CISCO SYSTEMS

Cisco ONS 15454 SDH Installation and Operations Guide

Product and Documentation Release 3.4
September 2002

C O N T E N T S

CHAPTER 6 **Circuits and Tunnels**   6-1

I N D E X

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

F I G U R E S

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

T A B L E S

Preface

This section explains who should read the *Cisco ONS 15454 SDH 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 SDH administrators who are responsible for hardware installation, software installation, node setup, and node and network configuration. For troubleshooting, maintenance, and card detail reference information, refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Organization

Chapter Number and Title	Description
Chapter 1, "Hardware Installation"	Provides rack installation and power instructions for the ONS 15454 SDH, including component installation such as cards, cables, electrical interface assemblies (EIAs), and Gigabit Interface Converters (GBICs).
Chapter 2, "Set Up PC and Log Into CTC"	Explains how to install the ONS 15454 SDH 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 15454 SDHs in IP networks and provides scenarios that show nodes in common IP configurations. Also explains how to create static routes and use the Open Shortest Path First (OSPF) protocol.
Chapter 5, "SDH Topologies"	Provides instructions for configuring SNCPs, MS-SPRings, subtending rings, linear 1+1 ADM protection, extended SNCP mesh networks, and DCC tunnels.

Chapter Number and Title	Description
Chapter 6, "Circuits and Tunnels"	Describes how to create standard VC high-order path circuits and VC low-order path tunnels as well as multiple drop circuits, and how to monitor circuits. The chapter also explains how to edit SNCP circuits and create path traces to monitor traffic.
Chapter 7, "Card Provisioning"	Provides procedures for changing the default transmission parameters for ONS 15454 SDH electrical and optical cards. The chapter also includes enabling optical cards for SDH.
Chapter 8, "SDH Performance Monitoring"	Provides performance monitoring thresholds for ONS 15454 SDH electrical and optical cards.
Chapter 9, "Ethernet Operation"	Explains how to use the Ethernet features of the ONS 15454 SDH, including transporting Ethernet traffic over SDH, 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, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.
Chapter 11, "SNMP"	Explains how Simple Network Management Protocol (SNMP) is used with the ONS 15454 SDH.
Appendix A "Circuit Routing"	Explains automated and manual circuit routing in detail.
Appendix B "Regulatory Compliance and Safety Information"	Provides customer, industry, and government requirements met by the ONS 15454 SDH. Installation warnings are also included.
Glossary	Defines commonly used terms.

Related Documentation

The following documentation can be used in conjunction with this manual:

- *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide, Release 3.4*

- *Cisco ONS 15454 SDH Product Overview, Release 3.4*

- *Release Notes for the Cisco ONS 15454 SDH, Release 3.4*

- *Cisco Warranty Services for ONG Products*

- *Installing the Cisco ONS 15454 SDH Conducted Emissions Kit* (Required for EMEA compliance only)

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
Bold text	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

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: 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 online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.

- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Hardware Installation

This chapter provides procedures for installing the Cisco ONS 15454 SDH. See Table 1-1 for a list of installation topics. See Table 1-2 for a list of procedures required to install an ONS 15454 SDH.

Table 1-1   Cisco ONS 15454 SDH Installation Topics

Installation Topics
1.1 Before You Begin, page 1-2
1.2 Rack Installation, page 1-4
1.3 Shelf-Assembly and FMEC Cover Removal and Replacement, page 1-13
1.4 Fan-Tray Assembly Installation, page 1-19
1.5 Ground and Power Installation, page 1-20
1.6 Using the Electrical Facility Connection Assembly, page 1-24
1.7 FMEC Installation, page 1-28
1.8 Installing the Common Control Cards, page 1-31
1.9 Optical, Electrical, and Ethernet Card Installation, page 1-35
1.10 Fiber-Optic Cable Installation, page 1-43
1.11 Cable Routing and Management, page 1-46
1.12 ONS 15454 SDH Shelf Assembly Specifications, page 1-50
1.13 Installation Checklist, page 1-54

Table 1-2   Cisco ONS 15454 SDH Installation-Related Procedures

Installation-Related Procedures
Procedure: Mount the Shelf Assembly in a Rack (One Person), page 1-7
Procedure: Mount the Shelf Assembly in a Rack (Two People), page 1-9
Procedure: Mount Multiple Shelf Assemblies in a Rack, page 1-10
Procedure: Mount the Air Ramp in a Rack, page 1-12
Procedure: Open and Remove the Front Door, page 1-14
Procedure: Reinstall and Close the Front Door, page 1-16
Procedure: Remove the FMEC Cover, page 1-17

Table 1-2   Cisco ONS 15454 SDH Installation-Related Procedures (continued)

Installation-Related Procedures
Procedure: Reinstall the FMEC Cover, page 1-18
Procedure: Install the Fan-Tray Assembly, page 1-19
Procedure: Ground the Shelf Assembly, page 1-21
Procedure: Install ONS 15454 SDH Power FMECs, page 1-22
Procedure: Install ONS 15454 SDH FMECs, page 1-29
Procedure: Verify Successful Turn Up of All FMECs, page 1-30
Procedure: Install the TCC-I Cards, page 1-31
Procedure: Install the XC10G Cards, page 1-33
Procedure: Install the Alarm Interface Controller (AIC-I) Card, page 1-34
Procedure: Install Optical, Electrical, and Ethernet Cards, page 1-37
Procedure: Install Gigabit Interface Converters, page 1-41
Procedure: Remove a Gigabit Interface Converter, page 1-43
Procedure: Install Fiber-Optic Cables on STM-N Cards, page 1-44
Procedure: Install the Fiber Boot, page 1-45
Procedure: Route Fiber-Optic Cables in the Shelf Assembly, page 1-47

1.1 Before You Begin

Read the installation procedures and precautions before you install the ONS 15454 SDH and connect the power source. The ONS 15454 SDH is powered using –48 VDC power. Positive, negative, and ground power terminals are located on Front Mount Electrical Connection (FMEC) cards in the Electrical Facility Connection Assembly (EFCA). Check the equipment lists and gather all necessary tools for proper installation. Install the ONS 15454 SDH 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   **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 power connector and/or 2) when the housing is open.**

Warning   **The ONS 15454 SDH is intended for installation in restricted access areas. A restricted access area is one where service personnel gain access by using a special tool, lock, key, or other means of security. A restricted access area is controlled by the authority responsible for the location.**

Warning   **Ultimate disposal of this product should be handled according to all national laws and regulations.**

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

Note   The ONS 15454 SDH is suitable for mounting on concrete or other non-combustible surfaces only.

Note   In this chapter, shelf assembly refers to the steel enclosure that holds cards and connects power, and node refers to the entire hardware and software system.

1.1.1 Cisco-Supplied Equipment

These materials are required for installation and are supplied with the ONS 15454 SDH. The shipped quantity of each item is in parentheses.

- Double-hole grounding lug for ground connection with a wire receptacle to accommodate the recommended #6 AWG (13.3 mm²) multi-strand copper wire (1)
- M4 x 8 mm pan-head Phillips screws (2)
- M6 x 20 mm socket set screws (2)
- M6 x 20 mm pan-head Phillips screws (8)
- Tie wraps 0.50-in. W x 6.0-in. L (24)
- ESD wrist strap (disposable) (1)
- Pinned Allen key for front door (1)
- Hex key 3-mm long arm (1)
- Bottom brackets for the fan-tray air filter
- Cable assembly, Ethernet, RJ45-RJ45 (1)
- *Cisco ONS 15454 SDH Installation Handbook* (1)
- Power cable (from fuse and alarm panel to assembly) (1)

Caution   Only use the power cable shipped with the ONS 15454 SDH.

1.1.2 User-Supplied Equipment

The following materials and tools are required for installation but are not supplied with the ONS 15454 SDH:

- Equipment rack (ETSI rack, 2200 mm H x 600 mm W x 300 mm D)
- Fuse and alarm panel

- Copper ground cable 13.3 mm² (#6 AWG) stranded, specified for up to 90° Celsius

- Alarm cable pairs for all alarm connections, 0.51 mm² or 0.64 mm² (#22 or #24 AWG), solid-tinned

- Single-mode SC fiber jumpers with UPC polish (55 dB or better) for optical cards

- Coaxial cable terminated with 1.0/2.3 Miniature Coax connectors for FMEC cards

- DB-37 cable

- Shielded building integrated timing supply (BITS)-clock coaxial cable terminated with 1.0/2.3 Miniature Coax connectors

- Labels

Note   Ring runs are not provided by Cisco and can hinder side-by-side shelf installation where space is limited.

1.1.2.1 Tools Needed

To install the ONS 15454 SDH, you need the following tools. These tools are not provided by Cisco.

- #2 Phillips screwdriver

- Medium slot-head screwdriver

- Small slot-head screwdriver

- Video fiber connector inspection instrument

- Cletop cleaning cassette

- Crimping tool—This tool must be large enough to accommodate the girth of the grounding lug when you crimp the grounding cable into the lug.

- Wire stripping tool

1.1.2.2 Test Equipment

To install the ONS 15454 SDH, you need the following test equipment. This equipment is not provided by Cisco.

- Voltmeter

- Power meter (only for use with fiber optics)

- Bit error rate (BER) tester for E1-N-14, E3-12, DS3i-N-12, and FMEC cards

1.2 Rack Installation

You can install up to three ONS 15454 SDHs in an ETSI rack. The shelf assembly has two front doors for added security, a fan-tray assembly module for cooling, and extensive fiber-management space. The EFCA in the upper shelf area provides access to user-defined (external) alarms, controls, and power terminals. Figure 1-1 shows the dimensions of the ONS 15454 SDH. For additional shelf assembly specifications, see the "ONS 15454 SDH Shelf Assembly Specifications" section on page 1-50.

The Cisco ONS 15454 SDH is typically connected to a fuse and alarm panel that provides centralized alarm connection points and distributed power. Fuse and alarm panels are third-party equipment and are not described in this documentation. For information about fuse and alarm panel requirements, consult the documentation for the related equipment.

Warning   **The chassis should be mounted on a rack that is permanently affixed to the floor. Ensure that your equipment rack is bolted to the floor and secured.**

Warning   **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

Warning   **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 45°C (113°F).**

Warning   **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety.**

Warning   **Care must be given when connecting nodes to the supply circuit so that wiring is not overloaded.**

The dimensions of the ONS 15454 SDH are shown in Figure 1-1 on page 1-6.

Figure 1-1   ONS 15454 SDH dimensions
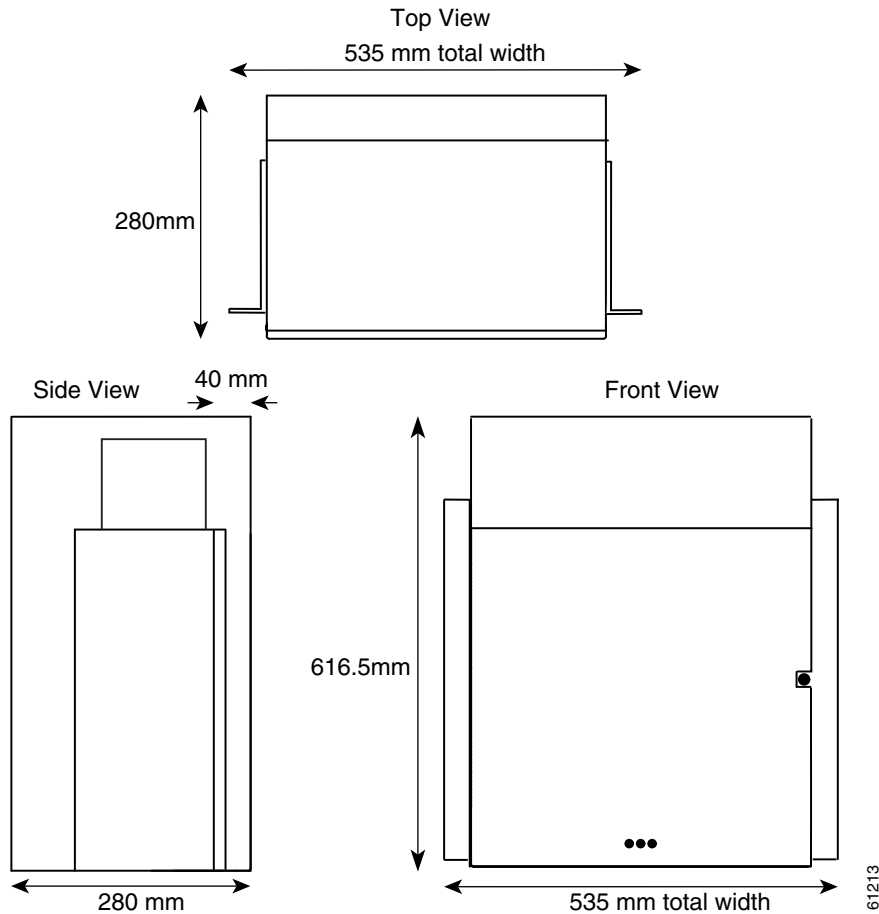
1.2.1 ONS 15454 SDH Bay Assembly

The Cisco ONS 15454 SDH bay assembly simplifies ordering and installing the ONS 15454 SDH because it allows you to order shelf assemblies pre-installed in an ETSI rack. The bay assembly is available in a three-shelf configuration. The three-shelf configuration includes three ONS 15454 SDH shelf assemblies, a slot for third-party fuses and alarm panels, two air ramps and two cable-management trays. A three-shelf ONS 15454 SDH bay assembly is shown in Figure 1-2.

Figure 1-2   Three-shelf ONS 15454 SDH bay assembly

ONS 15454s

Fuse & Alarm Panel,
mountable in the rack
if rack is 2200 mm high
or higher

Air Ramp

Air Ramp

61583
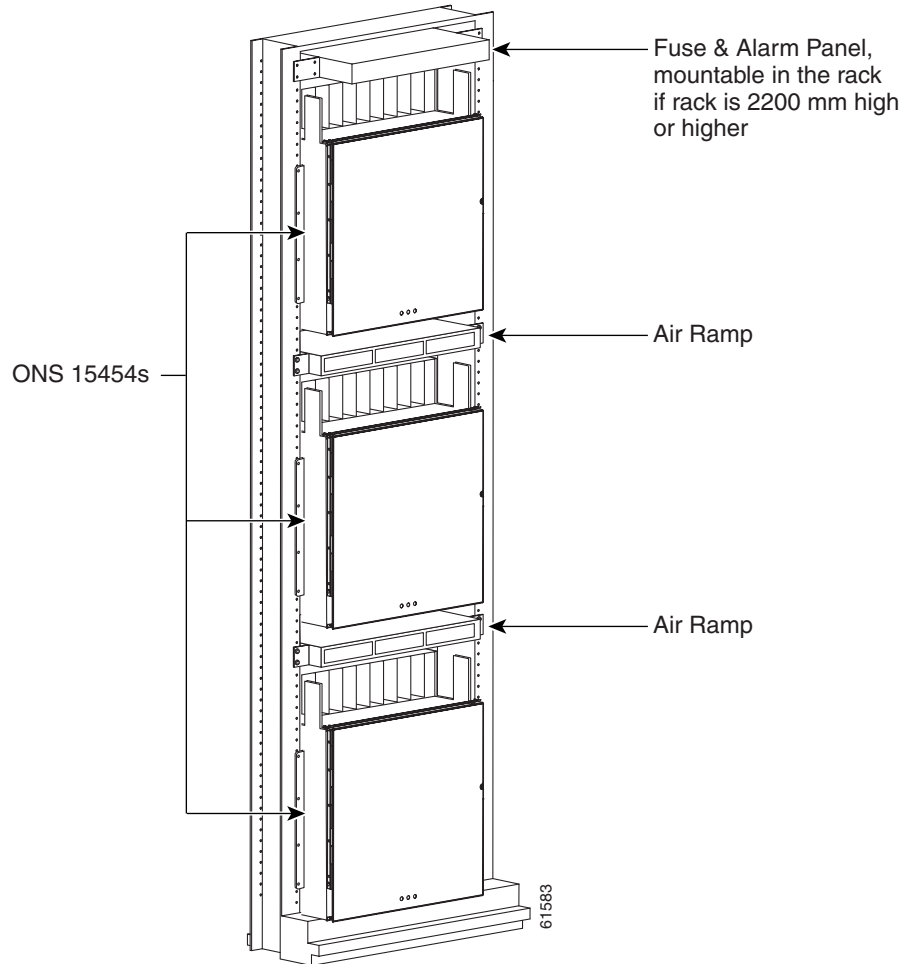
1.2.2 Mount a Single Shelf Assembly

The shelf assembly is most easily installed by two people. However, you can install it alone by using temporary set screws. Reduce extra weight if possible by emptying the shelf assembly and removing the front door. For more information, see the "Open and Remove the Front Door" procedure on page 1-14.

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

Purpose	This procedure allows one person to mount the shelf assembly in a rack. In a single shelf assembly configuration, one air ramp on the top and one air ramp on the bottom of the shelf assembly is recommended.
Tools/Equipment	• Hex tool
	• M6 mounting screws
Onsite/Remote	Onsite

> **Note**   The ONS 15454 SDH requires 616.5 mm (minimum) of vertical rack space and 40 mm below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 SDH is installed above a shelf assembly, the air ramp between the shelves provides space for air flow. To ensure the mounting is secure, use two to four M6 mounting screws for each side of the shelf assembly. A shelf assembly should be mounted at the bottom of the rack if it is the only unit in the rack.

Step 1   Verify that the proper fuse and alarm panel were installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to the manufacturer's instructions.

Step 2   Ensure that the shelf assembly is set for the desired rack size. Figure 1-3 shows the rack-mounting position for the ONS 15454 SDH.

Figure 1-3   Mounting an ONS 15454 SDH in a rack
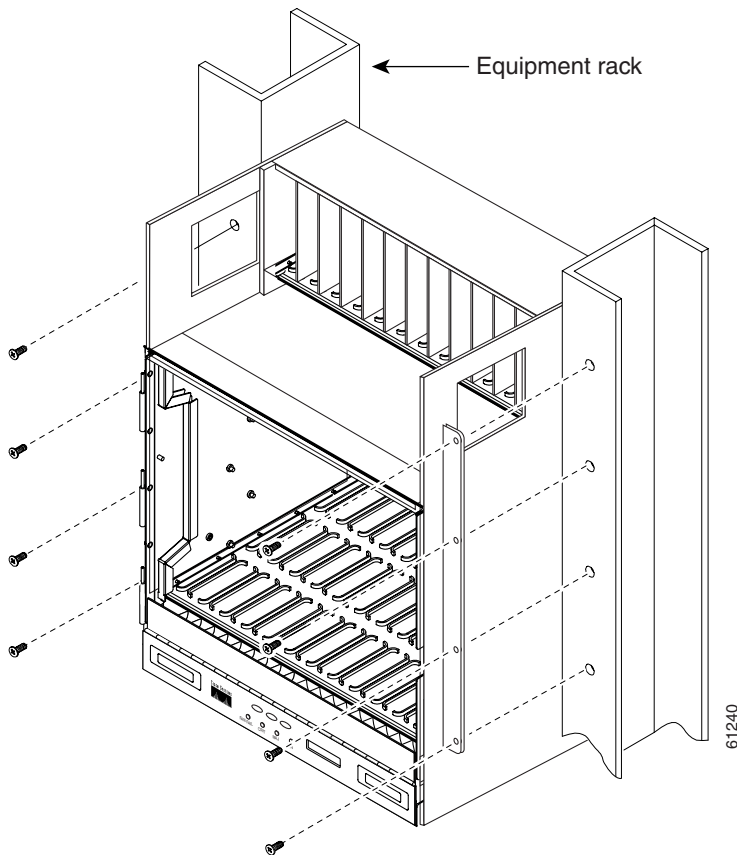
Step 3   Using the hex tool that shipped with the assembly, install the two temporary set screws into the holes that will not be used to mount the shelf. Let the set screws protrude sufficiently to hold the mounting brackets.

Step 4   Lift the shelf assembly to the desired position in the rack.

Step 5   Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 6   Install one mounting screw in each side of the assembly.

Step 7   When the shelf assembly is secured to the rack, install the remaining mounting screws.

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

Step 8   Using the hex tool, remove the temporary set screws.

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

Purpose	This procedure allows two people to mount the shelf assembly in a rack.
Tools/Equipment	• Hex tool
	• M6 mounting screws
Onsite/Remote	Onsite

> **Note**   The ONS 15454 SDH requires 616.5 mm (minimum) of vertical rack space and 40 mm below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 SDH is installed above a shelf assembly, the air ramp between the shelves provides space for air flow. To ensure the mounting is secure, use two to four M6 mounting screws for each side of the shelf assembly. A shelf assembly should be mounted at the bottom of the rack if it is the only unit in the rack.

Step 1   Verify that the proper fuse and alarm panel was installed in the top mounting space. If a fuse and alarm panel has not been installed, you must install one according to the manufacturer's instructions.

Step 2   Ensure that the shelf assembly is set for the desired rack size.

Step 3   Using the hex tool that shipped with the assembly, install the temporary mounting screws into the holes that will not be used to mount the shelf. Let the mounting screws protrude sufficiently to hold the mounting brackets.

Step 4   Lift the shelf assembly to the desired position in the rack.

Step 5   Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 6   Have one person hold the shelf assembly in place while the other person installs one mounting screw in each side of the assembly.

Step 7   When the shelf assembly is secured to the rack, install the remaining mounting screws.

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

Step 8   Remove the temporary mounting screws.

1.2.3 Mount Multiple Shelf Assemblies

The standard ETSI racks can hold three ONS 15454 SDHs and two air ramps. When mounting a shelf assembly in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Procedure: Mount Multiple Shelf Assemblies in a Rack

Purpose	This procedure allows multiple shelves to be assembled in a rack.
Tools/Equipment	• Hex tool
	• M6 mounting screws
Onsite/Remote	Onsite

Note   The ONS 15454 SDH requires 616.5 mm (minimum) of vertical rack space and 40 mm below the installed shelf assembly to allow air flow to the fan intake. If a second ONS 15454 SDH is installed above a shelf assembly, the air ramp between the shelves provides space for air flow. When using third-party equipment above the ONS 15454 SDH, provide a minimum of 40 mm between the third-party unit and the bottom of the ONS 15454 SDH. The third-party equipment must not vent heat upward into the ONS 15454 SDH.

Step 1   Mount the first ONS 15454 SDH in the bottom of the rack using the "Mount the Shelf Assembly in a Rack (One Person)" procedure on page 1-7 or the "Mount the Shelf Assembly in a Rack (Two People)" procedure on page 1-9.

Step 2   Mount the air ramp above the ONS 15454 SDH.

Step 3   Repeat this procedure for every ONS 15454 SDH you need to install.

Step 4   Install the third-party fuse and alarm panel in the top space.

1.2.3.1 Three-Node Configuration

A single ONS 15454 SDH can accommodate up to 120 DS-3/E-3 or 140 E-1 drops. If you need to drop more DS-3s, E-3s, or E-1s than the maximum allowed for a single node, you can link multiple nodes using a fiber-optic bus. However, you cannot merge multiple nodes into a single ONS 15454 SDH. You can use STM-4, STM-16, or STM-64 fiber spans to link the nodes as you would link any other network nodes. Nodes can be colocated in a facility to aggregate local traffic.

Figure 1-4 on page 1-11 shows a three-shelf node setup. Each shelf assembly is identified as a separate node in Cisco Transport Controller (CTC), the ONS 15454 SDH software interface. Traffic must be mapped using CTC cross-connect options. In the figure, each node uses redundant fiber-optic cards. Node 1 uses redundant STM-N transport and STM-N bus cards for a total of four cards. Nodes 2 and 3 each use two redundant STM-N bus cards for a total of four cards, with eight free slots remaining. The three-node example presented here is one of many ways to set up a multiple-node configuration.

Figure 1-4   Three-node fiber-optic bus configuration
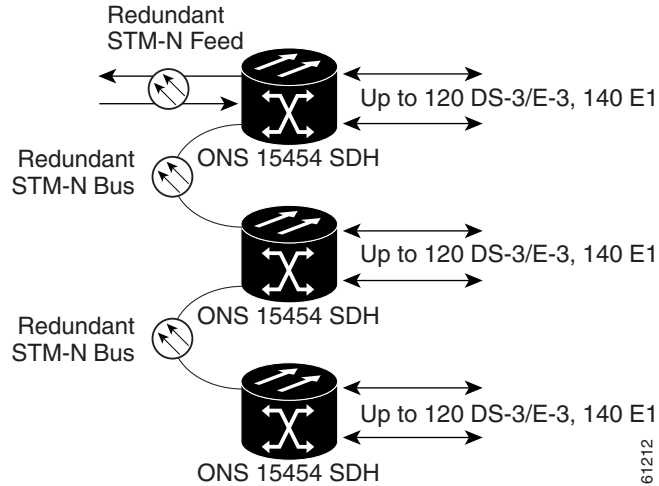
1.2.4 Mount the Air Ramp

The air ramp is needed if you install more than one shelf in the ETSI rack. Install the air ramp below the top shelf assembly. To ensure the air ramp is secure, use one or two M6 mounting screws for each side of the shelf assembly. Figure 1-5 on page 1-12 shows the rack-mounting position for the air ramp.

Note   Install the air ramp after you have connected and routed all cables for the ONS 15454 SDH.

Figure 1-5   *Mounting the air ramp in a rack*
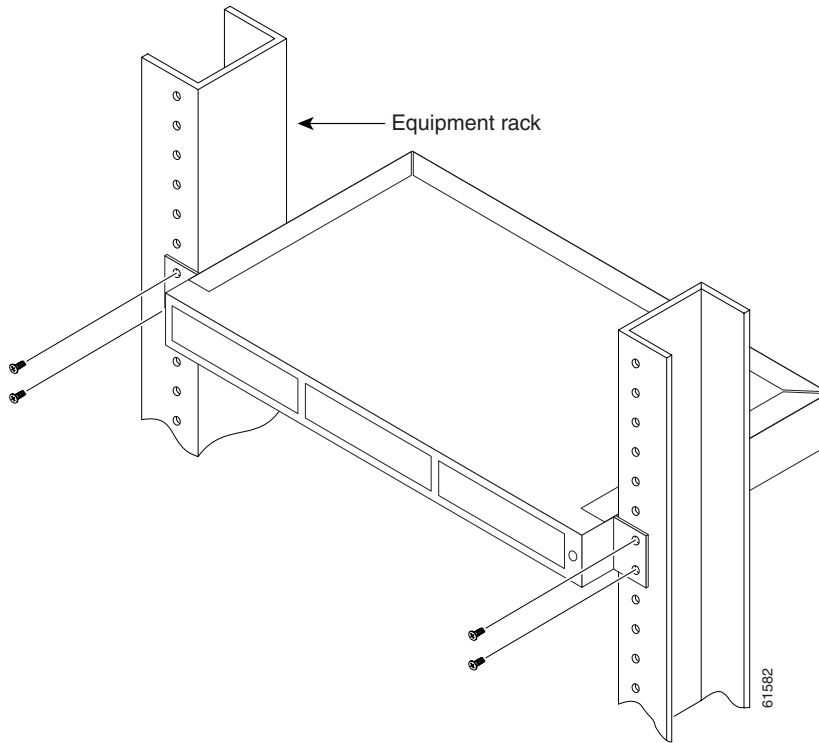
Procedure: Mount the Air Ramp in a Rack

Purpose	This procedure allows air ramps to be installed in a rack.
Tools/Equipment	• Hex tool
	• M6 mounting screws
Prerequisite Procedures	"Mount the Shelf Assembly in a Rack (One Person)" procedure on page 1-7
	"Mount the Shelf Assembly in a Rack (Two People)" procedure on page 1-9
	or "Mount Multiple Shelf Assemblies in a Rack" procedure on page 1-10
Onsite/Remote	Onsite

Step 1   Lift the air ramp to the desired rack position.

Step 2   Align the screw holes on the mounting ears with the mounting holes in the rack.

Step 3   Install one mounting screw in each side of the assembly.

Step 4   When the air ramp is secured to the rack, install the remaining mounting screws if necessary.

1.3 Shelf-Assembly and FMEC Cover Removal and Replacement

The Critical, Major, and Minor alarm LEDs visible through the front door indicate whether a critical, major, or minor alarm is present anywhere in the ONS 15454 SDH. 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.

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

Note When you are done installing/servicing the shelf assembly, the door must be reinstalled. The door serves as the electrical closure for the unit.

Figure 1-6   Front-door erasable label

SHELF ID:			RACK ID:				SERIAL #:			IP ADDRESS:			MAC ADDRESS:			
SLOT NUMBER	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
CARD NAME							TCC___	XC___	—	XC___	TCC___						

PORT ASSIGNMENTS (rows 1–42)

DANGER / GEFAHR / PELIGRO / DANGER / 危險

INVISIBLE LASER RADIATION MAY BE EMITTED FROM THE OPTICAL CARDS AT THE END OF UN-TERMINATED FIBER CABLES OR CONNECTORS. DO NOT STARE INTO THE BEAM OR VIEW DIRECTLY WITH OPTICAL INSTRUMENTS. THIS EQUIPMENT IS A CLASS I (CDRH)/Class 1M (IEC) LASER PRODUCT. THIS PRODUCT COMPLIES WITH THE RADIATION PERFORMANCE STANDARDS OF 21 CFR 1040.10 AND 1040.11, IEC 60825-1 AND IEC 60825-2.

DIE OPTISCHEN KARTEN KÖNNEN MÖGLICHERWEISE AM ENDE NICHT ANGESCHLOSSENER FASERKABEL ODER –STECKVERBINDER UNSICHTBARE LASERSTRAHLEN EMITTIEREN. NICHT IN DEN STRAHL BLICKEN, AUCH NICHT DIREKT MIT OPTISCHEN INSTRUMENTEN. DIESE AUSRÜSTUNG IST EIN LASERPRODUKT DER KLASSE I (CDRH)/Klasse 1M (IEC). DIESES PRODUKT. ERFÜLLT DIE STANDARDS FÜR STRAHLUNGSLEISTUNG 21 CFR 1040.10 UND 1040.11, IEC 60825-1 UND IEC 60825-2.

PODRÍA EMITIRSE RADIACIÓN LÁSER INVISIBLE DE LAS TARJETAS ÓPTICAS EN EL EXTREMO DE LOS CABLES O CONECTORES DE FIBRA ÓPTICA NO TERMINADOS, NO MIRAR DIRECTAMENTE AL HAZ NI VER DIRECTAMENTE CON INSTRUMENTOS ÓPTICOS. ESTE EQUIPO ES UN PRODUCTO DE LÁSER DE CLASE I (CDRH)/Clase 1M (CEI) ESTE PRODUCTO, CUMPLE CON LOS ESTÁNDARES DE DESEMPEÑO DE RADIACIÓN DE 21 CFR 1040.10 Y 1040.11, CEI 60825-1 Y CEI 60825-2.

ÉMISSION POSSIBLE DE RAYONS LASER À PARTIR DES CARTES OPTIQUES SE TROUVANT À L'ÉXTRÉMITÉ DES CONNECTEURS OU DES CÂBLES OPTIQUES NON ABOUTIS. NE PAS REGARDER LE FAISCEAU DIRECTEMENT NI L'EXAMINER À L'AIDE D'INSTRUMENTS OPTIQUES. CET APPAREIL EST UN PRODUIT LASER DE CLASSE I (CDRH)/CLASSE 1M (IEC) CE PRODUIT. EST CONFORME AUX NORMES DE PERFORMANCE DE RAYONNEMENT DE 21 CFR 1040.10 ET 1040.11, IEC 60825-1 ET IEC 60825-2.

未收尾的光纖電纜或接頭末端的光學卡可能會放射向眼看不見的輻射線。
請勿直接目視光束或以光學儀器直接查看。
本設備為CLASS I (CDRH) /第1M類 (IEC) 雷射製品。
本產品符合輻射性能標準（RADIATION PERFORMANCE STANDARDS）
或21CFR1040.10以及1040.11，IEC60825-1和IEC60825-2之規定。

CAUTION
THIS UNIT MAY HAVE MORE THAN ONE POWER CONNECTION. REMOVE ALL CONNECTIONS TO DEENERGIZE THE SYSTEM BEFORE SERVICING TO AVOID ELECTRIC SHOCK.

NO OPERATOR SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED PERSONNEL.

TO MAINTAIN EMI COMPLIANCE, REPLACE FRONT COVER AFTER SERVICING.

ELECTROSTATIC SENSITIVE DEVICES.

VORSICHT
DIESE EINHEIT HAT MÖGLICHERWEISE MEHR ALS EINEN STROMANSCHLUSS. VOR DER WARTUNG ALLE ANSCHLÜSSE ABTRENNEN, UM DAS SYSTEM VOM NETZ ZU TRENNEN, UM ELEKTRISCHE SCHLÄGE ZU VERMEIDEN.

TEILE IM INNEREN KÖNNEN NICHT VOM BEDIENER GEWARTET WERDEN. WARTUNGSARBEITEN SIND VON QUALIFIZIERTEM PERSONAL DURCHZUFÜHREN.

UM EMI-VORSCHRIFTEN ZU ERFÜLLEN, NACH DER WARTUNG VORDERE ABDECKUNG ERNEUT ANBRINGEN.

ELEKTROSTATISCH EMPFINDLICHES GERÄT.

PRECAUCIÓN
ES POSIBLE QUE ESTA UNIDAD TENGA MÁS DE UNA CONEXIÓN ELÉCTRICA. PARA EVITAR CHOQUE ELÉCTRICO, DESCONECTE TODAS LAS CONEXIONES ELÉCTRICAS DEL SISTEMA ANTES DE HACER REPARACIONES.

ESTA UNIDAD NO TIENE PIEZAS QUE PUEDAN SER REPARADAS POR EL USUARIO. LAS REPARACIONES DEBEN SER REALIZADAS POR PERSONAL CUALIFICADO.

PARA CUMPLIR CON LAS REGLAS DE INTERFERENCIA ELECTROMAGNÉTICA. VUELVA A COLOCAR LA CUBIERTA DELANTERA DESPUÉS DE HACER REPARACIONES.

DEPÓSITOS SENSIBLES A LA ENERGÍA ELECTROSTÁTICA.

ATTENTION
CETTE UNITÉ PEUT DISPOSER DE PLUSIEURS RACCORDEMENTS A UNE SOURCE D'ALIMENTATION. DÉBRANCHER LES CONNEXIONS POUR DÉSÉLECTRER LE SYSTÈME ET ÉVITER TOUT RISQUE D'ÉLECTROCUTION.

L'OPÉRATEUR NE DOIT PAS ENTRETENIR LES PIÈCES INTERNES. CONFIER L'ENTRETIEN DE CES PIÈCES A UN PERSONNEL QUALIFIE.

REMPLACEZ LE COUVERCLE AVANT APRÈS AVOIR RÉALISÉ L'ENTRETIEN. CONFORMÉMENT AUX NORMES EMI.

APPAREIL SENSIBLE À L'ÉLECTRICITÉ STATIQUE.

注 意
本設備可能有一個以上的電源接頭。
請在維修前先拔掉所有的連接，切斷本系統的電源，
以免發生電擊的危險。

內部零件須由合格的專業技師進行維修，操作員
不得自行進行維修。

為了保持符合EMI之規定，請在維修後將前蓋蓋好。

本設備有靜電感應。

P/N 47-12460-01

78098

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

Figure 1-7   Laser warning on the front-door label

☀ **DANGER**

GEFAHR
PELIGRO
DANGER
危險

INVISIBLE LASER RADIATION MAY BE EMITTED FROM THE OPTICAL CARDS AT THE END OF UN-TERMINATED FIBER CABLES OR CONNECTORS. DO NOT STARE INTO THE BEAM OR VIEW DIRECTLY WITH OPTICAL INSTRUMENTS. THIS EQUIPMENT IS A CLASS I (CDRH)/Class 1M (IEC) LASER PRODUCT. THIS PRODUCT COMPLIES WITH THE RADIATION PERFORMANCE STANDARDS OF 21 CFR 1040.10 AND 1040.11, IEC 60825-1 AND IEC 60825-2.

DIE OPTISCHEN KARTEN KÖNNEN MÖGLICHERWEISE AM ENDE NICHT ANGESCHLOSSENER FASERKABEL ODER –STECKVERBINDER UNSICHTBARE LASERSTRAHLEN EMITTIEREN. NICHT IN DEN STRAHL BLICKEN, AUCH NICHT DIREKT MIT OPTISCHEN INSTRUMENTEN. DIESE AUSRÜSTUNG IST EIN LASERPRODUKT DER KLASSE I (CDRH)/Klasse 1M (IEC) DIESES PRODUKT. ERFÜLLT DIE STANDARDS FÜR STRAHLUNGSLEISTUNG 21 CFR 1040.10 UND 1040.11, IEC 60825-1 UND IEC 60825-2.

PODRÍA EMITIRSE RADIACIÓN LÁSER INVISIBLE DE LAS TARJETAS ÓPTICAS EN EL EXTREMO DE LOS CABLES O CONECTORES DE FIBRA ÓPTICA NO TERMINADOS. NO MIRAR DIRECTAMENTE AL HAZ NI VER DIRECTAMENTE CON INSTRUMENTOS ÓPTICOS. ESTE EQUIPO ES UN PRODUCTO DE LÁSER DE CLASE I (CDRH)/Clase 1M (CEI) ESTE PRODUCTO. CUMPLE CON LOS ESTÁNDARES DE DESEMPEÑO DE RADIACIÓN DE 21 CFR 1040.10 Y 1040.11, CEI 60825-1 Y CEI 60825-2.

ÉMISSION POSSIBLE DE RAYONS LASER À PARTIR DES CARTES OPTIQUES SE TROUVANT À L'ÉXTRÉMITÉ DES CONNECTEURS OU DES CÂBLES OPTIQUES NON ABOUTIS. NE PAS REGARDER LE FAISCEAU DIRECTEMENT NI L'EXAMINER À L'AIDE D'INSTRUMENTS OPTIQUES. CET APPAREIL EST UN PRODUIT LASER DE CLASSE I (CDRH)/CLASSE 1M (IEC) CE PRODUIT. EST CONFORME AUX NORMES DE PERFORMANCE DE RAYONNEMENT DE 21 CFR 1040.10 ET 1040.11, IEC 60825-1 ET IEC 60825-2.

未收尾的光纖電纜或接頭末端的光學卡可能會放射肉眼看不見的輻射線。
請勿直接目視光束或以光學儀器直接查看。
本設備為CLASS I（CDRH）/第1M類(IEC)雷射製品。
本產品符合輻射性能標準(RADIATION PERFORMANCE STANDARDS)
或21CFR1040.10以及1040.11、IEC60825-1和IEC60825-2之規定。

78099

Procedure: Open and Remove the Front Door

Purpose	Use this procedure to open and remove the front door on the ONS 15454 SDH. The front door covers the shelf assembly, cable-management tray, fan-tray assembly, and LCD screen.
Tools/Equipment	Pinned hex key
Onsite/Remote	Onsite

✏ **Note**   The ONS 15454 SDH has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside of the shelf assembly on the right 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 SDH.

Step 1   Open the front door lock (Figure 1-8). The ONS 15454 SDH 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. A button on the right side of the shelf assembly releases the door.

Step 3   Swing the door open.

Figure 1-8   ONS 15454 SDH front door
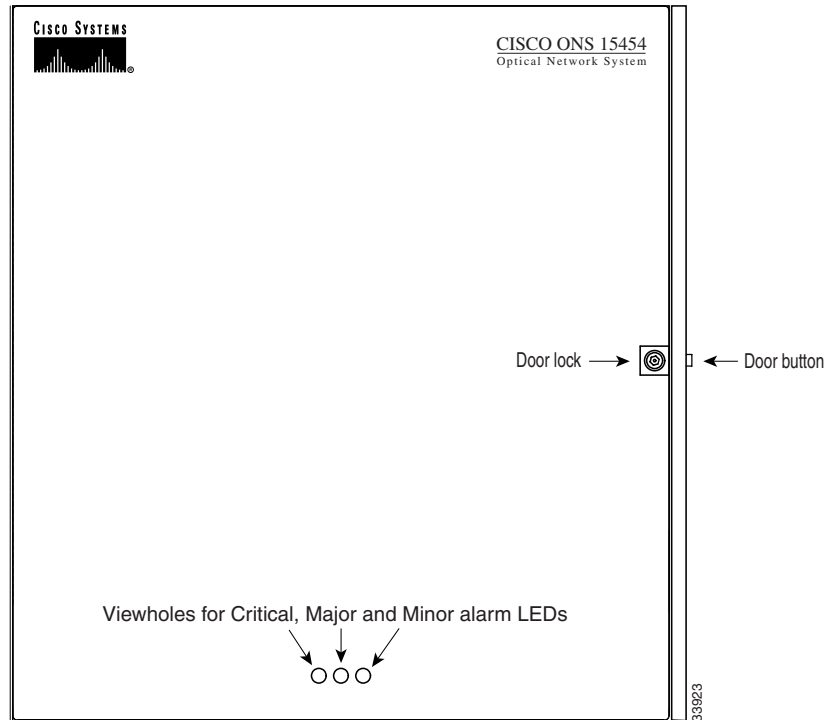
Step 4   Remove the ground wire from the door.

Step 5   Hold the door at the top left corner and remove the door from its hinges (Figure 1-9 on page 1-16).

Figure 1-9   Removing the ONS 15454 SDH front door

Translucent
circles
for LED
viewing

Door hinge

Assembly hinge pin

Assembly hinge

61237
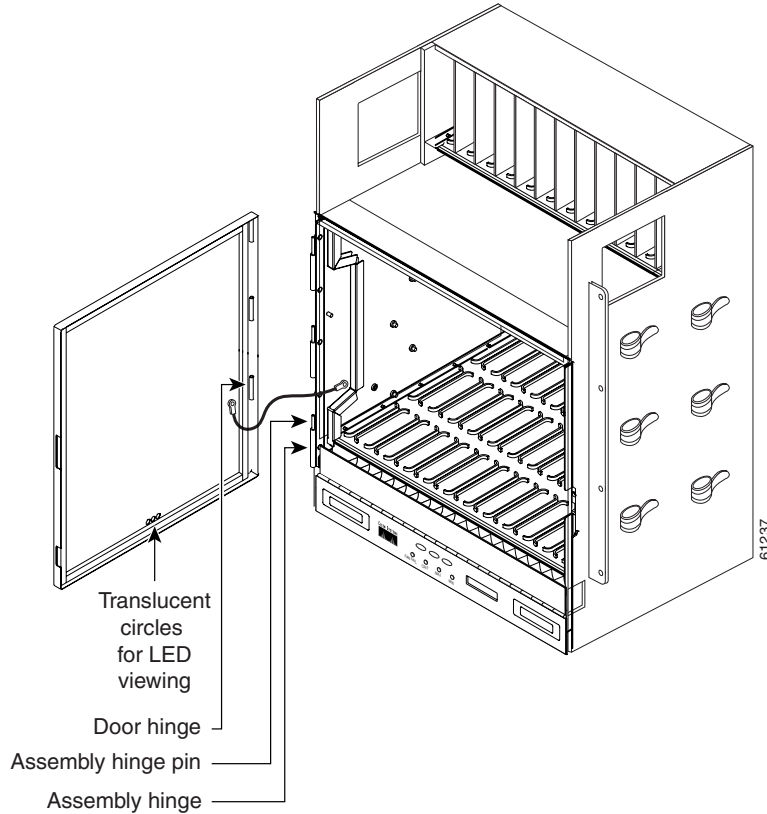
Procedure: Reinstall and Close the Front Door

Purpose	Use this procedure to replace the front door on the ONS 15454 SDH after you finish installing or servicing the shelf assembly.
Tools/Equipment	• Pinned hex key
	• Front door for the ONS 15454 SDH
Onsite/Remote	Onsite

Note   The ONS 15454 SDH has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside of the shelf assembly on the right 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 SDH.

Step 1   Hang the door on its hinges (Figure 1-9).

Step 2   Attach the ground wire.

Step 3   Close the door.

Step 4   Lock the door with the hex key provided, if required by your site practice.

Procedure: Remove the FMEC Cover

Purpose	This procedure explains how to remove the FMEC cover. The ONS 15454 SDH has a screw-in panel over the electrical facility connection assemblies. The FMEC cover protects the FMEC cards.
Tools/Equipment	• FMEC cover
Prerequisite Procedures	—
Onsite/Remote	Onsite

Note   The ONS 15454 SDH has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside of the shelf assembly on the right 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 SDH.

Step 1   Unscrew the screws on the cover as shown in Figure 1-10.

Figure 1-10   Unscrew the FMEC cover
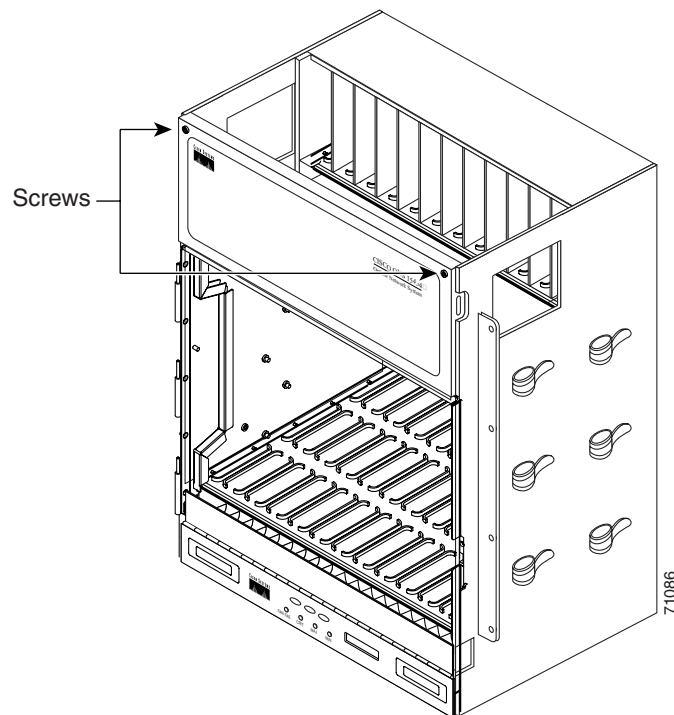
Step 2   Use the handles to pull the cover forward.

Step 3   Remove the ground wire from the left side of the door.

Step 4   Pull the right side of the hinge-locking spring shown in .

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

Figure 1-11   Remove the ONS 15454 SDH cover
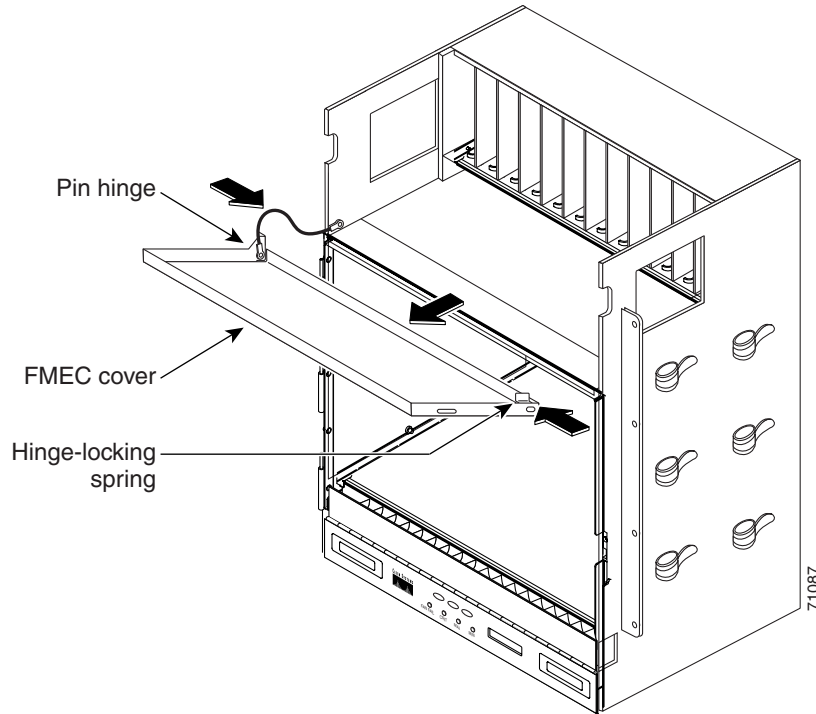
Step 5   Detach the cover from the pin of the hinge shown in Figure 1-11.

Step 6   Remove the cover carefully from the left pin of the hinge shown in Figure 1-11.

Procedure: Reinstall the FMEC Cover

Purpose	This procedure explains how to replace the FMEC cover.
Tools/Equipment	FMEC cover
Prerequisite Procedures	"Remove the FMEC Cover" procedure on page 1-17
Onsite/Remote	Onsite

Step 1   Insert the cover carefully onto the left pin of the hinge labeled as 3 in Figure 1-11.

Step 2   Move the cover to the right side towards the right pin of the hinge.

Step 3   Pull the right side of the hinge-locking spring labeled as 1 in Figure 1-11. Push the cover on the right pin until the spring snaps into place.

Step 4   Attach the ground wire.

Step 5   Attach the cover to the shelf using the screws on the top of the cover.

1.4 Fan-Tray Assembly Installation

The fan-tray assembly is a removable drawer that holds fans and fan-control circuitry for the ONS 15454 SDH. Cisco recommends removing the front door of the chassis when removing or installing the fan-tray assembly. The front of the fan-tray assembly has an LCD screen that provides slot and port-level information for all ONS 15454 SDH card slots, including the number of critical, major, and minor alarms.

Fan speed is controlled by TCC-I 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-I card fails, the fans automatically shift to high speed. The temperature measured by the TCC-I sensors is displayed on the LCD screen.

Note   Error messages appears on the TCC-I, fan-tray LED, and in CTC when the fan-tray assembly is removed from the shelf or when one fan is not working.

Procedure: Install the Fan-Tray Assembly

The fan-tray assembly is located at the bottom of the ONS 15454 SDH. After you install the fan-tray assembly, you only need to open the drawer if a fan fails, or if you need to replace or clean the fan-tray air filter. Do not operate an ONS 15454 SDH without a fan-tray air filter. Refer to the Maintenance Chapter in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* for information about cleaning and maintaining the fan-tray air filter.

Purpose	This procedure explains how to install the fan-tray assembly.
Tools/Equipment	• Fan-tray assembly
	• Air filter
Prerequisite Procedures	"Rack Installation" section on page 1-4
	"Mount the Air Ramp in a Rack" procedure on page 1-12
	"Open and Remove the Front Door" procedure on page 1-14
Onsite/Remote	Onsite

Warning   **Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.**

Step 1   Remove the front door of the shelf assembly. See the "Open and Remove the Front Door" procedure on page 1-14.

Step 2   Install the air filter. The air filter can be installed internally between the fan tray and shelf assembly, or externally by mounting the air filter bracket on the bottom of the shelf assembly. Slide the air filter into the bracket.

Step 3   Install the fan-tray assembly. The fan-tray assembly has locks on the outer edges. Press and hold the locks as you slide the fan-tray assembly into the shelf assembly. The electrical plug at the rear of the tray should plug into the corresponding receptacle on the assembly.

⚠

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

Step 4 To verify that the tray has plugged into the assembly, check that the LCD on the front of the fan-tray assembly is activated. Figure 1-12 shows the fan-tray location.

Figure 1-12   Installing the fan-tray assembly

LCD   Fan tray
             assembly
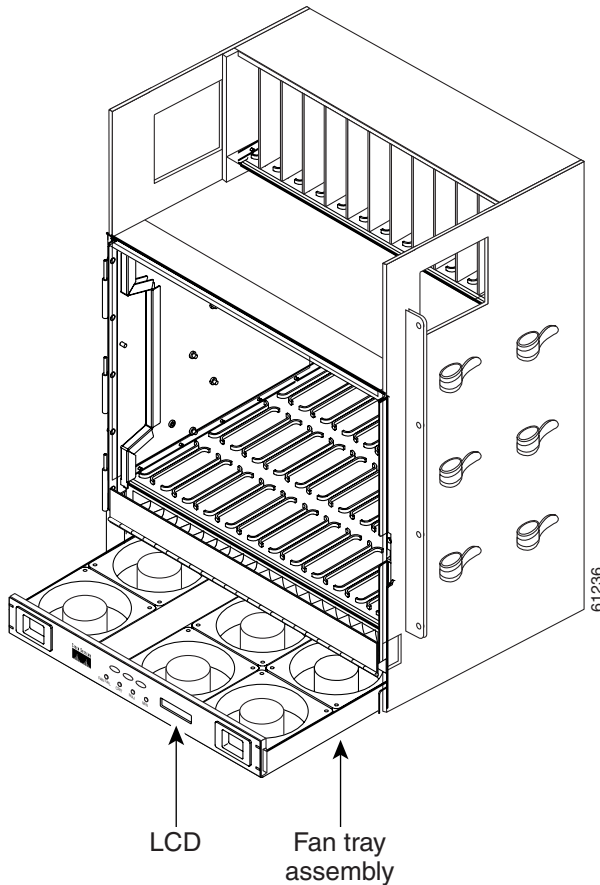
1.5 Ground and Power Installation

This section explains how to connect the ONS 15454 SDH assembly to ground and to the power supply. Ground the equipment according to ITU-T standards or local practices.

⚠

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.**

⚠ **Warning**   **The DC power supply systems (main, redundant, and service battery power supply systems) must be compliant with safety extra low voltage (SELV) requirements in accordance with IEC 60950 and UL 60950.**

⚠ **Warning**   **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

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

Procedure: Ground the Shelf Assembly

Purpose	This procedure explains how to connect the ONS 15454 SDH to earth ground. You must complete this procedure before connecting system power.
Tools/Equipment	• A 2-hole grounding lug—included in the installation kit.
	• Two Phillips head, M6 (metric) machine screws with locking washers—included in the installation kit.
	• Grounding wire—Use #6 AWG (13.3-mm²) copper wire.
	• #2 Phillips screwdriver.
	• Crimping tool—This tool must be large enough to accommodate the girth of the grounding lug when you crimp the grounding cable into the lug.
	• Wire stripping tool.
Prerequisite Procedures	"Rack Installation" section on page 1-4
	"Mount the Air Ramp in a Rack" procedure on page 1-12
	"Open and Remove the Front Door" procedure on page 1-14
	"Install the Fan-Tray Assembly" procedure on page 1-19
Onsite/Remote	Onsite

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

Step 1   Use a wire-stripping tool to remove approximately 0.75 inch (19 mm) of the covering from the end of the grounding wire.

Step 2   Insert the stripped end of the grounding wire into the open end of the grounding lug.

Step 3   Use the crimping tool to secure the grounding wire in two different places in the grounding lug.

Step 4   Locate the grounding receptacle on the side panel of the shelf (see Figure 1-13 on page 1-22).

Step 5   Place the grounding lug against the grounding receptacle on the side panel of the shelf.

Step 6   Insert one of the screws through the locking washer and through the hole in the grounding lug. Insert the screw into the threaded holes on the right side of the shelf. Ensure that the grounding lug will not interfere with other system hardware or rack equipment.

Step 7   Repeat Step 6 with the second screw.

Step 8   Prepare the other end of the grounding wire and connect it to an appropriate grounding point in your site to ensure adequate earth ground for the shelf.

Figure 1-13   Grounding the ONS 15454 SDH

Ground
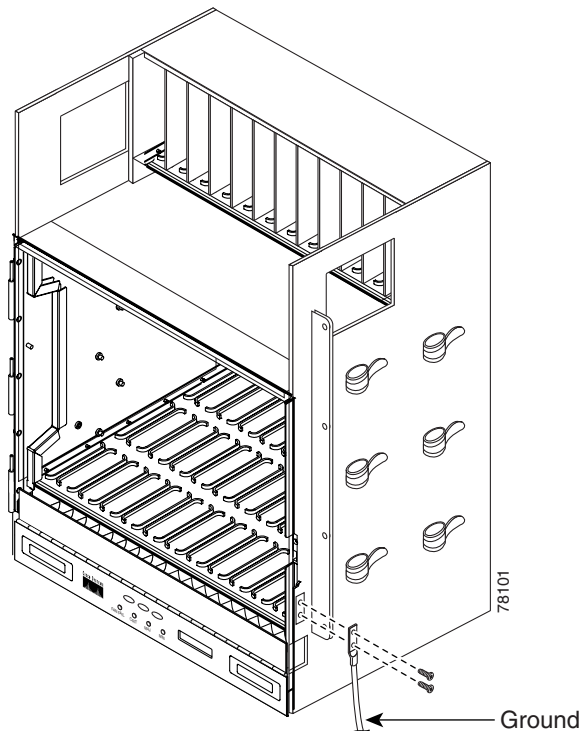
Procedure: Install ONS 15454 SDH Power FMECs

For proper system operation, both the MIC-A/P card and the MIC-C/T/P card must be installed in the shelf. If the system loses power or if both TCC-I cards are reset, you must reset the ONS 15454 SDH clock. After powering down, the date defaults to January 1, 1970, 00:04:15. To reset the clock, see the "Set Up Network Information" section on page 3-5.

Note   No more than 2 m (7 ft) of the power supply cable should be exposed between the equipment and the cable-management tray.

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

Purpose	Use this procedure to install the redundant power connections for the ONS 15454 SDH. The MIC-A/P and MIC-C/T/P FMECs use –48 VDC.
Tools/Equipment	• MIC-A/P FMEC with Phillips screws
	• MIC-C/T/P FMEC with Phillips screws
	• #2 Phillips screwdriver
	• Power cable shipped with the ONS 15454 SDH

⚠

Caution   Only use the power cable shipped with the ONS 15454 SDH.

Prerequisite Procedures	"Rack Installation" section on page 1-4
	"Mount the Air Ramp in a Rack" procedure on page 1-12
	"Open and Remove the Front Door" procedure on page 1-14
	"Install the Fan-Tray Assembly" procedure on page 1-19
	"Ground the Shelf Assembly" procedure on page 1-21
Onsite/Remote	Onsite

⚠

Caution   Ensure that the frame ground connection is made before installing power FMECs.

⚠

Caution   Do not apply power to the ONS 15454 SDH until you complete all installation steps and check the continuity of the –48 VDC battery and battery return.

⚠

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

Step 1   Insert the MIC-A/P FMEC in Slot 23 and the MIC-C/T/P FMEC in Slot 24 of the EFCA.

Step 2   Tighten the #2 Phillips screws on the FMEC faceplates into the EFCA assembly ONS 15454 SDH.

Step 3   Attach the connector on the end of the cable to the power FMEC.

Step 4   Tighten the screws of the connector on the power cable.

Step 5   Connect the power cable to the fuse panel or power source. Use the pin connection in Table 1-3 for the connections. The conductor (green with yellow stripes) is used for secondary grounding such as grounding to the rack.

Table 1-3   Pin Connection of the Power FMECs

Pins	Function	Cable Color
A1	Battery return	Black
A2	–48V battery	Red
A3	Ground	Green with yellow stripes

Note Only use listed compression-type connectors when terminating the battery, battery return, and ground conductors. Connectors must be suitable for copper conductors.

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

Caution Do not apply power to the ONS 15454 SDH until you complete all installation steps.

1.6 Using the Electrical Facility Connection Assembly

The ONS 15454 SDH has an Electrical Facility Connection Assembly (EFCA) located at the top of the shelf. The EFCA provides connection for installing external alarms, timing input and output, and craft interface terminals. This section describes the EFCA and the pin assignments for the field.

1.6.1 Alarm Installation

The MIC-A/P FMEC provides connection for alarm contacts into and out of the shelf assembly. The pin connectors, signal names, and functions are listed in Table 1-4.

Table 1-4   Alarm Pin Assignments

DB-62 Pin Connector	Signal Name	Function
1	ALMCUTOFF–	Alarm cutoff
2	ALMCUTOFF+	Alarm cutoff
3	ALMINP0–	Alarm input pair number 1
4	ALMINP0+	Alarm input pair number 1
5	ALMINP1–	Alarm input pair number 2
6	ALMINP1+	Alarm input pair number 2
7	ALMINP2–	Alarm input pair number 3
8	ALMINP2+	Alarm input pair number 3
9	ALMINP3–	Alarm input pair number 4
10	ALMINP3+	Alarm input pair number 4
11	EXALM0–	Extra alarm 0
12	EXALM0+	Extra alarm 0
13	FGND	Ground
14	EXALM1–	Extra alarm 1
15	EXALM1+	Extra alarm 1

Table 1-4   Alarm Pin Assignments (continued)

DB-62 Pin Connector	Signal Name	Function
16	EXALM2–	Extra alarm 2
17	EXALM2+	Extra alarm 2
18	EXALM3–	Extra alarm 3
19	EXALM3+	Extra alarm 3
20	EXALM4–	Extra alarm 4
21	EXALM4+	Extra alarm 4
22	EXALM5–	Extra alarm 5
23	EXALM5+	Extra alarm 5
24	EXALM6–	Extra alarm 6
25	EXALM6+	Extra alarm 6
26	FGND	Ground
27	EXALM7–	Extra alarm 7
28	EXALM7+	Extra alarm 7
29	EXALM8–	Extra alarm 8
30	EXALM8+	Extra alarm 8
31	EXALM9–	Extra alarm 9
32	EXALM9+	Extra alarm 9
33	EXALM10–	Extra alarm 10
34	EXALM10+	Extra alarm 10
35	EXALM11–	Extra alarm 11
36	EXALM11+	Extra alarm 11
37	ALMOUP0–	Normally open output pair number 1
38	ALMOUP0+	Normally open output pair number 1
39	FGND	Ground
40	ALMOUP1–	Normally open output pair number 2
41	ALMOUP1+	Normally open output pair number 2
42	ALMOUP2–	Normally open output pair number 3
43	ALMOUP2+	Normally open output pair number 3
44	ALMOUP3–	Normally open output pair number 4
45	ALMOUP3+	Normally open output pair number 4
46	AUDALM0–	Normally open minor audible alarm
47	AUDALM0+	Normally open minor audible alarm
48	AUDALM1–	Normally open major audible alarm
49	AUDALM1+	Normally open major audible alarm
50	AUDALM2–	Normally open critical audible alarm
51	AUDALM2+	Normally open critical audible alarm

Table 1-4   Alarm Pin Assignments (continued)

DB-62 Pin Connector	Signal Name	Function
52	FGND	Ground
53	AUDALM3–	Normally open remote audible alarm
54	AUDALM3+	Normally open remote audible alarm
55	VISALM0–	Normally open minor visible alarm
56	VISALM0+	Normally open minor visible alarm
57	VISALM1–	Normally open major visible alarm
58	VISALM1+	Normally open major visible alarm
59	VISALM2–	Normally open minor visible alarm
50	VISALM2+	Normally open minor visible alarm
61	VISALM3–	Normally open minor visible alarm
62	VISALM3+	Normally open minor visible alarm

1.6.2 Timing Installation

The MIC-C/T/P provides 1.0/2.3 Miniature Coax connectors that are used for timing input and output. The bottom connectors are for "1" timing, and the top connectors are for "2" timing. In each case, the left connector is the input and the right connector is the output. The input connectors for timing provide a 75-ohm termination. System cables are available that can convert timing clocks from 75 ohms to 100/120 ohms. Table 1-5 shows MIC-C/T/P pin assignments.

A high-impedance option (> 3 kohms or greater) is possible through a jumper on the MIC-C/T/P FMEC. You can change the top timing input to high impedance by removing the jumper on P3 on the MIC-C/T/P FMEC. You can change the bottom timing input to high impedance by removing the jumper on P2 on the MIC-C/T/P FMEC.

Note   Refer to ITU-T G.813 for rules about provisioning timing references.

Table 1-5   MIC-C/T/P Pin Assignment

PIN	Functions
IN 1	Input from external device
OUT 1	Output to external device
IN 2	Input from external device
OUT 2	Output to external device

For information about configuring timing in CTC, see "Setting Up ONS 15454 SDH Timing" section on page 3-18.

1.6.3 Modem Interface Installation

The modem connector of the MIC-C/T/P FMEC on the ONS 15454 SDH EFCA is reserved for future use.

1.6.4 Craft Interface Installation

You can use the CRAFT connector of the MIC-C/T/P FMEC on the ONS 15454 SDH EFCA to connect a workstation such as a VT100-type craft interface. Table 1-6 shows the pin assignments for the CRAFT connector.

Table 1-6   Craft Interface Pin Assignments

RJ-45 Pins	Function
1	—
2	BADMDTR
2	BADMTXD
4	BADMGND
5	BADMGND
6	BADMRXD
7	—
8	—

1.6.5 LAN Installation

Use the LAN connection of the MIC-C/T/P FMEC on the ONS 15454 SDH to connect the ONS 15454 SDH to a workstation, an Ethernet LAN, or a LAN modem for remote access to the node. For more information about the ONS 15454 SDH craft interface software (CTC) and how to connect to a LAN modem, see Chapter 2, "Set Up PC and Log Into CTC." Table 1-7 shows the LAN pin assignments.

Before you can connect an ONS 15454 SDH to other ONS 15454 SDHs or to a LAN, you must change the default IP address that is shipped with each ONS 15454 SDH (192.168.0.2). See the "Change IP Address, Default Router, and Network Mask Using the LCD" procedure on page 3-7.

.

Table 1-7   LAN Pin Assignments

LAN	RJ-45 Pin	Function
LAN 1 Connecting to DCE[1] (a hub or switch)	1	PNMSRX+
	2	PNMSRX–
	3	PNMSTX+
	4	—
	5	—
	6	PNMSTX–
	7	—
	8	—

Table 1-7   LAN Pin Assignments (continued)

LAN	RJ-45 Pin	Function
LAN 2 Connecting to DTE (a PC/workstation or router)	1	PRCKRX+
	2	PRCKRX−
	3	PRCKTX+
	4	—
	5	—
	6	PRCKTX−
	7	—
	8	—

1. The Cisco ONS 15454 SDH is DCE.

1.7 FMEC Installation

⚠

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

1.7.1 Slot Requirements

The ONS 15454 SDH EFCA has 12 FMEC slots numbered sequentially from left to right. Slots 18 to 22 and 25 to 29 provide electrical connections for the corresponding slots. They can host FMEC-E1, FMEC-E3/DS3, and FMEC-DS1/E1. Assignment is as follows:

- FMEC Slot 18 supports an electrical card in Slot 1.
- FMEC Slot 19 supports an electrical card in Slot 2.
- FMEC Slot 20 supports an electrical card in Slot 3.
- FMEC Slot 21 supports an electrical card in Slot 4.
- FMEC Slot 22 supports an electrical card in Slot 5.
- FMEC Slot 23 is used for the alarm and power card called the MIC-A/P.
- FMEC Slot 24 supports the timing, craft, and power card called the MIC-C/T/P.
- FMEC Slot 25 supports an electrical card in Slot 13.
- FMEC Slot 26 supports an electrical card in Slot 14.
- FMEC Slot 27 supports an electrical card in Slot 15.
- FMEC Slot 28 supports an electrical card in Slot 16.
- FMEC Slot 29 supports an electrical card in Slot 17.

Shelf assembly slots have symbols indicating the type of cards that you can install in them. Each ONS 15454 SDH FMEC has a corresponding symbol. The symbol on the FMEC must match the symbol on the slot. Table 1-8 shows the slot-FMEC symbol definitions.

Table 1-8   Slot and FMEC Symbols

Color/Shape	Definition
Orange/Circle	Electrical 75-ohm E-1 connection via 1.0/2.3 Miniature Coax connectors. Only install ONS 15454 SDH FMECs with a circle symbol on the faceplate.
Orange/Circle	Electrical 120-ohm E-1 connection via DB-37 connectors. Only install ONS 15454 SDH FMECs with a circle symbol on the faceplate.
Green/Star	Electrical 75-ohm E3/DS3 connection via 1.0/2.3 Miniature Coax connectors. Only install ONS 15454 SDH FMECs with a star symbol on the faceplate.
Red/Vertical ellipse	System power and interface for external alarms. Only install ONS 15454 SDH FMECs with a vertical ellipse symbol on the faceplate.
Red/Horizontal ellipse	System power and LAN timing. Only install ONS 15454 SDH FMECs with a horizontal ellipse symbol on the faceplate.

Table 1-9 lists the number of ports, line rates, connector options, and connector locations for ONS 15454 SDH electrical FMECs.

Table 1-9   FMEC, Ports, Line Rates, and Connectors

FMEC	Ports	Line Rate per Port	Connector Types	Connector Location
FMEC-E1	14	2.048 MBits/s (Mbps)	1.0/2.3 Miniature Coax connector	EFCA
FMEC-DS1/E1	14	2.048 MBits/s (Mbps)	DB-37	EFCA
FMEC-E3/DS3	12	34.368MBits/s (Mbps) 44.736 MBits/s (Mbps)	1.0/2.3 Miniature Coax connector	EFCA

Procedure: Install ONS 15454 SDH FMECs

Purpose	Use this procedure to install FMECs on the ONS 15454 SDH.
Tools/Equipment	• FMEC with Phillips screws
	• #2 Phillips screwdriver
Prerequisite Procedures	"Rack Installation" section on page 1-4
	"Mount the Air Ramp in a Rack" procedure on page 1-12
	"Open and Remove the Front Door" procedure on page 1-14
	"Install the Fan-Tray Assembly" procedure on page 1-19
	"Ground the Shelf Assembly" procedure on page 1-21
	"Install ONS 15454 SDH Power FMECs" procedure on page 1-22
Onsite/Remote	Onsite

Warning **Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.**

Step 1   Hold the FMEC by the faceplate.

Step 2   Slide the FMEC along the guide rails into the desired FMEC slot. See the "Slot Requirements" section on page 1-28 for slot assignments.

Figure 1-14   Installing FMECs on the ONS 15454 SDH
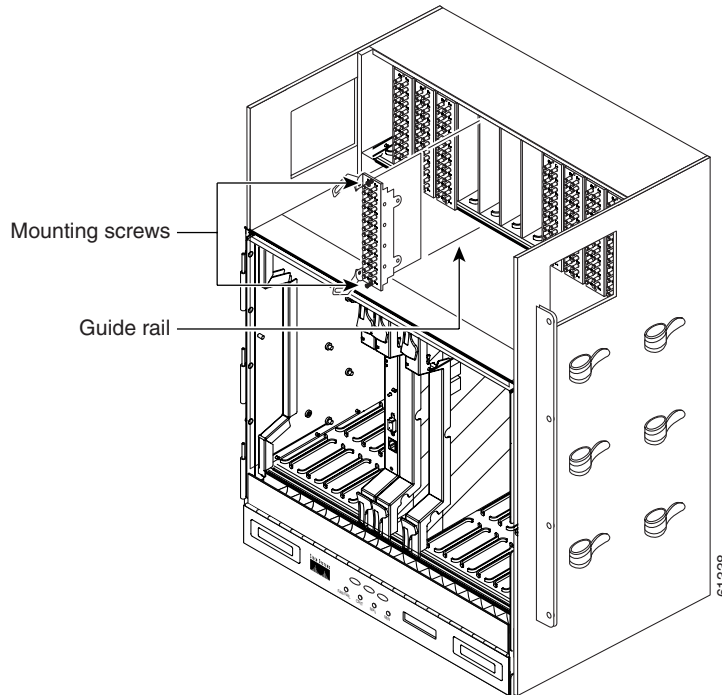
Step 3   Push the FMEC gently into the connector. The ONS 15454 SDH FMECs plug into electrical connectors on the back panel of the shelf assembly when the screws are tightened. Figure 1-14 shows FMEC installation.

Step 4   Tighten the screws.

Procedure: Verify Successful Turn Up of All FMECs

Purpose	Use this procedure to verify FMEC installation. The procedure for turning up ONS 15454 SDH FMECs is identical for each FMEC card. An unused FMEC slot should be filled with a blank faceplate (Cisco P/N 15454E-BLANK).
Prerequisite Procedures	"Install ONS 15454 SDH Power FMECs" procedure on page 1-22
	"Install ONS 15454 SDH FMECs" procedure on page 1-29
Onsite/Remote	Onsite

Step 1   Install the FMEC in the correct slot.

Step 2   Verify that power is applied to the shelf assembly.

Step 3   Verify that the FMEC appears in the correct slot in the CTC node view.

Step 4   Verify that the FMEC is white in the CTC node view.

Warning   **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

1.8 Installing the Common Control Cards

This section describes how to install the common control cards. You will need two Timing, Communication, and Control-International (TCC-I) cards, and two 10 Gigabit Cross Connect (XC10G) cards per node. This section also describes how to install the Alarm Interface Controller-International (AIC-I) card if required.

Warning   **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the back panel of the shelf assembly with your hand or any metal tool due to electrical hazard.**

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

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

Follow the recommended card installation order:

1. Complete the "Install the TCC-I Cards" procedure on page 1-31.

2. Complete the "Install the XC10G Cards" procedure on page 1-33.

3. Complete the "Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34, if necessary.

4. Turn to the table of contents, list of procedures, or index to locate any other procedures that you need to perform for your site.

Procedure: Install the TCC-I Cards

Purpose	This procedure installs redundant TCC-I cards. The first card you install in the ONS 15454 SDH must be a TCC-I, and it must initialize before you install any cross-connect or traffic cards.
Tools/Equipment	Two TCC-I cards per node

Prerequisite Procedures	Measure the voltage.
Onsite/Remote	Onsite

Step 1   Open the latches/ejectors of the first TCC-I card that you will install.

Step 2   Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 7 or 11).

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

> ✎
> **Note**   It is possible to close the latches/ejectors when the card is not completely plugged into the back panel of the shelf assembly. Ensure that you cannot insert the card any further. If you insert a card into a slot provisioned for a different card, all LEDs turn off.

Step 4   Verify the LED activity, as follows:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds. If the red FAIL LED does not illuminate, check the power.

2. The red FAIL LED blinks for 35 to 45 seconds.

3. The red FAIL LED remains illuminated 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. (The ACT/STBY LED may take several minutes to illuminate while the data communications channel [DCC] processor boots.)

> ✎
> **Note**   Alarm LEDs may be illuminated; disregard alarm LEDs until you are logged into CTC and can view the Alarms tab.

> ✎
> **Note**   When a newly installed TCC-I card has a different version of the ONS 15454 SDH software installed than the version running on the active TCC-I, the newly installed TCC-I card automatically copies the software version running on the active TCC-I. You do not need to do anything in this situation. However, the loading TCC-I 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-I card. After loading the new software for approximately 30 minutes, the TCC-I card becomes the standby card and the amber LED is illuminated.

Step 5   Verify that the ACT/STBY LED is green for active. The IP address for the node, the temperature of the ONS 15454 SDH, and the time of day will be displayed on the LCD. The default time and date is 12:00 AM, January 1, 1970.

Step 6   The LCD cycles through the IP address, node name, and software version. Verify that the correct software version displays on the LCD.

Step 7   If the LCD shows the correct software version, continue with Step 8. If the LCD does not show the correct software version, upgrade the software or remove the TCC-I card and install a replacement card.

Step 8   Open the latches/ejectors of the second TCC-I card and repeat Step 2 to Step 7. The second TCC-I ACT/STBY LED should be amber for standby.

Procedure: Install the XC10G Cards

Purpose	This procedure installs the XC10G cards.
Tools/Equipment	Two XC10G (cross-connect) cards per node
Prerequisite Procedures	Measure the voltage.
	"Install the TCC-I Cards" procedure on page 1-31
Onsite/Remote	Onsite

Step 1   Open the latches/ejectors of the first XC10G card that you will install.

Step 2   Use the latches/ejectors to firmly slide the card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10).

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

> **Note**   It is possible to close the latches/ejectors when the card is not completely plugged into the back panel of the shelf assembly. Ensure that you cannot insert the card any further.

Step 4   Verify the LED activity, as follows:

  1.   The red LED turns on and remains illuminated for 20 to 30 seconds.

  2.   The red LED blinks for 35 to 45 seconds.

  3.   The red LED remains illuminated for 5 to 10 seconds.

  4.   All LEDs blink once and turn on.

  5.   The ACT/STBY LED turns on.

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

  > **Note**   If the red FAIL LED does not illuminate, check the power.

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

Step 5   Verify that the ACT/STBY LED is green for active.

Step 6   Use the latches/ejectors to firmly slide the second cross-connect card along the guide rails until the card plugs into the receptacle at the back of the slot (Slot 8 or 10) and repeat Step 2 to Step 4. The second XC10G should have an amber ACT/STBY LED.

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

Procedure: Install the Alarm Interface Controller (AIC-I) Card

Purpose	Use this procedure to install the AIC-I card. The AIC-I card has input and output alarm contact closures and orderwire functions. The AIC-I card must be used with Software R3.4. The AIC-I is not compatible with Software R3.3.
Tools/Equipment	AIC-I card
Prerequisite Procedures	Measure the voltage.
	"Install the TCC-I Cards" procedure on page 1-31
	"Install the XC10G Cards" procedure on page 1-33
Onsite/Remote	Onsite

Step 1   Open the latches/ejectors on the AIC-I card.

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

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

> **Note**   It is possible to close the latches/ejectors when the card is not completely plugged into the back panel of the shelf assembly. Ensure that you cannot insert the card any further.

Step 4   Verify the LED activity, as follows:

1. The red FAIL LED starts blinking 1 second after the card is installed, then blinks for up to 10 seconds until the TCC has detected the AIC-I card.

2. After the TCC detects the AIC-I card, the PWR A and PWR B LEDs illuminate red and the two INPUT/OUTPUT LEDs illuminate green for several seconds.

3. The PWR A and PWR B LEDs turn green, the INPUT/OUTPUT LEDs turn off, and the ACT LEDs illuminates.

> **Note**   If the red FAIL LED does not illuminate, check the power.

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

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

Step 5   Verify that the MIC-A/P FMEC provides connection for alarm contacts into and out of the shelf assembly. For more information, see the "Alarm Installation" section on page 1-24.

1.9 Optical, Electrical, and Ethernet Card Installation

This section describes how to install ONS 15454 SDH optical, electrical, and Ethernet cards. The card installation order is important. Here is the proper sequence:

1. TCC-I cards, see the "Install the TCC-I Cards" procedure on page 1-31.

2. XC10G cards, see the "Install the XC10G Cards" procedure on page 1-33.

3. AIC-I cards, see the "Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34.

4. Optical cards, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37.

5. Electrical cards, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37.

6. Ethernet cards, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37.

Note   All cards boot from the active TCC-I card, which houses the ONS 15454 SDH software. Therefore, you must install the TCC-I card to boot any other cards. See Chapter 2, "Set Up PC and Log Into CTC" for information about the TCC-I card and software versions. See "Install the TCC-I Cards" procedure on page 1-31 for TCC-I installation procedures.

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

ONS 15454 SDH cards have electrical plugs at the back that plug into electrical connectors on the back panel of the shelf assembly. When the card ejectors are fully closed, the cards plug into the back panel of the shelf assembly. Figure 1-15 on page 1-39 shows card installation.

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

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

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).**

Warning   **Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.**

1.9.1 Slot Requirements

The ONS 15454 SDH shelf assembly has 17 card slots that are numbered sequentially from left to right. Slots 1 to 4 and 14 to 17 are multispeed slots. They can host any ONS 15454 SDH traffic card except OC48 ELR/STM16 EH 100 GHz and OC192/STM64. Slots 5, 6, 12, and 13 are high-speed slots. They can host any ONS 15454 SDH card.

Slots 7 and 11 are dedicated to TCC-I cards. Slots 8 and 10 are dedicated to XC10G cards. Slot 9 is used for the AIC-I card. Slots 3 and 15 can host E1N-14 and DS3i-N-12 cards that are used in 1:N protection schemes.

Note   Do not operate the ONS 15454 SDH with a single TCC-I card or a single 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 the slots. Each ONS 15454 SDH card has a corresponding symbol. The symbol on the card must match the symbol on the slot. Table 1-10 shows the slot and card symbol definitions.

Table 1-10   Slot and Card Symbols

Color/Shape	Definition
Orange/Circle	Multispeed slot (all traffic cards except OC48ELR/STM16 EH 100 GHz and OC192/STM64). Only install ONS 15454 SDH cards with a circle symbol on the faceplate.
Blue/Triangle	High-speed slot (all traffic cards). Only install ONS 15454 SDH cards with circle or a triangle symbol on the faceplate.
Purple/Square	TCC-I slot. Only install ONS 15454 SDH cards with a square symbol on the faceplate.
Green/Cross	XC10G slot. Only install ONS 15454 SDH cards with a cross symbol on the faceplate.
Red/P	Protection slot in 1:N protection schemes.
Red/Diamond	AIC-I slot. Only install ONS 15454 SDH cards with a diamond symbol on the faceplate. This slot is not used in this ONS 15454 SDH release and must be covered with a BLANK.
Brown/Star	Multispeed slot for future use.

Table 1-11 lists the number of ports, line rates, connector options, and connector locations for ONS 15454 SDH optical and electrical cards.

Table 1-11   Card Ports, Line Rates, and Connectors

Card	Ports	Line Rate per Port	Connector Types	Connector Location
E1N-14	14	2.048 MBits/s (Mbps)	1.0/2.3 Miniature Coax (via FMEC-E1)[1] DB-37 (via FMEC-DS1/E1)[1]	EFCA
E3-12	12	34.368MBits/s (Mbps)	1.0/2.3 Miniature Coax (via FMEC-E3/DS3)[1]	EFCA
DS3i-N-12	12	44.736 MBits/s (Mbps)	1.0/2.3 Miniature Coax (via FMEC-E3/DS3)[1]	EFCA
E100T-G	12	100 MBits/s (Mbps)	RJ-45	Faceplate
E1000-2-G	2	1000 MBits/s (Mbps)	SC (GBIC)	Faceplate
G1000-4	4	1000 MBits/s (Mbps)	SC (GBIC)	Faceplate
OC3 IR 4/STM1 SH 1310	4	155 MBits/s (Mbps)	SC	Faceplate
OC12/STM4-4	4	622 MBit/s (Mbps) per port	SC	Faceplate
OC12 IR/STM4 SH 1310	1	622 MBits/s (Mbps)	SC	Faceplate
OC12 LR/STM4 LH 1310	1	622 MBits/s (Mbps)	SC	Faceplate
OC12 LR/STM4 LH 1550	1	622 MBits/s (Mbps)	SC	Faceplate
OC48 IR/STM16 SH AS 1310	1	2.488 GBits/s (Gbps)	SC	Faceplate
OC48 LR/STM16 LH AS 1550	1	2.488 GBits/s (Gbps)	SC	Faceplate
OC48 ELR/STM16 EH 100 GHz	1	2.488 GBits/s (Gbps)	SC	Faceplate
OC192 LR/STM64 LH 1550	1	9.95 GBits/s (Gbps)	SC	Faceplate

1. 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 back panel of the shelf assembly and becomes active when the working card fails. The protect card then uses the physical connection of the failed card.

Procedure: Install Optical, Electrical, and Ethernet Cards

Purpose	Use this procedure to install optical, electrical, and Ethernet cards. The procedure for installing these cards is the same, but you must install the optical cards before installing the electrical cards. An unused card slot should be filled with a blank faceplate (Cisco P/N 15454E-BLANK).
Tools/Equipment	Cards you want to install

Prerequisite Procedures   "Install the TCC-I Cards" procedure on page 1-31

"Install the XC10G Cards" procedure on page 1-33

"Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34 (optional)

Onsite/Remote   Onsite

⚠️
Warning   **Invisible laser radiation can 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 can pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified can result in hazardous radiation exposure.**

⚠️
Warning   **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the back panel of the shelf assembly with your hand or any metal tool due to electrical hazard.**

⚠️
Warning   **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

⚠️
Caution   Before installing an OC192 LR/STM64 LH 1550 card, make sure the safety key on the faceplate is in the off position (labeled 0). When the safety key is in the on position (labeled 1), the laser is activated.

✎
Note   The optical (STM-N) card faceplates have SC connectors. Fiber-optic cables are routed to the front of cards. Electrical cards (such as the E1-N-14, the E3-12, and the DS3i-N-12) require EFCAs as cable-connection points for the shelf assembly.

Step 1   Open the card ejectors.

Step 2   Slide the card along the guide rails into the correct slot (Figure 1-15).

Figure 1-15   Installing cards in the ONS 15454 SDH

Ejector   Guide rail
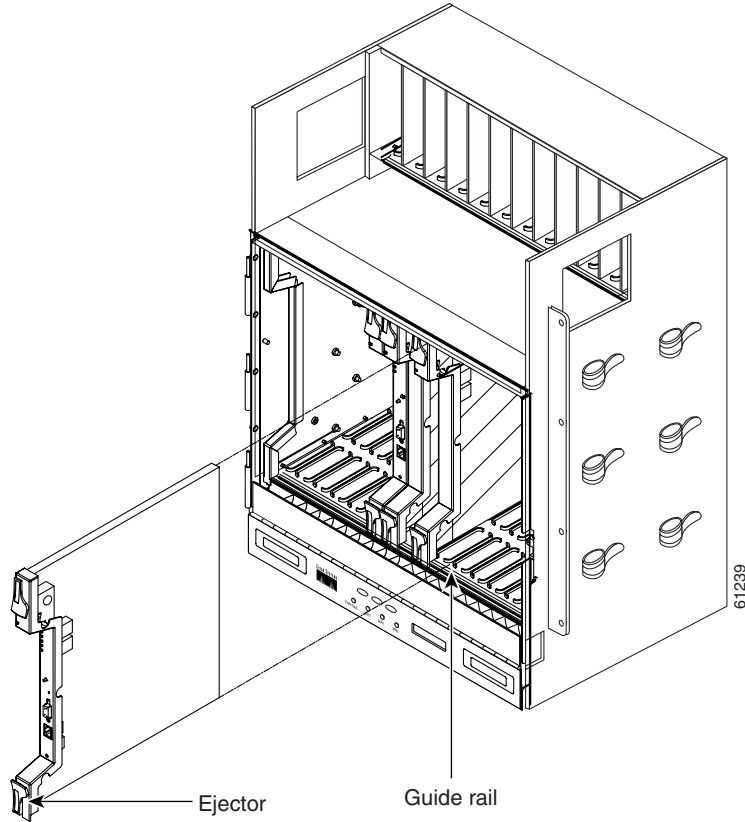
Step 3   Close the ejectors.

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

Step 5   Verify the LED activity, as described in Table 1-12.

Table 1-12   LED Activity During Optical and Electrical Card Installation

Card Type	LED Activity
STM1, STM4, STM4-4, STM16, STM64	1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds. 2. The red FAIL LED blinks for 35 to 45 seconds. 3. All LEDs blink once and turn off. 4. The ACT/STBY LED turns on.
E1N-14, DS3i-N-12, E3-12	1. The red FAIL LED turns on and remains illuminated for 10 to 15 seconds. 2. The red FAIL LED blinks for 30 to 40 seconds. 3. All LEDs blink once and turn off. 4. The ACT/STBY LED turns on.
Ethernet	1. The red FAIL LED turns on and remains illuminated for 10 to 15 seconds. 2. The red FAIL LED blinks for 30 to 40 seconds. 3. All LEDs blink once and turn off. 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 Use CTC to verify that the card appears in the correct slot on the CTC node view. See Chapter 2, "Set Up PC and Log Into CTC" for CTC information and setup instructions.

1.9.2 Card Software Installation

After you install an ONS 15454 SDH card in a valid card slot, the card software automatically updates to the version that operates correctly with the system software installed on the TCC-I. When the TCC-I is writing to the active or standby TCC-I, its Active or Standby LED will blink. To prevent memory corruption, do not pull the TCC-I out during this time.

You can use CTC inventory commands to configure the card software. See Chapter 7, "Card Provisioning" for more information.

1.9.3 Gigabit Interface Converter

Gigabit Interface Converters (GBICs) are hot-swappable input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC determines the maximum distance that the Ethernet traffic will travel from the card to the next network device.

Cisco provides two GBIC models for the E1000-2-G card and three for the G1000-4 card. The E1000-2-G supports the 15454E-GBIC-SX= for short-reach applications and the 15454E-GBIC-LX= for long-reach applications. The short-reach model connects to multimode fiber up to 550 m long. The long-reach model requires single-mode fiber up to 10 km long. The G1000-4 card supports both the 15454E-GBIC-SX= and 15454E-GBIC-LX= and additionally the 15454E-GBIC-ZX= for extra long-reach applications on the 1550-nm wavelength for up to eighty kilometers. Because the GBICs are very similar in appearance, check the GBIC label carefully before installing it. For a description of GBICs and their capabilities, see Chapter 9, "Ethernet Operation." A Gigabit Interface Converter is shown in Figure 1-16.

Figure 1-16   Gigabit Interface Converter
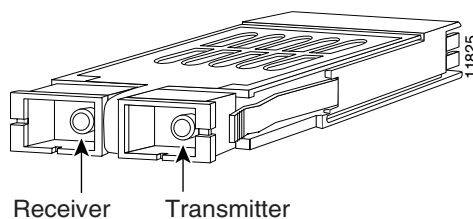
Table 1-13 shows the available GBICs.

Table 1-13   Available GBICs

GBIC	Product Number
Short-reach (1000BaseSX)	15454E-GBIC-SX=

Table 1-13   Available GBICs (continued)

GBIC	Product Number
Long-reach (1000BaseLX)	15454E-GBIC-LX=
Extra-long-reach (1000BaseZX) (for G1000-4 only)	15454E-GBIC-ZX=

Procedure: Install Gigabit Interface Converters

Purpose	Use this procedure to install the appropriate GBICs for your Ethernet cards.
Tools/Equipment	For E1000-2-G use either:
	• 15454E-GBIC-SX= for short-reach applications
	• 15454E-GBIC-LX= for long-reach applications
	For the G1000-4 card use either:
	• 15454E-GBIC-SX= for short-reach applications
	• 15454E-GBIC-LX= for long-reach applications
	• 15454E-GBIC-ZX= for extra long-reach applications
Onsite/Remote	Onsite

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 1-17 on page 1-42).

GBICs are hot-swappable and can be installed or removed when the card or shelf assembly is powered and running.

Note   GBICs are keyed to prevent incorrect installation.

Figure 1-17   Installing a GBIC on an E1000-2 card
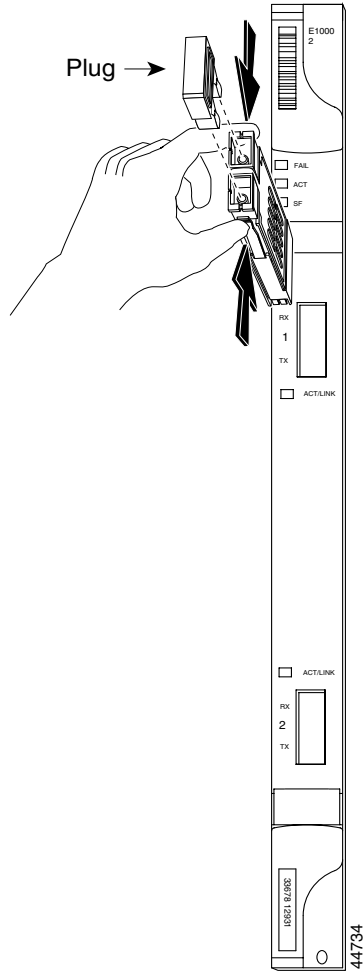
Step 4   Slide the GBIC through the cover flap until you hear a click.

The click indicates the GBIC is locked into the slot.

Note   GBICs are Class-1 laser products. These products have been tested and comply with Class-1 limits.

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

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 1-46 for routing instructions.

Procedure: Remove a Gigabit Interface Converter

Purpose	Use this procedure to remove the appropriate GBICs for your Ethernet cards.
Prerequisite Procedures	"Install Gigabit Interface Converters" procedure on page 1-41
Onsite/Remote	Onsite

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

⚠

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

Step 2   Release the GBIC from the slot by simultaneously squeezing the two plastic tabs 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.

1.10 Fiber-Optic Cable Installation

To install fiber-optic cables in the ONS 15454 SDH, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the ONS 15454 SDH cards. On optical card ports, the top connector is transmit and the bottom connector is receive. Cisco recommends that you label the transmit and receive and the working and protect at each end of the fiber span to avoid confusion. For information about fiber cable management, see the "Optical Cable Management" section on page 1-46.

⚠

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

⚠

Warning   **Invisible laser radiation can 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 can pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified can result in hazardous radiation exposure.**

⚠

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).**

✎

Note   Do not use fiber loopbacks with the OC192 LR/STM64 LH 1550 card unless you are using a 20-dB attenuator. Never connect a direct fiber loopback. Using fiber loopbacks causes irreparable damage to the OC192 LR/STM64 LH 1550 card.

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

Purpose	This section explains how to install optical fibers on STM-N cards. STM-N cards feature SC connectors.
Tools/Equipment	Fiber optic cabling
Prerequisite Procedures	"Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37
Onsite/Remote	Onsite

Note   Clean and inspect 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 1-18 shows the cable location.

Figure 1-18   Installing fiber-optic cables
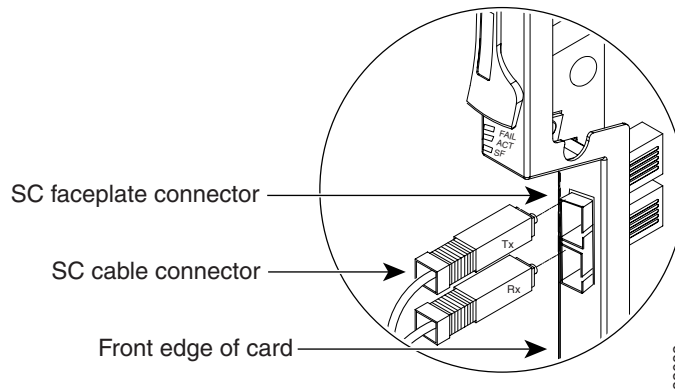
Step 2   Align the keyed ridge of the cable connector with the receiving slot on the faceplate connection point.

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

Step 4   Route fiber cables through the cable retaining clips on the optical card faceplate into the cable management tray on the bottom of the shelf assembly.

Step 5   From the cable management tray, route the fiber cables out of the nearest side of the shelf assembly through the cutout holes.

Procedure: Install the Fiber Boot

Purpose	Use this procedure to install fiber boots. Cisco provides clear plastic fiber boots for the STM-1, STM-4, and STM-16 cards. The boots prevent hanging fibers from bending too sharply and degrading performance. The boots also prevent the front door from interfering with hanging fibers. Figure 1-19 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.
Tools/Equipment	Fiber boot
Prerequisite Procedures	"Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37
Onsite/Remote	Onsite

Note The fiber boot does not support the OC-48 IR/STM-16 SH AS 1310, OC-48 LR/STM-16 LH AS 1550, or OC-192 LR/STM64 LH 1550 cards. The boots are not necessary for these cards because of the angled SC connectors on the cards.

Step 1   Position the open slot of the fiber boot under 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, (see Figure 1-19 on page 1-45).

Figure 1-19   Attaching a fiber boot
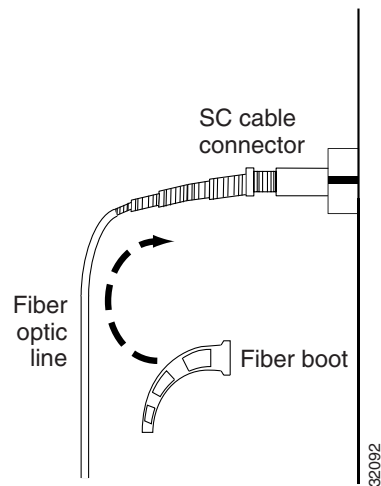
1.11 Cable Routing and Management

The ONS 15454 SDH 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 cable-routing channel opening that maintain the proper fiber-bend radius
- A fold-down door that provides access to the cable-management tray
- Cable tie-wrap facilities on Electrical Interface Assembly (EIA)s that secure cables to the cover panel
- Reversible jumper-routing fins that enable you to route cables out of either side by positioning the fins as desired
- Jumper-slack-storage reels (2) on each side panel that reduce fiber slack between connected devices

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

Note To remove the reels, unscrew the screw in the center of each reel.

