Messaging

STA

Spanning Tree Algorithm

STP

Shielded Twisted Pair

STS-1

Synchronous Transport Signal Level 1

SWS

SONET WAN Switch

SXC

SONET Cross Connect ASIC

T

TAC

Technical Assistance Center

TBOS

Telemetry Byte Oriented Serial protocol

TCA

Threshold Crossing Alert

TCC+

Timing Communications and Control+ Card

TCP/IP

Transmission Control Protocol/Internet Protocol

TDM

Time Division Multiplexing

TDS

Time Division Switching

TID

Target Identifier

TL1

Transaction Language 1

TLS

Transparent LAN service

TMN

Telecommunications Management Network

TSA

Time Slot Assignment

TSI

Time-Slot Interchange

Tx

Transmit

U

UAS

Unavailable Seconds

UDP/IP

User Datagram Protocol/Internet Protocol

UID

User Identifier

UPSR

Unidirectional Path Switched Ring

UTC

Universal Time Coordinated

UTP

Unshielded Twisted Pair

V

VDC

Volts Direct Current

Cisco ONS 15454 Installation and Operations Guide

VLAN

Virtual Local Area Network

VPN

Virtual Private Network

VT1.5

Virtual Tributary equals 1.544 megabits per second

W

WAN

Wide Area Network

W

Watts

X

XC

Cross Connect

XCVT

Cross Connect Virtual Tributary

X.25

Protocol providing devices with direct connection to a packet switched network

Glossary

Numerics

1:1 protection

A card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot. If the working card fails, the traffic from the working card switches to the protect card. When the failure on the working card is resolved, traffic reverts back to the working card if this option is set. This protection scheme is specific to electrical cards.

1+1 protection

A card protection scheme that pairs a single working card with a single dedicated protect card. A term specific to optical cards.

1:N protection

A card protection scheme that allows a single card to protect several working cards. When the failure on the working card is resolved, traffic reverts back to the working card. A term specific to electrical cards.

A

Access drop

Points where network devices can access the network.

Address mask

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the part that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

ADM

Add/drop multiplexer. ADM allows a signal to be added into or dropped from a SONET span.

Agent
1. 1. Generally, software that processes queries and returns replies on behalf of an application.
2. 2. In a network management system, a process that resides in all managed devices and reports the values of specified variables to management stations.

AID

Access Identifier. An access code used in TL1 messaging that identifies and addresses specific objects within the ONS 15454. These objects include individual pieces of equipment, transport spans, access tributaries, and others.

AMI

Alternate Mark Inversion. Line-code format used on T1 circuits that transmits ones by alternate positive and negative pulses. Zeroes are represented by 01 during each bit cell and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary-coded alternate mark inversion.

APS

Automatic Protection Switching. SONET switching mechanism that routes traffic from working lines to protect lines in case a line card failure or fiber cut occurs.

ATAG

Autonomous Message Tag. ATAG is used for TL1 message sequencing.

B

B8ZS

Binary 8-zero Substitution. A line-code type, used on T1 circuits, that substitutes a special code whenever 8 consecutive zeros are sent over the link. This code is then interpreted at the remote end of the connection. This technique guarantees ones density independent of the data stream. Sometimes called bipolar 8-zero substitution.

BER

Bit Error Rate. Ratio of received bits that contain errors.

Bit rate

Speed at which bits are transmitted, usually expressed in bits per second.

BITS

Building Integrated Timing Supply. A single building master timing supply that minimizes the number of synchronization links entering an office. Sometimes referred to as a Synchronization Supply Unit.

BLSR

Bidirectional Line Switched Ring. SONET ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically routed onto the protection fiber.

Blue band

Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

Bridge

Device that connects and passes packets between two network segments that use the same communications protocol. In general, a bridge will filter, forward, or flood an incoming frame based on the MAC address of that frame.

Broadcast

Data packet that will be sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*. See also *Broadcast address*.

Broadcast address

Special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones.

Broadcast storm

Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

Bus

Common physical signal path composed of wires or other media across which signals can be sent from one part of a computer to another.

C

C2 byte

The C2 byte is the signal label byte in the STS path overhead. This byte tells the equipment what the SONET payload envelope contains and how it is constructed.