Figure 1-20 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 1-20   Managing cables on the front panel

Reversible jumper routing fins

Fold down front door
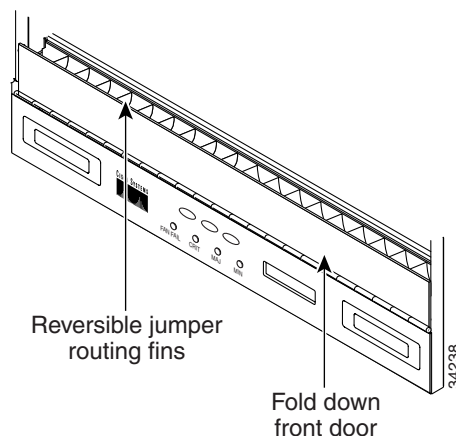
1.11.1 Optical Cable Management

Optical cables connect to the SC connectors on the faceplates of optical cards and GBICs. Route optical cables down through the fiber management clips on the optical card faceplate (shown in Figure 1-21) 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.

Procedure: Route Fiber-Optic Cables in the Shelf Assembly

Purpose	Use this procedure to route optical cable neatly into the cable management area.
Prerequisite Procedures	"Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37
	"Install Gigabit Interface Converters" procedure on page 1-41
	"Install Fiber-Optic Cables on STM-N Cards" procedure on page 1-44
Onsite/Remote	Onsite

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 (Figure 1-21).

Figure 1-21   Routing fiber-optic cables on the optical-card faceplate
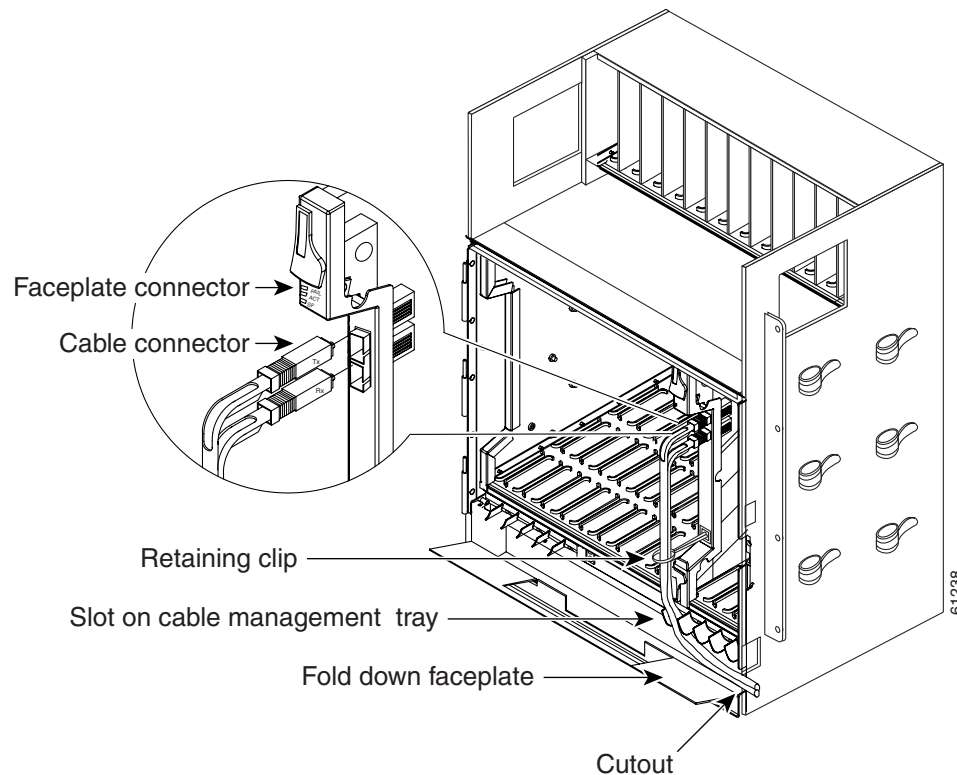
Step 3   GBICs do not have fiber clips. If you are routing optical cable from an E1000-2-G or G1000-4 card, skip to Step 5.

Step 4   Route the cables into the cable-management tray.

Step 5   Route the cables out either side of the cable-management tray and through the cutouts on each side of the shelf assembly. Use the reversible fiber guides to route cables out of the desired side.

Step 6   Close the fold-down front door when all cables in the front compartment are properly routed.

Figure 1-22 shows the fold-down front door of the shelf assembly opened to display the cable-routing channel.

Figure 1-22   Fold-down front door of the cable-management tray (displaying the cable routing channel)
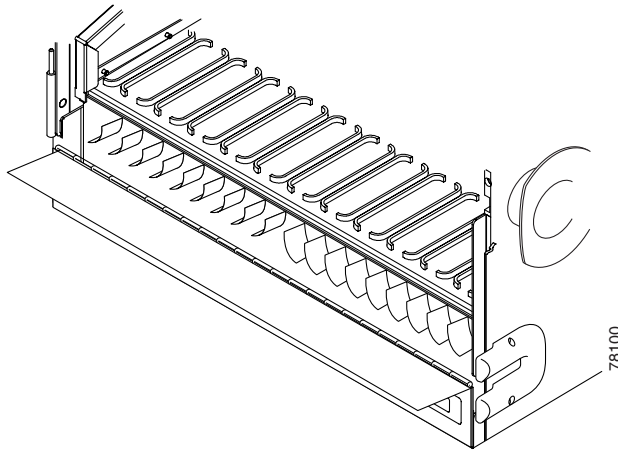
1.11.2 Coaxial Cable Management

Purpose	Use this procedure to route coaxial cable in the cable management area. Coaxial cables connect to FMEC-E1, FMEC-E3/DS3, and MIC-C/T/P cards on the ONS 15454 SDH EFCA.
Tools/Equipment	Coaxial cable
Prerequisite Procedures	"Install ONS 15454 SDH Power FMECs" procedure on page 1-22
	"Install ONS 15454 SDH FMECs" procedure on page 1-29
Onsite/Remote	Onsite

Step 1   Route the coaxial cables according to local site practice and through the side cutouts on either side of the ONS 15454 SDH. The rubber-coated edges of the side cutouts prevent the cables from chafing.

Note   When using the coaxial cable with 1.0/2.3 Miniature Coax connectors, remember that the maximum distance available depends on the loss of the cable. Generally, thinner cable has a lower maximum distance available than standard cable. If, for example, you only use the RG179 cable, the maximum available distance is 15 m (50 ft) versus 137 m (450 ft) available with the larger RG59 cable.

Step 2   Use short pigtails to terminate the shelf assembly.

Step 3   Use standard coaxial cable connected to the thinner cable for the remainder of the cable run. When using a 3-m (10-ft) section of the RG179, you can attach a maximum length of 133 m (437 ft) of RG59. When using a 9-m (30-ft) section of RG179, you can attach a maximum length of 95 m (311 ft) of RG59.

The shorter maximum distance for RG179 is due to a higher attenuation for the thinner cable. The attenuation for RG59 cable (based upon testing with Belden 923, the equivalent of 328A cable) is ~1.0 dB/30 m (~1.0 dB/100 ft) for the DS-3 data rate. The attenuation of RG179 is 6.3 db/30 m (6.3 db/100 ft). Use a cable loss figure of 5.0 dB for calculations. When using different types of coaxial cable, refer to the data sheets of these cables for loss calculation.

1.11.3 FMEC-DS1/E1 Cable Management

DB-37 cables connect to FMEC-DS1/E1 on the ONS 15454 SDH EFCA. Route the cables according to local site practice and through the side cutouts on either side of the ONS 15454 SDH. The rubber-coated edges of the side cutouts prevent the cables from chafing.

1.11.4 Alarm Cable Management

Alarm cables connect to the MIC-A/P card on the ONS 15454 SDH EFCA. Route the cables according to local site practice and through the side cutouts on either side of the ONS 15454 SDH. The rubber-coated edges of the side cutouts prevent the cables from chafing.

1.11.5 Timing Cable Management

Coaxial timing cables connect to the MIC-C/T/P card on the ONS 15454 SDH EFCA. Cable attenuation is allowed up to 6 dB at 2 MHz. Route the cables according to local site practice and through the side cutouts on either side of the ONS 15454 SDH. The coated edges of the side cutouts prevent the cables from chafing.

1.11.6 Craft Cable Management

Craft cables connect to the MIC-C/T/P card on the ONS 15454 SDH EFCA. Route the cables according to local site practice and through the side cutouts on either side of the ONS 15454 SDH. The coated edges of the side cutouts prevent the cables from chafing.

1.11.7 LAN Cable Management

LAN cables connect to the MIC-C/T/P card on the ONS 15454 SDH EFCA. Route the cables according to local site practice and through the side cutouts on either side of the ONS 15454 SDH. The coated edges of the side cutouts prevent the cables from chafing.

1.12 ONS 15454 SDH Shelf Assembly Specifications

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

1.12.1 Bandwidth

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

1.12.2 Slot Assignments for Cards

- Total card slots:
  - 17 slots (1 to 17) in the lower part of the shelf for common cards, electrical cards, and optical cards
  - 12 slots (18 to 29) in the upper part of the shelf for FMECs
- Multispeed slots (any card speeds up to OC48/STM16): Slots 1 to 4, 14 to 17
- High-speed slots (any card speeds up to OC192/STM64): Slots 5, 6, 12, 13
- Slots 6 and 12 are not to be used for electrical cards because they have no corresponding FMEC slots
- TCC-I: Slots 7 and 11
- XC10G (cross-connect): Slots 8 and 10
- AIC-I: Slot 9

1.12.3 Slot Assignments for FMECs

- FMEC Slot 18 supports an electrical card in Slot 1.
- FMEC Slot 19 supports an electrical card in Slot 2.
- FMEC Slot 20 supports an electrical card in Slot 3.
- FMEC Slot 21 supports an electrical card in Slot 4.
- FMEC Slot 22 supports an electrical card in Slot 5.
- FMEC Slot 23 is used for the alarm and power card called the MIC-A/P.
- FMEC Slot 24 supports the timing, craft, and power card called the MIC-C/T/P.
- FMEC Slot 25 supports an electrical card in Slot 13.
- FMEC Slot 26 supports an electrical card in Slot 14.
- FMEC Slot 27 supports an electrical card in Slot 15.
- FMEC Slot 28 supports an electrical card in Slot 16.
- FMEC Slot 29 supports an electrical card in Slot 17.

1.12.4 ONS 15454 SDH Cards

- TCC-I
- XC10G
- AIC-I
- E1-N-14
- DS3i-N-12
- E3-12
- STM1 SH 1310
- STM4 SH 1310-4
- STM4 SH 1310
- STM4 LH 1310
- STM4 SH 1550
- STM16 SH AS 1310
- STM16 LH AS 1550
- STM16 EH 100 GHz
- STM64 LH 1550
- E100-G
- E1000-2-G
- G1000-4
- BLANK (Faceplate)

Note   The STM-1, STM-4, STM-16, E1000-2-G, and G1000-4 cards are Class-1 laser products (according to both IEC 60825-1 2001-01 and 21CFR 1040.10 and 1040.11)."

Note   The STM-64 card is a Class-1M laser product (IEC 60825-1 2001-01)/Class-1 laser product (21CFR 1040.10 and 1040.11).

1.12.5 ONS 15454 SDH FMECs

- FMEC-E1
- FMEC-E3/DS3
- FMEC-DS1/E1
- MIC-A/P
- MIC-C/T/P
- BLANK-FMEC (faceplate)

1.12.6 Configurations

- Digital cross-connect
- Terminal mode
- Linear add/drop multiplexer
- 2-fiber multiplex section-shared protection ring (MS-SPRing)
- 4-fiber MS-SPRing
- Multi-ring interconnection
- Subnetwork connection protection (SNCP)
- Extended SNCP
- Virtual rings
- Hybrid SDH network topology
- Regenerator mode
- Wavelength multiplexer

1.12.7 Cisco Transport Controller

- 10 Base-T
- TCC-I access: RJ-45 connector
- EFCA access: LAN RJ-45 connector

1.12.8 External LAN Interface

- 10BaseT Ethernet
- EFCA access: LAN pin field

1.12.9 Modem Interface

- Hardware flow control
- 10BaseT
- EFCA access: MODEM RJ-45 connector

1.12.10 Alarm Interface

- Visual: Critical, Major, Minor, Remote
- Audible: Critical, Major, Minor, Remote
- Alarm contacts: open contact maximum 60 VDC, closed contact 2 mA
- EFCA access: Alarm-pin fields, 62-pin DB connectors

1.12.11 Database Storage

- Nonvolatile memory: 128 MB, 3.0V FLASH memory

1.12.12 Timing Interface

- 2 x coaxial inputs
- 2 x coaxial outputs
- EFCA access: BITS 1.0/2.3 Miniature Coax connector

1.12.13 System Timing

- Stratum 3E, per ITU-T G.813
- Free-running accuracy: ± 4.6 ppm
- Holdover stability: 3.7×10^{-7}/day, including temperature (< 255 slips in first 24 hours)
- Reference: External BITS, line, internal

1.12.14 Power Specifications

- Input voltage: –48 VDC
- Power consumption: Configuration dependent, 53W for fan tray
- Power Requirements:
  - Nominal: –48 VDC
  - Tolerance limits: –40.5 to –57.0 VDC
- Power terminals: 3WK3 Combo-D Power Cable Connector

1.12.15 Environmental Specifications

- Operating temperature: 0 to +40 degrees Celsius
- Operating humidity: 5 to 95%, noncondensing

1.12.16 Dimensions

- Height: 616.5 mm (24.27 inches)
- Width: 535 mm (17 inches) without mounting ears attached
- Depth: 280 mm (11.02 inches)
- Weight: 26 kg empty (57.3 lb)

1.12.17 Compliance

- Safety: IEC 60950, EN 60950, UL 60950, CSA C22.2 No. 60950, TS 001, AS/NZS 3260, IEC 60825-1, IEC 60825-2, 21 CFR 1040-10, and 21 CFR 1040.11.

- Class 1M (IEC 60825-1 2001.01) and Class 1 (21 CFR 1040.10 and 1040.11) laser product

1.13 Installation Checklist

This section provides a summary of the steps required to install the ONS 15454 SDH. The section assumes that individual cards are used with their default provisioning values or that they will be provisioned as required by technicians on site. A checklist is given in Table 1-14.

Table 1-14   Installation Checklist

Description	Check
The ONS 15454 SDH is mounted securely in the rack.	
The ONS 15454 SDH is grounded with the frame ground.	
Power runs to the ONS 15454 SDH.	
Visual and audible alarm pins connect to central alarm collection equipment.	
If used, cables for BITS, LAN, Alarm, and CRAFT connect to corresponding equipment.	
Coaxial cables are installed on the FMEC cards.	
Coaxial cables run onto the side of the ONS 15454 SDH.	
Power connections have proper fuses (15A recommended).	
-48 VDC (tolerance –40.5 to –57.0 VDC) power is present at MIC-A/P and MIC-C/T/P modules when power is applied.	
The fan-tray air filter is installed in the fan-tray assembly with the flow direction arrow on the filter frame pointing up.	
The fan-tray assembly is installed. When installed, fans run on high speed with no TCC-I installed.	
If used, Ethernet patchcords are connected to Ethernet cards.	
Fiber-optic and/or Ethernet patch cords route through the faceplate clips, into the cable-management tray, through the side cutouts, and along the sides of the ONS 15454 SDH.	
Coaxial cables route through the side cutouts and along the sides of the ONS 15454 SDH.	
The fan-tray assembly can be removed without disturbing fiber or Ethernet patch cords.	
The LCD works. (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.	
The air ramp(s) are mounted properly.	

Set Up PC and Log Into CTC

This chapter provides procedures for connecting PCs and workstations to the Cisco ONS 15454 SDH and starting Cisco Transport Controller (CTC) sessions. It also includes general information about CTC features and functions. Table 2-1 lists procedures for starting CTC. Table 2-2 lists information about learning basic CTC functions. Table 2-3 lists basic CTC features.

Table 2-1   Set Up PC and Log Into CTC

How to Set Up and Start a CTC Session
2.1 How CTC Works, page 2-2
2.2 Checking Computer Requirements, page 2-2
2.3 Running the CTC Setup Wizard, page 2-4
2.4 Setting Up the CTC Computer, page 2-10
2.5 Logging Into CTC, page 2-23
2.6 Accessing ONS 15454 SDH Behind Firewalls, page 2-27

Table 2-2   CTC Functions

Learning Basic CTC Functions
2.7 Printing CTC Data, page 2-29
2.8 Exporting CTC Data into Other Applications, page 2-30

Table 2-3   CTC Features

Using Basic CTC Features
2.9 Using the Node View, page 2-34
2.10 Using the Network View, page 2-39
2.11 Using the Card View, page 2-51
2.12 Navigating CTC, page 2-53
2.13 Viewing CTC Table Data, page 2-55

2.1 How CTC Works

CTC is a Java application downloaded from the ONS 15454 SDH Timing Communications and Control (TCC-I) card to your computer when you connect to an ONS 15454 SDH. Launched from a web browser, such as Netscape Navigator or Microsoft® Internet Explorer, CTC allows you to perform ONS 15454 SDH provisioning and administrative functions.

Every time you connect to an ONS 15454 SDH:

- A CTC launcher applet downloads from the TCC-I to your browser.
- The launcher verifies that your computer has a CTC version matching the version on the ONS 15454 SDH TCC-I.
- If the computer does not have CTC, or if the installed version is older than the TCC-I version, the launcher downloads the CTC program files from the TCC-I.
- The launcher then starts CTC as a separate application. Each ONS 15454 SDH can run up to four network-level CTC sessions (login node and its DCC-connected nodes) and one node-level session (login node only) at one time.

Note Performance might vary, depending upon the volume of activity in each session.

Note After making changes in CTC, it takes at least 30 seconds before the change is written to flash. If the active TCC is reset before the 30 second period has ended, changes may be lost.

2.2 Checking Computer Requirements

Requirements for PCs and Solaris workstations are provided in Table 2-4 and Table 2-5 on page 2-3.

2.2.1 Check Computer Hardware Requirements

The processor and RAM listed below represent the minimum computer requirements necessary to run CTC.

Table 2-4   Computer Hardware Requirements for CTC

Hardware	Requirements	Notes
Processor	Pentium II 300 MHz (minimum), UltraSPARC, or equivalent	300 Mhz is the recommended processor speed. You can use computers with less processor speed; however, you might experience longer response times and slower performance.
RAM	128 megabytes (minimum)	

Table 2-4   Computer Hardware Requirements for CTC (continued)

Hardware	Requirements	Notes
Hard drive	2 GB	CTC application files are downloaded from the TCC-I to your computer's Temp directory. These files occupy 3 to 5 MB of hard drive space.
Operating system	PC: Windows XP, Windows 95, Windows 98, Windows NT, or Windows 2000 Workstation: Solaris 2.6 or 2.7	
Cable	User-supplied Category 5 straight-through cable with RJ-45 connectors on each end to connect the computer to the ONS 15454 SDH directly or through a LAN	

2.2.2 Check Computer Software Requirements

To use CTC SDH Software R3.4, your computer must have a web browser with the correct Java Runtime Environment (JRE) installed. Use JRE 1.3.1_02 with ONS 15454 SDH Software R3.4.

From the ONS 15454 SDH software or documentation CD, install Netscape Communicator, the JRE, the required Java plug-in and the modified java.policy file. See "Running the CTC Setup Wizard" section on page 2-4 for detailed information about setting up your computer.

Table 2-5   Computer Software Requirements for CTC

Software	Requirements	Notes
Web browser	PC: Netscape Navigator 4.51 or higher, Netscape Communicator 4.61 or higher, or Internet Explorer 4.0 (service pack 2) or higher Solaris: Netscape Navigator 4.76 or higher is recommended.	Netscape Communicator 4.73 (Windows) and 4.76 (Solaris) are installed by the CTC Setup Wizard included on the Cisco ONS 15454 SDH software and documentation CDs.
Java Runtime Environment	PC and Solaris: Software R3.4 must use JRE 1.3.1_02 (PC and Solaris) Software R3.3 can use JRE 1.2.2_05 with Java Plug-in 1.2.2 minimum	JRE 1.3.1 is installed by the CTC Setup Wizard included on the Cisco ONS 15454 SDH software and documentation CDs.

Table 2-5   Computer Software Requirements for CTC (continued)

Software	Requirements	Notes
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 SDH software and documentation CDs.
PC mouse pointer scheme	PC: (Windows 95 or 98) set to Windows Standard PC: (Windows NT, Windows 2000, Windows XP) set to None To check the settings: **a.** Choose **Settings** > **Control Panel** from the Windows Start menu. **b.** Double-click the **Mouse** option. **c.** From the Pointers tab of the Mouse Properties dialog box, select the **Windows Standard** (or **none** for NT, Windows 2000, or XP) mouse scheme. **d.** Click **OK**.	

2.3 Running the CTC Setup Wizard

Cisco ONS 15454 SDH Software R3.4 provides a setup wizard that installs the files needed to use CTC on PCs and Solaris workstations. You can start the setup wizard from the Cisco ONS 15454 SDH software CD or from the Cisco ONS 15454 SDH documentation CD. The wizard will install:

- Netscape Communicator 4.73 (Windows) or 4.76 (Solaris)
- JRE 1.3.1_02 (Windows & Solaris)
- Cisco ONS 15454 SDH CTC online help
- Modified java.policy file

For Solaris workstations, the JRE might require patches to operate 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 Java Runtime Environment for UNIX" procedure on page 2-9 to set up JRE on the workstation. (In the procedures, [*JRE*] indicates the destination directory you selected for the JRE.)

Procedure: Run the CTC Installation Wizard for Windows

Purpose	Installs programs required to run CTC on Windows PCs: Netscape 4.73, JRE 1.3.1_02, and CTC online help. It also modifies the JRE policy file so CTC files can be downloaded to your computer when you connect to an ONS 15454 SDH.
Tools/Equipment	Cisco ONS 15454 SDH R3.4 software or documentation CD
Onsite/Remote	Onsite or remote

Step 1   Verify that your computer has the following:

- Processor—Pentium II, 300 Mhz or faster

- RAM—128 MB (minimum)

- Hard drive—2 GB is recommended. 50 MB of space must be available.

- Operating system—Windows 95, Windows 98, Windows NT 4.0 with Service Pack 5 or later, Windows 2000, or Windows XP

> **Note**   Processor and RAM requirements are guidelines. CTC performance will be faster if your computer has a faster processor and more RAM.

Step 2   Insert the Cisco ONS 15454 SDH R3.4 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's CD directory and double-click **setup.exe**.

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer (Figure 2-1).

Figure 2-1   Starting the Cisco Transport Controller Installation Wizard
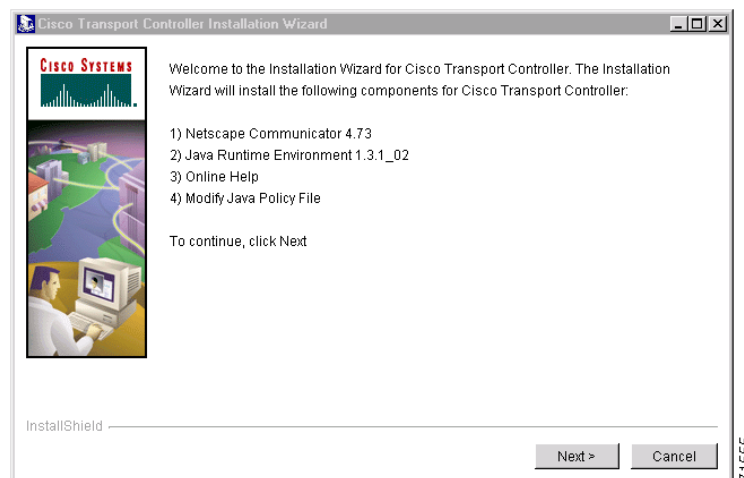
Step 3   Click **Next**.

Step 4   For installation type, choose **Typical** to install all the components, or choose **Custom** if you only want to install some of the components.

Step 5   Click **Next**.

Step 6   If you selected **Custom** in Step 4, select the CTC components you want to install by checking or unchecking the boxes; then, click **Next**. If you selected **Typical**, skip this step.

Step 7   The directory where the installation wizard will install CTC online help is displayed. The default is C:\Program Files\Cisco\CTC\Documentation.

Step 8   If you wish to change the CTC online help directory, type the new directory path in the *Directory Name* field, or click **Browse** to navigate to the directory. If you do not wish to change the directory, skip this step.

Step 9   Click **Next**.

Step 10   Review the components that will be installed. If you wish to change them, click **Back**. If you have an active CTC session (for example, you are running the setup program to install additional components), close CTC before going to the next step.

Step 11   Click **Next**. The InstallShield program begins the Netscape Communicator 4.73 Setup program.

Step 12   Complete the Netscape installation:

    a. In the Netscape Communicator 4.73 Setup dialog box, click **Next**.

    b. In the Software License Agreement dialog box, click **Yes**.

    c. In the Setup Type dialog box, click **Typical**; then, click **Next**.

> **Note**   If the Netscape installation hangs when installing RealPlayer G2, restart the CTC installation by pressing Ctrl + Alt + Del. In the Windows Security dialog box, click **Task Manager**. In the Windows Task Manager dialog box, click Cisco Transport Controller Installation Wizard; then, click the **End Task** button. Click **Yes** on the confirmation. Navigate to the drive containing the CTC CD and double-click **CTC.exe**. Repeat Steps 1 to 12. From Step 13, substep c, click **Custom**; then, click **Next**. From the next window, deselect **RealPlayer**. Continue with substep d.

    d. In the Netscape Desktop Preferences dialog box, check the boxes that apply; then, click **Next**.

    e. In the Program Folder dialog box, click **Next**.

    f. In the Start Copying Files dialog box, click **Install**. The program begins the Netscape installation.

    g. In the Question dialog box, click **No**.

    h. In the Restart Windows dialog box, click **No, I will restart later**; then, click **OK**. The Cisco Transport Controller Installation Wizard dialog box is displayed.

Step 13   Click **Next**. The Java 2 runtime environment installation begins.

Step 14   Complete the JRE installation:

    a. In the Software License Agreement dialog box, click **Yes**.

    b. In the Choose Destination Location dialog box, click **Next**.

    c. In the Select Browser dialog box, click the Microsoft Internet Explorer and Netscape 6 check boxes; then, click **Next**.

    When JRE installation is complete, the Cisco Transport Controller Installation Wizard dialog box is displayed.

Step 15   Click **Next**. The CTC online help is installed. When installed, the policy file selection is displayed.

Step 16   Choose the JRE policy file to modify:

    • Choose **User Policy File** (default) to modify the policy file that applies only to your user profile. This file will not be overwritten if you upgrade or reinstall the JRE. If you are the only user who will access an ONS 15454 SDH from the PC you are setting up, choose this option.

    • Select **System Policy File** to modify the system JRE policy file. This policy file applies to all computer users. If more than one individual will use this computer to access the ONS 15454 SDH, choose this option. However, if you reinstall or upgrade the JRE, the system policy file is overwritten and you will need to run the CTC Installation Setup program again to modify it.

Step 17   Click **Next**.

Step 18   If you selected System Policy File in Step 16, complete the following steps. If you selected User Policy File, proceed to Step 19.

     a.   The System Policy File Update dialog box displays the default policy file location (C:\Program Files\JavaSoft\jre). If you installed the JRE in a different location, enter the new path in the Directory Name field. After entering the path, or if the default path is correct, click **OK**.

     b.   Click **OK** in the confirmation dialog box.

Step 19   Click **Finish**.

Step 20   To connect to the ONS 15454 SDH, restart your computer and complete the "Setting Up the CTC Computer" procedure on page 2-10.

Procedure: Run the CTC Installation Wizard for UNIX

Purpose	This procedure installs programs required to run CTC on Solaris workstations: Netscape 4.76, JRE 1.3.1_02, and CTC online help. It also modifies the JRE policy file to allow CTC files to be downloaded to your computer after you connect to an ONS 15454 SDH.
Tools/Equipment	Cisco ONS 15454 SDH R3.4 software or documentation CD
Onsite/Remote	Onsite or remote

Step 1   Verify that your computer has the following:

- RAM—128 MB (minimum)
- Hard drive—Verify that 50 MB of space is available.
- Operating system—Solaris 2.5.x or 2.6.x

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

Step 2   From the command prompt, change the directory by typing:

     cd /cdrom/cdrom0/

Step 3   From the techdoc454 CD directory, type:

     ./setup.bat

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

- Netscape Communicator 4.76
- Java Runtime Environment 1.3.1_02
- CTC Online Help
- Modify Policy File—The JRE java.policy file is modified to enable CTC to download files needed to run the Cisco Transport Controller when you connect to an ONS 15454 SDH.

Step 4   Click **Next**.

Step 5   For installation type, choose **Typical** to install all components, or choose **Custom** if you do not want to install all of the components.

Step 6   Click **Next**.

Step 7   If you selected **Custom** in Step 4, select the CTC components you want to install by checking or unchecking the boxes; then, click **Next**. If you selected **Typical**, skip this step.

Step 8   The directory where the installation wizard will install CTC online help is displayed. The default is C:\Program Files\Cisco\CTC\Documentation. If you wish to change the CTC online help directory, type the new directory path in the Directory Name field, or click **Browse** to navigate to the directory.

Step 9   Click **Next**.

Step 10   Review the components that will be installed. If you wish to change them, click **Back**. If CTC is running (for example, if you are reinstalling components) close CTC before going to the next step.

Step 11   Click **Next**. The InstallShield program begins the Netscape Communicator 4.76 Setup program.

Step 12   Complete the Netscape installation:

    a. In the Netscape Communicator 4.73 Setup dialog box, click **Next**.

    b. In the Software License Agreement dialog box, click **Yes**.

    c. In the Setup Type dialog box, click **Typical**.

    d. In the Netscape Desktop Preferences dialog box, check the boxes that apply; then, click **Next**.

    e. In the Program Folder, click **Next**.

    f. In the Start Copying Files dialog box, click **Install**. The program begins the Netscape installation.

    g. In the Question dialog box, click **No**.

Step 13   In the Cisco Transport Controller Installation Wizard dialog box, click **Next**. The Java 2 runtime environment installation begins.

Step 14   Complete the JRE installation:

    a. In the Software License Agreement dialog box, click **Yes**.

    b. In the Choose Destination Location dialog box, click **Next**.

    c. In the Select Browser dialog box, click the Netscape 6 check boxes; then, click **Next**.

    The JRE is installed. When installation is complete, the Cisco Transport Controller Set Wizard dialog box is displayed.

Step 15   Click **Next**. The CTC online help is installed. When installed, the policy file selection is displayed.

Step 16   Choose the JRE policy file to modify:

    • Choose **User Policy File** (default) to create a policy file that applies only to your user profile. This file will not be overwritten if you upgrade or reinstall the JRE. If you are the only user who will access an ONS 15454 SDH using this computer, choose this option.

    • Select **System Policy File** to modify the system JRE policy file. This policy file applies to all users of this computer. If more than one individual will use this computer to access the ONS 15454 SDH, choose this option. However, if you reinstall or upgrade the JRE, the system policy file is overwritten and you will need to run the CTC Installation Setup program again to modify it.

Step 17   Click **Next**; then, click **Finish**.

> **Note**   Be sure to record the names of the directories you choose for Netscape, JRE, and the online documentation.

Step 18   If your installation included the JRE (that is, you chose the typical installation or selected JRE from the custom installation), proceed to "Set Up the Java Runtime Environment for UNIX" section on page 2-9.

> **Note**   The Java Runtime Environment (JRE) might require certain patches to run properly. The patch tar file can be found in the JRE/Solaris directory on the CD. Please read the JRE/Solaris/Solaris.txt file for more information. In addition to installing any needed patches, use the following procedure to set up JRE for use with Cisco Transport Controller on your UNIX system.

Procedure: Set Up the Java Runtime Environment for UNIX

Purpose	Sets up the Java Runtime Environment for UNIX workstations.
Prerequisite Procedures	"Run the CTC Installation Wizard for UNIX" procedure on page 2-7
Required/As Needed	Required if you installed the JRE during the CTC Installation Setup.
Onsite/Remote	Onsite or remote

> **Note**   In this procedure, *your JRE path* represents the destination directory you chose for the Java Runtime Environment during JRE installation. For example, if your JRE destination directory is /usr/bin/jre, substitute /usr/bin/jre wherever the text *your JRE path* occurs. Also, in the following procedures, *your Netscape path* refers to the destination directory you chose for Netscape, and must be substituted with your actual Netscape destination directory path.

> **Note**   CTC requires that the location of xterm is also in your path. If you have, for some reason, moved xterm from its default location, /usr/openwin/bin, you must change all occurrences of /usr/openwin/bin in the following procedure to reflect the actual path where xterm exists on your system.

Step 1   Set up the environment variable:

   a.   If you are using the csh shell, edit the .cshrc file in your home directory by appending the file with the lines:

   setenv JRE [JRE path]
   setenv NETSCAPE [Netscape path]
   setenv NPX_PLUGIN_PATH $JRE/j2re1_3_1_02/plugin/sparc/ns4
   set path = (/usr/openwin/bin $NETSCAPE $path)

   b.   If you are using the ksh or bash shell, edit the .profile file in your home directory by appending the file with the lines:

   JRE=*your JRE path*
   NETSCAPE=*your Netscape path*
   NPX_PLUGIN_PATH=$JRE/j2re1_3_1_02/plugin/sparc/ns4
   PATH=/usr/openwin/bin:$NETSCAPE:$PATH
   export JRE NPX_PLUGIN_PATH PATH

Step 2   Set the JRE reference:

   a.   From the command prompt, run the Control Panel by typing:

   your JRE path/**j2re1_3_1_02/bin/ControlPanel**

   b. Click the **Advanced** tab.

   c. From the combo box, select *JRE path*/**j2re1_3_1_02**. If the JRE path is not found, select **other** and enter the following in the Path text box:

      your JRE path/**j2re1_3_1_02**

   d. Click **Apply**. Proceed to the "Setting Up the CTC Computer" section on page 2-10.

> **Note**   If you are running multiple shells, before your new environment variable will be set you might need to invoke the same shell for which you changed the initialization file. (For example, if you added the environment variable to the .cshrc file, you must run your browser under the csh shell.)

2.4 Setting Up the CTC Computer

Before you run CTC on your Windows PC or Solaris workstation, you need to set up the computer for the specific method you will use to connect to the ONS 15454 SDH. Table 2-6 on page 2-10 lists the methods for connecting to the ONS 15454 SDH. Use the table to find the connection method you will use and check the Requirements column before performing the setup procedures.

> **Note**   For initial setup, you must use a direct connection to the ONS 15454 SDH.

Table 2-6   ONS 15454 SDH Connection Methods

Method	Description	Requirement
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15454 SDH using one of the following: • The RJ-45 jack on the MIC-C/T/P FMEC • A hub or switch to which the ONS 15454 SDH is connected	• If you do not use DHCP (Dynamic Host Configuration Protocol), you will need to change the computer IP address, subnet mask, and default router.

Table 2-6   ONS 15454 SDH Connection Methods (continued)

Method	Description	Requirement
Corporate LAN	Refers to a connection to the ONS 15454 SDH through a corporate or network operation center (NOC) LAN.	• The ONS 15454 SDH must be provisioned for LAN connectivity, including IP address, subnet mask, and default gateway. • The ONS 15454 SDH must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15454 SDH.
Remote	Refers to a connection made to the ONS 15454 SDH using a modem.	• A modem must be connected to the ONS 15454 SDH. • The modem must be provisioned for ONS 15454 SDH. To run CTC, the modem must be provisioned for Ethernet access.

Based on the cable connection method you choose, select the appropriate procedure:

- To set up your computer for local craft connections, choose a procedure from Table 2-7.
- To set up the computer for LAN access, complete the "Set Up a Computer for a Corporate LAN Connection" procedure on page 2-21.
- To set up the computer for remote access, complete the "Provision Remote Access to the ONS 15454 SDH" procedure on page 2-23.

Table 2-7   ONS 15454 SDH Craft Connection Options

Direct Connection Procedures	Description
• "Set Up a Windows PC for Craft Connection to an ONS 15454 SDH on the Same Subnet Using Static IP Addresses" procedure on page 2-12, or • "Set Up Solaris Workstations for a Direct Connection to an ONS 15454 SDH" procedure on page 2-19	Complete this procedure if: • You will connect to one ONS 15454 SDH; if you must connect to multiple ONS 15454 SDH nodes, you can reconfigure your computer's IP settings each time you connect to an ONS 15454 SDH. • You need to access non-ONS 15454 SDH applications such as ping and trace route.

Table 2-7   ONS 15454 SDH Craft Connection Options (continued)

Direct Connection Procedures	Description
• "Set Up a Windows PC for Craft Connection to an ONS 15454 SDH Using DHCP" procedure on page 2-14	Complete this procedure if: • The CTC computer is provisioned for DHCP. • The ONS 15454 SDH has DHCP forwarding enabled and is connected to a DHCP server.
• "Set Up a Windows PC for Craft Connection to an ONS 15454 SDH Using Automatic Host Detection" procedure on page 2-17	Complete this procedure if: • You are connecting to a node that resides in a secure network employing the ONS 15454 SDH proxy server. • You will connect to ONS 15454 SDH nodes at different locations and times. • You do not need to access a LAN or use non-ONS 15454 SDH applications such as ping.

After your computer is set up to connect to the ONS 15454 SDH, proceed to the "Logging Into CTC" section on page 2-23.

Procedure: Set Up a Windows PC for Craft Connection to an ONS 15454 SDH on the Same Subnet Using Static IP Addresses

Purpose Use this procedure to set up your computer for a local craft connection to the ONS 15454 SDH when:
- You will connect to one ONS 15454 SDH; if you must connect to multiple ONS 15454 SDH nodes, you can reconfigure your computer's IP address.
- You need to use non-ONS 15454 SDH applications such as ping.
- You need to access the corporate LAN.

Prerequisite Procedures "Setting Up the CTC Computer" procedure on page 2-10

Onsite/Remote Onsite

Step 1 Verify the operating system that is installed on your computer:
   a. From the Windows Start menu, choose **Settings > Control Panel**.
   b. In the Control Panel window, double-click the **System** icon.
   c. In the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 95, Windows 98, Windows 2000, Windows NT 4.0, or Windows XP.

Step 2 Complete the steps in Table 2-8 on page 2-13 or Table 2-9 on page 2-14 for the operating system installed on your PC.

Table 2-8   Set Up Windows 95, 98, or NT for Craft ONS 15454 SDH Connections on the Same Subnet Using Static IP Addresses

For Windows 95 or 98:	For Windows NT:
1. From the Windows Start menu, choose **Settings > Control Panel**.	1. From the Windows Start menu, choose **Settings > Control Panel**.
2. In the Control Panel dialog box, click the **Network** icon.	2. In the Control Panel dialog box, click the **Network** icon.
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**.
4. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.	4. Click the **IP Address** tab.
5. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.	5. In the IP Address window, click **Specify an IP address**.
6. Click the **IP Address** tab.	6. In the IP Address field, enter an IP address that is identical to the ONS 15454 SDH IP address shown on the ONS 15454 SDH LCD except for the last three digits. The last three digits must be between 1 and 254.
7. In the IP Address window, click **Specify an IP address**.	7. In the Subnet Mask field, type **255.255.255.0**.
8. In the IP Address field, enter an IP address that is identical to the ONS 15454 SDH IP address shown on the ONS 15454 SDH LCD except for the last three digits. The last three digits must be between 1 and 254.	8. Click the **Advanced** button.
9. In the Subnet Mask field, type **255.255.255.0**.	9. Under the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box is displayed.
10. Click **OK**.	10. Type the ONS 15454 SDH IP address in the Gateway Address field.
11. In the TCP/IP dialog box, click the **Gateway** tab.	11. Click **Add**.
12. In the New Gateway field, type the ONS 15454 SDH IP address. Click **Add**.	12. Click **OK**.
13. Verify that the IP address displays in the Installed Gateways field; then, click **OK**.	13. Click **Apply**.
14. When the prompt to restart your PC displays, click **Yes**.	14. In some cases, Windows NT will prompt you to reboot your PC. If you receive this prompt, click **Yes**.

Table 2-9   Set Up Windows 2000 or XP for Craft ONS 15454 SDH Connections on the Same Subnet Using Static IP Addresses

For Windows 2000:	For Windows XP:
1. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.	1. From the Windows Start Menu, choose **Control Panel > Network Connections**.
2. In the Local Area Connection Status dialog box, click **Properties**.	✎ **Note** If the Network Connections icon is not available, click Switch to Classic View.
3. In the General tab, choose **Internet Protocol (TCP/IP)**; then, click **Properties**.	2. From the Network Connections dialog box, click the **Local Area Connection** icon.
4. Click **Use the following IP address**.	3. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
5. In the IP Address field, enter an IP address that is identical to the ONS 15454 SDH IP address shown on the ONS 15454 SDH LCD except for the last three digits. The last three digits must be between 1 and 254.	4. In the IP Address field, enter an IP address that is identical to the ONS 15454 IP address shown on the ONS 15454 LCD 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**.	5. In the Subnet Mask field, type 255.255.255.0.
7. In the Default Gateway field, type the ONS 15454 SDH IP address.	6. In the Default Gateway field, type the ONS 15454 IP address.
8. Click **OK**.	7. Click **OK**.
9. In the Local Area Connection Status dialog box, click **Close**.	8. On the Local Area Connection Properties dialog box, click **OK**.
10. In the Local Area Connection Properties dialog box, click **OK**.	9. On the Local Area Connection Status dialog box, click **Close**.

Step 3   After you set up your PC, proceed to the "Logging Into CTC" procedure on page 2-23 to log into the ONS 15454 SDH.

Procedure: Set Up a Windows PC for Craft Connection to an ONS 15454 SDH Using DHCP

Purpose	Use this procedure to set up your computer for craft connection to the ONS 15454 SDH using DHCP.
Tools/Equipment	Category 5 (LAN) cable
Prerequisite Procedures	"Running the CTC Setup Wizard" procedure on page 2-4
	"Setting Up Network Information" procedure on page 3-5
Onsite/Remote	Onsite

⚠

Caution   You will not be able to connect to the ONS 15454 SDH if DHCP forwarding is not enabled on the ONS 15454 SDH or the ONS 15454 SDH is not connected to a DHCP server. By default, DHCP forwarding is not enabled. If you are connecting to an ONS 15454 SDH to perform initial shelf turnup, complete the "Set Up a Windows PC for Craft Connection to an ONS 15454 SDH on the Same Subnet Using Static IP Addresses" procedure on page 2-12.

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

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

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

    c.   In the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 95, Windows 98, Windows 2000, Windows NT 4.0, or Windows XP.

Step 2   Complete the steps in Table 2-10 on page 2-15 or Table 2-11 on page 2-16 for the operating system installed on your PC.

Table 2-10   Set Up Windows 95, 98, or NT for Craft ONS 15454 SDH Connections Using DHCP

For Windows 95 or 98:	For Windows NT:
1. From the Windows Start menu, choose **Settings > Control Panel**.	1. From the Windows Start menu, choose **Settings > Control Panel**.
2. In the Control Panel dialog box, click the **Network** icon.	2. In the Control Panel dialog box, click the **Network** icon.
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**.
4. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.	4. Click the **IP Address** tab.
5. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.	5. In the IP Address window, click **Obtain an IP address from a DHCP Server**.
6. Click the **IP Address** tab.	6. Click **OK**.
7. In the IP Address window, click **Obtain an IP address from a DHCP Server**.	7. Click **Apply**.
8. Click **OK**.	8. If Windows prompts you to restart your PC, click **Yes**.
9. When the prompt to restart your PC displays, click **Yes**.	

Table 2-11   Set Up Windows 2000 or XP for Craft ONS 15454 SDH Connections Using DHCP

For Windows 2000:	For Windows XP:
1. From the Windows Start menu, choose **Settings** > **Network and Dial-up Connections > Local Area Connection**.	1. From the Windows Start menu, choose **Control Panel> Network Connections**.
2. In the Local Area Connection Status dialog box, click **Properties**.	**Note** If the Network Connections icon is not available, click Switch to Classic View.
3. In the General tab, choose **Internet Protocol (TCP/IP)**; then, click **Properties**.	2. On the Network Connections dialog box, click **Local Area Connection**.
4. Click **Obtain an IP address from a DHCP Server**.	3. On the Local Area Connection Status dialog box, click **Properties**.
5. Click **OK**.	4. On the General tab, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
6. In the Local Area Connection Status dialog box, click **Close**.	5. Click **Obtain an IP address automatically**.
7. In the Local Area Connection Properties dialog box, click **OK**.	6. Click **OK**.
	7. On the Local Area Connection Properties dialog box, click **OK**.
	8. On the Local Area Connection Status dialog box, click **Close**.

Step 3   After you set up your PC, proceed to the "Logging Into CTC" procedure on page 2-23 to log into the ONS 15454 SDH.

Procedure: Set Up a Windows PC for Craft Connection to an ONS 15454 SDH Using Automatic Host Detection

Purpose	Use this procedure to set up your computer for local craft connection to the ONS 15454 SDH when:
	• You are connecting to a node that resides in a secure network employing the ONS 15454 SDH proxy server.
	• You will access nodes running CTC software Release 3.4 and earlier.
	• You will connect to multiple ONS 15454 SDH nodes and do not want to reconfigure your IP address each time.
	• You do not need to access a corporate LAN or use non-ONS 15454 SDH applications such as ping and trace route.
Prerequisite Procedures	"Setting Up the CTC Computer" procedure on page 2-10
Onsite/Remote	Onsite

Note   This procedure employs the ONS 15454 SDH automatic host detection to allow you to directly connect to multiple ONS 15454 SDH nodes successively without reconfiguring your computer's IP address. However, if proxy server is not enabled on the ONS 15454 SDH, DCC-connected nodes on different subnets will not be visible. Refer to the "Setting Up Network Information" section on page 3-5 and the "Scenario 9: Using the Proxy Server Features" section on page 4-16 for more information about the proxy server.

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

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

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

    c.   In the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 95, Windows 98, Windows 2000, Windows NT 4.0, or Windows XP.

Step 2   Complete the steps in Table 2-12 on page 2-18 or Table 2-13 on page 2-19 for the operating system installed on your PC.

Table 2-12   Set Up Windows 95, 98, or NT for Craft ONS 15454 SDH Connections Using Automatic Host Detection

For Windows 95 or 98:	For Windows NT:
1. From the Windows Start menu, choose **Settings** > **Control Panel**.	1. From the Windows Start menu, choose **Settings** > **Control Panel**.
2. In the Control Panel dialog box, click the **Network** icon.	2. In the Control Panel dialog box, click the **Network** icon.
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**.
4. In the TCP/IP Properties dialog box, click the **DNS Configuration** tab and choose **Disable DNS**.	4. Click the **IP Address** tab.
5. Click the **WINS Configuration** tab and choose **Disable WINS Resolution**.	5. In the IP Address window, click **Specify an IP address**.
6. Click the **IP Address** tab.	6. In the IP Address field, enter any legitimate IP address.
7. In the IP Address window, click **Specify an IP address**.	7. In the Subnet Mask field, type **255.255.255.0**.
8. In the IP Address field, enter any legitimate IP address.	8. Click the **Advanced** button.
9. In the Subnet Mask field, type **255.255.255.0**.	9. Under the Gateways List, click **Add**. The TCP/IP Gateway Address dialog box is displayed.
10. Click **OK**.	10. In the Gateway Address field, type the IP address entered in Step 6.
11. In the TCP/IP dialog box, click the **Gateway** tab.	11. Click **Add**.
12. In the New Gateway field, type the address entered in Step 8. Click **Add**.	12. Click **OK**.
13. Verify that the IP address displays in the Installed Gateways field; then, click **OK**.	13. Click **Apply**.
14. When the prompt to restart your PC displays, click **Yes**.	14. Reboot your PC.

Table 2-13   Set Up Windows 2000 or XP for Craft ONS 15454 SDH Connections Using Automatic Host Detection

For Windows 2000:	For Windows XP:
1. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection**.	1. From the Windows Start Menu, choose **Control Panel > Network Connections**.
2. In the Local Area Connection Status dialog box, click **Properties**.	✎ **Note** If the Network Connections icon is not available, click Switch to Classic View.
3. In the General tab, choose **Internet Protocol (TCP/IP)**; then, click **Properties**.	2. From the Network Connections dialog box, click the **Local Area Connection** icon.
4. Click **Use the following IP address**.	3. From the Local Area Connection Properties dialog box, choose **Internet Protocol (TCP/IP)**, then click **Properties**.
5. In the IP Address field, enter a legitimate IP address.	4. In the IP Address field, enter any legitimate IP address other than the node IP address as indicated on the LCD.
6. In the Subnet Mask field, type **255.255.255.0**.	5. In the Subnet Mask field, type 255.255.255.0.
7. In the Gateway Address field, type the IP address entered in Step 5.	6. In the Gateway Address field, type the IP address entered in Step 4.
8. Click **OK**.	7. Click **OK**.
9. In the Local Area Connection Status dialog box, click **Close**.	8. On the Local Area Connection Properties dialog box, click **OK**.
10. In the Local Area Connection Properties dialog box, click **OK**.	9. On the Local Area Connection Status dialog box, click **Close**.

Step 3   After you set up your PC, proceed to the "Logging Into CTC" procedure on page 2-23 to log into the ONS 15454 SDH.

Procedure: Set Up Solaris Workstations for a Direct Connection to an ONS 15454 SDH

A direct connection from a workstation to an ONS 15454 SDH means your computer is physically connected to the ONS 15454 SDH. Set up Solaris to connect directly to an ONS 15454 SDH when it is not connected to a LAN.

Purpose	Use this procedure to connect your workstation directly to the ONS 15454 SDH.
Tools/Equipment	Category 5 cable
Prerequisite Procedures	"Running the CTC Setup Wizard" procedure on page 2-4
Onsite/Remote	Onsite

Step 1   Choose a cable connection method:

- RJ-45 jack on the ONS 15454 SDH MIC-C/T/P FMEC: Attach a Category 5 cable from the workstation's network interface card (NIC) card to the RJ-45 jack on the ONS 15454 SDH MIC-C/T/P FMEC.

- Hub or switch: Attach a Category 5 cable from the workstation's NIC card to the RJ-45 jack on a hub or switch to which the ONS 15454 SDH is physically connected.

Step 2 Log into the workstation as the root user.

Step 3 Check to see if the interface is plumbed by typing:

```
# ifconfig device
```

For example:

```
# ifconfig hme1
```

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

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

Proceed to Step 4.

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

```
ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface.
```

Plumb the interface by typing:

```
# if config device plumb
```

For example:

```
# ifconfig hme1 plumb
```

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

```
# ifconfig interface ip_address netmask netmask up
```

For example:

```
# ifconfig hme0 10.20.30.40 netmask 255.255.255.0 up
```

> **Note** Enter an IP address that is identical to the ONS 15454 SDH IP address except for the last three digits. The last three digits must be between 1 and 254. In the Subnet Mask field, type **255.255.255.0.**

Step 5 Test the connection:

a. Start Netscape Navigator or Internet Explorer.

b. Enter the Cisco ONS 15454 SDH IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box display. If this occurs, proceed to Step 2 of the "Run the CTC Installation Wizard for UNIX" procedure on page 2-7 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

c. At the prompt, type:

```
ping ONS_15454_SDH_IP_address
```

For example, you would type **ping 192.168.1.1** to connect to an ONS 15454 SDH with default IP address 192.168.1.1. If your workstation is connected to the ONS 15454 SDH, an "*IP_address* is alive" message displays.

d. If CTC is not responding, a "Request timed out" message displays. Verify IP and submask information. Check that the cables connecting the workstation to the ONS 15454 SDH are securely attached. Check the Link Status by typing:

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

For example:

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

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

✎
Note   Check the man page for ndd. For example: **# man ndd**

Procedure: Set Up a Computer for a Corporate LAN Connection

Purpose	Use this procedure to set up your computer to access the ONS 15454 SDH through a corporate LAN.
Prerequisite Procedures	"Setting Up the CTC Computer" procedure on page 2-10
Onsite/Remote	Onsite or remote

Step 1   If your computer is connected to the corporate LAN, proceed to Step 2. If you changed your computer's network settings for direct access to the ONS 15454 SDH, change the settings back to the corporate LAN access settings. This generally means:

- Set the IP Address on the TCP/IP dialog box back to "Obtain an IP address automatically" (Windows 95 or 98) or "Obtain an IP address from a DHCP server" (Windows NT, 2000, or XP).

- If your LAN requires that domain name system (DNS) or windows internet name service (WINS) be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 2   If your computer is connected to a proxy server, disable proxy service or add the ONS 15454 SDH nodes as exceptions. To disable proxy service, complete one of the following procedures, depending on which web browser you use:

- "Disable Proxy Service Using Internet Explorer (Windows)" procedure on page 2-22
- "Disable Proxy Service Using Netscape (Windows and UNIX)" procedure on page 2-22

Procedure: Disable Proxy Service Using Internet Explorer (Windows)

Purpose	Disables proxy service for PCs running Internet Explorer.
Onsite/Remote	Onsite or remote

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   In the LAN Settings dialog box, complete one of the following options:

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

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

Purpose	Disables proxy service for PCs and UNIX workstations running Netscape.
Onsite/Remote	Onsite or remote

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, complete one of the following options:

- Choose **Direct connection to the Internet** to bypass the proxy server.
- Choose **Manual proxy configuration** to add exceptions to the proxy server; then, click **View**. In the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15454 SDH nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.

Procedure: Provision Remote Access to the ONS 15454 SDH

Purpose	Use this procedure to connect an ONS 15454 SDH using a LAN modem.
Tools/Equipment	Modem and modem documentation
Prerequisite Procedures	"Setting Up the CTC Computer" procedure on page 2-10
Onsite/Remote	Onsite or remote

Step 1   Connect the modem to the RJ-45 port on the MIC-C/T/P FMEC.

Step 2   Refer to the modem documentation to provision the modem for the ONS 15454 SDH:

- For CTC access, set the modem for Ethernet access.

- Assign an IP address to the modem that is on the same subnet as the ONS 15454 SDH.

- The IP address that the modem assigns to the CTC computer must be on the same subnet as the modem and the ONS 15454 SDH.

> ✎
> **Note**   For assistance with provisioning specific modems, contact the Cisco Technical Assistance Center. For contact information, refer to the preface in the Product Overview.

2.5 Logging Into CTC

> ✎
> **Note**   If you are loading and activating a new software build, you might need to close the browser and start CTC again.

.

Purpose	Use this procedure to log into the CTC. This procedure includes optional node login procedures.
Prerequisite Procedures	"Setting Up the CTC Computer" procedure on page 2-10
Onsite/Remote	Onsite or remote

Step 1   If the computer is not connected to the ONS 15454 SDH, complete the "Connect Computer to the ONS 15454 SDH" procedure on page 2-24.

Step 2   Complete the "Log Into CTC" procedure on page 2-24.

> ✎
> **Note**   For information about navigating in CTC, see the "Navigating CTC" section on page 2-53.

Step 3   As needed, complete the "Create Login Node Groups" procedure on page 2-26. Login node groups display nodes that are not connected to the login node via DCC.

Step 4   As needed, complete the "Add a Node to the Current Session or Login Group" procedure on page 2-27.

Procedure: Connect Computer to the ONS 15454 SDH

.

Purpose	Use this procedure to connect a CTC computer to the ONS 15454 SDH.
Tools/Equipment	Category 5 cable
Prerequisite Procedures	"Running the CTC Setup Wizard" procedure on page 2-4
	"Setting Up the CTC Computer" procedure on page 2-10
Required/As Needed	Required to access the Cisco Transport Controller
Onsite/Remote	Onsite or remote

Step 1 If your computer is set up for a local craft connection, connect a Category 5 cable from the PC or Solaris workstation NIC card to one of the following:

- The RJ-45 port on the MIC-C/T/P FMEC
- The RJ-45 port on a hub or switch to which the ONS 15454 SDH is physically connected

Step 2 If your computer is set up for a corporate LAN connection, connect a Category 5 cable from the PC or Solaris workstation NIC card to a LAN port.

Step 3 Proceed to the "Log Into CTC" procedure on page 2-24 to log into CTC.

Procedure: Log Into CTC

Purpose	Use this procedure to log into the Cisco Transport Controller, the graphical user interface software used to manage the ONS 15454 SDH.
Prerequisite Procedures	"Running the CTC Setup Wizard" procedure on page 2-4
	"Setting Up the CTC Computer" procedure on page 2-10
Required/As Needed	Required
Onsite/Remote	Onsite or remote

Note For information about CTC views and navigation, see "Navigating CTC" section on page 2-53.

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

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

Note If you are logging into ONS 15454 SDH nodes 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, you receive an INCOMPATIBLE-SW alarm and the IP address of the login node will display instead of the node name. To check the software version of a node, select **About CTC** from the CTC Help menu. To resolve an alarm, refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

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. The first time you connect to an ONS 15454 SDH, this process can take several minutes. After the download, the CTC Login dialog box displays (Figure 2-2).

Figure 2-2   CTC login dialog box

Step 3   In the Login dialog box, type a user name and password (both are case sensitive). For initial setup, type the user name **CISCO15** if it is not already displayed.

Note   The CISCO15 user is provided with every ONS 15454 SDH. 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.) To set up ONS 15454 SDH users and assign security, proceed to the "Creating Users and Setting Security" procedure on page 3-9.

Step 4   Each time you log into an ONS 15454 SDH, you can make selections on the following login options:

- Node Name—Displays the IP address entered in the web browser and a pull-down list of previously-entered ONS 15454 SDH IP addresses. You can select any ONS 15454 SDH 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. To create a login node group or add additional groups, see the "Create Login Node Groups" procedure on page 2-26.

- Disable Network Discovery—Check this box to view only the ONS 15454 SDH (and login node group members, if any) entered in the Node Name field. Nodes linked to the Node Name ONS 15454 SDH through the DCC are not displayed. Using this option can decrease the CTC startup time in networks with many DCC-connected nodes.

- Disable Circuit Management—Check this box if you do not want circuits to appear in the CTC node view Circuits tab, or the network view Circuits tab. To view all circuits on a node or network, log into CTC and do not check the Disable Circuit Management check box.

Step 5   Click **Login**. Figure 2-3 shows a CTC session initializing.

Figure 2-3   CTC session initialization

If login is successful, the CTC window displays the node view. From here, you can navigate to other CTC views to provision and manage the ONS 15454 SDH. If you need to perform the initial shelf turn up, see Chapter 3, "Node Setup." If login problems occur, refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Procedure: Create Login Node Groups

Purpose	Create a login node group to display ONS 15454 SDH nodes that have an IP connection but not a DCC connection to the login node.
Prerequisite Procedures	• "Setting Up the CTC Computer" procedure on page 2-10
	• "Logging Into CTC" procedure on page 2-23
Required/As Needed	As needed
Onsite/Remote	Onsite or remote

Step 1 Log into an ONS 15454 SDH on the network. See the "Log Into CTC" procedure on page 2-24 for instructions.

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

Step 3 Click the **Login Node Group** tab and click **Create Group**.

Step 4 Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.

Step 5 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 6 Click **OK**.

The next time you log into an ONS 15454 SDH, 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.

Procedure: Add a Node to the Current Session or Login Group

Purpose	Add a node to the current CTC session
Onsite/Remote	Onsite or remote

Step 1   Log into an ONS 15454 SDH on the network. See the "Log Into CTC" procedure on page 2-24 for instructions.

Step 2   From the CTC File menu, click **Add Node** (or click the **Add Node** button on the toolbar).

Step 3   In the Add Node dialog box, enter the node name (or IP address).

Step 4   If you want to add the node to the current login group, check **Add Node to Current Login Group**. Otherwise, leave it unchecked.

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

Step 5   Click **OK**.

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

2.6 Accessing ONS 15454 SDH Behind Firewalls

If an ONS 15454 SDH 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 port on the ONS 15454 SDH and/or CTC computer, depending on whether one or both devices reside behind firewalls.

> **Note**   For information about firewall settings using the Provisioning > Network > Gateway Settings feature, see Chapter 4, "IP Networking."

If the ONS 15454 SDH is in a protected network and the CTC computer is in an external network, as shown in Figure 2-4, enable the IIOP listener port specified by the firewall administrator on the ONS 15454 SDH. The ONS 15454 SDH sends the port number to the CTC computer during the initial contact between the devices using Hypertext Transfer Protocol (HTTP). After the CTC computer obtains the ONS 15454 SDH IIOP port, the computer opens a direct session with the node using the specified IIOP port.

Figure 2-4   ONS 15454 SDH residing behind a firewall
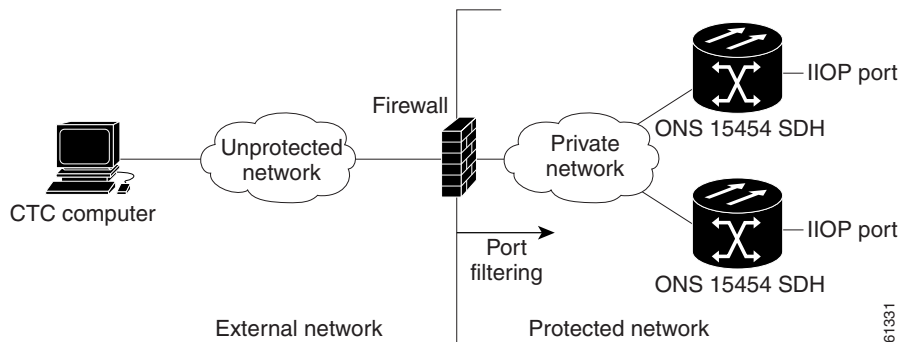
If the CTC computer and the ONS 15454 SDH both reside behind firewalls (Figure 2-5 on page 2-28), set the IIOP port on both the CTC computer and the ONS 15454 SDH. Each firewall can use a different IIOP port.

For example, if the CTC computer firewall uses IIOP Port 4000, and the ONS 15454 SDH 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 SDH.

Figure 2-5   CTC computer and ONS 15454 SDH residing behind firewalls
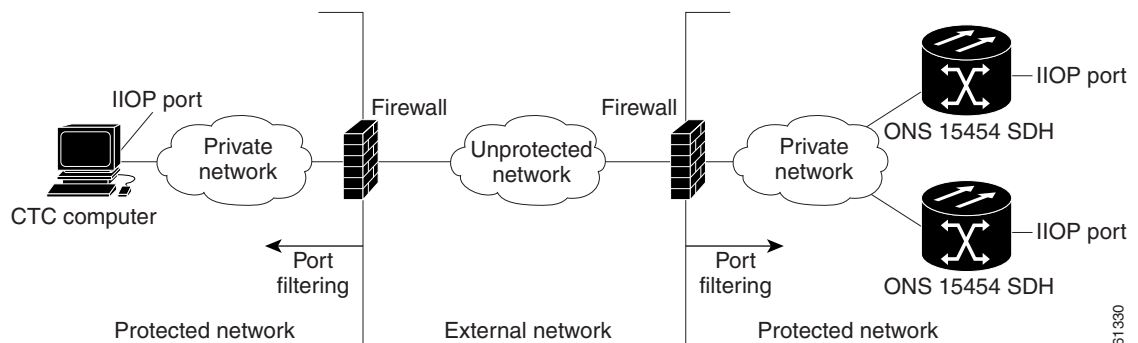
Procedure: Set the IIOP Listener Port on the ONS 15454 SDH

Purpose	Sets the IIOP listener port on the ONS 15454 SDH.
Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
Prerequisite Information	IIOP listener port number from LAN or firewall administrator
Onsite/Remote	Onsite or remote

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

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

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

- Default - TCC Fixed—Used to connect to ONS 15454 SDH from within a firewall or if no firewall is used

- Standard Constant (683)—Uses port 683, the Common Object Request Broker Architecture (CORBA) default port number
- Other Constant—Allows you to set an IIOP port specified by your firewall administrator

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

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

Both ONS 15454 SDH TCC-Is will reboot, one at a time.

Procedure: Set the IIOP Listener Port on CTC

Purpose	Sets the IIOP listener port on the Cisco Transport Controller.
Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
Prerequisite Information	IIOP listener port number from LAN or firewall administrator
Onsite/Remote	Onsite or remote

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

Step 2   In 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 15454 SDH from within a firewall or if no firewall is used
- Standard Constant (683)—Uses port 683
- Other Constant—Allows you to specify an IIOP port defined by your administrator

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

Step 5   Click **OK** to close the window.

2.7 Printing 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.

Procedure: Print CTC Window and Table Data

Purpose	Prints CTC windows and table data. Before you start, make sure your PC is connected to a printer.
Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
Onsite/Remote	Onsite or remote

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

Step 2   In the Print dialog box (Figure 2-6) 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 Figure 2-6).

Figure 2-6   Selecting CTC data for print
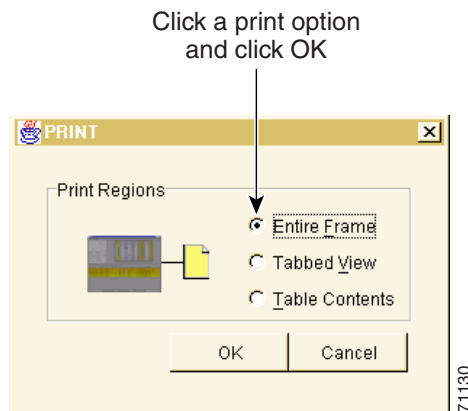
Step 3   Click **OK**.

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

2.8 Exporting CTC Data into 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.

Procedure: Export CTC Data

Purpose	Use the following procedure to export CTC data for use in other applications.

Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
	Table 2-14 shows CTC data that can be exported.
Onsite/Remote	Onsite or remote

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

Step 2   In the Export dialog box (Figure 2-7) 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 starting 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 2-7   Selecting CTC data for export
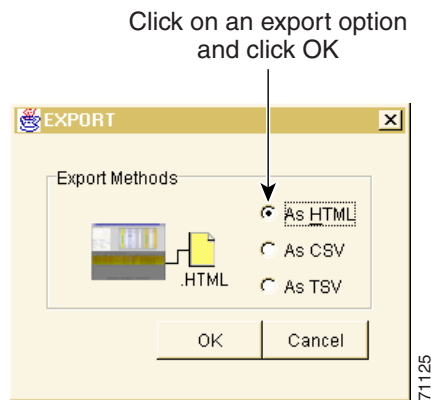
Step 3   Click **OK**.

Step 4   In the Save dialog box, 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.

Table 2-14   Table Data with Export Capability

View or Card	Tab	Subtab(s)
Network	Alarms	—
	Conditions	—
	History	—
	Circuits	Circuits
	Provisioning	Alarm Profiles, Overhead Circuits
	Maintenance	Software

Table 2-14   Table Data with Export Capability (continued)

View or Card	Tab	Subtab(s)
Node	Alarms	—
	Conditions	—
	History	Session, Node
	Circuits	Circuits
	Provisioning	Ether Bridge (Spanning Trees, Thresholds)
		Network (General, Static Routing, OSPF, RIP)
		MS-SPRing
		Alarm Behavior
		Defaults Editor
		UCP (Neighbor, IPCC, Interface, Circuits)
	Inventory	—
	Maintenance	Ether Bridge (Spanning Trees, MAC Table, Trunk Utilization)
		MS-SPRing
		Software
		Overhead Circuits
		Audit
		Routing Table
		RIP Routing Table
STM-N Cards	Alarms	—
	Conditions	—
	History	Session, Card
	Circuits	Circuits
	Provisioning	Line, Line Thresholds, VC4, Alarm Behavior
	Maintenance	Loopback, Info
	Performance	—
DS3I Card	Alarms	—
	Conditions	—
	History	Session, Card
	Circuits	Circuits
	Provisioning	Line, Line Thresholds, Elect Path Thresholds, SDH Thresholds, Alarm Behavior
	Maintenance	Loopback
	Performance	—

Table 2-14   Table Data with Export Capability (continued)

View or Card	Tab	Subtab(s)
E1 Card	Alarms	—
	Conditions	—
	History	Session, Card
	Circuits	Circuits
	Provisioning	Line, Line Thresholds, Elect Path Thresholds, SDH Thresholds, Alarm Behavior
	Maintenance	Loopback
	Performance	—
E3 Card	Alarms	—
	Conditions	—
	History	Session, Card
	Circuits	—
	Provisioning	Line, Line Thresholds, Elect Path Thresholds, SDH Thresholds, Alarm Behavior
	Maintenance	Loopback
	Performance	—
G1000-4 Card	Alarms	—
	Conditions	—
	History	Session, Card
	Circuits	Circuits
	Provisioning	Port, Enet Thrshlds, Alarming
	Maintenance	Loopback
	Performance	Statistics, Utilization, History
E100T-12-G, E1000-2-G Cards	Alarms	—
	Conditions	—
	History	Session, Card
	Circuits	Circuits
	Provisioning	Ether Port, Ether VLAN, Alarm Behavior
	Maintenance	Loopback
	Performance	Statistics, Utilization, History

Step 6   Click **Save**.

2.9 Using the Node View

CTC has three main ONS 15454 SDH views: node, network, and card view. The CTC node view, shown in Figure 2-8, displays when you start a CTC session on an ONS 15454 SDH. 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 SDH 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 user, and security level of the user. The graphic area depicts the ONS 15454 SDH FMECs and cards in the shelf assembly.

The CTC window displays when you start a CTC session on an ONS 15454 SDH (Figure 2-8). The window includes a menu bar, a toolbar, a status area, and a graphic area displaying the upper and lower node shelves.

The upper shelf displays status information about the selected objects and a graphic of the current view. The lower shelf displays tabs and subtabs that you use to view ONS 15454 SDH information and perform ONS 15454 SDH provisioning and maintenance.

Figure 2-8   CTC window elements in the node view (default session view)
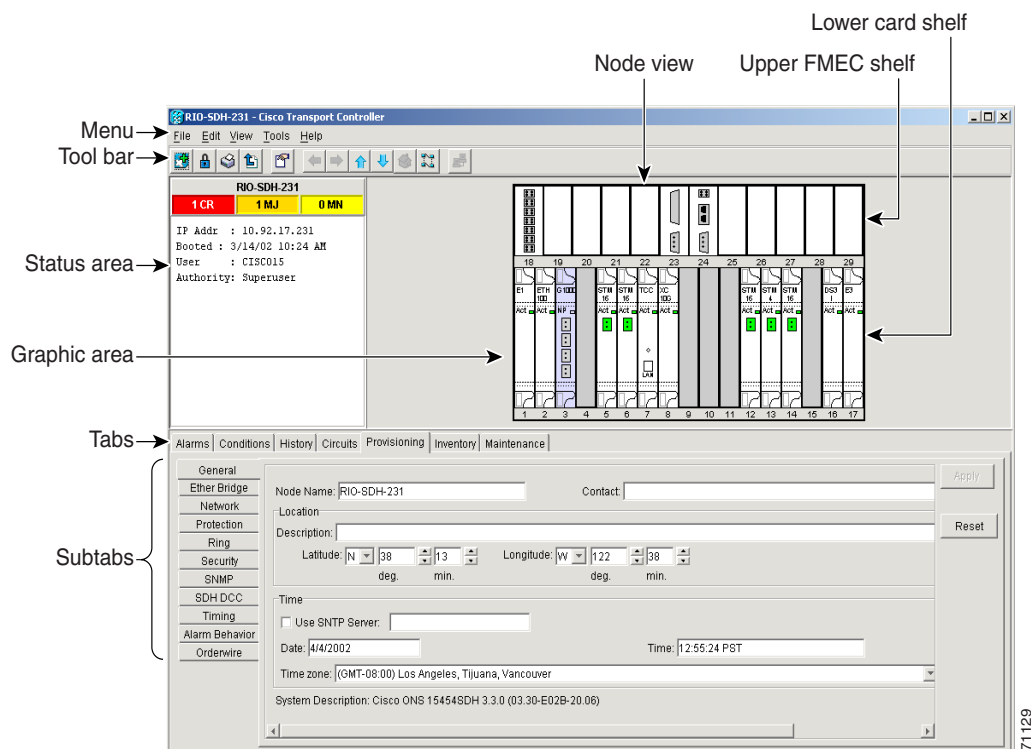
2.9.1 Node View Card Color and Graphic Definitions

The graphic area of the CTC window depicts the ONS 15454 SDH shelf assembly. The colors of the FMECs, cards, Act/Standby/NP, and ports in the graphic reflect the real-time status of the physical FMECs, cards, slots, and ports (Table 2-15). FMECs cannot be preprovisioned and the FMEC ports displayed in CTC do not change color.

Table 2-15   Node View FMEC Color, Card Color, Port Color, and Port Graphics

Upper Shelf FMEC Color	Status
White	A functioning card is installed.
Yellow	A minor alarm condition exists.
Orange (Amber)	A major alarm condition exists.
Red	A critical alarm exists.
Lower Shelf Card Color	**Status**
Grey	Slot is not provisioned; no card is installed.
Purple	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 (Amber)	Slot is provisioned; a major alarm condition exists.
Red	Slot is provisioned; a critical alarm exists.
Lower Shelf Act/Sty/NP/Ldg Color	**Status**
Yellow with Sty Graphic	The card is in standby.
Green with Act Graphic	The card is active.
Purple with NP Graphic	The card is not present.
White with Ldg Graphic	The card is resetting.
Lower Shelf Port Color	**Status**
Green	Port is in service (IS).
Grey	Port is out of service (OOS).
Light Blue	Port is in maintenance mode (OOS_MT).
Purple	Port is out of service until a valid signal is received (OOS_AINS).
Lower Shelf Port Graphics	**Status**
Multiple diagonal lines on port	Port is in service and card was reset.
Loop graphic on port	Port is in service and has a loopback provisioned in Card View > Maintenance > Loopback.

2.9.2 Node View Card Shortcuts

If you move your mouse over FMECs in the upper shelf of the graphic, tooltips displays the equipment FMEC card type. If you move your mouse over cards in the lower shelf in the graphic, tooltips displays 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 preprovision a card in the lower shelf (i.e., provision a slot before installing the card in the lower shelf).

Note   The FMECs in the upper shelf cannot be preprovisioned.

Note CTC software does not monitor for the presence or absence of FMECs unless the TCC-I card(s) has reached the active/standby state. During transitional states such as power-up or TCC-I reset, CTC ignores the FMEC inventory displayed in node view.

Procedure: Add a Node to the Current Session

Purpose	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.
Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
Onsite/Remote	Onsite or remote

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

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

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

Step 4 Click **OK**.

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

2.9.3 Check Inventory from the Node View

The Inventory tab (Figure 2-9 on page 2-37) displays information about cards installed in the ONS 15454 SDH node including location, equipment type, hardware part numbers, hardware revisions, and serial numbers. The Inventory tab provides information about ONS 15454 SDH Product Change Notices (PCNs) and Field Service Bulletins (FSBs). Using the ONS 15454 SDH export feature, you can export inventory data from ONS 15454 SDH nodes into spreadsheet and database programs to consolidate ONS 15454 SDH information for network inventory management and reporting.

Figure 2-9   Displaying ONS 15454 SDH hardware information

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

- Location—The slot where the card is installed

- Eqpt Type—Equipment type the slot is provisioned for, such as STM-4 or E-1

- Actual Eqpt Type—The actual card that is installed in the slot, for example, STM4 SH 1310 or E1N-14

Tip   You can preprovision a slot before the card is installed by right-clicking the slot in node view and selecting a card type. FMECs, located in the upper shelf, cannot be preprovisioned.

- HW Part #—Card part number, printed on the top of the card

- HW Rev—Card revision number

- Serial #—Card serial number, 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

- Delete button —Used to delete equipment from CTC

- Reset button—Used to remotely reboot a card

2.9.4 View CTC Software Versions on One Node

CTC software is preloaded on the ONS 15454 SDH TCC-I cards; therefore, you do not need to install software on the TCC-I. 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 SDH software (Figure 2-10).

When you upgrade CTC software, the TCC-I stores the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. To view software versions on the network, see the "View CTC Software Versions on the Network" section on page 2-50.

Figure 2-10   Viewing software versions
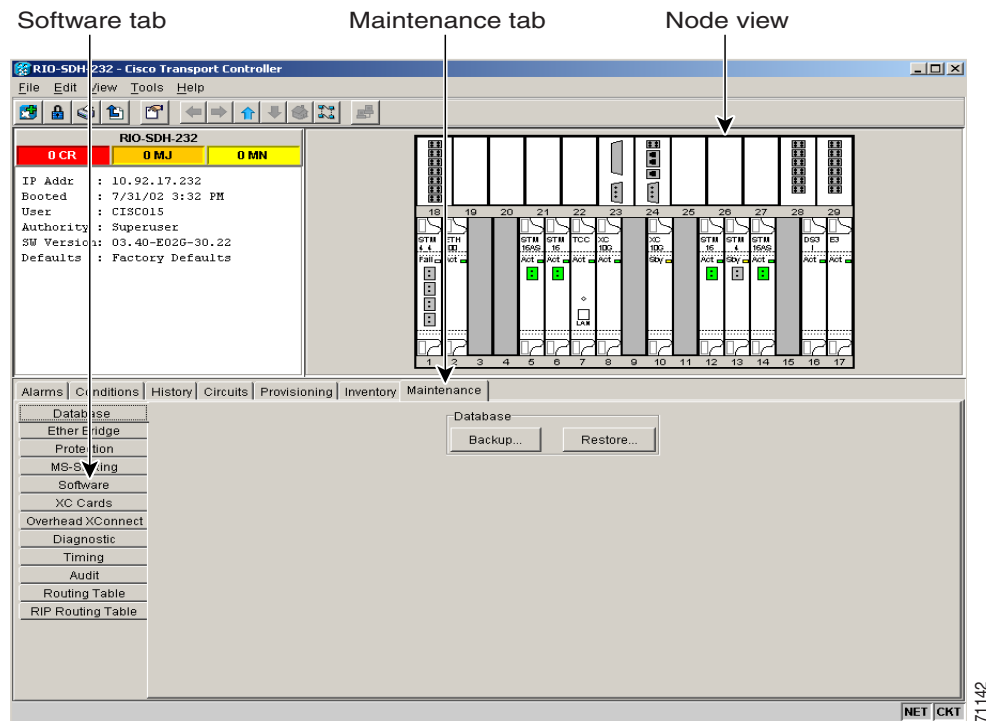
2.9.5 Node View Tabs

Use the node view tabs and subtabs shown in Table 2-16 to provision and manage the ONS 15454 SDH.

Table 2-16   Node View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the node and updates them in real time.	—
Conditions	Displays a list of standing conditions on the node.	—

Table 2-16   Node View Tabs and Subtabs (continued)

Tab	Description	Subtabs
History	Provides a history of node alarms including date, type, and severity of each alarm.	Session, Node: 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.
Circuits	Create, delete, edit, and search circuits.	Circuits
Provisioning	Provision the ONS 15454 SDH node.	General, Ether Bridge, Network, Protection, MS-SPRing, Security, SNMP, SDH DCC, Timing, Alarm Behavior, Defaults Editor, UCP
Inventory	Provides inventory information (part number, serial number, CLEI codes) for cards installed in the node. Allows you to delete and reset cards.	—
Maintenance	Perform maintenance tasks for the node.	Database, Ether Bridge, Protection, MS-SPRing, Software, XC Cards, Overhead XConnect, Diagnostic, Timing, Audit, Routing Table, RIP Routing Table

2.10 Using the Network View

Network view (Figure 2-11 on page 2-40) allows you to view and manage ONS 15454 SDH nodes that have DCC connections to the node running the CTC session and any login node groups you have selected. (Nodes that are optically connected to the login node will not display if you selected Exclude Dynamically Discovered Nodes in the Login dialog box.)

The graphic area displays a background image with colored ONS 15454 SDH icons. The icon colors indicate the node status. 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 2-11   Two-node network displayed in CTC network view

Icon color indicates
node status

Dots indicate
selected node

Bold letters and
asterisk show
login node
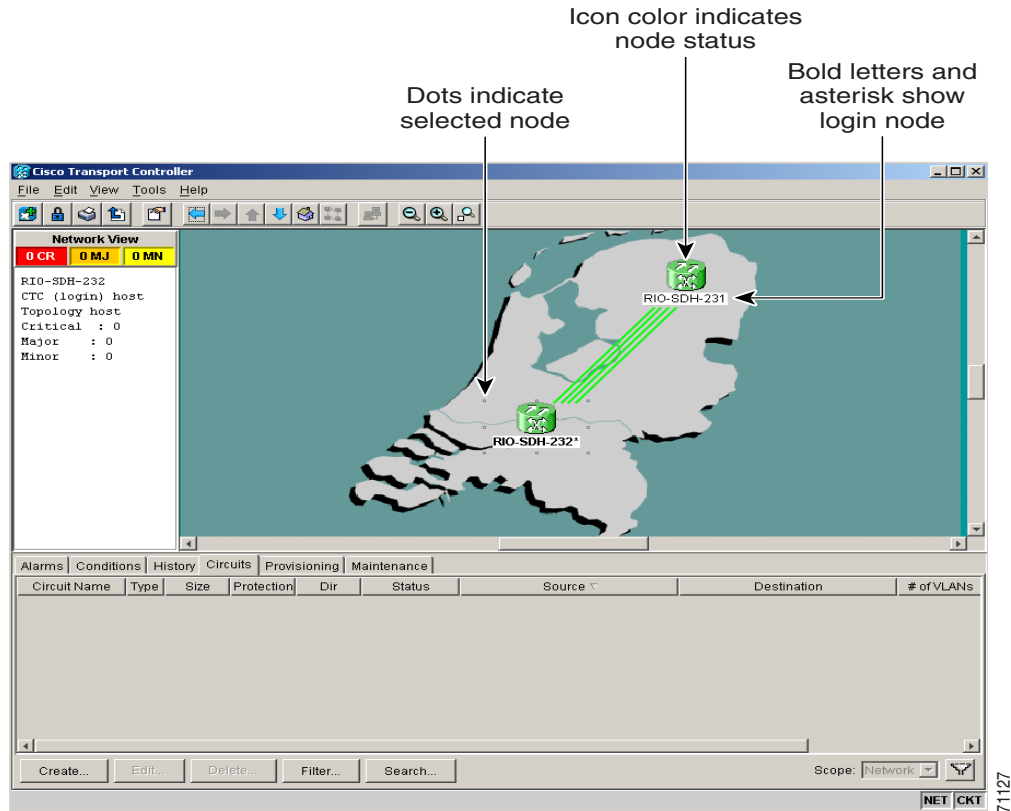
2.10.1 Network View Node Color Definitions

The colors of nodes displayed in network view show alarm status.

Table 2-17   Node Status in Network View

Color of Node Icon	Alarm Status
Green	No alarms
Yellow	Minor alarms
Orange (Amber)	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

2.10.2 Network View User Options

Right-click the network view graphic area or a node, span, or domain (domains are described in the "Create and Manage Domains in the Network View" procedure on page 2-43) to display shortcut menus. Table 2-18, Table 2-19, and Table 2-20 list the actions that are available from the network view.

Table 2-18   Network View User Options from the Node Icon

Action	Procedure
Node icon actions:	
Open a node	Any of the following: • Double-click a node icon. • Right-click a node icon, and choose **Open Node** from the shortcut menu. • Click a node and from the View menu, choose **Go to Selected Object View**. • From the View menu, choose **Go to Other Node**. Select a node from the Select Node dialog box. • Double-click a node alarm or event in the Alarms or History tab.
Reset the default 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 set in node view on the Provisioning > General tabs.
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 "Creating VC High-Order Path Circuits" procedure on page 6-3, or "Creating VC Low-Order Path Tunnels for Port Grouping" procedure on page 6-12.
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.
Move a node icon	Press the **Ctrl** key and the left mouse button simultaneously and drag the node icon to a new location.

Table 2-19   Network View User Options from the Span Icon

Action	Procedure
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.
Span (straight lines between nodes) actions:	
Perform an SNCP protection switch for an entire span	Right-click a network span and click **Circuits**. See "Perform SNCP span switching" for subnetwork connection protection (SNCP) span switching procedures.

Table 2-19   Network View User Options from the Span Icon (continued)

Action	Procedure
Display the Circuits on Span dialog box for PCA circuits.	Right-click a network span and click **PCA Circuits**. For circuit creation procedures, see the "Creating VC High-Order Path Circuits" procedure on page 6-3, or "Creating VC Low-Order Path Tunnels for Port Grouping" procedure on page 6-12.
Upgrade a span	Right-click a span and choose **Span Upgrade** from the shortcut menu. **Note** For detailed span upgrade information and instructions, refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.
Display a link end point	Right-click a span. From the shortcut menu, select **Go To** *node/slot/port* for the drop port you want to view. CTC displays the card in card view.

Table 2-20   Network View User Options from the Graph Menu

Action	Procedure
Map or background image actions:	
Create a new domain	Choose **Create New Domain.** See the "Create and Manage Domains in the Network View" procedure on page 2-43.
Center the map	Any of the following: • Right-click the map in the background and choose **Center Graph**. • Click and drag the vertical and horizontal scroll bars framing the map image. • Click the arrow buttons at the ends of the vertical and horizontal scroll bars framing the map image.
Stretch the map to fit into the network view window	Right-click on the map in the background and choose **Fit Graph to Window**.
Reset map to default view	Right-click on the map in the background and choose **Reset Zooming (1:1)**.
Enlarge the map	Any of the following: • Click the **Zoom In** icon. • Right-click on the map in the background and choose **Zoom In**.
Reduce the map size	Any of the following: • Click the **Zoom Out** icon. • Right-click on the map in the background and choose **Zoom Out**.
Enlarge a selected area of the map	Any of the following: • Click the **Zoom Selected Area** icon. Left-click the desired start point on the map, drag the mouse to the desired end point of the map, and release the mouse. • Right-click the map in the background and choose **Zoom Selected Area**. Left-click the desired start point on the map, drag the mouse to the desired end point of the map, and release the mouse.

Table 2-20   Network View User Options from the Graph Menu (continued)

Action	Procedure
Change the color behind the map image	Right-click the map in the background and choose **Set Background Color**. The Choose Color menu appears with three tabs: Swatches, HSB, and RGB. Make a selection using your mouse; then, click **OK**. For more information, see the "Modify the Network or Domain Background Color" procedure on page 2-47.
Set a user-defined background image	Right-click the map or image in the background and choose **Set Background Image**. From the menu, select any JPEG or GIF image that is accessible on a local or network drive. For more information, see the "Change the Network View Background Image" procedure on page 2-49.
Remove a map or user-defined background image	Right-click the map or image in the background and choose **Remove Background Image**.

Procedure: Create and Manage Domains in the Network View

Purpose	Domains are groups of ONS 15454 SDH nodes displayed as icons on the network view map. Adding domains to the network view map makes networks with many nodes easier to manage. You must have superuser login access to create, delete, or rename a domain, add a node to a domain, or remove a node from a domain.
Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
Onsite/Remote	Onsite or remote

Note   Domains you create will be seen by all CTC users on the network. When you create a domain and add a node, other CTC users might see the node disappear momentarily from the network view. Also, when the domain view is open, CTC switches to the network view if the domain is removed by another CTC user.

Step 1   Right-click the network map and choose **Create New Domain** (Figure 2-12 on page 2-44) from the shortcut menu. When the domain icon appears on the map, type the domain name.

Figure 2-12   Creating a domain

Right-click and choose
Create New Domain
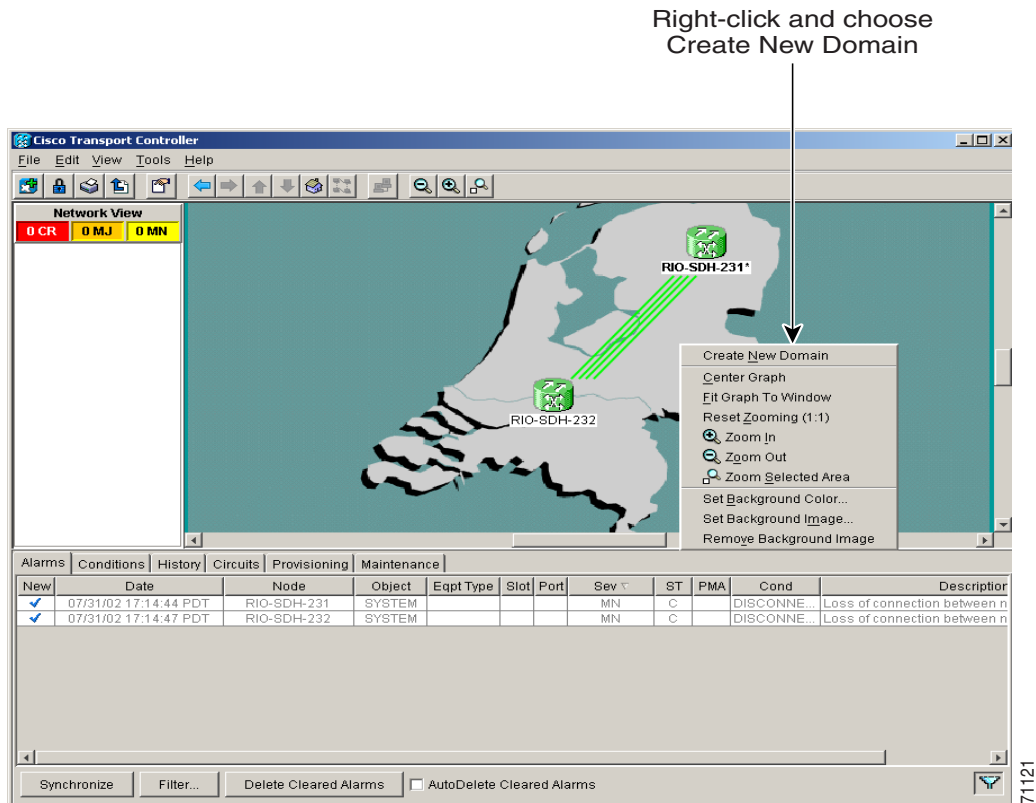
Step 2   Press **Ctrl** on the keyboard; then, click and drag a node icon to the domain icon (Figure 2-12 on page 2-44). Release the mouse button when the node icon is over the domain icon. Repeat this step for each node you want to add to the domain.

After you add a node to a domain, the span lines leading to nodes within the domain become thicker. The thick lines might represent multiple spans. The thick line is green if all spans it represents are active, and grey if any one span it represents has errors. The domain icon color reflects the highest alarm severity of any node within it. For node color and alarm status, see Table 2-17 on page 2-40.

Figure 2-13   Adding nodes to a domain
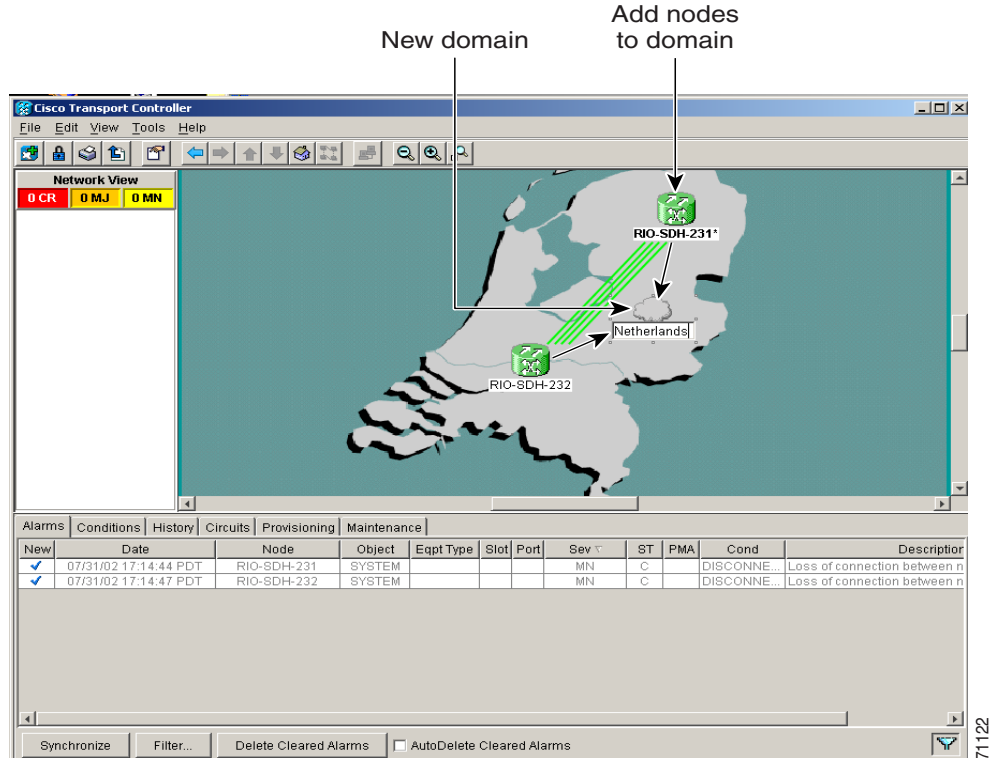
Step 3   Open the domain by double-clicking the domain icon, or by right-clicking the domain and choosing
Open Domain. Verify that the selected nodes are within the domain as shown in Figure 2-14.

Within the domain, external nodes and domains that are directly connected to nodes inside the domain
are displayed in a dimmed color. DCC links with one or two ends that are inside the domain are also
displayed.

Figure 2-14   Nodes displayed within the domain
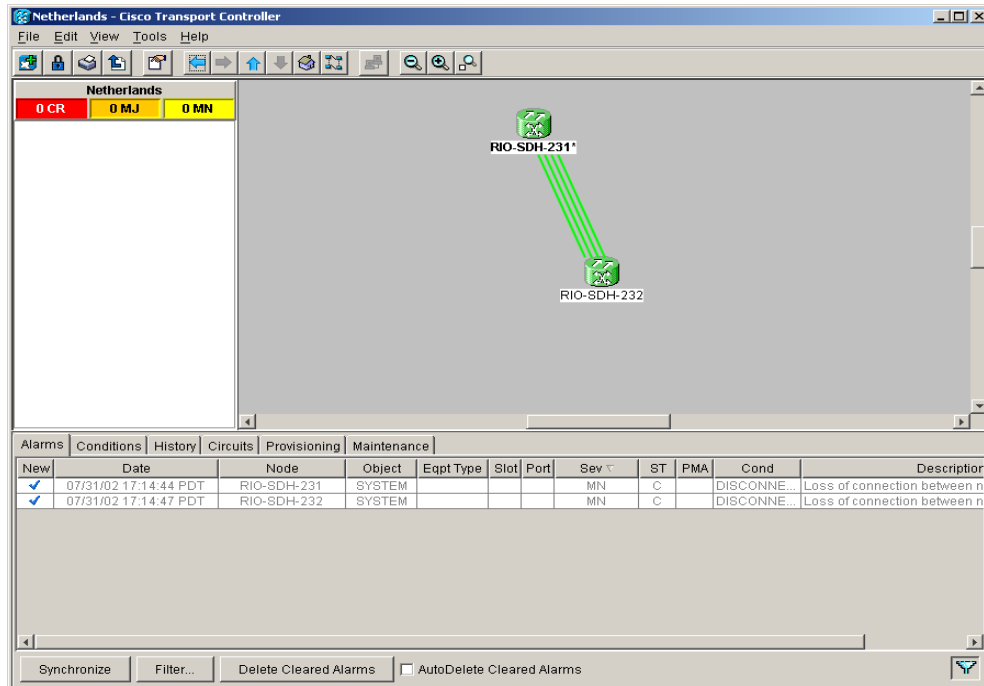
Step 4   Right-click the domain view area and choose **Go to Parent View** from the shortcut menu to return to the network view.

You manage ONS 15454 SDH nodes that reside within a domain the same way that you manage ONS 15454 SDH nodes on the network map. Table 2-21 shows the domain actions.

Table 2-21   Managing Domains

Action	Procedure
A domain must be created before the following domain menu options are available:	
Move a domain	Pressing **Ctrl**, drag the domain icon to the new location.
Move a node out of a domain and back to the network map	From the domain view, right-click a node and choose **Move Node Back to Parent View**.
Domain actions:	
Open a domain	Right-click the domain icon and choose **Open Domain**.
Show domain overview	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.
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.
Remove domain	Right-click the domain icon and choose **Remove Domain**. Any nodes residing in the domain are returned to the network map.

Procedure: Modify the Network or Domain Background Color

Purpose	You can change the color of the background for the network view and the domain view (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.
Prerequisite Procedures	"Running the CTC Setup Wizard" procedure on page 2-4
Onsite/Remote	Onsite or remote

Step 1 From the network view, right-click the domain map area or background color and choose **Set Background Color** from the shortcut menu.

Step 2 In the Choose Color dialog box, select the **Swatches**, **HSB**, or **RGB** tab.

- Swatches—Displays small color samples in a box (Figure 2-15). Click the color sample to display a preview of the color in the lower portion of the Choose Color dialog box. When you have made your selection, click **OK**.

Figure 2-15   Choosing a swatch from the color menu
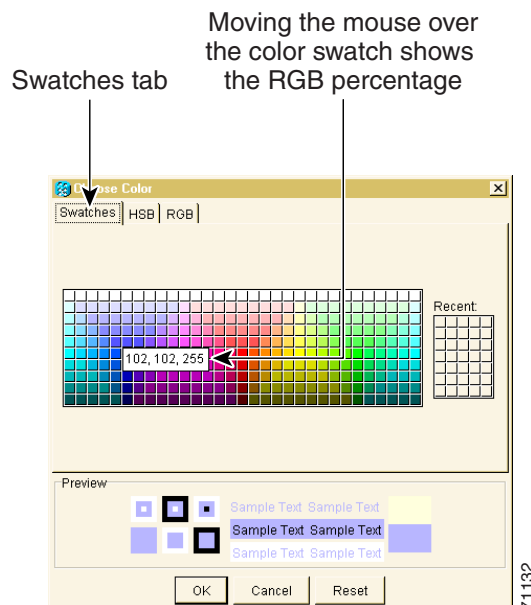
- HSB—Allows you to change the hue, saturation, and brightness of your background color (Figure 2-16 on page 2-48). Click a color on the color map. Click the H, S, or B button. Use the scroll bar to display the full range of the selected color for hue, saturation, or brightness depending on the button selected. For example, click on B then drag the scroll bar up and down. A lighter and then darker version of the selected color displays in the preview area shown in the lower portion of the Choose Color dialog box. After making your selection, click **OK**.

Figure 2-16   Changing hue, saturation, or brightness from the color menu
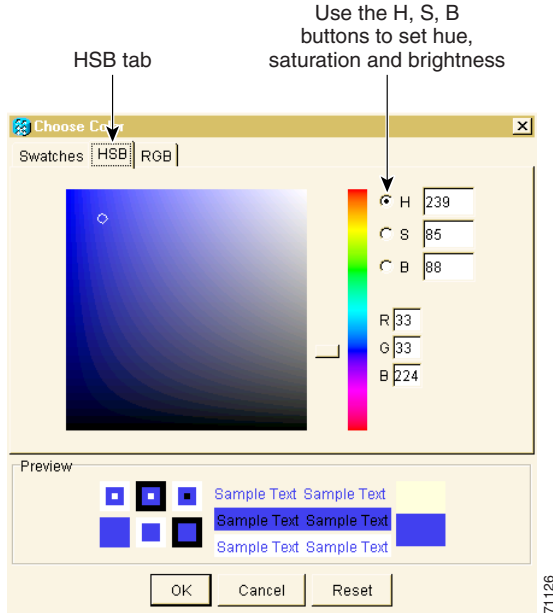
• RGB—Displays red, green, and blue percentages from 0 to 255 (Figure 2-17). Click and drag the red, blue, or green percentage bar to create the desired color or enter a number in the field next to the bar. Check your selection in the preview area in the lower portion of the Choose Color dialog box; then, click **OK**.

Figure 2-17   Choosing red, blue, or green from the color menu

Procedure: Change the Network View Background Image

Purpose	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. Changing the map does not affect other CTC users.
Prerequisite Procedures	"Logging Into CTC" procedure on page 2-23
	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.
Onsite/Remote	Onsite or remote

⚠️

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 might stop responding in the Network view or Circuit tab 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 can also right-click the network or domain map and select **Set Background Image**.)

Step 2   In the **Map** tab of the Preferences dialog box (Figure 2-18 on page 2-50), complete one of the following options:

- Uncheck **Use Default Map** and click **Browse**. Navigate to the graphic file you want to use as a background. Select the file. Click **Open**.

- Choose a new default map from the menu. There are 6 default map options: Germany, Japan, Netherlands, South Korea, United Kingdom, and United States.

Figure 2-18   Changing the background image from the Preferences dialog box

Enter or browse to
custom map or image

Choose from a list
of default maps
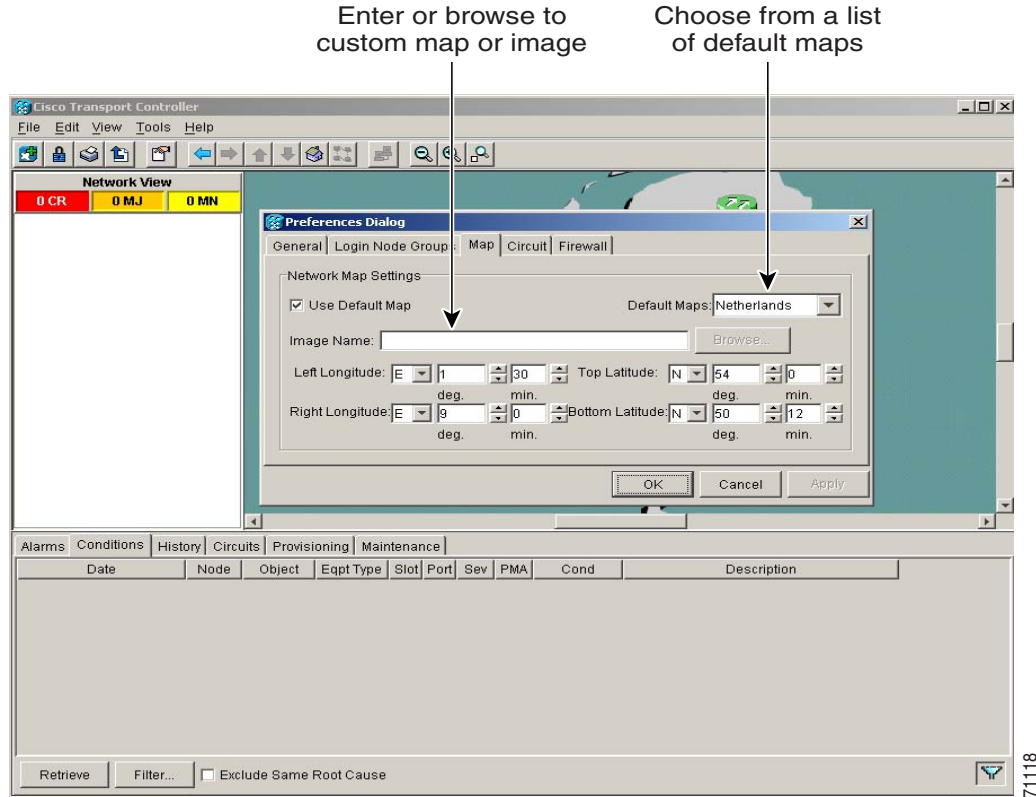
Step 3   (Optional) Enter the coordinates for the map image edges in the longitude and latitude fields on the Preferences dialog box. CTC uses the map's longitude and latitude to position the node icons based on the node coordinates entered for each node on the **Provisioning > General** tabs. Coordinates 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 4   Click **Apply** and then click **OK**.

Step 5   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.

2.10.3 View CTC Software Versions on the Network

CTC software is preloaded on the ONS 15454 SDH TCC-I cards; therefore, you do not need to install software on the TCC-I. When a new CTC software version is released, you must follow procedures provided by the Cisco TAC on the web at http://www.cisco.com/public/support/tac/home.shtml to upgrade the ONS 15454 SDH software.

When you upgrade CTC software, the TCC-I stores the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. To view software in the CTC network view, click the **Maintenance > Software** tabs. To view software versions on one node, see the "View CTC Software Versions on One Node" procedure on page 2-38.

2.11 Using the Card View

The card view (Figure 2-19) displays information about individual ONS 15454 SDH cards. Use this view to perform card-specific maintenance, provisioning, and performance monitoring. A graphic of the selected card is shown in the graphic area. The status area displays the node name, slot, number of alarms, equipment type, and card status—Active, Not Present, or Failed—for the card. 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 SDH cards except the FMECS, TCC-I, and XC10G cards.

Figure 2-19   CTC card view showing a DS3I card
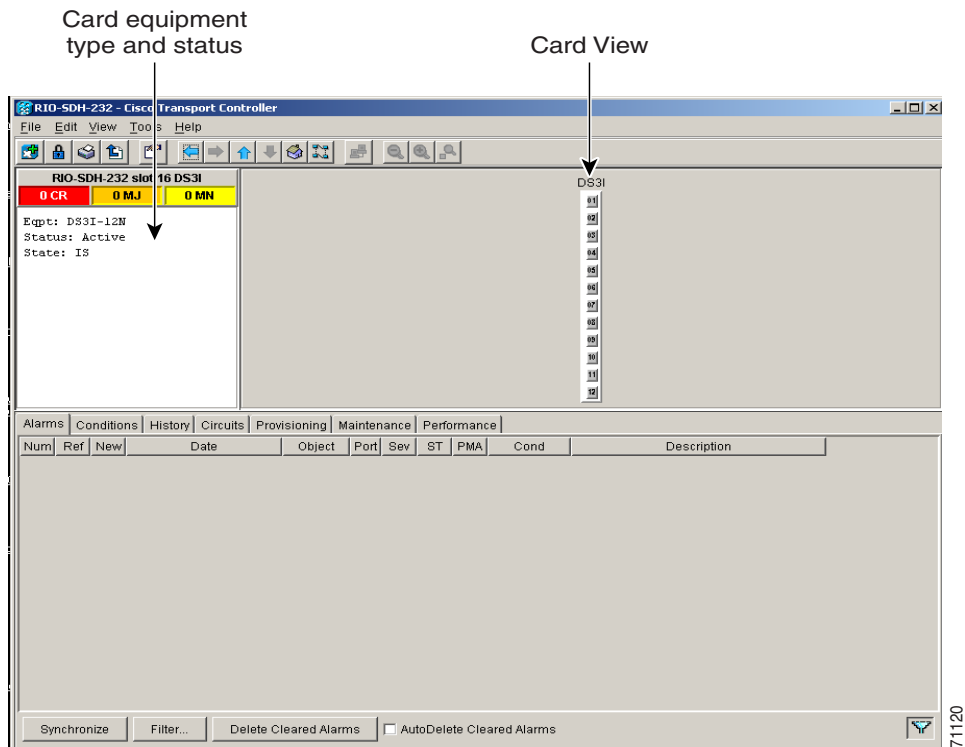
2.11.1 Card and Port Color Definitions

The graphic area of the CTC window depicts the ONS 15454 SDH shelf assembly. The colors of the card and port(s) in the graphic reflect the real-time status of the physical card and port(s) (Table 2-22 on page 2-52).

Note   Port graphics showing loopbacks and card resets do not appear on the card view level. Proceed to node view to see special port graphics.

Table 2-22   Card View Card and Port Colors

Upper Shelf FMEC Color	Status
N/A	FMECs do not display a card view.
Lower Shelf Card Color in Card View	**Status**
White	A functioning card is installed.
Yellow	A minor alarm condition exists with the card.
Orange (Amber)	A major alarm condition exists with the card.
Red	A critical alarm condition exists with the card.
Port Color	**Status**
Grey	Port is out of service.
Green	Port is in service.

2.11.2 Card Shortcuts

If you move your mouse over the port graphic, tooltips displays additional information about the port, including the port status (active or standby) and the alarm profile. Right-clicking the card view graphic reveals a shortcut menu, which you can use to go to the parent view (node view).

2.11.3 Tabs

Use the card view tabs and subtabs, shown in Table 2-23, to provision and manage the ONS 15454 SDH.

Table 2-23   Card View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the card and updates them in real-time.	—
Conditions	Displays a list of standing conditions on the card.	—
History	Provides a history of card alarms including date, object, port, and severity of each alarm.	Session, Card: The Session subtab displays alarms and events for the current session. The Card subtab displays alarms and events retrieved from a fixed-size log on the card.
Circuits	Create, delete, edit, and search circuits.	Circuits
Provisioning	Provision an ONS 15454 SDH card.	Line, Line Thresholds (different threshold options are available for electrical and optical cards), VC4, Elect Path Thresholds or SDH Thresholds, and Alarm Behavior
Maintenance	Perform maintenance tasks for the card.	Loopback, Protection
Performance	Perform performance monitoring for the card.	—

2.12 Navigating CTC

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 2-20).

Figure 2-20   CTC Node view showing popup information
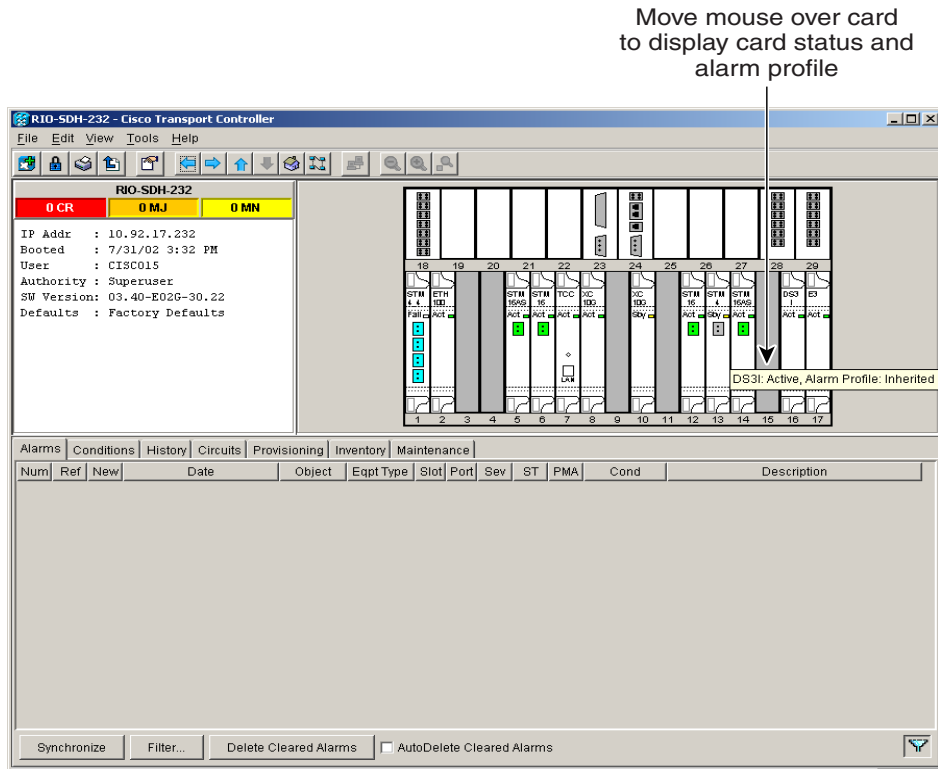
Different methods for navigating within the CTC window are described in Table 2-24 on page 2-54.

Table 2-24   CTC Window Navigation

Technique	Description
View menu and toolbar	Provide commands to display:
	• 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.
	• Home view (the node you initially logged into).
	• Network view.
	• Other node (View menu only).
	• Different zoom levels (toolbar only).
Double-click	• A node in network view displays the node in node view.
	• A card in node view displays the card in card view.
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 SDH SNCP 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.
	• Over span in network view—Displays circuit (node, slot, port) and protection information.
	• Over card in node view—Displays card type and alarm profile.
	• Over card port in node view—Displays port state and alarm profile.

2.13 Viewing CTC Table Data

Much of the ONS 15454 SDH 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 "Export CTC Data" procedure on page 2-30 and the "Viewing CTC Table Data" procedure on page 2-55.

2.13.1 Change the CTC Table Display

To change the display of a CTC table, left-click to change the order to ascending or descending. Right-click a column header to display a shortcut menu that has table column display options (Figure 2-21).

Figure 2-21   Table shortcut menu that customizes table appearance
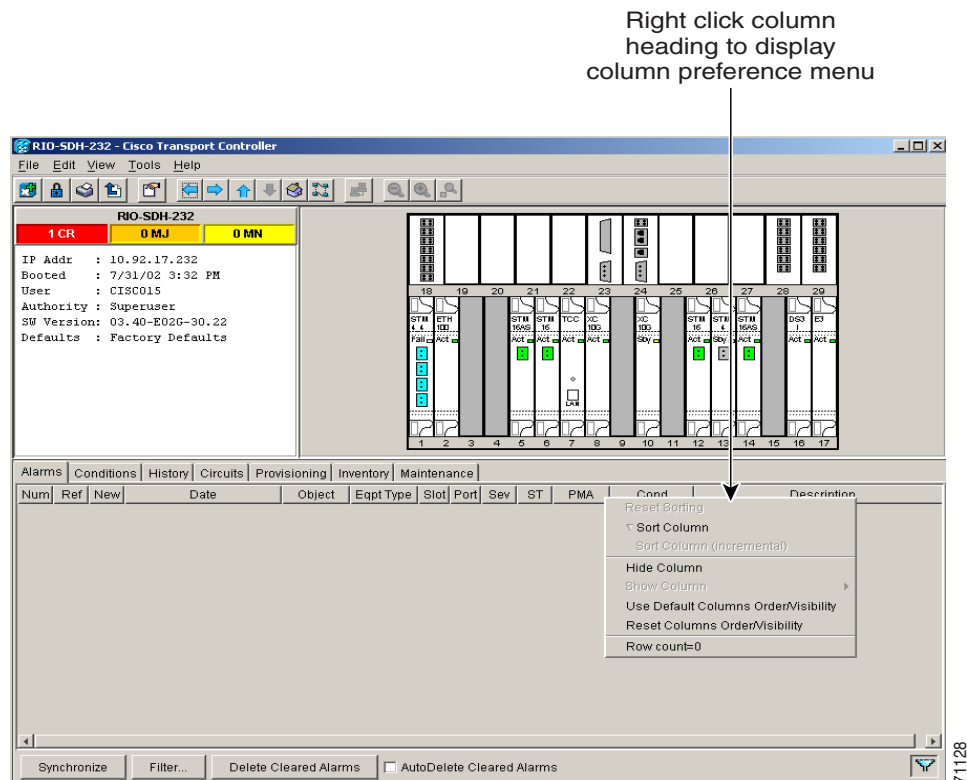
Table 2-25 on page 2-56 lists the options that you can use to customize information display in CTC tables.

Table 2-25   Table Display Options

Task	Click	Right-Click Shortcut Menu
Resize column	Drag header separator to the right or left.	—
Rearrange column order	Drag column header to the right or left.	—
Column header actions:		
Reset sorting	—	Choose **Reset Sorting.**
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).**
Hide column	—	Choose **Hide Column.**
Display a hidden column	—	Choose **Show Column** > **Num** or **Ref**.
Revert to default columns	—	Choose **Use Default Columns Order/Visibility.**
Reset column order and display all hidden columns	—	Choose **Reset Columns Order/Visibility.**
View table row count	—	Choose **Row count**; it is the last item on the shortcut menu.

Node Setup

This chapter explains how to set up a Cisco ONS 15454 SDH node using Cisco Transport Controller (CTC). Table 3-1 lists node setup topics. Table 3-2 lists node setup procedures. The chapter also includes a list of required information for node setup. Refer to Chapter 2, "Set Up PC and Log Into CTC" for CTC setup procedures.

Table 3-1   Node Setup Topics

Node Setup Topics
3.1 Before You Begin, page 3-2
3.2 Setting Up Basic Node Information, page 3-3
3.3 Setting Up Network Information, page 3-5
3.4 Creating Users and Setting Security, page 3-9
3.5 Setting Up ONS 15454 SDH Timing, page 3-18
3.6 Creating Card Protection Groups, page 3-26
3.7 Setting Network Element Defaults, page 3-30

Table 3-2   Node Setup Procedures

Node Setup Procedures
Procedure: Add the Node Name, Contact, Location, Date, and Time, page 3-3
Procedure: Set a Port Name for a Card, page 3-4
Procedure: Set Up Network Information, page 3-5
Procedure: Change IP Address, Default Router, and Network Mask Using the LCD, page 3-7
Procedure: Set Up Passwords from Network View, page 3-11
Procedure: Set Up Passwords from Node View, page 3-13
Procedure: Change a User's Security Settings, page 3-14
Procedure: Delete a User's Security Settings, page 3-16
Procedure: Set Up External, Line, or Mixed Timing for the ONS 15454 SDH, page 3-21
Procedure: Set Up Internal Timing for the ONS 15454 SDH, page 3-24
Procedure: Create Protection Groups, page 3-27
Procedure: Edit Protection Groups, page 3-29

Table 3-2   Node Setup Procedures (continued)

Node Setup Procedures
Procedure: Delete Protection Groups, page 3-30
Procedure: Edit Network Element Defaults, page 3-31
Procedure: Import Network Element Defaults, page 3-32
Procedure: Export Network Element Defaults, page 3-32

3.1 Before You Begin

Before you begin node setup, you will need:

- Node name
- Contact name (optional)
- Location (optional)
- Longitude and latitude (optional)
- Date and time
- Time zone

If the ONS 15454 SDH will be connected to a network, you will need:

- The IP address and subnet mask to assign to the node
- The IP address of the default router
- The IP address of the Dynamic Host Configuration Protocol (DHCP) server (if DHCP is used)

If you are responsible for setting up IP networking for the ONS 15454 SDH 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 SDH 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 the "Setting Up the CTC Computer" section on page 2-10.

3.2 Setting Up Basic Node Information

Setting basic information for each Cisco ONS 15454 SDH node is one of the first provisioning tasks you perform. This information includes node name, location, contact, latitude, longitude, dates, and time.

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

Purpose	Use this procedure to set node name, location, contact, latitude, longitude, dates, and time.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Start CTC for an ONS 15454 SDH node. The CTC node view is displayed.

Step 2   Click the **Provisioning > General** tabs (Figure 3-1).

Figure 3-1   Setting up general node information
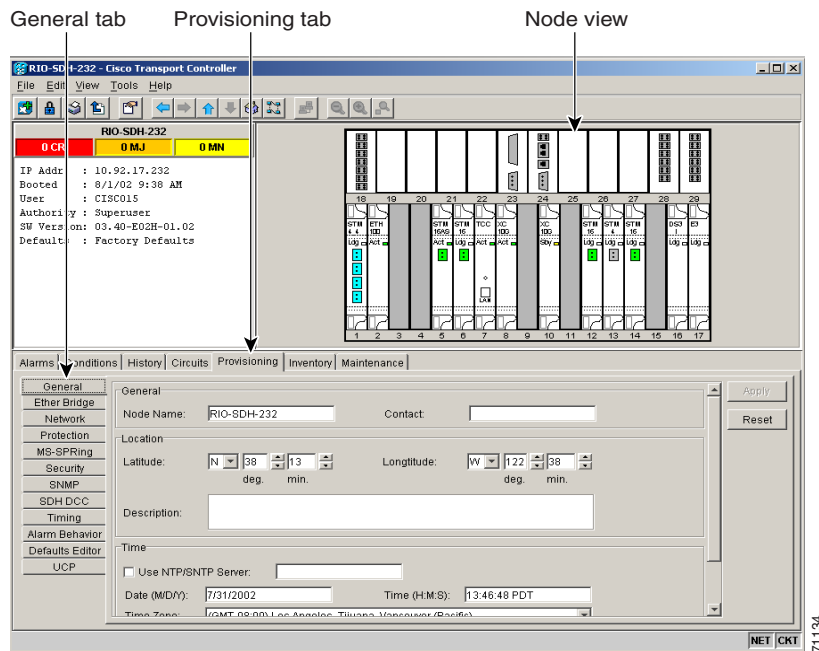
Step 3   Enter the following:

- Node Name—Type a name for the node. For TL1 compliance, names must begin with an alphabetical character and have no more than 20 alphanumeric characters. (TL1 is not available in SDH Software R3.4 and earlier.)

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

- Location—Type the node location, for example, a city name or specific office location (optional).

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

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

CTC uses the latitude and longitude to position node icons on the network view map.

> **Note** You can also position nodes manually by pressing **Ctrl** and dragging the node icon to a new location.

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/NTP Server—When checked, CTC uses a Simple Network Time Protocol (SNTP) server or a Network Time Protocol (NTP) server to set the date and time of the node. Using an SNTP/NTP server ensures that all ONS 15454 SDH network nodes use the same date and time reference. The server synchronizes the time of the nodes after power outages or software upgrades.

   If you check Use SNTP/NTP Server, type the server's IP address in the next field. If you do not use an SNTP/NTP server, complete the Date, Time, and Time Zone fields. The ONS 15454 SDH 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 if you did not select Use SNTP/NTP Server.
- Time—Type the current time if you did not select Use SNTP/NTP Server.
- Time Zone—Select the time zone if you did not select Use SNTP/NTP Server.

Step 4 Click **Apply**.

Procedure: Set a Port Name for a Card

Purpose	Use this procedure to assign a name to one port on a card.
Prerequisite Procedures	Verify card installation
Onsite/Remote	Onsite or remote

Step 1 Log into the node where you want to set a port name for a card or cards. The node (default) view displays. See the "Log Into CTC" procedure on page 2-24 for instructions.

Step 2 Double-click the card that has the port you want to provision.

Step 3 Click the **Provisioning** tab.

Step 4 Click the **Name** column for the port number you are naming and enter the desired port name.

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

Step 5 Click **Apply**.

3.3 Setting Up Network Information

Before you connect a node to other nodes or to a LAN, you must change the default IP address that is shipped with each ONS 15454 SDH (192.168.1.1). 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 15454 SDH nodes often exist as subnetworks, which are created by adding a subnet mask to the ONS 15454 SDH IP address.

Procedure: Set Up Network Information

Purpose	Use this procedure to start provisioning a network. Additional ONS 15454 SDH networking information and procedures, including IP addressing examples, static route scenarios, and Open Shortest Path First (OSPF) protocol options, are provided in Chapter 4, "IP Networking."
Prerequisite Information	• The IP address and subnet mask to assign to the node • The IP address of the default router • The IP address of the DHCP server (if DHCP is used)
Onsite/Remote	Onsite or remote

Step 1 Log into CTC or navigate to the node view. Click the **Provisioning > Network > General** tabs (Figure 3-2).

Figure 3-2   Setting up general network information
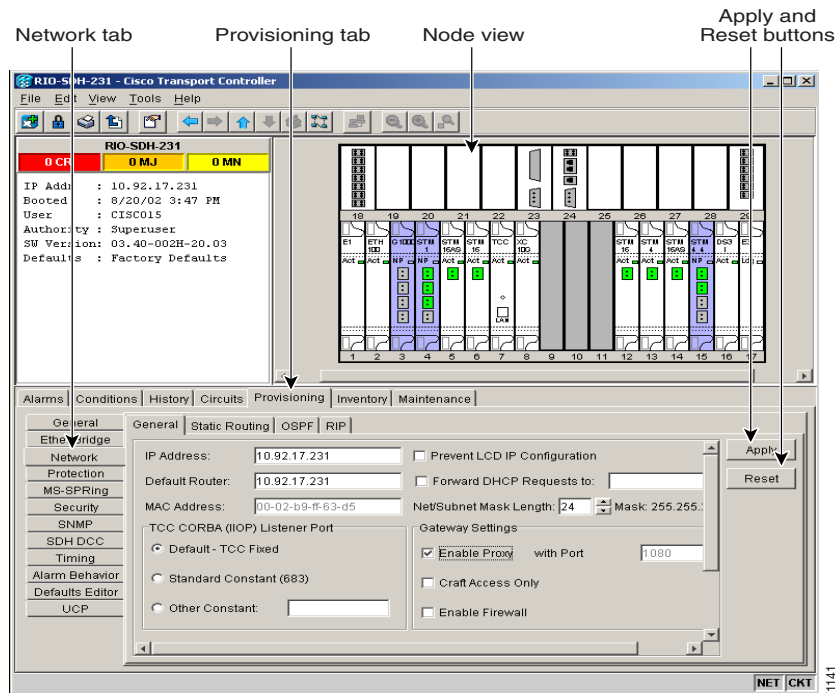
Step 2 Complete the following:

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

- Prevent LCD IP Config—If checked, this field prevents the ONS 15454 SDH IP address from being changed using the liquid crystal display (LCD). If you want to use the LCD, see the "Change IP Address, Default Router, and Network Mask Using the LCD" procedure on page 3-7.

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

- Subnet Mask Length—If the ONS 15454 SDH is part of a subnet, type the subnet mask length (a 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 15454 SDH nodes in the same subnet.

> **Note** The MAC Address field is read only. It displays the ONS 15454 SDH address used by the IEEE 802 Media Access Control (MAC) layer.

- Forward DHCP Requests To—When checked, this field 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 SDH node can find temporary IP addresses from the DHCP server.

- TCC CORBA (IIOP) Listener Port—Sets a listener port to allow communication with the ONS 15454 SDH through firewalls. See the "Accessing ONS 15454 SDH Behind Firewalls" section on page 2-27 for more information.

- Gateway Settings—See "Scenario 9: Using the Proxy Server Features" section on page 4-16 for detailed information.

  - Craft Access Only—When this choice is enabled, the ONS 15454 SDH neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15454 SDH, but they cannot communicate directly with any other DCC-connected ONS 15454 SDH.

    In a configuration where all nodes are on the same subnet, if you start a CTC session before proper provisioning, the login node appears grey in the CTC network view. Other CTC users are not be able to open the grey-colored node to access their node. Provision a static route on the node that is LAN-connected, or, if you are directly connected to the node, provision craft access. For procedures, see the "Scenario 5: Using Static Routes to Connect to LANs" section on page 4-6 or the "Scenario 9: Using the Proxy Server Features" section on page 4-16.

  - Enable Proxy—When this choice is enabled, the ONS 15454 SDH responds to CTC client requests with a list of DCC-connected ONS 15454 SDH nodes for which the node serves as a proxy. The CTC client establishes connections through the proxy server for any ONS 15454 SDH in the returned list. By using the proxy, the CTC client can connect to nodes that the PC on which the CTC client runs cannot access. If Enable Proxy is off, the node responds to CTC requests with an empty list, indicating that it is not willing to serve as a proxy.

  - Enable Firewall—If this choice is selected, the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15454 SDH can communicate with machines connected to the LAN port or connected through the DCC. However, the DCC-connected machines cannot communicate with the LAN-connected machines, and the LAN-connected machines cannot communicate with the DCC-connected machines. A CTC node using the LAN

to reach the firewalling node can use the proxy capability to manage the unreachable, DCC-connected nodes. CTC connected to a DCC-connected node can only manage other DCC-connected nodes and the firewall itself.

Step 3   Click **Apply**.

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

Changing the network configuration causes both ONS 15454 SDH TCC-I cards to reboot, one at a time.

✎
Note   CTC software does not monitor for the presence or absence of FMECs unless the TCC-I card(s) is active/standby. During transitional states such as power-up or TCC-I reset, CTC ignores the FMEC inventory displayed in node view.

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

Purpose	You can change the ONS 15454 SDH IP address, subnet mask, and default router address using the Slot, Status, and Port buttons on the front panel LCD.
Prerequisite Procedures	• The IP address and subnet mask to assign to the node
	• The IP address of the default router
	• The IP address of the DHCP server (if DHCP is used)
Onsite/Remote	Onsite or remote

Step 1   On the ONS 15454 SDH front panel, repeatedly press the **Slot** button until Node appears on the LCD.

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

Step 2   Repeatedly press the **Port** button until the following displays:

• To change the node IP address, "Status=IpAddress" (Figure 3-3)

• To change the node network mask, "Status=Net Mask"

• To change the default router IP address, "Status=Default Rtr"

Figure 3-3   Selecting the IP address option
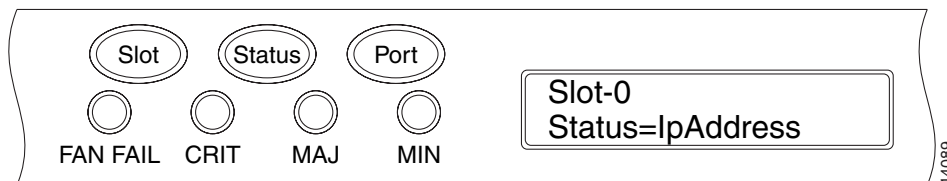
Step 3   Press the **Status** button to display the node IP address (Figure 3-4 on page 3-8), the node subnet mask length, or the default router IP address.

Figure 3-4   Changing the IP address

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

172.020.214.107
<Next   Done   Mod>

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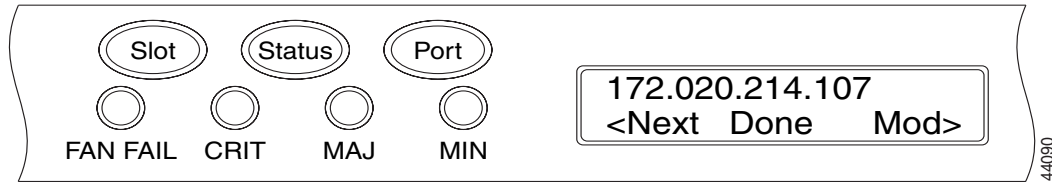
Step 4   Push the **Slot** button to move to the IP address or subnet mask digit you need to change. The selected digit flashes.

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 3-5).

Figure 3-5   Selecting the save configuration option

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

Slot-0
Status=Save Cfg.

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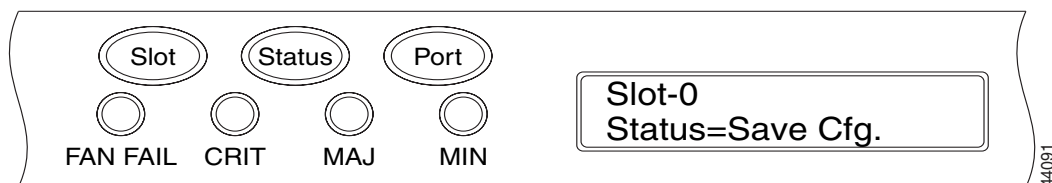
Step 8   Press the **Status** button to select the Save Configuration option.

A Save and REBOOT message appears (Figure 3-6).

Figure 3-6   Saving and rebooting the TCC-I

Slot   Status   Port

FAN FAIL   CRIT   MAJ   MIN

Save and REBOOT?
<Apply   Revert>

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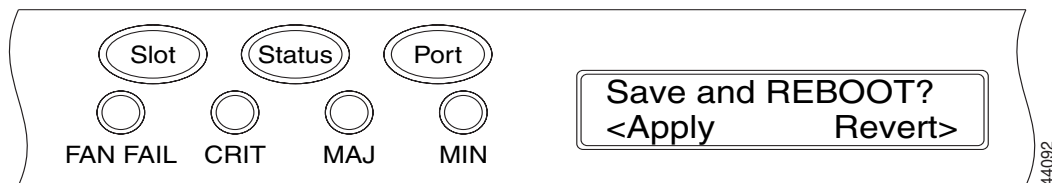
Step 9   Press the **Slot** button to save the new IP address configuration. (Or press **Port** to cancel the configuration.)

Saving the new configuration causes the TCC-I 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-I reboot is complete.

Note   CTC software does not monitor for the presence or absence of FMECs unless the TCC-I card(s) is active/standby. During transitional states such as power-up or TCC-I reset, CTC ignores the FMEC inventory displayed in node view.

3.4 Creating Users and Setting Security

Use the CISCO15 user, provided with each ONS 15454 SDH, to set up other ONS 15454 SDH users. You can add up to 500 users to one ONS 15454 SDH. Each ONS 15454 SDH 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 SDH 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.

Note   The CISCO15 superuser can be deleted if you have at least one other superuser defined. When CISCO15 is deleted, all new users must use passwords unless the database is deleted.

Each ONS 15454 SDH 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 3-3.

Table 3-3   ONS 15454 SDH User Idle Times

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

Table 3-4 shows the actions that each user can perform in node view. In the following tables, Yes means the user can use the specified tab or screen. Table cells with dashes (—) mean the user cannot use the specified tab.

Table 3-4   ONS 15454 SDH Security Levels—Node View

CTC Tab	Subtab	Actions	Retrieve	Maint.	Provision.	Super-user
Alarms	—	Synchronize alarms	Yes	Yes	Yes	Yes
		Filter alarms	Yes	Yes	Yes	Yes
		Delete cleared alarms	Yes	Yes	Yes	Yes
Conditions	—	Retrieve conditions	Yes	Yes	Yes	Yes
		Filter	Yes	Yes	Yes	Yes
History	Session	Filter	Yes	Yes	Yes	Yes
	Node	Retrieve and filter alarms and events	Yes	Yes	Yes	Yes

Table 3-4   ONS 15454 SDH Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maint.	Provision.	Super-user
Circuits	—	Create, delete, edit, or filter circuits	No	No	Yes	Yes
		Search for circuits	Yes	Yes	Yes	Yes
Provisioning	General	Edit	No	No	Yes	Yes
	Ether Bridge	Spanning Trees: Edit	No	No	Yes	Yes
		Thresholds: Create or delete	No	No	Yes	Yes
	Network	General: Edit	No	No	No	Yes
		Static Routing: Create, edit, or delete	No	No	Yes	Yes
		OSPF: Edit	Edit area ID	Edit area ID	Yes	Yes
		Routing Information Protocol (RIP): Edit	No	No	Yes	Yes
	Protection	Create, delete, or edit	No	No	Yes	Yes
		Browse groups	Yes	Yes	Yes	Yes
	MS-SPRing	All (MS-SPRing), view ring map, and squelch table	No	Partial view	Partial edit	Yes
	Security	Users: Create or delete	No	No	No	Yes
		Users: Change password	Same user	Same user	Same user	All users
		Legal disclaimer: HTML/Preview	View only	View only	View only	Yes
	SNMP	Create, delete, or edit	No	No	No	Yes
		Browse trap destinations	Yes	Yes	Yes	Yes
	SDH DCC	Create, delete, or edit	No	No	No	Yes
		View SDCC terminations	Yes	Yes	Yes	Yes
	Timing	Edit	No	Partial edit	Yes	Yes
	Alarm Behavior	Edit	No	No	Yes	Yes
	Defaults Editor	Import or export	No	Export only	Export only	Yes
	UCP	Node, neighbor, IPCC, interface, circuit	No	No	Yes	Yes
Inventory	—	Delete card	No	No	Yes	Yes
		Reset card	No	Yes	Yes	Yes
		View equipment information	Yes	Yes	Yes	Yes

Table 3-4   ONS 15454 SDH Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maint.	Provision.	Super-user
Maintenance	Database	Backup or restore	No	No	No	Yes
	Ether Bridge	Spanning tree retrieve	Yes	Yes	Yes	Yes
		Spanning tree clear/clear all	No	Yes	Yes	Yes
		MAC table retrieve	Yes	Yes	Yes	Yes
		MAC table clear/clear all	No	Yes	Yes	Yes
		Trunk utilization refresh	Yes	Yes	Yes	Yes
	Protection	Switch/lockout operations	View only	View only	Yes	Yes
	MS-SPRing	MS-SPRing maintenance	No	Yes	Yes	Yes
	Software	Download/activate/revert	No	No	No	Yes
	XC Cards	Switch/lock/unlock	No	Yes	Yes	Yes
	Overhead XConnect	View port, circuit, and circuit type	No	Yes	Yes	Yes
	Diagnostic	Retrieve diagnostics file	No	No	No	Yes
		Lamp test	No	Yes	Yes	Yes
	Timing	Edit	No	Yes	Yes	Yes
	Audit	Retrieve audit trail	Yes	Yes	Yes	Yes
	Routing Table	Refresh	Yes	Yes	Yes	Yes
	RIP Routing Table	Refresh	Yes	Yes	Yes	Yes

Procedure: Set Up Passwords from Network View

You can perform ONS 15454 SDH user management tasks from network or node view. If you perform user management tasks in node view, you must add the same user name and password to each node the user will access. See the "Set Up Passwords from Node View" procedure on page 3-13 for more information.

Purpose	Create new users with security settings from network view. In network view, you can add, edit, or delete users from multiple nodes at one time.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   In network view, select the **Provisioning > Security** tabs (Figure 3-7 on page 3-12).

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

Figure 3-7   Creating new users from the network view

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

- Name—Type the user name.

- Password—Type the user password. The password must contain alphanumeric characters, where at least one character is numerical (0-9) and at least one special character is used (+, #,%), for example, testpass+12. The password cannot contain the associated user ID. For example, if your user ID is maintenance, the password cannot be maintenance12+.

> **Note**   For TL1 compliance, the password must be a minimum of six and a maximum of ten alphanumeric characters, where at least one character is numerical (0-9) and at least one special character is used (+, #,%), for example, ILM+12. (TL1 is not available in SDH Software R3.4 and earlier.)

- Confirm Password—Type the password again to confirm it.

- Security Level—Select the user's security level:

  - Retrieve users can retrieve and view CTC information but cannot set or modify parameters.

  - Maintenance users can access only the ONS 15454 SDH 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.

Step 4   In the Select applicable nodes list box, deselect any nodes where you do not want to add the user. (All network nodes are selected by default.)

Step 5   Click **OK**.

> **Note** New users can also be created from node view. If you add a user in node view, you can only add, edit, or delete users from that node (Figure 3-8).

Procedure: Set Up Passwords from Node View

> **Note** This procedure sets up one user and password for one node. You must repeat this procedure for every node a user needs to open. If you add a user in network view, you can assign a single user to multiple nodes by clicking a check box. See the "Set Up Passwords from Network View" procedure on page 3-11 for more information.

Purpose	Use this procedure to create new users, assign passwords, and set security levels one node at a time.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   In node view, select the **Provisioning** > **Security > User** tabs (Figure 3-8).

Step 2   On the User tab, click **Create**.

Figure 3-8   Creating new users from the node view

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

- Name—Type the user name.

- Password—Type the user password. The password must contain alphanumeric characters, where at least one character is numerical (0-9) and at least one special character is used (+, #,%), for example, testpass+12. The password cannot contain the associated user ID. For example, if your user ID is maintenance, the password cannot be maintenance12+.

> **Note** For TL1 compliance, the password must be a minimum of six and a maximum of ten alphanumeric characters, where at least one character is numerical (0-9) and at least one special character is used (+, #,%), for example, ILM+12. (TL1 is not available in SDH Software R3.4 and earlier.)

- Confirm Password—Type the password again to confirm it.
- Security Level—Select the user's security level:
    - Retrieve users can retrieve and view CTC information but cannot set or modify parameters.
    - Maintenance users can access only the ONS 15454 SDH 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.

Step 4   Click **OK**.

Procedure: Change a User's Security Settings

Purpose	Change a user's security settings.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
	"Set Up Passwords from Network View" section on page 3-11
Onsite/Remote	Onsite or remote

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

Step 2   Click a name in the list of users.

Figure 3-9   Changing a user's security settings from the network view
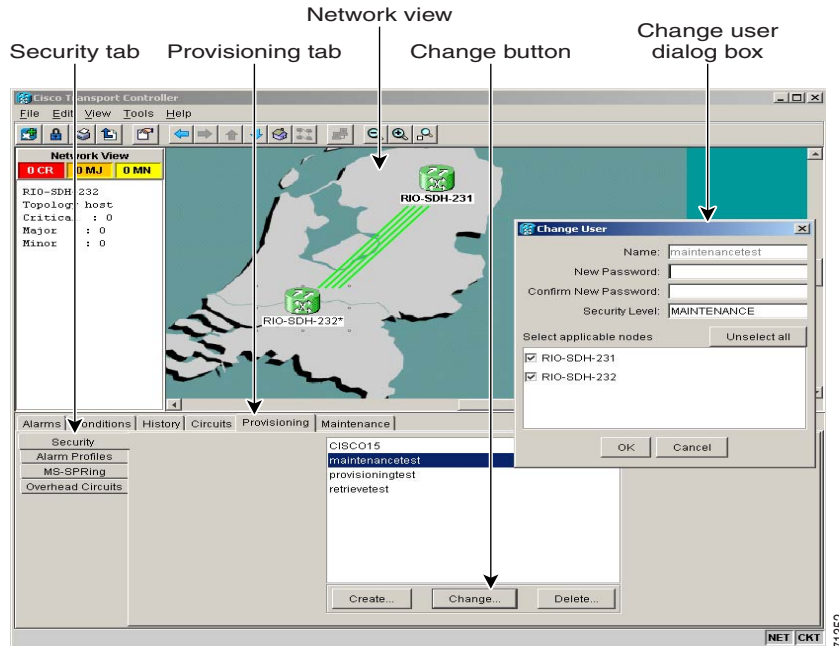
Step 3   In the Selected User dialog box, edit the user information: name, password, password confirmation, and/or security level. (A superuser does not need to enter an old password. Other users must enter their old password when changing their own passwords.)

Step 4   If you do not want the user changes to apply to all network nodes, deselect the nodes that you do not want to change 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.

Note   User security settings can also be changed from node view (Figure 3-10 on page 3-16).

Figure 3-10   Changing a user's security settings from the node view
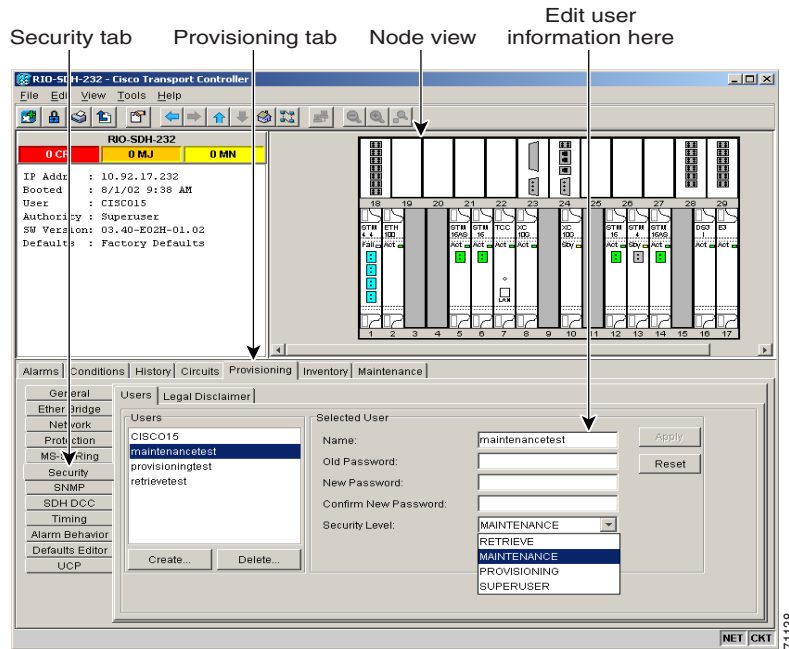
Procedure: Delete a User's Security Settings

Purpose	Delete a user's security settings.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
	"Set Up Passwords from Network View" section on page 3-11
Onsite/Remote	Onsite or remote

Step 1   In network view, select the **Provisioning > Security** tabs (Figure 3-11).

Step 2   Click **Delete**.

Figure 3-11   Deleting a user from the network view
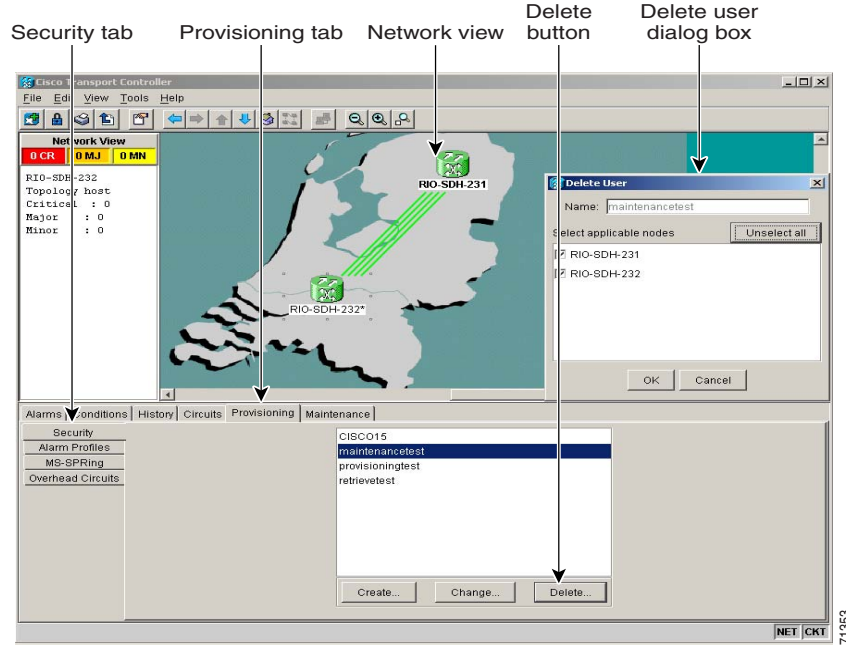
Step 3   In the Delete User dialog box, enter the name of the user you want to delete.

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**.

> **Note**   User security settings can also be deleted from node view (Figure 3-12 on page 3-18).

Figure 3-12   Deleting a user from the node view
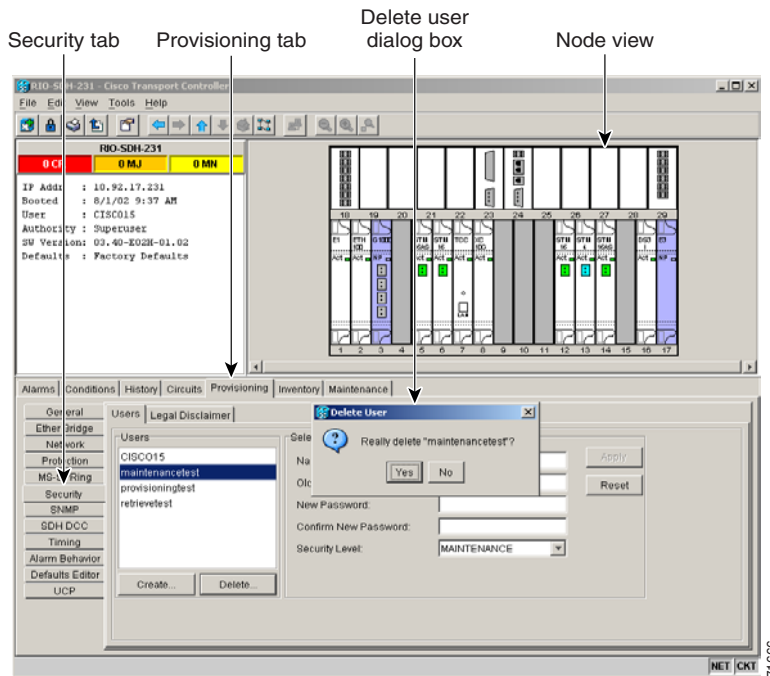
3.5 Setting Up ONS 15454 SDH Timing

SDH timing parameters must be set for each ONS 15454 SDH.

3.5.1 Timing Sources and Modes

Each ONS 15454 SDH independently accepts its timing reference from one of three sources:

- The Timing A and Timing B connectors on the MIC-C/T/P FMEC in Slot 24.

Note   CTC refers to Timing A and Timing B as BITS (building integrated timing supply) 1 and BITS 2.

- An STM-N card installed in the ONS 15454 SDH. The STM-N card is connected to a node that receives timing through a BITS source.
- The internal ST3 clock on the TCC-I card.

You can set ONS 15454 SDH timing to one of three modes: external, line, or mixed. If timing is coming from the MIC-C/T/P FMEC timing connector, set ONS 15454 SDH timing to external. If the timing comes from an STM-N card, set the timing to line.

Note   The line timing mode is not available for 64 KHz BITS facilities.

In typical ONS 15454 SDH networks:

- One node is set to external. The external node derives its timing from a MIC-C/T/P FMEC timing connector. The MIC-C/T/P FMEC, in turn, derives its timing from a Primary Reference Source (PRS) such as a Stratum 1 clock or global positioning satellite (GPS) signal.

- The other nodes are set to line. The line nodes derive timing from the externally timed node through the STM-N trunk cards.

You can set three timing references for each ONS 15454 SDH. The first two references are typically two FMEC-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 SDH TCC-I card. This clock is a Stratum 3 (ST3). If an ONS 15454 SDH becomes isolated, timing is maintained at the ST3 level.

⚠

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

3.5.2 Network Timing Example

Figure 3-13 on page 3-20 shows an ONS 15454 SDH network timing setup example. Node 1 is set to external timing. Two timing references are set to BITS. These are Stratum 1 timing sources connected to the MIC-C/T/P FMEC. The third reference is set to internal clock. The Timing A and Timing B out connectors on the MIC-C/T/P FMEC of Node 3 are used to provide timing to outside equipment.

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 MIC-C/T/P FMEC. Reference 1 is set to the trunk card closest to the timing source. At Node 2, Reference 1 is 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 3-13   NS 15454 SDH timing example
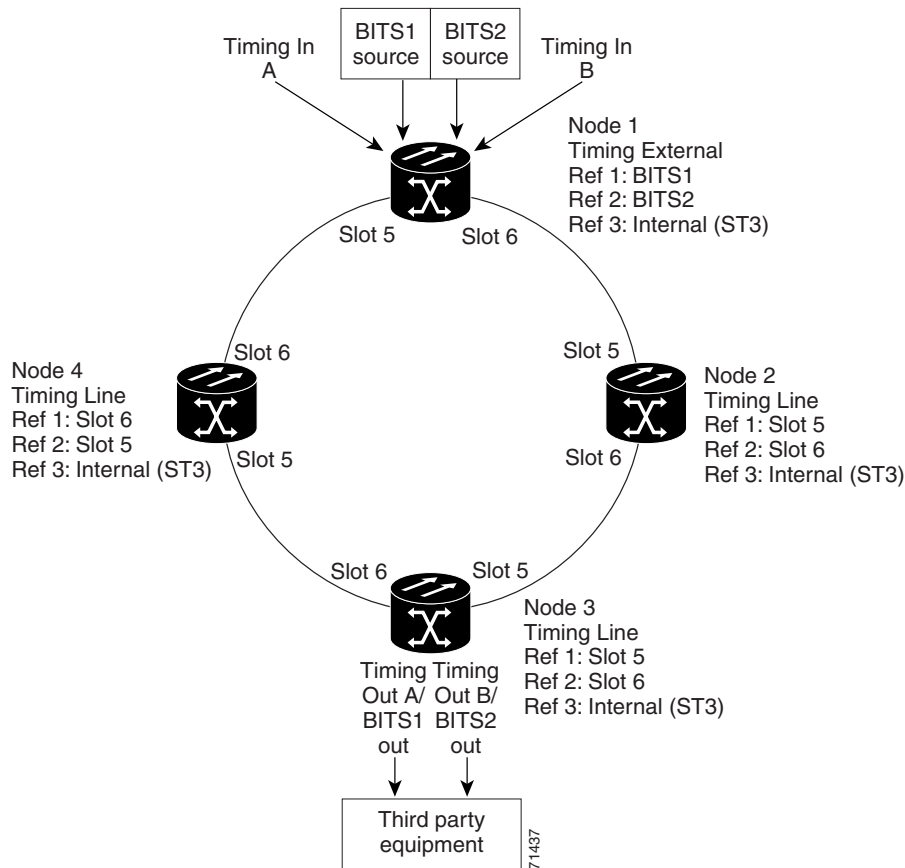
3.5.3 Synchronization Status Message

Synchronization Status Message (SSM) communicates information about the quality of the timing source. The SSM supported in SDH is G.811, STU, G812T, G812L, SETS, DUS (ordered from high quality to low quality). SSM messages are carried on bits 5 to 8 of SDH overhead byte S1. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

Note   The message set in the S_{an1} to S_{an4} column is a copy of the set defined in SDH bits 5 to 8 of byte S1.

Table 3-5   Assignment of Bit Patterns as Shown in ITU G.704

Quality Level (QL)	S_{an1}, S_{an2}, S_{an3}, or S_{an4} S1 bits b5-b8	SDH Synchronization QL Description
0	0000	Quality unknown (existing synchronization network)
1	0001	Reserved
2	0010	Rec. G.811
3	0011	Reserved

Table 3-5   Assignment of Bit Patterns as Shown in ITU G.704 (continued)

Quality Level (QL)	S_{an1}, S_{an2}, S_{an3}, or S_{an4} S1 bits b5-b8	SDH Synchronization QL Description
4	0100	Synchronization Supply Unit A (SSU-A)
5	0101	Reserved
6	0110	Reserved
7	0111	Reserved
8	1000	Synchronization Supply Unit B (SSU-B)
9	1001	Reserved
10	1010	Reserved
11	1011	Synchronous Equipment Timing Source (SETS)
12	1100	Reserved
13	1101	Reserved
14	1110	Reserved
15	1111	Do not use for synchronization

Procedure: Set Up External, Line, or Mixed Timing for the ONS 15454 SDH

Note   CTC refers to Timing A and Timing B as BITS 1 and BITS 2. The MIC-C/T/P FMEC connector is labeled as Timing A and Timing B.

Purpose	Use this procedure to set external, line, or mixed timing for your ONS 15454 SDH nodes. To set up internal timing, see the "Set Up Internal Timing for the ONS 15454 SDH" procedure on page 3-24.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
	"Add the Node Name, Contact, Location, Date, and Time" section on page 3-3
	"Set Up Network Information" section on page 3-5
Onsite/Remote	Onsite or remote

Step 1   From the CTC node view, click the **Provisioning > Timing** tabs (Figure 3-14 on page 3-22).

Figure 3-14   Setting Up external, line, or mixed ONS 15454 SDH timing
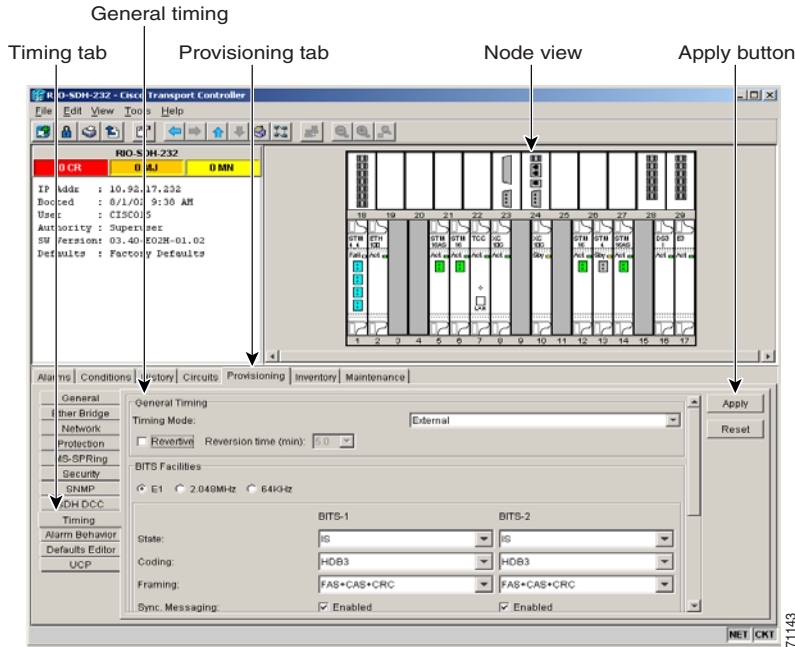
Step 2   In the General Timing section, complete the following information:

- Timing Mode—Choose **External** if the ONS 15454 SDH derives its timing from a MIC-C/T/P FMEC; choose **Line** if timing is derived from an STM-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references. (Because mixed timing may cause timing loops, Cisco does not recommend its use. Use this mode with care.)

- Revertive—If this check box is selected, the ONS 15454 SDH 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 SDH will wait before reverting 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.

- E1, 2.048 MHz, 64 KHz—Choose **E1**, **2.048 MHz**, or **64 KHz** depending on the signal supported in your market. For example, 64 KHz is used in Japan. E1, 2.048 MHz, and 64 KHz are physical signal modes used to transmit the external clock (from a GPS, for example) to BITS.

- 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—Choose the coding used by your BITS reference, either **HDB3** or **AMI**. If you selected 2.048 MHz, or 64 KHz, the coding option is disabled.

- Framing—Choose the framing used by your BITS reference, either **unframed**, **FAS**, **FAS + CAS**, **FAS + CRC**, or **FAS + CAS + CRC**. If you selected 2.048 MHz or 64 KHz, the framing option is disabled.

- Sync Messaging—Select the check box to enable SSM. SSM is used to deliver clock quality. The SSM supported in SDH is G811, STU, G812T, G812L, SETS, DUS (ordered from high quality to low quality). If you selected 2.048 MHz or 64 KHz, the SSM option is disabled.

- AIS Threshold—Sets the quality level at which a node sends an Alarm Indication Signal (AIS) from the BITS 1 Out and BITS 2 Out FMEC connectors. When a node times at or below the AIS threshold quality, an AIS is sent. (The AIS threshold is used when Sync. Messaging is disabled or framing is set to unframed, FAS, or FAS + CAS.)

- LBO—Choose a BITS cable length. Line build out (LBO) relates to the BITS cable length.

- Sa bit—Choose one of 5 Sa bits (**Sa4**, **Sa5**, **Sa6**, **Sa7**, or **Sa8**). The Sa bit transmits the SSM message. If you selected 2.048 MHz or 64 KHz, the Sa bit option is disabled.

Step 4   Under Reference Lists, complete the information (Figure 3-15 on page 3-24):

> **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 attached to the node's MIC-C/T/P FMEC Timing A and Timing B Out connectors. If you attach equipment to the Timing A Out or Timing B Out connector, you normally attach it to a node with line mode because equipment near the External timing reference can be directly wired to the reference.

- NE Reference—Allows you to define three timing references (Ref 1, Ref 2, Ref 3). The node uses Reference 1 unless a failure occurs to that reference, in which case, the node uses Reference 2. If Reference 2 fails, the node uses Reference 3, which is typically set to Internal Clock. The internal clock is the Stratum 3 clock provided on the TCC-I. The options displayed depend on the Timing Mode setting.

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

  - Timing Mode set to Line—Your 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, select 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 connected to the Timing A Out or Timing B Out FMEC connector. Normally, Timing Out is used with line nodes, so the options displayed are the working optical cards. Timing A Out and Timing B Out are enabled as soon as BITS-1 and BITS-2 facilities are placed in service.

Figure 3-15   Reference list in the ONS 15454 SDH Timing tab
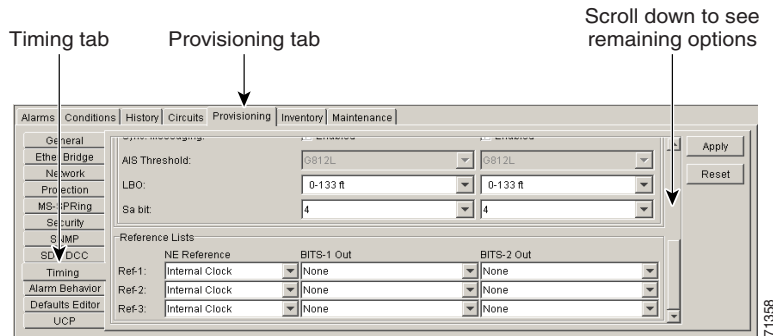
Step 5 Click **Apply**.

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

Procedure: Set Up Internal Timing for the ONS 15454 SDH

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

⬛ **Note** CTC refers to Timing A and Timing B as BITS 1 and BITS 2. The MIC-C/T/P FMEC connector is labeled as Timing A and Timing B.

Purpose	Use this procedure to set internal timing for your ONS 15454 SDH nodes. To set up external, line, or mixed timing, see the "Set Up External, Line, or Mixed Timing for the ONS 15454 SDH" procedure on page 3-21.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
	"Add the Node Name, Contact, Location, Date, and Time" section on page 3-3
	"Set Up Network Information" section on page 3-5
Onsite/Remote	Onsite or remote

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

Step 2 From the CTC node view, click the **Provisioning > Timing** tabs (Figure 3-16).

Figure 3-16   Setting up internal ONS 15454 SDH timing
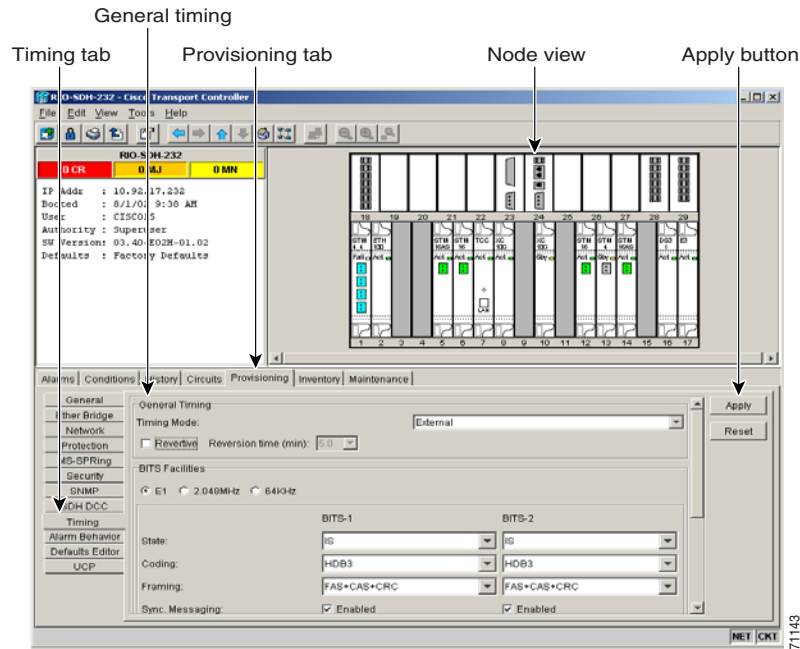
Step 3   In the General Timing section, enter the following:

- Timing Mode—Choose **External**.
- Revertive—Not relevant for internal timing; the default setting (checked) is sufficient.
- Revertive Time—Not relevant for internal timing; the default setting (5 minutes) is sufficient.

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

- E1, 2.048 MHz, 64 KHz—Choose **E1**, **2.048 MHz**, or **64 KHz** depending on the signal supported in your market. For example, 64 KHz is used in Japan. E1, 2.048 MHz, and 64 KHz are physical signal modes used to transmit the external clock (from a GPS for example) to BITS.
- State—Set BITS 1 and BITS 2 to **OOS** (Out of Service).
- Coding—Not relevant for internal timing; the default (HDB3) is sufficient.
- Framing—Not relevant for internal timing; the default (FAS + CAS + CRC) is sufficient.
- Sync Messaging—The box is checked automatically. SSM is used to deliver clock quality. The SSM supported in SDH is G811, STU, G812T, G812L, SETS, DUS (ordered from high quality to low quality). If you selected 2.048 MHz, or 64 KHz, the SSM option is disabled.
- AIS Threshold—Not relevant for internal timing.
- LBO—Not relevant for internal timing; line build out (LBO) relates to the BITS cable length.
- Sa bit—Not relevant for internal timing; the Sa bit is used to transmit the SSM message.

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 that was set up in Step 1 to Step 6.

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

Step 9   In the General Timing section, enter the following:

- Timing Mode—Set to **Line**.

- Revertive—Not relevant for internal timing; the default setting (checked) is sufficient.

- Revertive Time—The default setting (5 minutes) is sufficient.

Step 10   In the Reference Lists section, enter the following:

- NE Reference

    – Ref-1—Use the pull-down menu to choose the STM-N trunk card with the closest connection to the node in Step 3.

    – Ref-2—Use the pull-down menu to choose the STM-N trunk card with the next closest connection to the node in Step 3.

    – Ref-3—Use the pull-down menu to choose **Internal Clock**.

Step 11   Click **Apply**.

Step 12   Repeat Step 7 to Step 11 at each node that will be timed by the node serving as the timing source.

3.6 Creating Card Protection Groups

The ONS 15454 SDH provides several card protection methods. When you set up protection for ONS 15454 SDH 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 3-6 shows the protection types that can be set up for ONS 15454 SDH cards.

Table 3-6   Protection Types

Type	Cards	Description
1:1	E1-N-14 E3-12 DS3i-N-12	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. Use the slot that is next to the protect slot, toward the center of the shelf. 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	E1-N-14 DS3i-N-12	Assigns one protect card for several working cards. The maximum is 1:5. Protect cards (E1-N-14, DS3i-N-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 E1-N-14 can only protect E1-N-14 cards. If a failure clears, traffic reverts to the working card after the reversion time has elapsed.

Table 3-6   Protection Types (continued)

Type	Cards	Description
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 STM-1 card can only be protected by Port 1 of another STM-1 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 SDH. Unprotected is the default protection type.

Procedure: Create Protection Groups

Purpose	Use this procedure to create card protection groups for the ONS 15454 SDH. Unprotected cards can cause signal loss if a card fails or incurs a signal error.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
	"Add the Node Name, Contact, Location, Date, and Time" section on page 3-3
	"Set Up Network Information" section on page 3-5
	"Setting Up ONS 15454 SDH Timing" section on page 3-18
Onsite/Remote	Onsite or remote

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

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

Figure 3-17   Creating card protection groups
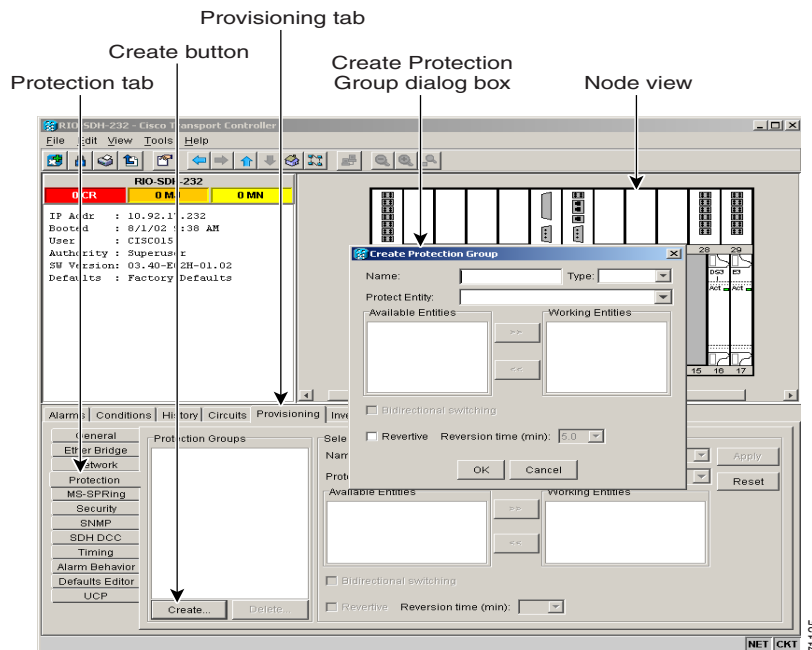
Step 3   In the Create Protection Group dialog box, enter the following:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric characters.

- Type—Choose the protection type (1:1, 1:N, or 1+1) from the pull-down menu. 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 E1-N-14 and DS3i-N-12 cards are displayed.

- Protect Card or Port—Choose the protect card (if you are using 1:1 or 1:N) or protect port (if you are using 1+1) from the pull-down menu.

Based on these selections, a list of available working cards or ports is displayed under Available Cards or Available Ports. Figure 3-18 shows a 1:1 protection group.

Figure 3-18   Creating a 1:1 protection group
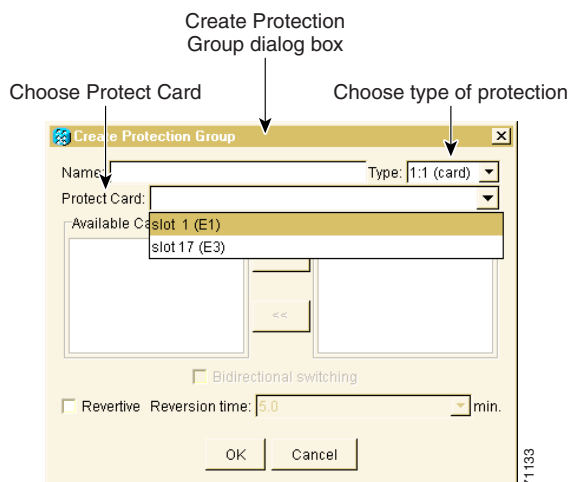
Step 4 From the Available Cards or Available Ports list, choose the card or port that you want to be the working card or port (the card(s) or port(s) that will be protected by the card or port selected in Protect Cards or Protect Ports). Click the top arrow button to move each card or port to the Working Cards or Working Ports list.

Step 5 Complete the remaining fields:

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

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

- Reversion time—If Revertive is checked, enter the amount of time that will elapse after a failure is corrected before the ONS 15454 SDH will revert to the working card or port.

Step 6 Click **OK**.

⚠️

Caution Before running traffic on a protected card within a protection group, enable the ports of all protection group cards. See the "Put Ports In or Out of Service" procedure on page 5-56.

✎

Note To convert protection groups, see the "Converting E1 and DS3i Cards From 1:1 to 1:N Protection" section on page 7-18.

Procedure: Edit Protection Groups

Purpose	Use this procedure to make changes to your card protection scheme.
Prerequisite Procedures	"Create Protection Groups" section on page 3-27
Onsite/Remote	Onsite or remote

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

Step 2 In the Protection Groups section, choose a protection group.

Step 3 In the Selected Group section, edit the fields as appropriate:

- Name—Type a name for the protection group. The name can have up to 32 alphanumeric characters.

- Type—Choose the protection type (1:1, 1:N, or 1+1) from the pull-down menu. The protection selected determines the cards that are available to serve as protect and working cards. For example, if you choose 1:1 protection, only E1, E3, and DS3i cards are displayed.

- Protect Card or Port—Choose the protect card (if you are using 1:1 or 1:N) or protect port (if you are using 1+1) from the pull-down menu.

Based on these selections, a list of available working cards or ports is displayed under Available Cards or Available Ports.

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 (that is, 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 or 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 SDH reverts traffic to the working card or port after a failure has been corrected for the amount of time entered in the Reversion time field.

- Reversion time—If Revertive is checked, enter the amount of time following a failure correction that the ONS 15454 SDH will revert to the working card or port.

Step 6 Click **Apply**.

Procedure: Delete Protection Groups

Purpose	Use this procedure to delete a card protection group.
Prerequisite Procedures	"Create Protection Groups" section on page 3-27
Onsite/Remote	Onsite or remote

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 the protect card 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 the protect card is standby, 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**.

3.7 Setting Network Element Defaults

This section describes the factory-configured (default) network element (NE) settings for the Cisco ONS 15454 SDH. It includes descriptions of card default settings and node default settings and provides procedures for importing, exporting and editing the settings. Ethernet card settings are not included in the factory-configured settings.

The NE defaults are pre-installed on each ONS 15454 SDH (on the TCC-I cards). The NE defaults include card-level and node-level defaults.

If you use the Defaults Editor or import a new defaults file, that is, if defaults are changed, the changes apply only to cards installed subsequently (after the defaults change) or to slots pre-provisioned subsequently. A new defaults file will not take effect for cards already installed when the change takes place or for slots already pre-provisioned when the change takes place.

Changes made manually to the node-level default settings (either when you initially turn up a node or change node settings later) override the default settings. If you change the default settings, using either the Defaults Editor or by importing a new defaults file, the new defaults take effect immediately.

Use the following procedures if you need to edit, import, or export NE defaults.

Procedure: Edit Network Element Defaults

Purpose	This procedure edits the NE defaults using the NE Defaults Editor. The new defaults can either be applied only to the node on which they are edited or exported to a file and imported for use on other nodes.
Tools/Equipment	None
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Required/As Needed	As needed

Step 1   After logging into the node, click the **Provisioning>Defaults Editor** tabs.

Step 2   Under Defaults Selector, choose either a card (if editing card-level defaults) or NODE (if editing node-level defaults). Clicking on NODE lists all available NE defaults (both node- and card-level) under Property Name.

Step 3   Locate a default you want to change under Property Name.

Step 4   Click in the **Default Value** column for the default property you are changing and either choose a value from the drop-down menu (available for some node-level settings only), or type in the desired new value.

> **Note**   Clicking **Reset** before clicking **Apply** will return all values to their original setting.

Step 5   Click **Apply** (click in the **Property Name** column to activate the Apply button if it is unavailable).

Step 6   A dialog box opens telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

> **Note**   Changes to node settings take effect upon clicking **Apply**. Changes to the IIOP Listener Port setting reboots the TCC-I. Changes made to card settings using the Defaults Editor do not change the settings for cards that are currently installed. Card settings must be manually changed by opening the cards.

Procedure: Import Network Element Defaults

Purpose	This procedure imports the NE defaults using the NE Defaults Editor. The defaults can either be imported from the CTC software CD (factory defaults) or from a customized file exported and saved from a node.
Tools/Equipment	None
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Required/As Needed	As needed

Step 1 After logging into the node, click the **Provisioning>Defaults Editor** tabs.

Step 2 Click **Import**.

Step 3 Click **Browse** and browse to the file you are importing if the correct file name and location of the desired file do not appear in the Import Defaults from File dialog box.

Step 4 When the correct file name and location appear in the dialog box, click **OK**.

A pencil icon will appear next to any default value that will be changed as a result of importing the new defaults file.

Step 5 Click **Apply**.

Step 6 A dialog box opens telling you that applying defaults for node level attributes overrides current provisioning and asks if you want to continue. Click **Yes**.

Note Changes to node settings take effect upon clicking **Apply**. Changes to the IIOP Listener Port setting reboots the TCC-I. Changes made to card settings using the Defaults Editor do not change the settings for cards that are currently installed. Card settings must be manually changed by opening the cards.

Procedure: Export Network Element Defaults

Purpose	This procedure exports the NE defaults using the NE Defaults Editor. The exported defaults can be imported to other nodes.
Tools/Equipment	None
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Required/As Needed	As needed

Step 1 After logging into the node, click the **Provisioning>Defaults Editor** tabs.

Step 2 Click **Export**.

Step 3 Click **Browse** and browse to the location where you want to export the file if it does not appear in the Export Defaults to File dialog box.

Step 4 Change the file name to something easy to remember (the file name has no extension).

Step 5 Click **OK**.

3.7.1 Card Default Settings

The tables in this section list the default settings for each card. Cisco provides the following settings preprovisioned for the ONS 15454 optical and electrical cards:

- Auto In-Service (AINS) Soak Time (E1, E3, DS3I, and STM-N cards) is the length of time that elapses between an AINS port receiving a valid signal and when it automatically changes to in-service status.

- Line Type (E1 and DS3I cards) defines the type of framing used.

- Loopback (DS3I) defines whether or not far end loopbacks are inhibited for the DS3I card.

- Line Length (DS3I) defines the distance (in feet) from the backplane connection to the next termination point.

- Port State (E1, E3, DS3I, and STM-N cards) sets the port to one of the four available states (IS, OOS, OOS_MT, or OOS_AINS), depending on whether you need ports in or out of service.

- PM Threshold Settings (E1, E3, DS3I, and STM-N cards) set the performance monitoring parameters for gathering performance data and detecting problems early.

Note   For more information about performance monitoring, see Chapter 8, "SDH Performance Monitoring."

Table 3-7 lists the E1 card default settings.

Table 3-7   E1 Card Default Settings

Property Name	Default Value
E1.config.AINSSoakTime	08:00 (hours:minutes)
E1.config.LineType	E1 MF
E1.config.State	OOS
E1.pmthresholds.line.nearend.15min.CV	17790 (BPV count)
E1.pmthresholds.line.nearend.15min.ES	65 (seconds)
E1.pmthresholds.line.nearend.15min.SES	10 (seconds)
E1.pmthresholds.line.nearend.1day.CV	17790 (BPV count)
E1.pmthresholds.line.nearend.1day.ES	648 (seconds)
E1.pmthresholds.line.nearend.1day.SES	100 (seconds)
E1.pmthresholds.path.farend.15min.BBE	0 (count)
E1.pmthresholds.path.farend.15min.EB	0 (count)
E1.pmthresholds.path.farend.15min.ES	0 (seconds)
E1.pmthresholds.path.farend.15min.SES	0 (seconds)
E1.pmthresholds.path.farend.15min.UAS	0 (seconds)
E1.pmthresholds.path.farend.1day.BBE	0 (count)
E1.pmthresholds.path.farend.1day.EB	0 (count)
E1.pmthresholds.path.farend.1day.ES	0 (seconds)
E1.pmthresholds.path.farend.1day.SES	0 (seconds)

Table 3-7   E1 Card Default Settings (continued)

Property Name	Default Value
E1.pmthresholds.path.farend.1day.UAS	0 (seconds)
E1.pmthresholds.path.nearend.15min.BBE	9 (count)
E1.pmthresholds.path.nearend.15min.EB	9 (count)
E1.pmthresholds.path.nearend.15min.ES	65 (seconds)
E1.pmthresholds.path.nearend.15min.SES	10 (seconds)
E1.pmthresholds.path.nearend.15min.UAS	10 (seconds)
E1.pmthresholds.path.nearend.1day.BBE	90 (count)
E1.pmthresholds.path.nearend.1day.EB	90 (count)
E1.pmthresholds.path.nearend.1day.ES	648 (seconds)
E1.pmthresholds.path.nearend.1day.SES	100 (seconds)
E1.pmthresholds.path.nearend.1day.UAS	10 (seconds)
E1.pmthresholds.vclo.farend.15min.BBE	15 (count)
E1.pmthresholds.vclo.farend.15min.EB	18 (count)
E1.pmthresholds.vclo.farend.15min.ES	65 (seconds)
E1.pmthresholds.vclo.farend.15min.SES	10 (seconds)
E1.pmthresholds.vclo.farend.15min.UAS	10 (seconds)
E1.pmthresholds.vclo.farend.1day.BBE	150 (count)
E1.pmthresholds.vclo.farend.1day.EB	180 (seconds)
E1.pmthresholds.vclo.farend.1day.ES	648 (seconds)
E1.pmthresholds.vclo.farend.1day.SES	100 (seconds)
E1.pmthresholds.vclo.farend.1day.UAS	10 (seconds)
E1.pmthresholds.vclo.nearend.15min.BBE	15 (count)
E1.pmthresholds.vclo.nearend.15min.EB	18 (count)
E1.pmthresholds.vclo.nearend.15min.ES	65 (seconds)
E1.pmthresholds.vclo.nearend.15min.SES	10 (seconds)
E1.pmthresholds.vclo.nearend.15min.UAS	10 (seconds)
E1.pmthresholds.vclo.nearend.1day.BBE	150 (count)
E1.pmthresholds.vclo.nearend.1day.EB	180 (count)
E1.pmthresholds.vclo.nearend.1day.ES	648 (seconds)
E1.pmthresholds.vclo.nearend.1day.SES	100 (seconds)
E1.pmthresholds.vclo.nearend.1day.UAS	10 (seconds)

Table 3-8 lists the E3 card default settings.

Table 3-8   E3 Card Default Settings

Property Name	Default Value
E3.config.AINSSoakTime	08:00 (hours:minutes)
E3.config.State	OOS
E3.pmthresholds.line.nearend.15min.CV	387 (BPV count)
E3.pmthresholds.line.nearend.15min.ES	25 (seconds)
E3.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
E3.pmthresholds.line.nearend.15min.SES	4 (seconds)
E3.pmthresholds.line.nearend.1day.CV	3865 (BPV count)
E3.pmthresholds.line.nearend.1day.ES	250 (seconds)
E3.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
E3.pmthresholds.line.nearend.1day.SES	40 (seconds)
E3.pmthresholds.path.nearend.15min.ES	20 (seconds)
E3.pmthresholds.path.nearend.15min.SES	3 (seconds)
E3.pmthresholds.path.nearend.15min.UAS	10 (seconds)
E3.pmthresholds.path.nearend.1day.ES	200 (seconds)
E3.pmthresholds.path.nearend.1day.SES	7 (seconds)
E3.pmthresholds.path.nearend.1day.UAS	10 (seconds)
E3.pmthresholds.vc4.farend.15min.BBE	25 (count)
E3.pmthresholds.vc4.farend.15min.EB	15 (count)
E3.pmthresholds.vc4.farend.15min.ES	12 (seconds)
E3.pmthresholds.vc4.farend.15min.SES	3 (seconds)
E3.pmthresholds.vc4.farend.15min.UAS	10 (seconds)
E3.pmthresholds.vc4.farend.1day.BBE	250 (count)
E3.pmthresholds.vc4.farend.1day.EB	125 (count)
E3.pmthresholds.vc4.farend.1day.ES	100 (seconds)
E3.pmthresholds.vc4.farend.1day.SES	7 (seconds)
E3.pmthresholds.vc4.farend.1day.UAS	10 (seconds)
E3.pmthresholds.vc4.nearend.15min.BBE	25 (count)
E3.pmthresholds.vc4.nearend.15min.EB	15 (count)
E3.pmthresholds.vc4.nearend.15min.ES	20 (seconds)
E3.pmthresholds.vc4.nearend.15min.SES	3 (seconds)
E3.pmthresholds.vc4.nearend.15min.UAS	10 (seconds)
E3.pmthresholds.vc4.nearend.1day.BBE	250 (count)
E3.pmthresholds.vc4.nearend.1day.EB	125 (count)
E3.pmthresholds.vc4.nearend.1day.ES	200 (seconds)
E3.pmthresholds.vc4.nearend.1day.SES	7 (seconds)

Table 3-8   E3 Card Default Settings (continued)

Property Name	Default Value
E3.pmthresholds.vc4.nearend.1day.UAS	10 (seconds)
E3.pmthresholds.vclo.farend.15min.BBE	15 (count)
E3.pmthresholds.vclo.farend.15min.EB	15 (count)
E3.pmthresholds.vclo.farend.15min.ES	12 (seconds)
E3.pmthresholds.vclo.farend.15min.SES	3 (seconds)
E3.pmthresholds.vclo.farend.15min.UAS	10 (seconds)
E3.pmthresholds.vclo.farend.1day.BBE	125 (count)
E3.pmthresholds.vclo.farend.1day.EB	125 (count)
E3.pmthresholds.vclo.farend.1day.ES	100 (seconds)
E3.pmthresholds.vclo.farend.1day.SES	7 (seconds)
E3.pmthresholds.vclo.farend.1day.UAS	10 (seconds)
E3.pmthresholds.vclo.nearend.15min.BBE	15 (count)
E3.pmthresholds.vclo.nearend.15min.EB	15 (count)
E3.pmthresholds.vclo.nearend.15min.ES	12 (seconds)
E3.pmthresholds.vclo.nearend.15min.SES	3 (seconds)
E3.pmthresholds.vclo.nearend.15min.UAS	10 (seconds)
E3.pmthresholds.vclo.nearend.1day.BBE	125 (count)
E3.pmthresholds.vclo.nearend.1day.EB	125 (count)
E3.pmthresholds.vclo.nearend.1day.ES	100 (seconds)
E3.pmthresholds.vclo.nearend.1day.SES	7 (seconds)
E3.pmthresholds.vclo.nearend.1day.UAS	10 (seconds)

Table 3-9 lists the DS3I card default settings

Table 3-9   DS3I Card Default Settings

Property Name	Default Value
DS3I.config.AINSSoakTime	08:00 (hours:minutes)
DS3I.config.FeInhibitLpbk	FALSE
DS3I.config.LineLength	0—225 (feet)
DS3I.config.LineType	CBIT
DS3I.config.State	OOS
DS3I.pmthresholds.cpbitpath.farend.15min.CV	382 (count)
DS3I.pmthresholds.cpbitpath.farend.15min.ES	25 (seconds)
DS3I.pmthresholds.cpbitpath.farend.15min.SAS	2 (seconds)
DS3I.pmthresholds.cpbitpath.farend.15min.SES	4 (seconds)
DS3I.pmthresholds.cpbitpath.farend.15min.UAS	10 (seconds)
DS3I.pmthresholds.cpbitpath.farend.1day.CV	3820 (count)

Table 3-9   DS3I Card Default Settings (continued)

Property Name	Default Value
DS3I.pmthresholds.cpbitpath.farend.1day.ES	250 (seconds)
DS3I.pmthresholds.cpbitpath.farend.1day.SAS	8 (seconds)
DS3I.pmthresholds.cpbitpath.farend.1day.SES	40 (seconds)
DS3I.pmthresholds.cpbitpath.farend.1day.UAS	10 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.15min.CV	382 (count)
DS3I.pmthresholds.cpbitpath.nearend.15min.ES	25 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.15min.SAS	2 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.15min.SES	4 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.15min.UAS	10 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.1day.CV	3820 (count)
DS3I.pmthresholds.cpbitpath.nearend.1day.ES	250 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.1day.SAS	8 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.1day.SES	40 (seconds)
DS3I.pmthresholds.cpbitpath.nearend.1day.UAS	10 (seconds)
DS3I.pmthresholds.line.nearend.15min.CV	387 (BPV count)
DS3I.pmthresholds.line.nearend.15min.ES	25 (seconds)
DS3I.pmthresholds.line.nearend.15min.LOSS	10 (seconds)
DS3I.pmthresholds.line.nearend.15min.SES	4 (seconds)
DS3I.pmthresholds.line.nearend.1day.CV	3865 (BPV count)
DS3I.pmthresholds.line.nearend.1day.ES	250 (seconds)
DS3I.pmthresholds.line.nearend.1day.LOSS	10 (seconds)
DS3I.pmthresholds.line.nearend.1day.SES	40 (seconds)
DS3I.pmthresholds.pbitpath.nearend.15min.AISS	10 (seconds)
DS3I.pmthresholds.pbitpath.nearend.15min.CV	25 (count)
DS3I.pmthresholds.pbitpath.nearend.15min.ES	20 (seconds)
DS3I.pmthresholds.pbitpath.nearend.15min.SAS	2 (seconds)
DS3I.pmthresholds.pbitpath.nearend.15min.SES	3 (seconds)
DS3I.pmthresholds.pbitpath.nearend.15min.UAS	10 (seconds)
DS3I.pmthresholds.pbitpath.nearend.1day.AISS	10 (seconds)
DS3I.pmthresholds.pbitpath.nearend.1day.CV	250 (count)
DS3I.pmthresholds.pbitpath.nearend.1day.ES	200 (seconds)
DS3I.pmthresholds.pbitpath.nearend.1day.SAS	8 (seconds)
DS3I.pmthresholds.pbitpath.nearend.1day.SES	7 (seconds)
DS3I.pmthresholds.pbitpath.nearend.1day.UAS	10 (seconds)
DS3I.pmthresholds.vc4.farend.15min.BBE	25 (count)
DS3I.pmthresholds.vc4.farend.15min.EB	15 (count)

Table 3-9   DS3I Card Default Settings (continued)

Property Name	Default Value
DS3I.pmthresholds.vc4.farend.15min.ES	12 (seconds)
DS3I.pmthresholds.vc4.farend.15min.SES	3 (seconds)
DS3I.pmthresholds.vc4.farend.15min.UAS	10 (seconds)
DS3I.pmthresholds.vc4.farend.1day.BBE	250 (count)
DS3I.pmthresholds.vc4.farend.1day.EB	125 (count)
DS3I.pmthresholds.vc4.farend.1day.ES	100 (seconds)
DS3I.pmthresholds.vc4.farend.1day.SES	7 (seconds)
DS3I.pmthresholds.vc4.farend.1day.UAS	10 (seconds)
DS3I.pmthresholds.vc4.nearend.15min.BBE	25 (count)
DS3I.pmthresholds.vc4.nearend.15min.EB	15 (count)
DS3I.pmthresholds.vc4.nearend.15min.ES	12 (seconds)
DS3I.pmthresholds.vc4.nearend.15min.SES	3 (seconds)
DS3I.pmthresholds.vc4.nearend.15min.UAS	10 (seconds)
DS3I.pmthresholds.vc4.nearend.1day.BBE	250 (count)
DS3I.pmthresholds.vc4.nearend.1day.EB	125 (count)
DS3I.pmthresholds.vc4.nearend.1day.ES	100 (seconds)
DS3I.pmthresholds.vc4.nearend.1day.SES	7 (seconds)
DS3I.pmthresholds.vc4.nearend.1day.UAS	10 (seconds)
DS3I.pmthresholds.vclo.farend.15min.BBE	15 (count)
DS3I.pmthresholds.vclo.farend.15min.EB	15 (count)
DS3I.pmthresholds.vclo.farend.15min.ES	12 (seconds)
DS3I.pmthresholds.vclo.farend.15min.SES	3 (seconds)
DS3I.pmthresholds.vclo.farend.15min.UAS	10 (seconds)
DS3I.pmthresholds.vclo.farend.1day.BBE	125 (count)
DS3I.pmthresholds.vclo.farend.1day.EB	125 (count)
DS3I.pmthresholds.vclo.farend.1day.ES	100 (seconds)
DS3I.pmthresholds.vclo.farend.1day.SES	7 (seconds)
DS3I.pmthresholds.vclo.farend.1day.UAS	10 (seconds)
DS3I.pmthresholds.vclo.nearend.15min.BBE	15 (count)
DS3I.pmthresholds.vclo.nearend.15min.EB	15 (count)
DS3I.pmthresholds.vclo.nearend.15min.ES	12 (seconds)
DS3I.pmthresholds.vclo.nearend.15min.SES	3 (seconds)
DS3I.pmthresholds.vclo.nearend.15min.UAS	10 (seconds)
DS3I.pmthresholds.vclo.nearend.1day.BBE	125 (count)
DS3I.pmthresholds.vclo.nearend.1day.EB	125 (count)
DS3I.pmthresholds.vclo.nearend.1day.ES	100 (seconds)

Table 3-9   DS3I Card Default Settings (continued)

Property Name	Default Value
DS3I.pmthresholds.vclo.nearend.1day.SES	7 (seconds)
DS3I.pmthresholds.vclo.nearend.1day.UAS	10 (seconds)

Table 3-10 lists the STM-1 card default settings.