Collision

In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.

Concatenation

A mechanism for allocating contiguous bandwidth for payload transport. Through the use of Concatenation Pointers, multiple OC-1s can be linked together to provide contiguous bandwidth through the network, from end to end.

Crosspoint

A set of physical or logical contacts that operate together to extend the speech and signal channels in a switching network.

CTAG

Correlation Tag. A unique identifier given to each input command by the TL1 operator. When the ONS 15454 system responds to a specific command, it includes the command's CTAG in the reply. This eliminates discrepancies about which response corresponds to which command.

Cisco ONS 15454 Installation and Operations Guide

CTC

Cisco Transport Controller. A Java-based graphical user interface (GUI) that allows operations, administration, maintenenance, and provisioning (OAM&P) of the ONS 15454 using an Internet browser.

CTM

Cisco Transport Manager. A Java-based network management tool used to support large networks of Cisco 15000-class equipment.

CV

code violation

D

DCC

Data Communications Channel. Used to transport information about operation, administration, maintenance, and provisioning (OAM&P) over a SONET interface. DCC can be located in section DCC (SDCC) or line overhead (LDCC.)

Demultiplex

To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. See also *Multiplexing*.

Destination

The endpoint where traffic exits an ONS 15454 network. Endpoints can be a path (STS or STS/VT for optical card endpoints), port (for electrical circuits, such as DS1, VT, DS3, STS), or card (for circuits on DS1 and Ethernet cards).

DSX

Digital Signal Cross-connect frame. A manual bay or panel where different electrical signals are wired. A DSX permits cross-connections by patch cords and plugs.

DWDM

Dense Wave Division Multiplexing. A technology that increases the information carrying capacity of existing fiber optic infrastructure by transmitting and receiving data on different light wavelengths. Many of these wavelengths can be combined on a single strand of fiber.

E

EDFA

Erbium Doped Fiber Amplifier. A type of fiber optical amplifier that transmits a light signal through a section of erbium-doped fiber and amplifies the signal with a laser pump diode. EDFA is used in transmitter booster amplifiers, in-line repeating amplifiers, and in receiver preamplifiers.

EIA

Electrical Interface Assemblies. Provides connection points for the ONS 15454 and DS-1, DS-3, or EC-1 units.

EMI

Electromagnetic Interference. Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

Envelope

The part of messaging that varies in composition from one transmittal step to another. It identifies the message originator and potential recipients, documents its past, directs its subsequent movement by the Message Transfer System (MTS), and characterizes its content.

EOW

Express Orderwire. A permanently connected voice circuit between selected stations for technical control purposes.

Ethernet switch

An Ethernet data switch. Ethernet switches provide the capability to increase the aggregate LAN bandwidth by allowing simultaneous switching of packets between switch ports. Ethernet switches subdivide previously-shared LAN segments into multiple networks with fewer stations per network.

External timing reference

A timing reference obtained from a source external to the communications system, such as one of the navigation systems. Many external timing references are referenced to Coordinated Universal Time (UTC).

F

Falling threshold

A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, this triggers an event to reset the rising threshold. See also *rising threshold*.

FDDI

Fiber Distributed Data Interface. LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

Frame

Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control that surrounds the user data contained in the unit.

Free run synchronization mode

Occurs when the external timing sources have been disabled and the ONS 15454 is receiving timing from its Stratum 3 level internal timing source.

G

GBIC

Gigabit Interface Converter. A hot-swappable input/output device that plugs into a Gigabit Ethernet port to link the port with the fiber optic network.

H

Hard reset

The physical removal and insertion of a card. A card pull.

HDLC

High-Level Data Link Control. Bit-oriented, synchronous, data-link layer protocol developed by ISO. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

Host number

Part of IP address used to address an individual host within the network or subnetwork.

Hot swap

The process of replacing a failed component while the rest of the system continues to function normally.

I

Input alarms

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IP address

32-bit address assigned to host using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.

K

K bytes

Automatic protection switching bytes. K bytes are located in the SONET line overhead and monitored by equipment for an indication to switch to protection.

L

LAN

Local Area Network. High-speed, low error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LCD

Liquid Crystal Display. An alphanumeric display using liquid crystal sealed between two pieces of glass. LCDs conserve electricity.