Table 3-10   STM-1 Card Default Settings

Property Name	Default Value
STM1.config.line.AINSSoakTime	08:00 (hours:minutes)
STM1.config.line.State	OOS
STM1.pmthresholds.ms.farend.15min.BBE	1312 (count)
STM1.pmthresholds.ms.farend.15min.EB	1312 (seconds)
STM1.pmthresholds.ms.farend.15min.ES	87 (count)
STM1.pmthresholds.ms.farend.15min.SES	1 (seconds)
STM1.pmthresholds.ms.farend.15min.UAS	3 (seconds)
STM1.pmthresholds.ms.farend.1day.BBE	13120 (count)
STM1.pmthresholds.ms.farend.1day.EB	13120 (count)
STM1.pmthresholds.ms.farend.1day.ES	864 (seconds)
STM1.pmthresholds.ms.farend.1day.SES	4 (seconds)
STM1.pmthresholds.ms.farend.1day.UAS	10 (seconds)
STM1.pmthresholds.ms.nearend.15min.BBE	1312 (count)
STM1.pmthresholds.ms.nearend.15min.EB	1312 (count)
STM1.pmthresholds.ms.nearend.15min.ES	87 (seconds)
STM1.pmthresholds.ms.nearend.15min.NPJC-PDET	60 (count)
STM1.pmthresholds.ms.nearend.15min.NPJC-PGEN	60 (count)
STM1.pmthresholds.ms.nearend.15min.PPJC-PDET	60 (count)
STM1.pmthresholds.ms.nearend.15min.PPJC-PGEN	60 (count)
STM1.pmthresholds.ms.nearend.15min.PSC	1 (count)
STM1.pmthresholds.ms.nearend.15min.PSD	300 (seconds)
STM1.pmthresholds.ms.nearend.15min.SES	1 (seconds)
STM1.pmthresholds.ms.nearend.15min.UAS	3 (seconds)
STM1.pmthresholds.ms.nearend.1day.BBE	13120 (count)
STM1.pmthresholds.ms.nearend.1day.EB	13120 (count)
STM1.pmthresholds.ms.nearend.1day.ES	864 (seconds)
STM1.pmthresholds.ms.nearend.1day.NPJC-PDET	5760 (count)
STM1.pmthresholds.ms.nearend.1day.NPJC-PGEN	5760 (count)
STM1.pmthresholds.ms.nearend.1day.PPJC-PDET	5760 (count)
STM1.pmthresholds.ms.nearend.1day.PPJC-PGEN	5760 (count)

Table 3-10   STM-1 Card Default Settings (continued)

Property Name	Default Value
STM1.pmthresholds.ms.nearend.1day.PSC	5 (count)
STM1.pmthresholds.ms.nearend.1day.PSD	600 (seconds)
STM1.pmthresholds.ms.nearend.1day.SES	4 (seconds)
STM1.pmthresholds.ms.nearend.1day.UAS	10 (seconds)
STM1.pmthresholds.path.nearend.15min.BBE	25 (count)
STM1.pmthresholds.path.nearend.15min.EB	15 (count)
STM1.pmthresholds.path.nearend.15min.ES	12 (seconds)
STM1.pmthresholds.path.nearend.15min.SES	3 (seconds)
STM1.pmthresholds.path.nearend.15min.UAS	10 (seconds)
STM1.pmthresholds.path.nearend.1day.BBE	250 (count)
STM1.pmthresholds.path.nearend.1day.EB	125 (count)
STM1.pmthresholds.path.nearend.1day.ES	100 (seconds)
STM1.pmthresholds.path.nearend.1day.SES	7 (seconds)
STM1.pmthresholds.path.nearend.1day.UAS	10 (seconds)
STM1.pmthresholds.rs.nearend.15min.BBE	10000 (count)
STM1.pmthresholds.rs.nearend.15min.EB	10000 (count)
STM1.pmthresholds.rs.nearend.15min.ES	500 (seconds)
STM1.pmthresholds.rs.nearend.15min.SES	500 (seconds)
STM1.pmthresholds.rs.nearend.1day.BBE	100000 (count)
STM1.pmthresholds.rs.nearend.1day.EB	100000 (count)
STM1.pmthresholds.rs.nearend.1day.ES	5000 (seconds)
STM1.pmthresholds.rs.nearend.1day.SES	5000 (seconds)

Table 3-11 lists the STM-4 card default settings.

Table 3-11   STM-4 Cards Default Settings

Property Name	Default Value
STM4.config.line.AINSSoakTime	08:00 (hours:minutes)
STM4.config.line.State	OOS
STM4.pmthresholds.ms.farend.15min.BBE	5315 (count)
STM4.pmthresholds.ms.farend.15min.EB	5315 (count)
STM4.pmthresholds.ms.farend.15min.ES	87 (seconds)
STM4.pmthresholds.ms.farend.15min.SES	1 (seconds)
STM4.pmthresholds.ms.farend.15min.UAS	3 (seconds)
STM4.pmthresholds.ms.farend.1day.BBE	5315 (count)
STM4.pmthresholds.ms.farend.1day.EB	5315 (count)
STM4.pmthresholds.ms.farend.1day.ES	864 (seconds)

Table 3-11   STM-4 Cards Default Settings (continued)

Property Name	Default Value
STM4.pmthresholds.ms.farend.1day.SES	4 (seconds)
STM4.pmthresholds.ms.farend.1day.UAS	10 (seconds)
STM4.pmthresholds.ms.nearend.15min.BBE	53150 (count)
STM4.pmthresholds.ms.nearend.15min.EB	53150 (count)
STM4.pmthresholds.ms.nearend.15min.ES	87 (seconds)
STM4.pmthresholds.ms.nearend.15min.NPJC-PDET	60 (count)
STM4.pmthresholds.ms.nearend.15min.NPJC-PGEN	60 (count)
STM4.pmthresholds.ms.nearend.15min.PPJC-PDET	60 (count)
STM4.pmthresholds.ms.nearend.15min.PPJC-PGEN	60 (count)
STM4.pmthresholds.ms.nearend.15min.PSC	1 (count)
STM4.pmthresholds.ms.nearend.15min.PSC-W	1 (count)
STM4.pmthresholds.ms.nearend.15min.PSD	300 (seconds)
STM4.pmthresholds.ms.nearend.15min.PSD-W	300 (seconds)
STM4.pmthresholds.ms.nearend.15min.SES	1 (seconds)
STM4.pmthresholds.ms.nearend.15min.UAS	3 (seconds)
STM4.pmthresholds.ms.nearend.1day.BBE	53150 (count)
STM4.pmthresholds.ms.nearend.1day.EB	53150 (count)
STM4.pmthresholds.ms.nearend.1day.ES	864 (seconds)
STM4.pmthresholds.ms.nearend.1day.NPJC-PDET	5760 (count)
STM4.pmthresholds.ms.nearend.1day.NPJC-PGEN	5760 (count)
STM4.pmthresholds.ms.nearend.1day.PPJC-PDET	5760 (count)
STM4.pmthresholds.ms.nearend.1day.PPJC-PGEN	5760 (count)
STM4.pmthresholds.ms.nearend.1day.PSC	5 (count)
STM4.pmthresholds.ms.nearend.1day.PSC-W	5 (count)
STM4.pmthresholds.ms.nearend.1day.PSD	600 (seconds)
STM4.pmthresholds.ms.nearend.1day.PSD-W	600 (seconds)
STM4.pmthresholds.ms.nearend.1day.SES	4 (seconds)
STM4.pmthresholds.ms.nearend.1day.UAS	10 (seconds)
STM4.pmthresholds.path.nearend.15min.BBE	25 (count)
STM4.pmthresholds.path.nearend.15min.EB	15 (count)
STM4.pmthresholds.path.nearend.15min.ES	12 (seconds)
STM4.pmthresholds.path.nearend.15min.SES	3 (seconds)
STM4.pmthresholds.path.nearend.15min.UAS	10 (seconds)
STM4.pmthresholds.path.nearend.1day.BBE	250 (count)
STM4.pmthresholds.path.nearend.1day.EB	125 (count)
STM4.pmthresholds.path.nearend.1day.ES	100 (seconds)

Table 3-11   STM-4 Cards Default Settings (continued)

Property Name	Default Value
STM4.pmthresholds.path.nearend.1day.SES	7 (seconds)
STM4.pmthresholds.path.nearend.1day.UAS	10 (seconds)
STM4.pmthresholds.rs.nearend.15min.BBE	10000 (count)
STM4.pmthresholds.rs.nearend.15min.EB	10000 (count)
STM4.pmthresholds.rs.nearend.15min.ES	500 (seconds)
STM4.pmthresholds.rs.nearend.15min.SES	500 (seconds)
STM4.pmthresholds.rs.nearend.1day.BBE	100000 (count)
STM4.pmthresholds.rs.nearend.1day.EB	100000 (count)
STM4.pmthresholds.rs.nearend.1day.ES	5000 (seconds)
STM4.pmthresholds.rs.nearend.1day.SES	5000 (seconds)

Table 3-12 lists the STM4-4 card default settings.

Table 3-12   STM4-4 Cards Default Settings

Property Name	Default Value
STM4-4.config.line.AINSSoakTime	08:00 (hours:minutes)
STM4-4.config.line.State	OOS
STM4-4.pmthresholds.ms.farend.15min.BBE	5315 (count)
STM4-4.pmthresholds.ms.farend.15min.EB	5315 (count)
STM4-4.pmthresholds.ms.farend.15min.ES	87 (seconds)
STM4-4.pmthresholds.ms.farend.15min.SES	1 (seconds)
STM4-4.pmthresholds.ms.farend.15min.UAS	3 (seconds)
STM4-4.pmthresholds.ms.farend.1day.BBE	53150 (count)
STM4-4.pmthresholds.ms.farend.1day.EB	53150 (count)
STM4-4.pmthresholds.ms.farend.1day.ES	864 (seconds)
STM4-4.pmthresholds.ms.farend.1day.SES	4 (seconds)
STM4-4.pmthresholds.ms.farend.1day.UAS	10 (seconds)
STM4-4.pmthresholds.ms.nearend.15min.BBE	5315 (count)
STM4-4.pmthresholds.ms.nearend.15min.EB	5315 (count)
STM4-4.pmthresholds.ms.nearend.15min.ES	87 (seconds)
STM4-4.pmthresholds.ms.nearend.15min.NPJC-PDET	60 (count)
STM4-4.pmthresholds.ms.nearend.15min.NPJC-PGEN	60 (count)
STM4-4.pmthresholds.ms.nearend.15min.PPJC-PDET	60 (count)
STM4-4.pmthresholds.ms.nearend.15min.PPJC-PGEN	60 (count)
STM4-4.pmthresholds.ms.nearend.15min.PSC	1 (count)
STM4-4.pmthresholds.ms.nearend.15min.PSC-W	1 (count)
STM4-4.pmthresholds.ms.nearend.15min.PSD	300 (seconds)

Table 3-12   STM4-4 Cards Default Settings (continued)

Property Name	Default Value
STM4-4.pmthresholds.ms.nearend.15min.PSD-W	300 (seconds)
STM4-4.pmthresholds.ms.nearend.15min.SES	1 (seconds)
STM4-4.pmthresholds.ms.nearend.15min.UAS	3 (seconds)
STM4-4.pmthresholds.ms.nearend.1day.BBE	53150 (count)
STM4-4.pmthresholds.ms.nearend.1day.EB	53150 (count)
STM4-4.pmthresholds.ms.nearend.1day.ES	864 (seconds)
STM4-4.pmthresholds.ms.nearend.1day.NPJC-PDET	5760 (count)
STM4-4.pmthresholds.ms.nearend.1day.NPJC-PGEN	5760 (count)
STM4-4.pmthresholds.ms.nearend.1day.PPJC-PDET	5760 (count)
STM4-4.pmthresholds.ms.nearend.1day.PPJC-PGEN	5760 (count)
STM4-4.pmthresholds.ms.nearend.1day.PSC	5 (count)
STM4-4.pmthresholds.ms.nearend.1day.PSC-W	5 (count)
STM4-4.pmthresholds.ms.nearend.1day.PSD	600 (seconds)
STM4-4.pmthresholds.ms.nearend.1day.PSD-W	600 (seconds)
STM4-4.pmthresholds.ms.nearend.1day.SES	4 (seconds)
STM4-4.pmthresholds.ms.nearend.1day.UAS	10 (seconds)
STM4-4.pmthresholds.path.nearend.15min.BBE	25 (count)
STM4-4.pmthresholds.path.nearend.15min.EB	15 (count)
STM4-4.pmthresholds.path.nearend.15min.ES	12 (seconds)
STM4-4.pmthresholds.path.nearend.15min.SES	3 (seconds)
STM4-4.pmthresholds.path.nearend.15min.UAS	10 (seconds)
STM4-4.pmthresholds.path.nearend.1day.BBE	250 (count)
STM4-4.pmthresholds.path.nearend.1day.EB	125 (count)
STM4-4.pmthresholds.path.nearend.1day.ES	100 (seconds)
STM4-4.pmthresholds.path.nearend.1day.SES	7 (seconds)
STM4-4.pmthresholds.path.nearend.1day.UAS	10 (seconds)
STM4-4.pmthresholds.rs.nearend.15min.BBE	10000 (count)
STM4-4.pmthresholds.rs.nearend.15min.EB	10000 (count)
STM4-4.pmthresholds.rs.nearend.15min.ES	500 (seconds)
STM4-4.pmthresholds.rs.nearend.15min.SES	500 (seconds)
STM4-4.pmthresholds.rs.nearend.1day.BBE	100000 (count)
STM4-4.pmthresholds.rs.nearend.1day.EB	100000 (count)
STM4-4.pmthresholds.rs.nearend.1day.ES	5000 (seconds)
STM4-4.pmthresholds.rs.nearend.1day.SES	5000 (seconds)

Table 3-13 lists the STM-16 card default settings.

Table 3-13   STM-16 Cards Default Settings

Property Name	Default Value
STM16.config.line.AINSSoakTime	08:00 (hours:minutes)
STM16.config.line.State	OOS
STM16.pmthresholds.ms.farend.15min.BBE	21260 (count)
STM16.pmthresholds.ms.farend.15min.EB	21260 (count)
STM16.pmthresholds.ms.farend.15min.ES	87 (seconds)
STM16.pmthresholds.ms.farend.15min.SES	1 (seconds)
STM16.pmthresholds.ms.farend.15min.UAS	3 (seconds)
STM16.pmthresholds.ms.farend.1day.BBE	212600 (count)
STM16.pmthresholds.ms.farend.1day.EB	212600 (count)
STM16.pmthresholds.ms.farend.1day.ES	864 (seconds)
STM16.pmthresholds.ms.farend.1day.SES	4 (seconds)
STM16.pmthresholds.ms.farend.1day.UAS	10 (seconds)
STM16.pmthresholds.ms.nearend.15min.BBE	21260 (count)
STM16.pmthresholds.ms.nearend.15min.EB	21260 (count)
STM16.pmthresholds.ms.nearend.15min.ES	87 (seconds)
STM16.pmthresholds.ms.nearend.15min.NPJC-PDET	60 (count)
STM16.pmthresholds.ms.nearend.15min.NPJC-PGEN	60 (count)
STM16.pmthresholds.ms.nearend.15min.PPJC-PDET	60 (count)
STM16.pmthresholds.ms.nearend.15min.PPJC-PGEN	60 (count)
STM16.pmthresholds.ms.nearend.15min.PSC	1 (count)
STM16.pmthresholds.ms.nearend.15min.PSC-R	1 (count)
STM16.pmthresholds.ms.nearend.15min.PSC-S	1 (count)
STM16.pmthresholds.ms.nearend.15min.PSC-W	1 (count)
STM16.pmthresholds.ms.nearend.15min.PSD	300 (seconds)
STM16.pmthresholds.ms.nearend.15min.PSD-R	300 (seconds)
STM16.pmthresholds.ms.nearend.15min.PSD-S	300 (seconds)
STM16.pmthresholds.ms.nearend.15min.PSD-W	300 (seconds)
STM16.pmthresholds.ms.nearend.15min.SES	1 (seconds)
STM16.pmthresholds.ms.nearend.15min.UAS	3 (seconds)
STM16.pmthresholds.ms.nearend.1day.BBE	212600 (count)
STM16.pmthresholds.ms.nearend.1day.EB	212600 (count)
STM16.pmthresholds.ms.nearend.1day.ES	864 (seconds)
STM16.pmthresholds.ms.nearend.1day.NPJC-PDET	5760 (count)
STM16.pmthresholds.ms.nearend.1day.NPJC-PGEN	5760 (count)
STM16.pmthresholds.ms.nearend.1day.PPJC-PDET	5760 (count)

Table 3-13   STM-16 Cards Default Settings (continued)

Property Name	Default Value
STM16.pmthresholds.ms.nearend.1day.PPJC-PGEN	5760 (count)
STM16.pmthresholds.ms.nearend.1day.PSC	5 (count)
STM16.pmthresholds.ms.nearend.1day.PSC-R	5 (count)
STM16.pmthresholds.ms.nearend.1day.PSC-S	5 (count)
STM16.pmthresholds.ms.nearend.1day.PSC-W	5 (count)
STM16.pmthresholds.ms.nearend.1day.PSD	600 (seconds)
STM16.pmthresholds.ms.nearend.1day.PSD-R	600 (seconds)
STM16.pmthresholds.ms.nearend.1day.PSD-S	600 (seconds)
STM16.pmthresholds.ms.nearend.1day.PSD-W	600 (seconds)
STM16.pmthresholds.ms.nearend.1day.SES	4 (seconds)
STM16.pmthresholds.ms.nearend.1day.UAS	10 (seconds)
STM16.pmthresholds.path.nearend.15min.BBE	25 (count)
STM16.pmthresholds.path.nearend.15min.EB	15 (count)
STM16.pmthresholds.path.nearend.15min.ES	12 (seconds)
STM16.pmthresholds.path.nearend.15min.SES	3 (seconds)
STM16.pmthresholds.path.nearend.15min.UAS	10 (seconds)
STM16.pmthresholds.path.nearend.1day.BBE	250 (count)
STM16.pmthresholds.path.nearend.1day.EB	125 (count)
STM16.pmthresholds.path.nearend.1day.ES	100 (seconds)
STM16.pmthresholds.path.nearend.1day.SES	7 (seconds)
STM16.pmthresholds.path.nearend.1day.UAS	10 (seconds)
STM16.pmthresholds.rs.nearend.15min.BBE	10000 (count)
STM16.pmthresholds.rs.nearend.15min.EB	10000 (count)
STM16.pmthresholds.rs.nearend.15min.ES	500 (seconds)
STM16.pmthresholds.rs.nearend.15min.SES	500 (seconds)
STM16.pmthresholds.rs.nearend.1day.BBE	100000 (count)
STM16.pmthresholds.rs.nearend.1day.EB	100000 (count)
STM16.pmthresholds.rs.nearend.1day.ES	5000 (seconds)
STM16.pmthresholds.rs.nearend.1day.SES	5000 (seconds)

Table 3-14 lists the STM-64 card default settings.

Table 3-14   STM-64 Cards Default Settings

Property Name	Default Value
STM64.config.line.AINSSoakTime	08:00 (hours:minutes)
STM64.config.line.State	OOS
STM64.pmthresholds.ms.farend.15min.BBE	85040 (count)

Table 3-14   STM-64 Cards Default Settings (continued)

Property Name	Default Value
STM64.pmthresholds.ms.farend.15min.EB	85040 (count)
STM64.pmthresholds.ms.farend.15min.ES	87 (seconds)
STM64.pmthresholds.ms.farend.15min.SES	1 (seconds)
STM64.pmthresholds.ms.farend.15min.UAS	3 (seconds)
STM64.pmthresholds.ms.farend.1day.BBE	85040 (count)
STM64.pmthresholds.ms.farend.1day.EB	85040 (count)
STM64.pmthresholds.ms.farend.1day.ES	864 (seconds)
STM64.pmthresholds.ms.farend.1day.SES	4 (seconds)
STM64.pmthresholds.ms.farend.1day.UAS	10 (seconds)
STM64.pmthresholds.ms.nearend.15min.BBE	85040 (count)
STM64.pmthresholds.ms.nearend.15min.EB	85040 (count)
STM64.pmthresholds.ms.nearend.15min.ES	87 (seconds)
STM64.pmthresholds.ms.nearend.15min.NPJC-PDET	60 (count)
STM64.pmthresholds.ms.nearend.15min.NPJC-PGEN	60 (count)
STM64.pmthresholds.ms.nearend.15min.PPJC-PDET	60 (count)
STM64.pmthresholds.ms.nearend.15min.PPJC-PGEN	60 (count)
STM64.pmthresholds.ms.nearend.15min.PSC	1 (count)
STM64.pmthresholds.ms.nearend.15min.PSC-R	1 (count)
STM64.pmthresholds.ms.nearend.15min.PSC-S	1 (count)
STM64.pmthresholds.ms.nearend.15min.PSC-W	1 (count)
STM64.pmthresholds.ms.nearend.15min.PSD	300 (seconds)
STM64.pmthresholds.ms.nearend.15min.PSD-R	300 (seconds)
STM64.pmthresholds.ms.nearend.15min.PSD-S	300 (seconds)
STM64.pmthresholds.ms.nearend.15min.PSD-W	300 (seconds)
STM64.pmthresholds.ms.nearend.15min.SES	1 (seconds)
STM64.pmthresholds.ms.nearend.15min.UAS	3 (seconds)
STM64.pmthresholds.ms.nearend.1day.BBE	850400 (count)
STM64.pmthresholds.ms.nearend.1day.EB	850400 (count)
STM64.pmthresholds.ms.nearend.1day.ES	864 (seconds)
STM64.pmthresholds.ms.nearend.1day.NPJC-PDET	5760 (count)
STM64.pmthresholds.ms.nearend.1day.NPJC-PGEN	5760 (count)
STM64.pmthresholds.ms.nearend.1day.PPJC-PDET	5760 (count)
STM64.pmthresholds.ms.nearend.1day.PPJC-PGEN	5760 (count)
STM64.pmthresholds.ms.nearend.1day.PSC	5 (count)
STM64.pmthresholds.ms.nearend.1day.PSC-R	5 (count)
STM64.pmthresholds.ms.nearend.1day.PSC-S	5 (count)

Table 3-14   STM-64 Cards Default Settings (continued)

Property Name	Default Value
STM64.pmthresholds.ms.nearend.1day.PSC-W	5 (count)
STM64.pmthresholds.ms.nearend.1day.PSD	600 (seconds)
STM64.pmthresholds.ms.nearend.1day.PSD-R	600 (seconds)
STM64.pmthresholds.ms.nearend.1day.PSD-S	600 (seconds)
STM64.pmthresholds.ms.nearend.1day.PSD-W	600 (seconds)
STM64.pmthresholds.ms.nearend.1day.SES	4 (seconds)
STM64.pmthresholds.ms.nearend.1day.UAS	10 (seconds)
STM64.pmthresholds.path.nearend.15min.BBE	25 (count)
STM64.pmthresholds.path.nearend.15min.EB	15 (count)
STM64.pmthresholds.path.nearend.15min.ES	12 (seconds)
STM64.pmthresholds.path.nearend.15min.SES	3 (seconds)
STM64.pmthresholds.path.nearend.15min.UAS	10 (seconds)
STM64.pmthresholds.path.nearend.1day.BBE	250 (count)
STM64.pmthresholds.path.nearend.1day.EB	125 (count)
STM64.pmthresholds.path.nearend.1day.ES	100 (seconds)
STM64.pmthresholds.path.nearend.1day.SES	7 (seconds)
STM64.pmthresholds.path.nearend.1day.UAS	10 (seconds)
STM64.pmthresholds.rs.nearend.15min.BBE	10000 (count)
STM64.pmthresholds.rs.nearend.15min.EB	10000 (count)
STM64.pmthresholds.rs.nearend.15min.ES	500 (seconds)
STM64.pmthresholds.rs.nearend.15min.SES	500 (seconds)
STM64.pmthresholds.rs.nearend.1day.BBE	100000 (count)
STM64.pmthresholds.rs.nearend.1day.EB	100000 (count)
STM64.pmthresholds.rs.nearend.1day.ES	5000 (seconds)
STM64.pmthresholds.rs.nearend.1day.SES	5000 (seconds)

3.7.2 Node Default Settings

Table 3-15 on page 3-48 lists the ONS 15454 SDH node-level default settings for the Cisco ONS 15454 SDH. Cisco provides the following types of settings preprovisioned for each ONS 15454 SDH node:

- Subnetwork connection protection (SNCP) reversion
- MS-SPRing reversion
- LMSP protection
- IIOP listener port
- Timing parameters

Table 3-15   Node Default Settings

Property Name	Default Value
NODE.circuits.sncp.ReversionTime	5.0 (minutes)
NODE.circuits.sncp.Revertive	FALSE
NODE.general.DefaultsDescription	Factory defaults
NODE.general.IIOPListenerPort (reboots node)	57790 (port #)
NODE.general.LoginWarningMessage	**WARNING** This system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.
NODE.protection.lmsp.BidirectionalSwitching	FALSE
NODE.protection.lmsp.ReversionTime	5.0 (minutes)
NODE.protection.lmsp.Revertive	FALSE
NODE.protection.msspr.RingReversionTime	5.0 (minutes)
NODE.protection.msspr.RingRevertive	TRUE
NODE.protection.msspr.SpanReversionTime	5.0 (minutes)
NODE.protection.msspr.SpanRevertive	TRUE
NODE.timing.bits-1.AISThreshold	G812L
NODE.timing.bits-1.Coding	HDB3
NODE.timing.bits-1.Framing	FAS+CAS+CRC
NODE.timing.bits-1.State	IS
NODE.timing.bits-2.AISThreshold	G812L
NODE.timing.bits-2.Coding	HDB3
NODE.timing.bits-2.Framing	FAS+CAS+CRC
NODE.timing.bits-2.State	IS
NODE.timing.general.Mode	External
NODE.timing.general.ReversionTime	5.0 (minutes)
NODE.timing.general.Revertive	FALSE

IP Networking

This chapter explains how to set up Cisco ONS 15454 SDH nodes in IP networks. The chapter does not provide a comprehensive explanation of IP networking concepts and procedures.

Note   To set up ONS 15454 SDH nodes within an IP network, you must work with a LAN administrator or other individual at your site who has IP network 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.

Table 4-1 lists IP networking topics. Table 4-2 lists IP networking routing procedures on the ONS 15454 SDH.

Table 4-1   IP Networking Topics

IP Networking Topics

Table 4-2   IP Networking Procedures

IP Networking Procedures

Table 4-2   IP Networking Procedures (continued)

IP Networking Procedures
Procedure: Set Up OSPF, page 4-12
Procedure: Set Up or Change Routing Information Protocol, page 4-16

4.1 Before You Begin

Determine how your network will be connected. There are many different ONS 15454 SDH connection options within an IP environment:

- ONS 15454 SDH nodes can be connected to LANs directly or through a router.

- IP subnetting can create ONS 15454 SDH node groups, allowing 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 SDH to serve as a gateway for ONS 15454 SDH nodes that are not connected to the LAN.

- You can create static routes to enable connections among multiple CTC sessions with ONS 15454 SDH nodes that reside on the same subnet but have different destination IP addresses.

- If ONS 15454 SDH nodes are connected to open shortest path first (OSPF) networks, ONS 15454 SDH network information is automatically communicated across multiple LANs and WANs.

ONS 15454 SDH IP addressing generally has eight common scenarios or configurations. Each of these scenarios is described in this chapter. Use the scenarios as building blocks for more complex network configurations.

Table 4-3 provides a general list of items to check when setting up ONS 15454 SDH nodes in IP networks. Additional procedures for troubleshooting Ethernet connections and IP networks are provided in Chapter 9, "Ethernet Operation."

Table 4-3   General ONS 15454 SDH IP Networking Checklist

Item	What to Check
PC/workstation	Each CTC computer must have the following: • Web browser • Java Runtime Environment • Java.policy file (modified for CTC) See the "Check Computer Software Requirements" section on page 2-3 for detailed information.
Link integrity	Link integrity exists between: • CTC computer and network hub/switch • ONS 15454 SDH nodes (backplane wire-wrap pins or RJ-45 port) and network hub/switch • Router ports and hub/switch ports
ONS 15454 SDH hub/switch ports	Set the hub or switch port that is connected to the ONS 15454 SDH to 10 Mbps half-duplex.

Table 4-3   General ONS 15454 SDH IP Networking Checklist (continued)

Item	What to Check
Ping	Ping the node to test connections between computers and ONS 15454 SDH nodes.
IP addresses/subnet masks	ONS 15454 SDH IP addresses and subnet masks are set up correctly.
Optical connectivity	ONS 15454 SDH optical trunk ports are in service; DCC is enabled on each trunk port.

4.2 Scenario 1: CTC and ONS 15454 SDH Nodes on Same Subnet

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

Note   Instructions for creating DCC connections are provided in Chapter 5, "SDH Topologies" within the MS-SPRing, SNCP, and linear ADM procedures.

Figure 4-1   Scenario 1: CTC and ONS 15454 SDH nodes 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 SDH #2
IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

SDH RING

ONS 15454 SDH #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15454 SDH #3
IP Address 192.168.1.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

71295

4.3 Scenario 2: CTC and ONS 15454 SDH Nodes 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 15454 SDH nodes 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 15454 SDH nodes connected to router
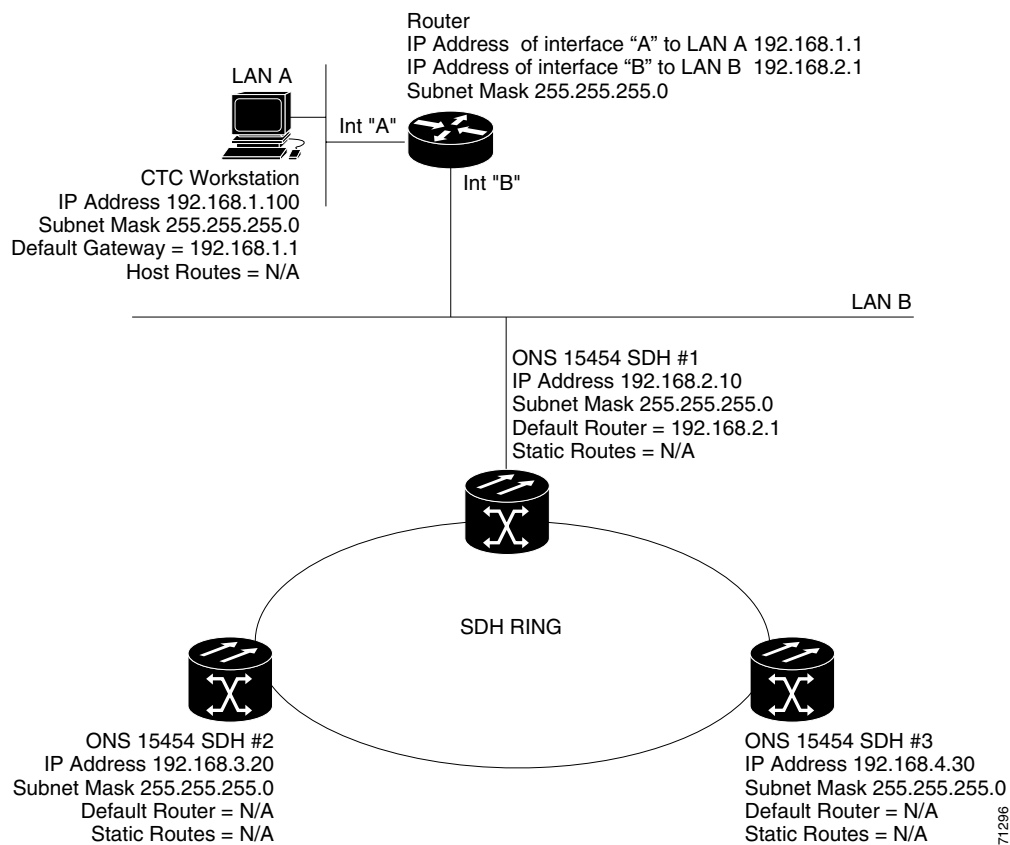
4.4 Scenario 3: Using Proxy ARP to Enable an ONS 15454 SDH Gateway

Scenario 3 is similar to Scenario 1, but only one ONS 15454 SDH (Node 1) connects to the LAN (Figure 4-3). Two ONS 15454 SDH nodes (2 and 3) connect to ONS 15454 SDH 1 through the SDH DCC. Because all three ONS 15454 SDH nodes are on the same subnet, Proxy ARP enables ONS 15454 SDH 1 to serve as a gateway for ONS 15454 SDH nodes 2 and 3.

Figure 4-3   Scenario 3: Using Proxy ARP to enable an ONS 15454 SDH gateway

CTC Workstation
IP Address 192.168.1.100
Subnet Mark at CTC Workstation 255.255.255.0
Default Gateway = N/A

LAN A

ONS 15454 SDH #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

SDH RING

ONS 15454 SDH #2
IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15454 SDH #3
IP Address 192.168.1.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

71297

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 SDH to respond to the ARP request for ONS 15454 SDH nodes not connected to the LAN. (ONS 15454 SDH Proxy ARP requires no user configuration.) For this to occur, the DCC-connected ONS 15454 SDH nodes must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15454 SDH that is not connected to the LAN, the gateway ONS 15454 SDH returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15454 SDH to the MAC address of the proxy ONS 15454 SDH. The proxy ONS 15454 SDH uses its routing table to forward the datagram to the non-LAN ONS 15454 SDH. The routing table is built using the OSPF IP routing protocol. (An OSPF example is presented in the "Scenario 7: Using OSPF" section on page 4-10.)

4.5 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 15454 SDH nodes 2 and 3, ONS 15454 SDH 1 is entered as the default gateway on the CTC computer using the "Setting Up the CTC Computer" section on page 2-10.

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 SDH #1
IP Address 192.168.1.10
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

SDH RING

ONS 15454 SDH #2
IP Address 192.168.2.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15454 SDH #3
IP Address 192.168.3.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

4.6 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15454 SDH nodes to CTC sessions on one subnet connected by a router to ONS 15454 SDH nodes 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 15454 SDH nodes 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 15454 SDH nodes residing on subnet 192.168.2.0 are connected through ONS 15454 SDH 1 to the router through interface B. Proxy ARP enables ONS 15454 SDH 1 as a gateway for ONS 15454 SDH nodes 2 and 3. To connect to CTC computers on LAN A, a static route is created on ONS 15454 SDH 1.

Figure 4-5   Scenario 5: Static route with one CTC computer used as a destination
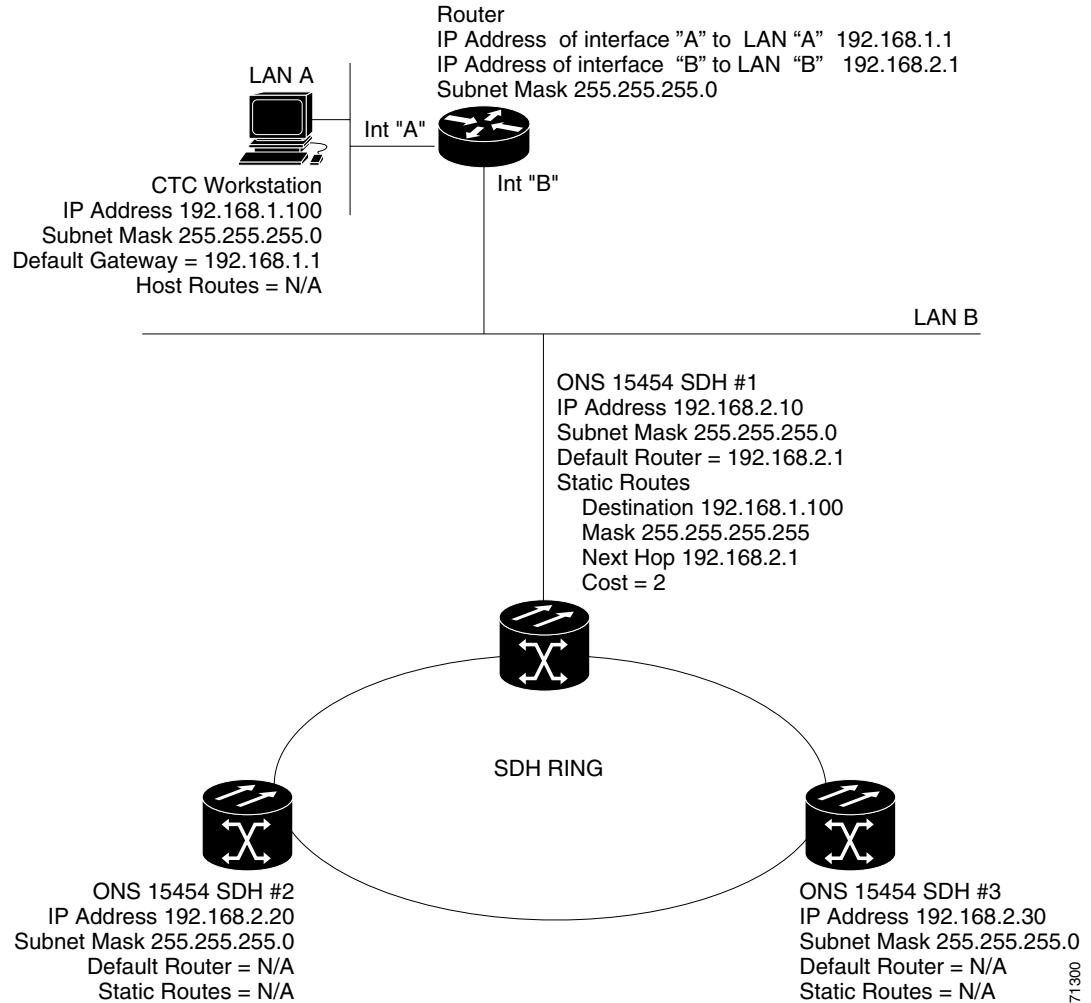
The destination and subnet mask entries control access to the ONS 15454 SDH nodes.

- If a single CTC computer is connected to the router, enter the complete CTC "host route" IP address as the destination with a subnet mask of 255.255.255.255.

- If all CTC computers on a subnet are connected to the router, enter the destination subnet (in this example, 192.168.1.0) and a subnet mask of 255.255.255.0.

- If all CTC computers on all subnets are connected to the router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 4-6 on page 4-8 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
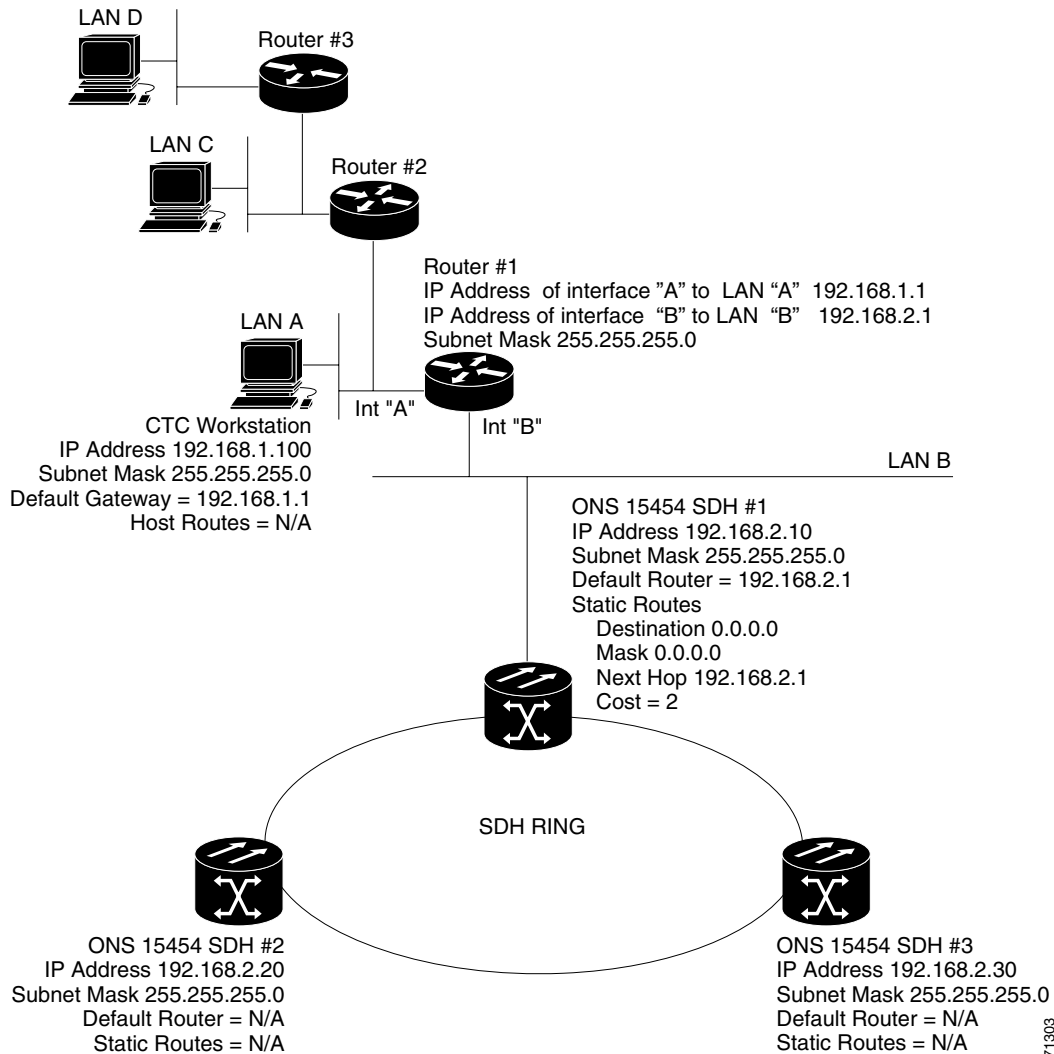
Procedure: Create a Static Route

Purpose	Use this procedure to create a static route. Static routes are used for two purposes:
	• To connect ONS 15454 SDH nodes to CTC sessions on one subnet connected by a router to ONS 15454 SDH nodes residing on another subnet.
	• To enable multiple CTC sessions among ONS 15454 SDH nodes residing on the same subnet.
Onsite/Remote	Onsite or remote

Step 1   Start CTC for an ONS 15454 SDH node and choose the **Provisioning** > **Network** tabs.

Step 2   Click the **Static Routing** tab. Click **Create**.

Figure 4-7   Create Static Route dialog box
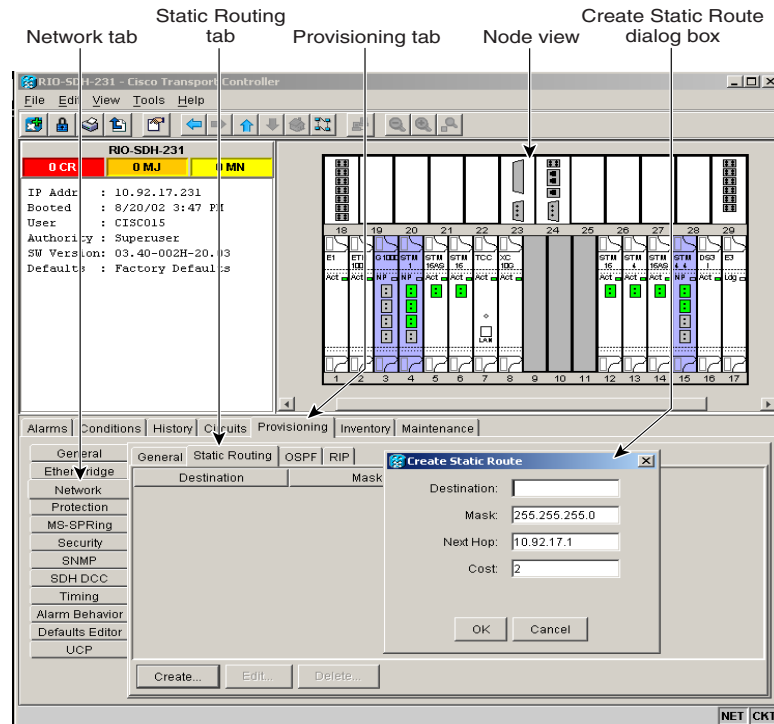
Step 3   In the Create Static Route dialog box enter the following:

- 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 SDH and the computer. In this example, the cost is two: one hop from the ONS 15454 SDH 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.

4.7 Scenario 6: Static Route for Multiple CTCs

Scenario 6 shows a static route used when multiple CTC computers need to access ONS 15454 SDH nodes residing on the same subnet (Figure 4-8). In this scenario, CTC 1 and 2 and all ONS 15454 SDH nodes are on the same IP subnet; ONS 15454 SDH 1 and CTC 1 are attached to LAN A. ONS 15454 SDH 2 and CTC 2 are attached to LAN B. Static routes are added to ONS 15454 SDH 1 pointing to CTC 1, and to ONS 15454 SDH 2 pointing to CTC 2. The static route is entered from the node's perspective.

Figure 4-8   *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 SDH #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

SDH RING

LAN B

ONS 15454 SDH #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 SDH #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

71301

4.8 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 15454 SDH nodes use the OSPF protocol in internal ONS 15454 SDH networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15454 SDH nodes so that the ONS 15454 SDH topology is sent to OSPF routers on a LAN. Advertising the ONS 15454 SDH network topology to LAN routers eliminates the need to manually enter static routes for ONS 15454 SDH subnetworks. Figure 4-9 shows the same network enabled for OSPF. Figure 4-10 on page 4-12 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 SDH 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 SDH OSPF topology for advertising to an OSPF network, you must assign an OSPF Area ID to the ONS 15454 SDH network. Coordinate the area ID number assignment with your LAN administrator. In general, all DCC-connected ONS 15454 SDH nodes are assigned the same OSPF Area ID.

Figure 4-9   Scenario 7: OSPF enabled

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

LAN A

Int "A"

Int "B"

CTC Workstation
IP Address 192.168.1.100
Subnet Mask 255.255.255.0
Default Gateway = 192.168.1.1
Host Routes = N/A

LAN B

ONS 15454 SDH #1
IP Address 192.168.2.10
Subnet Mask 255.255.255.0
Default Router = 192.168.2.1
Static Routes = N/A

SDH RING

ONS 15454 SDH #2
IP Address 192.168.3.20
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

ONS 15454 SDH #3
IP Address 192.168.4.30
Subnet Mask 255.255.255.0
Default Router = N/A
Static Routes = N/A

71302

Figure 4-10   Scenario 7: OSPF not enabled
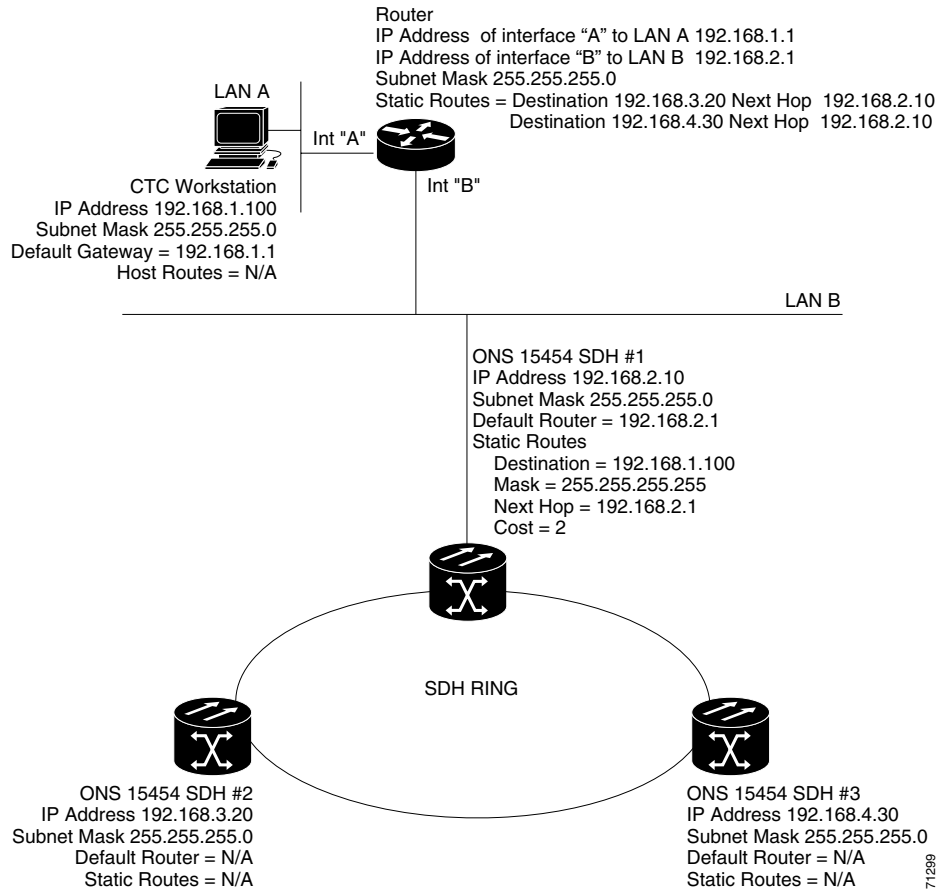
Procedure: Set Up OSPF

Purpose	Use the following procedure to enable OSPF on each ONS 15454 SDH node that you want included in the OSPF network topology.
Prerequisite Information	ONS 15454 SDH 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 SDH network is connected before enabling OSPF.
Onsite/Remote	Onsite or remote

Step 1   Start CTC for an ONS 15454 SDH node.

Step 2   In node view, choose the **Provisioning** > **Network** > **OSPF** tabs. The OSPF pane has several options (Figure 4-11).

Figure 4-11   Enabling OSPF on the ONS 15454 SDH
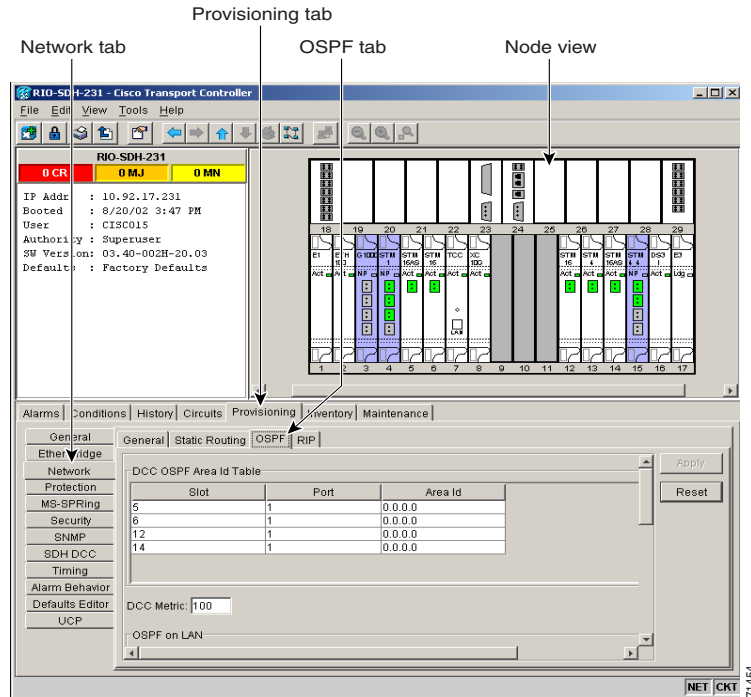
Step 3   Complete the following:

- DCC OSPF Area ID—Click the Area ID next to the slot and port field. Enter the number that identifies the ONS 15454 SDH nodes 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 SDH OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15454 SDH nodes that directly connect to OSPF routers.

- LAN Port Area ID—Enter the OSPF Area ID for the router port where the ONS 15454 SDH is connected. (This number is different from the DCC Area ID.)

Step 5   In the Authentication Type area, click the button that says **No Athentication** or **Simple Password** and complete the following:

- Authentication Type—Use the menu to select **Simple Password** or **No Authentication**. (The button name depends on the options selected.) If the router where the ONS 15454 SDH is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.

- Enter Authentication Key—If authentication is enabled, enter the OSPF key (password).

- Confirm Authentication Key—Enter the OSPF key again for confirmation purposes.

Step 6   Complete the following (Figure 4-12):

Note   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 SDH is connected.

- Router Priority—Select the designated router for a subnet.
- Hello Interval (sec)—Set the number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.
- Dead Interval—Set 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)—Indicate the service speed. One second is the default.
- Retransmit Interval (sec)—Set the time that will elapse before a packet is resent. Five seconds is the default.
- LAN Metric—Set a "cost" for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

Figure 4-12   The OSPF area range table and virtual link table
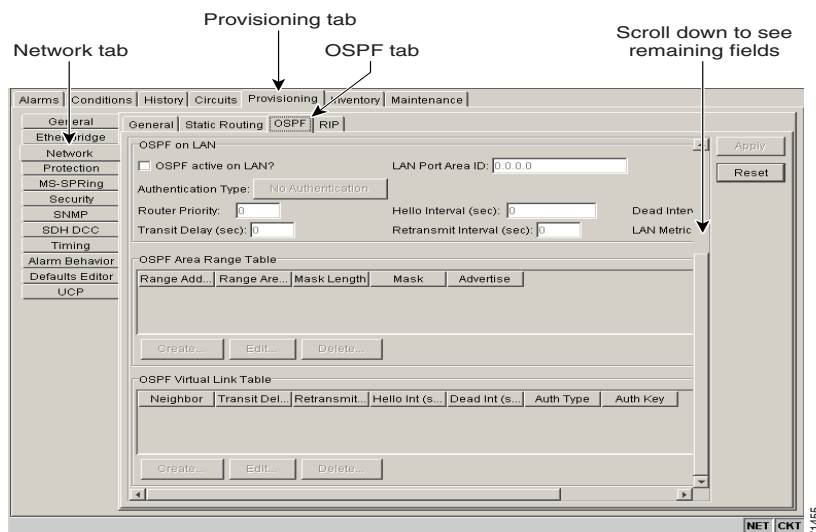
Step 7   In the OSPF Area Range Table area, complete the following:

Note   Area range tables consolidate the information that is propagated outside an OSPF Area border. One ONS 15454 SDH in the ONS 15454 SDH OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15454 SDH OSPF area.

a.   Under OSPF Area Range Table, click **Create**.

b.   In the Create Area Range dialog box, enter the following:

- Range Address—Enter the area IP address for the ONS 15454 SDH nodes that reside within the OSPF area. For example, if the ONS 15454 SDH OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.

- Range Area ID—Enter the OSPF Area ID for the ONS 15454 SDH nodes. This is either the ID in the DCC OSPF Area ID field or the ID in the Area ID for LAN Port field.

- Mask Length—Enter the subnet mask length. In the Range Address example, this is 16.

- Mask—Displays the subnet mask used to reach the destination host or network.

- 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 SDH OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

    a. Under OSPF Virtual Link Table, click **Create**.

    b. In the Create Virtual Link dialog box, complete the following fields. (The OSPF settings must match OSPF settings for the ONS 15454 SDH OSPF area.)

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

- Transit Delay (sec)—The service speed. One second is the default.

- Retransmit Int (sec)—Sets the time that will elapse before a packet is resent. Five seconds is the default.

- Hello Int (sec)—The number of seconds between OSPF hello packet advertisements sent by OSPF routers. Ten seconds is the default.

- Dead Int (sec)—Sets the number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. Forty seconds is the default.

- Auth Type—If the router where the ONS 15454 SDH is connected uses authentication, choose **Simple Password**. Otherwise, set it to **No Authentication**.

    c. Click **OK**.

Step 9   After entering ONS 15454 SDH OSPF area data, click **Apply**.

If you changed the Area ID, the TCC-I cards will reset, one at a time.

4.9 Scenario 8: Using RIP

The Routing Information Protocol (RIP) is widely used for routing traffic in the global Internet. RIP is an interior gateway protocol, which means that it performs routing within a single autonomous system. Exterior gateway protocols, such as the Border Gateway Protocol (BGP), perform routing between different autonomous systems.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by one, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform

other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. To configure the ONS 15454 SDH for RIP, see the "Set Up or Change Routing Information Protocol" procedure on page 4-16.

Procedure: Set Up or Change Routing Information Protocol

Purpose	Use this procedure to enable RIP on the ONS 15454 SDH. Perform this task if you want to include the ONS 15454 SDH in RIP-enabled networks.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
	You will need to create a static route to the router adjacent to the ONS 15454 SDH in order for the ONS 15454 SDH to send its routing information out to the network. See the "Create a Static Route" procedure on page 4-8 for more information.
Onsite/Remote	Onsite or remote

Step 1 Display the node view.

Step 2 Click the **Provisioning > Network > RIP** tabs.

Step 3 Check the **RIP Active?** check box if you are activating RIP.

Step 4 Choose either **RIP Version 1** or **RIP Version 2** from the drop-down menu, depending on which version is supported in your network.

Step 5 Set the **RIP metric**. The RIP metric can be set to a number between 1 and 15 and represents the number of hops.

Step 6 Under **Authentication**, select the authentication type. If the router where the ONS 15454 SDH is connected requires authentication, choose **Simple Password**. Otherwise, choose **No Authentication**. (default). You must click the **No Authentication** button to choose the Simple Password option.

4.10 Scenario 9: Using the Proxy Server Features

The ONS 15454 proxy server is a set of functions that allows you to network ONS 15454 SDH nodes in environments where visibility and accessibility between ONS 15454s and CTC computers must be restricted. For example, you can set up a network so that field technicians and network operation center (NOC) personnel can both access the same ONS 15454 SDH nodes while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15454 SDH is provisioned as a gateway NE (GNE) and the other ONS 15454 SDH nodes are provisioned as element NEs (ENEs). The GNE ONS 15454 SDH tunnels connections between CTC computers and ENE ONS 15454 SDH nodes, providing management capability while preventing access for non-ONS 15454 SDH management purposes.

The ONS 15454 SDH proxy server performs the following tasks:

- Isolates DCC IP traffic from Ethernet (craft port) traffic and accepts packets based on filtering rules. The filtering rules (see Table 4-5 on page 4-21 and Table 4-6 on page 4-22) depend on whether the packet arrives at the ONS 15454 SDH DCC interface or the TCC-I Ethernet interface.

- Monitors ARP request packets on its Ethernet port. If the ARP request is from an address that is not on the current subnet, the ONS 15454 SDH creates an entry in its ARP table. The ARP entry allows the ONS 15454 SDH to reply to an address over the local Ethernet so craft technicians can connect to ONS 15454 SDH nodes without changing the IP addresses of their computers.

- Processes SNTP/NTP requests. Element ONS 15454 SDH NEs can derive time of day from an SNTP/NTP LAN server through the GNE ONS 15454 SDH.

- Process SNMPv1 traps. The GNE ONS 15454 SDH receives SNMPv1 traps from the ENE ONS 15454 SDH nodes and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15454 SDH proxy server is provisioned using the following three check boxes in the Provisioning > Network > General tab (see Figure 4-13 on page 4-18):

- Craft Access Only—When this option is enabled, the ONS 15454 SDH neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15454 SDH, but they cannot communicate directly with any other DCC-connected ONS 15454 SDH.

- Enable Proxy—When this option is enabled, the ONS 15454 SDH serves as a proxy for connections between CTC clients and ONS 15454 SDH nodes that are DCC-connected to the proxy ONS 15454 SDH. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client can connect to nodes that it cannot directly reach from the host on which it runs. If Enable Proxy is off, the node does not establish proxy connections for any CTC clients, although any established proxy connections will continue until the CTC client exits.

- Enable Firewall—If this option is selected, the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15454 SDH can communicate with machines connected to the LAN port or connected through the DCC. However, the DCC-connected machines cannot communicate with the LAN-connected machines, and the LAN-connected machines cannot communicate with the DCC-connected machines. A CTC client using the LAN to connect to the firewall-enabled node can use the proxy capability to manage the DCC-connected nodes that would otherwise be unreachable. A CTC client connected to a DCC-connected node can only manage other DCC-connected nodes and the firewall itself.

Figure 4-13   Proxy server gateway settings
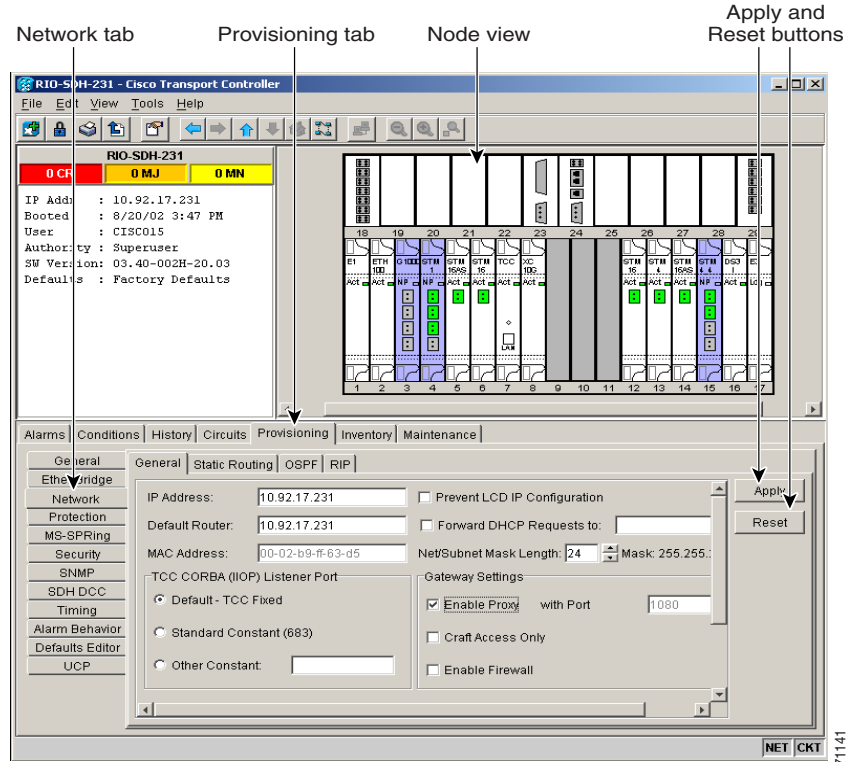
Figure 4-14 on page 4-19 shows an ONS 15454 SDH proxy server implementation. A GNE ONS 15454 SDH is connected to a central office LAN and to ENE ONS 15454 SDH nodes. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ONS 15454 SDH ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

In the example, the ONS 15454 SDH GNE is assigned an IP address within the central office LAN and is physically connected to the LAN through its LAN port. ONS 15454 SDH ENEs are assigned IP addresses that are outside the central office LAN and given private network IP addresses. If the ONS 15454 SDH ENEs are co-located, the craft LAN ports could be connected to a hub. However, the hub should have no other network connections.

Figure 4-14   Scenario 9: ONS 15454 SDH Proxy Server with GNE and ENEs on the same subnet
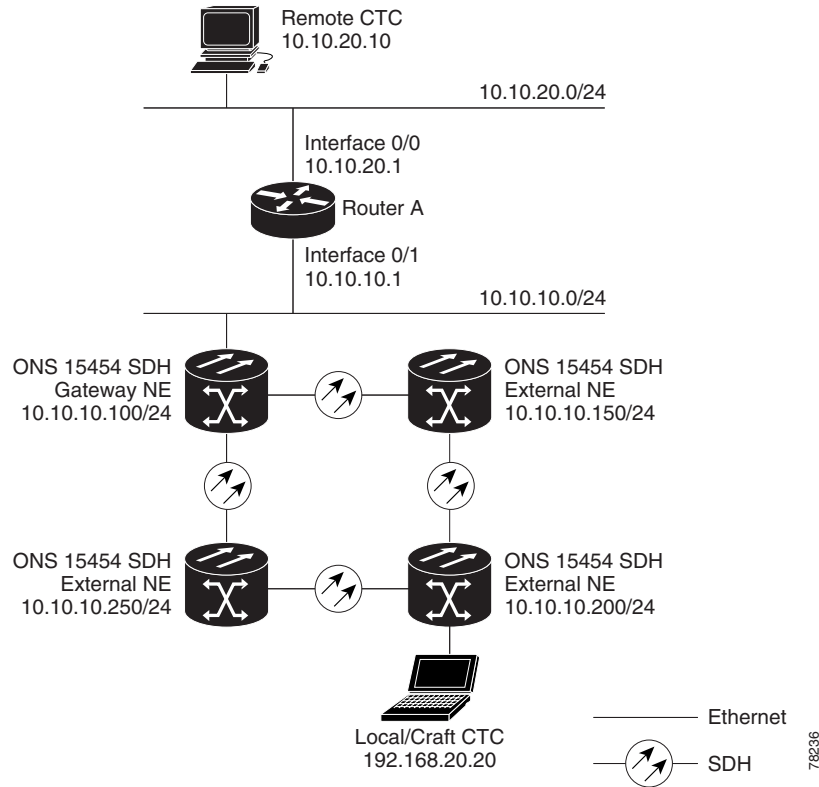
Table 4-4 shows recommended settings for ONS 15454 SDH GNEs and ENEs in the configuration shown in Figure 4-14.

Table 4-4   ONS 15454 SDH Gateway and Element NE Settings

Setting	ONS 15454 SDH Gateway NE	ONS 15454 SDH Element NE
Craft Access Only	Off	On
Enable Proxy	On	On
Enable Firewall	On	On
OSPF	Off	Off
SNTP Server (if used)	SNTP server IP address	ONS 15454 SDH GNE IP address
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15454 SDH GNE

Figure 4-15 on page 4-20 shows the same proxy server implementation with ONS 15454 SDH ENEs on different subnets. Figure 4-16 on page 4-21 shows the implementation with ONS 15454 SDH ENEs in multiple rings. In each example, ONS 15454 SDH GNEs and ENEs are provisioned with the settings shown in Table 4-4.

Figure 4-15   Scenario 9: ONS 15454 SDH Proxy Server with GNE and ENEs on different subnets

Remote CTC
10.10.20.10

10.10.20.0/24

Interface 0/0
10.10.20.1

Router A

Interface 0/1
10.10.10.1

10.10.10.0/24

ONS 15454 SDH
Gateway NE
10.10.10.100/24

ONS 15454 SDH
External NE
192.168.10.150/24

ONS 15454 SDH
External NE
192.168.10.250/24

ONS 15454 SDH
External NE
192.168.10.200/24

Local/Craft CTC
192.168.20.20

Ethernet

SDH
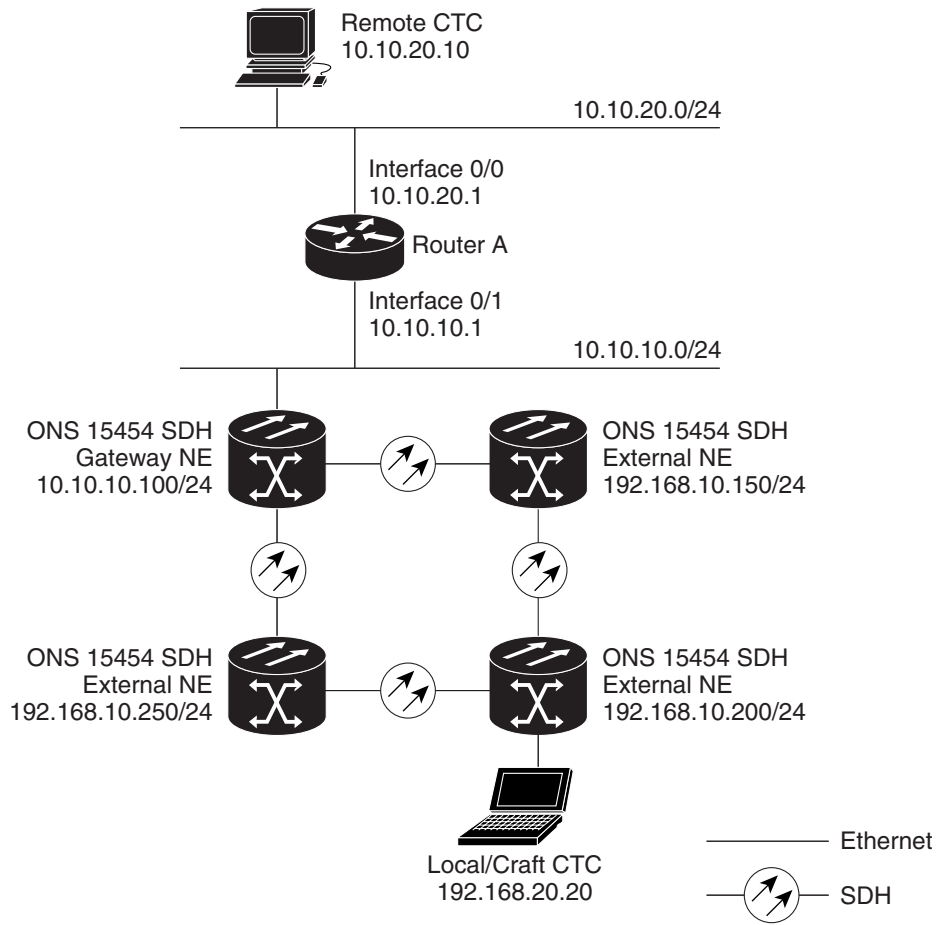
78237

Figure 4-16   Scenario 9: ONS 15454 SDH Proxy Server with ENEs on multiple rings
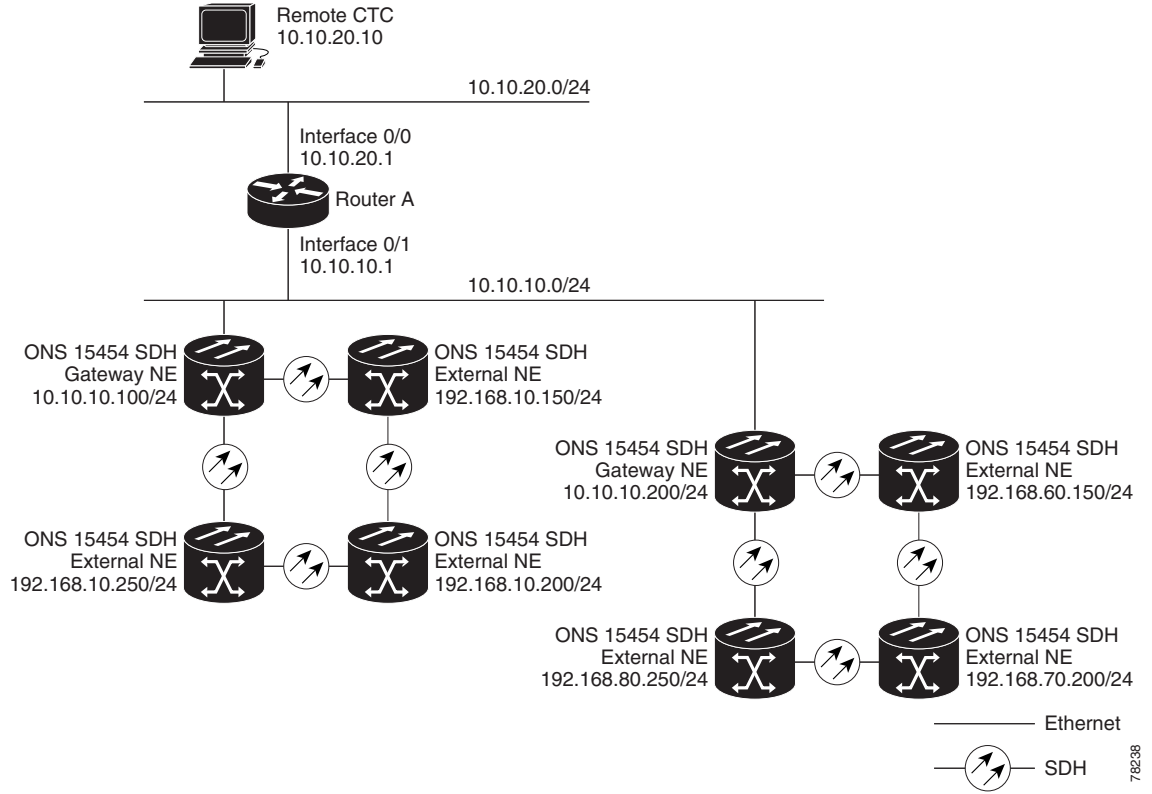
Table 4-5 shows the rules the ONS 15454 SDH follows to filter packets when Enable Firewall is enabled. If the packet is addressed to the ONS 15454 SDH, additional rules, shown in Table 4-6 on page 4-22, are applied. Rejected packets are silently discarded.

Table 4-5   Proxy Server Firewall Filtering Rules

Packets Arrive At	Accepted
TCC-I Ethernet Interface	• The ONS 15454 SDH itself • The ONS 15454 SDH's subnet broadcast address • Within the 224.0.0.0/8 network (reserved network used for standard multicast messages) • 255.255.255.255
DCC Interface	• The ONS 15454 SDH itself • An OSPF peer (another DCC-connected ONS 15454 SDH) • Within the 224.0.0.0/8 network

Table 4-6   Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15454 SDH

Packets Arrive At	Accepted	Rejected
TCC-I Ethernet Interface	• All UDP packets except those in the Rejected column	• UDP packets addressed to the SNMP trap relay port (391) are rejected.
DCC Interface	• All UDP packets • All TCP packets except those in the Rejected column • OSPF packets • ICMP packets	• TCP packets addressed to the Telnet port are rejected. • TCP packets addressed to the IO card Telnet ports are rejected. • TCP packets addressed to the proxy server port are rejected. • All other packets are rejected.

If you implement the proxy server, keep the following rules in mind:

1. All DCC-connected ONS 15454 SDH nodes on the same Ethernet segment must have the same Craft Access Only setting. Mixed values will produce unpredictable results, and may leave some nodes unreachable through the shared Ethernet segment.

2. All DCC-connected ONS 15454 SDH nodes on the same Ethernet segment must have the same Enable Firewall setting. Mixed values will produce unpredictable results. Some nodes may become unreachable.

3. All DCC-connected ONS 15454 SDH nodes in the same SDCC area must have the same Enable Firewall setting. Mixed values will produce unpredictable results. Some nodes may become unreachable.

4. If you check Enable Firewall, always check Enable Proxy. If Enable Proxy is not checked, CTC will not be able to see nodes on the DCC side of the ONS 15454 SDH.

5. If Craft Access Only is checked, check Enable Proxy. If Enable Proxy is not checked, CTC will not be able to see nodes on the DCC side of the ONS 15454 SDH.

If nodes become unreachable in cases 1 and 2, you can correct the setting by performing one of the following:

• Disconnect the craft computer from the unreachable ONS 15454 SDH. Connect to the ONS 15454 SDH through another ONS 15454 SDH in the network that has a DCC connection to the unreachable ONS 15454 SDH.

• Disconnect the Ethernet cable from the unreachable ONS 15454 SDH. Connect a CTC computer directly to the ONS 15454 SDH.

4.11 Viewing the ONS 15454 SDH Routing Table

ONS 15454 SDH routing information is displayed on the Maintenance > Routing Table tabs
(Figure 4-17). 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 SDH interface used to access the destination. Values are:

  - cpm0—The ONS 15454 SDH Ethernet interface, that is, the RJ-45 jack on the TCC-I and the LAN connectors on the MIC-C/T/P FMEC.

  - pdcc0—An SDCC interface, that is, an STM-N trunk card identified as the SDCC termination.

  - lo0—A loopback interface.

Figure 4-17   Viewing the ONS 15454 SDH routing table

Table 4-7 shows sample routing entries for an ONS 15454 SDH.

Table 4-7   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

Table 4-7   Sample Routing Table Entries (continued)

Entry	Destination	Mask	Gateway	Interface
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 SDH 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 that 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 SDH 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 that 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 that 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 an SDH 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 an SDH SDCC interface is used to reach the gateway.

5

SDH Topologies

This chapter explains how to set up the Cisco ONS 15454 SDH in different SDH topologies. Table 5-1 lists network setup topics.

Table 5-1   Network Setup Topics

5.1 Before You Begin

To avoid errors during network configuration, Cisco recommends that you draw the complete ONS 15454 SDH 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.

The ONS 15454 SDH node offers numerous types of protection. Table 5-2 on page 5-2 shows the three main categories of protection types found in a network topology.

Table 5-2   Network Protection Types

Protection Category	Protection Type	For more information
Equipment	1:1, 1+1, 1:N	"Creating Card Protection Groups" section on page 3-26
Path	Subnetwork connection protection (SNCP ring)	"Creating SNCP Rings" section on page 5-3 "Adding and Removing Nodes from an SNCP Ring" section on page 5-10
	Extended SNCP mesh networks	"Extended SNCP Mesh Networks" section on page 5-54
Line (Multiplex Section)	Automatic protection switching (APS), 1:1, 1+1, 1:N	"MS-SPRing Automatic Protection Switching" section on page 5-23 "Creating Card Protection Groups" section on page 3-26
	Multiplex section shared protection ring (MS-SPRing), two-fiber and four-fiber	"Creating MS-SPRings" section on page 5-14
	Linear add/drop multiplexers (ADM)	"Creating Linear ADM Configurations" section on page 5-47

Table 5-3 shows the number of DCCs used by each SDH ring type.

Table 5-3   ONS 15454 SDH Rings

Ring Type	Number of DCCs Per Node
SNCP Ring	2 DCCs*
2-Fiber MS-SPRing	2 DCCs*
4-Fiber MS-SPRing	2 DCCs*

* Total DCC usage must be equal to or less than 10 DCCs.

Table 5-4 is a quick reference indicating when to perform a lockout on the ONS 15454 SDH node.

Table 5-4   ONS 15454 SDH Lockout Matrix

Protection Type	XC10G Switch using CTC	Soft Reset of Active XC10G	Card Pull of Active XC10G	Soft Reset of Active TCC-I	Card Pull of Active TCC-I
Linear	No Lockout	No Lockout	Lockout Span	No Lockout	No Lockout
SNCP	No Lockout	No Lockout	Lockout[1]	No Lockout	No Lockout
2-fiber MS-SPRing	Lockout[2]	Lockout[2]	Lockout[2]	No Lockout	Lockout[2]
4-fiber MS-SPRing	Lockout[2]	Lockout[2]	Lockout[2]	No Lockout	Lockout[2]

1. Lockout all circuits originating from this node because the span card on the remote node detects AIS-P and LOP-P.

2. Lockout the spans coming to this node from the adjacent nodes. The "lockout" is applied on the adjacent node.

Note: The above lockouts do not address "Database Restore" and "Software Upgrades."

The ONS 15454 SDH is a Class 1 (CDRH) and Class 1M (IEC) laser system. Some procedures require the installation or removal of optical cards and fibers. Take appropriate safety precautions while performing these procedures.

Warning   **Voltage is present on the backplane when the system is operating. To reduce risk of an electric shock, keep hands and fingers out of the power supply bays and backplane areas.**

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.**

5.2 Creating SNCP Rings

Subnetwork connection protection (SNCP) rings provide duplicate fiber paths in the network. 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. With SNCP networks, switching occurs at the end of the path and is triggered by defects or alarms along the path.

The network can be divided into a number of interconnected subnetworks. Within each subnetwork, protection is provided at the path level and the automatic protection switching between two paths is provided at the subnetwork boundaries. The node at the end of the path and the intermediate nodes in the path select the best traffic signal. The virtual container is not terminated at the intermediate node; instead, it compares the quality of the signal on the two incoming ports and selects the better signal.

CTC automates ring configuration. SNCP network traffic is defined within the ONS 15454 SDH on a circuit-by-circuit basis. If an extended SNCP mesh network circuit is not defined within a 1+1 or MS-SPRing line protection scheme and path protection is available and specified, CTC uses an SNCP ring as the default protection mechanism.

Figure 5-1 on page 5-4 shows a basic SNCP ring configuration. If Node A sends a signal to Node C, the working signal travels on the working traffic path through Node B. The same signal is also sent on the protect traffic path through Node D. If a fiber break occurs (Figure 5-2 on page 5-4), Node C switches its active receiver to the protect signal coming through Node D.

Because each traffic path is transported around the entire ring, SNCPs are best suited for networks where traffic concentrates at one or two locations and is not widely distributed. SNCP ring capacity is equal to its bit rate. Services can originate and terminate on the same SNCP ring, or they can be passed to an adjacent access or interoffice ring for transport to the service-terminating node.

Figure 5-1   Basic, four-node, SNCP ring
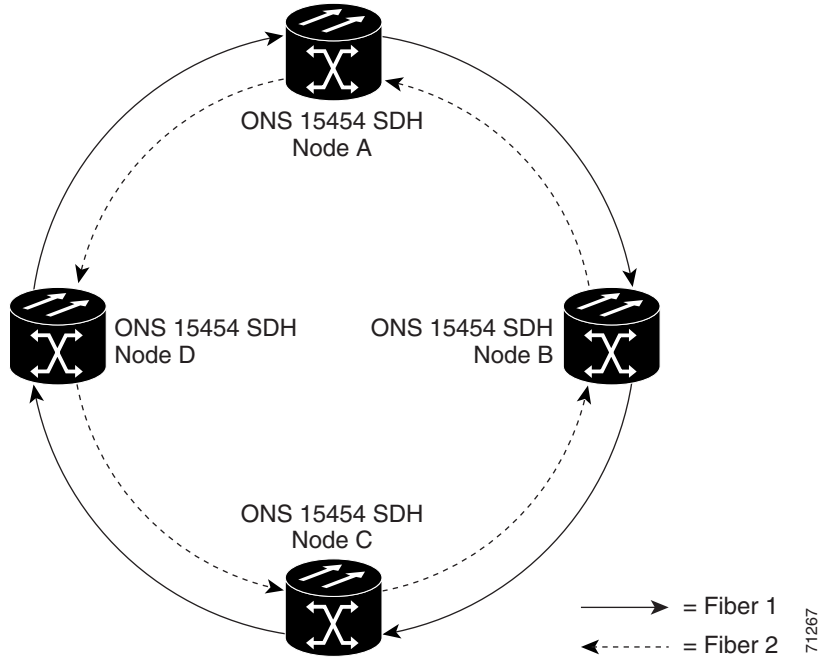
Figure 5-2   SNCP ring with a fiber break
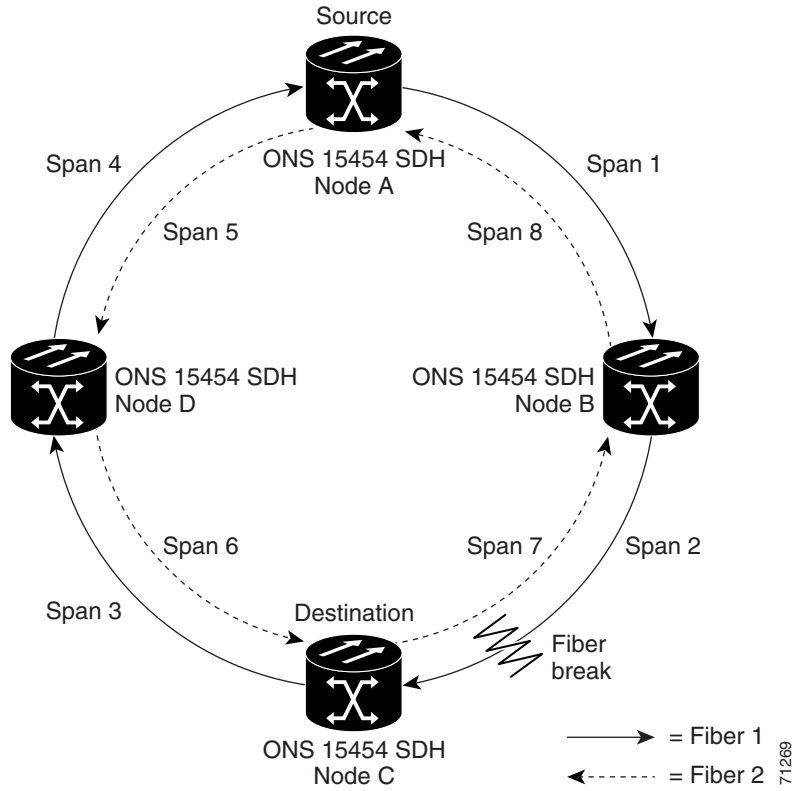
5.2.1 Sample SNCP Ring

Figure 5-3 shows a common SNCP ring application. STM-1 path circuits provide remote switch connectivity to a host V5.x switch. In the example, each remote switch requires eight E-1s to return to the host switch. Figure 5-4 on page 5-6 and Figure 5-5 on page 5-6 show the shelf layout for each node in the example.

Figure 5-3   STM-1 SNCP ring
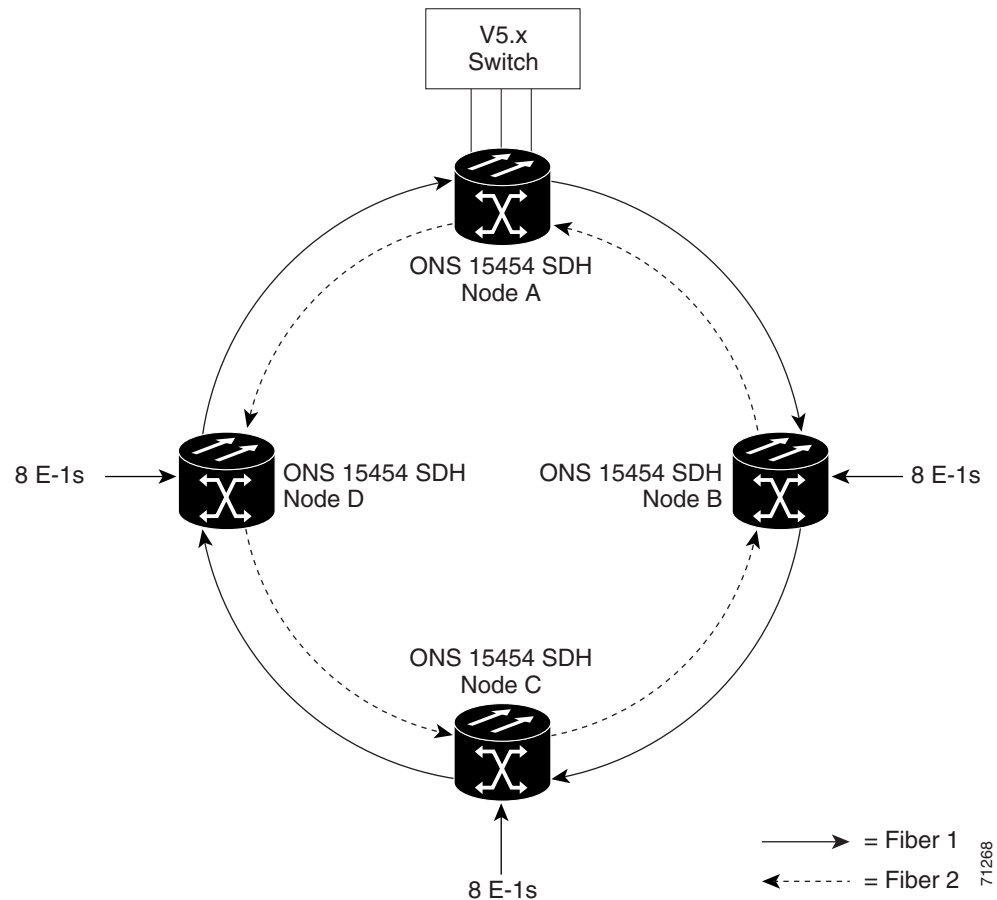
Node A has four E1-14 cards to provide 56 active E-1 ports. The other sites only require two E1-14 cards to carry the eight E-1s to and from the remote switch. You can use the other half of each ONS 15454 SDH shelf assembly to provide support for a second or third ring to other existing or planned remote sites.

In this sample STM-1 SNCP ring, Node A contains four E1-14 cards and two STM-1 cards. Six free slots are available, which you can provision with cards or leave empty.

Note   Fill unused card slots with a blank faceplate (Cisco P/N 15454E-BLANK). The blank faceplate ensures proper airflow when operating the ONS 15454 SDH.

Figure 5-4 on page 5-6 shows the shelf setup for these cards.

Figure 5-4   Card setup of Node A in the STM-1 SNCP ring example
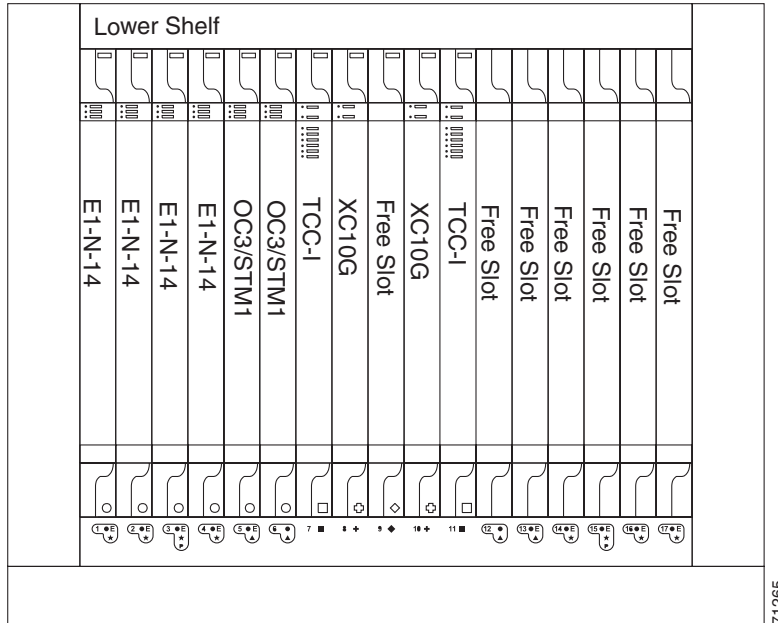
In Figure 5-3 on page 5-5, Nodes B through D each contain two E1-14 cards and two STM-1 cards. Eight free slots are available that you can provision with other cards or leave empty. Figure 5-5 shows the shelf assembly setup for this sample configuration.

Figure 5-5   Card setup of Nodes B through D in the STM-1 SNCP ring example
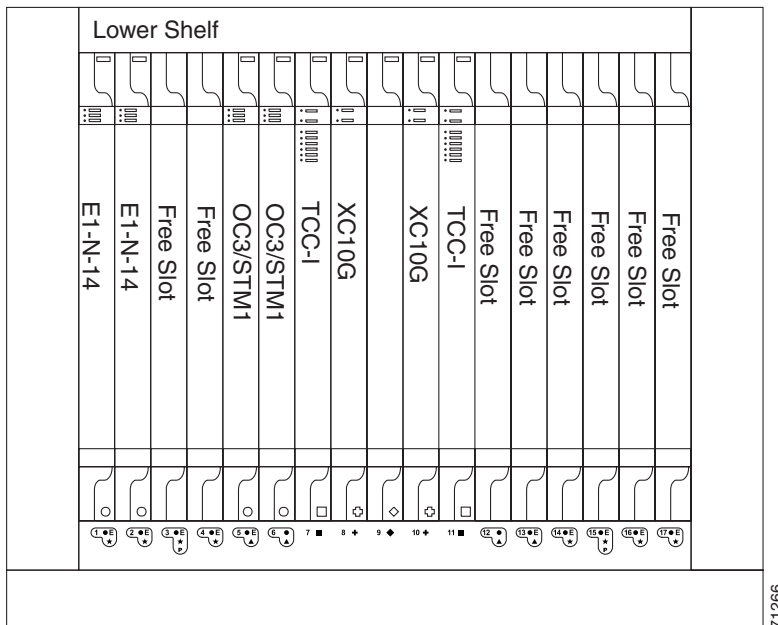
5.2.2 Setting Up an SNCP Ring

To set up an SNCP ring, perform five basic procedures:

Step 1   Complete the "Install the SNCP Ring Trunk Cards" procedure on page 5-7.

Step 2   Complete the "Configure the SNCP Ring DCC Terminations and Place Ports in Service" procedure on page 5-8.

Step 3   Configure the timing. See the "Set Up External, Line, or Mixed Timing for the ONS 15454 SDH" procedure on page 3-21 or the "Set Up Internal Timing for the ONS 15454 SDH" procedure on page 3-24.

Step 4   After configuring the timing, set up the SNCP circuits. SNCP signal thresholds—the levels that determine when the SNCP path is switched—are set at the circuit level. To create SNCP circuits, see Chapter 6, "Circuits and Tunnels."

Step 5   Repeat Step 1 to Step 4 to configure additional nodes. To create an extended SNCP mesh network, see the "Extended SNCP Mesh Networks" section on page 5-54. To create circuits, see the "Creating VC High-Order Path Circuits" section on page 6-3.

Procedure: Install the SNCP Ring Trunk Cards

⚠️

Caution   Always wear an authorized ESD wrist band when removing or installing ONS 15454 SDH cards.

Purpose	Install the SNCP ring trunk cards as the first step in setting up an SNCP ring.
Tools/Equipment	You will need all STM-N cards that you will use in the SNCP ring.
Onsite/Remote	Onsite

Step 1   Install the STM-N cards that you will use as the SNCP trunk cards. You can install the STM-1, STM-4, and STM-16 cards in Slots 1 to 6 and 12 to 17. The STM-64 card can only be installed in Slots 5, 6, 12, or 13.

Step 2   Allow the cards to boot. For more information about installing cards, see the "Optical, Electrical, and Ethernet Card Installation" section on page 1-35.

Step 3   Attach the fiber to the west and east STM-N card ports at each node as follows. Refer to Figure 5-6 on page 5-8 while installing the fiber.

- To avoid errors, make the west port the farthest slot to the left and the east port the farthest slot to the right.

- Plug fiber from a west port at one node into the east port on the adjacent node. Figure 5-6 on page 5-8 shows fiber connections for a four-node SNCP ring with trunk cards in Slot 5 (west) and Slot 12 (east).

- Plug fiber from the transmit (Tx) connector of an STM-N card at one node into the receive (Rx) connector of an STM-N card at the adjacent node. The card displays a signal failure (SF) LED if Tx and Rx fibers are mismatched after the DCCs are on and the ports are in service.

Figure 5-6   Connecting fiber to a four-node SNCP ring
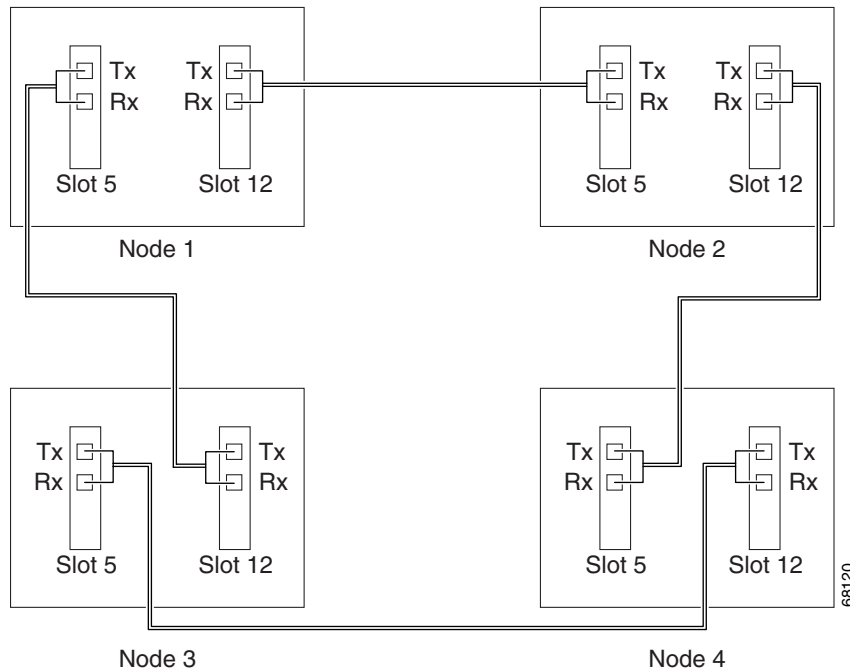
Procedure: Configure the SNCP Ring DCC Terminations and Place Ports in Service

Note   The SDH and SONET versions of the Cisco ONS 15454 do not interoperate via DCC.

Purpose	Create the DCC terminations and place ports in service after installing the STM-N cards.
Prerequisite Procedures	"Install the SNCP Ring Trunk Cards" procedure on page 5-7
Onsite/Remote	Onsite or remote

Step 1   Start CTC for the first node that you will provision for the SNCP.

Step 2   Click the **Provisioning > SDH DCC** tabs.

Step 3   In the SDCC Terminations section, click **Create**.

Step 4   In the Create SDCC Terminations dialog box, press the **Ctrl** key and click the two slots/ports that will serve as the SNCP ports at the node. For example, Slot 5 (STM-16)/Port 1 and Slot 14 (STM-16)/Port 1.

Figure 5-7   Creating SDCC terminations
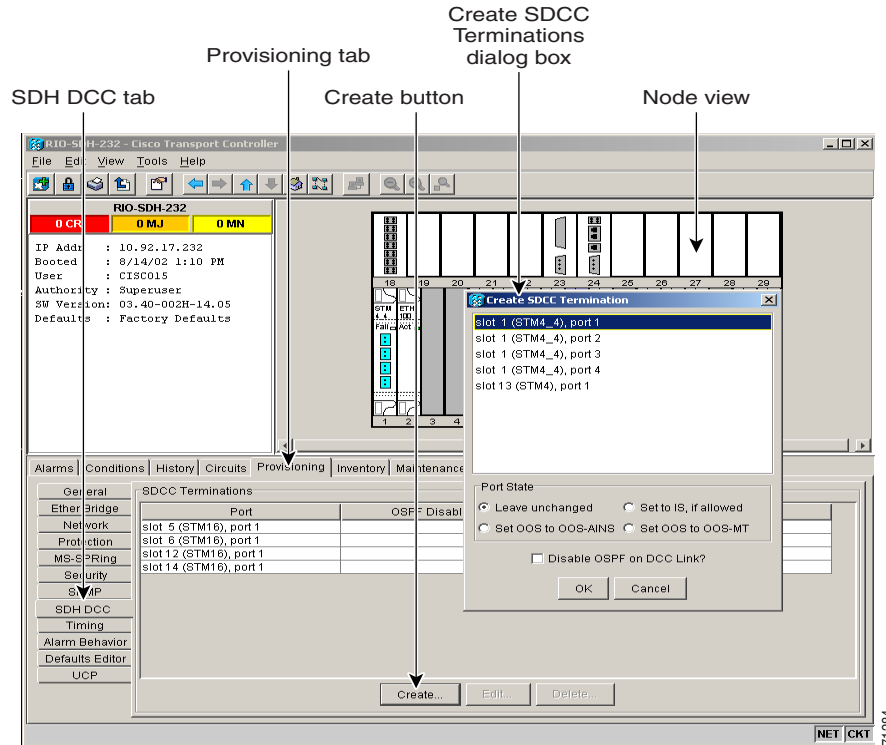
Step 5   Select the **Set to IS, if allowed** radio button. This radio button places the trunk card ports in service.

Note   There are four port state options. Select the port state that best fits your requirements. For example, you can select the set OOS to OOS-MT radio button if you are provisioning the SNCP before installing cards and fiber. Also, you can select the OOS-MT port state if you want to avoid DCC termination alarms until you configure all DCCs on the SNCP.

Note   Below the port state options you can also enable or disable OSPF on the DCC according to your requirements.

Step 6   Click **OK**.

Step 7   The slots and ports appear in the SDCC Terminations list.

Step 8   Complete Step 3 to 6 at each node that will be in the SNCP.

Note   The ONS 15454 SDH uses the SDH regenerator section DCC (SDCC) for data communications. It does not use the multiplex section DCCs; therefore, the multiplex section DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 SDH networks. For more detail, see the "Creating DCC Tunnels" section on page 6-34.

Step 9 After configuring the SDH DCC, set the timing for the node. For procedures, see the "Setting Up ONS 15454 SDH Timing" section on page 3-18.

5.3 Adding and Removing Nodes from an SNCP Ring

This section explains how to add and remove nodes in an ONS 15454 SDH SNCP ring configuration. To add or remove a node in an SNCP ring, perform two basic procedures:

Step 1 Switch traffic on the effected spans to route traffic away from the area of the ring where service will be performed. See the "Switch SNCP Ring Traffic" procedure on page 5-10.

Step 2 Add or remove an SNCP node.

- To add an SNCP node, see the "Add an SNCP Node" procedure on page 5-12.
- To remove an SNCP node, see the "Remove an SNCP Node" procedure on page 5-13.

Procedure: Switch SNCP Ring Traffic

Purpose	Use this procedure to route traffic away from the area of the ring where service will be performed by switching traffic on the effected spans.
Prerequisite Procedures	This procedure assumes that you are adding or removing a node from an existing SNCP ring.
Onsite/Remote	Onsite or remote

Step 1 From CTC, display the network view.

Step 2 Right-click the span that will be cut to add or delete a node and choose **Circuits** from the shortcut menu (Figure 5-8).

Figure 5-8   Using the span shortcut menu to display circuits
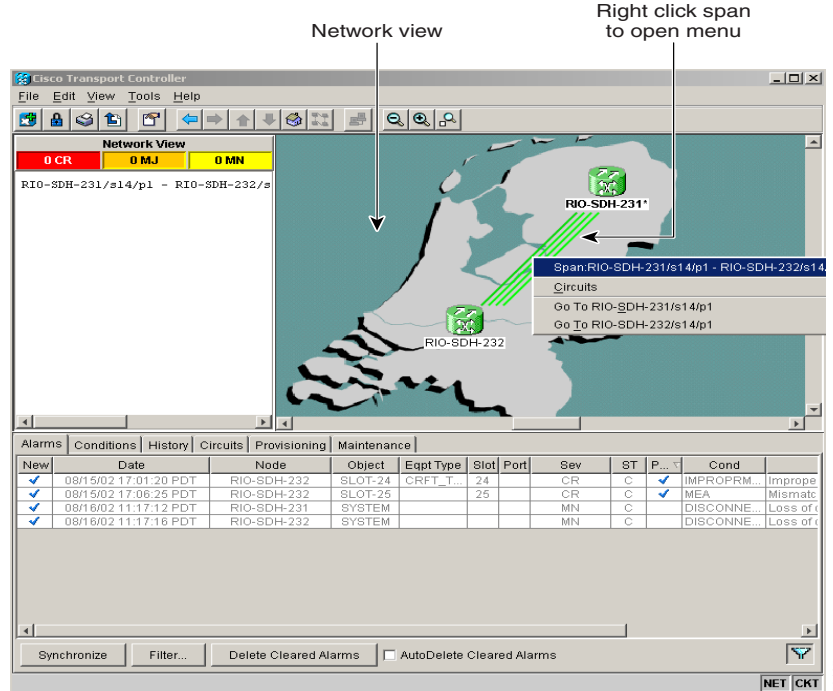
Step 3   In the Circuits on Span dialog box (Figure 5-9 on page 5-12), choose a protection option from the
Perform SNCP span switching menu from the following choices:

- **CLEAR**—Removes a previously set switch command.

- **MANUAL_SWITCH AWAY**—Switches the span if the new span is error free.

- **FORCE_SWITCH AWAY**—Forces the span to switch, even if the path has signal degrade (SD) or
  signal failure (SF) conditions. Force switch states have a higher priority than manual switches.

- **LOCKOUT OF PROTECTION**—Prevents traffic from switching to the protect circuit path under
  any circumstances. Of all switch states, Lockout has the highest priority.

⚠

Caution   Force and lockout commands override normal protective switching mechanisms. Applying these
commands incorrectly can cause traffic outages.

Figure 5-9   Switching SNCP circuits
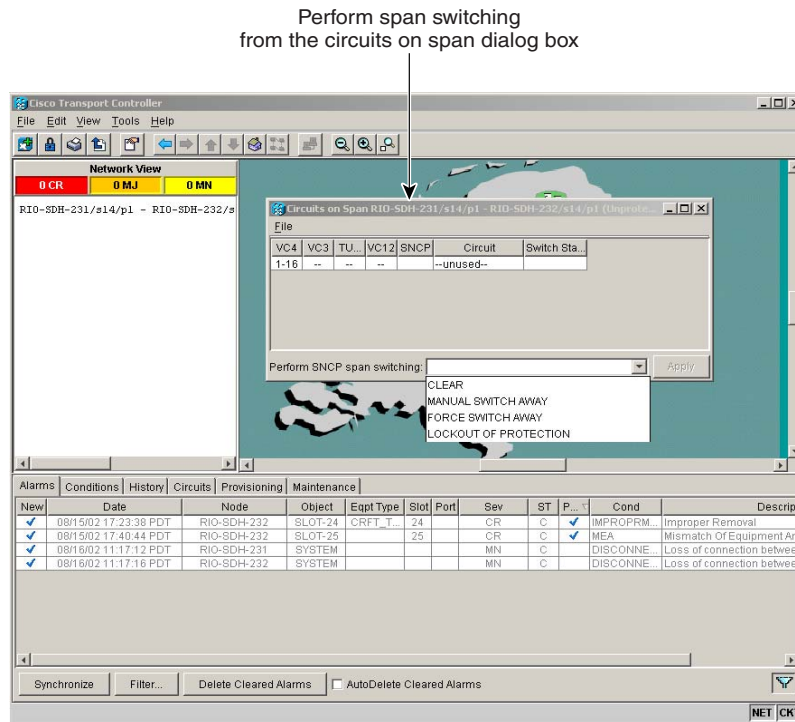
Step 4   Click Apply.

Step 5   When the confirmation dialog box appears, click **Yes** 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 an SNCP Node

Purpose	This procedure explains how to add SNCP nodes. You can only add one node at a time.
Prerequisite Procedures	"Switch SNCP Ring Traffic" procedure on page 5-10
Onsite/Remote	Onsite only

Step 1   Start CTC for one of the SNCP ring nodes and display the network view.

Step 2   Clear any alarms or conditions on the ring nodes. See the "Check for Alarms" procedure on page 5-57.

Step 3   At the node that you will add to the SNCP, complete the following steps:

    a.   Verify that the STM-N cards are installed and fiber is available to connect to the other nodes.

    b.   Run test traffic through the cards that will connect to the SNCP.

    c.   Complete the "Setting Up an SNCP Ring" procedure on page 5-7 to provision the new node.

Step 4   Start CTC for a node that will physically connect to the new node.

Step 5 See the "Switch SNCP Ring Traffic" procedure on page 5-10 to initiate a FORCE switch to move traffic away from the span that will connect to the new node.

⚠

Caution Traffic is not protected during a protection switch.

Step 6 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 7 Replace the removed fiber connections with connections from the new node.

✎

Note Perform Step 7 on site at the new node.

Step 8 Log out of CTC and then log back into the new node in the ring.

Step 9 Display the network view. The new node should appear in the network view. Wait for a few minutes to allow all the nodes to appear.

Step 10 Click the **Circuits** tab and wait for all the circuits to appear, including spans. Circuits that will pass through the new node display as **incomplete**.

Step 11 In the network view, right-click the new node and choose **Update Circuits With New Node** from the list of options.

Step 12 Click the **Circuits** tab and verify that no incomplete circuits are displayed. If incomplete circuits are displayed, repeat Step 10.

Step 13 Use the "Switch SNCP Ring Traffic" procedure on page 5-10 to clear the protection switch.

Procedure: Remove an SNCP Node

⚠

Caution Although the following procedure is designed to minimize traffic outages while nodes are removed, traffic will be lost when you delete and recreate circuits that passed through the removed node.

Purpose	This procedure explains how to remove SNCP nodes.
Prerequisite Procedures	"Switch SNCP Ring Traffic" procedure on page 5-10
Onsite/Remote	Perform these steps onsite and not from a remote location.

Step 1 Start CTC for one of the SNCP ring nodes and display the network view. Clear any alarms or conditions on the ring nodes. See the "Check for Alarms" procedure on page 5-57.

Step 2 Complete the "Switch SNCP Ring Traffic" procedure on page 5-10 to initiate a FORCE switch to move traffic away from the node you will remove. 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   Log into the node that you will remove. If you are already logged in, display the node view.

Step 4   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. Choose the circuit(s) to delete. To choose multiple circuits, press the **Shift** or **Ctrl** key while selecting circuits.

c. Click **Delete**.

d. Click **Yes** when prompted.

Step 5   From the node that will be deleted, remove the east and west span fibers. At this point, the node is no longer a part of the ring.

Step 6   Reconnect the span fibers of the nodes remaining in the ring.

Step 7   Log out of CTC and then log back into a node in the ring.

Step 8   Click the **Alarms** tab of each newly connected node and verify that the span cards are free of alarms. Resolve any alarms before proceeding.

Step 9   If the removed node was the building integrated timing supply (BITS), select a new node as the BITS source or select another node as the master timing node.

Step 10   See the "Switch SNCP Ring Traffic" procedure on page 5-10 to clear the protection switch.

5.4 Creating MS-SPRings

MS-SPRings share the ring bandwidth equally between working and protection traffic. Half of the payload bandwidth is reserved for protection in each direction, making the communication pipe half-full under normal operation.

There are two types of MS-SPRings: two-fiber and four-fiber. Two-fiber MS-SPRings share service and protection equally, but only two physical fibers are required. For more information, see the "Two-Fiber Multiplex Section Shared Protection Ring" section on page 5-16. With four-fiber MS-SPRings, the nodes on both sides of the failed span perform a span switch and use the second pair of fibers as the new working route. For more information, see the "Four-Fiber MS-SPRings" section on page 5-21.

An MS-SPRing node can terminate traffic it receives from either side of the ring. Therefore, MS-SPRings are suited for distributed node-to-node traffic applications such as interoffice networks and access networks.

MS-SPRings allow bandwidth to be reused around the ring and can carry more traffic than a network with traffic flowing through one central hub. MS-SPRings can also carry more traffic than an SNCP operating at the same STM-N rate. Table 5-5 shows the bidirectional bandwidth capacities of two-fiber MS-SPRings. The capacity is the STM-N rate divided by two, multiplied by the number of nodes in the ring and minus the number of pass-through VC4 circuits.

Table 5-5   Two-Fiber MS-SPRing Capacity

STM Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
STM-4	VC4 1-2	VC4 3-4	$2 \times N^{1} - PT^{2}$
STM-16	VC4 1-8	VC4 9-16	$8 \times N - PT$
STM-64	VC4 1-32	VC4 33-64	$32 \times N - PT$

1. N equals the number of ONS 15454 SDH nodes configured as MS-SPRing nodes.

2. PT equals the number of VC4 circuits passed through ONS 15454 SDH nodes in the ring. (Capacity can vary depending on the traffic pattern.)

Table 5-6 shows the bidirectional bandwidth capacities of four-fiber MS-SPRings.

Table 5-6   Four-Fiber MS-SPRing Capacity

STM Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
STM-16	VC4 1-16 (Fiber 1)	VC4 1-16 (Fiber 2)	$16 \times N - PT$
STM-64	VC4 1-64 (Fiber 1)	VC4 1-64 (Fiber 2)	$64 \times N - PT$

Figure 5-10 shows an example of MS-SPRing bandwidth reuse. The same VC4 carries three different traffic sets simultaneously on different spans on the ring: one set from Node 3 to Node 1, one set from Node 1 to Node 2, and another set from Node 2 to Node 3.

Figure 5-10   MS-SPRing bandwidth reuse
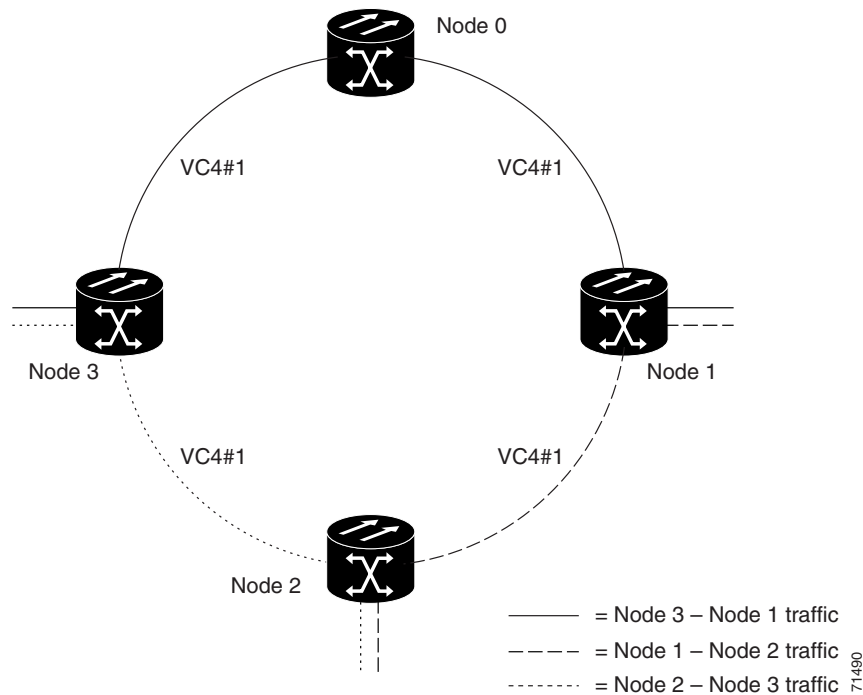
5.4.1 Two-Fiber Multiplex Section Shared Protection Ring

The ONS 15454 SDH can support a number of ring combinations if the total DCC usage is equal to or less than 10 DCCs. Each MS-SPRing can have up to 16 ONS 15454 SDH nodes. Because the working and protect bandwidths must be equal, you can create only STM-4 (two-fiber only), STM-16, or STM-64 MS-SPRings.

Note   MS-SPRings with 16 or fewer nodes meet the ITU-T G.841 switch time requirement.

In two-fiber MS-SPRings, each fiber is divided into working and protect bandwidths. For example, in an STM-16 MS-SPRing (Figure 5-11), VC4s 1 to 8 carry the working traffic, and VC4s 9 to 16 are reserved for protection. Working traffic (VC4s 1 to 8) travels in one direction on one fiber and in the opposite direction on the second fiber. The CTC circuit routing routines calculate the shortest path for circuits based on requirements set by the circuit provisioner, traffic patterns, and distance. For example, in Figure 5-11, circuits going from Node 0 to Node 1 typically travel on Fiber 1, unless that fiber is full, in which case circuits are routed on Fiber 2 through Node 3 and Node 2. Traffic from Node 0 to Node 2 (or Node 1 to Node 3), can be routed on either fiber, depending on circuit provisioning requirements and traffic loads.

Figure 5-11   Four-node, two-fiber MS-SPRing
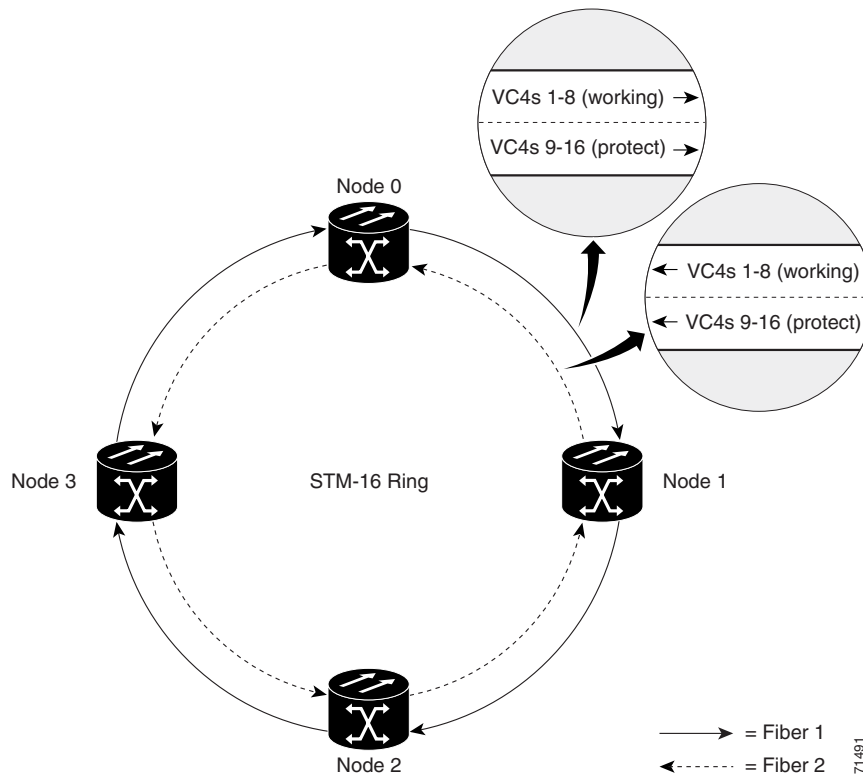
The SDH K1 and K2 bytes carry the information that governs MS-SPRing protection switches. Each MS-SPRing node monitors the K bytes to determine when to switch the SDH signal to an alternate physical path. The K bytes communicate failure conditions and actions taken between nodes in the ring.

If a break occurs on one fiber, working traffic that was targeted for a node beyond the break switches to the protect bandwidth on the second fiber. The traffic travels in the reverse direction on the protect bandwidth until it reaches its destination node. At that point, traffic is switched back to the working bandwidth.

Figure 5-12 shows a sample traffic pattern on a four-node, two-fiber MS-SPRing.

Figure 5-12   Four-node, two-fiber MS-SPRing sample traffic pattern
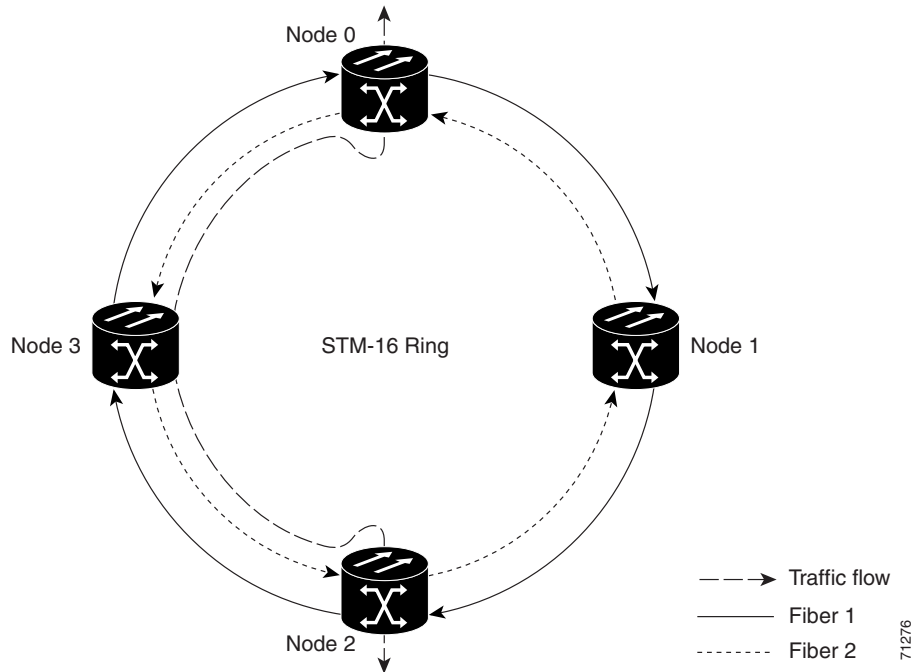
Figure 5-13 on page 5-18 shows how traffic is rerouted after a line break between Node 0 and Node 3.

- All circuits originating on Node 0 and carried to Node 2 on Fiber 2 are switched to the protect bandwidth of Fiber 1. For example, a circuit carried on VC4-1 on Fiber 2 is switched to VC4-9 on Fiber 1. A circuit carried on VC4-2 on Fiber 2 is switched to VC4-10 on Fiber 1. Fiber 1 carries the circuit to Node 3 (the original routing destination). Node 3 switches the circuit back to VC4-1 on Fiber 2 where it is routed to Node 2 on VC4-1.

- 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 VC4-2 on Fiber 1 is switched to VC4-10 on Fiber 2. Fiber 2 carries the circuit to Node 0 where the circuit is switched back to VC4-2 on Fiber 1 and then dropped to its destination.

Figure 5-13   Four-node, two-fiber MS-SPRing traffic pattern following line break
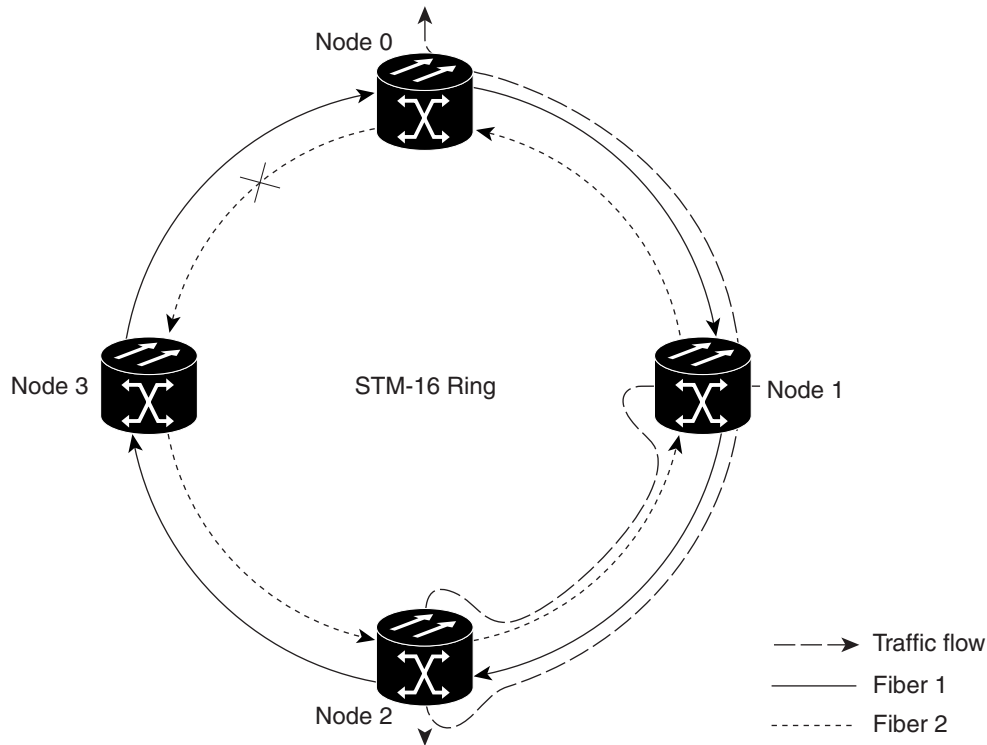
5.4.1.1 Sample MS-SPRing Application

Figure 5-14 shows a sample two-fiber MS-SPRing 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 E-3s over two STM-1 spans to Node 0. Carrier 2 provides twelve E-3s directly. Node 0 receives the signals and delivers them around the ring to the appropriate node.

- The ring also brings 14 E-1s back from each remote site to Node 0. Intermediate nodes serve these shorter regional connections.

- The ONS 15454 SDH STM-1 card supports a total of four STM-1 ports so that two additional STM-1 spans can be added at little cost.

Figure 5-14   Five-node MS-SPRing
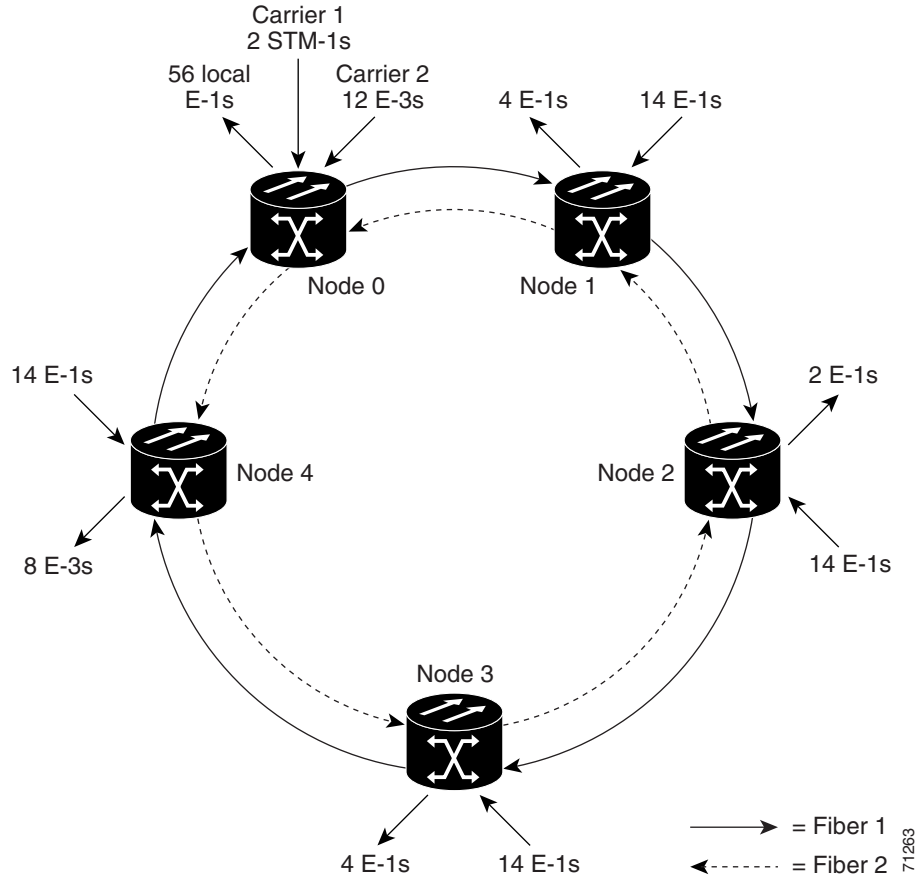
Figure 5-15 shows the shelf assembly layout for Node 0, which has one free slot. Figure 5-16 shows the shelf assembly layout for the remaining sites in the ring. In this MS-SPRing configuration, an additional eight E-3s at Node IDs 1 and 3 can be activated. An additional four E-3s can be added at Node ID 4, and ten E-3s can be added at Node ID 2. Each site has free slots for future traffic needs.

Figure 5-15   Shelf assembly layout for Node 0 in Figure 5-14

Lower Shelf

E1-N-14 | E1-N-14 | E1-N-14 | E1-N-14 | E1-N-14 | Free Slot | TCC-I | XC10G | Free Slot | XC10G | TCC-I | OC48/STM16 | OC48/STM16 | OC3/STM1 | OC3/STM1 | E3-12 | E3-12

71270
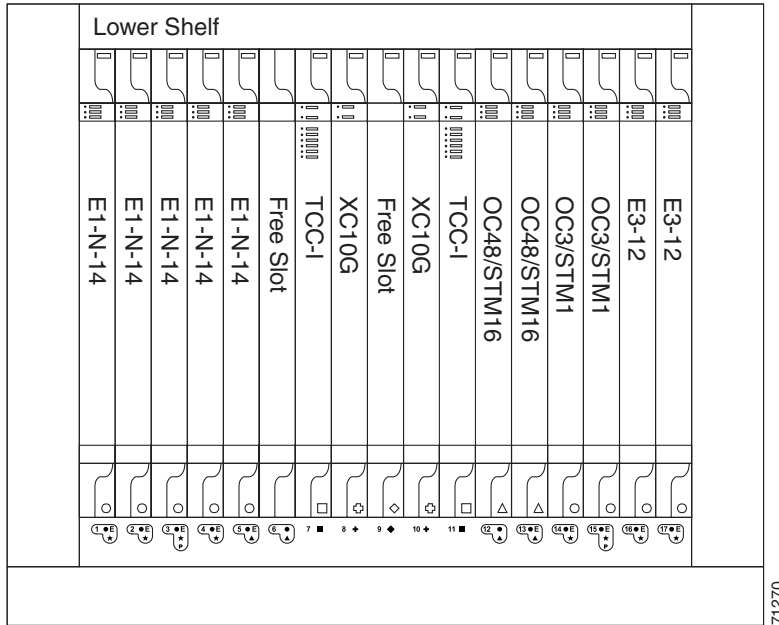
Figure 5-16   Shelf assembly layout for Nodes 1 to 4 in Figure 5-14

Lower Shelf

E1-N-14 | E1-N-14 | Free Slot | Free Slot | Free Slot | Free Slot | TCC-I | XC10G | Free Slot | XC10G | TCC-I | OC48/STM16 | OC48/STM16 | Free Slot | Free Slot | E3-12 | E3-12

71264
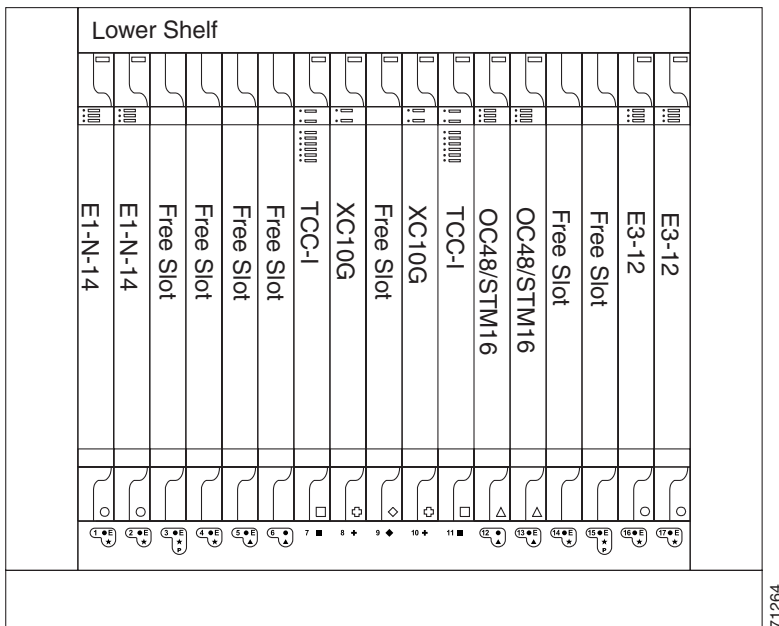
5.4.2 Four-Fiber MS-SPRings

The ONS 15454 SDH can support many ring combinations if the total DCC usage is equal to or less than 10 DCCs. Each MS-SPRing can have up to 16 ONS 15454 SDH nodes. Because the working and protect bandwidths must be equal, you can create only STM-16 or STM-64 MS-SPRings.

Note MS-SPRings with 16 or fewer nodes meet the ITU-T G.841 switch time requirement.

Four-fiber MS-SPRings double the bandwidth of two-fiber MS-SPRings. Four-fiber MS-SPRings increase the reliability and flexibility of traffic protection because they allow span switching as well as ring switching. Two fibers are allocated for working traffic and two fibers for protection, as shown in Figure 5-17. To implement a four-fiber MS-SPRing, you must install four STM-16 cards or four STM-64 cards at each MS-SPRing node.

Figure 5-17   Four-node, four-fiber MS-SPRing
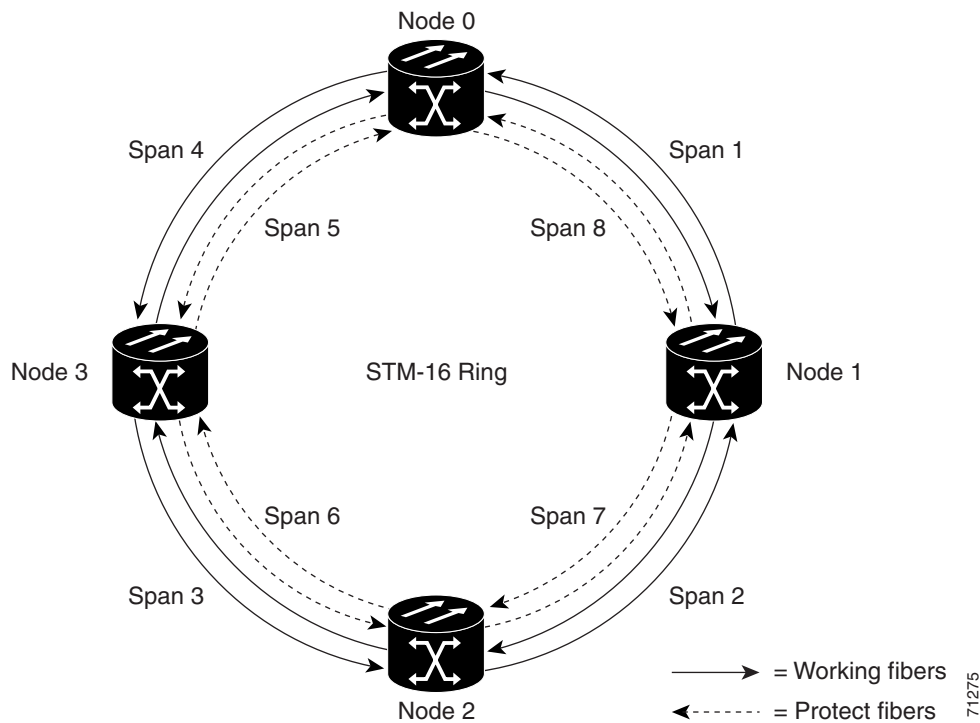
Four-fiber MS-SPRings provide span and ring switching:

- Span switching occurs when a working span fails (Figure 5-18 on page 5-22). Traffic switches to the protect fibers between the nodes (Node 0 and Node 1 in the Figure 5-18 example) and then returns to the working fibers that did not fail. Multiple span switches can occur at the same time.

- Ring switching occurs when a span switch cannot recover traffic (Figure 5-19 on page 5-22), 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 5-18   Four-fiber MS-SPRing span switch

Node 0

Span 4

Span 5

Span 8

Span 1

STM-16 Ring

Node 3

Node 1

Span 6

Span 7

Span 3

Span 2

= Working fibers

= Protect fibers

Node 2

71278
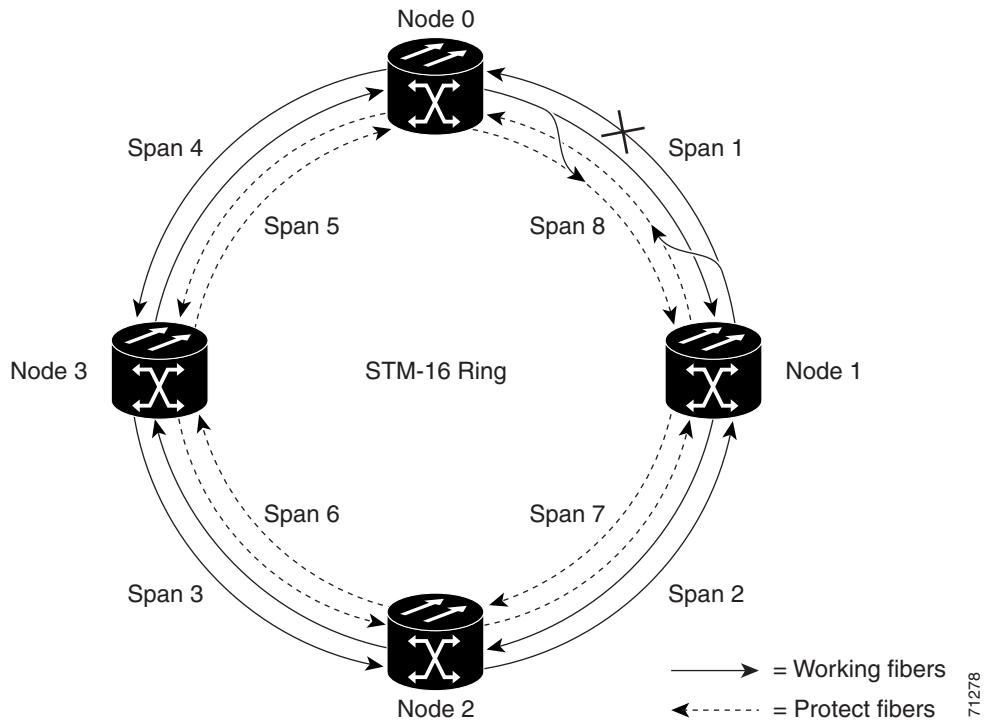
Figure 5-19   Four-fiber MS-SPRing switch

Node 0

Span 4

Span 5

Span 8

Span 1

STM-16 Ring

Node 3

Node 1

Span 6

Span 7

Span 3

Span 2

= Working fibers

= Protect fibers

Node 2

71279
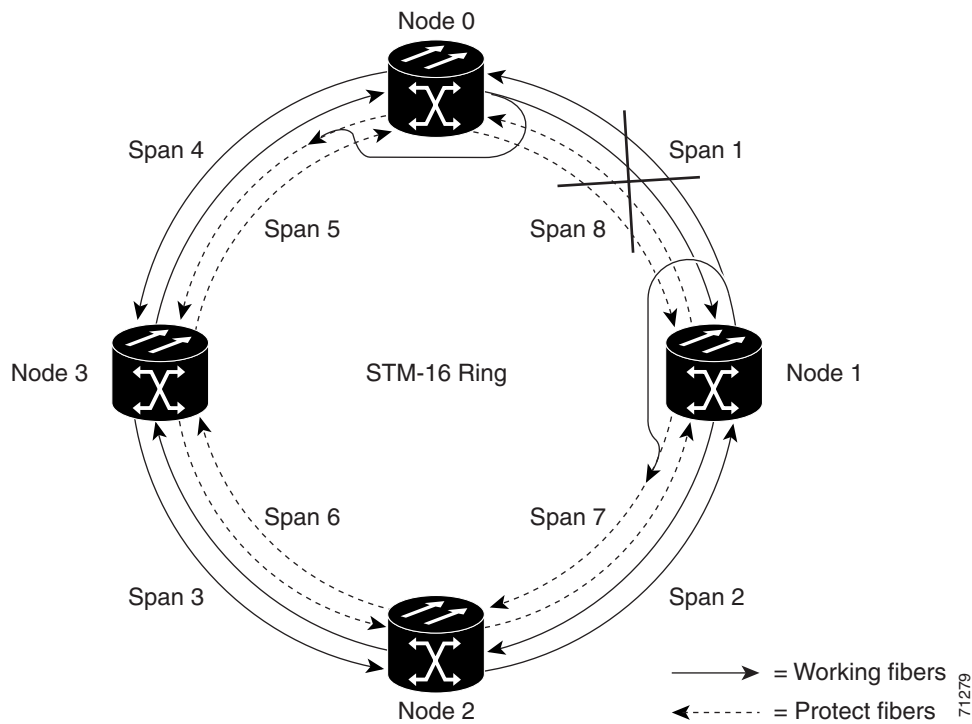
5.4.3 MS-SPRing Automatic Protection Switching

The ONS 15454 SDH uses the K3 overhead byte for MS-SPRing APS to allow an ONS 15454 SDH MS-SPRing to have more than 16 nodes. If an MS-SPRing is routed through third-party equipment that cannot transparently transport the K3 byte, you can remap the ring to either the Z2, E2, or F1 byte on STM-16 cards. (K3 byte remapping is not available on any STM-N cards other than STM-16.) If you remap the K3 byte, you must remap it to the same byte on each MS-SPRing trunk card that connects to the third-party equipment. All other MS-SPRing trunk cards should remain mapped to the K3.

For example, in Figure 5-20, an MS-SPRing span between Node 2 and Node 4 passes through third-party equipment. Because this equipment cannot transparently transport the K3 byte, the STM-16 card at Node 2/Slot 12 and the STM-16 card at Node 4/Slot 5 are provisioned to use an alternate byte. Other MS-SPRing trunk cards are not changed.

Figure 5-20   MS-SPRing with a remapped K3 byte
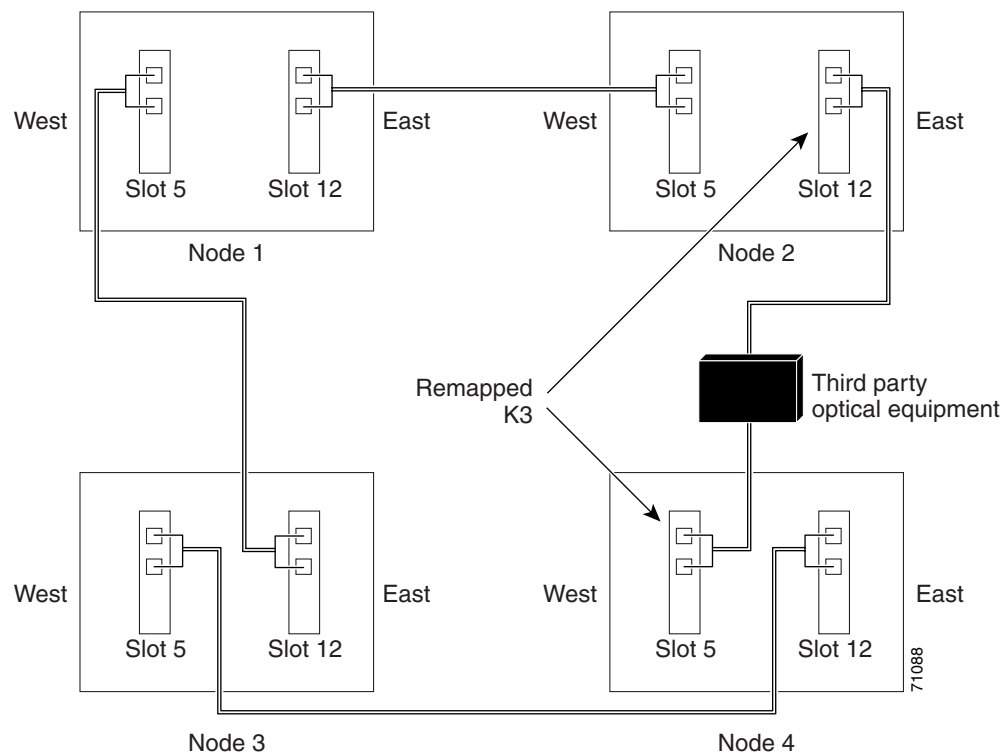
Do not perform K3 byte remapping unless a remap is required to provision an MS-SPRing that uses third-party equipment. See the "Remap the K3 Byte" procedure on page 5-28 as needed.

5.4.4 Setting Up MS-SPRings

To set up an MS-SPRing on the ONS 15454 SDH, perform the following procedures:

Step 1 Complete the "Install the MS-SPRing Trunk Cards" procedure on page 5-24.

Step 2 Complete the "Create the MS-SPRing DCC Terminations and Place Ports in Service" procedure on page 5-26.

Step 3 Set up MS-SPRing timing. See the "Set Up External, Line, or Mixed Timing for the ONS 15454 SDH" procedure on page 3-21 or the "Set Up Internal Timing for the ONS 15454 SDH" procedure on page 3-24.

Step 4 If an MS-SPRing span passes through equipment that cannot transparently transport the K3 byte, remap the MS-SPRing extension byte on the trunk cards at each end of the span. See the "Remap the K3 Byte" procedure on page 5-28.

Step 5 Complete the "Provision the MS-SPRing Using the Wizard" procedure on page 5-28.

Procedure: Install the MS-SPRing Trunk Cards

⚠
Caution Always wear an authorized ESD wrist band when removing or installing ONS 15454 SDH cards.

Purpose	To set up an MS-SPRing on the ONS 15454 SDH, you must first use this procedure to install the MS-SPRing trunk cards.
Tools/Equipment	All STM-N cards that will be used in the MS-SPRing.
Onsite/Remote	Onsite

Step 1 Install the STM-4, STM-16, or STM-64 cards that will serve as the MS-SPRing trunk cards. You can install the STM-4 and STM-16 cards in Slots 1 to 6 and 12 to 17. The STM-64 card can only be installed in Slots 5, 6, 12, or 13.

Step 2 Allow the cards to boot. For more information about installing cards, see the "Optical, Electrical, and Ethernet Card Installation" section on page 1-35.

Step 3 Attach the fiber to the east and west MS-SPRing ports at each node.

- To avoid errors, make the west port the farthest slot to the left and the east port the farthest slot to the right.
- Plug fiber from a west port at one node into the east port on the adjacent node. Figure 5-21 on page 5-25 shows fiber connections for a two-fiber MS-SPRing with trunk cards in Slot 5 (west) and Slot 12 (east).

Figure 5-21   Connecting fiber to a four-node, two-fiber MS-SPRing
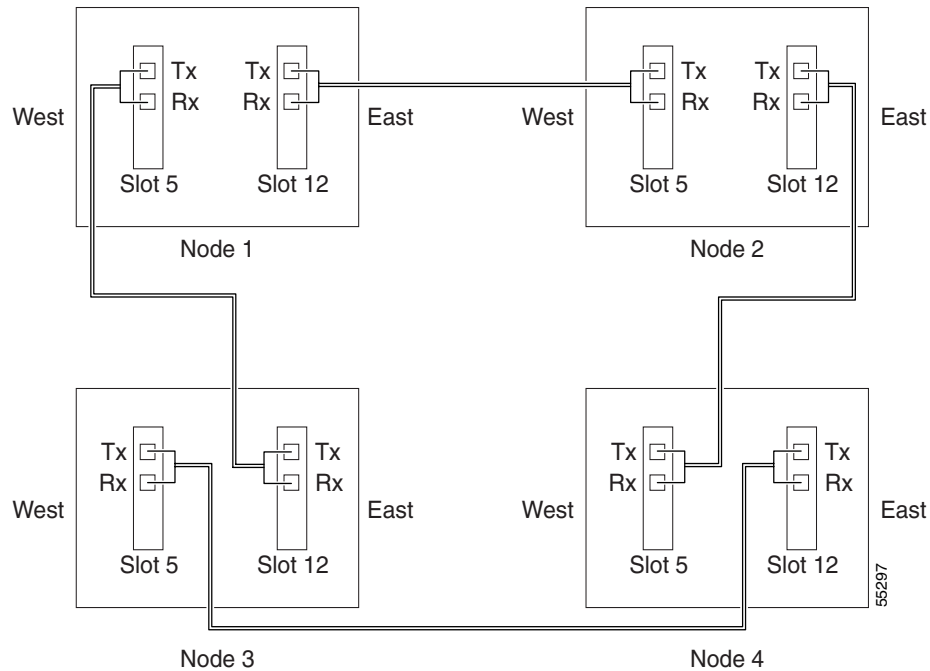
- Plug fiber from the transmit (Tx) connector of an STM-N card at one node into the receive (Rx) connector of an STM-N card at the adjacent node. The card displays an SF LED if Tx and Rx fibers are mismatched after the DCCs are created and the ports are in service.

- For four-fiber MS-SPRings, use the same east/west connection pattern for the working and protect fibers. Do not mix working and protect card connections. The MS-SPRing will not function if working and protect cards are interconnected. Figure 5-22 on page 5-26 shows fiber connections for a four-fiber MS-SPRing. Slot 5 (west) and Slot 12 (east) carry the working traffic. Slot 6 (west) and Slot 13 (east) carry the protect traffic.

Figure 5-22   Connecting fiber to a four-node, four-fiber MS-SPRing
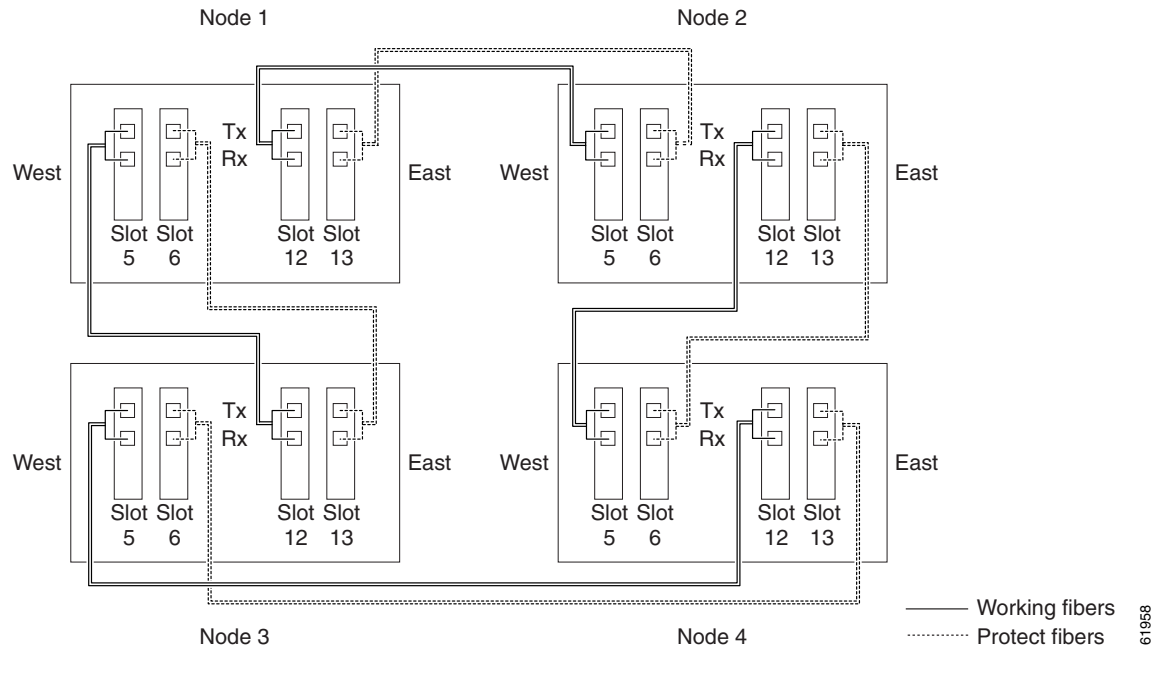
Procedure: Create the MS-SPRing DCC Terminations and Place Ports in Service

Note   The SDH and SONET versions of the Cisco ONS 15454 do not interoperate via DCC. DCC interoperability is not available for ONS 15454 SDH Software R3.4 and earlier.

Purpose	Create the DCC terminations and place ports in service after installing the STM-N cards.
Prerequisite Procedures	"Install the MS-SPRing Trunk Cards" procedure on page 5-24
Onsite/Remote	Onsite or remote

Step 1   Start CTC for the first node that you will provision for the MS-SPRing.

Step 2   Click the **Provisioning > SDH DCC** tabs.

Step 3   In the SDCC Terminations section, click **Create** (Figure 5-23 on page 5-27).

Step 4   In the Create SDCC Terminations dialog box, press **Ctrl** and click the two slots/ports that will serve as the MS-SPRing ports at the node. For example, Slot 5 (STM-16)/Port 1 and Slot 12 (STM-16)/ Port 1. For four-fiber MS-SPRings, provision the working cards, but not the protect cards, as DCC terminations.

Figure 5-23   Creating SDCC terminations
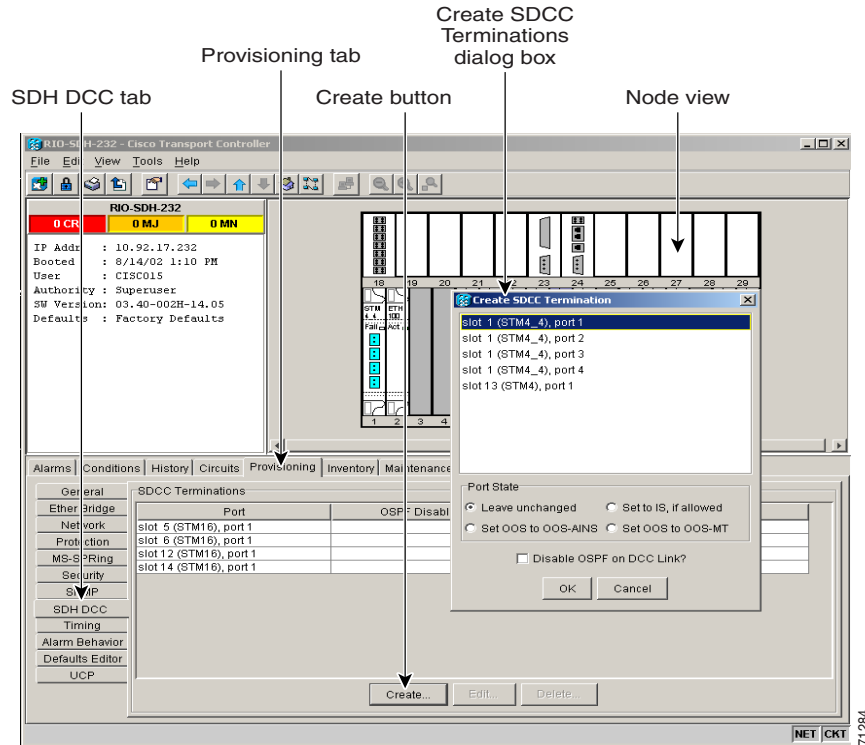
Step 5   Select the **Set to IS, if allowed** radio button. This radio button places the trunk card ports in service.

> **Note**   There are four port state options. Select the port state that best fits your requirements. For example, you can select the set OOS to OOS-MT radio button if you are provisioning the MS-SPRing before installing cards and fiber. Also, you can select the OOS-MT port state if you want to avoid DCC termination alarms until you configure all DCCs on the MS-SPRing.

Step 6   (Optional) Below the port state options you can also enable or disable OSPF on the DCC according to your requirements.

Step 7   Click **OK**.

Step 8   The slots/ports appear in the SDCC Terminations list.

Step 9   Complete Steps 3 to 7 at each node that will be in the MS-SPRing.

> **Note**   The ONS 15454 SDH uses the SDH regenerator section DCC (SDCC) for data communications. It does not use the multiplex section DCCs; therefore, the multiplex section DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 SDH networks. For more detail, see the "Creating DCC Tunnels" section on page 6-34.

Step 10   After configuring the SDH DCC, set the timing for the node. For procedures, see the "Setting Up ONS 15454 SDH Timing" section on page 3-18.

Procedure: Remap the K3 Byte

Purpose	Only use the K3 byte remapping procedure when it is required to run MS-SPRings through third-party equipment that cannot transparently transport the K3 (see the "Sample MS-SPRing Application" section on page 5-18). K3 bytes can only be remapped on STM-16 cards.
Prerequisite Procedures	"Create the MS-SPRing DCC Terminations and Place Ports in Service" procedure on page 5-26
Onsite/Remote	Onsite or remote

Step 1 Start CTC for one of the nodes that connects to the third-party equipment.

Step 2 Double-click the STM-16 card that connects to the third-party equipment. The card view displays.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Click **MS-SPRing Ext Byte** and choose the alternate byte: **Z2**, **E2**, or **F1**.

Step 5 Click **Apply**.

Step 6 (Four-fiber MS-SPRing only) Repeat Steps 2 to 5 for each protect card.

Step 7 (Two-fiber MS-SPRing only) Repeat Steps 2 to 5 at the node and card on the other end of the MS-SPRing span.

Procedure: Provision the MS-SPRing Using the Wizard

Purpose	After enabling the ports, create a two-fiber or four-fiber MS-SPRing using this procedure.
Prerequisite Procedures	"Create the MS-SPRing DCC Terminations and Place Ports in Service" procedure on page 5-26
	"Setting Up ONS 15454 SDH Timing" section on page 3-18
Onsite/Remote	Onsite or remote

Step 1 Start CTC for a node in the MS-SPRing and go to the network view.

Step 2 From network view, choose the **Provisioning > MS-SPRing** tabs.

Step 3 Click the **Create MS-SPRings** button.

Step 4 In the Create MS-SPRing dialog box (Figure 5-24 on page 5-29), set the MS-SPRing properties.

- Type—Select the MS-SPRing ring type, either **two-fiber** or **four-fiber**.
- Speed—Select the type of trunk card you are using: **STM-4**, **STM-16**, or **STM-64**.
- Ring ID—Assign a ring ID (a number between 0 and 9999). Nodes in the same MS-SPRing must have the same ring ID.
- Ring Reversion—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 an MS-SPRing ring should have the same ring reversion setting, particularly if **never** (i.e., non-revertive) is selected.

Figure 5-24   Setting MS-SPRing properties
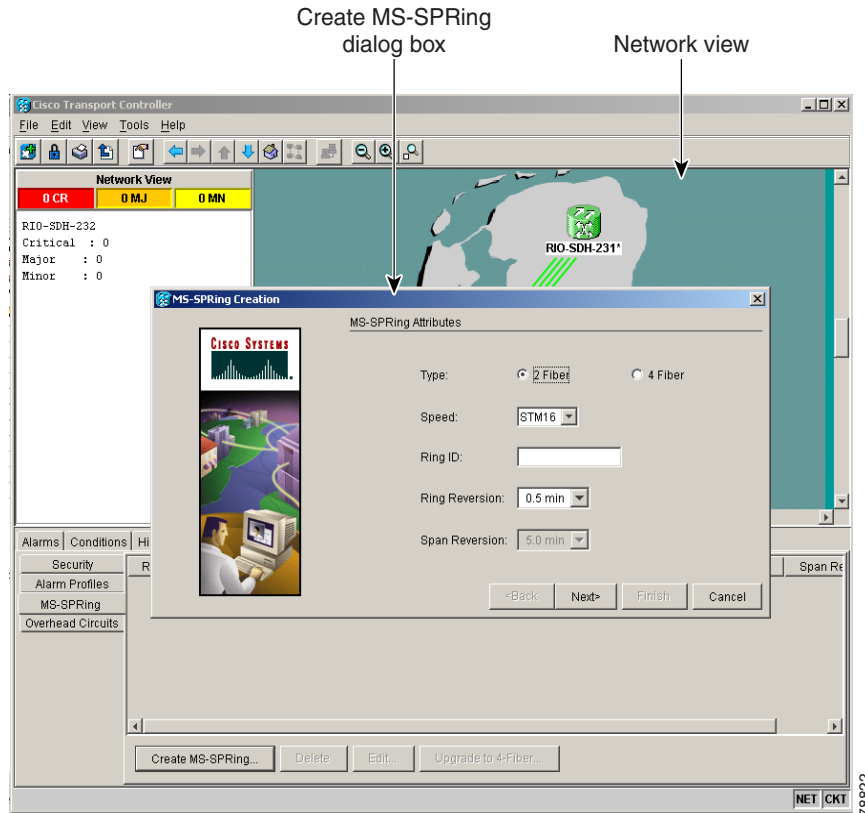
For four-fiber MS-SPRings, complete the following:

- Span Reversion—Choose the amount of time that will elapse before the traffic reverts to the original working path following a traffic failure. The default is 5 minutes. Span reversions can be set to Never. If you set a ring 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.

Note   To avoid reversion time mismatches, Cisco recommends that you use the same span reversion time throughout the ring.

Step 5   Click **Next**.

Step 6   Click on the span you want to include in the MS-SPRing and click the **Add Span** button. Perform this step for each span you are adding to the MS-SPRing.

Step 7   Click the **Finish** button after you have selected enough spans to create a two-fiber or four-fiber MS-SPRing.

Note   Some or all of the following alarms display during MS-SPRing setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, MSSP-OOSYNC. The alarms will clear automatically. If the alarms do not clear, follow alarm troubleshooting procedures provided in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Step 8 From the network view, verify the following:

- A green span line appears between all MS-SPRing nodes.

- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and MSSP-OOSYNC alarms are cleared.

Step 9 Test the MS-SPRing using testing procedures normal for your site; here is a common test procedure:

   a. Run test traffic through the ring.

   b. From network view, click the **Provisioning > MS-SPRing** tabs.

   c. Click on the ring and click the **Edit** button.

   d. Right click on an East port and choose **MANUAL RING** from the Set East Protection Operation list (Figure 5-25). Click **Apply**.

Figure 5-25   Choosing the manual ring option
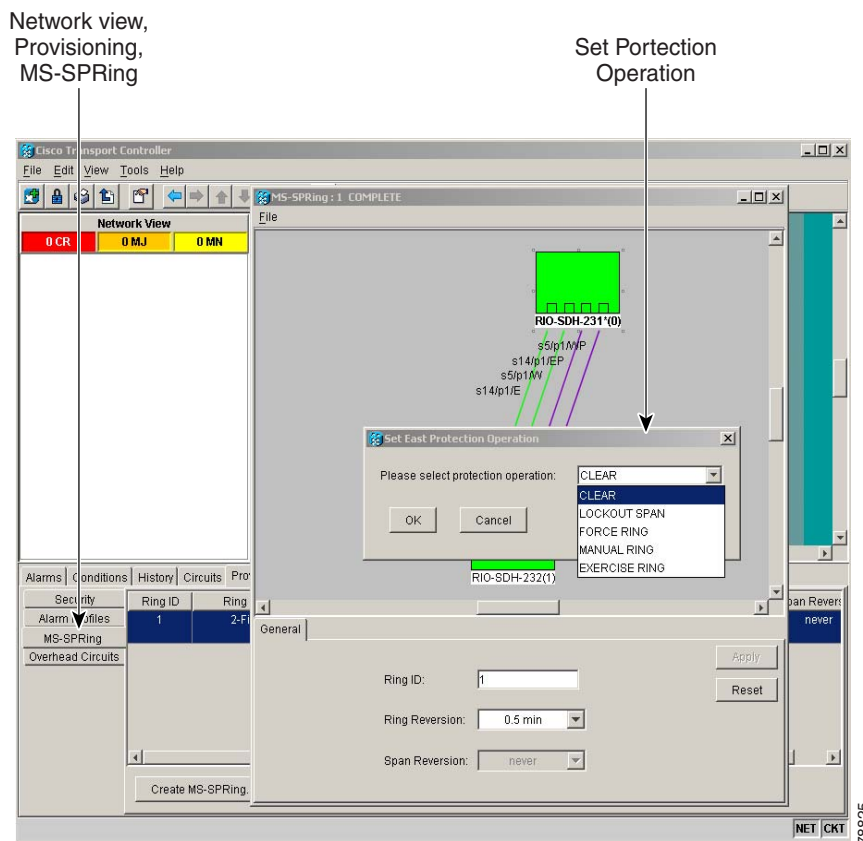
   e. Click the **Conditions** tab and click **Retrieve**. You should see a Ring Switch West event, and the far-end node that responded to this request should report a Ring Switch East event.

   f. Verify that traffic switches normally.

   g. Choose **Clear** from the Set East Protection Operation list and click **Apply**.

   h. Repeat Steps a to g for the West Switch.

   i. Disconnect the fibers at any node on the ring and verify that traffic switches normally.

5.5 Adding Nodes to an MS-SPRing

This section explains how to add nodes in an ONS 15454 SDH MS-SPRing configuration. You can only add one node at a time to an MS-SPRing. To add a node to an MS-SPRing, perform five procedures:

Step 1 First, check for alarms and conditions on the existing MS-SPRing. See the "Check for Alarms" procedure on page 5-57.

Step 2 Install cards and configure the new node. See the "Install Cards and Configure the New MS-SPRing Node" procedure on page 5-31.

Step 3 Before connecting the fiber, route traffic away from the area of the ring where service will be performed. See the "Switch MS-SPRing Traffic Before Connecting a New Node" procedure on page 5-32.

Step 4 After switching ring traffic, connect the fiber. See the "Connect Fiber to the New Node" procedure on page 5-33.

Step 5 Add an MS-SPRing node. See the "Provision the Ring for the New Node" procedure on page 5-34.

Procedure: Install Cards and Configure the New MS-SPRing Node

Purpose	This procedure explains the steps necessary to setup the new MS-SPRing node. You can only add one node at a time to an ONS 15454 SDH MS-SPRing.
Prerequisite Procedures	"Check for Alarms" procedure on page 5-57
Onsite/Remote	Onsite only

Step 1 Install the STM-4, STM-16, or STM-64 cards that you will add to the MS-SPRing. You can install the STM-4 and STM-16 cards in Slots 1 to 6 and 12 to 17. The STM-64 card can only be installed in Slots 5, 6, 12, or 13.

Step 2 Allow the cards to boot. For more information about installing cards, see the "Optical, Electrical, and Ethernet Card Installation" section on page 1-35. Run test traffic through the node to ensure the cards are functioning properly.

Step 3 Log into the new node. Complete the "Add the Node Name, Contact, Location, Date, and Time" procedure on page 3-3.

Step 4 Provision the SDH DCC and place ports in service for the new node's cards. Complete the "Create the MS-SPRing DCC Terminations and Place Ports in Service" procedure on page 5-26.

Step 5 Configure the MS-SPRing timing. See the "Set Up External, Line, or Mixed Timing for the ONS 15454 SDH" procedure on page 3-21 or the "Set Up Internal Timing for the ONS 15454 SDH" procedure on page 3-24.

Step 6 If the new node will connect to third-party equipment that cannot transport the K3 byte, see the "Remap the K3 Byte" procedure on page 5-28 to remap trunk cards that connect to the third-party equipment. Make sure the trunk card at the other end of the span is mapped to the same byte that is set on the new node.

Step 7 Complete the "Provision the MS-SPRing Using the Wizard" procedure on page 5-28.

Procedure: Switch MS-SPRing Traffic Before Connecting a New Node

Purpose	Use this procedure to route traffic away from the area of the ring where service will be performed.
Prerequisite Procedures	"Check for Alarms" procedure on page 5-57
	"Install Cards and Configure the New MS-SPRing Node" procedure on page 5-31
Onsite/Remote	Onsite or remote

Step 1   Log into the existing node that will connect to the new node through its east port (Node 4 in the Figure 5-26 example).

Figure 5-26   Three-node MS-SPRing before adding a new node

West — Tx / Rx — Slot 5 — Tx / Rx — Slot 12 — East — Node 1
West — Tx / Rx — Slot 5 — Tx / Rx — Slot 12 — East — Node 2
West — Tx / Rx — Slot 5 — Tx / Rx — Slot 12 — East — Node 3
West — Tx / Rx — Slot 5 — Tx / Rx — Slot 12 — East — Node 4

68118
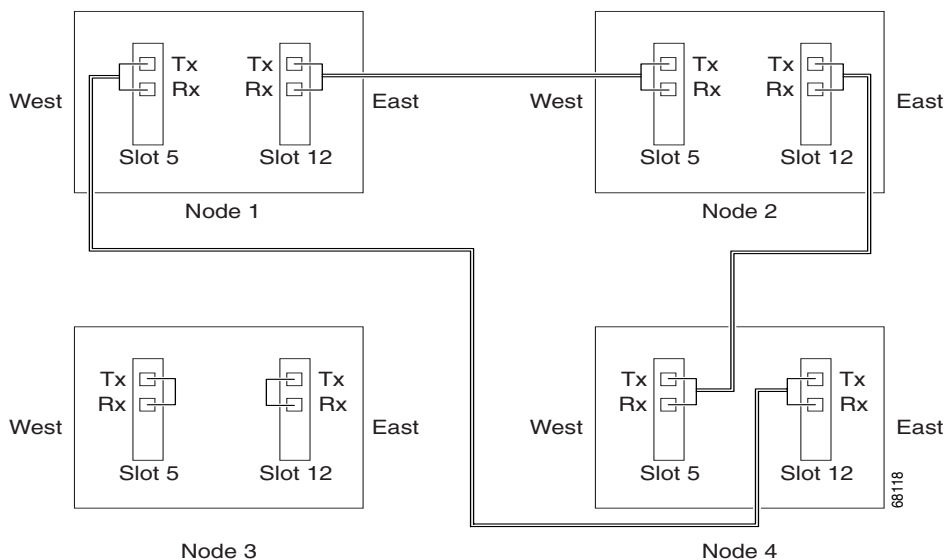
⚠ **Caution**   Traffic is unprotected during a protection switch.

Step 2   Switch protection on the node's east port:

   a.   Click the **Maintenance > MS-SPRing** 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.

Step 3   Log into the existing node that will connect to the new node through its west port (Node 1 in the Figure 5-26 example).

Step 4   Switch protection on the node's west port:

   a.   Click the **Maintenance > MS-SPRing** tabs.

   b.   From the West Switch list, choose **FORCE RING**. Click **Apply**.

Procedure: Connect Fiber to the New Node

Purpose	Use this procedure to connect fiber to the new node.
Prerequisite Procedures	"Check for Alarms" procedure on page 5-57
	"Install Cards and Configure the New MS-SPRing Node" procedure on page 5-31
	"Switch MS-SPRing Traffic Before Connecting a New Node" procedure on page 5-32
Onsite/Remote	Onsite or remote

Note While performing this procedure, use the diagram that you created showing the nodes, cards (slots), and spans (east and west) that will connect to the new node.

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 example in Figure 5-26 on page 5-32, 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 example in Figure 5-26 on page 5-32, this is Node 1/Slot 5.

Step 2 Replace the removed fibers with fibers connected from the new node. Connect the west port to the east port and the east port to the west port. Figure 5-27 shows the MS-SPRing example after the node is connected.

Figure 5-27   MS-SPRing with a newly added fourth node
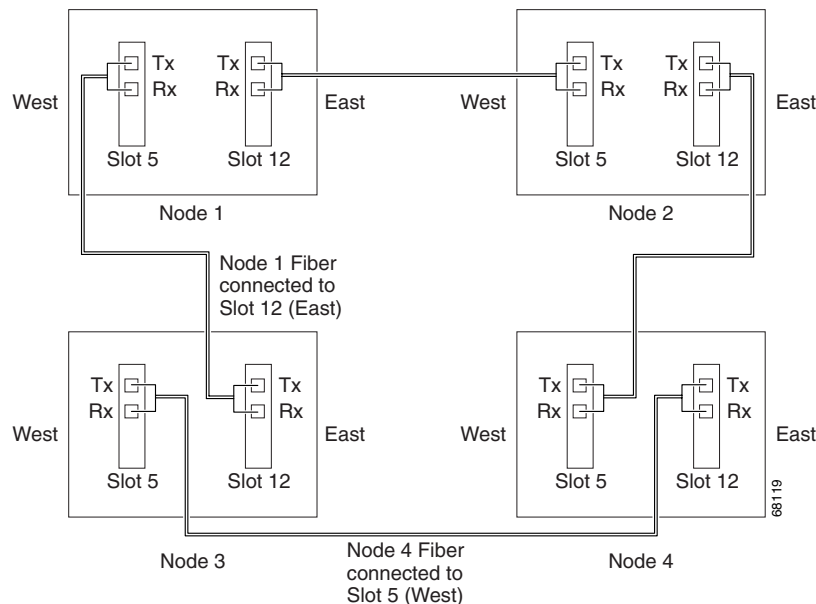
Step 3 Exit CTC.

✎

Note   The new node will not appear in the ring until you exit CTC, restart, and provision the ring to accept the new node.

Procedure: Provision the Ring for the New Node

Purpose	Use this procedure to finish provisioning a new node in the ring.
Prerequisite Procedures	"Connect Fiber to the New Node" procedure on page 5-33
Onsite/Remote	Onsite or remote

Step 1   Start CTC again from any node in the MS-SPRing.

Step 2   In node (default) view, choose the **Provisioning > MS-SPRing** tabs.

Step 3   Click a ring and then click **Ring Map**.

Step 4   In the MS-SPRing Map Ring Change dialog box, click **Yes**.

Step 5   In the MS-SPRing Map dialog box, verify that the new node is added. If it is, click **Accept**. If it does not appear, start CTC for the new node. Verify that the MS-SPRing is provisioned correctly according to the "Provision the MS-SPRing Using the Wizard" procedure on page 5-28, then repeat Steps 1 to 4 in this procedure. If the node still does not appear, repeat all procedures for adding a node, making sure that no errors were made.

Step 6   Display the network view and 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 7   Right-click the new node and choose **Update Circuits With New Node** from the shortcut menu. Verify that the number of updated circuits displayed in the dialog box is correct.

Step 8   Choose the **Circuits** tab and verify that no incomplete circuits are present.

Step 9   Clear the protection switch on the existing node using its east port to connect to the new node. Then, clear the protection switch on the existing node using its west port to connect to the new node. The protection switches were first performed in the "Switch MS-SPRing Traffic Before Connecting a New Node" procedure on page 5-32.

    a.   To clear the protection switch from the east port, display the node view and then display the **Maintenance > MS-SPRing** tabs. From the East Switch list choose **CLEAR**. Click **Apply**.

    b.   To clear the protection switch from the west port, display the node view and then display the **Maintenance > MS-SPRing** tabs. From the West Switch list choose **CLEAR**. Click **Apply**.

5.6 Removing Nodes from an MS-SPRing

This section explains how to remove nodes in an ONS 15454 SDH MS-SPRing configuration.

Procedure: Remove an MS-SPRing Node

Purpose	Use this procedure to remove a node from an MS-SPRing. This procedure is designed to minimize traffic outages during node deletions.
Prerequisite Information	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 5-27 on page 5-33, 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. Node 2 is connected to Node 1 through its west port.
Onsite/Remote	Onsite or remote

Step 1   Start CTC for a node on the same MS-SPRing as the node you will remove, and display the network view. Clear any alarms or conditions on the network/ring. See the "Check for Alarms" procedure on page 5-57.

> **Note**   Do not Start CTC for the node that you will remove.

Step 2   Use the following substeps to delete all the circuits that originate or terminate in that node. Refer to Figure 5-28 on page 5-36.

> **Note**   If a circuit has multiple drops, delete only the drops that terminate on the node you want to delete.

Figure 5-28   Deleting circuits from node view
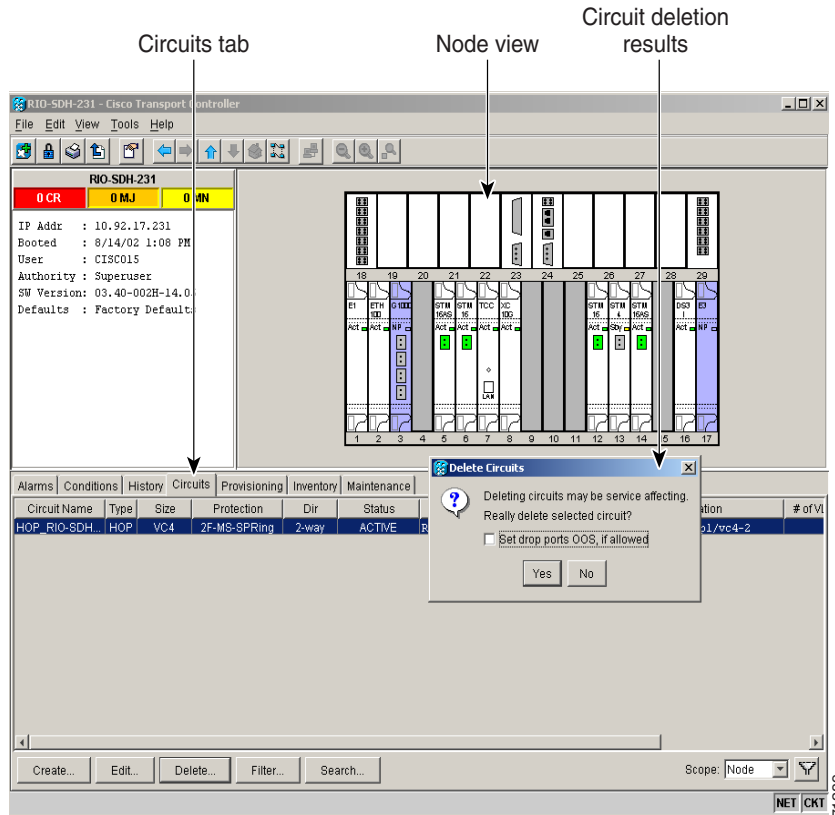
a. Click the **Circuits** tab. The circuits that use this node are displayed.

b. Choose 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, choose the circuit, click **Edit**, and remove the drops.

Step 3   Switch traffic away from the ports of neighboring nodes that will be disconnected when the node is removed.

> **Note**   Refer to the list you created. Refer to the information you that you collected about node connections. See the prerequisite information section at the beginning of this procedure.

> ⚠ **Caution**   Traffic is unprotected during the protection switch.

a. Start CTC for the neighboring node that is connected through its east port to the removed node.

b. Click the **Maintenance > MS-SPRing** tabs.

c. From the East Switch list, choose **FORCE RING**. Click **Apply**.

d. Start CTC for the node that is connected through its west port to the removed node.

e. Click the **Maintenance > MS-SPRing** tabs.

f. From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 4 Remove all fiber connections between the node being removed and the two neighboring nodes.

Step 5 Reconnect the two neighboring nodes directly, west port to east port.

Step 6 If the removed node contained trunk STM-16 cards with K3 bytes mapped to an alternate byte, use the "Remap the K3 Byte" procedure on page 5-28 to verify and remap, if needed, the MS-SPRing extended bytes on the newly connected neighboring nodes.

Step 7 Exit CTC, then start CTC for a node on the reduced ring.

Step 8 Wait for the MS-SPRing Map Ring Change dialog box to display. When the dialog box displays, click **Yes**.

> **Note** If the dialog box does not display after 10 to 15 seconds, choose the **Provisioning > MS-SPRing** tabs and click **Ring Map**.

Step 9 In the MS-SPRing Ring Map dialog box, click **Accept**.

Step 10 Display the network view; then, choose the **Circuits** tab.

Step 11 Delete, then recreate any incomplete circuits. See the "Create an Automatically Routed High-Order Path Circuit" procedure on page 6-4. Recreate the incomplete circuits one at a time.

Step 12 Clear the protection switches on the neighboring nodes.

a. Display the node with the protection switch on its east port.

b. Click the **Maintenance > MS-SPRing** tabs and choose **CLEAR** from the East Switch list. Click **Apply**.

c. Start CTC for the node with the protection switch on its west port.

d. Click the **Maintenance > MS-SPRing** tabs and choose **CLEAR** from the West Switch list. Click **Apply**.

Step 13 If a BITS clock is not used at each node, check that the synchronization is set to one of the eastbound or westbound MS-SPRing 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 SDH timing, see the "Setting Up ONS 15454 SDH Timing" section on page 3-18.)

5.7 Upgrading a Two-Fiber MS-SPRing to a Four-Fiber MS-SPRing

Two-fiber STM-16 or STM-64 MS-SPRings can be upgraded to four-fiber MS-SPRings. To upgrade, install two STM-16 or STM-64 cards at each two-fiber MS-SPRing node, then start CTC and upgrade the MS-SPRing from two-fiber to four-fiber. The fibers that were divided into working and protect bandwidths for the two-fiber MS-SPRing are now fully allocated for working MS-SPRing traffic.

> **Note** Optical transmit and receive levels should be in their acceptable range as shown in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Procedure: Upgrade a Two-Fiber MS-SPRing to a Four-Fiber MS-SPRing from Node View

Purpose	Use this procedure to upgrade from a two-fiber MS-SPRing to a four-fiber MS-SPRing.
Prerequisite Procedures	This procedure assumes you have a two-fiber MS-SPRing configured. Verify that there are no protection operations or protection switches before attempting to upgrade the ring.
Onsite/Remote	Onsite

Step 1 Start CTC for one of the two-fiber MS-SPRing nodes and display the network view. Clear any alarms or conditions. See the "Check for Alarms" procedure on page 5-57.

Step 2 Install two STM-16 or STM-64 cards at each MS-SPRing node. You must install the same STM-N card rate as the two-fiber ring. See the "Optical, Electrical, and Ethernet Card Installation" section on page 1-35.

Step 3 Connect the fiber to the new cards. Use the same east/west connection scheme that connected the two-fiber connections. Figure 5-22 on page 5-26 shows an example of how to connect fiber.

Step 4 Set the card ports in service for each new STM-N card. See the "Put Ports In or Out of Service" procedure on page 5-56 for more information.

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 MS-SPRing protect ring.

Step 6 Upgrade the MS-SPRing.

> **Note** The upgrade button will be disabled until the ring is upgradeable, which means that there have to be enough protect cards in each shelf with ports in service, no SDCC terminations, and no other protection groups. If all of your nodes meet these conditions, then the **Upgrade to 4-Fiber** button is enabled.

    a. Display the network view and click the **Provisioning > MS-SPRing** tabs.

    b. Click the two-fiber MS-SPRing you want to upgrade; then, click the **Upgrade to 4-Fiber** button.

    c. In the Upgrade MS-SPRing dialog box, click a span reversion time from the pull-down menu, then click **Next**. The span reversion time sets the amount of time that will elapse before the traffic reverts to the original working path following a traffic failure. The default is 5 minutes.

    d. Complete the following from the protection pull-down menus:

       – West Protect—Assign the east MS-SPRing port that will connect to the east protect fiber. (In Figure 5-22 on page 5-26, this is Slot 6.)

       – East Protect—Assign the east MS-SPRing port that will connect to the east protect fiber. (In Figure 5-22 on page 5-26, this is Slot 13.)

    e. Click **Finish**.

Step 7 Test the MS-SPRing using testing procedures normal for your site; here is a common test procedure:

    a. Run test traffic through the ring.

    b. Log into a node on the ring, click the **Maintenance > MS-SPRing** 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 should 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 to e for the West Switch.

    g. Disconnect the fibers at any node on the ring and verify that traffic switches normally.

5.8 Moving MS-SPRing Trunk Cards

⚠
Caution   To ensure that circuit and provisioning data is preserved, call the Technical Assistance Center (TAC) before performing this procedure. For a complete list of TAC phone numbers, refer to the section called "About this Guide."

⚠
Caution   To change MS-SPRing trunk cards, you will drop one node at a time from the current MS-SPRing. This procedure is service affecting during the time needed to complete the steps in the following procedure. Service disruption applies to all MS-SPRing nodes where cards will change slots. Review all the steps before you proceed.

Figure 5-29 shows a four node STM-16 MS-SPRing using trunk cards in Slots 6 and 12 at all four nodes. In this example, the user moves trunk cards at Node 4 in Slots 6 and 12 to Slots 5 and 6. Node 4 must be temporarily removed from the active MS-SPRing while the trunk cards are moved.

Figure 5-29   Four-node MS-SPRing before a trunk card switch
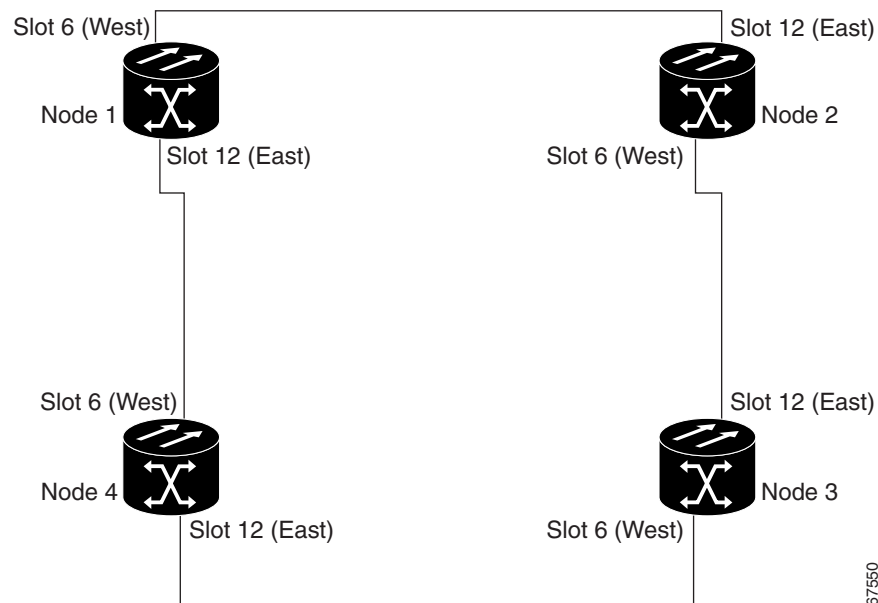
Figure 5-30 shows the MS-SPRing after the cards are moved.

Figure 5-30   Four-node MS-SPRing after the trunk cards are moved to different slots at one node
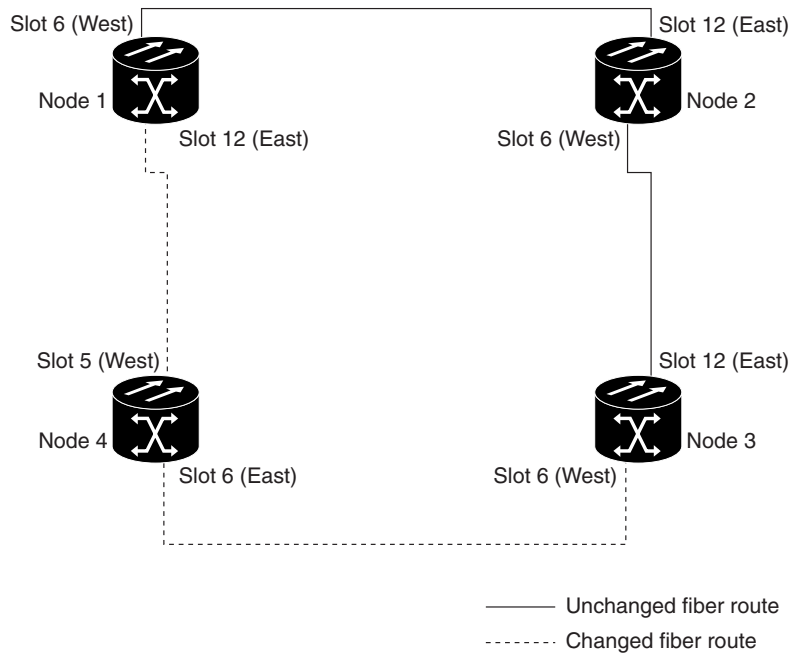
Procedure: Move an MS-SPRing Trunk Card

⚠

Caution   Always wear an authorized ESD wrist band when removing or installing ONS 15454 SDH cards.

Purpose	Use this procedure to move one MS-SPRing trunk card to a different slot. Repeat this procedure for each card you want to move. Although the procedure uses STM-16 MS-SPRing trunk cards, you can use the same procedure for STM-4 or STM-64 cards.
Prerequisite Procedures	Clear active alarms for the STM-16 or STM-4 card host nodes or the MS-SPRing configuration. For more information, see "Check for Alarms" procedure on page 5-57
Onsite/Remote	Onsite

Step 1   Start CTC for one of the MS-SPRing nodes and display the network view. Clear any alarms or conditions in the network/ring. See the "Check for Alarms" procedure on page 5-57.

Step 2   Switch traffic away from the node where the trunk card will be moved:

   a.   Start CTC for the node that is connected through its east port to the target node. (In the example in Figure 5-29 on page 5-39, this is Node 1.) Click the **Maintenance > MS-SPRing** 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-REQ) is generated. This is normal.

⚠️

Caution   Traffic is unprotected during a protection switch.

    c.   Start CTC for the node that is connected through its west port to the target node. (In the example in Figure 5-29 on page 5-39, this is Node 3.) Click the **Maintenance > MS-SPRing** tabs.

    d.   From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 3   Start CTC on the target node.

Step 4   Click the **Circuits** tab. Write down the circuit information or, from the File menu, choose **Print** or **Export** to print or export the information. You will need this information to restore the circuits later. See the "Printing CTC Data" section on page 2-29 and the "Exporting CTC Data into Other Applications" section on page 2-30 for more information.

Step 5   Delete the circuits on the card you are removing:

    a.   Highlight the circuit(s). To choose multiple circuits, press the **Shift** or **Ctrl** key while selecting circuits.

    b.   Click **Delete**.

    c.   In the Delete Circuit dialog box, click **Yes**.

Step 6   Delete the SDH DCC termination on the card you are removing:

    a.   Click the **Provisioning > SDH DCC** tabs.

    b.   From the SDCC Terminations list, click the SDH DCC you need to delete and click **Delete**.

    c.   Click the **Set Unused Port Out of Service** check box.

Step 7   Disable the ring on the target node:

    a.   Click the **Provisioning > MS-SPRing** tabs.

    b.   Highlight the ring and click **Delete**.

    c.   In the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.

Step 8   If an STM-N card is a timing source, choose the **Provisioning > Timing** tabs and set timing to **Internal**.

Step 9   Physically remove the card.

Step 10   Insert the card into its new slot and wait for the card to boot.

Step 11   To delete the card in CTC from its former slot, right-click the card in node view and choose **Delete Card** from the list of options.

Step 12   Place the port(s) back in service.

Step 13   Follow the steps described in the "Setting Up MS-SPRings" section on page 5-24 to reenable the ring using the same cards (in their new slots) and ports for east and west. Use the same MS-SPRing Ring ID and Node ID that was used before the trunk card was moved.

Step 14   Recreate the circuits that were deleted. See "Create an Automatically Routed High-Order Path Circuit" procedure on page 6-4.

Step 15   If you use line timing and the card you are moving is a timing reference, reenable the timing parameters on the card. See the "Setting Up ONS 15454 SDH Timing" section on page 3-18 for instructions.

5.9 Subtending Rings

The ONS 15454 SDH supports up to ten SDH DCCs. Therefore, one ONS 15454 SDH node can terminate and groom any ring combination if the total DCC usage is equal to or less than 10 DCCs.

Figure 5-31 shows an ONS 15454 SDH with multiple subtending rings.

Figure 5-31   ONS 15454 SDH with multiple subtending rings
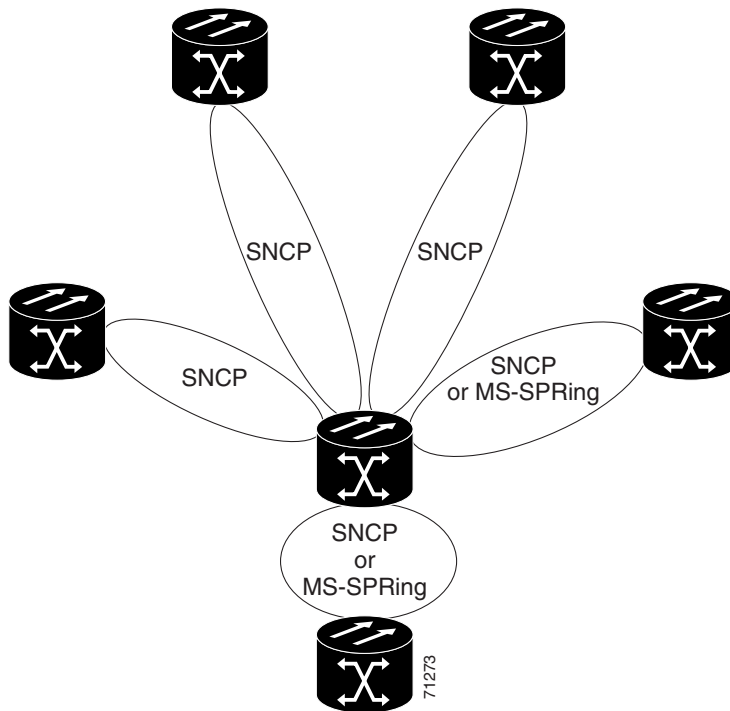
Figure 5-32 shows an SNCP ring subtending from an MS-SPRing. In this example, Node 3 is the only node serving both the MS-SPRing and SNCP ring. STM-N cards in Slots 5 and 12 serve the MS-SPRing, and STM-N cards in Slots 6 and 13 serve the SNCP ring.

Figure 5-32   SNCP ring subtending from an MS-SPRing
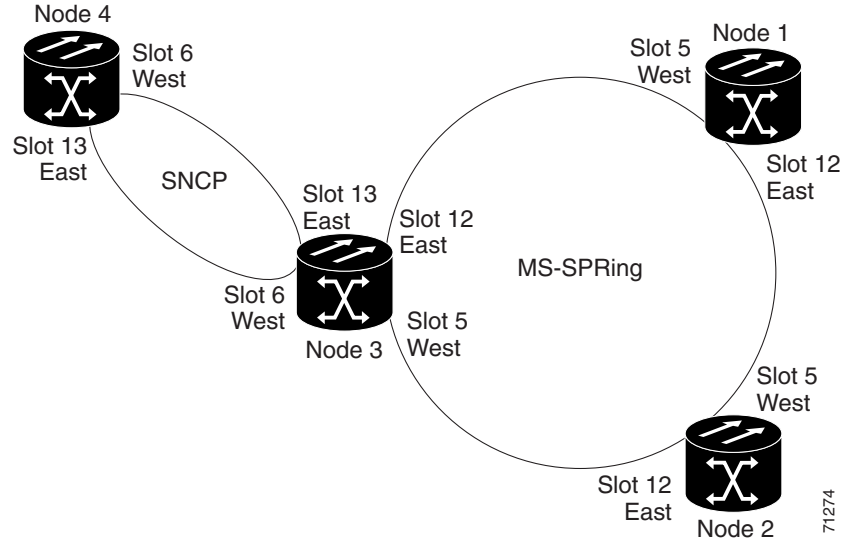
Figure 5-33 shows two MS-SPRings shared by one ONS 15454 SDH. The ONS 15454 SDH can support two MS-SPRings on the same node. This capability allows you to deploy an ONS 15454 SDH in applications requiring SDH Digital Crossconnect Systems (DCSs) or multiple SDH ADMs.

In Figure 5-33, Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7. Two MS-SPRing 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 MS-SPRings shown in Figure 5-33, nodes in different MS-SPRings can use the same node ID.

Figure 5-33   MS-SPRing subtending from an MS-SPRing
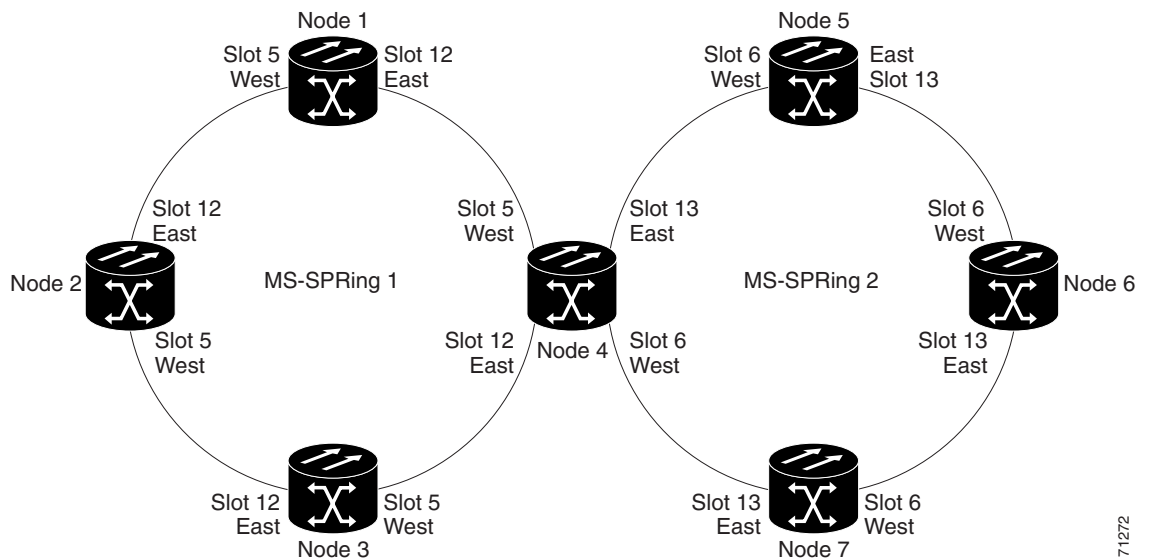
After subtending two MS-SPRings, you can route circuits from nodes in one ring to nodes in the second ring. For example in Figure 5-33 on page 5-43, you can route a circuit from Node 1 to Node 7. The circuit would normally travel from Node 1 to Node 4 to Node 7. If fiber breaks occur, for example between Nodes 1 and 4 and Nodes 4 and 7, traffic is rerouted around each ring: in our example, Nodes 2 and 3 in Ring 1 and Nodes 5 and 6 in Ring 2.