Line layer

Refers to the segment between two SONET devices in the circuit. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization. Sometimes called a maintenance span.

Line timing mode

A node that derives its clock from the SONET lines.

Link budget

The difference between the output power and receiver power of an optical signal expressed in dB. Link refers to an optical connection and all of its component parts (optical transmitters, repeaters, receivers, and cables).

Link integrity

The network communications channel is intact.

Loopback test

Test that sends signals then directs them back toward their source from some point along the communications path. Loopback tests are often used to test network interface usability.

LOW

Local Orderwire. A communications circuit between a technical control center and selected terminal or repeater locations.

M

MAC address

Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as the hardware address, MAC-layer address, and physical address.

Maintenance user

A security level that limits user access to maintenance options only. See also *Superuser*, *Provisioning User*, and *Retrieve User*.

Managed device

A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers.

Managed object

In network management, a network device that can be managed by a network management protocol. Sometimes called an MIB object.

Mapping

A logical association between one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.

MIB

Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Multicast

Single packets copied by the network and sent to a specific subset of network addresses.

Multiplex payload

Generates section and line overhead, and converts electrical/optical signals when the electrical/optical card is transmitting.

Multiplexing

Scheme that allows multiple logical signals to be transmitted simultaneously across a single physical channel. Compare with *Demultiplex*.

N

NE

Network Element. In an Operations Support System, a single piece of telecommunications equipment used to perform a function or service integral to the underlying network.

Network number

Part of an IP address that specifies the network where the host belongs.

NMS

Network Management System. System that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.

Node

Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes, which vary in routing and other functional capabilities, can be interconnected by links, and serve as control points in the network. Node is sometimes used generically to refer to any entity that can access a network. In this manual the term "node" usually refers to an ONS 15454.

NPJC

negative pointer justification count

O

OAM&P

Operations, Administration, Maintenance, and Provisioning. Provides the facilities and personnel required to manage a network.

Optical amplifier

A device that amplifies an optical signal without converting the signal from optical to electrical and back again to optical energy.

Optical receiver

An opto-electric circuit that detects incoming lightwave signals and converts them to the appropriate signal for processing by the receiving device.

Orderwire

Equipment that establishes voice contact between a central office and carrier repeater locations.

Output contacts (alarms)

Triggers that drive visual or audible devices such as bells and lights. Output contacts can control other devices such as generators, heaters, and fans.

P

Passive devices

Components that do not require external power to manipulate or react to electronic output. Passive devices include capacitors, resisters, and coils.

Path Layer

The segment between the originating equipment and the terminating equipment. This path segment may encompass several consecutive line segments or segments between two SONET devices.

Payload

Portion of a cell, frame, or packet that contains upper-layer information (data).

Ping

Packet internet grouper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

PPJC

positive pointer justification count

PPMN

Path Protected Mesh Network. PPMN extends the protection scheme of a unidirectional path switched ring (UPSR) beyond the basic ring configuration to the meshed architecture of several interconnecting rings.

Priority queuing

Routing feature that divides data packets into two queues: one low-priority and one high-priority.

Provisioning user

A security level that allows the user to access only provisioning and maintenance options in CTC. See also *Superuser*, *Maintenance user,* and *Retrieve user*.

Q

Queue

In routing, a backlog of packets waiting to be forwarded over a router interface.

R

Red band

DWDM wavelengths are broken into two distinct bands: red and blue. The red band is the higher frequency band. The red band DWDM cards for the ONS 15454 operate on wavelengths between 1547.72nm and 1560.61nm.

Retrieve user

A security level that allows the user to retrieve and view CTC information but not set or modify parameters. See also *Superuser*, *Maintenance user*, and *Provisioning user.*

Revertive switching

A process that sends electrical interfaces back to the original working card after the card comes back online.

Rising threshold

The number of occurrences (collisions) that must be exceeded to trigger an event.

RMON

Remote Network Monitoring. Allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

S

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP monitors and controls network devices and manages configurations, statistics collection, performance, and security.

SNTP

Simple Network Time Protocol. Using an SNTP server ensures that all ONS 15454 network nodes use the same date and time reference. The server synchronizes alarm timing during power outages or software upgrades.