Procedure: Subtend an SNCP Ring from an MS-SPRing

Purpose	Use this procedure to subtend an SNCP ring from an MS-SPRing. A subtended ring reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling.
Prerequisite Procedures	This procedure requires an established MS-SPRing and one node with STM-N cards and fibers to carry the SNCP ring. The procedure also assumes you can set up an SNCP ring. (For SNCP ring setup procedures, see the "Creating SNCP Rings" section on page 5-3.)
Onsite/Remote	Onsite

Step 1   In the node that will subtend the SNCP (Node 3 in Figure 5-32 on page 5-43), install the STM-N cards that will serve as the SNCP trunk cards (Node 3, Slots 6 and 13).

Step 2   Attach fibers from these cards to the SNCP trunk cards on the SNCP nodes. In Figure 5-32 on page 5-43, Node 3/Slot 6 connects to Node 5/Slot 13, and Slot 13 connects to Node 6/Slot 6.

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

Step 4   Click **Create**.

Step 5   In the Create SDCC Terminations dialog box, click the slot and port that will carry the SNCP ring.

Step 6   Select the **Set to IS, if allowed** radio button. This radio button places the trunk card ports in service.

> **Note**   There are four port state options. Select the port state that best fits your requirements. For example, you can select the set OOS to OOS-MT radio button if you are provisioning the SNCP before installing cards and fiber. Also, you can select the OOS-MT port state if you want to avoid DCC termination alarms until you configure all DCCs on the SNCP.

Step 7   (Optional) Below the port state options you can also enable or disable OSPF on the DCC according to your requirements.

Step 8   Click **OK**.

The selected slots/ports are displayed in the SDCC Terminations section.

Step 9   Follow Steps 1 to 8 for the other nodes you will use for the SNCP ring.

Step 10   Display the network view to view the subtending ring.

Procedure: Subtend an MS-SPRing from an SNCP Ring

Purpose	Use this procedure to subtend an MS-SPRing from an SNCP ring. A subtended ring reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling.
Prerequisite Procedures	This procedure requires an established SNCP ring and one node with STM-N cards and fibers to connect to the MS-SPRing. The procedure also assumes you can set up an MS-SPRing. (For MS-SPRing setup procedures, see the "Setting Up MS-SPRings" section on page 5-24.)
Onsite/Remote	Onsite

Step 1 In the node that will subtend the MS-SPRing (Node 3 in the Figure 5-32 on page 5-43 example), install the STM-N cards that will serve as the MS-SPRing trunk cards (in Figure 5-32, Node 3, Slots 6 and 13).

Step 2 Attach fibers from these cards to the MS-SPRing trunk cards on the MS-SPRing nodes. In Figure 5-32, Node 3/Slot 6 connects to Node 5/Slot 13, and Slot 13 connects to Node 6/Slot 6.

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

Step 4 Click **Create**.

Step 5 In the Create SDCC Terminations dialog box, click the slot and port that will carry the MS-SPRing.

Step 6 Select the **Set to IS, if allowed** radio button. This radio button places the trunk card ports in service.

> **Note**   There are four port state options. Select the port state that best fits your requirements. For example, you can select the set OOS to OOS-MT radio button if you are provisioning the MS-SPRing before installing cards and fiber. Also, you can select the OOS-MT port state if you want to avoid DCC termination alarms until you configure all DCCs on the MS-SPRing.

Step 7 (Optional) Below the port state options you can also enable or disable OSPF on the DCC according to your requirements.

Step 8 Click **OK**.

Step 9 The selected slots/ports are displayed under SDCC Terminations.

Step 10 Configure the MS-SPRing. See the "Provision the MS-SPRing Using the Wizard" procedure on page 5-28.

Step 11 Follow Steps 1 to 10 for the other nodes that will be in the MS-SPRing.

Step 12 Display the network view to see the subtending ring.

Procedure: Subtend an MS-SPRing from an MS-SPRing

Purpose	Use this procedure to subtend an MS-SPRing from an MS-SPRing. Subtending rings from an ONS 15454 SDH reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling.
Prerequisite Procedures	This procedure requires an established MS-SPRing and one node with STM-N cards and fibers to carry the MS-SPRing. The procedure also assumes you know how to set up an MS-SPRing. For MS-SPRing setup procedures, see the "Creating MS-SPRings" section on page 5-14.
Onsite/Remote	Onsite

Step 1   In the node that will subtend the MS-SPRing (Node 4 in Figure 5-33 on page 5-43), install the STM-N cards that will serve as the MS-SPRing trunk cards (Node 4, Slots 6 and 13).

Step 2   Attach fibers from these cards to the MS-SPRing trunk cards on the MS-SPRing nodes. In Figure 5-33 on page 5-43, 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 > SDH DCC** tabs.

Step 4   Click **Create**.

Step 5   In the Create SDCC Terminations dialog box, click the slot and port that will carry the MS-SPRing.

Step 6   Select the **Set to IS, if allowed** radio button. This radio button places the trunk card ports in service.

> ✎
> **Note**   There are four port state options. Select the port state that best fits your requirements. For example, you can select the set OOS to OOS-MT radio button if you are provisioning the MS-SPRing before installing cards and fiber. Also, you can select the OOS-MT port state if you want to avoid DCC termination alarms until you configure all DCCs on the MS-SPRing.

Step 7   (Optional) Below the port state options you can also enable or disable OSPF on the DCC according to your requirements.

Step 8   Click **OK**.

Step 9   The selected slots/ports are displayed in the SDCC Terminations section.

Step 10 To configure the MS-SPRing, use the "Provision the MS-SPRing Using the Wizard" procedure on page 5-28. The subtending MS-SPRing must have a ring ID that differs from the ring ID of the first MS-SPRing.

Step 11 Follow Steps 1 to 10 for the other nodes that will be in the subtending MS-SPRing.

Step 12 Display the network view to see the subtending ring.

Figure 5-34 shows an example of two subtending MS-SPRings.

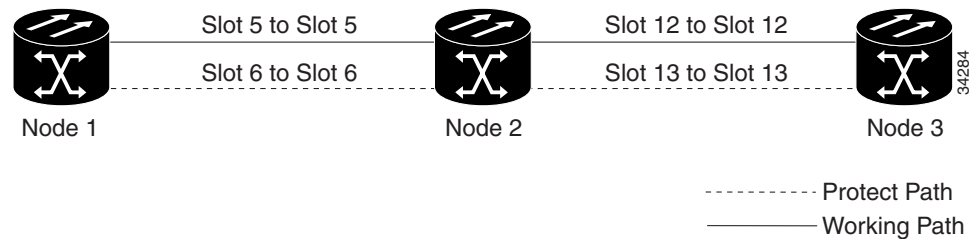*Figure 5-34   Viewing subtending MS-SPRings on the network view*
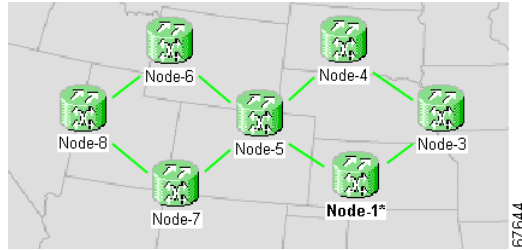
5.10 Creating Linear ADM Configurations

You can configure ONS 15454 SDH nodes as a line of ADMs by configuring one set of STM-N cards as the working path and a second set as the protect path. Unlike rings, linear (point-to-point) ADMs require that the STM-N cards at each node have a 1+1 protection scheme to ensure that a break to the working line is automatically routed to the protect line.

Figure 5-35 shows three ONS 15454 SDH nodes in a linear ADM configuration. Working traffic flows from Node 1/Slot 6 to Node 2/Slot 6, and from Node 2/Slot 12 to Node 3/Slot 12. You create the protect path by placing Slot 6 in 1+1 protection with Slot 5 at Nodes 1 and 2, and placing Slot 12 in 1+1 protection with Slot 13 at Nodes 2 and 3.

Figure 5-35   Linear (point-to-point) ADM configuration

Procedure: Create a Linear ADM

Purpose	Use this procedure to create a linear ADM. Complete the steps for each node that will be included in the linear ADM.
Prerequisite Procedures	Complete the general setup information for the node that you want to configure for linear ADM. For procedures, see the "Setting Up Basic Node Information" section on page 3-3.
	Set up the network information for the node. For procedures, see the "Setting Up Network Information" section on page 3-5.
Onsite/Remote	Onsite or remote

Step 1   Set up 1+1 protection for the STM-N cards in the ADM. In Figure 5-35 on page 5-47, 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 Card Protection Groups" section on page 3-26.

Step 2   For STM-N ports connecting ONS 15454 SDH nodes, set the SDH DCC terminations.

    a.   Start CTC for a linear ADM node and choose the **Provisioning > SDH DCC** tabs.

    b.   In the SDCC Terminations section, click **Create**.

> **Note**   The terminating nodes (Nodes 1 and 3 in Figure 5-35 on page 5-47) will have one SDCC, and the intermediate nodes (Node 2 in Figure 5-35) will have two SDCCs.

Step 3   Select the **Set to IS, if allowed** radio button. This radio button places the card ports in service.

> **Note**   There are four port state options. Select the port state that best fits your requirements. For example, you can select the set OOS to OOS-MT radio button if you are provisioning the ADM before installing cards and fiber. Also, you can select the OOS-MT port state if you want to avoid DCC termination alarms until you configure all DCCs on all nodes.

Step 4   (Optional) Below the port state options you can also enable or disable OSPF on the DCC according to your requirements.

Step 5   Click **OK**.

Step 6   The slots/ports appear in the SDCC Terminations list.

Step 7   Complete Step 1 to 5 at each node.

> **Note**   The ONS 15454 SDH uses the SDH regenerator section DCC (SDCC) for data communications. It does not use the multiplex section DCCs; therefore, the multiplex section DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 SDH networks. For more detail, see the "Creating DCC Tunnels" section on page 6-34.

Step 8   Set up the node timing. If a node is using line timing, set the working STM-N card as the timing source. See the "Setting Up ONS 15454 SDH Timing" section on page 3-18.

Procedure: Convert a Linear ADM to an SNCP Ring

> ⚠ **Caution**   This procedure is service affecting.

> ⚠ **Caution**   Always wear an authorized ESD wrist band when removing or installing ONS 15454 SDH cards.

Purpose	The following procedures describe how to convert a three-node linear ADM to an SNCP ring.
Tools	SDH test set.
Prerequisite Information	This procedure assumes you have an existing linear ADM that you want to convert to an SNCP ring.
Onsite/Remote	Onsite

Step 1 Start CTC for one of the nodes that you want to convert from a linear ADM to an SNCP ring.

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

Step 3 Under Protection Groups, choose 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 it is, proceed 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, choose the Protect/Active slot.

   a. From the Switch Commands, choose **Manual**.

   b. Click **Yes** on the confirmation dialog box.

   c. Under Selected Group, verify that the working slot/port is 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, choose **Clear**. A Confirm Clear Operation dialog box 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 STM-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.

   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.

Step 7 Physically remove one of the protect fibers running between the middle and end nodes. For example, in Figure 5-36 on page 5-50, the fiber from Node 2/Slot 13 to Node 3/Slot 13 is removed. The corresponding STM-16 card will cause an LOS condition for that fiber and port.

Figure 5-36   Converting a linear ADM to an SNCP ring
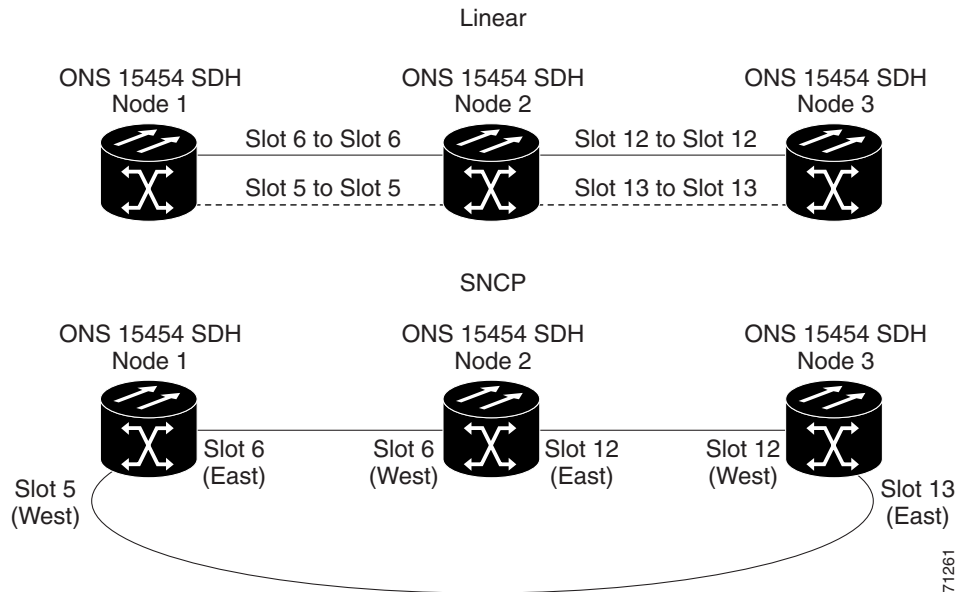
Step 8   Physically reroute the other protect fiber to connect the two end nodes. In the Figure 5-36 example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 is rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

If you are leaving the STM-N cards in place, proceed to Step 13. If you are removing the cards, complete Steps 9 to 12. (In this example, cards in Node 2/Slots 5 and 13 are removed.)

Step 9   In the middle node, place the cards you are removing out of service.

   a.   Display the first card in card view and choose the **Provisioning > Line** tabs.

   b.   Under Status, choose **OOS**. 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.

   b.   Right-click the card you just took out of service (e.g., Slot 5) and choose **Delete Card**.

   c.   Click **Yes** on the confirmation dialog box.

   d.   Repeat Steps a to c for the second card (e.g., Slot 13).

Step 11   Save all circuit information.

   a.   In node view, choose the **Provisioning > Circuits** tab.

   b.   Record the circuit information using one of the following methods:

   –   From the File menu, choose **Print** to print the circuits table.

   –   From the File menu, choose **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 CTC Data" section on page 2-29 and the "Exporting CTC Data into Other Applications" section on page 2-30 for more information.

Step 12   Remove the STM-N cards that are no longer connected to the end nodes (Slots 5 and 13, in the example).

Step 13   In CTC, display one of the end nodes (Node 1 or Node 3 in the example).

Step 14   Click the **Provisioning > SDH DCC** tabs.

Step 15   In the SDCC Terminations section, click **Create**.

Step 16   In the Create SDCC Terminations dialog box, choose the slot/port that was the protect slot in the linear ADM. For example, in Node 1 the previous protect slot is Slot 5/Port 1 (STM-16).

Step 17   Click **OK**.

An EOC SDCC alarm will occur until you create an SDCC termination on the adjacent node.

Step 18   Display the node on the opposite end (Node 3 in the Figure 5-36 example) and repeat Steps 14 to 17.

Step 19   Delete and reenter the circuits one at a time. (See the "Creating VC High-Order Path Circuits" section on page 6-3.)

> ✎
>
> **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. (In the example, the protect path is Node 1/Slot 5 to Node 2/Slot 5 to Node 3/Slot 13.) With the new SNCP, create circuits with protection.

Deleting the first circuit and recreating it to the same card/port should restore the circuit immediately.

Step 20   Monitor your SDH 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 in the example) is working. To do this, display the network view and move your cursor to the green span (between Node 1 and Node 3 in the example).

Although the cursor only shows the first circuit created, do not become alarmed that the other circuits are not present. Verify with the SDH test set that the original circuits and the new circuits are operational. The original circuits were created on the counterclockwise linear path.

Step 22   Display the network view to view the newly created ring.

Procedure: Convert a Linear ADM to an MS-SPRing

> ⚠
>
> **Caution**   This procedure is service affecting.

> ⚠
>
> **Caution**   Always wear an authorized ESD wrist band when removing or installing ONS 15454 SDH cards.

Purpose	The following procedures describe how to convert a three-node linear ADM to an MS-SPRing.
Tools	SDH test set.
Prerequisite Information	This procedure assumes you have an existing linear ADM that you want to convert to an MS-SPRing.
Onsite/Remote	Onsite

Step 1   Start CTC for 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, choose 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 it is, proceed 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, choose the Protect/Active slot.

    a.   From the Switch Commands pull-down menu, choose **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 to Step d.

    d.   From the Switch Commands, choose **Clear**. A Confirm Clear Operation dialog box 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 STM-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 SDH 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 example in Figure 5-37 on page 5-53, the fiber running from Node 2/Slot 13 to Node 3/Slot 13 is removed. The corresponding end-node trunk card will display an LOS alarm.

Figure 5-37   Converting a linear ADM to an MS-SPRing
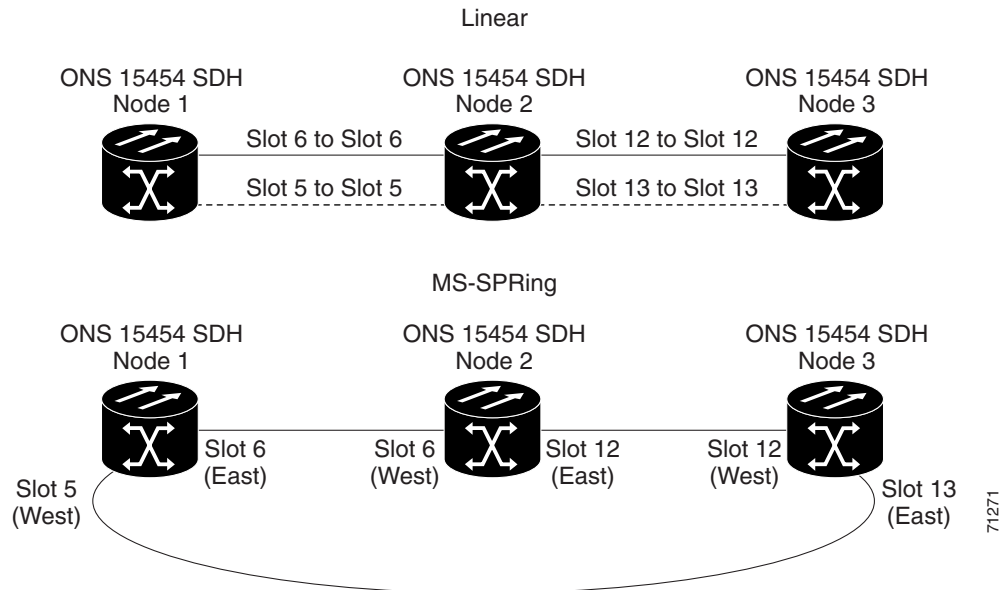
Step 8   Physically reroute the other protect fiber so it connects the two end nodes. In the Figure 5-37 example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 is rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

If you are leaving the STM-N cards in place, proceed to Step 13. If you are removing the cards, complete Steps 9 to 12. (In this example, the cards in Node 2/Slots 5 and 13 are removed.)

Step 9   In the middle node, place the cards that you are removing out of service.

   a.   Display the first card in card view, then choose the **Provisioning > Line** tabs.

   b.   Under Status, choose **OOS**. Click **Apply**.

   c.   Repeat Steps a and b for the second card.

Step 10   Delete the cards from CTC.

   a.   From the View menu, choose **Node View**.

   b.   Right-click the card you just took out of service (e.g., Slot 5) and choose **Delete Card**.

   c.   Click **Yes** on the confirmation dialog box.

   d.   Repeat Steps a through c for the second card (e.g., Slot 13).

Step 11   Save all circuit information.

   a.   In node view, choose the **Provisioning > Circuits** tab.

   b.   Record the circuit information using one of the following procedures:

       –   From the File menu, choose **Print** to print the circuits table.

       –   From the File menu, choose **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 CTC Data" section on page 2-29 and the "Exporting CTC Data into Other Applications" section on page 2-30 for more information.

Step 12   Remove the STM-N cards that are no longer connected to the end nodes (Slots 5 and 13 in the example).

Step 13   Start CTC for an end node. In node view, click the **Provisioning > SDH 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 [STM-16] 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   Start CTC for the node on the opposite end (Node 3 in Figure 5-37) and repeat Steps 13 to 16.

Step 18   For circuits running on an MS-SPRing protect VC4 (VC4 3 to 4 for an STM-4 MS-SPRing, VC4s 9 to 16 for an STM-16 MS-SPRing, and VC4s 33 to 64 for an STM-64), delete and recreate the circuit:.

    a.   Delete the first circuit by clicking the **Circuits** tab. Choose the circuit, click **Delete**, and click **Yes** when prompted.

    b.   Recreate the circuit on VC4s 3 to 4 (for an STM-4 MS-SPRing), VC4s 9 to 16 (for an STM-16 MS-SPRing), or VC4s 33 to 64 (for an STM-64 MS-SPRing) on the fiber that served as the protect fiber in the linear ADM. During circuit creation, uncheck **Route Automatically** and **Fully Protected Path** on the Circuit Creation dialog box so you can manually route the circuit on the appropriate VC4s. See the "Create a Unidirectional Circuit with Multiple Drops" procedure on page 6-17 for more information.

    c.   Repeat Steps a and b for each circuit residing on an MS-SPRing protect VC4.

    ✎   **Note**   Deleting circuits is traffic affecting.

Step 19   Follow all procedures in the "Setting Up MS-SPRings" section on page 5-24 to configure the MS-SPRing. The ring should have an East/West logical connection. While it may not physically be possible to connect the STM-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 MS-SPRing. Do not accept the MS-SPRing ring map until all nodes are provisioned.

    ✎   **Note**   E-W Mismatch alarms will occur until all nodes are provisioned.

Step 20   Display the network view to verify the newly created ring.

5.11 Extended SNCP Mesh Networks

In addition to single MS-SPRings, SNCP rings, and ADMs, you can extend ONS 15454 SDH traffic protection by creating extended SNCP mesh networks. Extended SNCPs include multiple ONS 15454 SDH topologies and extend the protection provided by a single SNCP ring to the meshed architecture of several interconnecting rings.

In an extended SNCP, circuits travel diverse paths through a network of single or multiple meshed rings. When you create circuits, you can provision CTC to automatically route circuits across the extended SNCP, 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 5-38, 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; CTC then automatically creates cross-connections at Nodes 3, 8, 7, and 9 to provide the primary circuit path.
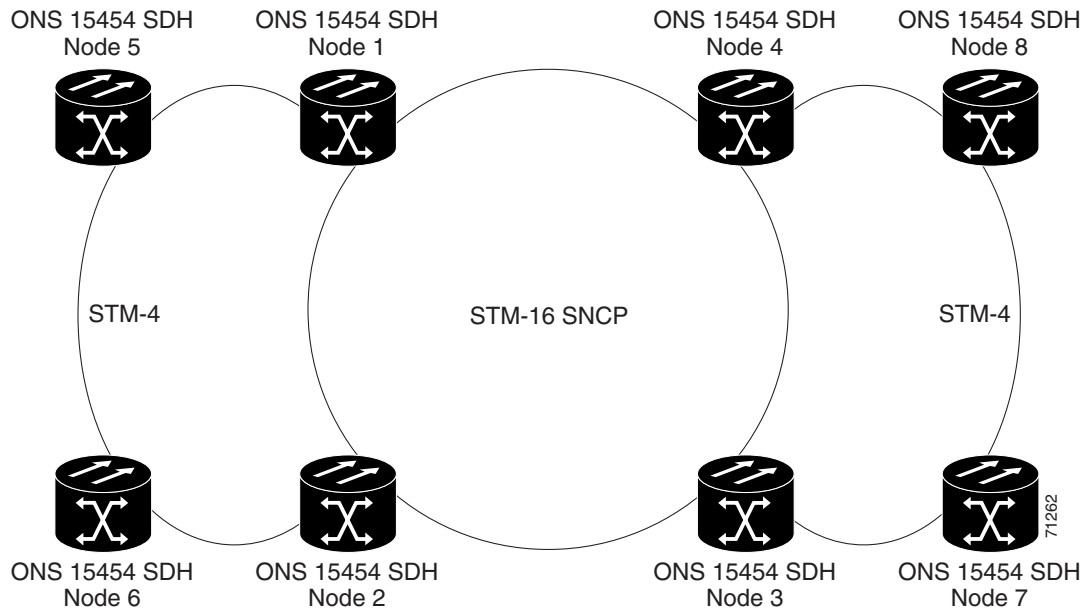
If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 that, in this example, passes through Nodes 2, 1, and 11. Cross-connections are automatically created at Nodes, 3, 2, 1, 11, and 9, shown by the dashed line. If a failure occurs on the primary path, traffic switches 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 5-38 Extended SNCP mesh network
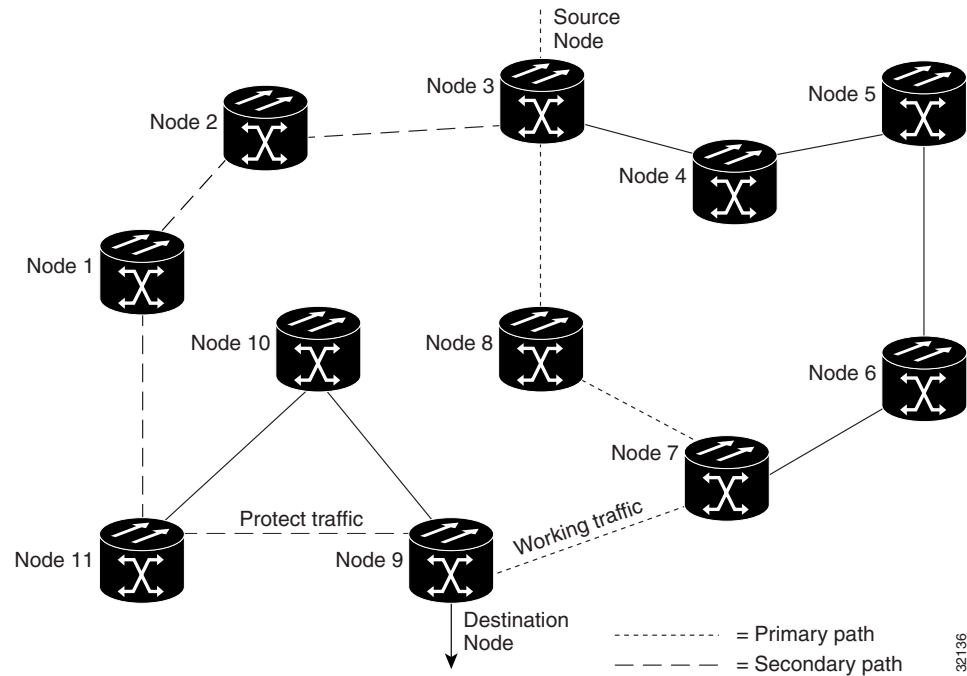
Extended SNCPs also allow spans of different SDH line rates to be mixed together in "virtual rings." Figure 5-39 on page 5-56 shows Nodes 1, 2, 3, and 4 in a standard STM-16 ring. Nodes 5, 6, 7, and 8 link to the backbone ring through STM-4 fiber. The "virtual ring" is formed by Nodes 5, 6, 7, and 8 uses both STM-16 and STM-4 speeds.

ONS 15454 SDH   ONS 15454 SDH   ONS 15454 SDH   ONS 15454 SDH
Node 5   Node 1   Node 4   Node 8

STM-4   STM-16 SNCP   STM-4

ONS 15454 SDH   ONS 15454 SDH   ONS 15454 SDH   ONS 15454 SDH
Node 6   Node 2   Node 3   Node 7

71262

5.12 Common Ring-Related Procedures

You enable card ports and check for alarms during all topology-provisioning procedures. Use the following procedures when required.

Procedure: Put Ports In or Out of Service

Purpose	Use this procedure to put a port in service or to remove a port from service.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Note   To provision Ethernet cards, see Chapter 9, "Ethernet Operation."

Step 1   Display the node (default) view.

Step 2   In the shelf graphic, double-click the card with the port(s) you want to put in or out of service. The card view displays.

Step 3   Click the **Provisioning > Line** tabs.

Step 4   Under State, choose one of the following:

- **IS**—Puts the port in service.

- **OOS**—Puts the port out of service.

- **OOS_MT**—Sets the port to a maintenance state; alarms are suppressed and loopbacks can be performed.

- **OOS_AINS**—Sets the port to an auto-inservice state; alarms are suppressed and loopbacks can be performed until a signal is received for the time specified in AINS Soak, after which the state is changed to IS.

Step 5   If you set State to OOS-AINS, set the soak period time in the AINS Soak field. This is the amount of time that the state will stay in OOS-AINS state after the signal is continuously received.

Step 6   Click **Apply**.

Step 7   Repeat this procedure for each port as needed.

Procedure: Check for Alarms

Purpose	This procedure explains how to check for alarms.
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Log into CTC on a network node and display the network view.

Step 2   Verify the following:

- All spans on the network view are green.
- In the **Alarms** tab (Figure 5-40 on page 5-58), no critical or major alarms are present, nor any facility alarms, such as LOS or LOF. In a ring, these facility conditions may be reported as minor alarms.
- In the **Conditions** tab (Figure 5-41 on page 5-58), no ring switches are active.

If trouble is indicated, for example, if a major alarm exists, resolve the problem before proceeding. Refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* for alarm troubleshooting procedures.

Figure 5-40 on page 5-58 shows how to check spans and alarms in the network view. Figure 5-41 on page 5-58 shows how to check conditions in the network view.

Figure 5-40   Checking spans and alarms in the network view

Figure 5-41   Checking conditions in network view

Circuits and Tunnels

This chapter explains how to create and administer Cisco ONS 15454 SDH VC high-order path circuits and VC low-order path tunnels. Table 6-1 lists the chapter topics. Table 6-2 lists circuit and tunnel procedures on the Cisco ONS 15454 SDH.

Table 6-1   Circuit and Tunnel Topics

Table 6-2   Circuit and Tunnel Procedures

Chapter 6   Circuits and Tunnels

■ **Introduction**

Table 6-2   Circuit and Tunnel Procedures (continued)

Circuit and Tunnel Procedures

Procedure: Monitor a Path Trace on STM-N Ports, page 6-25

Procedure: Create a Half Circuit using an STM-N Card as a Destination in an MS-SPRing or 1+1 Topology, page 6-26

Procedure: Create a Half Circuit using an STM-N as a Destination in an SNCP, page 6-27

Procedure: Filter the Display of Circuits, page 6-29

Procedure: View Circuits on a Span, page 6-30

Procedure: Change a Circuit State, page 6-31

Procedure: Edit a Circuit Name, page 6-32

Procedure: Change Active and Standby Span Color, page 6-32

Procedure: Provision a DCC Tunnel, page 6-35

6.1 Introduction

You can create VC high-order path circuits and VC low-order path tunnels across and within ONS 15454 SDH nodes and assign different attributes to circuits. For example, you can:

- Create one-way, two-way, or broadcast circuits.
- Assign user-defined names to circuits.
- Assign different circuit sizes. The E3 and DS3I cards must use VC low-order path tunnels. E1 cards, optical cards, and Ethernet cards use VC high-order path circuits. Available sizes are VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, and VC4-64c for optical cards and some Ethernet cards depending on the card type. Of the Ethernet cards, only the G-1000 can use VC4-3c and VC4-8c.

Note   To create Ethernet circuits, see the "E-Series Circuit Configurations" section on page 9-15 or the "G1000-4 Circuit Configurations" section on page 9-33.

- Automatically or manually route VC high-order path circuits.
- Automatically route VC low-order path tunnels.
- Automatically create multiple circuits.
- Provide full protection to the circuit path.
- Provide only protected sources and destinations for circuits.
- Define a secondary circuit source or destination that allows you to interoperate an ONS 15454 SDH subnetwork connection protection (SNCP) ring with third-party equipment SNCPs.
- Create PCA circuits. You can provision circuits to carry traffic on MS-SPRing protection channels when conditions are fault-free. Traffic routed on MS-SPRing protection channels, called extra traffic, has lower priority than the traffic on the working channels and has no means for protection.

   During ring or span switches, protection channel circuits are pre-empted and squelched. For example, in a 2-fiber STM-16 MS-SPRing, VC4s 9-16 can carry extra traffic when no ring switches are active, but protection channel circuits on these VC4s are pre-empted when a ring switch occurs. When the conditions that caused the ring switch are corrected and the ring switch removed, protection channel circuits are restored (assuming the MS-SPRing is provisioned as revertive).

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

6-2

September 2002

Provisioning traffic on MS-SPRing protection channels is performed during circuit provisioning. The protection channel checkbox displays whenever Fully Protected Path is deselected on the circuit creation wizard. See the "Create an Automatically Routed High-Order Path Circuit" procedure on page 6-4 or "Create a Manually Routed High-Order Path Circuit" procedure on page 6-9 for more information. When provisioning protection channel circuits, two considerations are important to keep in mind:

- If MS-SPRings are provisioned as non-revertive, protection channel circuits will not be restored following a ring or span switch until the MS-SPRing is manually switched.

- Protection channel circuits will be routed on working channels when you upgrade an MS-SPRing, either from a a 2-fiber to a 4-fiber, or from one optical speed to a higher one. For example, if you upgrade a 2-fiber STM-16 MS-SPRing to an STM-64, VC4s 9-16 on the STM-16 MS-SPRing become working channels on the STM-64 MS-SPRing.

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 SDH to allow a circuit to enter and exit an ONS 15454 SDH. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15454 SDH network) to the drop or destination (where traffic exits an ONS 15454 SDH network).

6.2 Creating VC High-Order Path Circuits

This section explains how to create VC high-order path circuits. The E1 card, STM-N cards, and Ethernet cards all use high-order path circuits. To create circuits for E3 and DS3I cards, see the "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12. For an explanation of circuits and tunnels, see the "Cross-Connect Card Capacities" section on page 6-33.

You can create unidirectional or bidirectional, revertive or non-revertive, high-order path circuits. CTC can route circuits automatically or you can use CTC to manually route circuits.

You can provision circuits at any of the following points:

- Before cards are installed. The ONS 15454 SDH 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 cannot carry traffic until you install the cards and place their ports in service. For card installation procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37. For ring-related procedures, see Chapter 5, "SDH Topologies."

- After cards are installed, but before their ports are in service (enabled). You must place the ports in service before circuits will carry traffic.

- After cards are installed and their ports are in service. Circuits will carry traffic as soon as the signal is received.

Note Circuits assigned to a state other than OOS using an E1, E3, and DS3I card for the source and destination ports can change to IS even though a signal is not present on the ports. Some cross connects transition to IS, while others are OOS_AINS. A circuit state called partial may appear during a manual transition for some abnormal reason, such as a CTC crash, communication error, or one of the connections could not be changed.

Procedure: Create an Automatically Routed High-Order Path Circuit

Purpose	Use this procedure to create an automatically routed, high-order path circuit. 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.
Prerequisite Procedures	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 3-27.
Onsite/Remote	Onsite or remote

Step 1   Log into a node on the network where you will create the circuit.
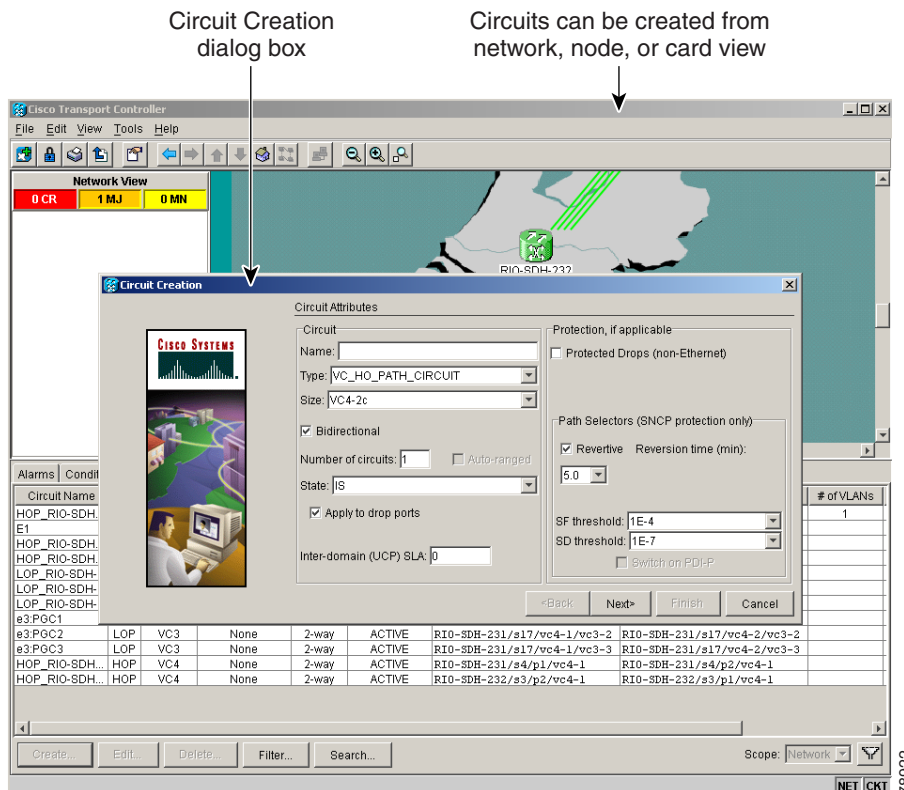
Note   Circuits can be created from the network view, node view, or card view.

Step 2   From the View menu, select **Go to Network View**.

Step 3   Click the **Circuits** tab, then click **Create** (Figure 6-1).

Figure 6-1   Creating an automatically routed circuit (high-order path circuit)

Step 4   In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.

> **Note** If you will ever create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

- Type—Select **VC_HO_Path_Circuit (HOP)**. The circuit type determines the circuit-provisioning options that are displayed. The E3 and DS3I cards must use VC low-order path tunnels. See the "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12 for more information.

- Size—Select the circuit size (VC_HO_Path_Circuits only). VC high-order path circuits can be VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c for optical cards and some Ethernet cards depending on the card type. Of the Ethernet cards, only the G-1000 can use VC4-3c and VC4-8c. The "c" indicates concatenated VC4s.

- Bidirectional—Check this box to create a two-way circuit; uncheck it to create a one-way circuit.

- Number of circuits—Type the number of circuits you want to create. The default is 1. If you enter more than one, you can use auto-ranging to create the additional circuits automatically.

- Auto-ranged—This check box is automatically selected when you enter more than 1 in the Number of circuits field. Leave the box checked if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically. Uncheck the box if you do not want to create circuits automatically.

- State—Choose one of the following service states to apply to the circuit:
  - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.
  - IS—The circuit is in service.
  - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Check this box to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If not checked, CTC will not change the state of the source and destination ports.

> **Note** LOS alarms display if in service (IS) ports are not receiving signals.

- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Select this box if you want the circuit routed to protected drops only, that is, to ONS 15454 SDH cards that are in 1:1, 1:N, or 1+1 protection. If you select this box, CTC only displays protected cards as source and destination choices.

Step 5 If the circuit will be routed on an SNCP, set the following SNCP path selector defaults as follows:

- 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—Choose from one E-3, one E-4, or one E-5.

- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.

- Switch on PDI-P—Check this box if you want traffic to switch when a VC4 payload defect indicator is received (VC4 circuits only).

Step 6   Click **Next**.

Step 7   In the Circuit Source dialog box, set the circuit source.

Options include node, slot, port, and VC4. The options displayed depend on the circuit type, the circuit properties selected in Step 4, and the cards installed in the node. Click **Use Secondary Source** if you need to create an SNCP bridge/selector circuit entry point in a multivendor SNCP.

> **Note**   E1 cards use VC4 circuits. All 12 of the E1 ports use VC4 bandwidth.

> **Note**   For information about Ethergroups, see the "E-Series Circuit Configurations" section on page 9-15 and the "G1000-4 Circuit Configurations" section on page 9-33.

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

Step 9   In the Circuit Destination dialog box, enter the appropriate information for the circuit destination. If the circuit is bidirectional, click **Use Secondary Destination** if you need to create an SNCP bridge/selector circuit destination point in a multivendor SNCP. (To add secondary destinations to unidirectional circuits, see the "Create a Unidirectional Circuit with Multiple Drops" procedure on page 6-17.)

Step 10   Click **Next**.

Step 11   Under Circuit Routing Preferences (Figure 6-2 on page 6-7), choose **Route Automatically**. The following options are available:

- Using Required Nodes/Spans—Select this check box to specify nodes and spans to include or exclude in the CTC-generated circuit route.

- Review Route Before Creation—Select this check box to review and edit the circuit route before the circuit is created.

Figure 6-2   Setting circuit routing preferences

Circuit Creation
dialog box routing preferences
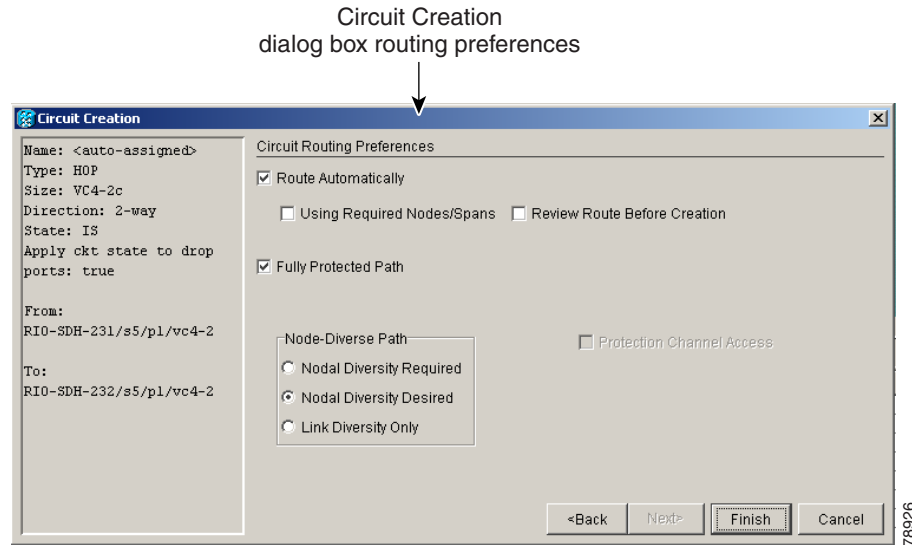
Step 12 Set the circuit path protection as follows:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and go to Step 13. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have SNCP path segments with primary and alternate paths. The path diversity options only apply to SNCP path segments, if any exist.

- To create an unprotected circuit, uncheck **Fully Protected Path** and go to Step 14.

- To route the circuit on an MS-SPRing protection channel, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **OK** on the Warning dialog box, then go to Step 14.

⚠
Caution   Circuits routed on PCA are not protected and are preempted during MS-SPRing and span switches.

Step 13 If you selected **Fully Protected Path**, choose one of the following:

- Nodal Diversity Required—Ensures that the primary and alternate paths within the extended SNCP mesh network portions of the complete circuit path are nodally diverse. (For information about extended SNCP, see the "Extended SNCP Mesh Networks" section on page 5-54.)

- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the extended SNCP mesh network portion of the complete circuit path.

- Link Diversity Only—Specifies that only link-diverse primary and alternate paths for extended SNCP mesh network portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 14 If you selected **Using Required Nodes/Spans** in Step 11, complete the following substeps. If you did not select this check box, proceed to Step 15.

  a. Click **Next** to display the Circuit Route Constraints screen (Figure 6-3 on page 6-8).

  b. On the circuit map, click a node or span. (Span is also called link in CTC.)

  c. Click **Include** to include the node or span in the circuit. Click **Exclude** to exclude the node or 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.

d. Repeat Step c for each node or span you want to include or exclude.

e. Review the circuit route. After you add the spans and nodes, you can use the **Up** and **Down** buttons to change the circuit routing order.

f. Click **Remove** to remove a node or span.

g. If you selected **Review Route Before Creation** in Step 11, click **Next** and follow Step 15. When you are finished, click **Finish** and go to Step 16.

Figure 6-3   Specifying circuit constraints
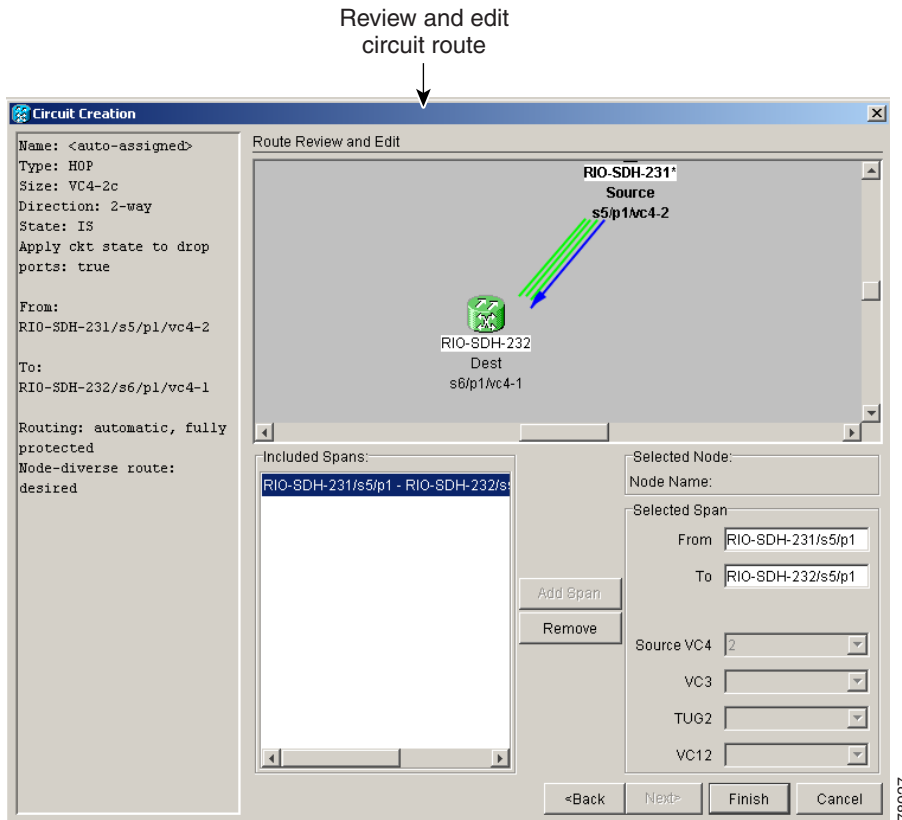
Step 15 If you selected **Review Route Before Creation** in Step 11, click **Next** to display the route. If you did not select this check box proceed to Step 16. The following options are available:

- 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.

Step 16 After you click **Finish**, CTC creates the circuit and returns to the Circuits window. If you entered more than one in the Number of Circuits field in Step 4, 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, proceed to Step 17.

Step 17   If you left the ports out of service in Step 4, the cards must be installed and the ports placed in service before circuits will carry traffic. For card installation procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37. For ring-related procedures, see Chapter 5, "SDH Topologies."

Procedure: Create a Manually Routed High-Order Path Circuit

Purpose	Use this procedure to create a manually routed high-order path circuit.
Prerequisite Procedures	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 3-27.
Onsite/Remote	Onsite or remote

Step 1   Log into a node on the network where you will create the circuit.

✎
Note   Circuits can be created from the network view, node view, or card view.

Step 2   From the View menu, select **Go to Network View**.

Step 3   Click the **Circuits** tab, then click **Create**.

Step 4   In the Circuit Creation dialog box (Figure 6-4 on page 6-10), complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.

  ✎
  Note   If you will ever create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

- Type—Select **VC_HO_Path_Circuit (HOP)**. The circuit type determines the circuit-provisioning options that are displayed. The E1, E3, and DS3I cards must use VC low-order path tunnels. See the "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12.

- Size—Select the circuit size (VC_HO_Path_Circuits only). VC high-order path circuits can be VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c for optical cards and some Ethernet cards depending on the card type. Of the Ethernet cards, only the G-1000 can use VC4-3c and VC4-8c. The "c" indicates concatenated VC4s.

- Bidirectional—For this procedure, leave the Bidirectional check box checked (default).

- 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—Deselect the box if you do not want to create multiple circuits automatically. This check box is automatically selected when you enter more than 1 in the Number of circuits field. Leave the box selected if you are creating multiple optical circuits with the same source and destination and you want CTC to create the circuits automatically.

- State—Choose one of the following service states to apply to the circuit:
  - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.
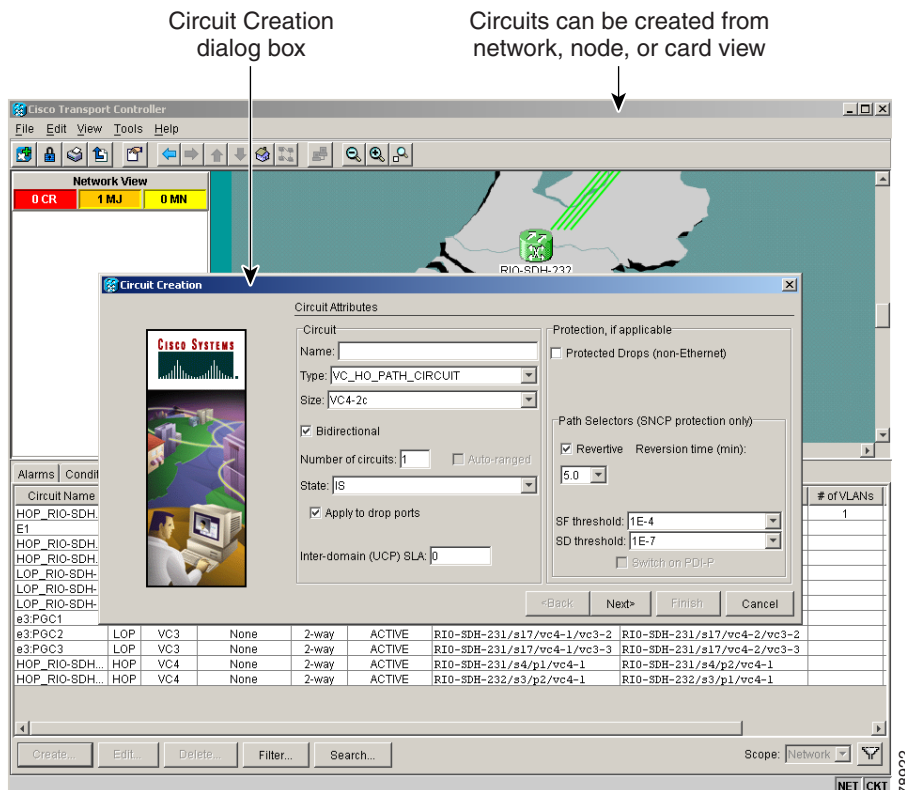
- – IS—The circuit is in service.

- – OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

- – OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- • Apply to drop ports—Check this box to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If not checked, CTC will not change the state of the source and destination ports.

Note LOS alarms display if in service (IS) ports are not receiving signals.

- • Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- • Protected Drops—Check this box if you want the circuit routed to protected drops only, that is, to ONS 15454 SDH cards that are in 1:1, 1:N, or 1+1 protection. If you check this box, CTC only displays protected cards as source and destination choices.

Figure 6-4   Creating a manually routed circuit

Step 5 If the circuit will be routed on an SNCP, set the following SNCP path selector defaults as follows:

- Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted traffic 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—Choose from one E-3, one E-4, or one E-5.

- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.

- (VC4 circuits only) Switch on PDI-P—Check this box if you want traffic to switch when a VC4 payload defect indicator is received.

Step 6   Click **Next**.

Step 7   In the Circuit Source dialog box, set the circuit source.

Options include node, slot, port, and VC4. The options displayed depend on the circuit type, the circuit properties selected in Step 4, and the cards installed in the node.

✎
Note   E1 cards use VC4 circuits. All 12 of the E1 ports use VC4 bandwidth.

✎
Note   For information about Ethergroups, see the "E-Series Circuit Configurations" section on page 9-15 and the "G1000-4 Circuit Configurations" section on page 9-33.

Step 8   Click **Use Secondary Source** if you need to create an SNCP bridge/selector circuit entry point in a multivendor SNCP.

Step 9   Click **Next**.

Step 10   In the Circuit Destination dialog box, enter the appropriate information for the circuit destination. If the circuit is bidirectional, click **Use Secondary Destination** if you need to create an SNCP bridge/selector circuit destination point in a multivendor SNCP.

✎
Note   To add secondary destinations to unidirectional circuits, see the "Create a Unidirectional Circuit with Multiple Drops" procedure on page 6-17.

Step 11   Click **Next**.

Step 12   Under Circuit Routing Preferences (Figure 6-2), deselect **Route Automatically**.

Step 13   Set the circuit path protection as follows:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and go to Step 14. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have SNCP path segments with primary and alternate paths. The path diversity options only apply to SNCP path segments, if any exist.

- To create an unprotected circuit, uncheck **Fully Protected Path** and go to Step 15.

- To route the circuit on an MS-SPRing protection channel, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **OK** on the Warning dialog box, then go to Step 15.

⚠

Caution   Circuits routed on PCA are not protected and are preempted during MS-SPRing and span switches.

Step 14   If you selected **Fully Protected Path** in Step 13, choose one of the following. If you did not select **Fully Protected Path**, go to Step 15.

- Nodal Diversity Required—Ensures that the primary and alternate paths within the extended SNCP mesh network portions of the complete circuit path are nodally diverse. (For information about extended SNCP, see the "Extended SNCP Mesh Networks" section on page 5-54.)

- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the extended SNCP mesh network portion of the complete circuit path.

- Link Diversity Only—Specifies that only link-diverse primary and alternate paths for extended SNCP mesh network portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 15   Click **Next**. The Route Review and Edit screen 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 16   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 VC4, change it in the Source VC4 fields.

  c. Click **Add Span**.

The span is added to the Included Spans list and the span arrow turns blue.

Step 17   Repeat Step 16 until the circuit is provisioned from the source to the destination node.

When provisioning a protected circuit, you need to select only one path of MS-SPRing or 1+1 spans from the source to the drop. In SNCP, you must select both paths around the ring for the circuit to be protected.

Step 18   When the circuit is provisioned, click **Finish**.

If you entered more than one in the Number of Circuits field in the Circuit Attributes dialog box in Step 4, the Circuit Source dialog box is displayed so you can create the remaining circuits.

Step 19   If you left the ports out of service in Step 4, the cards must be installed and the ports placed in service before circuits will carry traffic. For card installation procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37. For ring-related procedures, see Chapter 5, "SDH Topologies."

6.3 Creating VC Low-Order Path Tunnels for Port Grouping

This section explains how to create VC low-order path tunnels for the E3 and DS3I cards. The E1 card, STM-N cards, and Ethernet cards all use high-order path circuits. See the "Creating VC High-Order Path Circuits" section on page 6-3. For more information about cross-connections and signal rates, see the "Cross-Connect Card Capacities" section on page 6-33.

VC low-order path tunnels (VC_LO_PATH_TUNNEL) are automatically set to bidirectional with port grouping enabled. Three ports form a port group. For example, in one E3 or one DS3I card, there are four port groups: Ports 1 to 3 = PG1, Ports 4 to 6 = PG2, Ports 7 to 9 = PG3, and Ports 10 to 12 = PG4.

Note CTC shows VC3-level port groups, but the XC10G creates only VC4-level port groups. VC4 tunnels must be used to transport VC3 signal rates.

Tunnels are routed automatically. The following rules apply to port-grouped circuits:

- A port group goes through a VC_LO_PATH_TUNNEL circuit, with a set size of VC4.
- The circuit must be bidirectional and cannot use multiple drops.
- The circuit number must be set to one.
- The Auto-ranged field must be set to Yes.
- The Use secondary destination field must be set to No.
- The Route Automatically field must be set to Yes.
- Monitor circuits cannot be created on a VC3 circuit in a port group.
- Circuits assigned to a state other than OOS using an E1, E3, and DS3I card for the source and destination ports can change to IS even though a signal is not present on the ports. Some cross connects transition to IS, while others are OOS_AINS. A circuit state called partial may appear during a manual transition for some abnormal reason, such as a CTC crash, communication error, or one of the connections could not be changed.

You can provision circuits at any of the following points:

- Before cards are installed. The ONS 15454 SDH 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.) For card installation procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37. For ring-related procedures, see Chapter 5, "SDH Topologies."
- After cards are installed, but before ports are in service (enabled). You must place the ports in service before circuits will carry traffic.
- After cards are installed and their ports are in service. Circuits will carry traffic when the signal is received.

Procedure: Create a Low-Order Path Tunnel for Port Grouping

Purpose	Use this procedure to create an automatically routed, low-order path tunnel for port grouping.
Prerequisite Procedures	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 3-27.
Onsite/Remote	Onsite or remote

Step 1 Log into a node on the network where you will create the circuit.

Note Circuits can be created from the network view, node view, or card view.

Step 2 From the View menu, select **Go to Network View**.

Step 3 Click the **Circuits** tab, then click **Create**.

Step 4 In the Circuit Creation dialog box (Figure 6-5 on page 6-15), complete the following fields:

- Name—(optional) Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.

> **Note** If you will ever create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

- Type—Select **VC_LO_Path_Tunnel**. The circuit type determines the circuit-provisioning options that are displayed. The E3 and DS3I cards must use VC low-order path tunnels.

- Size—This field is automatically set to VC4.

- For VC3 Port Grouping Only—The check box is automatically selected.

- Bidirectional—The check box is automatically selected. (VC low-order path tunnels are bidirectional.)

- Number of circuits—This field automatically lists one port group.

  Three ports form one port group. For example, in one E3 or one DS3I card, there are four port groups: Ports 1 to 3 = PG1, Ports 4 to 6 = PG2, Ports 7 to 9 = PG3, and Ports 10 to 12 = PG4. Low-order path tunneling is performed at the VC3 level.

- Auto-ranged—The check box is automatically selected.

  If you select the source and destination of one circuit, CTC automatically determines the source and destination for the remaining circuits in the Number of circuits field and creates them. To determine the source and destination, CTC increments the most specific part of the end point. An end point can be a port or a VC4. If CTC cannot find a valid destination, 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.

- State—Choose one of the following service states to apply to the circuit:

  – OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

  – IS—The circuit is in service.

  – OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

  – OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Check this box to apply the state chosen in the State field to the circuit source and destination ports. CTC applies the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If not checked, CTC will not change the state of the source and destination ports.

> **Note** LOS alarms display if in service (IS) ports are not receiving signals.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Select this box if you want the circuit routed to protected drops only, that is, to ONS 15454 SDH cards that are in 1:1, 1:N, or 1+1 protection. If you select this box, CTC only displays protected cards as source and destination choices.

Figure 6-5   Creating an automatically routed circuit (low-order path tunnel)
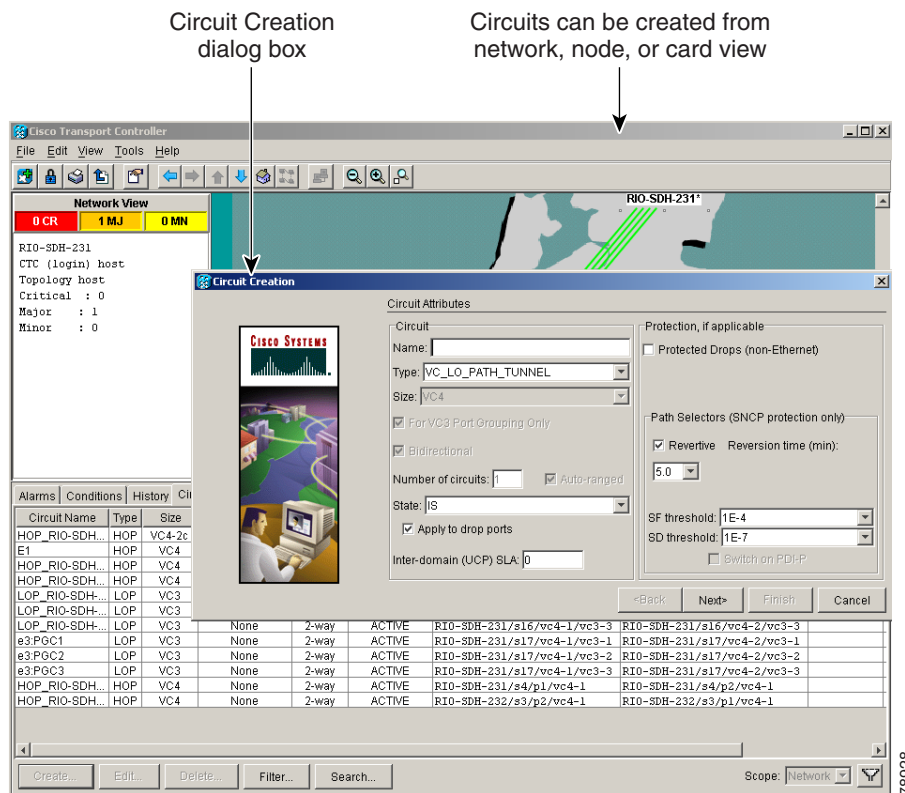
Step 5   If the circuit will be routed on an SNCP, set the SNCP path selector defaults as follows:

- Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted the traffic 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—Choose from one E-3, one E-4, or one E-5.

- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.

- Switch on PDI-P—The check box is automatically deselected.

Step 6   Click **Next**.

Step 7   In the Circuit Source dialog box, set the circuit source.

Options include node, slot, and VC4. The options displayed depend on the circuit type, the circuit properties selected in Step 4, and the cards installed in the node. For Ethergroups, see the "E-Series Circuit Configurations" section on page 9-15 and the "G1000-4 Circuit Configurations" section on page 9-33.

Step 8   Click **Next**.

Step 9   In the Circuit Destination dialog box, enter the appropriate information for the circuit destination.

Options include node, slot, and VC4. The options displayed depend on the circuit type, the circuit properties selected in Step 4, and the cards installed in the node.

Step 10   Click **Next**. Under Circuit Routing Preferences, **Route Automatically** is selected.

Step 11   Set the circuit path protection as follows:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and go to Step 12. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have SNCP path segments with primary and alternate paths. The path diversity options only apply to SNCP path segments, if any exist.

- To create an unprotected circuit, uncheck **Fully Protected Path** and go to Step 13.

- To route the circuit on an MS-SPRing protection channel, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **OK** on the Warning dialog box, then go to Step 13.

⚠

Caution   Circuits routed on PCA are not protected and are preempted during MS-SPRing and span switches.

Step 12   If you selected **Fully Protected Path**, choose one of the following. If you did not select **Fully Protected Path**, go to Step 13.

- Nodal Diversity Required—Ensures that the primary and alternate paths within the extended SNCP mesh network portions of the complete circuit path are nodally diverse. (For information about extended SNCP, see the "Extended SNCP Mesh Networks" section on page 5-54.)

- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the extended SNCP mesh network portion of the complete circuit path.

- Link Diversity Only—Specifies that only link-diverse primary and alternate paths for extended SNCP mesh network portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 13   Click **Finish**. CTC creates the circuit and returns to the Circuits window.

Step 14   If you left the ports out of service in Step 4, the cards must be installed and the ports placed in service before circuits will carry traffic. For card installation procedures, see the "Install Optical, Electrical, and Ethernet Cards" procedure on page 1-37. For ring-related procedures, see Chapter 5, "SDH Topologies."

6.4 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 receive (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 "Using Alarm Profiles" section on page 10-10 for information.

Procedure: Create a Unidirectional Circuit with Multiple Drops

Purpose	Use this procedure to create a unidirectional circuit with multiple drops.
Prerequisite Procedures	—
Onsite/Remote	Onsite or remote

Step 1 Use the "Create an Automatically Routed High-Order Path Circuit" procedure on page 6-4 to create a circuit. To make it unidirectional, uncheck the **Bidirectional** check box in the Circuit Creation dialog box.

Step 2 After the unidirectional circuit is created, in network, node or card view select the **Circuits** tab.

Step 3 Select the unidirectional circuit and click **Edit** (or double-click the circuit).

Step 4 In 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 In the Define New Drop dialog box, complete the appropriate fields to define the new circuit drop: Node, Slot, Port, and VC4.

Step 6 Under Target Circuit State, choose one of the following service states to apply to the circuit:

- OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

- IS—The circuit is in service.

- OOS-AINS—The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

- OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- No change—(default) The circuit remains in the current state.

Step 7 Set the circuit path protection as follows:

- To route the circuit on a protected path, leave **Fully Protected Path** checked (default) and go to Step 8. CTC creates a fully protected circuit route based on the path diversity option you choose. Fully protected paths might or might not have SNCP path segments with primary and alternate paths. The path diversity options only apply to SNCP path segments, if any exist.

- To create an unprotected circuit, uncheck **Fully Protected Path** and go to Step 9.

- To route the circuit on an MS-SPRing protection channel, uncheck **Fully Protected Path,** check **Protection Channel Access**, click **OK** on the Warning dialog box, then go to Step 9.

⚠

Caution   Circuits routed on PCA are not protected and are preempted during MS-SPRing and span switches.

Step 8 If you selected **Fully Protected Path**, choose one of the following. If you did not select **Fully Protected Path**, go to Step 9.

- Nodal Diversity Required—Ensures that the primary and alternate paths within the extended SNCP mesh network portions of the complete circuit path are nodally diverse. (For information about extended SNCP, see the "Extended SNCP Mesh Networks" section on page 5-54.)

- Nodal Diversity Desired—Specifies that node diversity is preferred, but if node diversity is not possible, CTC creates link-diverse paths for the extended SNCP mesh network portion of the complete circuit path.

- Link Diversity Only—Specifies that only link-diverse primary and alternate paths for extended SNCP mesh network portions of the complete circuit path are needed. The paths might be node-diverse, but CTC does not check for node diversity.

Step 9   Click **OK**.

Step 10   If you need to create additional drops, repeat Steps 4 to 9. If not, click **Close**. The **Close** button is represented as an icon in the upper right hand corner of the screen.

Step 11   Verify that the new drops appear on the Edit Circuit map as follows:

- 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, the text "Drop #1, Drop #2" appears under the node graphic.

6.5 Creating Monitor Circuits

You can set up secondary circuits to monitor traffic on primary bidirectional circuits. Monitor circuits can be created on E1 or STM-N cards. Figure 6-6 shows an example of a monitor circuit. At Node 1, a VC4 is dropped from Port 1 of an STM-1 card. To monitor the VC4 traffic, test equipment is plugged into Port 2 of the STM-1 card and a monitor circuit to Port 2 is provisioned in CTC. Circuit monitors are one-way. The monitor circuit in Figure 6-6 is used to monitor VC4 traffic received by Port 1 of the STM-1 card.

Note   Monitor circuits cannot be used with EtherSwitch circuits.

Figure 6-6   VC4 monitor circuit received at an STM-1 port
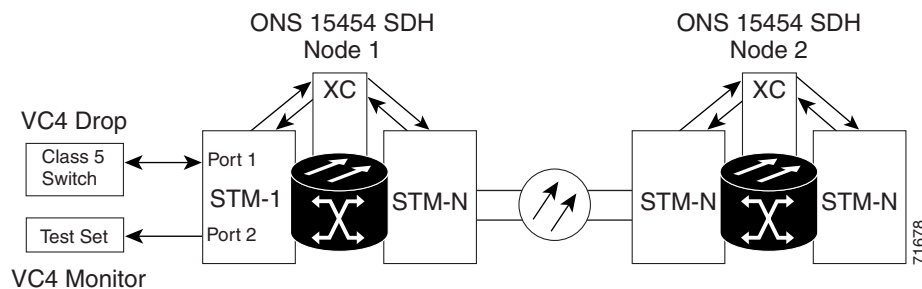
Procedure: Create a Monitor Circuit

Purpose   Use this procedure to set up secondary circuits to monitor traffic on primary bidirectional circuits.

	Prerequisite Procedures	For unidirectional circuits, create a drop to the port where the test equipment is attached.
	Onsite/Remote	Onsite or remote

Step 1   In node view, choose the **Circuits** tab.

Step 2   Click the bidirectional circuit that you want to monitor. Click **Edit**.

Step 3   In the Edit Circuit dialog box, click the **Monitors** tab.

The Monitors tab displays ports that you can use to monitor the circuit you selected in Step 2.

Step 4   Choose a port. The monitor circuit displays traffic coming into the node at the card/port you select.

Step 5   Click **Create Monitor Circuit**.

Step 6   In the Circuit Creation dialog box, choose the destination node, slot, port, and VC4 for the monitored circuit. In the Figure 6-6 example, this is Port 2 on the STM-1 card.

Step 7   If **Use Secondary Destination** is chosen, enter the slot, port, and VC4.

Step 8   Click **Next**.

Step 9   In the Circuit Creation dialog box confirmation, review the monitor circuit information. To route the monitor circuit on an MS-SPRing protection channel, check **Protection Channel Access** and click **OK** on the Warning dialog box.

Step 10   Click **Finish**.

Step 11   In the Edit Circuit dialog box, click **Close**. The **Close** button is represented as an icon in the upper right hand corner of the screen. The new monitor circuit displays on the Circuits tab.

6.6 Searching for Circuits

CTC provides the ability to search for ONS 15454 SDH circuits using the circuit name. You can conduct a search at the network, node, or card level, and search for whole words and/or include capitalization as a search parameter.

Procedure: Search for ONS 15454 SDH Circuits

	Purpose	Use this procedure to search for ONS 15454 SDH circuits based on circuit name.
	Prerequisite Procedures	"Creating VC High-Order Path Circuits" section on page 6-3 or "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12
	Onsite/Remote	Onsite or remote

Step 1   Display the appropriate CTC view.

- Network view to conduct searches at the network level

- Node (default) view to conduct searches at the node or network level

- Card view to conduct searches at the card, node, or network level

Step 2   Click the **Circuits** tab.

Step 3   If you are in node or card view, choose the scope for the search in the Scope field.

Step 4   Click **Search**.

Step 5   In the Circuit Name Search dialog box, complete the following:

- Find What—Enter the circuit name you want to find.

- Match Whole Word Only—If checked, CTC selects circuits only if the entire word matches the name 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 6   Click **Find Next**.

Step 7   Repeat Steps 5 and 6 until you are finished, then click **Cancel**.

6.7 Editing SNCP Circuits

Use the Edit Circuits window to change SNCP selectors and switch protection paths. In this window, you can:

- View the SNCP 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 SNCP circuits to better see circuit flow between nodes

Procedure: Edit an SNCP Circuit

Purpose	Use this procedure to edit SNCP circuits.
Prerequisite Procedures	"Creating VC High-Order Path Circuits" section on page 6-3 or "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12
Onsite/Remote	Onsite or remote

Step 1   Log into the source or drop node of the SNCP circuit.

Step 2   Click the **Circuits** tab.

Step 3   Click the circuit you want to edit, then click **Edit**.

Step 4   In the Edit Circuit window, click the **SNCP Selectors** tab.

Step 5   Edit the SNCP selectors.

- Revert 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—(VC4 circuits only) Sets the SNCP signal failure BER threshold.

- SD Ber Level—(VC4 circuits only) Sets the SNCP signal degrade BER threshold.

- PDI-P—(VC4 circuits only) When checked, traffic switches if a VC4 payload defect indication is received.

- 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.

  - 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 verify that the selector switches as you expect.

6.8 Creating a Path Trace

Use a J1 path trace to monitor interruptions or changes to circuit traffic. The J1 path trace for each drop port transmits a repeated, fixed-length string. If the string received at a circuit drop port along the circuit does not match the string the port expects to receive, an alarm is raised. To set up path trace on the ports, you must repeat the following procedure for each port. Table 6-3 shows the ONS 15454 SDH cards that support path trace. Cards not listed in the table do not support the J1 byte.

Table 6-3   ONS 15454 SDH Cards Supporting J1 Path Trace

J1 Function	Card
Transmit and Receive	E3
	DS3I
	G1000-4
Receive Only	OC3 IR 4/STM1 SH 1310
	OC48 IR/STM16 SH AS 1310
	OC48 LR/STM16 LH AS 1550
	OC192 LR/STM64 LH 1550

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

> **Note** There are two types of J1 bytes, high-order (HO-J1) and low-order (LO-J1). The electrical cards support LO-J1 (VC3). The optical cards support HO-J1 (VC4) and cannot monitor the LO-J1 byte.

> **Note** Path trace is available for VC3 and VC4 circuits. In ONS 15454 SDH Software R3.4 and earlier, you can set the VC3 J1 transmit string on E3 and DS3I cards, but VC3 is not monitored by STM-N cards.

Procedure: Create a J1 Path Trace

Purpose	Use this procedure to create a path trace on a circuit source and destination port. This procedure assumes you are setting up a path trace on a bidirectional circuit, and you will set transmit strings at the circuit source and destination.
Tools/Equipment	ONS 15454 SDH cards capable of path trace. See Table 6-3 on page 6-21.
Prerequisite Procedures	"Creating VC High-Order Path Circuits" section on page 6-3 or "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12
Onsite/Remote	Onsite or remote

Step 1   Log into a node on the network where you will create the path trace.

Step 2   From node view, click the **Circuits** tab.

Step 3   For the circuit you want to monitor, verify that the source and destination ports are on a card that can transmit and receive the path trace string (E3, DS3I, or G1000-4). See Table 6-3 for a complete list of cards.

If neither port is on a transmit/receive card, you will not be able to complete this procedure. If one port is on a transmit/receive card and the other is on a receive-only card, you can set up the transmit string at the transmit/receive port and the receive string at the receive-only port, but you will not be able to transmit in both directions.

Step 4   Click the circuit you want to trace, then click **Edit**.

Step 5   In the Edit Circuit window, check the **Show Detailed Map** box at the bottom of the window. A detailed map of the source and destination ports is displayed.

Step 6   Provision the circuit source transmit string:

    a.   On the detailed circuit map, right-click the circuit source port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu (Figure 6-7).

Figure 6-7   Selecting the detailed circuit map

From network, node or card view
choose Circuits, Edit, Show Detailed Map
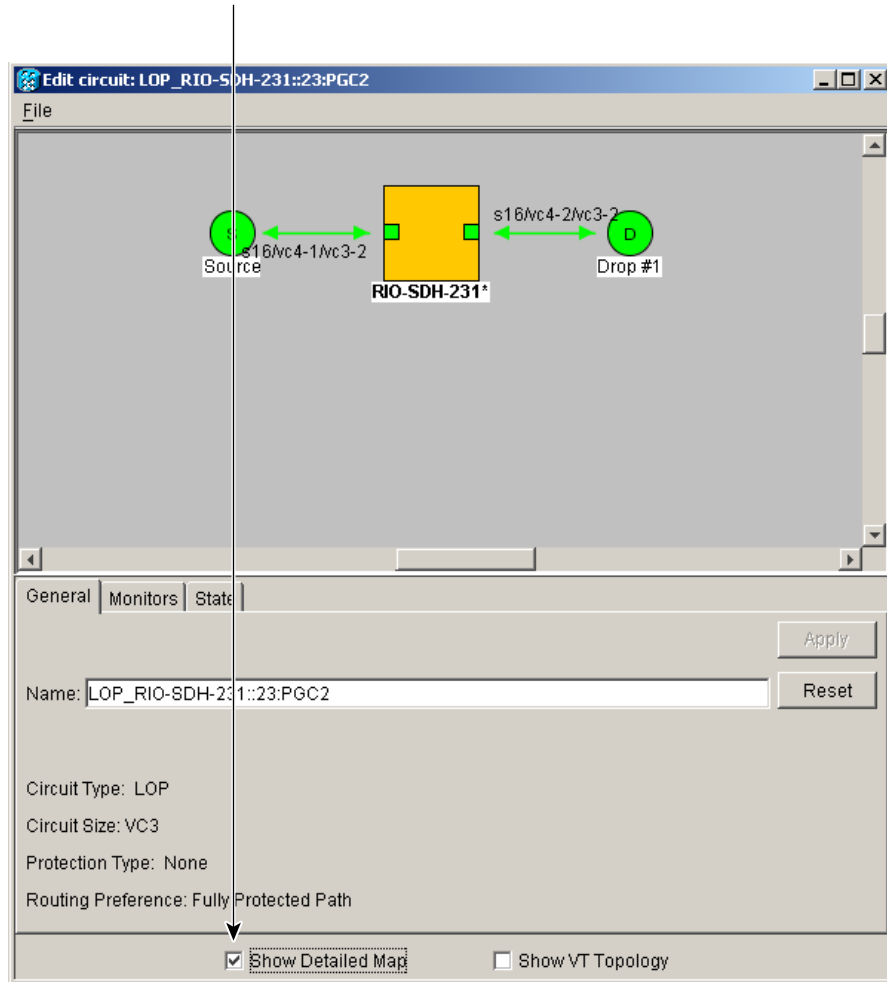
b. Choose the format of the transmit string by clicking either the **16 byte** or the **64 byte** selection button.

c. In the New Transmit String field, enter the circuit source transmit string. Enter a string that makes the source port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

d. Click **Apply**, then click **Close**.

Step 7 Provision the circuit destination transmit string.

a. In the Edit Circuit window, right-click the circuit destination port and choose **Edit Path Trace** from the shortcut menu.

b. In the New Transmit String field, enter the string that you want the circuit destination to transmit. Enter a string that makes the destination port easy to identify, such as the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits a string of null characters.

c. Click **Apply**.

Step 8   Provision the circuit destination expected string.

    a.   In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu.

       – Auto—The first string received from the source port is the baseline. An alarm is raised when a string that differs from the baseline is received. Continue with Substep b.

       – Manual—The string entered in Current Expected String is the baseline. An alarm is raised when a string that differs from the Current Expected String is received. Enter the string that the circuit destination should receive from the circuit source in the New Expected String field.

    b.   Click the **Disable AIS on TIM-P** check box if you want to suppress the alarm indication signal when the Path Trace Identifier Mismatch Path (TIM-P) alarm is displayed. Refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* for descriptions of alarms and conditions.

    c.   Click **Apply**, then click **Close**.

Step 9   Provision the circuit source expected string.

    a.   In the Edit Circuit window, right-click the circuit source port and choose **Edit Path Trace** from the shortcut menu.

    b.   In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu.

       – Auto—Uses the first string received from the port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received. Continue with Substep c.

       – 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. Enter the string that the circuit source should receive from the circuit destination in the New Expected String field.

    c.   Click the **Disable AIS on TIM-P** check box if you want to suppress the alarm indication signal when the TIM-P alarm is displayed. Refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* for descriptions of alarms and conditions.

    d.   Click **Apply**, then click **Close**.

Step 10   After you set up the path trace, the received string is displayed in the Received box on the path trace setup window. The following options are available:

- 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).

⚠️ **Caution**   Clicking Default will generate alarms if the port on the other end is provisioned with a different string.

The Expect and Receive strings are updated every few seconds only if Path Trace Mode is set to Auto or Manual.

When you display the detailed circuit window, path trace is indicated by an M (manual path trace) or an A (automatic path trace) at the circuit source and destination ports.

Procedure: Monitor a Path Trace on STM-N Ports

Purpose	Use this task to monitor a path trace on STM-N ports within the circuit path.
Tools/Equipment	ONS 15454 SDH cards capable of receiving path trace must be installed at the STM-N circuit ports. See Table 6-3 on page 6-21.
Prerequisite Procedures	"Create a J1 Path Trace" section on page 6-22
Onsite/Remote	Onsite or remote

Step 1   Start CTC on a node in the network where path trace was provisioned on the circuit source and destination ports.

Step 2   Click **Circuits**.

Step 3   Choose the VC4 circuit that has path trace provisioned on the source and destination ports, then click **Edit**.

Step 4   In the Edit Circuit window, click the **Show Detailed Map** box at the bottom of the window. A detailed circuit graphic showing source and destination ports is displayed.

Step 5   On the detailed circuit map, right-click the circuit STM-N port (the square on the left or right of the source node icon) and choose **Edit Path Trace** from the shortcut menu.

> **Note**   The STM-N port must be on a receive-only card listed in Table 6-3 on page 6-21. If not, the Edit Path Trace menu item will not display.

Step 6   In the Circuit Path Trace window, enable the path trace expected string by choosing **Auto** or **Manual** from the Path Trace Mode drop-down menu:

- Auto—Uses the first string received from the port at the other end as the baseline string. An alarm is raised when a string that differs from the baseline is received. For STM-N ports, Auto is recommended, since Manual mode requires you to trace the circuit on the Edit Circuit window to determine whether the port is the source or destination path.

- 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 7   If you set Path Trace Mode to Manual, enter the string that the STM-N port should receive in the New Expected String field. To do this, trace the circuit path on the detailed circuit window to determine whether the port is in the circuit source or destination path, then set the New Expected String to the string transmitted by the circuit source or destination. If you set Path Trace Mode to Auto, ignore the New Expected String field.

Step 8   The **Disable AIS on TIM-P** check box cannot be selected.

> **Note**   SDH Software R3.4 and earlier does not support changes to the **Disable AIS on TIM-P** field. The STM-N path trace monitoring does not generate AIS on TIM-P.

Step 9   Click **Apply**, then click **Close**.

6.9 Creating Half Circuits

The following procedures describe how to create STM-N circuits from a drop to an STM-N card on the same node in an MS-SPRing or 1+1 topology, and how to create an STM-N circuit from a drop to an STM-N card on the same node in an SNCP.

Procedure: Create a Half Circuit using an STM-N Card as a Destination in an MS-SPRing or 1+1 Topology

Purpose	Use this procedure to create a high-order path circuit from a drop to an E1 or STM-N card on the same node in an MS-SPRing or 1+1 topology.
Tools/Equipment	—
Prerequisite Procedures	—

Step 1 From node view, go to the View menu and select **Go to Network View**.

Step 2 Click the **Circuits** tab, then click **Create**.

Step 3 In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.

  Note If you will ever create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

- Type—Select **VC_HO_Path_Circuit (HOP)**. The circuit type determines the circuit-provisioning options that are displayed. The E3 and DS3I cards must use VC low-order path tunnels. See the "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12 for more information.

- Size—Select the circuit size (VC_HO_Path_Circuits only). VC high-order path circuits can be VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c for optical cards and some Ethernet cards depending on the card type. Of the Ethernet cards, only the G-1000 can use VC4-3c and VC4-8c. The "c" indicates concatenated VC4s.

- Bidirectional—Leave this box checked (default).

- Number of circuits—Type the number of circuits you want to create. The default is 1.

- Auto-ranged—Deselect this box. This check box is automatically selected when you enter more than 1 in the Number of circuits field.

- State—Choose one of the following service states to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.
  - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

> – OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If not checked, CTC will not change the state of the source and destination ports.

✎
Note   LOS alarms display if in service (IS) ports are not receiving signals.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- *Protected Drops*—Uncheck this box.

Step 4   Click **Next**.

Step 5   Provision the circuit source.

    a. From the Node pull-down menu, choose the node that will contain the circuit.

    b. From the Slot pull-down menu, choose the slot containing the card where the circuit will originate.

    c. From the Port pull-down menu, choose the port where the circuit will originate.

Step 6   Click **Next**.

Step 7   Provision the circuit destination.

    a. From the Node pull-down menu, select the node chosen in Step 5a.

    b. From the Slot pull-down menu, choose the STM-N or E1 card to map the high-order path circuit to a VC-4.

    c. Choose the destination VC-4 from the submenus that display.

Step 8   Click **Finish.** If you entered more than 1 in the Number of circuits field and did not select Auto-ranged, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.

After completing the circuit(s), CTC displays the Circuits window.

Step 9   In the Circuits window, verify that the newly created circuit(s) appear in the circuits list.

Procedure: Create a Half Circuit using an STM-N as a Destination in an SNCP

Purpose	Use this procedure to create a high-order path circuit from a drop to an E1 or STM-N card on the same node in an SNCP.
Tools/Equipment	—
Prerequisite Procedures	—

Step 1   From node view, go to the View menu and select **Go to Network View**.

Step 2   Click the **Circuits** tab, then click **Create**.

Step 3   In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.

  Note If you will ever create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

- Type—Select **VC_HO_Path_Circuit (HOP)**. The circuit type determines the circuit-provisioning options that are displayed. The E3 and DS3I cards must use VC low-order path tunnels. See the "Creating VC Low-Order Path Tunnels for Port Grouping" section on page 6-12 for more information.

- Size—Select the circuit size (VC_HO_Path_Circuits only). VC high-order path circuits can be VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c for optical cards and some Ethernet cards depending on the card type. Of the Ethernet cards, only the G-1000 can use VC4-3c and VC4-8c. The "c" indicates concatenated VC4s.

- Bidirectional—Leave checked for this circuit (default).

- Number of circuits—Type the number of circuits you want to create. The default is 1.

- Auto-ranged—Deselect this check box. This check box is automatically selected when you enter more than 1 in the Number of circuits field.

- State—Choose one of the following service states to apply to the circuit:
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.
  - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Check this box if you want to apply the state chosen in the State field to the circuit source and destination ports. CTC will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If not checked, CTC will not change the state of the source and destination ports.

  Note LOS alarms display if in service (IS) ports are not receiving signals.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave this box unchecked.

Step 4 If the circuit will be routed on an SNCP, set the SNCP path selector defaults as follows:

- Revertive—Check this box if you want traffic to revert to the working path when the conditions that diverted traffic 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—Choose from one E-3, one E-4, or one E-5.

- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.

- Switch on PDI-P—(VC4 circuits only) Check this box if you want traffic to switch when a VC4 payload defect indicator is received.

Step 5   Click **Next**.

Step 6   Provision the circuit source.

    a. From the Node pull-down menu, choose the node that will contain the circuit.

    b. From the Slot pull-down menu, choose the slot containing the card where the circuit will terminate.

    c. From the Port pull-down menu, choose the port where the circuit will terminate.

Step 7   Click **Next**.

Step 8   Provision the circuit destination.

    a. From the Node pull-down menu, select the node that will contain the circuit. This will be the same as the node chosen in Step 6a.

    b. Choose the choose the STM-N or E1 card to map the high-order path circuit to a VC-4.

    c. Choose the destination VC-4 from the submenus that display.

Step 9   Click **Use Secondary Destination** and repeat Steps 6 to 9 to define the secondary destination.

Step 10   Click **Finish.** If you entered more than 1 in the Number of circuits field and did not check the Auto-ranged check box, the Circuit Creation dialog box is displayed so you can create the remaining circuits. Repeat this procedure for each additional circuit.

    After completing the circuit(s), CTC displays the Circuits window.

Step 11   In the Circuits window, verify that the newly created circuit(s) appear in the circuits list.

6.10 Filtering, Viewing, and Changing Circuit Options

Use the following procedures to set up circuit filters, view circuits on an ONS 15454 SDH span, change the state of a circuit, edit a circuit name, or change the color of active (working) and standby (protect) circuit spans.

Procedure: Filter the Display of Circuits

Purpose	This procedure filters the display of circuits in the ONS 15454 SDH network, node, or card view.
Tools/Equipment	—
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Switch to the appropriate CTC view, as follows:

- To filter network circuits, from the View menu, choose **Go to Network View**.

- To filter circuits that originate, terminate, or pass through a specific node, from the View menu, choose **Go to Other Node**; then, choose the node you want to search and click **OK**.

- To filter circuits that originate, terminate, or pass through a specific card, switch to node view, then double-click the card on the shelf graphic to display the card in card view.

Step 2   Click the **Circuits** tab.

Step 3   Set the attributes for filtering the circuit display.

   a.   Click the **Filter** button.

   b.   In the Filter Dialog, set the filter attributes:

- Name—Enter a complete or partial circuit name to filter circuits based on circuit name; otherwise leave the field blank.

- Direction—Choose one of the following options: **Any** (direction not used to filter circuits), **1-way** (display only one-way circuits), or **2-way** (display only two-way circuits).

- Status—Choose one of the following options: **Any** (status not used to filter circuits), **Active** (display only active circuits), **Incomplete** (display only incomplete circuits, that is, circuits missing a connection or span to form a complete path), or **Upgradable** (display only upgradable circuits).

- Slot—Enter a slot number to filter circuits based on source or destination slot; otherwise leave the field blank.

- Port—Enter a port number to filter circuits based on source or destination port; otherwise leave the field blank.

- Type—Choose one of the following options: **Any** (type not used to filter circuits), **VC_HO_PATH_CIRCUIT** (displays only high-order path circuits), **VC_LO_PATH_CIRCUIT** (displays only low-order path circuits), or **VC_LO_PATH_TUNNEL** (displays only low-order path tunnels).

- Size—Click the appropriate check boxes to filter circuits based on size: **VC3**, **VC4**, **VC4-2c**, **VC4-3c**, **VC4-4c**, **VC4-8c**, **VC4-16c**, or **VC4-64c**. The check boxes displayed depend on the entry selected in the Type field.

Step 4   Click **OK**. Circuits matching the attributes in the Filter Circuits dialog box are displayed in the Circuits window.

Step 5   To turn filtering off, click the **Filter** icon in the lower right corner of the Circuits window. Click the icon again to turn filtering on, and click the **Filter** button to change the filter attributes.

Procedure: View Circuits on a Span

Purpose	View circuits on an ONS 15454 SDH span.
Tools/Equipment	—
Prerequisite Procedures	"Creating MS-SPRings" section on page 5-14
	Circuits must be created on the MS-SPRing using PCA. See "Creating VC High-Order Path Circuits" section on page 6-3
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

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

Step 2   Place your mouse cursor directly over the span (green line) containing the circuits you want to view, press the right mouse button, and choose one of the following:

- **Circuits**—To view MS-SPRing, SNCP, 1+1, or unprotected circuits on the span.
- **PCA Circuits**—To view circuits routed on a MS-SPRing protected channel. (This option does not display if the span you right-clicked is not a MS-SPRing span.)

Step 3   In the Circuits on Span dialog box, view the following information for circuits provisioned on the span:

- VC4—The number of VC4s used by the circuits
- VC3—The number of VC3s used by the circuits
- TUG2—The number of TUG2s used by the circuits
- VC12—The number of VC12s used by the circuits
- SNCP—(SNCP span only) Checked for SNCP circuits
- Circuit—Displays the circuit name
- Switch State—(SNCP span only) Displays the switch state of the circuit, that is, whether any span switches are active. For SNCP spans, switch types include: CLEAR (no spans are switched), MANUAL SWITCH AWAY (a manual switch is active), FORCE SWITCH AWAY (a force switch is active), and LOCKOUT OF PROTECTION (a span lockout is active).

> **Note**   You can perform other procedures from the Circuits on Span dialog box. If the span is in a SNCP, you can switch the span traffic. If you want to edit a circuit on the span, double-click the circuit. See the "Edit a Circuit Name" procedure on page 6-32 for instructions.

Procedure: Change a Circuit State

Purpose	Use this procedure to change the state of a circuit.
Tools/Equipment	—
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Click the **Circuits** tab.

Step 2   Click the circuit with the state you want to change.

Step 3   From the Tools menu, choose **Circuits > Set Circuit State**.

> **Note**   Alternatively, you can click the **Edit** button, then click the **State** tab on the Edit Circuits window.

Step 4   In the Set Circuit State dialog box change the circuit state by choosing one of the following from the Target Circuit State drop-down menu:

- IS—Places the circuit in service.

  - OOS—Places the circuit out of service.

  - OOS-AINS—Places the circuit in an out of service, auto in service state.

  - OOS-MT—Places the circuit in an out of service, maintenance state.

Step 5 If you want to apply the state to the circuit source and destination ports, check the **Apply to Drop Ports** check box.

Step 6 Click **OK**.

> **Note** CTC will not change the state of the circuit source and destination port in certain circumstances, for example, if the circuit size is smaller than the port and you change the state from IS to OOS. If this occurs, a message is displayed and you will need to change the port state manually.

Procedure: Edit a Circuit Name

Purpose	Use this procedure to edit a circuit name.
Tools/Equipment	—
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1 Click the **Circuits** tab.

Step 2 Click the circuit you want to rename, then click **Edit** (or you can double-click the circuit).

Step 3 In the General tab, click the Name field and edit or rename the circuit. Names can be up to 48 alphanumeric and/or special characters.

> **Note** If you will ever create a monitor circuit on this circuit, do not make the name longer than 44 characters because monitor circuits will add "_MON" (four characters) to the circuit name.

Step 4 Click the **Apply** button.

Step 5 From File menu, select **Close**.

Step 6 In the Circuits window, verify that the circuit was correctly renamed.

Procedure: Change Active and Standby Span Color

Purpose	Use this procedure to change the color of active (working) and standby (protect) circuit spans displayed on the detailed circuit map of the Edit Circuits window. By default, working spans are green and protect spans are purple.
Tools/Equipment	—

| **Prerequisite Procedures** | "Log Into CTC" procedure on page 2-24 |
| **Onsite/Remote** | Onsite or remote |

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

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

Step 3   Complete one or more of the following steps, as required:

- To change the color of the active (working) span, go to Step 4.
- To change the color of the standby (protect) span, go to Step 5.
- To return active and standby spans to the default colors, go to Step 6.

Step 4   To change the color of the active span:

a.   Next to Active Span Color, click the **Color** button.

b.   In the Pick a Color dialog box, click the color for the active span, or click the **Reset** button if you want the active span to display the last applied (saved) color.

c.   Click **OK** to close the Pick a Color dialog box. If you want to change the standby span color, go to Step 5. If not, click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box displayed.

Step 5   To change the color of the standby span:

a.   Next to Standby Span Color, click the **Color** button.

b.   In the Pick a Color dialog box, click the color for the standby span, or click the **Reset** button if you want the standby span to display the last applied (saved) color.

c.   Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box displayed.

Step 6   If you want to return the active and standby spans to their default colors:

a.   From the Edit menu, choose **Preferences**.

b.   In the Preferences dialog box, click the **Circuits** tab.

c.   Click the **Reset to Defaults** button.

d.   Click **OK** to save the change and close the Preferences dialog box, or click **Apply** to save the change and keep the Preferences dialog box displayed.

6.11 Cross-Connect Card Capacities

The XC10G is required to operate the ONS 15454 SDH. XC10Gs support high-order cross-connections (VC4 and above). The XC10G does not support any low-order circuits such as VC-11, VC-12, and VC3. The XC10G card works with the TCC-I card to maintain connections and set up cross-connects within the node. You can create circuits using Cisco Transport Controller (CTC). The XC10G card cross connects standard VC4, VC4-4c, VC4-16c, and VC4-64c signal rates and non-standard VC4-2c, VC4-3c, and VC4-8c signal rates, providing a maximum of 384 x 384 VC4 cross-connections. Any VC4 on any port can be connected to any other port, meaning that the VC cross-connection capacity is non-blocking. The XC10G card manages up to 192 bidirectional VC4 cross-connects.

VC4 tunnels must be used with the E3 and DS3I cards to transport VC3 signal rates. Three ports form a port group. For example, in one E3 or one DS3I card, there are four port groups: Ports 1 to 3 = PG1, Ports 4 to 6 = PG2, Ports 7 to 9 = PG3, and Ports 10 to 12 = PG4.

Note In SDH Software R3.4 and earlier, the XC10G does not support VC3 circuits for the E3 and DS3I cards. You must create a VC tunnel. See the "Create a Low-Order Path Tunnel for Port Grouping" procedure on page 6-13 for more information.

Note The *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* contains detailed specifications of the XC10G card.