Soft reset

A soft reset reloads the operating system, application software, etc., and reboots the card. It does not initialize the ONS 15454 ASIC hardware.

SONET

Synchronous Optical Network. High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

Source

The endpoint where traffic enters an ONS 15454 network. Endpoints can be a path (STS or STS/VT for optical card endpoints), port (for electrical circuits, such as DS1, VT, DS3, STS), or card (for circuits on DS1 and Ethernet cards).

Spanning tree

Loop-free subset of a network topology. See also *STA* and *STP*.

SPE

Synchronous Payload Envelope. A SONET term describing the envelope that carries the user data or payload.

SSM

Sync Status Messaging. A SONET protocol that communicates information about the quality of the timing source using the S1 byte of the line overhead.

STA

Spanning-Tree Algorithm. An algorithm used by the spanning tree protocol to create a spanning tree. See also *Spanning tree* and *STP*.

Cisco ONS 15454 Installation and Operations Guide

Static route

A route that is manually entered into a routing table. Static routes take precedence over routes chosen by all dynamic routing protocols.

STP

Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm to enable a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. See also *Spanning tree, STA,* and *Learning bridge.*

STS-1

Synchronous Transport Signal 1. Basic building block signal of SONET, operating at 51.84 Mbps for transmission over OC-1 fiber. Faster SONET rates are defined as STS-n, where n is a multiple of 51.84 Mbps. See also *SONET.*

Subnet mask

32-bit address mask used in IP to indicate the bits of an IP address that are used for the subnet address. Sometimes referred to simply as mask. See also *IP address mask* and *IP address.*

Subnetwork

In IP networks, a network confined to a particular subnet address. Subnetworks are networks segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. Sometimes called a subnet.

Subtending rings

SONET rings that incorporate nodes that are also part of an adjacent SONET ring.

Superuser

A security level that can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. A superuser is usually the network element administrator. See also *Retrieve user*, *Maintenance user*, and *Provisioning user.*

T

T1

T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network using AMI or B8ZS coding. See also *AMI*, *B8ZS*, and *DS-1*.

Tag

Identification information, including a number plus other information.

TDM

Time Division Multiplexing. Allocates bandwidth on a single wire for information from multiple channels based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

Telcordia

Telcordia Technologies, Inc., formerly named Bellcore. Eighty percent of the U.S. telecommunications network depends on software invented, developed, implemented, or maintained by Telcordia.

TID

Target Identifier. Identifies the particular network element (in this case, the ONS 15454) where each TL1 command is directed. The TID is a unique name given to each system at installation.

TLS

Transparent LAN Service. Provides private network service across a SONET backbone.

Transponder

Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength.

Trap

Message sent by an SNMP agent to an NMS (CTM), console, or terminal to indicate the occurrence of a significant event, such as an exceeded threshold.

Tributary

The lower-rate signal directed into a multiplexer for combination (multiplexing) with other low rate signals to form an aggregate higher rate level.

Trunk

Network traffic travels across this physical and logical connection between two switches. A backbone is composed of a number of trunks. See also *Backbone*.

Tunneling

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. See also *encapsulation*.

U

Unicast

The communication of a single source to a single destination.

UPSR

Unidirectional Path Switched Ring. Path-switched SONET rings that employ redundant, fiber- optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over.

Upstream

Set of frequencies used to send data from a subscriber to the headend.

Cisco ONS 15454 Installation and Operations Guide

V

Virtual fiber

A fiber that carries signals at different rates and uses the same fiber optic cable.

Virtual ring

Entity in a source-route bridging (SRB) network that logically connects two or more physical rings together either locally or remotely. The concept of virtual rings can be expanded across router boundaries.

Virtual wires

Virtual wires route external alarms to one or more alarm collection centers across the SONET transport network.

VLAN

Virtual LAN. Group of devices located on a number of different LAN segments that are configured (using management software) to communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN

Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level. (See also *Tunneling*.)

VT

Virtual Tributary. A structure designed for the transport and switching of sub-DS3 payloads.

VT layer

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.

Numerics

A

C

Cisco ONS 15454 Installation and Operations Guide

N

O

T

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com