6.12 Creating DCC Tunnels

SDH provides four data communications channels (DCCs) for network element operations, administration, maintenance, and provisioning: one on the SDH regenerator section layer and three on the SDH multiplex section layer. The ONS 15454 SDH uses regenerator section DCC for inter-15454 data communications. It does not use the multiplex section DCCs; therefore, the multiplex section DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 SDH networks. If D4 through D12 are used as data DCCs, they cannot be used for DCC tunneling.

A DCC tunnel end-point is defined by slot, port, and DCC, where DCC can be either the regenerator section DCC, Tunnel 1, Tunnel 2, or Tunnel 3. You can link a regenerator section DCC to a multiplex section DCC (Tunnel 1, Tunnel 2, or Tunnel 3) and a multiplex section DCC to a regenerator section DCC. You can also link multiplex section DCCs to multiplex section DCCs and link regenerator section DCCs to regenerator section DCCs. To create a DCC tunnel, you connect the tunnel end points from one ONS 15454 SDH optical port to another.

Each ONS 15454 SDH can support up to 32 DCC tunnel connections. Table 6-4 shows the DCC tunnels that you can create.

Table 6-4   DCC Tunnels

DCC	SDH Layer	SDH Bytes	STM-1 (All Ports)	STM-4, STM-16, STM-64
SDCC	Regenerator Section	D1 - D3	Yes	Yes
Tunnel 1	Multiplex Section	D4 - D6	No	Yes
Tunnel 2	Multiplex Section	D7 - D9	No	Yes
Tunnel 3	Multiplex Section	D10 - D12	No	Yes

Figure 6-8 shows a DCC tunnel example. Third-party equipment is connected to STM-1 cards at Node 1/Slot 3/Port 1 and Node 3/Slot 3/Port 1. Each ONS 15454 SDH node is connected by STM-16 trunk cards. In the example, three tunnel connections are created, one at Node 1 (STM-1 to STM-16), one at Node 2 (STM-16 to STM-16), and one at Node 3 (STM-16 to STM-1).

✎
Note   A DCC will not function on a mixed network of ONS 15454 SDH nodes and ONS 15454 SONET nodes. DCC tunneling is required for ONS 15454 SDH nodes transporting data through ONS 15454 SONET nodes.

Figure 6-8   DCC tunnel
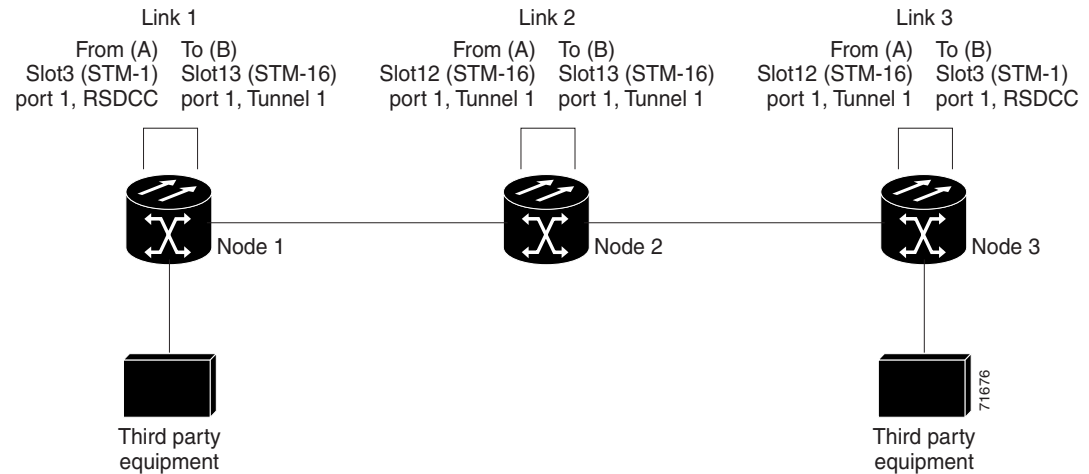
When you create DCC tunnels, keep the following guidelines in mind:

• Each ONS 15454 SDH can have a maximum of 32 DCC tunnel connections.

• Each ONS 15454 SDH can have a maximum of 10 regenerator section DCC terminations.

• A regenerator section DCC that is terminated cannot be used as a DCC tunnel end-point.

• A regenerator section DCC that is used as a DCC tunnel end-point cannot be terminated.

• All DCC tunnel connections are bidirectional.

✎
Note   A multiplex section DCC cannot be used for tunneling if a data DCC is assigned.

Procedure: Provision a DCC Tunnel

Purpose	Use this procedure to create a DCC tunnel to transport traffic from ONS 15454 SONET platforms or from third-party SDH equipment across ONS 15454 SDH networks.
Onsite/Remote	Onsite or remote
Tools/Equipment	—
Prerequisite Procedures	"Log Into CTC" procedure on page 2-24

✎
Note   Each ONS 15454 SDH can have up to 32 DCC tunnel connections. Terminated regenerator section DCCs used by the ONS 15454 SDH cannot be used as a DCC tunnel end-point, and a regenerator section DCC that is used as a DCC tunnel end-point cannot be terminated. All DCC tunnel connections are bidirectional.

Step 1   Log into an ONS 15454 SDH that is connected to the non-ONS 15454 SDH network.

Step 2   From the node view, choose **Go to Network View**.

Step 3   Click the **Provisioning > Overhead Circuits** tabs.

Step 4   Click **Create** (Figure 6-9).

Figure 6-9   Creating a DCC tunnel
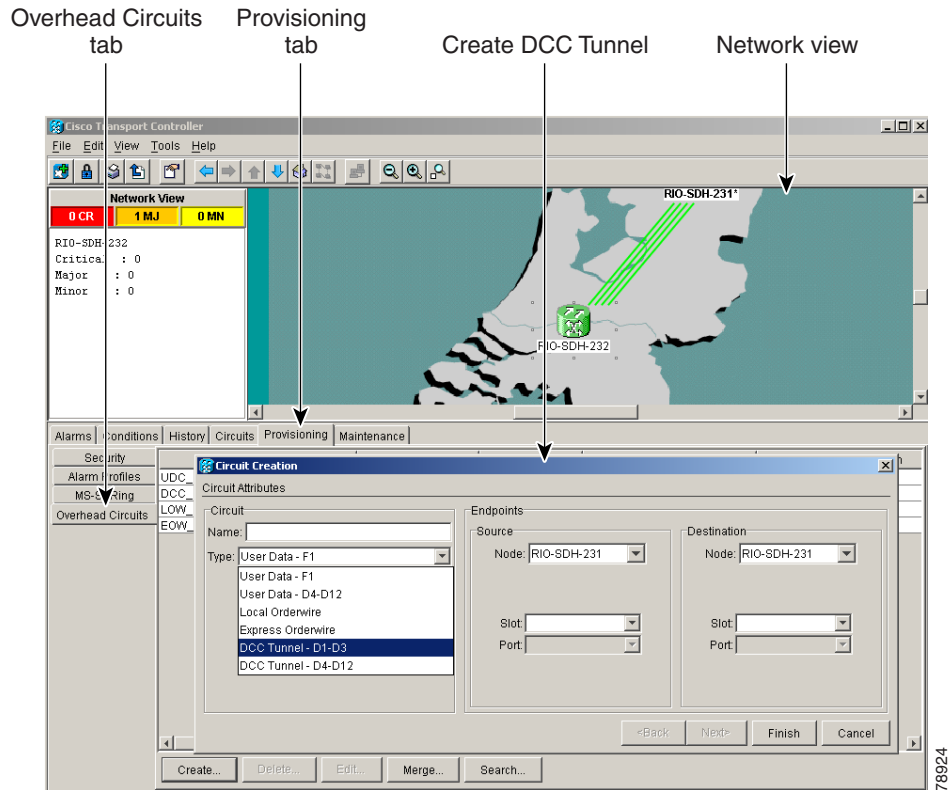
Step 5   In the Circuit Creation dialog box, provision the DCC tunnel as follows:

- Name—Type the tunnel name.

- Type—Choose one of the following options:

  - **DCC Tunnel-D1-D3**—Allows you to choose either the regenerator section DCC (D1-D3) or a multiplex section DCC (D4-D6, D7-D9, or D10-D12) as the source or destination endpoints.

  - **DCC Tunnel-D4-D12**—Provisions the full multiplex section DCC as a tunnel.

- Source Node—Choose the source node.

- Slot—Choose the source slot.

- Port—If displayed, select the source port.

- Channel—Displayed if you chose DCC Tunnel-D1-D3 as the tunnel type. Choose one of the following:

  - **DCC1 (D1-D3)**—The regenerator section DCC

  - **DCC2 (D4-D6)**—Multiplex section DCC 1

     – **DCC3 (D7-D9)**—Multiplex section DCC 2

     – **DCC4 (D10-D12)**—Multiplex section DCC 3

> **Note**   DCC options are not displayed if they are used by the ONS 15454 SDH (regenerator section DCC) or other tunnels.

Step 6   Click **OK**.

Step 7   Put the ports hosting the DCC tunnel in service. See the "Put Ports In or Out of Service" procedure on page 5-56 for instructions.

       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.

CHAPTER **7**

Card Provisioning

This chapter provides procedures for changing the default transmission parameters and performance monitoring (PM) thresholds for Cisco ONS 15454 SDH electrical and optical cards. The chapter also provides procedures for converting the E1-N-14 and DS3i-N-12 cards from 1:1 to 1:N protection. (E3-12 cards only support 1:1 protection.)

Setting up CTC for performing pointer justification count monitoring is described in Chapter 8, "SDH Performance Monitoring."

Setting up CTC for intermediate-path performance monitoring is described in Chapter 8, "SDH Performance Monitoring."

Ethernet card provisioning is described in Chapter 9, "Ethernet Operation."

Table 7-1   Card Provisioning Topics

Card Provisioning Topics
7.1 Front Mount Electrical Connection (FMEC) Cards, page 7-4
7.2 Provisioning Electrical Cards, page 7-4
7.3 Converting E1 and DS3i Cards From 1:1 to 1:N Protection, page 7-18
7.4 Provisioning Intermediate-Path Performance Monitoring, page 7-21
7.5 Provisioning Optical Cards, page 7-22
7.7 Optical Card Protection, page 7-33
7.8 Provisioning Ethernet Cards, page 7-33
7.9 Provisioning the Alarm Interface, page 7-33

Table 7-2   Card Provisioning Tasks

Card Provisioning Tasks
Procedure: Modify Line and Threshold Settings for the E-1 Card, page 7-7
Procedure: Modify Line and Threshold Settings for the E3-12 Card, page 7-10
Procedure: Convert E1-N-14 Cards From 1:1 to 1:N Protection, page 7-18
Procedure: Convert DS3i-N-12 Cards From 1:1 to 1:N Protection, page 7-20
Procedure: Provision Line Transmission Settings for OC-N/STM-N Cards, page 7-23
Procedure: Provision Threshold Settings for STM-N Cards, page 7-25

Table 7-2   Card Provisioning Tasks (continued)

Card Provisioning Tasks
Procedure: Provision the AIC-I Card, page 7-34
Procedure: Provision External Alarms and Controls on the AIC-I Card, page 7-34
Procedure: Create a User Data Channel Circuit on the AIC-I, page 7-38
Procedure: Provision the AIC-I Orderwire, page 7-38

Because much of the electrical and optical card provisioning involves PM thresholds, refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* for definitions and general information about ONS 15454 SDH performance monitoring parameters. In addition, refer to the ITU-T G.707, G.783, and G.841 documents. The default thresholds delivered with ONS 15454 SDH cards are based on specifications contained in those documents.

Note   For information about creating protection groups, see the 3.6 Creating Card Protection Groups, page 3-26 in Chapter 3, "Node Setup." For circuit creation procedures, see Chapter 6, "Circuits and Tunnels."

Note   You start Cisco Transport Controller (CTC) by using your web browser and typing the IP address of the ONS15454 SDH shelf to be controlled into the address bar. You have to use a login with Provisioning or Superuser authority. Starting the CTC can take a few minutes depending on the speed of your IP connection to the ONS15454 SDH shelf. After having typed the IP address into the address bar, CTC will start with windows like the ones as shown in Figure 7-1, Figure 7-2, and Figure 7-3.

Figure 7-1   CTC login prompt
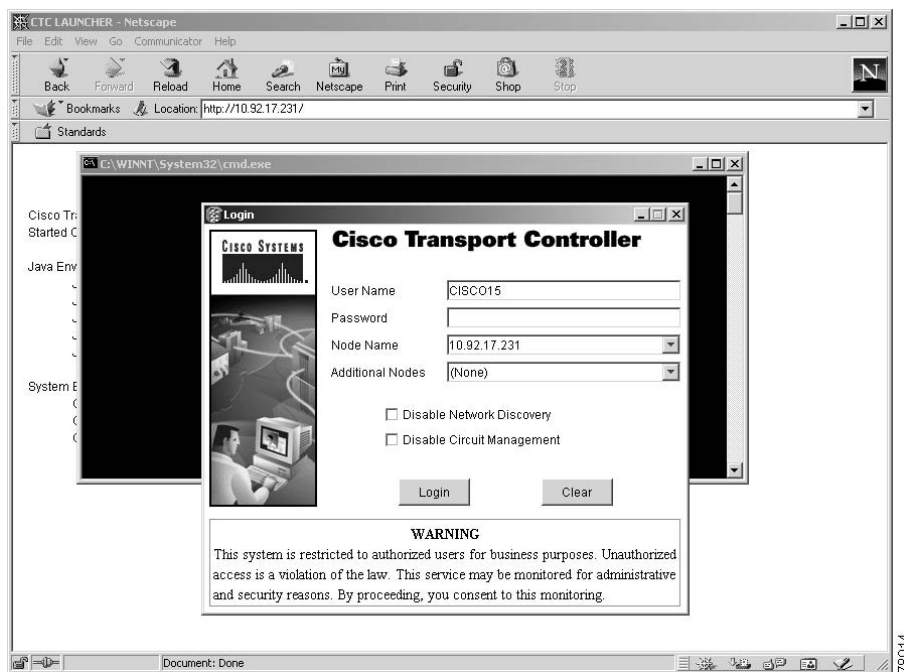
Figure 7-2   Reaction of the web browser after login

Downloading CTC from the ONS 15454 SDH node can take up to a few minutes, depending on the speed of the web connection to the node to be controlled.

Figure 7-3   Node view of the ONS 15454 SDH node
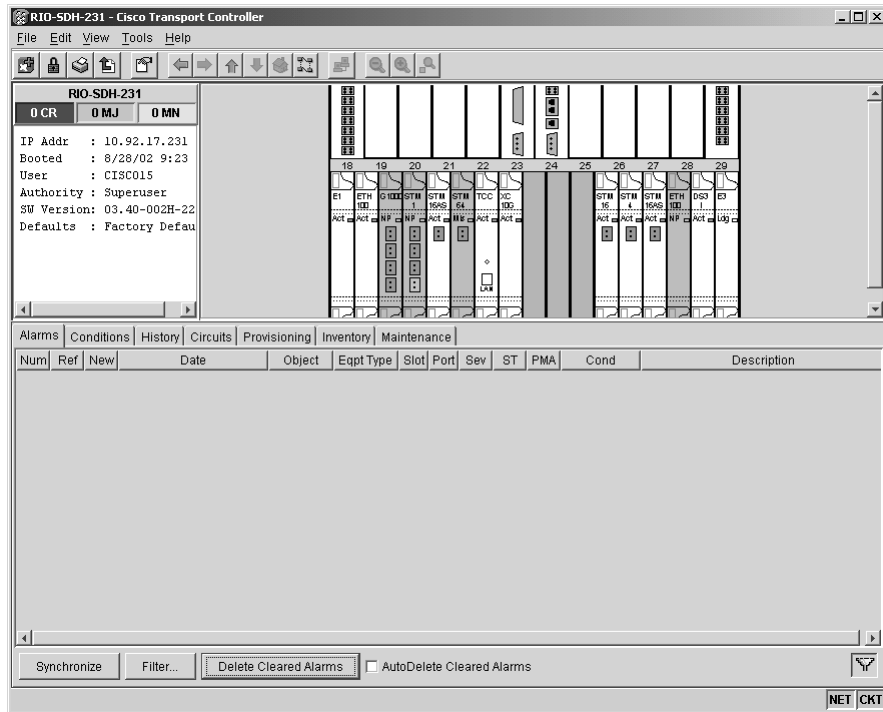
7.1 Front Mount Electrical Connection (FMEC) Cards

The ONS 15454 SDH Front Mount Electrical Connection (FMEC) cards are feedthrough cards that enable front access for the interfaces. They do not require any parameters to be set during provisioning. The only internal data that these cards have is inventory data.

The FMEC cards are:

• FMEC-E1

• FMEC-E3/DS3

• FMEC-DS1/E1

• MIC-A/P

• MIC-C/T/P

7.2 Provisioning Electrical Cards

The ONS 15454 SDH electrical cards are preprovisioned with settings that you can modify to manage transmission quality.

The electrical cards are:

• E1-N-14

• E3-12

• DS3i-N-12

When you open a card in CTC node view (which means double-click on this card) and choose the Provisioning tab, the following subtabs are commonly displayed:

• Line—Sets line setup parameters, such as line type, line coding, and line length. This is also where you put ports in and out of service.

• Line Thresholds—Sets the line-level PM thresholds.

• Elect Path Thresholds—Sets the path-level PM thresholds for electrical (E1, E3, DS3) traffic.

• SDH Thresholds—Sets the path-level PM thresholds for SDH traffic.

• Alarm Behavior—Sets alarm profiles for individual ports. See Chapter 10, "Alarm Monitoring and Management." for information about creating alarm profiles.

As an example, Figure 7-4 shows the window with the choices for an E1-N-14 card.

Figure 7-4   Provisioning line parameters on the E1-N-14 card
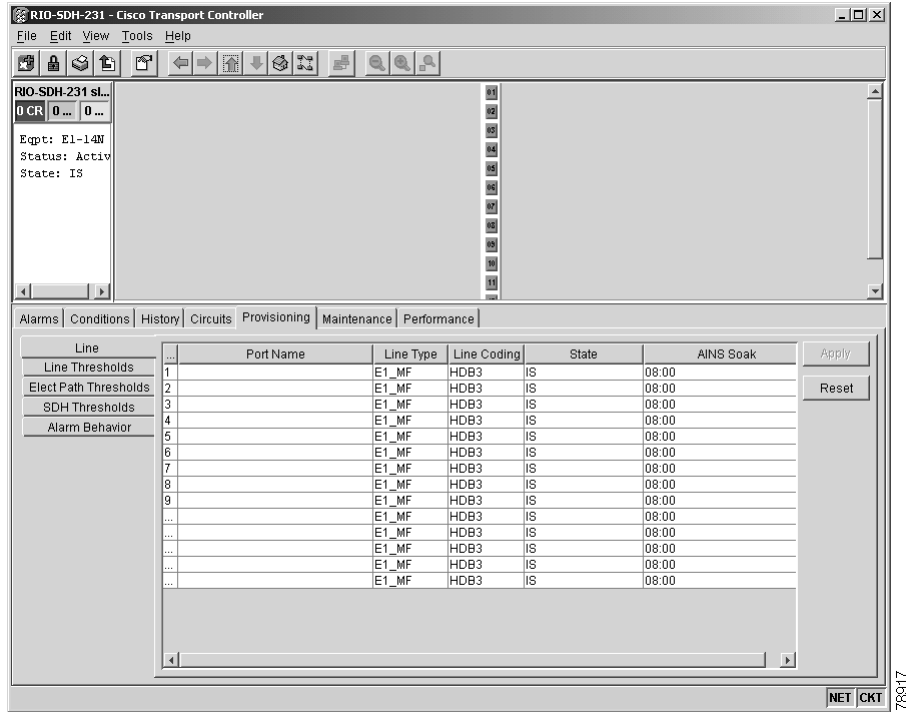
Table 7-3 provides an overview of E1-N-14, E3-12, and DS3i-N-12 parameters. An X means the item is available for the card. A dash means the item is not available for the card.

Table 7-3   E1, E3, and DS-3 Card Provisioning Overview

Provisioning Item	E1-N-14	E3-12	DS3i-N-12
Line Subtab			
Port #	X	X	X
Port Name	X	X	X
Line Type	X	—	X
Detected Line Type	—	—	X
Line Coding	X	—	X
Line Length	—	—	X
State	X	X	X
AINS Soak	X	X	X
Line Thresholds Subtab			
Port	X	X	X
CV	X	X	X
ES	X	X	X
SES	X	X	X
LOSS	—	X	X

Table 7-3   E1, E3, and DS-3 Card Provisioning Overview (continued)

Provisioning Item	E1-N-14	E3-12	DS3i-N-12
Elect Path Thresholds Subtab			
Port	X	X	X
CVP (or CVCP)	—	—	X
EB	X	—	—
BBE	X	—	—
ES	X	X	—
ESP (or ESCP)	—	—	X
SES	X	X	—
SESP (or SESCP)	—	—	X
SAS	X	—	—
SASP (or SASCP)	—	—	X
UAS	X	X	—
UASP (or UASCP)	—	—	X
AISSP	—	—	X
SDH Thresholds Subtab			
Port	X	X	X
ES	X	X	X
SES	X	X	X
EB	X	X	X
UAS	X	X	X
BBE	X	X	X
Alarm Behavior Subtab			
Port	X	X	X
Profile	X	X	X
Suppress Alarms	X	X	X

7.2.1 E1-N-14 Card Parameters

The ONS 15454 SDH E-1 cards (E1-N-14) provide fourteen E-1 ports. Each port operates at 2.048 MBits/s (Mbps). Default thresholds are based on recommendations in ITU-T G.841.

Procedure: Modify Line and Threshold Settings for the E-1 Card

Purpose	Set the E1 (2.048 Mbps) interface parameters for required connection
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1 Display the E1-N-14 in CTC card view.

Step 2 Click the **Provisioning** tab (Figure 7-4).

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **SDH Thresholds**, or **Alarm Behavior** tab.

Step 4 Modify the settings shown in Table 7-4. For drop-down lists, choose an item from the list. For numerics, double-click the field and type the new number.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 to 5 for each subtab that has parameters you want to provision.

Table 7-4   E1-N-14 Card Parameters

Parameter	Description	Options
Line Subtab		
Port #	Port number	1–14
Port Name	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.	E1_MF (default) E1_CRCMF E1_UNFRAM
Line Coding	Defines the line coding type.	HDB3
State	Places the port in or out of service.	IS (in service) OOS (out of service, default) OOS_MT (out of service, maintenance) OOS_AINS (out of service, auto in-service)
AINS Soak	Auto-in service soak. The period traffic is run on ONS 15454 SDH with alarms suppressed (OOS_AINS).	Numeric. The range is 00:00 hours and minutes to 48:45 hours and minutes 08:00 is the default
Line Thresholds Subtab		
Port #	Port number	1–14
CV	Coding violations	Numeric. Defaults: 17790 (15 min) 177900 (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)
Elect Path Thresholds Subtab (Electrical Path Thresholds)		
Port #	Port number	1–14
EB	Errored blocks	Numeric. Defaults: 9 (15 minutes, near end) 0 (15 minutes, far end) 90 (1 day, near end) 0 (1 day, far end)

Table 7-4   E1-N-14 Card Parameters (continued)

Parameter	Description	Options
BBE	Background block error	Numeric. Defaults: 9 (15 minutes, near end) 0 (15 minutes, far end) 90 (1 day, near end) 0 (1 day, far end)
ES	Errored seconds	Numeric. Defaults: 65 (15 minutes, near end) 0 (15 minutes, far end) 648 (1 day, near end) 0 (1 day, far end)
SES	Severely errored seconds	Numeric. Defaults: 10 (15 minutes, near end) 0 (15 minutes, far end) 100 (1 day, near end) 0 (1 day, far end)
UAS	Unavailable seconds	Numeric. Default: 10 (15 minutes, near end) 0 (15 minutes, far end) 10 (1 day, near end) 0 (1 day, far end)
SDH Thresholds Subtab		
Port #	Port number	1–14
ES	Errored seconds	Numeric. Defaults: 65 (15 minutes, near end, VC LO) 648 (1 day, near end, VC LO) 65 (15 minutes, far end, VC LO) 648 (1 day, far end, VC LO)
SES	Severely errored seconds	Numeric. Defaults: 10 (15 minutes, near end, VC LO) 100 (1 day, near end, VC LO) 10 (15 minutes, far end, VC LO) 100 (1 day, far end, VC LO)
EB	Errored blocks	Numeric. Defaults: 18 (15 minutes, near end, VC LO) 180 (1 day, near end, VC LO) 18 (15 minutes, far end, VC LO) 180 (1 day, far end, VC LO)
UAS	Unavailable seconds	Numeric. Defaults: 10 (15 minutes, near end, VC LO) 10 (1 day, near end, VC LO) 10 (15 minutes, far end, VC LO) 10 (1 day, far end, VC LO)

Table 7-4   E1-N-14 Card Parameters (continued)

Parameter	Description	Options
BBE	Background block error	Numeric. Defaults: 15 (15 minutes, near end, VC LO) 150 (1 day, near end, VC LO) 15 (15 minutes, far end, VC LO) 150 (1 day, far end, VC LO)
Alarm Behavior Subtab		
Port	Port number	1–14
Profile	Sets the alarm profile for the port.	Default Inherited Custom profiles (if any)
Suppress Alarms	Suppresses the alarm display for the port.	Unchecked (default) Checked

7.2.2 E3-12 Card Parameters

The ONS 15454 SDH E3-12 card provides twelve E3 ports. Each port operates at 34.368 MBits/s (Mbps). Default thresholds are based on recommendations in ITU-T G.841.

Procedure: Modify Line and Threshold Settings for the E3-12 Card

Purpose	Set the E3 (34.368 MBits/s [Mbps]) interface parameters for required connection
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide* "Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1 Display the E3-12 in CTC card view.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Thresholds**, **Elect Path Thresholds**, **SDH Thresholds**, or **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.

Step 5 Click **Apply**.

Step 6 Repeat Steps 3 to 5 for each subtab that has parameters you want to provision.

Table 7-5   E3-12 Card Parameters

Parameter	Description	Options
Line Subtab		
Port #	Port number	1–12
Port Name	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.
State	Places port in or out of service.	IS (in service) OOS (out of service, default) OOS_MT (out of service, maintenance) OOS_AINS (out of service, auto in-service)
AINS Soak	Auto-in service soak. The period traffic is run on ONS 15454 SDH with alarms suppressed (OOS_AINS).	Numeric. The range is 00:00 hours and minutes to 48:45 hours and minutes
Line Thresholds Subtab		
Port #	Port number	1–12
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 Thresholds Subtab (Electrical Path)		
Port #	Port number	1–12
ES	Errored seconds	Numeric. Defaults: 20 (15 minutes, near end) 200 (1 day, near end)
SES	Severely errored seconds	Numeric. Defaults: 3 (15 minutes, near end) 7 (1 day, near end)
UAS	Unavailable seconds	Numeric. Defaults: 10 (15 minutes, near end) 10 (1 day, near end)
SDH Thresholds Subtab		

Table 7-5   E3-12 Card Parameters (continued)

Parameter	Description	Options
Port #	Port number	1–12
ES	Errored seconds	Numeric. Defaults: 12 (15 minutes, near end, VC LO) 100 (1 day, near end, VC LO) 20 (15 minutes, near end, VC 4) 200 (1 day, near end, VC 4) 12 (15 minutes, far end, VC LO) 100 (1 day, far end, VC LO) 15 (15 minute, far end, VC 4) 100 (1 day, far end, VC 4)
SES	Severely errored seconds	Numeric. Defaults: 3 (15 minutes, near end, VC LO) 7 (1 day, near end, VC LO) 3 (15 minutes, near end, VC 4) 7 (1 day, near end, VC 4) 3 (15 minutes, far end, VC LO) 7 (1 day, far end, VC LO) 3 (15 minute, far end, VC 4) 7 (1 day, far end, VC 4)
EB	Errored blocks	Numeric. Defaults: 15 (15 minutes, near end, VC LO) 125 (1 day, near end, VC LO) 15 (15 minutes, near end, VC 4) 125 (1 day, near end, VC 4) 15 (15 minutes, far end, VC LO) 125 (1 day, far end, VC LO) 15 (15 minute, far end, VC 4) 100 (1 day, far end, VC 4)
UAS	Unavailable seconds	Numeric. Defaults: 10 (15 minutes, near end, VC LO) 10 (1 day, near end, VC LO) 10 (15 minutes, near end, VC 4) 10 (1 day, near end, VC 4) 10 (15 minutes, far end, VC LO) 10 (1 day, far end, VC LO) 10 (15 minute, far end, VC 4) 10 (1 day, far end, VC 4)

Table 7-5   E3-12 Card Parameters (continued)

Parameter	Description	Options
BBE	Background block error	Numeric. Defaults: 15 (15 minutes, near end, VC LO) 125 (1 day, near end, VC LO) 25 (15 minutes, near end, VC 4) 250 (1 day, near end, VC 4) 15 (15 minutes, far end, VC LO) 125 (1 day, far end, VC LO) 25 (15 minute, far end, VC 4) 250 (1 day, far end, VC 4)
Alarm Behavior Subtab		
Port	Port number	1–12
Profile	Sets the alarm profile for the port.	Default Inherited Custom profiles (if any)
Suppress Alarms	Suppresses the alarm display for the port.	Unchecked (default) Checked

7.2.3 DS3i-N-12 Card Parameters

The DS3i-N-12 cards provide twelve DS-3 ports. Each port operates at 44.736 MBits/s (Mbps). The DS3i-N-12 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.

Procedure: Modify Line and Threshold Settings for the DS3i-N-12 Card

Purpose	Set the DS3 (44.736 MBits/s [Mbps]) interface parameters for required connection
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide* "Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Display the DS3i-N-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 Thresholds**, **Elect Path Thresholds**, **SDH Thresholds**, or **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.

Step 5   Click **Apply**.

Step 6   Repeat Steps 3 to 5 for each subtab that has parameters you want to provision.

Table 7-6   DS3i-N-12 Card Parameters

Parameter	Description	Options
Line Subtab		
Port #	Port number	1–12
Port Name	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.	UNFRAMED M23 C BIT (default) AUTO PROVISION FMT
Detected Line Type	Displays the detected line type.	Read-only
Line Coding	Defines the DS3E transmission coding type.	B3ZS
Line Length[1]	Defines the distance (in feet) from backplane connection to the next termination point.	0–225 (default) 226–450
State	Places port in or out of service.	IS (in service) OOS (out of service, default) OOS_MT (out of service, maintenance) OOS_AINS (out of service, auto in-service)
AINS Soak	Auto-in service soak. The period traffic is run on ONS 15454 SDH with alarms suppressed (OOS_AINS).	Numeric. The range is 00:00 hours and minutes to 48:45 hours and minutes
Line Thresholds Subtab		
Port #	Port number	1–12
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 Thresholds Subtab (Electrical Path)		
Port #	Port number	1–12

Table 7-6   DS3i-N-12 Card Parameters (continued)

Parameter	Description	Options
CVP (or CVCP)	Coding violations path	Numeric. Defaults: 25 (15 minutes, near end, DS3 Pbit) 250 (1 day, near end, DS3 Pbit) 382 (15 minutes, near end, DS3 CPbit) 3820 (1 day, near end, DS3 CPbit) 382 (15 minutes, far end, DS3 CPbit) 3820 (1 day, far end, DS3 CPbit)
ESP (or ESCP)	Errored seconds path	Numeric. Defaults: 20 (15 minute, near end, DS3 Pbit) 200 (1 day, near end, DS3 Pbit) 25 (15 minutes, near end, DS3 CPbit) 250 (1 day, near end, DS3 CPbit) 25 (15 minutes, far end, DS3 CPbit) 250 (1 day, far end, DS3 CPbit)
SESP (or SESCP)	Severely errored seconds path	Numeric. Defaults: 3 (15 minute, near end, DS3 Pbit) 7 (1 day, near end, DS3 Pbit) 4 (15 minutes, near end, DS3 CPbit) 40 (1 day, near end, DS3 CPbit) 4 (15 minutes, far end, DS3 CPbit) 40 (1 day, far end, DS3 CPbit)
SASP (or SASCP)	Severely errored frame/Alarm indication signal path	Numeric. Defaults: 2 (15 minute, near end, DS3 Pbit) 8 (1 day, near end, DS3 Pbit) 2 (15 minutes, near end, DS3 CPbit) 8 (1 day, near end, DS3 CPbit) 2 (15 minutes, far end, DS3 CPbit) 8 (1 day, far end, DS3 CPbit)
UASP (or UASCP)	Unavailable seconds path	Numeric. Defaults: 10 (15 minute, near end, DS3 Pbit) 10 (1 day, near end, DS3 Pbit) 10 (15 minutes, near end, DS3 CPbit) 10 (1 day, near end, DS3 CPbit) 10 (15 minutes, far end, DS3 CPbit) 10 (1 day, far end, DS3 CPbit)
AISSP	AIS seconds path	Numeric. Defaults: 10 (15 minute, near end, DS3 Pbit) 10 (1 day, near end, DS3 Pbit)
SDH Thresholds Subtab		
Port #	Port number	1–12

Table 7-6   DS3i-N-12 Card Parameters (continued)

Parameter	Description	Options
ES	Errored seconds	Numeric. Default: 12 (15 minutes, near end, VC LO) 100 (1 day, near end, VC LO) 12 (15 minutes, far end, VC LO) 100 (1 day, far end, VC LO) 12 (15 minutes, near end, VC 4) 100 (1 day, near end, VC 4) 12 (15 minutes, far end, VC 4) 100 (1 day, far end, VC 4)
SES	Severely errored seconds	Numeric. Default: 3 (15 minutes, near end, VC LO) 7 (1 day, near end, VC LO) 3 (15 minutes, far end, VC LO) 7 (1 day, far end, VC LO) 3 (15 minutes, near end, VC 4) 7 (1 day, near end, VC 4) 3 (15 minutes, far end, VC 4) 7 (1 day, far end, VC 4)
EB	Errored blocks	Numeric. Default: 15 (15 minutes, near end, VC LO) 125 (1 day, near end, VC LO) 15 (15 minutes, far end, VC LO) 125 (1 day, far end, VC LO) 15 (15 minutes, near end, VC 4) 125 (1 day, near end, VC 4) 15 (15 minutes, far end, VC 4) 125 (1 day, far end, VC 4)
UAS	Unavailable seconds	Numeric. Default: 15 (15 minutes, near end, VC LO) 10 (1 day, near end, VC LO) 10 (15 minutes, far end, VC LO) 10 (1 day, far end, VC LO) 10 (15 minutes, near end, VC 4) 10 (1 day, near end, VC 4) 10 (15 minutes, far end, VC 4) 10 (1 day, far end, VC 4)
BBE	Background block error	Numeric. Default: 15 (15 minutes, near end, VC LO) 125 (1 day, near end, VC LO) 15 (15 minutes, far end, VC LO) 125 (1 day, far end, VC LO) 25 (15 minutes, near end, VC 4) 250 (1 day, near end, VC 4) 225 (15 minutes, far end, VC 4) 250 (1 day, far end, VC 4)

Alarm Behavior Subtab

Table 7-6   DS3i-N-12 Card Parameters (continued)

Parameter	Description	Options
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.	Unchecked (default) Checked

1. To convert meters (m) to feet (ft.), multiply by 3.28. To convert feet to meters, multiply by .328.

7.3 Converting E1 and DS3i Cards From 1:1 to 1:N Protection

The ONS 15454 SDH provides several protection options for E1-N-14 and DS3i-N-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 E1-N-14 or DS3i-N-12 card in Slot 3 or 15 on the same side of the ONS 15454 SDH as the cards it protects. Slot 3 protects cards in Slots 1 to 2 and 4 to 6. Slot 15 protects cards in Slots 12 to 14 and 16 to 17. An E1-N-14 or DS3i-N-12 card installed in Slot 3 or 15 can protect up to five E1-N-14 or DS3i-N-12 cards. If you install a DS3i-N-12 or E1-N-14 card in another slot, it is not able to protect other E1-N-14 or DS3i-N-12 cards in 1:N protection.

To create 1:1 protection for E1-N-14 and DS3i-N-12 cards, see the 3.6 Creating Card Protection Groups, page 3-26.

Procedure: Convert E1-N-14 Cards From 1:1 to 1:N Protection

Note   This procedure assumes E1-N-14 cards are installed in Slots 1 through 6 and/or Slots 12 through 17.

Purpose	Setting E1-N-14 cards to 1:N protection
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*, and either a protection card installed in Slot 3 (for protection of cards in Slots 1 to 6); or a protection card installed in Slot 15 (for protection of cards in Slots 12 to 17)
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

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

Step 2   In the Protection Groups list, click the protection group that contains Slot 3 or Slot 15 (where you will install the E1-N-14 card that protects the others).

⚠
Caution   Protection conversion must be carried out on a card that is not carrying traffic so that traffic will not be interrupted.

Step 3   Ensure the working and protect cards are in normal status.

The cards contained in the 1:1 protection group are listed under Selected Group in the Maintenance > Protection tabs.

The normal card status in the protection group is for one slot to say Working/Active and for the other to say Protect/Standby. If one of the cards says Protect/Active, it means that the protect card is carrying traffic for the working card because the working card has an error condition or alarm. This condition or alarm must be solved before the card protection type can be converted, since the current protection group has to be deleted. Click the **Alarms** tab and troubleshoot the alarms according to the methods in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

If the traffic switch from the working card to the protect card was carried out as an automatic protection switch, this will be indicated in the Conditions tab by conditions that begin with "AUTOSW" such as AUTOSW-AIS-SNCP, AUTOSW-LOP-SNCP, AUTOSW-SDBER-SNCP, AUTOSW-SFBER-SNCP, or AUTOSW-UNEQ-SNCP. Once the alarm that caused the autoswitch is solved, traffic should revert back to the working card and the card should say Working/Active in the Selected Group list.

If the traffic switch was carried out by a switch command, clear the switch by the following steps:

a.   Under Selected Group, click the protect card.

b.   Next to Switch Commands, click **Clear**.

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.

Step 4   Repeat Steps 1 to 3 for each protection group that you need to convert.

Step 5   Verify that no standing alarms exist for any of the E1-N-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   Under Protection Groups, click the 1:1 protection group containing 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 8 and 9 for other protection groups.

Step 11   Verify that the card boots up properly.

Step 12   Click the **Provisioning > Protection** tabs.

Step 13   Click **Create**. The Create Protection Group dialog box opens with the protect card in the Protect Entity field and the cards available for protection listed in the Available Entities list.

Step 14 Type a name for the protection group in the Name field (optional).

Step 15 Click **Type** and choose **1:N (card)** from the pull-down menu.

Step 16 Verify that the E1-N-14 card appears in the Protect Entities field.

Step 17 In the Available Entities list, highlight the cards that you want in the protection group. Click the Arrow (>>) button to move the cards to the Working Entities list.

Step 18 Click **OK**.

The protection group appears in the Protection Groups list on the Protection subtab.

Procedure: Convert DS3i-N-12 Cards From 1:1 to 1:N Protection

Note This procedure assumes that DS3i-N-12 cards are installed in Slots 1 to 6 and/or Slots 12 to 17.

Purpose	Verify that the ONS 15454 shelf is ready for turnup
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*, and either a protection card installed in Slot 3 (for protection of cards in Slots 1 to 6) or a protection card installed in Slot 15 (for protection of cards in Slots 12 to 17) "Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

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

Step 2 In the Protection Groups list, click the protection group that contains Slot 3 or Slot 15 (where you will install the DS3i-N-12 card that protects the others).

Step 3 Ensure the working and protect cards are in normal status.

The cards contained in the 1:1 protection group are listed under Selected Group in the Maintenance > Protection tabs.

The normal card status in the protection group is for one slot to say Working/Active and for the other to say Protect/Standby. If one of the cards says Protect/Active, it means that the protect card is carrying traffic for the working card because the working card has an error condition or alarm. This condition or alarm must be solved before the card protection type can be converted, since the current protection group has to be deleted. Click the **Alarms** tab and troubleshoot the alarms according to the methods in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

If the traffic switch from the working card to the protect card was carried out as an automatic protection switch, this will be indicated in the Conditions tab by conditions that begin with "AUTOSW" such as AUTOSW-AIS-SNCP, AUTOSW-LOP-SNCP, AUTOSW-SDBER-SNCP, AUTOSW-SFBER-SNCP, or AUTOSW-UNEQ-SNCP. Once the alarm that caused the autoswitch is solved, traffic should revert back to the working card and the card should say Working/Active in the Selected Group list.

If the traffic switch was carried out by a switch command, clear the switch by the following steps:

a. Under Selected Group, click the protect card.

b. Next to Switch Commands, click **Clear**.

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.

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 DS3i-N-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 Under Protection Groups, click the 1:1 protection group containing 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 you are deleting more than one protection group, repeat Steps 6 – 8 for each group.

Step 11 Verify that the card boots up properly.

Step 12 Click the **Provisioning > Protection** tabs.

Step 13 Click **Create**. The Create Protection Group dialog box opens with the protect card in the Protect Entity field and the cards available for protection listed in the Available Entities list.

Step 14 Type a name for the protection group in the Name field (optional).

Step 15 Click **Type** and choose **1:N (card)** from the pull-down menu.

Step 16 Verify that the DS3i-N-12 card appears in the Protect Entities field.

Step 17 In the Available Entities list, highlight the cards that you want in the protection group. Click the Arrow (**>>**) button to move the cards to the Working Entities list.

Step 18 Click **OK**.

The protection group appears in the Protection Groups list on the Protection subtab.

7.4 Provisioning Intermediate-Path Performance Monitoring

Intermediate path performance monitoring (IPPM) allows you to transparently monitor traffic originating on E-1, E-3, and DS-3 cards (path-terminating equipment) as it passes through STM-1, STM-4, STM-16, and STM-64 cards (line-terminating equipment). To use IPPM, you create the VC4 circuit on the E-1, E-3 or DS-3 card, then enable IPPM on the STM-N cards that carry the circuit.

Near-end performance monitoring data on individual VC4 payloads is available by enabling IPPM.

For example, suppose you have a VC4 circuit that originates and terminates on E-N cards at Nodes 1 and 4. You want to monitor the circuit as it passes through STM-N cards at Nodes 2 and 3. To do this, open the STM-N card, select the **Provisioning > VC4** tabs, and check **Enable IPPM** for the appropriate VC4, in this example, Line 1, VC4 1 (Figure 7-5).

Figure 7-5   IPPM provisioned for VC4 on an OC-4 STM-1 card
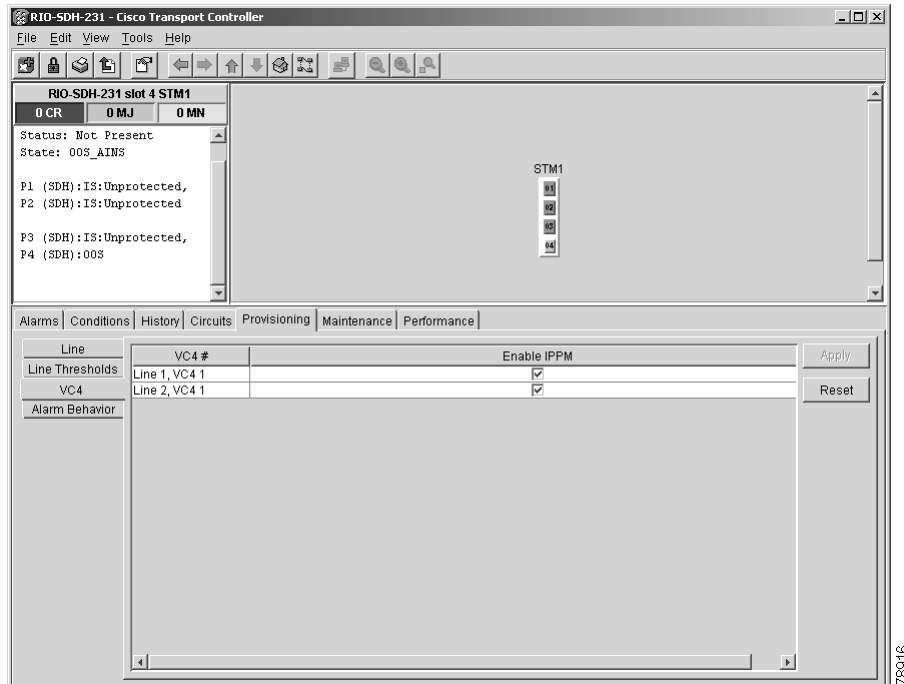
After enabling IPPM, performance is displayed on the Performance tab for the STM-N card. IPPM enables per-path statistics for VC4 CV-P (coding violations), VC4 ES-P (errored seconds), VC4 FC-P (failure count), VC4 SES-P (severely errored seconds), and VC4 UAS-P (unavailable seconds). Only one VC4 per port can be monitored at one time. For additional information about ONS 15454 SDH performance monitoring, see to Chapter 8, "SDH Performance Monitoring."

7.5 Provisioning Optical Cards

This section explains how to provision line and threshold settings for OC-N/STM-N cards, and how to provision OC-N/STM-N cards for SDH.

Note   The expression OC-N/STM-N is used because the numbering in SONET (OC-N) and SDH (STM-N) are not the same. OC-3 corresponds with STM-1, etc.

The OC-N/STM-N abbreviation stands for any of the following cards:

- OC3 IR 4/STM1 SH 1310
- OC12 IR/STM4 SH 1310
- OC12 LR/STM4 LH 1310
- OC12 LR/STM4 LH 1550
- OC12 IR/STM4 SH 1310-4
- OC48 IR/STM16 SH AS 1310
- OC48 LR/STM16 LH AS 1550

- OC48 ELR/STM16 EH 100 GHz

- OC192 LR/STM64 LH 1550

The OC48 ELR/STM16 EH 100 GHz cards are available in eighteen different wavelength versions for dense wavelength division multiplexing (DWDM). For a list of available wavelengths, refer to the "OC48 ELR/STM 16 EH 100 GHz Card Specifications" section in Chapter 3 of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*, Release 3.4. In the following tables, all these cards are abbreviated as STM-1, STM-4, STM-16, and STM-64.

7.6 Modifying Optical Card Transmission Quality

The STM-1, STM-4, STM-16 and STM-64 cards are preprovisioned with settings that you can modify to manage transmission quality. For each optical card, you can specify thresholds for near and far end nodes at the Line, Section, and Path levels for 15-minute and 1-day intervals. Depending on the card, you can specify Line, Section, and Path thresholds.

Procedure: Provision Line Transmission Settings for OC-N/STM-N Cards

Purpose	Setting line parameters for optical cards
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Display the OC-N/STM-N card in CTC card view.

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

Step 3   Modify the settings shown in Table 7-7.

Step 4   Click **Apply**.

Table 7-7   OC-N/STM-N Card Line Settings

Heading	Description	Options
Port#	Port number	1–4 (STM-1, STM-4-4) 1 (STM-4, STM-16, STM-64)
Port Name	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.
SF BER	Sets the signal fail bit error rate.	1E-3 1E-4 (default) 1E-5
SD BER	Sets the signal degrade bit error rate.	1E-5 1E-6 1E-7 (default) 1E-8 1E-9
ProvidesSync	If checked, the card is provisioned as a network element timing reference on the Provisioning > Timing tabs.	Read-only Yes (checked) No (unchecked)
EnableSyncMsg	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.	Yes (checked, default) No (unchecked)
Send DoNotUse	When checked, sends a DUS (do not use) message on the S1 byte.	Yes (checked) No (unchecked; default)
PJVc4Mon#	Enables pointer justification count for the VC-4 monitor.	0 (default) 1
State	Places port in or out of service.	IS (in service) OOS (out of service, default) OOS_MT (out of service, maintenance) OOS_AINS (out of service, auto in-service)
AINS Soak	Auto-in service soak. The period traffic is run on ONS 15454 SDH with alarms suppressed (OOS_AINS).	Numeric. The range is 00:00 hours and minutes to 48:45 hours and minutes
Type	Defines the port as SDH.	SDH

Procedure: Provision Threshold Settings for STM-N Cards

Purpose	Modifying threshold settings for optical cards
Tools/Equipment	Computer with CTC
Prerequisite Procedures	All shelf and card installation procedures in the *Cisco ONS 15454 SDH Installation and Operations Guide*
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Display the STM-N card in CTC card view (Figure 7-6).

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

Step 3   Modify the settings shown in Table 7-8.

Step 4   Click **Apply**.

Figure 7-6   Provisioning thresholds for the OC48 IR/STM16 SH AS 1310 card

Note   Default thresholds apply to all optical cards unless otherwise specified.

Table 7-8   STM-N Card Threshold Settings

Heading	Description	Options
Port	Port number	1–4 (STM-1) 1 (STM-4, STM-16, STM-64)
EB	Errored blocks	Numeric. Defaults: 1312 (STM-1, 15 minutes, near end, MS) 13120 (STM-1, 1 day, near end, MS) 1312 (STM-1, 15 minutes, far end, MS) 13120 (STM-1, 1 day, far end, MS) 10000 (STM-1, 15 minutes, near end, RS) 100000 (STM-1, 1 day, near end, RS) 15 (STM-1, 15 minutes, near end, Path) 125 (STM-1, 1 day, near end, Path) 15 (STM-1, 15 minutes, far end, Path) 125 (STM-1, 1 day, far end, Path) 5315 (STM-4, 15 minutes, near end, MS) 53150 (STM-4, 1 day, near end, MS) 5315 (STM-4, 15 minutes, far end, MS) 53150 (STM-4, 1 day, far end, MS) 10000 (STM-4, 15 minutes, near end, RS) 100000 (STM-4, 1 day, near end, RS) 15 (STM-4, 15 minutes, near end, Path) 125 (STM-4, 1 day, near end, Path) 21260 (STM-16, 15 minutes, near end, MS) 212600 (STM-16, 1 day, near end, MS) 21260 (STM-16, 15 minutes, far end, MS) 212600 (STM-16, 1 day, far end, MS) 10000 (STM-16, 15 minutes, near end, RS) 100000 (STM-16, 1 day, near end, RS) 15 (STM-16, 15 minutes, near end, Path) 125 (STM-16, 1 day, near end, Path) 85040 (STM-64, 15 minutes, near end, MS) 850400 (STM-64, 1 day, near end, MS) 85040 (STM-64, 15 minutes, far end, MS) 850400 (STM-64, 1 day, far end, MS) 10000 (STM-64, 15 minutes, near end, RS) 100000 (STM-64, 1 day, near end, RS) 15 (STM-64, 15 minute, near end, Path) 125 (STM-64, 1 day, near end, Path)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
ES	Errored seconds	Numeric. Defaults:
		87 (STM-1, 15 minutes, near end, MS)
		864 (STM-1, 1 day, near end, MS)
		87 (STM-1, 15 minutes, far end, MS)
		864 (STM-1, 1 day, far end, MS)
		500 (STM-1, 15 minutes, near end, RS)
		5000 (STM-1, 1 day, near end, RS)
		12 (STM-1, 15 minutes, near end, Path)
		100 (STM-1, 1 day, near end, Path)
		12 (STM-1, 15 minutes, far end, Path)
		100 (STM-1, 1 day, far end, Path)
		87 (STM-4, 15 minutes, near end, MS)
		864 (STM-4, 1 day, near end, MS)
		87 (STM-4, 15 minutes, far end, MS)
		864 (STM-4, 1 day, far end, MS)
		500 (STM-4, 15 minutes, near end, RS)
		5000 (STM-4, 1 day, near end, RS)
		12 (STM-4, 15 minutes, near end, Path)
		100 (STM-4, 1 day, near end, Path)
		87 (STM-16, 15 minutes, near end, MS)
		864 (STM-16, 1 day, near end, MS)
		87 (STM-16, 15 minutes, far end, MS)
		864 (STM-16, 1 day, far end, MS)
		500 (STM-16, 15 minutes, near end, RS)
		5000 (STM-16, 1 day, near end, RS)
		12 (STM-16, 15 minutes, near end, Path)
		100 (STM-16, 1 day, near end, Path)
		87 (STM-64, 15 minutes, near end, MS)
		864 (STM-64, 1 day, near end, MS)
		87 (STM-64, 15 minutes, far end, MS)
		864 (STM-64, 15 minutes, far end, MS)
		500 (STM-64, 15 minutes, near end, RS)
		5000 (STM-64, 1 day, near end, RS)
		12 (STM-64, 15 minute, near end, Path)
		100 (STM-64, 1 day, near end, Path)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
BBE	Background block errors	Numeric. Defaults:
		1312 (STM-1, 15 minutes, near end, MS) 13120 (STM-1, 1 day, near end, MS) 1312 (STM-1, 15 minutes, far end, MS) 13120 (STM-1, 1 day, far end, MS) 10000 (STM-1, 15 minutes, near end, RS) 100000 (STM-1, 1 day, near end, RS) 25 (STM-1, 15 minutes, near end, Path) 250 (STM-1, 1 day, near end, Path) 25 (STM-1, 15 minutes, far end, Path) 250 (STM-1, 1 day, far end, Path)
		5315 (STM-4, 15 minutes, near end, MS) 53150 (STM-4, 1 day, near end, MS) 5315 (STM-4, 15 minutes, far end, MS) 53150 (STM-4, 1 day, far end, MS) 10000 (STM-4, 15 minutes, near end, RS) 100000 (STM-4, 1 day, near end, RS) 25 (STM-4, 15 minutes, near end, Path) 250 (STM-4, 1 day, near end, Path)
		21260 (STM-16, 15 minutes, near end, MS) 212600 (STM-16, 1 day, near end, MS) 21260 (STM-16, 15 minutes, far end, MS) 212600 (STM-16, 1 day, far end, MS) 10000 (STM-16, 15 minutes, near end, RS) 100000 (STM-16, 1 day, near end, RS) 25 (STM-16, 15 minutes, near end, Path) 250 (STM-16, 1 day, near end, Path)
		85040 (STM-64, 15 minutes, near end, MS) 850400 (STM-64, 1 day, near end, MS) 85040 (STM-64, 15 minutes, far end, MS) 850400 (STM-64, 15 minutes, far end, MS) 10000 (STM-64, 15 minutes, near end, RS) 100000 (STM-64, 1 day, near end, RS) 25 (STM-64, 15 minute, near end, Path) 250 (STM-64, 1 day, near end, Path)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
SES	Severely errored seconds	Numeric. Defaults:
		1 (STM-1, 15 minutes, near end, MS) 4 (STM-1, 1 day, near end, MS) 1 (STM-1, 15 minutes, far end, MS) 4 (STM-1, 1 day, far end, MS) 500 (STM-1, 15 minutes, near end, RS) 5000 (STM-1, 1 day, near end, RS) 3 (STM-1, 15 minutes, near end, Path) 7 (STM-1, 1 day, near end, Path) 3 (STM-1, 15 minutes, far end, Path) 7 (STM-1, 1 day, far end, Path)
		1 (STM-4, 15 minutes, near end, MS) 4 (STM-4, 1 day, near end, MS) 1 (STM-4, 15 minutes, far end, MS) 4 (STM-4, 1 day, far end, MS) 500 (STM-4, 15 minutes, near end, RS) 5000 (STM-4, 1 day, near end, RS) 3 (STM-4, 15 minutes, near end, Path) 7 (STM-4, 1 day, near end, Path)
		1 (STM-16, 15 minutes, near end, MS) 4 (STM-16, 1 day, near end, MS) 1 (STM-16, 15 minutes, far end, MS) 4 (STM-16, 1 day, far end, MS) 500 (STM-16, 15 minutes, near end, RS) 5000 (STM-16, 1 day, near end, RS) 3 (STM-16, 15 minutes, near end, Path) 7 (STM-16, 1 day, near end, Path)
		1 (STM-64, 15 minutes, near end, MS) 4 (STM-64, 1 day, near end, MS) 1 (STM-64, 15 minutes, far end, MS) 4 (STM-64, 1 day, far end, MS) 500 (STM-64, 15 minutes, near end, RS) 5000 (STM-64, 1 day, near end, RS) 3 (STM-64, 15 minute, near end, Path) 7 (STM-64, 1 day, near end, Path)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
UAS	Unavailable seconds	Numeric. Defaults: 3 (STM-1, 15 minutes, near end, MS) 10 (STM-1, 1 day, near end, MS) 3 (STM-1, 15 minutes, far end, MS) 10 (STM-1, 1 day, far end, MS) 10 (STM-1, 15 minutes, near end, Path) 10 (STM-1, 1 day, near end, Path) 10 (STM-1, 15 minutes, far end, Path) 10 (STM-1, 1 day, far end, Path) 3 (STM-4, 15 minutes, near end, MS) 10 (STM-4, 1 day, near end, MS) 3 (STM-4, 15 minutes, far end, MS) 10 (STM-4, 1 day, far end, MS) 10 (STM-4, 15 minutes, near end, Path) 10 (STM-4, 1 day, near end, Path) 3 (STM-16, 15 minutes, near end, MS) 10 (STM-16, 1 day, near end, MS) 3 (STM-16, 15 minutes, far end, MS) 10 (STM-16, 1 day, far end, MS) 10 (STM-16, 15 minutes, near end, Path) 10 (STM-16, 1 day, near end, Path) 3 (STM-64, 15 minutes, near end, MS) 10 (STM-64, 1 day, near end, MS) 3 (STM-64, 15 minutes, far end, MS) 10 (STM-64, 1 day, far end, MS) 3 (STM-64, 15 minute, near end, Path) 10 (STM-64, 1 day, near end, Path)
PPJC-Pdet	Positive pointer justification count, STS path detected	Numeric. Defaults: 60 (STM-1, 15 minutes, near end, MS) 5760 (STM-1, 1 day, near end, MS) 60 (STM-4, 15 minutes, near end, MS) 5760 (STM-4, 1 day, near end, MS) 60 (STM-16, 15 minutes, near end, MS) 5760 (STM-16, 1 day, near end, MS) 60 (STM-64, 15 minutes, near end, MS) 60 (STM-64, 1 day, near end, MS)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
NPJC-Pdet	Negative pointer justification count, STS path detected	Numeric. Defaults: 60 (STM-1, 15 minutes, near end, MS) 5760 (STM-1, 1 day, near end, MS) 60 (STM-4, 15 minutes, near end, MS) 5760 (STM-4, 1 day, near end, MS) 60 (STM-16, 15 minutes, near end, MS) 5760 (STM-16, 1 day, near end, MS) 60 (STM-64, 15 minutes, near end, MS) 60 (STM-64, 1 day, near end, MS)
PPJC-Pgen	Positive pointer justification count, STS path generated	Numeric. Defaults: 60 (STM-1, 15 minutes, near end, MS) 5760 (STM-1, 1 day, near end, MS) 60 (STM-4, 15 minutes, near end, MS) 5760 (STM-4, 1 day, near end, MS) 60 (STM-16, 15 minutes, near end, MS) 5760 (STM-16, 1 day, near end, MS) 60 (STM-64, 15 minutes, near end, MS) 60 (STM-64, 1 day, near end, MS)
NPJC-Pgen	Negative pointer justification count, STS path generated	Numeric. Defaults: 60 (STM-1, 15 minutes, near end, MS) 5760 (STM-1, 1 day, near end, MS) 60 (STM-4, 15 minutes, near end, MS) 5760 (STM-4, 1 day, near end, MS) 60 (STM-16, 15 minutes, near end, MS) 5760 (STM-16, 1 day, near end, MS) 60 (STM-64, 15 minutes, near end, MS) 60 (STM-64, 1 day, near end, MS)
PSC	Protection switching count (line)	Numeric. Defaults: 1 (STM-1, 15 minutes, near end, MS) 5 (STM-1, 1 day, near end, MS) 1 (STM-4, 15 minutes, near end, MS) 5 (STM-4, 1 day, near end, MS) 1 (STM-16, 15 minutes, near end, MS) 5 (STM-16, 1 day, near end, MS) 1 (STM-64, 15 minutes, near end, MS) 5 (STM-64, 1 day, near end, MS)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
PSD	Protection switching duration (line)	Numeric. Defaults: 300 (STM-1, 15 minutes, near end, MS) 600 (STM-1, 1 day, near end, MS) 300 (STM-4, 15 minutes, near end, MS) 600 (STM-4, 1 day, near end, MS) 300 (STM-16, 15 minutes, near end, MS) 600 (STM-16, 1 day, near end, MS) 300 (STM-64, 15 minutes, near end, MS) 600 (STM-64, 1 day, near end, MS)
PSC-W	Protection switching count - working line	Numeric. Defaults: 1 (STM-4, 15 minutes, near end, MS) 5 (STM-4, 1 day, near end, MS) 1 (STM-16, 15 minutes, near end, MS) 5 (STM-16, 1 day, near end, MS) 1 (STM-64, 15 minutes, near end, MS) 5 (STM-64, 1 day, near end, MS)
PSD-W	Protection switching duration - working line	Numeric. Defaults: 300 (STM-4, 15 minutes, near end, MS) 600 (STM-4, 1 day, near end, MS) 300 (STM-16, 15 minutes, near end, MS) 600 (STM-16, 1 day, near end, MS) 300 (STM-64, 15 minutes, near end, MS) 600 (STM-64, 1 day, near end, MS)
PSC-S	Protection switching count - span	Numeric. Defaults: 1 (STM-16, 15 minutes, near end, MS) 5 (STM-16, 1 day, near end, MS) 1 (STM-64, 15 minutes, near end, MS) 5 (STM-64, 1 day, near end, MS)
PSD-S	Protection switching duration - span	Numeric. Defaults: 300 (STM-16, 15 minutes, near end, MS) 600 (STM-16, 1 day, near end, MS) 300 (STM-64, 15 minutes, near end, MS) 600 (STM-64, 1 day, near end, MS)

Table 7-8   STM-N Card Threshold Settings (continued)

Heading	Description	Options
PSC-R	Protection switching count - ring	Numeric. Defaults: 1 (STM-16, 15 minutes, near end, MS) 5 (STM-16, 1 day, near end, MS) 1 (STM-64, 15 minutes, near end, MS) 5 (STM-64, 1 day, near end, MS)
PSD-R	Protection switching duration - ring	Numeric. Defaults: 300 (STM-16, 15 minutes, near end, MS) 600 (STM-16, 1 day, near end, MS) 300 (STM-64, 15 minutes, near end, MS) 600 (STM-64, 1 day, near end, MS)

7.7 Optical Card Protection

The ONS 15454 SDH currently supports 1+1 span protection to create redundancy for optical cards. Optical cards in any two slots can be paired for protection. 1+1 protection pairs a single working card with a single dedicated protect card. If the working card fails, the protect cards takes over.

With non-revertive 1+1 protection, when a failure occurs and the signal switches from the working card to the protect card, the signal stays switched to the protect card until it is manually switched back. Revertive 1+1 protection automatically switches the signal back to the working card when the working card comes back on line. Establishing optical card protection groups is covered in Chapter 3, "Node Setup."

7.8 Provisioning Ethernet Cards

Three Ethernet cards are available for the ONS 15454 SDH.

- E100T-G, providing twelve electrical 10/100BaseT Ethernet interfaces
- E1000-G, providing two optical Gigabit Ethernet interfaces
- G1000-4, providing four optical Gigabit Ethernet interfaces

Ethernet card provisioning is described in Chapter 9.

7.9 Provisioning the Alarm Interface

The ONS 15454 SDH can monitor alarms through the Alarm Interface Card-International (AIC-I). The AIC-I card provides 16 external alarm inputs and four alarm inputs or outputs (user-configured). The inputs are routed to the AIC-I through the backplane from the MIC-A/P card. (For more information about the AIC-I and MIC-A/P card specifications, see the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.)

Procedure: Provision the AIC-I Card

Purpose	Use this procedure to create external (environmental) alarms, external controls, orderwire tunnels, an extension type, or a station number for the AIC-I card.
Tools/Equipment	An AIC-I card installed in Slot 9
Prerequisite Procedures	"Install ONS 15454 SDH Power FMECs" procedure on page 1-22
	"Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34
Onsite/Remote	Onsite or remote

Step 1 Complete the "Log Into CTC" procedure on page 2-24 at the node with the AIC-I card you want to provision.

Step 2 As needed, complete the "Provision External Alarms and Controls on the AIC-I Card" procedure on page 7-34.

Step 3 As needed, complete the "Create a User Data Channel Circuit on the AIC-I" procedure on page 7-38.

Step 4 As needed, complete the "Provision the AIC-I Orderwire" procedure on page 7-38.

Tip Before you begin, make a list of the ONS 15454 SDH slots and ports that require orderwire communication.

Procedure: Provision External Alarms and Controls on the AIC-I Card

Purpose	Use this task to provision external alarms and controls on the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9.
Prerequisite Procedures	"Install ONS 15454 SDH Power FMECs" procedure on page 1-22
	"Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Note Specifications for the AIC-I card are located in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Step 1 From the CTC node (default login) view, double-click the AIC-I card on the CTC shelf graphic to display the card view.

Step 2 Click the **Provisioning > Card** tabs and complete the following fields for the card:

- *Input/Output*—Click the External Alarm radio button to provision the 16 alarm inputs controlled by the AIC-I card. Click the External Control radio to provision the four contacts that can be used as inputs or outputs. Selecting only External Alarm gives you 20 external alarm ports and no external control ports. If you select External Control, four more ports are converted to external control ports, leaving you with 16 external alarm ports.

- *Station Number*—Enter a four-digit number unique to the node. This is the orderwire "phone number" for this node. The station number is used to call this node over the orderwire channel.

  The default station number is 0000 and cannot be deleted. It is considered the party line number because it calls all nodes on the network when dialed.

Step 3   If you are provisioning external alarms, click the **External Alarms** tab (Figure 7-7). If you are not provisioning external alarms, skip Steps 4 and 5, and go directly to Step 6.

Figure 7-7   Provisioning external alarms on the AIC-I card
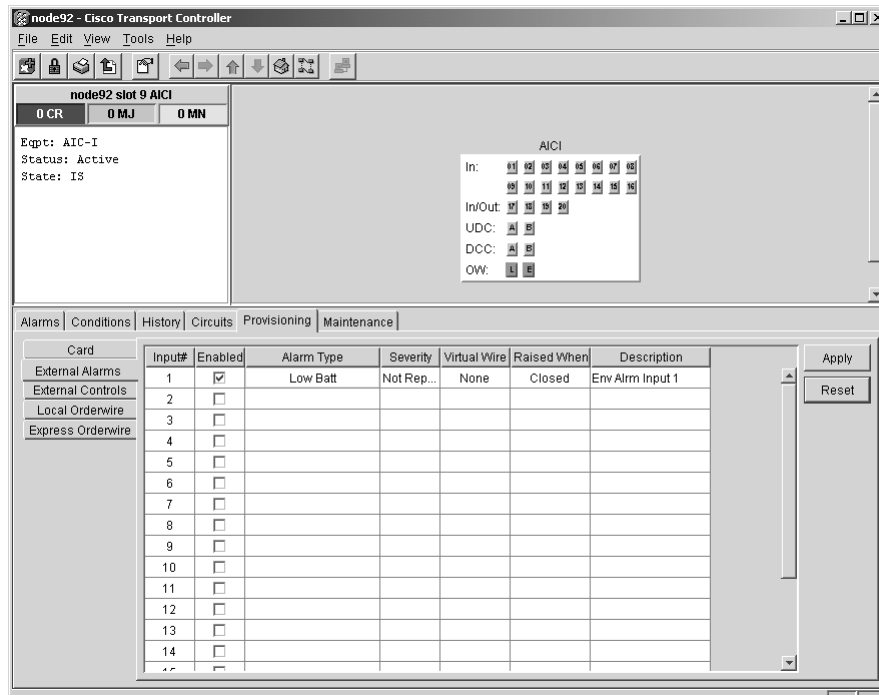
Step 4   Complete the following fields for each external device wired to the ONS 15454 SDH backplane:

- *Enabled*—Check to activate the fields for the alarm input number.

- *Alarm Type*—Choose an alarm type from the provided list as follows:
    - Compressor Failure
    - Air Cond Fail
    - Air Dryer Fail
    - Battery Discharge
    - Battery Fail
    - Cool Fan Fail
    - Ctrl PwrMaj Fail
    - Ctrl PwrMin Fail
    - Engine Fail
    - Engine Operating
    - Explosive Gas

- Fire Detector Fail

- Fire

- Flood

- Fuse Fail

- Generator Fail

- High Airflow

- High Humidity

- High Temp

- High Water

- Intrusion

- Low Batt

- Low fuel

- Low Humidity

- Low Cable Press

- Low Temp

- Low Water

- Misc (default)

- Open Door

- Comm. Pwr Fail

- Pump Fail

- 48 Power Supp. Fail

- Rectifier Fail

- Rectifier High Volt

- Rectifier Low Volt

- Smoke

- Toxic Gas

- Ventilation Fail

- *Severity*—Choose a severity from the list as follows:

  - Not Reported (default)

  - Not Alarmed

  - Minor

  - Major

  - Critical

  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, choose a virtual wire from the list as follows, or choose **None** if no assignment is required:

- None (default)

- Wire 1

- Wire 2

- Wire 3

- Wire 4

- *Raised When*—Choose the contact condition that will trigger the alarm in CTC from the following two options:

  - Closed (default)

  - Open

- *Description*—A default description is provided in this line for every external alarm that is enabled. If you double-click the cell, you can modify the description. The description can contain up to 24 characters.

To provision additional devices, complete Steps 3 and 4 for each additional device.

Step 5   Click **Apply**.

Step 6   If you are provisioning external controls, click the **External Controls** subtab and complete the following fields for each external control wired to the ONS 15454 SDH backplane:

- *Control #*—Assign a number, 1 to 4.

- *Enabled*—Click to activate the fields for the alarm input number.

- *Control Type*—Choose the control type from the list as follows:

  - Air conditioner

  - Engine

  - Fan

  - Generator

  - Heat

  - Light

  - Sprinkler

  - Miscellaneous.

- *Trigger Type*—Choose 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.

To provision additional controls, complete Step 6 for each additional device.

Step 7   Click **Apply**.

Procedure: Create a User Data Channel Circuit on the AIC-I

Purpose	Use this task to create a User Data Channel (UDC) circuit on the ONS 15454 SDH. A UDC circuit allows you to create a dedicated data channel between nodes.
Tools/Equipment	None
Prerequisite Procedures	"Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Display the network view. (From the View menu in node view, click **Go to Network View**.)

Step 2   Click the **Provisioning > Overhead Circuits** tabs.

Step 3   Click **Create**.

Step 4   In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name must be alphanumeric and up to 32 characters (including spaces).
- Type—Choose from following two options in the list:
    - User Data-F1 (default)
    - User Data D-4-D-12

> **Note**   None of the other Type options are used to create a UDC.

Step 5   Under Endpoints, choose the source and destination nodes from the drop-down menus.

Step 6   Under Endpoints, choose the source and destination optical ports and slots from the drop-down menus.

Step 7   Click **Finish**.

Procedure: Provision the AIC-I Orderwire

Purpose	Use this task to provision orderwire on the AIC-I card.
Tools/Equipment	An AIC-I card must be installed in Slot 9.
Prerequisite Procedures	"Install the Alarm Interface Controller (AIC-I) Card" procedure on page 1-34
	"Log Into CTC" procedure on page 2-24
Onsite/Remote	Onsite or remote

Step 1   Display the network view. (From the View menu in node view, click **Go to Network View.**)

Step 2   Click the **Provisioning > Overhead Circuits** tabs.

Step 3   Click **Create**.

Step 4 In the Circuit Creation dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name must be alphanumeric and up to 32 characters (including spaces).

- Type—Choose from following options (as appropriate for the orderwire path you want to create):

    – Local Orderwire

    – Express Orderwire

    If regenerators are not used between ONS 15454 SDH nodes, you can use either local or express AIC-I orderwire channels. If regenerators exist, use the express orderwire channel. You can provision up to four ONS 15454 SDH OC-N ports for each orderwire path.

- PCM—Choose from either of the two following options as appropriate:

    – A-law (default)

    – Mu-law

The Circuit Creation dialog box for a local orderwire is shown in Figure 7-8. Provisioning procedures are the same for both types of orderwire.

⚠
Caution   When provisioning orderwire for ONS 15454 SDHs 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.

Figure 7-8   Provisioning local orderwire
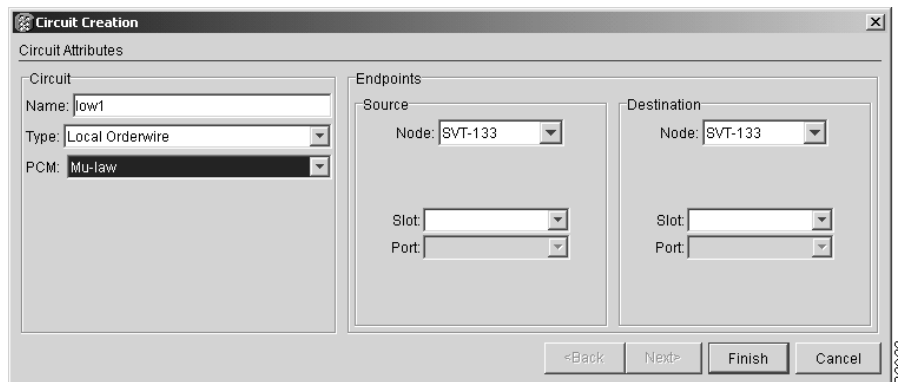
Step 5 Under Endpoints, choose the source and destination nodes from the drop-down menus.

Step 6 Under Endpoints, choose the source and destination optical ports and slots from the drop-down menus.

Step 7 Click **Finish**.

SDH Performance Monitoring

Performance monitoring (PM) parameters 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. For information about Ethernet PMs, see Chapter 9, "Ethernet Operation." For information about card thresholds see the "Setting Network Element Defaults" section on page 3-30 and Chapter 7, "Card Provisioning."

For additional information regarding PM parameters, see ITU G.826, Telcordia GR-820-CORE, and Telcordia GR-253-CORE. Table 8-1 lists PM reference topics. Table 8-2 lists PM procedures.

Table 8-1   Reference Topics for Performance Monitoring

Reference Topics
8.1 Using the Performance Monitoring Window, page 8-2
8.2 Changing Thresholds, page 8-12
8.3 Enabling Intermediate Path Performance Monitoring, page 8-14
8.4 Enabling Pointer Justification Count Parameters, page 8-15
8.5 SDH Performance Monitoring for Electrical Cards, page 8-18
8.6 SDH Performance Monitoring for Optical Cards, page 8-29

Table 8-2   Procedure List for Enabling and Monitoring Performance

Perform the Following Tasks As Needed
Procedure: View PMs, page 8-2
Procedure: Select Fifteen-Minute PM Intervals on the Performance Monitoring Window, page 8-3
Procedure: Select 1 Day PM Intervals on the Performance Monitoring Window, page 8-4
Procedure: Select Near End PMs on the Performance Monitoring Window, page 8-5
Procedure: Select Far End PMs on the Performance Monitoring Window, page 8-6
Procedure: Select Card Ports on the Performance Monitoring Window, page 8-8
Procedure: Use the Baseline Button on the Performance Monitoring Window, page 8-10
Procedure: Clearing PM Counts on the Performance Monitoring Window, page 8-11
Procedure: Enable Intermediate Path Performance Monitoring, page 8-14
Procedure: Enable Pointer Justification Count Performance Monitoring, page 8-17

8.1 Using the Performance Monitoring Window

The following sections describe how to use basic CTC window 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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."

Procedure: View PMs

Purpose	View PM counts to detect performance problems early.
Prerequisite Procedures	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

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 window in the Param column. The parameter numbers appear on the right portion of the window in the Curr (current), and Prev (previous) columns.

8.1.2 Changing the Window Intervals

Changing the window view allows you to view PMs in 15-minute intervals or 24-hour periods. Figure 8-2 shows the time interval radio buttons on the Performance Monitoring window.

Figure 8-2   Time interval radio buttons on the card view Performance tab

Fifteen-minute and twenty-four hour intervals
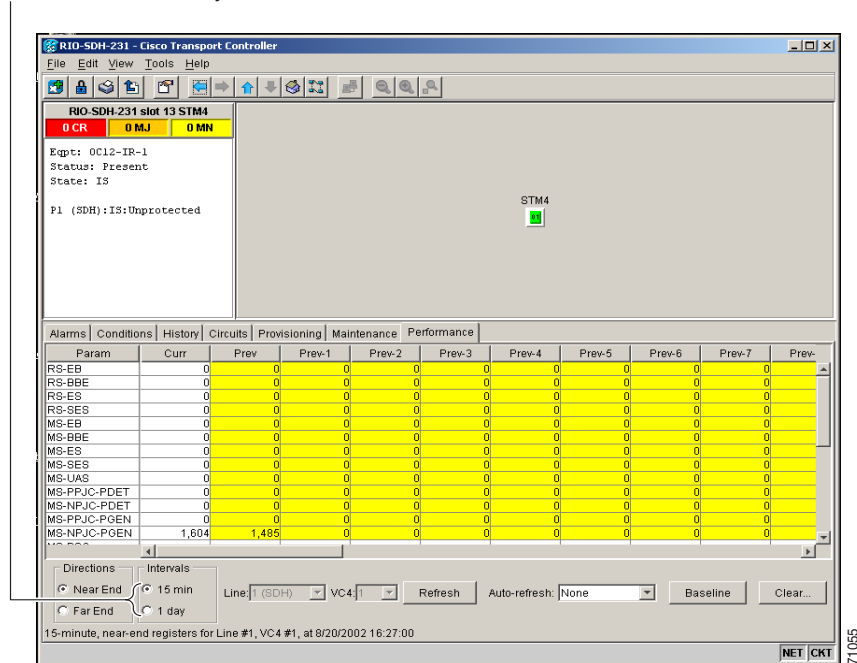
Procedure: Select Fifteen-Minute PM Intervals on the Performance Monitoring Window

Purpose	Change the window view to display PMs in 15-minute intervals.
Prerequisite Procedures	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

Step 2   From the card view, click the **Performance** tab.

Click the **15 min** radio button. Figure 8-2 shows the time interval buttons on the Performance Monitoring window.

Step 3   Click the **Refresh** button. Performance monitoring parameters display in 15-minute intervals synchronized with the time of day.

Step 4   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. For information about viewing TCAs, see "Viewing History" section on page 10-7.

Step 5   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 monitoring for less than 15 minutes after the counter started, changing node timing settings, changing the time zone settings in CTC, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 15-minute interval appears with a white background.

Procedure: Select 1 Day PM Intervals on the Performance Monitoring Window

Purpose	Change the window view to display PMs in 1 day intervals.
Prerequisite Procedures	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

Step 2   From the card view, click the **Performance** tab.

Click the **1 day** radio button. Figure 8-2 shows the time interval buttons on the Performance Monitoring window.

Step 3   Click the **Refresh** button. Performance monitoring displays in 1 day periods synchronized with the time of day.

Step 4   View the Current column to find PM counts for the current 1 day 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 1 day period, a TCA will be raised. The value represents the counter for each specific performance monitoring parameter. For information on viewing TCAs, see "Viewing History" section on page 10-7.

Step 5   View the Prev columns to find PM counts for the preceding 1 day period.

![pencil icon]

Note   If a complete count over a 1 day 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 in CTC, replacing a card, resetting a card, or changing port states. When the problem is corrected, the subsequent 1 day period appears with a white background.

8.1.3 Viewing Near End and Far End PMs

Select the Near End or Far End radio button depending on the PMs you wish to view. Only cards that allow both near-end and far-end monitoring have these radio buttons as an option. Figure 8-3 shows the Near End and Far End radio buttons on the Performance Monitoring window.

Figure 8-3   Near End and Far End radio buttons on the card view Performance tab

Near End and Far End buttons

Procedure: Select Near End PMs on the Performance Monitoring Window

Purpose	Select the Near End radio button to view PMs on the near end.
Prerequisite Procedures	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

Step 2   From the card view, click the **Performance** tab.

Step 3   Click the **Near End** radio 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 Window

Purpose	Select the Far End radio button to view PMs on the far end.
Prerequisite Procedures	Only cards that allow far-end monitoring have this radio button as an option.
	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

Step 2   From the card view, click the **Performance** tab.

Step 3   Click the **Far End** radio 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 Port Selection Menu

Use the port selection menus to monitor PMs for near-end or far-end signals on a selected port. Different port selection menus appear depending on the card type and the circuit type. Figure 8-4 and Figure 8-5 on page 8-8 show port selection menus on the Performance Monitoring window for a DS3i card and an STM-1 card.

Figure 8-4   Port selection menus for a DS3i card
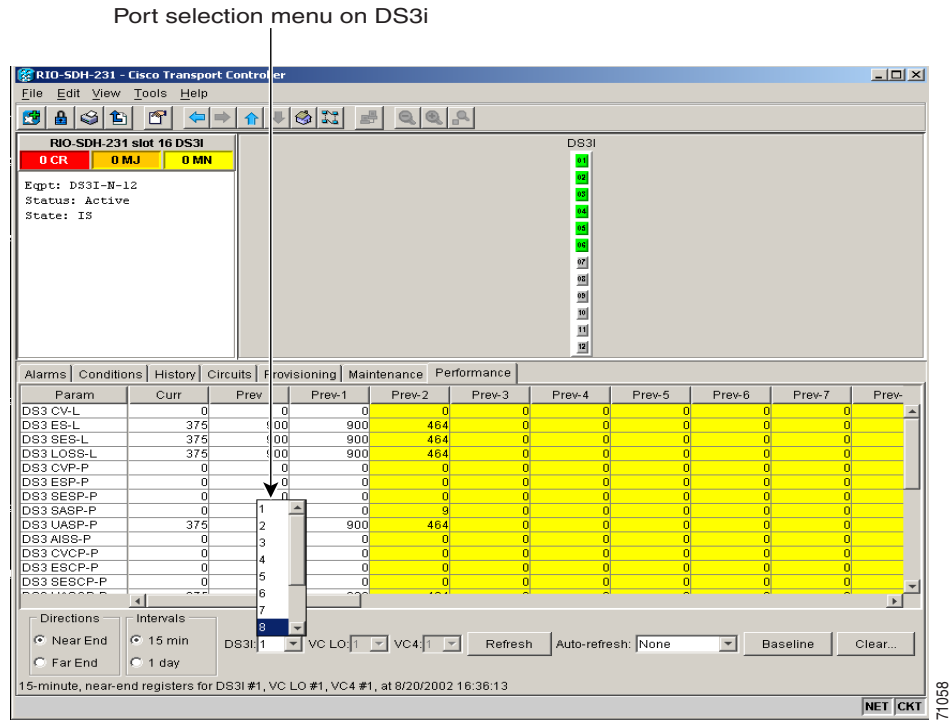
Figure 8-5   Port selection menus for an STM4-4 card

Port selection menu on STM4-4
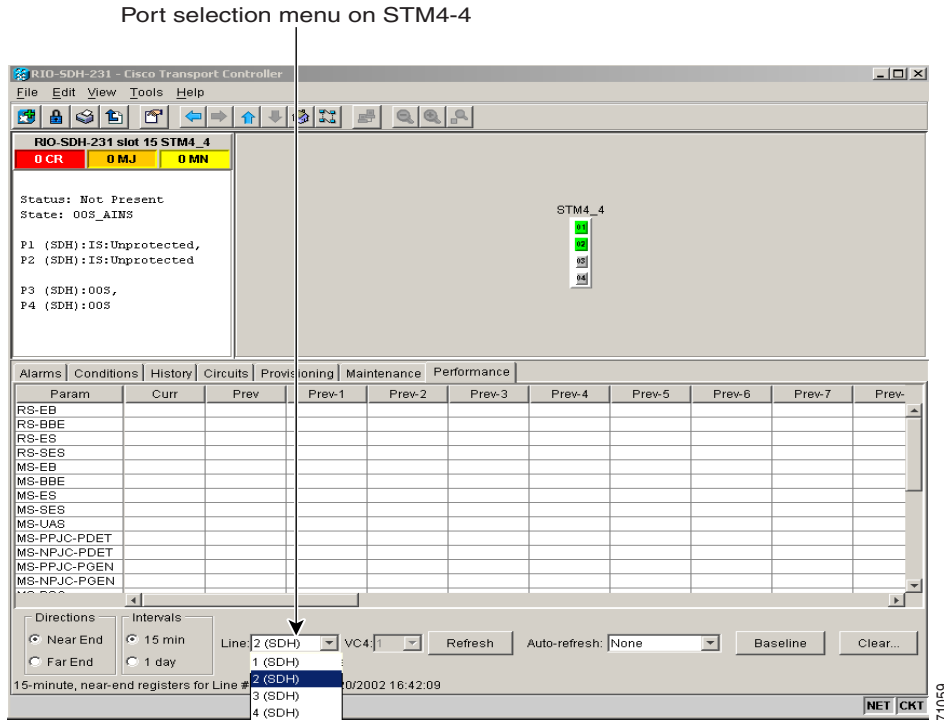
Procedure: Select Card Ports on the Performance Monitoring Window

Purpose	Use the port selection menus to monitor PMs for near-end or far-end signals on a selected port.
Prerequisite Procedures	Different port selection menus appear depending on the card type and the circuit type. The appropriate types (E1, E3, DS3i, VC4, and line) appear based on the card. For example, the STM-64 card port selection menu lists line and VC4 types.
	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

Step 2 From the card view, click the **Performance** tab.

Step 3 Click one of the port selection menus labeled in Figure 8-4 on page 8-7 and Figure 8-5 on page 8-8. Depending on the card, other options may be available (i.e., E1, E3, DS3i, VC4, and line).

Step 4   Click the **Refresh** button. For PM definitions, see the "SDH Performance Monitoring for Electrical Cards" section on page 8-18, and the "SDH Performance Monitoring for Optical Cards" section on page 8-29.

8.1.5 Using the Baseline Button

In SDH Software R3.4 and earlier, the Baseline button located on the far right of the window 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 window view changes, the total number of PM counts on the card and on the window appear in the appropriate cell.

The baseline values are discarded if you select a new port, interval, near-end, far-end, VC4, or change the view to a different window and then return to the Performance Monitoring window. The Baseline button enables you to easily see how quickly PM counts are rising without having to perform calculations. Figure 8-6 shows the Baseline button on the Performance Monitoring window.

Figure 8-6   Baseline button for clearing displayed PM counts

Procedure: Use the Baseline Button on the Performance Monitoring Window

Purpose	The Baseline button clears the PM count displayed on 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 window view changes, the total number of PM counts on the card and on the window appear in the appropriate column. The baseline values are discarded if you change the view to a different window and then return to the Performance Monitoring window.
Prerequisite Procedures	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

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 window clears certain PM counts depending on the option selected. Figure 8-7 shows the Clear button on the Performance Monitoring window.

⚠
Caution   Clicking the Clear button can potentially mask problems if used incorrectly. This button is commonly used for testing purposes such as clearing a count that results in the unavailable seconds (UAS) count incrementing.

Figure 8-7   Clear button for clearing PM counts

Procedure: Clearing PM Counts on the Performance Monitoring Window

Purpose	Use the Clear button to clear certain PM counts depending on the option selected.
Prerequisite Procedures	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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

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 only highlights the card.)

Step 2   From the card view, click the **Performance** tab.

Step 3   Click the **Clear** button.

Step 4   From the Clear Statistics dialog box, 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 radio 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 window display.

- **All interfaces on port x**: Clearing all interfaces on port x erases from the card and the window 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, as well as the 24-hour near-end and far-end counts are cleared from both the card and the window display.

- **All interfaces on card**: Clearing all interfaces on the card erases from the card and the window display all PM counts for data and ports on all interfaces.

Step 5   From the Zero Data dialog box, 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 PMs. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a 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.

Card thresholds can be set up before cards are installed. For more information, see the "Setting Network Element Defaults" section on page 3-30. You can program PM threshold ranges on cards individually from the Provisioning > Threshold tabs on the card view. For procedures on provisioning card thresholds, such as line and path, see Chapter 7, "Card Provisioning." Figure 8-8 shows the Provisioning > Threshold tabs for an STM-64 card. Figure 8-9 on page 8-13 shows the Provisioning > Threshold tabs for a DS3i card.

Figure 8-8   Threshold tab for setting threshold values (Example of an STM64 card)

Figure 8-9   Threshold tab for setting threshold values (Example of a DS3i card)
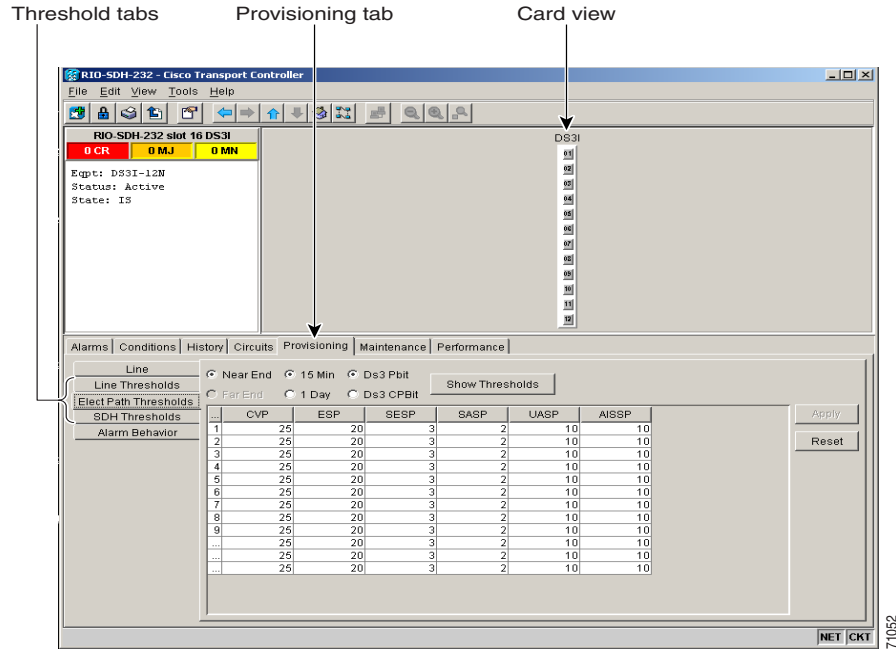
Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical DS3i installed for emergency phone calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

Note   A TCA is not reported if 0 or a number exceeding the threshold range is entered as the threshold value.

Note   Under the Provisioning > Threshold tab, the E1 card has user-defined thresholds for the E1 receive (Rx) path PMs. In the Threshold tab they are displayed as EB, BBE, ES, SES, and UAS without the Rx prefix. No threshold settings are associated with the E1 transmit (Tx) path PMs. Displayed in the Performance tab are the PM counts received for the E1 Rx path PMs. The displayed E1 Tx path PM values are based on calculations performed by the card and therefore have no TCAs that require provisioning.

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 SDH networks only use line-terminating equipment (LTE), not path-terminating equipment (PTE). After enabling IPPM provisioning on the line card, service providers can monitor high-order paths that are configured in pass-through mode on an ONS 15454 SDH operating in SDH AU4 mode, thus making troubleshooting and maintenance activities more efficient.

SDH Software R3.4 allows LTE cards to monitor near-end PM data on individual high-order paths by enabling IPPM. IPPM occurs only on high-order paths which have IPPM enabled, and TCAs are raised only for PM parameters on the selected IPPM paths.

Note The E1 and STM-1 cards can monitor far-end IPPM.

The ONS 15454 SDH 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.

Procedure: Enable Intermediate Path Performance Monitoring

Purpose	Enable IPPM to monitor high-order paths that are configured in pass-through mode on an ONS 15454 SDH operating in SDH AU4 mode.
Prerequisite Procedures	If no VC4 circuit exists, perform VC4 Circuit Creation. For information about circuit creation, see Chapter 6, "Circuits and Tunnels."
	The circuit must pass through an STM-N card before you can enable IPPM on the circuit.
Onsite/Remote	Onsite or remote

Step 1 Open the LTE 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 only highlights the card.) See the list of Cisco ONS 15454 SDH LTE cards below.

Line-Terminating Equipment

OC3 IR 4/STM1 SH 1310	OC12 IR/STM4 SH 1310
OC12 LR/STM4 LH 1310	OC12 LR/STM4 LH 1550
OC12-4 IR/STM4-4	OC48 IR/STM16 SH AS 1310
OC48 LR/STM16 LH AS 1550	OC48 ELR/STM16 EH 100 GHz
OC192 LR/STM64 LH 1550	E1

Step 2   Select the **Provisioning > VC4** tabs (Figure 8-10).

Figure 8-10   VC4 tab for enabling IPPM
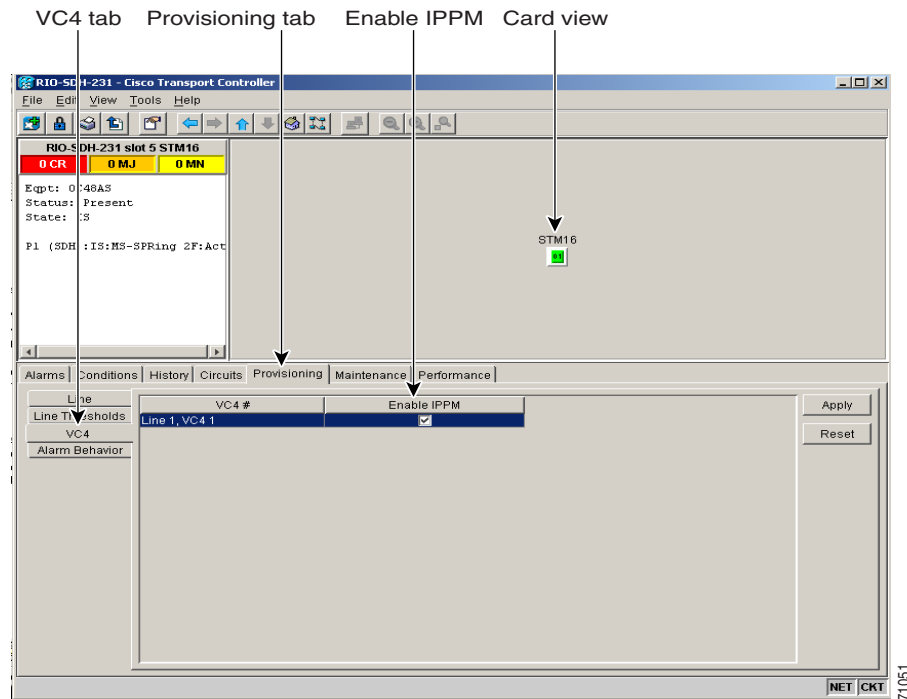
Step 3   Click **Enable IPPM** for the VC4 you want to monitor.

Step 4   Click **Apply**.

8.4 Enabling Pointer Justification Count Parameters

Pointers provide a way to align the phase variations in VC4 payloads. Pointer justification counts indicate frequency adjustments on SDH networks. The VC4 payload pointer is located in the H1 and H2 bytes of the AU pointers section and is a count of the number of bytes the VC4 POH J1 byte is away from the H3 byte, not including the section overhead bytes.

When a network is out of synch, jitter and wander occur on the transported signal. Excessive wander can cause terminating equipment to slip. It also causes slips at the SDH and plesiochronous digital hierarchy (PDH) boundaries. Slips cause different effects in service: voice service has intermittent audible clicks; compressed voice technology has short transmission errors or dropped calls; fax machines lose scanned lines or experience dropped calls; digital video transmission has distorted pictures or frozen frames; encryption service loses the encryption key causing data to be transmitted again.

Figure 8-11 shows pointer justification count parameters on the Performance Monitoring window. You can enable positive pointer justification count (PPJC) and negative pointer justification count (NPJC) performance monitoring parameters for LTE cards. See the "Enable Intermediate Path Performance Monitoring" procedure on page 8-14 for a list of Cisco ONS 15454 SDH LTE cards.

Figure 8-11   Viewing pointer justification count parameters

To avoid problems with data when timing differences exist, dummy bytes can be inserted into the VC4. There are negative (NPJC) and positive (PPJC) pointer justification count parameters. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications. H3 bytes are called negative justification bytes and carry extra payload data for one frame during a pointer decrease.

PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications. The three bytes following the last H3 byte in the VC4 are called positive justification bytes and carry three dummy bytes of information for one frame during a pointer increment.

A consistently large pointer justification count indicates clock synchronization problems between nodes. A difference between the counts means the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count.

For pointer justification count definitions, depending on the cards in use, see the "E1 Card Performance Monitoring Parameters" section on page 8-18, the "STM-1 Card Performance Monitoring Parameters" section on page 8-29, the "STM-4 and STM4-4 Card Performance Monitoring Parameters" section on page 8-32, or the "STM-16 and STM-64 Card Performance Monitoring Parameters" section on page 8-37.

In CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. Figure 8-12 shows the PJVC4Mon# menu on the Provisioning window.

Figure 8-12   Line tab for enabling pointer justification count parameters
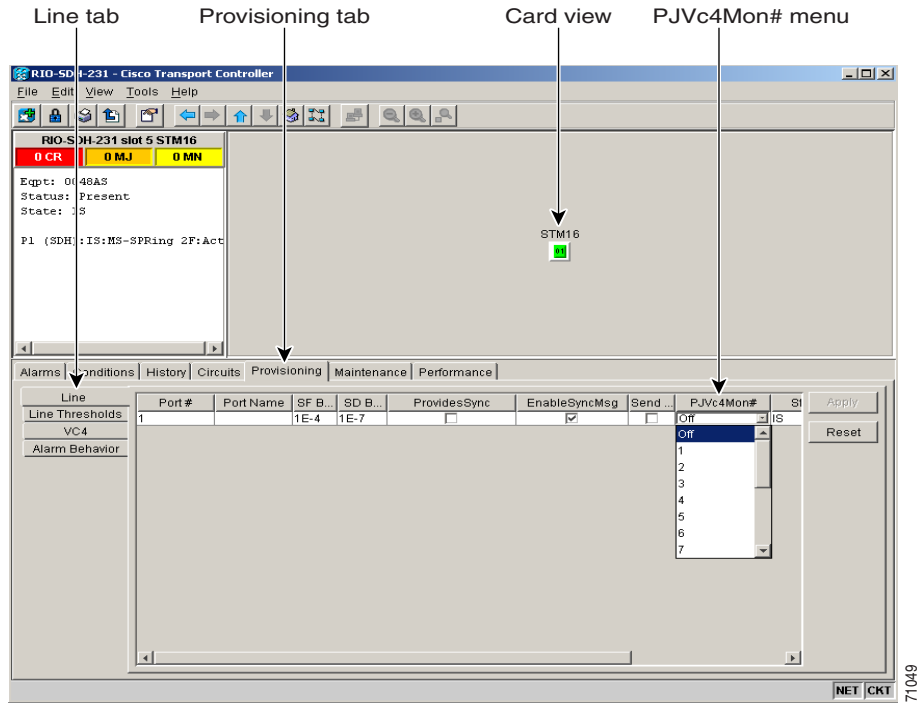
Procedure: Enable Pointer Justification Count Performance Monitoring

Purpose	Enable pointer justification counts to monitor the clock synchronization between nodes.
Prerequisite Procedures	Before you view pointer justification 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 Chapter 6, "Circuits and Tunnels" and Chapter 7, "Card Provisioning."
Onsite/Remote	Onsite or remote

Step 1   Open the LTE 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 only highlights the card.) See the list of Cisco ONS 15454 SDH LTE cards below.

Line-Terminating Equipment

OC3 IR 4/STM1 SH 1310   OC12 IR/STM4 SH 1310

OC12 LR/STM4 LH 1310   OC12 LR/STM4 LH 1550

OC12-4 IR/STM4-4   OC48 IR/STM16 SH AS 1310

Line-Terminating Equipment

OC48 LR/STM16 LH AS 1550   OC48 ELR/STM16 EH 100 GHz

OC192 LR/STM64 LH 1550

Step 2   From the card view, click the **Provisioning > Line** tabs.

Step 3   Click the **PJVC4Mon#** menu and select a number.

- Select **off** to disable pointer justification monitoring.
- The values 1 to N are the VC4 numbers on one port. One VC4 per port can be enabled from the **PJVC4Mon#** card menu, as follows:
  - STM-1 PJVC4Mon# card menu: **off** or **1** can be selected on a total of 4 ports.
  - STM-4 PJVC4Mon# card menu: **off**, **1**, or any number through 4 can be selected on 1 port.
  - STM4-4 PJVC4Mon# card menu: **off**, or 1 through 4 can be selected on a total of 4 ports.
  - STM-16 PJVC4Mon# card menu: **off**, **1**, or any number through 16 can be selected on 1 port.
  - STM-64 PJVC4Mon# card menu: **off**, **1**, or any number through 64 can be selected on 1 port.

Step 4   Click **Apply** and return to the **Performance** tab to view PM parameters.


8.5 SDH Performance Monitoring for Electrical Cards

The following sections define performance monitoring parameters for the E1, E3, and DS3i electrical cards.

8.5.1 E1 Card Performance Monitoring Parameters

Figure 8-13 on page 8-19 shows the signal types that support near-end and far-end PMs for the E1 card. Figure 8-14 on page 8-19 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the E1 card.

Figure 8-13   Monitored signal types for the E1 card
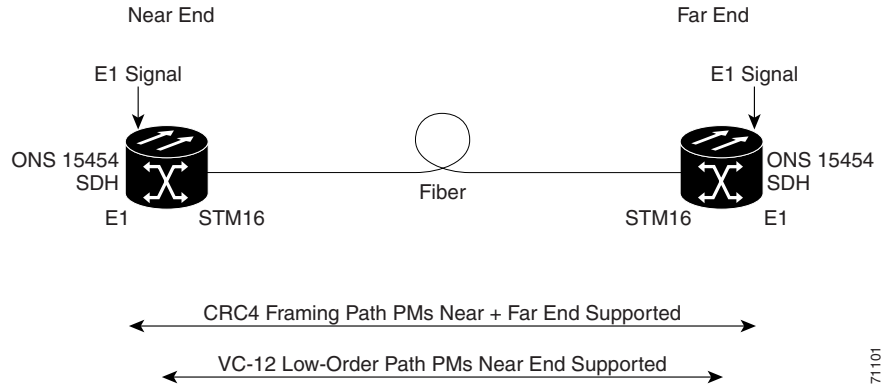
Figure 8-14   PM read points on the E1 card
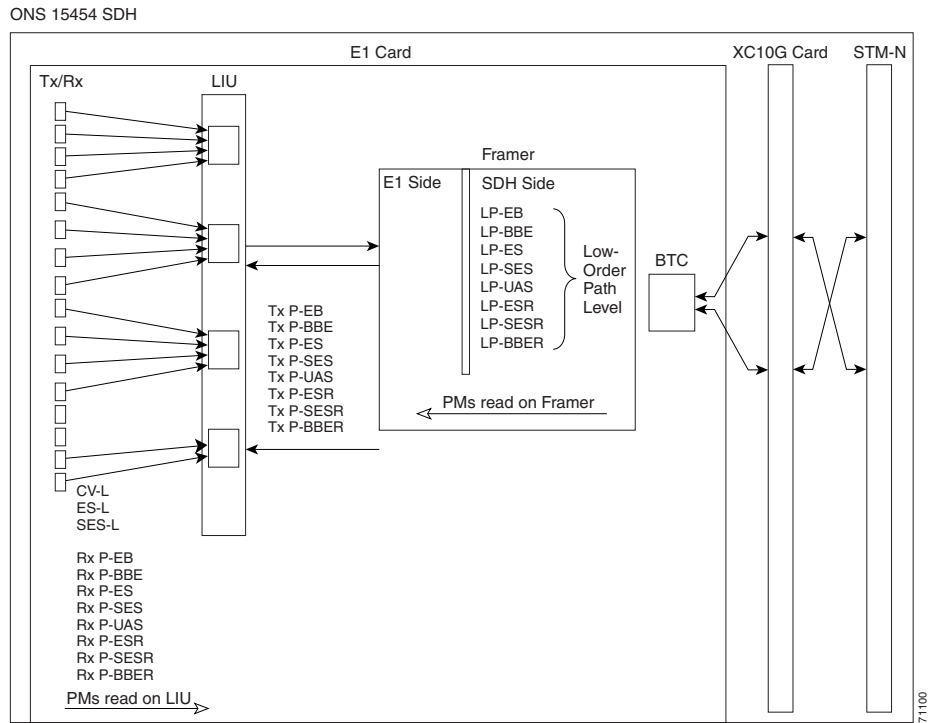
The PM parameters for the E1 card are described in Table 8-3 on page 8-20, Table 8-4 on page 8-20, and Table 8-5 on page 8-21.

Table 8-3   Line PMs for the E1 Card, Near-end

Parameter	Definition
E1 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.
E1 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.
E1 SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 2048) and/or defects on the line.

Note   Under the Provisioning>Threshold tab, the E1 card has user-defined thresholds for the E1 Rx path PMs. In the Threshold tab, they are displayed as EB, BBE, ES, SES, and UAS without the Rx prefix.

Table 8-4   CEPT and CRC4 Framing Path PMs, both Tx and Rx for the E1 Card, Near-end and Far-End

Parameter	Definition
E1 (Tx or Rx) P-EB	Path Errored Block (P-EB) indicates that one or more bits are in error within a block.
E1 (Tx or Rx) P-BBE	Path Background Block Error (P-BBE) is an errored block not occurring as part of an SES.
E1 (Tx or Rx) P-ES	Path Errored Second (P-ES) is a one-second period with one or more errored blocks or at least one defect.
E1 (Tx or Rx) P-SES	Path Severely Errored Seconds (P-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
E1 (Tx or Rx) P-UAS	Receive Path Unavailable Seconds (E1 Rx P-UAS) is a count of one-second intervals when the E1 path is unavailable on the receive end of the signal. The E1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. Once unavailable, the E1 path becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time. Transmit Path Unavailable Seconds (E1 Tx P-UAS) is a count of one-second intervals when the E1 path is unavailable on the transmit end of the signal. The E1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. Once unavailable, the E1 path becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time.
E1 (Tx or Rx) P-ESR	Path Errored Second Ratio (P-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.

Table 8-4   *CEPT and CRC4 Framing Path PMs, both Tx and Rx for the E1 Card, Near-end and Far-End*

Parameter	Definition
E1 (Tx or Rx) P-SESR	Path Severely Errored Second Ratio (P-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
E1 (Tx or Rx) P-BBER	Path Background Block Error Ratio (P-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

Table 8-5   *VC-12 Low-Order Path PMs for the E1 Card, Near-end and Far-end*

Parameter	Definition
LP-EB	Low-Order Path Errored Block (LP-EB) indicates that one or more bits are in error within a block.
LP-BBE	Low-Order Path Background Block Error (LP-BBE) is an errored block not occurring as part of an SES.
LP-ES	Low-Order Path Errored Second (LP-ES) is a one-second period with one or more errored blocks or at least one defect.
LP-SES	Low-Order Path Severely Errored Seconds (LP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
LP-UAS	Low-Order Path Unavailable Seconds (LP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as LP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as LP-SESs.
LP-ESR	Low-Order Path Errored Second Ratio (LP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
LP-SESR	Low-Order Path Severely Errored Second Ratio (LP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
LP-BBER	Low-Order Path Background Block Error Ratio (LP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

8.5.2 E3 Card Performance Monitoring Parameters

Figure 8-15 shows the signal types that support near-end and far-end PMs for the E3 card. Figure 8-16 on page 8-22 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the E3 card.

Figure 8-15   Monitored signal types for the E3 card
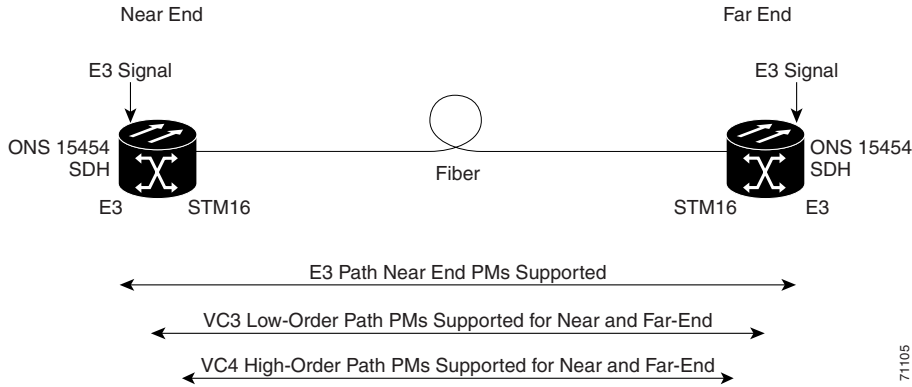
Figure 8-16   PM read points on the E3 card
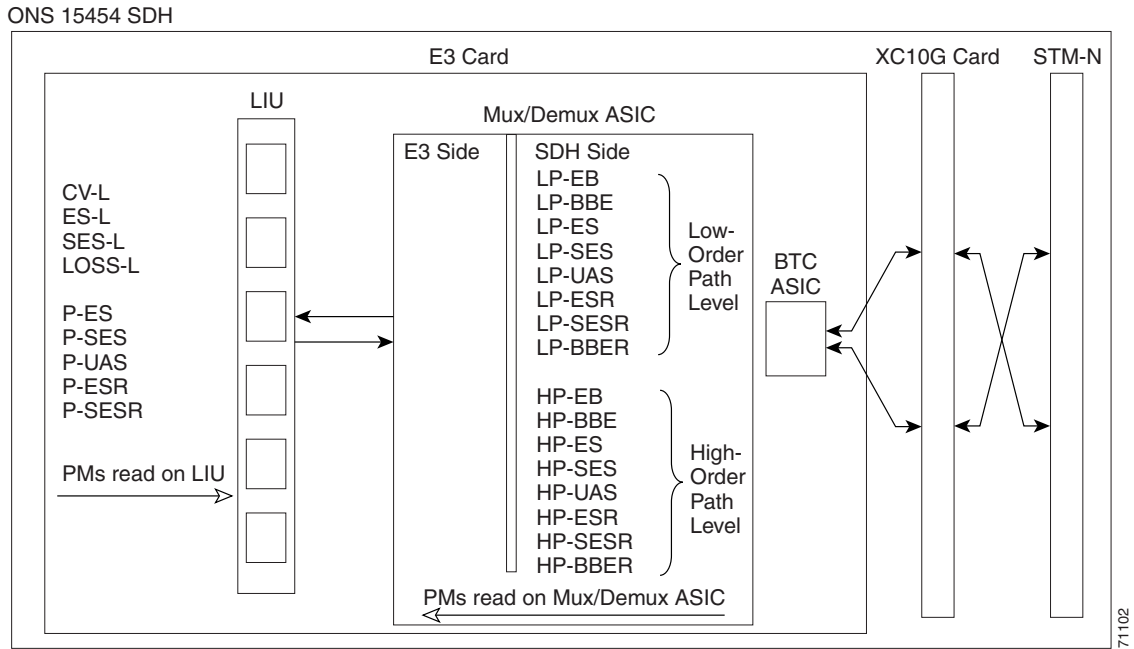
The PM parameters for the E3 card are described in Table 8-6, Table 8-7, Table 8-8, and Table 8-9.

Table 8-6   E3 Line PMs for the E3 Card, Near-End

Parameter	Definition
E3 CV-L	Code Violation Line (CV-L) indicates that the number of coding violations occurring on the line. This parameter is a count of BPVs and EXZs occurring over the accumulation period.
E3 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.

Table 8-6   E3 Line PMs for the E3 Card, Near-End (continued)

Parameter	Definition
E3 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.
E3 LOSS-L	Line Loss of Signal (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Table 8-7   E3 Path PMs for the E3 Card, Near-End

Parameter	Definition
E3 P-ES	Path Errored Second (P-ES) is a one-second period with at least one defect.
E3 P-SES	Path Severely Errored Seconds (P-SES) is a one-second period containing at least one defect. SES is a subset of ES.
E3 P-UAS	Path Unavailable Seconds (P-UAS) is a count of the seconds when the path was unavailable. A path becomes unavailable when ten consecutive seconds occur that qualify as P-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as P-SESs.
E3 P-ESR	Path Errored Second Ratio (P-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
E3 P-SESR	Path Severely Errored Second Ratio (P-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.

Table 8-8   VC3 Low-Order Path PMs for the E3 Card, Near-End and Far-End

Parameter	Definition
LP-EB	Low-Order Path Errored Block (LP-EB) indicates that one or more bits are in error within a block.
LP-BBE	Low-Order Path Background Block Error (LP-BBE) is an errored block not occurring as part of an SES.
LP-ES	Low-Order Path Errored Second (LP-ES) is a one-second period with one or more errored blocks or at least one defect.
LP-SES	Low-Order Path Severely Errored Seconds (LP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
LP-UAS	Low-Order Path Unavailable Seconds (LP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as LP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as LP-SESs.
LP-ESR	Low-Order Path Errored Second Ratio (LP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.

Table 8-8   VC3 Low-Order Path PMs for the E3 Card, Near-End and Far-End (continued)

Parameter	Definition
LP-SESR	Low-Order Path Severely Errored Second Ratio (LP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
LP-BBER	Low-Order Path Background Block Error Ratio (LP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

Table 8-9   VC4 High-Order Path PMs for the E3 Card, Near-End and Far-End

Parameter	Definition
HP-EB	High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block.
HP-BBE	High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES.
HP-ES	High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect.
HP-SES	High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
HP-UAS	High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
HP-ESR	High-Order Path Errored Second Ratio (HP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
HP-SESR	High-Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
HP-BBER	High-Order Path Background Block Error Ratio (HP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

8.5.3 DS3i Card Performance Monitoring Parameters

Figure 8-17 shows the signal types that support near-end and far-end PMs for the DS3i card. Figure 8-18 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3i card.

Figure 8-17   Monitored signal types for the DS3i card
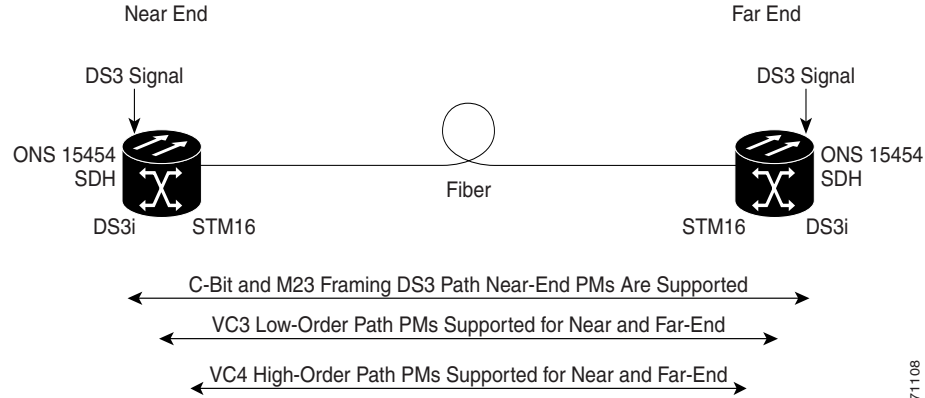
Figure 8-18   PM read points on the DS3i card
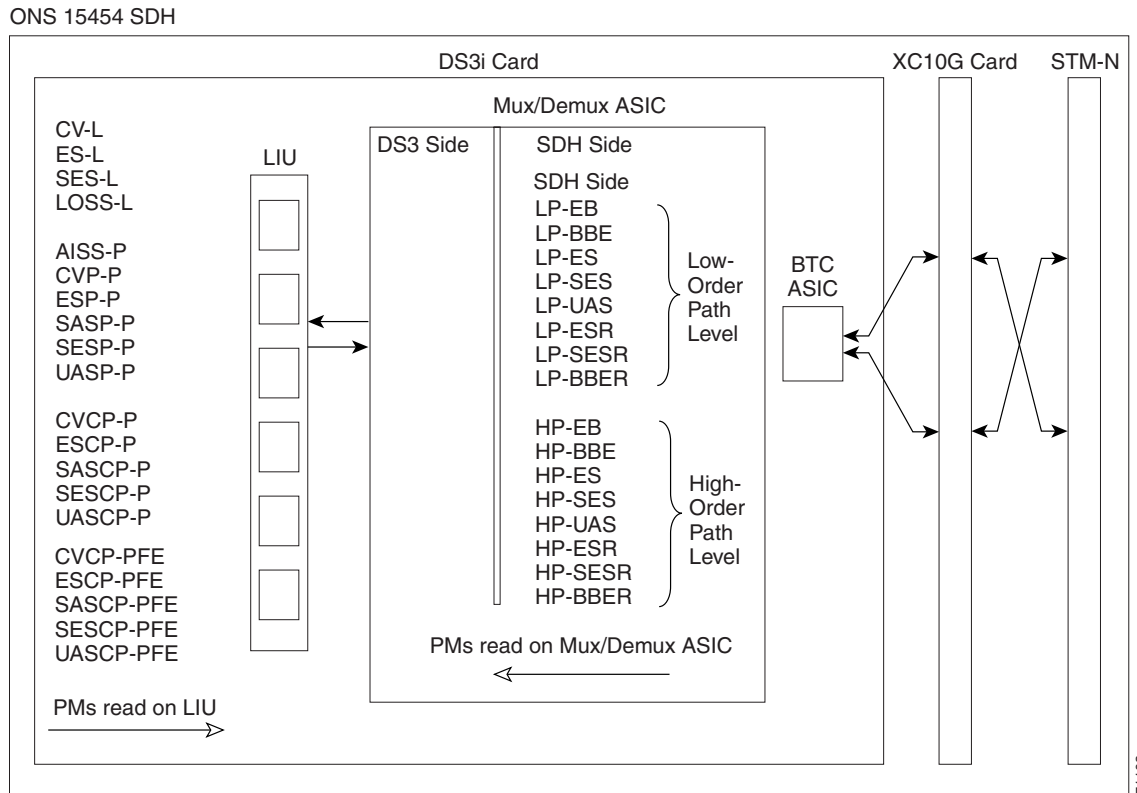
The PM parameters for the DS3i card are described in Table 8-10, Table 8-11, Table 8-12, Table 8-13, Table 8-14, and Table 8-15.

Table 8-10   DS3 Line PMs for the DS3i Card, Near-End

Parameter	Definition
DS3 CV-L	Code Violation Line (CV-L) indicates that the number of coding violations occurring on the line. This parameter is a count of BPVs and 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 8-11   C-Bit and M23 Framing DS3 Path PMs for the DS3i Card, Near-End

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 8-12   CP-Bit Framing DS3 Path PMs for the DS3i Card, Near-End

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 8-12   CP-Bit Framing DS3 Path PMs for the DS3i Card, Near-End (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 8-13   CP-Bit Path PMs for the DS3i Cards, Far-End

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.

Table 8-14   VC3 Low-Order Path PMs for the DS3i Card, Near-End and Far-End

Parameter	Definition
LP-EB	Low-Order Path Errored Block (LP-EB) indicates that one or more bits are in error within a block.
LP-BBE	Low-Order Path Background Block Error (LP-BBE) is an errored block not occurring as part of an SES.
LP-ES	Low-Order Path Errored Second (LP-ES) is a one-second period with one or more errored blocks or at least one defect.
LP-SES	Low-Order Path Severely Errored Seconds (LP-SES) is a one-second period containing $\geq 30\%$ errored blocks or at least one defect. SES is a subset of ES.

Table 8-14   VC3 Low-Order Path PMs for the DS3i Card, Near-End and Far-End (continued)

Parameter	Definition
LP-UAS	Low-Order Path Unavailable Seconds (LP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as LP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as LP-SESs.
LP-ESR	Low-Order Path Errored Second Ratio (LP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
LP-SESR	Low-Order Path Severely Errored Second Ratio (LP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
LP-BBER	Low-Order Path Background Block Error Ratio (LP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

Table 8-15   VC4 High-Order Path PMs for the DS3i Card, Near-End and Far-End

Parameter	Definition
HP-EB	High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block.
HP-BBE	High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES.
HP-ES	High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect.
HP-SES	High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
HP-UAS	High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
HP-ESR	High-Order Path Errored Second Ratio (HP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
HP-SESR	High-Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
HP-BBER	High-Order Path Background Block Error Ratio (HP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

8.6 SDH Performance Monitoring for Optical Cards

The following sections define performance monitoring parameters and definitions for the STM-1, STM-4, STM-16, and STM-64 cards.

8.6.1 STM-1 Card Performance Monitoring Parameters

Figure 8-19 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the STM-1 card.

Figure 8-19   PM read points on the STM-1 card
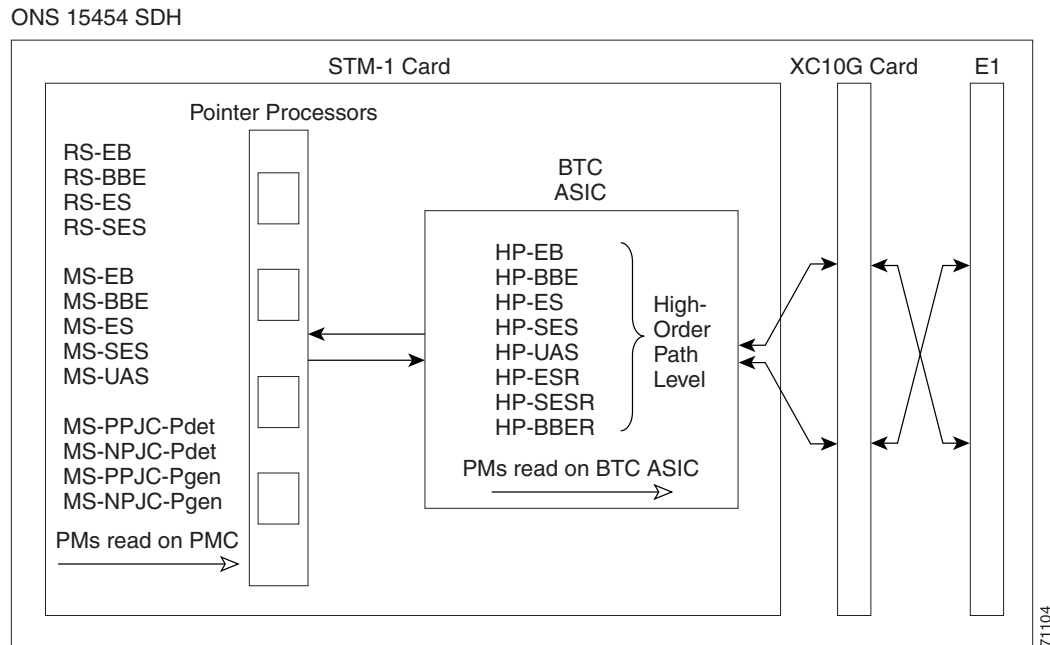
Note   For PM locations relating to protection switch counts, see the Telcordia GR-253-CORE document.

The PM parameters for the STM-1 card are described in Table 8-16, Table 8-17, Table 8-18, Table 8-19, and Table 8-20.

Table 8-16   Regenerator Section PMs for the STM-1 Card, Near-End

Parameter	Definition
RS-EB	Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block.
RS-BBE	Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES.

Table 8-16   Regenerator Section PMs for the STM-1 Card, Near-End (continued)

Parameter	Definition
RS-ES	Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect.
RS-SES	Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains ≥30% errored blocks or at least one defect. SES is a subset of ES.

Table 8-17   Multiplex Section PMs for the STM-1 Card, Near-End and Far-End

Parameter	Definition
MS-EB	Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block.
MS-BBE	Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES.
MS-ES	Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect.
MS-SES	Multiplex Section Severely Errored Second (MS-SES) is a one-second period which contains ≥X% errored blocks or at least one defect. SES is a subset of ES. For more information, see ITU-T G.829 Section 5.1.3.
MS-UAS	Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS.

Note   For information about Troubleshooting SNCP switch counts, see the alarm troubleshooting information in the *Cisco ONS 15454 SDH Troubleshooting and Reference Guide*. For information about creating circuits that perform a switch, see Chapter 6, "Circuits and Tunnels."

Table 8-18   1+1 LMSP Protection Switch Count PMs for the STM-1 Cards, Near-End

Parameter	Definition
MS-PSC (1+1 protection)	In a 1+1 protection scheme for a working card, Multiplex Section Protection Switching Count (MS-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, MS-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 MS-PSC PM is only applicable if revertive line-level protection switching is used. **Note** MS-SPRing is not supported on the STM-1 card; therefore, the MS-PSD-W, MS-PSD-S, and MS-PSD-R PMs do not increment.
MS-PSD	Multiplex Section Protection Switching Duration (MS-PSD) applies to the length of time, in seconds, that service is carried on another line. For a working line, MS-PSD is a count of the number of seconds that service was carried on the protection line. For the protection line, MS-PSD is a count of the seconds that the line was used to carry service. The MS-PSD PM is only applicable if revertive line-level protection switching is used. **Note** MS-SPRing is not supported on the STM-1 card; therefore, the MS-PSD-W, MS-PSD-S, and MS-PSD-R PMs do not increment.

Note   In CTC, the count fields for MS-PPJC and MS-NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. See the "Enable Pointer Justification Count Performance Monitoring" procedure on page 8-17.

Table 8-19   Pointer Justification Count PMs for the STM-1 Card, Near-End

Parameter	Definition
MS-PPJC-Pdet	Multiplex Section, Positive Pointer Justification Count, Path Detected (MS-PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SDH signal.
MS-NPJC-Pdet	Multiplex Section, Negative Pointer Justification Count, Path Detected (MS-NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SDH signal.
MS-PPJC-Pgen	Multiplex Section, Positive Pointer Justification Count, Path Generated (MS-PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path.
MS-NPJC-Pgen	Multiplex Section, Negative Pointer Justification Count, Path Generated (MS-NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path.

Note SDH path PMs will not count unless IPPM is enabled. For additional information, see the "Enabling Intermediate Path Performance Monitoring" section on page 8-14.

Table 8-20   High-Order VC4 and VC4-Xc Path PMs for the STM-1 Card, Near-End and Far-End

Parameter	Definition
HP-EB	High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block.
HP-BBE	High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES.
HP-ES	High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect.
HP-SES	High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
HP-UAS	High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
HP-ESR	High-Order Path Errored Second Ratio (HP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
HP-SESR	High-Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
HP-BBER	High-Order Path Background Block Error Ratio (HP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

8.6.2 STM-4 and STM4-4 Card Performance Monitoring Parameters

Figure 8-20 shows the signal types that support near-end and far-end PMs for the STM-4 and STM4-4 cards. Figure 8-21 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the STM-4 and STM4-4 cards.

Figure 8-20   Monitored signal types for the STM-4 and STM4-4 cards
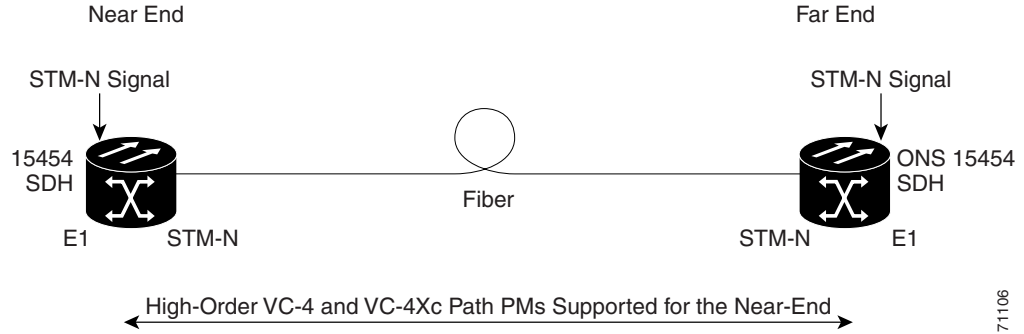
Note   PMs on the protect VC4 are not supported for MS-SPRing.

Figure 8-21   PM read points on the STM-4 and STM4-4 cards
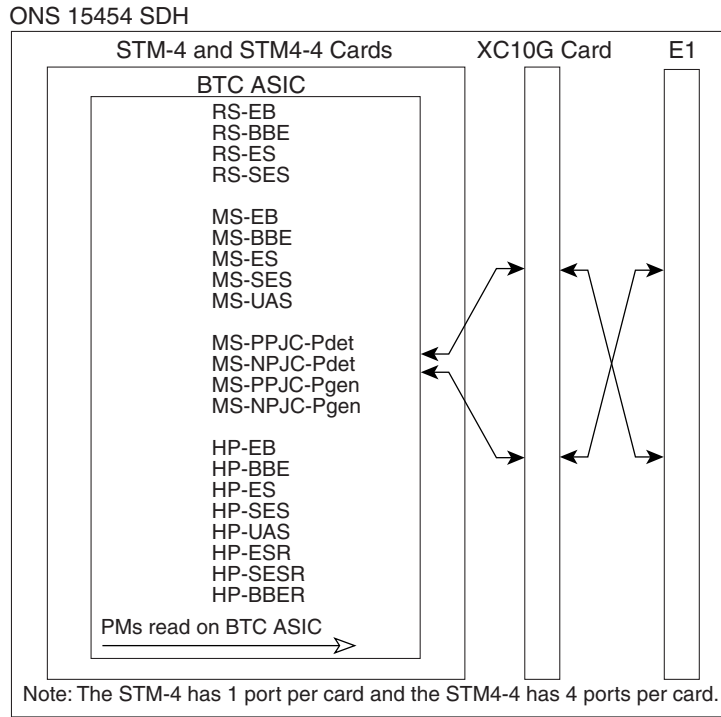
Note   For PM locations relating to protection switch counts, see the Telcordia GR-1230-CORE document.

The PM parameters for the STM-4 and STM4-4 cards are described in Table 8-21, Table 8-22, Table 8-23, Table 8-24, and Table 8-25.

Table 8-21   Regenerator Section PMs for the STM-4 and STM4-4 Cards, Near-End and Far-End

Parameter	Definition
RS-EB	Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block.
RS-BBE	Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES.
RS-ES	Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect.
RS-SES	Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains ≥30% errored blocks or at least one defect. SES is a subset of ES.

Table 8-22   Multiplex Section PMs for the STM-4 and STM4-4 Cards, Near-End and Far-End

Parameter	Definition
MS-EB	Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block.
MS-BBE	Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES.
MS-ES	Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect.
MS-SES	Multiplex Section Severely Errored Second (MS-SES) is a one-second period which contains ≥X% errored blocks or at least one defect. SES is a subset of ES. For more information, see ITU-T G.829 Section 5.1.3.
MS-UAS	Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS.

Table 8-23   Pointer Justification Count PMs for the STM-4 and STM4-4 Cards, Near-End

Parameter	Definition
Note	In CTC, the count fields for MS-PPJC and MS-NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. For procedures, see the "Enable Pointer Justification Count Performance Monitoring" procedure on page 8-17.
MS-PPJC-Pdet	Multiplex Section Positive Pointer Justification Count, Path Detected (MS-PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SDH signal.
MS-NPJC-Pdet	Multiplex Section Negative Pointer Justification Count, Path Detected (MS-NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SDH signal.

Table 8-23   Pointer Justification Count PMs for the STM-4 and STM4-4 Cards, Near-End (continued)

Parameter	Definition
MS-PPJC-Pgen	Multiplex Section Positive Pointer Justification Count, Path Generated (MS-PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path.
MS-NPJC-Pgen	Multiplex Section Negative Pointer Justification Count, Path Generated (MS-NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path.

Table 8-24   Protection Switch Count PMs for the STM-4 and STM4-4 Cards, Near-End

Parameter	Definition
Note	For information about Troubleshooting SNCP switch counts, see the alarm troubleshooting information in the *Cisco ONS 15454 SDH Troubleshooting and Reference Guide*. For information about creating circuits that perform a switch, see Chapter 6, "Circuits and Tunnels."
MS-PSC (MS-SPRing)	For a protect line in a 2-fiber ring, Multiplex Section Protection Switching Count (MS-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 MS-SPRing, the MS-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 MS-PSC of the protect span will increment again. **Note** 4-fiber MS-SPRing is not supported on the STM-4 and STM4-4 cards; therefore, the MS-PSC-S, and MS-PSC-R PMs do not increment.
MS-PSC (1+1 protection)	In a 1+1 protection scheme for a working card, Multiplex Section Protection Switching Count (MS-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, MS-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 MS-PSC PM is only applicable if revertive line-level protection switching is used.
MS-PSD	For an active protection line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Duration (MS-PSD) is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. MS-PSD increments on the active protect line and MS-PSD-W increments on the failed working line. **Note** 4-fiber MS-SPRing is not supported on the STM-4 and STM4-4 cards; therefore, the MS-PSD-S, and MS-PSD-R PMs do not increment.

Table 8-24   Protection Switch Count PMs for the STM-4 and STM4-4 Cards, Near-End (continued)

Parameter	Definition
MS-PSC-W	For a working line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Count-Working (MS-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.
MS-PSD-W	For a working line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Working (MS-PSD-W) is a count of the number of seconds that service was carried on the protection line. MS-PSD-W increments on the failed working line and PSD increments on the active protect line.

Table 8-25   High-Order VC4 and VC4-Xc Path PMs for the STM-4 and STM4-4 Cards, Near-End

Parameter	Definition
Note	SDH path PMs will not count unless IPPM is enabled. For additional information, see the "Enabling Intermediate Path Performance Monitoring" section on page 8-14. The far-end IPPM feature is not supported on the STM-4 and STM4-4 cards. However, SDH path PMs can be monitored by logging into the far-end node directly.
HP-EB	High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block.
HP-BBE	High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES.
HP-ES	High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect.
HP-SES	High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
HP-UAS	High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
HP-ESR	High-Order Path Errored Second Ratio (HP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
HP-SESR	High-Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
HP-BBER	High-Order Path Background Block Error Ratio (HP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

8.6.3 STM-16 and STM-64 Card Performance Monitoring Parameters

Figure 8-22 shows the signal types that support near-end and far-end PMs for the STM-16 and STM-64 cards. Figure 8-23 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the STM-16 and STM-64 cards.

Figure 8-22   Monitored signal types for the STM-16 and STM-64 cards
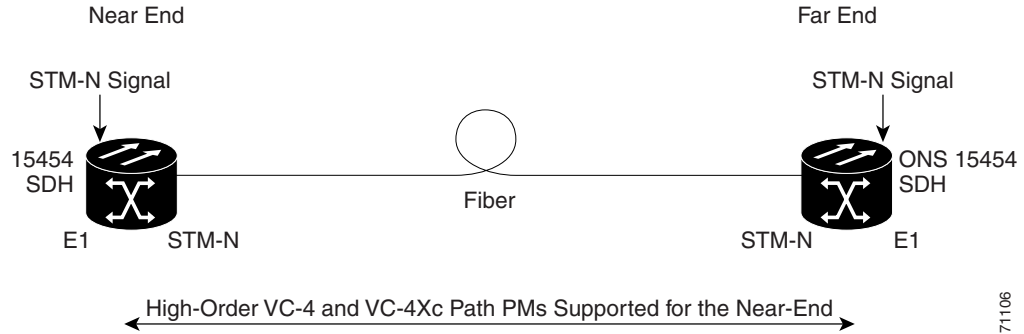
Note   PMs on the protect VC4 are not supported for MS-SPRing.

Figure 8-23   PM read points on the STM-16 and STM-64 cards
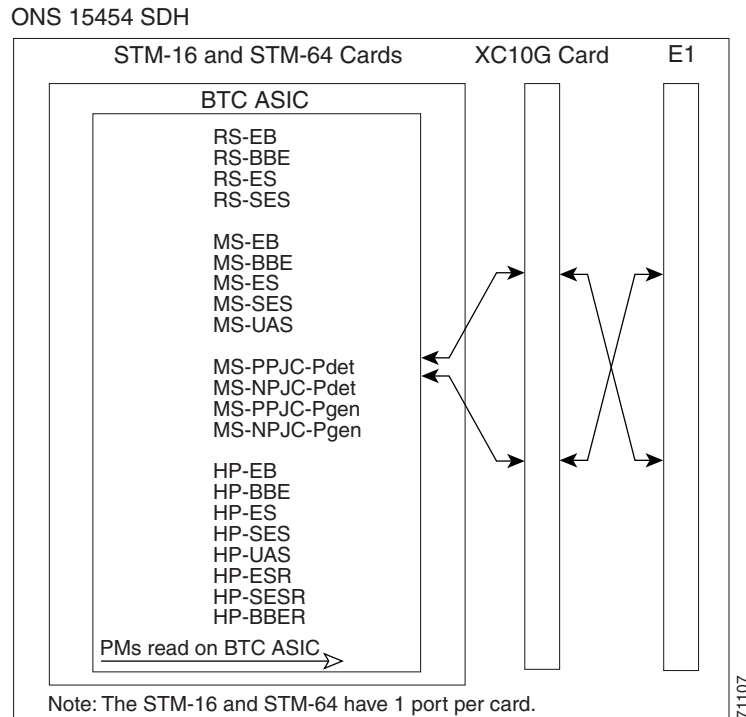
Note   For PM locations relating to protection switch counts, see the Telcordia GR-1230-CORE document.

The PM parameters for the STM-16 and STM-64 cards are described in Table 8-26, Table 8-27, Table 8-28, Table 8-29, and Table 8-30.

Table 8-26   Regenerator Section PMs for the STM-16 and STM-64 Cards, Near-End and Far-End

Parameter	Definition
RS-EB	Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block.
RS-BBE	Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES.
RS-ES	Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect.
RS-SES	Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains ≥30% errored blocks or at least one defect. SES is a subset of ES.

Table 8-27   Multiplex Section PMs for the STM-16 and STM-64 Cards, Near-End and Far-End

Parameter	Definition
MS-EB	Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block.
MS-BBE	Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES.
MS-ES	Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect.
MS-SES	Multiplex Section Severely Errored Second (MS-SES) is a one-second period which contains ≥X% errored blocks or at least one defect. SES is a subset of ES. For more information, see ITU-T G.829 Section 5.1.3.
MS-UAS	Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS.

Table 8-28   Pointer Justification Count PMs for the STM-16 and STM-64 Cards, Near-End

Parameter	Definition
Note	In CTC, the count fields for MS-PPJC and MS-NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. For procedures, see the "Enable Pointer Justification Count Performance Monitoring" procedure on page 8-17.
MS-PPJC-Pdet	Multiplex Section Positive Pointer Justification Count, Path Detected (MS-PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SDH signal.

Table 8-28   Pointer Justification Count PMs for the STM-16 and STM-64 Cards, Near-End (continued)

Parameter	Definition
MS-NPJC-Pdet	Multiplex Section Negative Pointer Justification Count, Path Detected (MS-NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SDH signal.
MS-PPJC-Pgen	Multiplex Section Positive Pointer Justification Count, Path Generated (MS-PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path.
MS-NPJC-Pgen	Multiplex Section Negative Pointer Justification Count, Path Generated (MS-NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path.

Table 8-29   Protection Switch Count PMs for the STM-16 and STM-64 Cards, Near-End

Parameter	Definition
	For information about Troubleshooting SNCP switch counts, see the alarm troubleshooting information in the *Cisco ONS 15454 SDH Troubleshooting and Reference Guide*. For information about creating circuits that perform a switch, see Chapter 6, "Circuits and Tunnels."
MS-PSC (MS-SPRing)	For a protect line in a 2-fiber ring, Multiplex Section Protection Switching Count (MS-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 MS-SPRing, the MS-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 MS-PSC of the protect span will increment again.
MS-PSC (1+1 protection)	In a 1+1 protection scheme for a working card, Multiplex Section Protection Switching Count (MS-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, MS-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 MS-PSC PM is only applicable if revertive line-level protection switching is used.
MS-PSD	For an active protection line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Duration (MS-PSD) is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. MS-PSD increments on the active protect line and MS-PSD-W increments on the failed working line.

Table 8-29   Protection Switch Count PMs for the STM-16 and STM-64 Cards, Near-End (continued)

Parameter	Definition
MS-PSC-W	For a working line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Count-Working (MS-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. MS-PSC-W increments on the failed working line and MS-PSC increments on the active protect line.
	For a working line in a 4-fiber MS-SPRing, MS-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. MS-PSC-W increments on the failed line and MS-PSC-R or MS-PSC-S increments on the active protect line.
MS-PSD-W	For a working line in a 2-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Working (MS-PSD-W) is a count of the number of seconds that service was carried on the protection line. MS-PSD-W increments on the failed working line and MS-PSD increments on the active protect line.
MS-PSC-S	In a 4-fiber MS-SPRing, Multiplex Section Protection Switching Count-Span (MS-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.
MS-PSD-S	In a 4-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Span (MS-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.
MS-PSC-R	In a 4-fiber MS-SPRing, Multiplex Section Protection Switching Count-Ring (MS-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.
MS-PSD-R	In a 4-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Ring (MS-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 8-30   High-Order VC4 and VC4-Xc Path PMs for the STM-16 and STM-64 Cards

Parameter	Definition
Note	SDH path PMs will not count unless IPPM is enabled. For additional information, see the "Enabling Intermediate Path Performance Monitoring" section on page 8-14. The far-end IPPM feature is not supported on the STM-16 and STM-64 cards. However, SDH path PMs can be monitored by logging into the far-end node directly.
HP-EB	High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block.

Table 8-30   High-Order VC4 and VC4-Xc Path PMs for the STM-16 and STM-64 Cards (continued)

Parameter	Definition
HP-BBE	High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES.
HP-ES	High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect.
HP-SES	High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing $\geq$ 30% errored blocks or at least one defect. SES is a subset of ES.
HP-UAS	High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
HP-ESR	High-Order Path Errored Second Ratio (HP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
HP-SESR	High-Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
HP-BBER	High-Order Path Background Block Error Ratio (HP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.

Ethernet Operation

The Cisco ONS 15454 SDH integrates Ethernet into an SDH time-division multiplexing (TDM) platform. The ONS 15454 SDH supports both E-series Ethernet cards and the G-series Ethernet card. This chapter describes the Ethernet capabilities of the ONS 15454 SDH. Table 9-1 lists Ethernet topics. Table 9-2 lists Ethernet procedures.

Table 9-1   Ethernet Topics

Ethernet Topics
9.1 G1000-4 Card, page 9-2
9.2 E-Series Cards, page 9-10
9.3 E-Series Multicard and Single-Card EtherSwitch, page 9-13
9.4 E-Series Circuit Configurations, page 9-15
9.5 G1000-4 Circuit Configurations, page 9-33
9.6 E-Series VLAN Support, page 9-38
9.7 E-Series Spanning Tree (IEEE 802.1D), page 9-43
9.8 G1000-4 Performance and Maintenance Windows, page 9-46
9.9 Remote Monitoring Specification Alarm Thresholds, page 9-54

Table 9-2   Ethernet Procedures

Ethernet Procedures
Procedure: Provision G1000-4 Ethernet Ports, page 9-7
Procedure: Provision E-Series Ethernet Ports, page 9-11
Procedure: Provision an E-Series EtherSwitch Circuit (Multicard or Single-Card), page 9-16
Procedure: Provision an E-Series Shared Packet Ring Circuit, page 9-19
Procedure: Provision an E-Series Hub-and-Spoke Ethernet Circuit, page 9-23
Procedure: Provision an E-Series Single-Card EtherSwitch Manual Cross-Connect, page 9-28
Procedure: Provision an E-Series Multicard EtherSwitch Manual Cross-Connect, page 9-30
Procedure: Provision a G1000-4 EtherSwitch Circuit, page 9-34
Procedure: Provision a G1000-4 Manual Cross-Connect, page 9-36
Procedure: Provision Ethernet Ports for VLAN Membership, page 9-41

Table 9-2   Ethernet Procedures (continued)

Ethernet Procedures
Procedure: Display Available VLANs, page 9-43
Procedure: Enable E-Series Spanning Tree on Ethernet Ports, page 9-44
Procedure: Retrieve the MAC Table Information, page 9-54
Procedure: Create Ethernet RMON Alarm Thresholds, page 9-56

9.1 G1000-4 Card

The G1000-4 card reliably transports Ethernet and IP data across an SDH backbone. The G1000-4 card maps up to four Gigabit-Ethernet interfaces onto an SDH transport network. A single card provides scalable and provisionable transport bandwidth at the signal levels up to VC4-16C per card. The card provides line rate forwarding for all Ethernet frames (unicast, multicast, and broadcast) and can be configured to support Jumbo frames (defined as a maximum of 10,000 bytes). The G-series card incorporates features optimized for carrier-class applications such as:

- High availability (including hitless (< 50 ms) performance under software upgrades and all types of SONET/SDH equipment protection switches)
- Hitless reprovisioning
- Support of Gigabit Ethernet traffic at full line rate

The G1000-4 card allows an Ethernet private line service to be provisioned and managed very much like a traditional SONET or SDH line. G1000-4 card applications include providing carrier-grade transparent LAN services (TLS), 100-Mbps Ethernet private line services (when combined with an external 100-Mb Ethernet switch with Gigabit uplinks), and high availability transport for applications such as storage over metropolitan-area network (MAN)/WANs.

You can map the four ports on the G1000-4 independently to any combination of VC4, VC4-2c, VC4-3c, VC4-8c, and VC4-16c circuit sizes, provided the sum of the circuit sizes that terminate on a card do not exceed VC4-16c.

To support a Gigabit Ethernet port at full line rate, an STM circuit with a capacity greater or equal to 1 Gbps (bidirectional 2 Gbps) is needed. A VC4-8c is the minimum circuit size that can support a Gigabit Ethernet port at full line rate.The G1000-4 supports a maximum of two ports at full line rate.

Ethernet cards may be placed in any of the 12 multipurpose card slots. In most configurations, at least two of the 12 slots need to be reserved for optical trunk cards, such as the STM-64 card. The reserved slots give the ONS 15454 SDH a practical maximum of ten G1000-4 cards. The G1000-4 card requires the XC10G card to operate. For more information about the G1000-4 card specifications, see the Card Reference chapter in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

The G1000-4 transmits and monitors the SDH J1 Path Trace byte in the same manner as ONS 15454 SDH cards. For more information, see the "Creating a Path Trace" section on page 6-21.

9.1.1 G1000-4 Application

Figure 9-1 shows an example of a G1000-4 card application. In this example, data traffic from the Gigabit Ethernet port of a high-end router travels across the ONS 15454 SDH point-to-point circuit to the Gigabit Ethernet port of another high-end router.

Figure 9-1   Data traffic using a G1000-4 point-to-point circuit
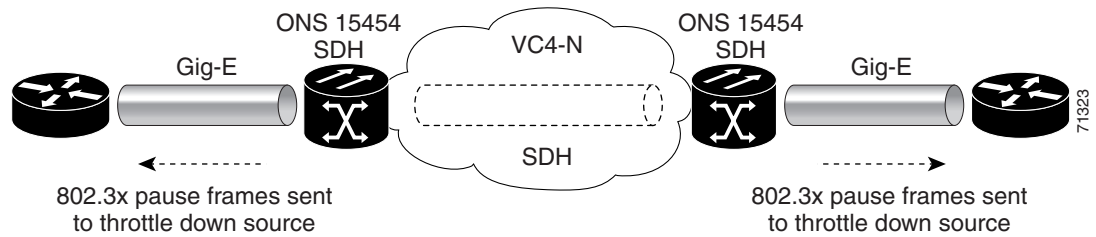
The G1000-4 card transports any Layer 3 protocol that can be encapsulated and transported over Gigabit Ethernet, such as IP or IPX, over an SDH network. The data is transmitted on the Gigabit Ethernet fiber into the standard Cisco Gigabit Interface Converter (GBIC) on a G1000-4 card. The G1000-4 card transparently maps Ethernet frames into the SDH payload by multiplexing the payload onto an SDH STM-N card. When the SDH payload reaches the destination node, the process is reversed and the data is transmitted from the standard Cisco GBIC in the destination G1000-4 card onto the Gigabit Ethernet fiber.

The G1000-4 card discards certain types of erroneous Ethernet frames rather than transport them over SDH. Erroneous Ethernet frames include corrupted frames with CRC errors and under-sized frames that do not conform to the minimum 60-byte-length Ethernet standard. The G1000-4 card forwards valid frames unmodified over the SDH network. Information in the headers is not affected by the encapsulation and transport. For example, packets with formats that include IEEE 802.1Q information will travel through the process unaffected.

9.1.2 802.3x Flow Control and Frame Buffering

The G1000-4 card supports IEEE 802.3x flow control and frame buffering to reduce data traffic congestion. To buffer over-subscription, 512 kb of buffer memory is available for the receive and transmit channels on each port. When the buffer memory on the Ethernet port nears capacity, the ONS 15454 SDH uses IEEE 802.3x flow control to send back a pause frame to the source at the opposite end of the Gigabit Ethernet connection.

The pause frame instructs that source to stop sending packets for a specific period of time. The sending station waits the requested time before sending more data. Figure 9-1 illustrates pause frames being sent from the ONS 15454 SDH to the sources of the data. The G1000-4 card does not respond to pause frames received from client devices.

This flow control mechanism matches the sending and receiving device throughput to that of the bandwidth of the STM circuit. For example, a router may transmit to the Gigabit Ethernet port on the G1000-4 card. This particular data rate may occasionally exceed 622 Mbps, but the ONS 15454 SDH circuit assigned to the G1000-4 card port may be only VC4-4c (622.08 Mbps). In this example, the ONS 15454 SDH sends out a pause frame and requests that the router delay its transmission for a certain period of time. With a flow control capability combined with the substantial per-port buffering capability, a private line service provisioned at less than full line rate capacity (VC4-8c) is nevertheless very efficient because frame loss can be controlled to a large extent.

Some important characteristics of the flow control feature on the G1000-4 include:

*   The G1000-4 card only supports asymmetric flow control. Flow control frames are sent to the external equipment, but no response from the external equipment is necessary or acted upon.

*   Received flow control frames are quietly discarded. They are not forwarded onto the SDH path, and the G1000-4 card does not respond to the flow control frames.

- On the G1000-4 card, you can only enable flow control on a port when auto-negotiation is enabled on the device attached to that port. For more information, see the "G1000-4 Port Provisioning" section on page 9-7.

Because of these characteristics, the link auto-negotiation and flow control capability on the attached Ethernet device must be correctly provisioned for successful link auto-negotiation and flow control on the G1000-4. If link auto-negotiation fails, the G1000-4 does not use flow control (default).

⚠

Caution   Without flow control, traffic loss can occur if the input traffic rate is higher than the bandwidth of the circuit for an extended period of time.

9.1.3 Ethernet Link Integrity Support

The G1000-4 supports end-to-end Ethernet link integrity. This capability is integral to providing an Ethernet private line service and correct operation of Layer 2 and Layer 3 protocols on the attached Ethernet devices at each end. End-to-end Ethernet link integrity essentially means that if any part of the end-to-end path fails, the entire path fails. Failure of the entire path is ensured by turning off the transmit lasers at each end of the path. The attached Ethernet devices recognize the disabled transmit laser as a loss of carrier and consequently an inactive link.

✎

Note   Some network devices can be configured to ignore a loss of carrier condition. If such a device attaches to a G1000-4 card at one end, then alternative techniques (such as use of Layer 2 or Layer 3 protocol keep alive messages) are required to route traffic around failures. The response time of such alternate techniques is typically much longer than techniques that use link state as an indication of an error condition.

As shown in Figure 9-2, a failure at any point of the path (A, B, C, D, or E) causes the G1000-4 card at each end to disable its transmit laser at their ends, which causes the devices at both ends to detect link down. If one of the Ethernet ports is administratively disabled or set in loopback mode, the port is considered a "failure" for the purposes of end-to-end link integrity because the end-to-end Ethernet path is unavailable. The port "failure" also causes both ends of the path to be disabled.

Figure 9-2   End-to-end Ethernet link integrity support
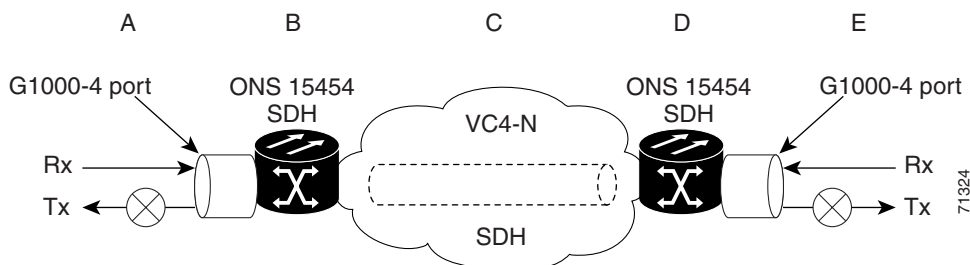
9.1.4 Gigabit EtherChannel/IEEE 802.3ad Link Aggregation

The end-to-end Ethernet link integrity feature of the G1000-4 can be used in combination with Gigabit EtherChannel (GEC) capability on attached devices. The combination provides an Ethernet traffic restoration scheme that has a faster response time than alternate techniques such as spanning-tree

rerouting, yet is more bandwidth efficient because spare bandwidth does not need to be reserved. The G1000-4 supports GEC, which is a Cisco proprietary standard similar to the IEEE link aggregation standard (IEEE 802.3ad). Figure 9-3 illustrates G1000-4 GEC support.

Figure 9-3   G1000-4 Gigabit EtherChannel (GEC) support
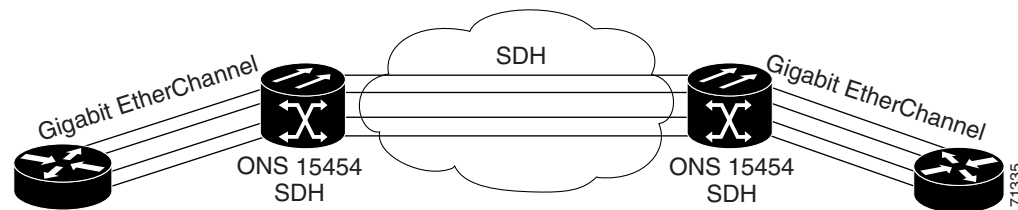
Although the G1000-4 card does not actively run GEC, it supports the end-to-end GEC functionality of attached Ethernet devices. If two Ethernet devices running GEC connect through G1000-4 cards to an ONS 15454 SDH network, the ONS 15454 SDH side network is transparent to the EtherChannel devices. The EtherChannel devices operate as if they are directly connected to each other. Any combination of G1000-4 parallel circuit sizes can be used to support GEC throughput.

GEC provides line-level active redundancy and protection (1:1) for attached Ethernet equipment. It can also bundle parallel G1000-4 data links together to provide more aggregated bandwidth. STP operates as if the bundled links are one link and permits GEC to utilize these multiple parallel paths. Without GEC, STP only permits a single non-blocked path. GEC can also provide G1000-4 card-level protection or redundancy because it can support a group of ports on different cards (or different nodes) so that if one port or card has a failure, then traffic is rerouted over the other port or card.

9.1.5 G1000-4 LEDs

G1000-4 series Ethernet card faceplates have two card-level LEDs and a colored LED next to each port (Figure 9-4 on page 9-6). The LED states are described in Table 9-3 on page 9-6.

Figure 9-4   G1000-4 card faceplate LEDs
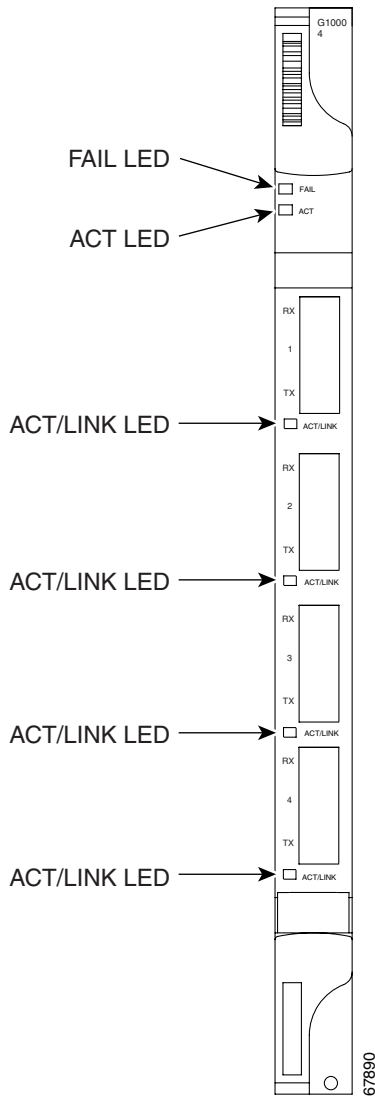
Table 9-3   G1000-4 Card-Level LEDs

LED	LED State	Description
FAIL LED	Red	The card's processor is not ready or a catastrophic software failure occurred on the card. The RED LED is normally illuminated while the card boots up and turns off when the software is deemed operational.
ACT LED	Green	The card is active and the software is operational.
ACT/LINK LED	Off	No link exists to the Ethernet port.
ACT/LINK LED	Solid Amber	A link exists to the Ethernet port, but traffic flow is inhibited. For example, a lack of circuit set-up, an error on the line, or a disabled port may inhibit traffic flow.

Table 9-3   G1000-4 Card-Level LEDs

LED	LED State	Description
ACT/LINK LED	Solid Green	A link exists to the Ethernet port, but no traffic is carried on the port.
ACT/LINK LED	Flashing Green	A link exists to the Ethernet port and traffic is carried on the port. The LED flash rate reflects the traffic rate for the port.

9.1.6 G1000-4 Port Provisioning

This section explains how to provision Ethernet ports on a G1000-4 card. Most provisioning requires filling in two fields: Enabled and Flow Control Negotiation. You can also configure the maximum frame size permitted, either Jumbo or 1548 bytes.

Media Type indicates the type of GBIC installed. For more information on GBICs for the G1000-4 card, see the "G1000-4 Gigabit Interface Converters" section on page 9-9. The Negotiation Status column displays the result of the most recent auto-negotiation. The type of flow control that was negotiated will be displayed.

Note You can only provision flow control on the G1000-4 by enabling auto-negotiation. If the attached device does not support auto-negotiation or is not correctly configured to support the G1000-4's asymmetric flow control, flow control is ignored.

Procedure: Provision G1000-4 Ethernet Ports

Step 1 From the node view, double-click the G1000-4 card graphic to open the card view.

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

Figure 9-5 shows the Provisioning tab with the Port subtab selected.

Figure 9-5   Provisioning G1000-4 Ethernet ports
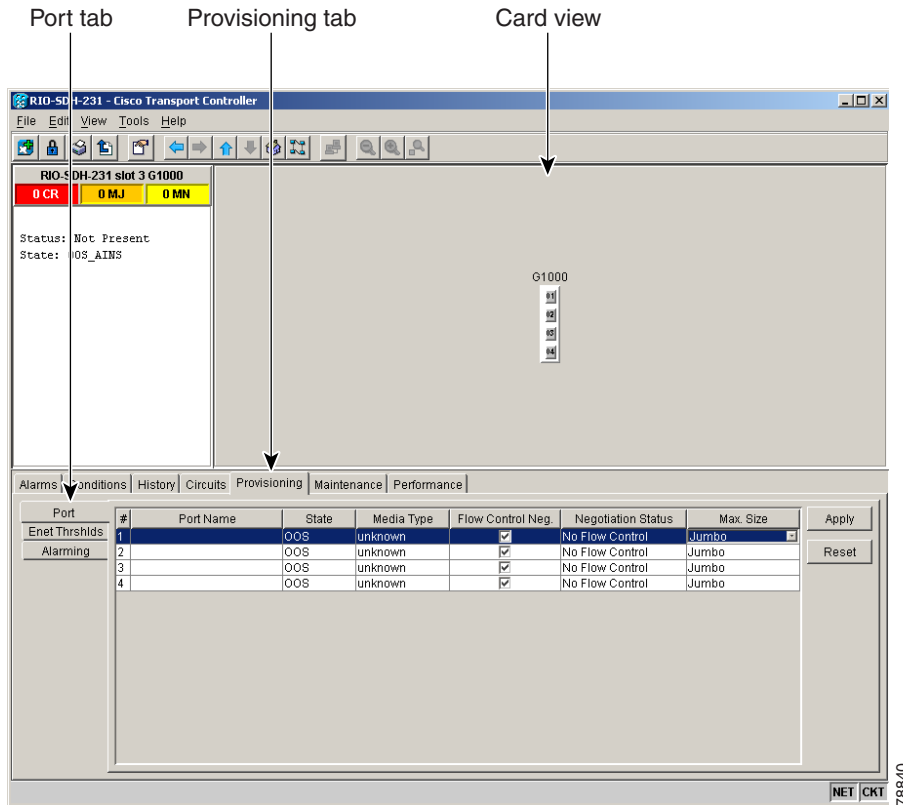
Step 3   For each G1000-4 port, provision the following parameters:

- Port Name—If you want to label the port, type the port name.

- State—Choose **IS** or **OOS-AINS** to activate or prepare a port for service. The following port states are available:

  – IS—The circuit is in service.

  – OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

  – OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

  – OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Flow Control Neg—Click this check box to enable flow control negotiation on the port (default). If you do not want to enable flow control, uncheck the box.

Note   To activate flow control, the Ethernet device attached to the G1000-4 card must be set to auto-negotiation. If flow control is enabled but the negotiation status indicates no flow control, check the auto-negotiation settings on the attached Ethernet device.

- Max Size—To permit the acceptance of jumbo-size Ethernet frames, select **Jumbo** (default). If you do not want to permit jumbo-size Ethernet frames, select **1548**.

> **Note**   The maximum frame size of 1548 bytes, instead of the common maximum frame size of 1518 bytes, enables the port to accept valid Ethernet frames that use new protocols. New protocols, such as MPLS, add bytes and may cause the frame size to exceed the common 1518 byte maximum.

Step 4   Click **Apply**.

Step 5   Refresh the Ethernet statistics:

   a.   Click the **Performance** > **Statistics** tabs.

   b.   Click the **Refresh** button.

> **Note**   Reprovisioning an Ethernet port on the G1000-4 card does not reset the Ethernet statistics for that port. See the "Statistics Window" section on page 9-47 for information about clearing the statistics for the G1000-4 port. Reprovisioning an Ethernet port on the E-series Ethernet cards resets the Ethernet statistics for that port.

9.1.7 G1000-4 Gigabit Interface Converters

Gigabit Interface Converters (GBICs) are hot-swappable input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. Figure 9-6 shows a GBIC. The type of GBIC determines the maximum distance that the Ethernet traffic will travel from the card to the next network device.

The G1000-4 card supports three types of standard Cisco GBICs: SX, LX, and ZX.

1000BASE-SX operates on multi-mode, fiber-optic link spans of up to 550 m in length. 1000BASE-LX operates on single-mode, fiber-optic link spans of up to 10 km in length. 1000BASE-ZX operates on single-mode, fiber-optic link spans of up to 70 km in length. Link spans of up to 100 km are possible using premium single-mode fiber or dispersion-shifted single-mode fiber.

Figure 9-6   Gigabit Interface Converter

Receiver   Transmitter
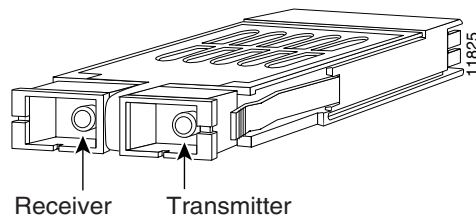
Table 9-4 shows the available GBICs for the G1000-4 card.

Table 9-4   G1000-4 Card GBICs

GBIC	Span Length	Product Number
Short wavelength (1000BASE-SX)	550 m	15454-GBIC-SX

Table 9-4   G1000-4 Card GBICs

GBIC	Span Length	Product Number
Long wavelength/long haul (1000BASE-LX)	10 km	15454-GBIC-LX
Extended distance (1000BASE-ZX)	70 km	15454-GBIC-ZX

⚠

Caution   Use only GBICs certified for use in the ONS 15454 SDH G1000-4 card (Cisco product numbers 15454-GBIC-SX, 15454-GBIC-LX and 15454-GBIC-ZX).

For GBIC installation and cabling instructions, see the "Install Gigabit Interface Converters" procedure on page 1-41.

9.2 E-Series Cards

The E-series cards incorporate Layer 2 switching, while the G-series card is a straight mapper card. E-series cards support VLAN, IEEE 802.1Q, spanning tree, and IEEE 802.1D. An ONS 15454 SDH holds a maximum of ten Ethernet cards. You can insert Ethernet cards in any multipurpose slot. For card specifications, see the Card Reference chapter in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

9.2.1 E100T-G Card

E100T-G cards provide twelve switched, IEEE 802.3-compliant, 10/100BaseT Ethernet ports. The 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.

9.2.2 E1000-2-G Card

E1000-2-G cards provides two switched, IEEE 802.3-compliant, Gigabit Ethernet (1000 Mbps) ports that support full duplex operation.

9.2.3 E-Series LEDs

E-series Ethernet card faceplates have three card-level LEDs and a pair of port-level LEDs next to each port. The SF LED is inactive.

Table 9-5   E-Series 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 card. When the ACT LED is green, it indicates that the Ethernet card is active and the software is operational.

Table 9-6   E-Series Port-Level LEDs

LED State	Description
Amber	Transmitting and receiving
Solid Green	Idle and link integrity
Green Light Off	Inactive connection or unidirectional traffic

For detailed specifications of the Ethernet cards, refer to the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

9.2.4 E-Series Port Provisioning

This section explains how to provision Ethernet ports on an E-series Ethernet card. Most provisioning requires filling in two fields: Enabled and Mode. However, you can also map incoming traffic to a low-priority or high-priority queue using the Priority column, and disable spanning tree with the Stp Enabled column. For more information about spanning tree, see the "E-Series Spanning Tree (IEEE 802.1D)" section on page 9-43. 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 E-Series Ethernet Ports

Step 1   Display CTC and double-click the card graphic to open the Ethernet card.

Step 2   Click the **Provisioning > Ether Port** tabs (Figure 9-7).

Figure 9-7   Provisioning E-100 series Ethernet ports

Step 3   From the Port window, choose the appropriate mode for each Ethernet port.

The following are valid choices for the E100T-G card:

- Auto
- 10 Half
- 10 Full
- 100 Half
- 100 Full

The following are valid choices for the E1000-2-G card:

- Auto
- 1000 Full

Note   Both 1000 Full and Auto mode set the E1000-2-G 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-G card to auto-negotiate 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-G port handshakes with the connected network device to determine if that device supports flow control.

Step 4   Click the **Enabled** check box(es) 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.

9.2.5 E-Series Gigabit Interface Converters

Gigabit interface converters (GBICs) are hot-swappable input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC determines the maximum distance that the Ethernet traffic will travel from the card to the next network device.

The E1000-2-G card supports SX and LX GBICs.

1000BASE-SX operates on multi-mode, fiber-optic link spans of up to 550 m in length. 1000BASE-LX operates on single-mode, fiber-optic links of up to 10 km in length.

Table 9-7 shows the available GBICs.

Table 9-7   Available GBICs

GBIC	Span Length	Product Number
Short wavelength (1000BASE-SX)	550 m	15454-GBIC-SX
Long wavelength/long haul (1000BASE-LX)	10 km	15454-GBIC-LX

For GBIC installation and cabling instructions, see the "Install Gigabit Interface Converters" procedure on page 1-41.

⚠
Caution   Use only GBICs certified for use in the ONS 15454 SDH E1000-2-G card (Cisco product numbers 15454-GBIC-SX and 15454-GBIC-LX).

⚠
Caution   E1000-2-G cards lose traffic for approximately 30 seconds when an ONS 15454 SDH database is restored. Traffic is lost during the period of spanning-tree reconvergence. The CARLOSS alarm will appear and clear during this period.

9.3 E-Series Multicard and Single-Card EtherSwitch

The ONS 15454 SDH enables multicard and Single-card EtherSwitch modes for E-series cards. At the Ethernet card view in CTC, click the **Provisioning > Ether Card** tabs to reveal the Card Mode option.

9.3.1 E-Series Multicard EtherSwitch

Multicard EtherSwitch provisions two or more Ethernet cards to act as a single Layer 2 switch. It supports one VC4-2c circuit or two VC4 circuits. The bandwidth of the single switch formed by the Ethernet cards matches the bandwidth of the provisioned Ethernet circuit up to VC4-2c worth of bandwidth. Figure 9-8 illustrates a Multicard EtherSwitch configuration.

Figure 9-8   Multicard EtherSwitch configuration
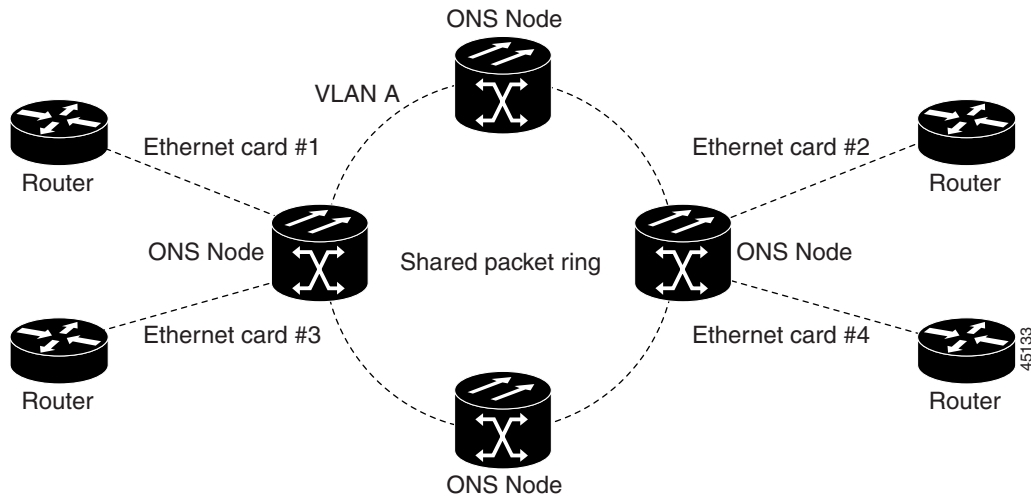
9.3.2 E-Series Single-Card EtherSwitch

Single-card EtherSwitch allows each Ethernet card to remain a single switching entity within the ONS 15454 SDH shelf. This option allows a full VC4-4c worth of bandwidth between two Ethernet circuit points. Figure 9-9 illustrates a Single-card EtherSwitch configuration.

Figure 9-9   Single-card EtherSwitch configuration
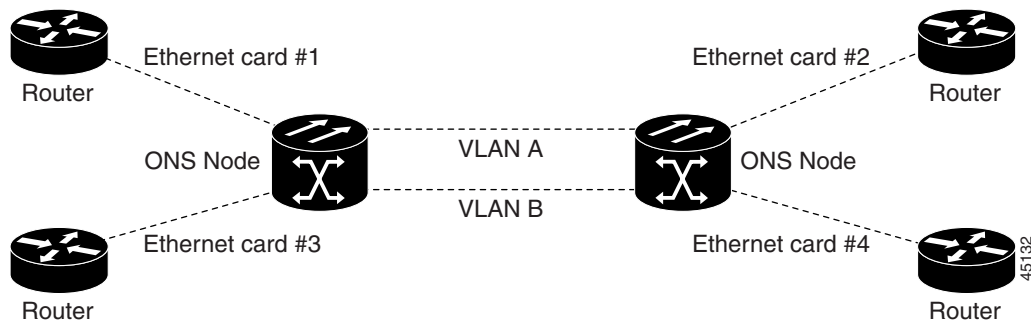
Four scenarios exist for provisioning maximum Single-card EtherSwitch bandwidth:

1. VC4-4c
2. VC4-2c + VC4-2c
3. VC4-2c + VC4 + VC4
4. VC4 + VC4 + VC4 + VC4

Note   When configuring scenario 3, the VC4-2c must be provisioned before either of the VC4 circuits.

9.4 E-Series 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 STM channel on the ONS 15454 optical interface and also to bridge non-ONS SDH network segments.

> **Note**   When making a VC4-4c Ethernet circuit, Ethernet cards must be configured as Single-card EtherSwitch. Multicard mode does not support VC4-4c Ethernet circuits.

9.4.1 E-Series Ethernet Circuits

The ONS 15454 SDH can set up a point-to-point (straight) Ethernet circuit as Single-card or Multicard. Multicard EtherSwitch (Figure 9-10) limits bandwidth to VC4-2c of bandwidth between two Ethernet circuit points, but allows you to add nodes and cards and make a shared packet ring. Single-card EtherSwitch (Figure 9-11 on page 9-16) allows a full VC4-4c of bandwidth between two Ethernet circuit points.

Figure 9-10   Multicard EtherSwitch circuit

ONS 15454 SDH #1

192.168.1.25
255.255.255.0
VLAN test 1
Slot 4, port 1

192.168.1.50
255.255.255.0
VLAN test 1
Slot 15, port 1

192.168.1.100
255.255.255.0
VLAN test 1
Slot 5, port 1

ONS 15454 SDH #2

ONS 15454 SDH #3

192.168.1.75
255.255.255.0
VLAN test 1
Slot 17, port 1

———— SDH
- - - - - - Ethernet

71362
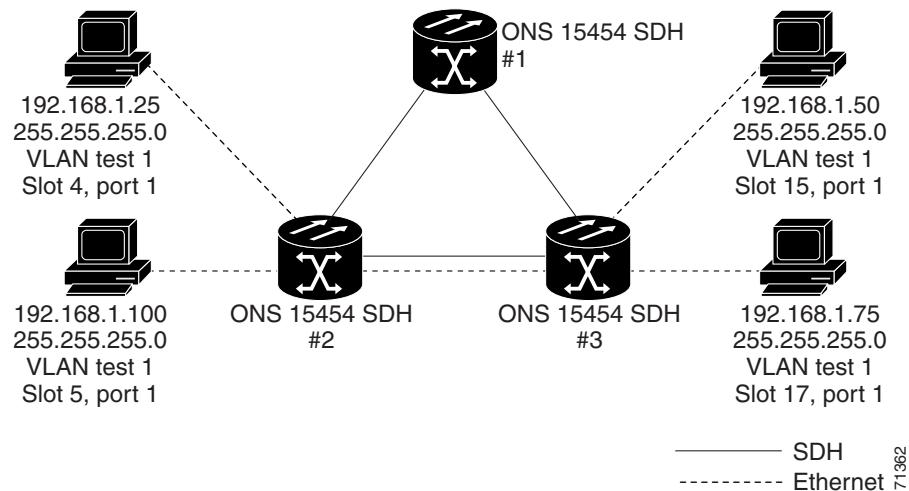
Figure 9-11   Single-card EtherSwitch circuit
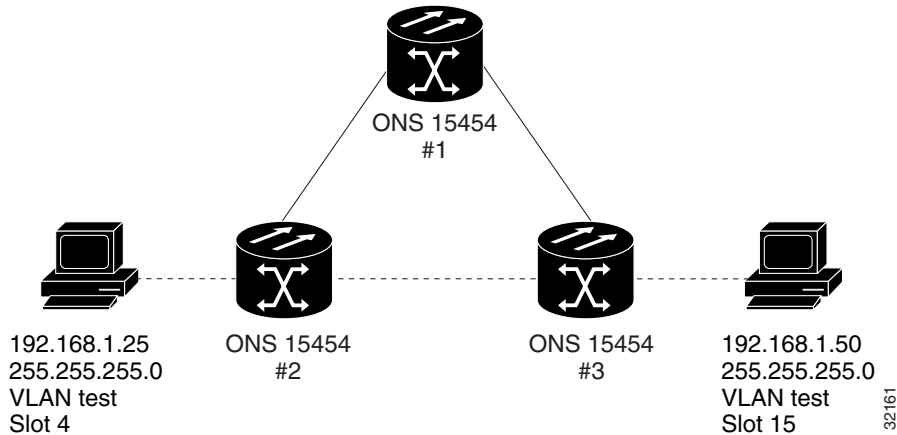
Procedure: Provision an E-Series EtherSwitch Circuit (Multicard or Single-Card)

Step 1   From the node view, double-click one of the Ethernet cards that will carry the circuit.

> **Note**   Change card settings only if there are no circuits using this card.

Step 2   Click the **Provisioning > Ether Card** tabs.

Step 3   Under Card Mode, choose one of the following:

- For Multicard EtherSwitch circuit groups, choose **Multicard EtherSwitch Group.** Click **Apply**.
- For Single-card EtherSwitch circuits, choose **Single-card EtherSwitch.** Click **Apply**.

Step 4   For Multicard EtherSwitch circuits only, repeat Steps 1 to 3 for all other Ethernet cards in the ONS 15454 SDH that will carry the circuit.

Step 5   From the View menu, choose **Go to Other Node**.

Step 6   In the Select Node dialog box, select the other ONS 15454 Ethernet circuit endpoint node and repeat Steps 1 to 5.

Step 7   Click the **Circuits** tab and click **Create**.

Step 8   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Select **VC_HO_PATH_CIRCUIT**.
- Size—Select the circuit size. The valid circuit sizes for an Ethernet Multicard circuit are VC4 and VC4-2c. The valid circuit sizes for an Ethernet Single-card circuit are VC4, VC4-2c and VC4-4c.
- Bidirectional—Leave the default unchanged (checked).
- Number of circuits—Leave the default unchanged (1).
- Auto-ranged—Not available.
- State—Choose **IS** (in service). Ethergroup circuits are stateless, and always in service.
- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series Ethernet card ports.

- Create cross connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.

- Inter-domain (UCP) SLA—If the circuit will travel on a unified control plane (UCP) channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave the default unchanged (unchecked).

Step 9   If the circuit will be routed on an SNCP, set the SNCP path selectors.

Step 10   Click **Next**.

Step 11   Provision the circuit source.

  a.   From the Node pull-down menu, select one of the EtherSwitch circuit endpoint nodes. (Either end node can be the EtherSwitch circuit source.)

  b.   From the Slot pull-down menu, select one of the following:

   – If you are building a Multicard EtherSwitch circuit, choose **Ethergroup**.

   – If you are building a Single-card EtherSwitch circuit, choose the Ethernet card where you enabled the Single-card EtherSwitch.

Step 12   Click **Next**.

Step 13   Provision the circuit destination.

  a.   From the Node pull-down menu, select the second EtherSwitch circuit endpoint node.

  b.   From the Slot pull-down menu, select one of the following:

   – If you are building a Multicard EtherSwitch circuit, choose **Ethergroup**.

   – If you are building a Single-card EtherSwitch circuit, choose the Ethernet card where you enabled the Single-card EtherSwitch.

Step 14   Click **Next**.

Step 15   If the desired VLAN already exists, go to Step 18. Under Circuit VLAN Selection, click **New VLAN**.

Step 16   In the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—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.

Step 17   Click **OK**.

Step 18   Under Circuit VLAN Selection, highlight the VLAN name and click the Arrow (**>>**) button to move the available VLAN(s) to the Circuit VLANs column.

Step 19   If you are building a Single-card EtherSwitch circuit and want to disable spanning-tree protection on this circuit, uncheck the **Enable Spanning Tree** check box and click **OK** in the Disabling Spanning Tree dialog. The Enable Spanning Tree check box will remain checked or unchecked for the creation of the next Single-card point-to-point Ethernet circuit.

⚠

Caution   Disabling spanning-tree protection increases the likelihood of logic loops on an Ethernet network.

⚠

Caution   Turning off spanning tree on a circuit-by-circuit basis means that the ONS 15454 SDH is no longer protecting the Ethernet circuit and that the circuit must be protected by another mechanism in the Ethernet network.

⚠

Caution   Multiple circuits with spanning-tree protection enabled will incur blocking if the circuits traverse the same E-series Ethernet card and use the same VLAN.

✎

Note   You can disable or enable spanning-tree protection on a circuit-by-circuit basis only for single-card point-to-point Ethernet circuits. Other E-series Ethernet configurations disable or enable spanning tree on a port-by-port basis at the card view of CTC under the Provisioning tab.

Step 20   Click **Next**.

Step 21   Confirm that the following information about the circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 SDH circuit nodes

Step 22   Click **Finish**.

Step 23   Complete the "Provision E-Series Ethernet Ports" procedure on page 9-11.

Step 24   Complete the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

9.4.2 E-Series Shared Packet Ring Ethernet Circuits

This section provides steps for creating a shared packet ring (Figure 9-12). Your network architecture may differ from the example.

Figure 9-12   Shared packet ring Ethernet circuit
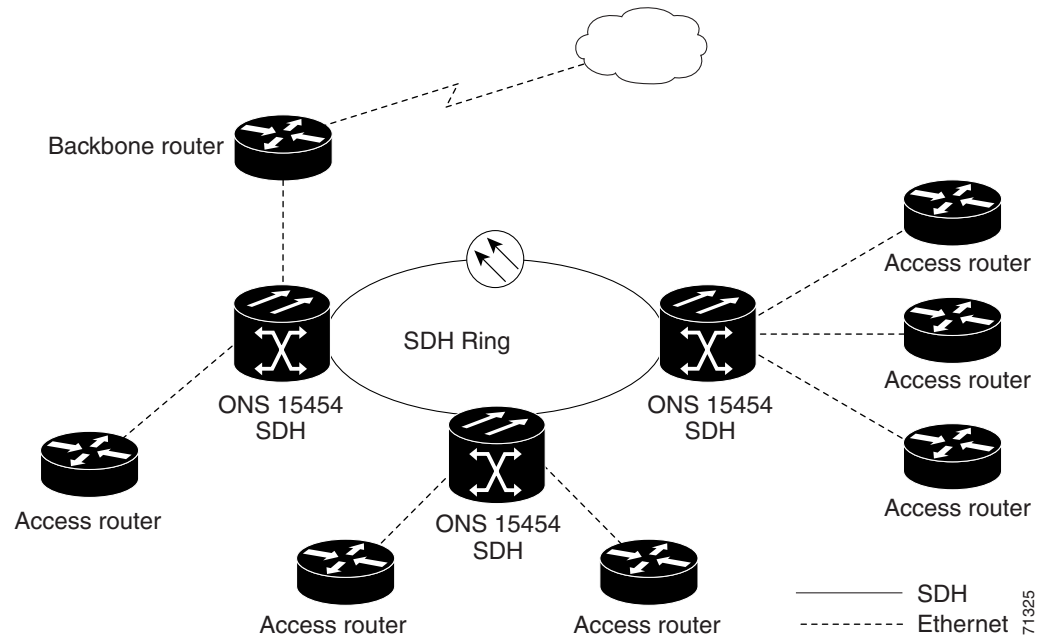
Procedure: Provision an E-Series Shared Packet Ring Circuit

Step 1   From the node view, double-click one of the Ethernet cards that will carry the circuit.

> **Note**   Change card settings only if there are no circuits using this card.

Step 2   Click the **Provisioning > Ether Card** tabs.

Step 3   Verify that Multi-card EtherSwitch Group is selected. If Multi-card EtherSwitch Group is not selected, select it and **c**lick **Apply**.

Step 4   Repeat Steps 1 to 3 for all other Ethernet cards in the ONS 15454 SDH that will carry the shared packet ring.

Step 5   Click the **Circuits** tab and click **Create**.

Step 6   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.

- Type—Select **VC_HO_PATH_CIRCUIT**.

- Size—Select the circuit size. For shared packet ring Ethernet, valid circuit sizes are VC4 or VC4-2c.

- Bidirectional—Leave checked for this circuit (default).

- Number of circuits—Leave set to 1 (default).

- Auto-ranged—Unavailable.

- State—Choose a service state to apply to the circuit.

  - IS—The circuit is in service.

  - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

  - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series Ethernet card ports.

- Create cross connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave unchecked.

Step 7 If the circuit will be routed on an SNCP, set the SNCP path selectors.

Step 8 Click **Next**.

Step 9 Provision the circuit source.

    a. From the Node pull-down menu, select one of the shared packet ring circuit endpoint nodes. (Either end node can be the shared packet ring circuit source.)

    b. From the Slot pull-down menu, choose **Ethergroup**.

Step 10 Click **Next**.

Step 11 Provision the circuit destination.

    a. From the Node pull-down menu, select the second shared packet ring circuit endpoint node.

    b. From the Slot pull-down menu, select **Ethergroup**.

Step 12 Click **Next**.

Step 13 Review the VLANs listed under Available VLANs (Figure 9-13 on page 9-21). If the VLAN you want to use is displayed, go to Step 15. If you need to create a new VLAN, complete the following steps:

    a. Click the **New VLAN** button.

    b. In the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—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 SDH network supports a maximum of 509 user-provisionable VLANs.

    c. Click **OK**.

Figure 9-13   Choosing a VLAN name and ID
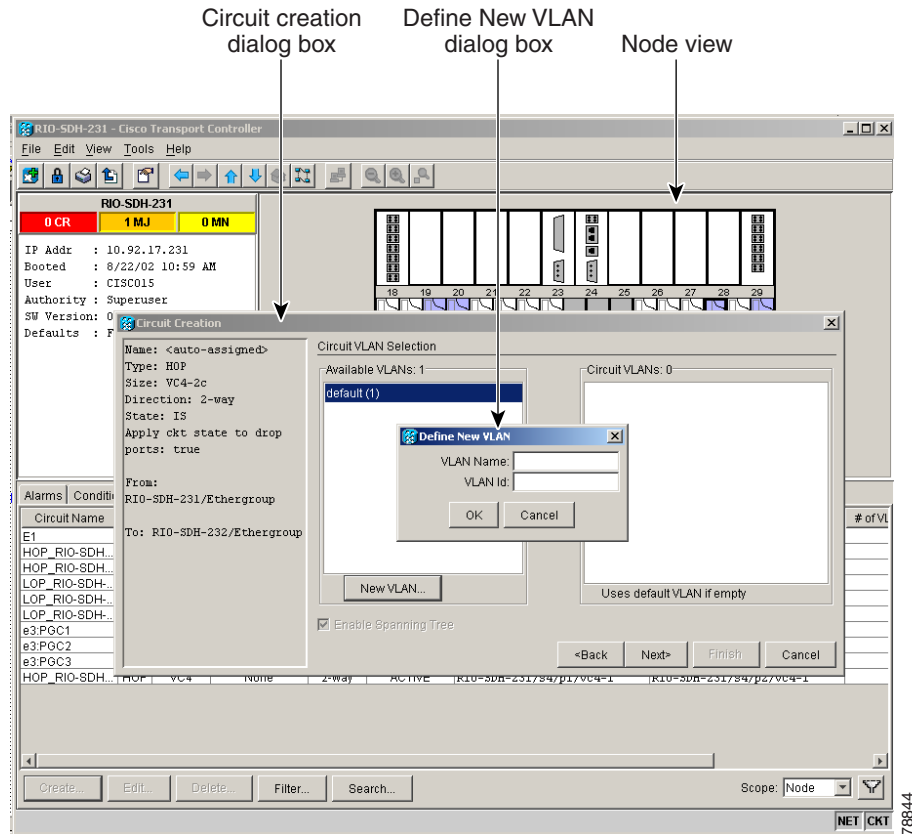
Step 14   Click the VLAN you want to use in the Available VLANs column, then click the Arrow (**>>**) button to move the VLAN to the Circuit VLANs column. See Figure 9-14.

Note   Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Figure 9-14   Selecting VLANs
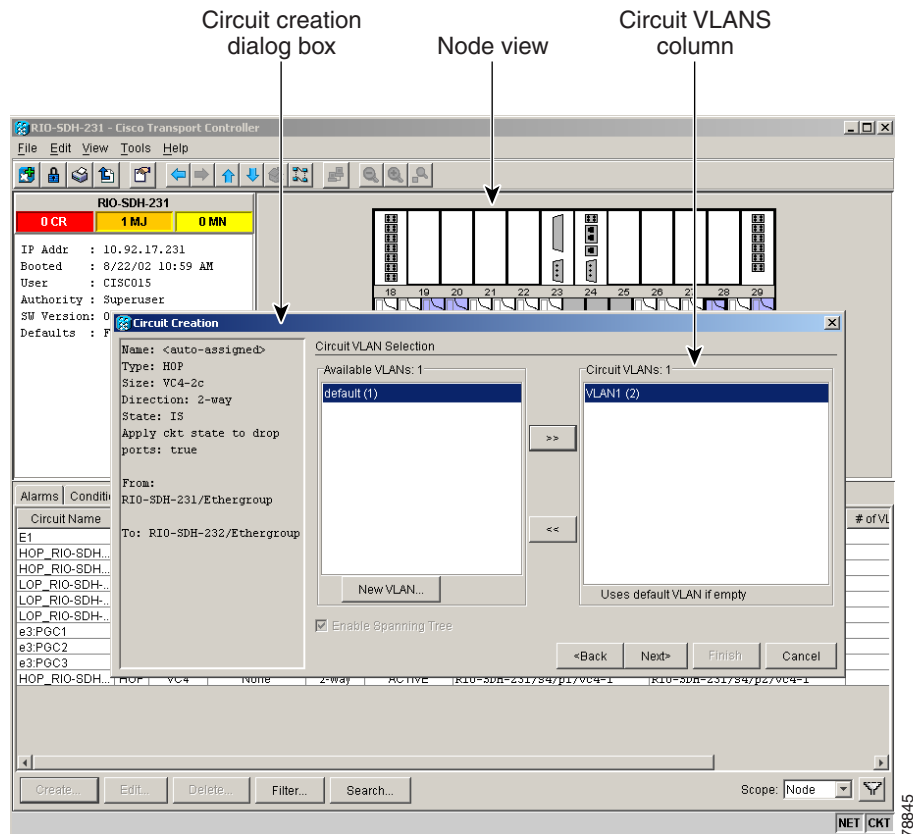
Step 15   Click **Next**.

Step 16   Under Circuit Routing Preferences, uncheck the **Route Automatically** check box and click **Next**.

Step 17   Under Route Review and Edit panel, click the source node, then click either span (green arrow) leading from the source node.

The span turns white.

Step 18   Click **Add Span**.

The span turns blue. CTC adds the span to the Included Spans list.

Step 19   Click the node at the end of the blue span.

Step 20   Click the green span with the source node from Step 17.

The span turns white.

Step 21   Click **Add Span**.

The span turns blue.

Step 22   Repeat Steps 18 to 21 for every node in the ring.

Step 23   Verify that the new circuit is correctly configured. If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information.

Note   If the circuit is incorrect, you can also click **Finish**, delete the completed circuit, and begin the procedure again.

Step 24   Click **Finish**.

Step 25   Complete the "Provision E-Series Ethernet Ports" procedure on page 9-11.

Step 26   Complete the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

9.4.3 E-Series 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 9-15 illustrates a sample hub-and-spoke ring. Your network architecture may differ from the example.

Figure 9-15   Hub-and-spoke Ethernet circuit
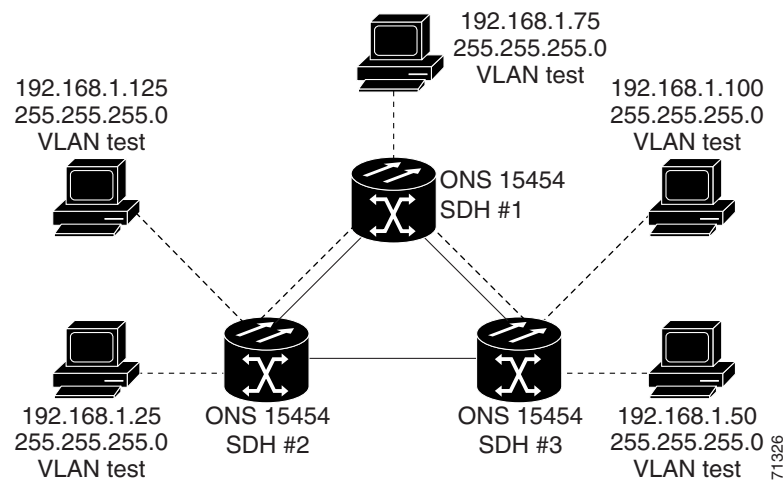
Procedure: Provision an E-Series Hub-and-Spoke Ethernet Circuit

Step 1   From the node view, double-click the Ethernet card that will carry the circuit.

> **Note**   Change card settings only if there are no circuits using this card.

Step 2   Click the **Provisioning > Ether Card** tabs.

Step 3   Under Card Mode, choose **Single-card EtherSwitch** and **c**lick **Apply**.

Step 4   Navigate to the other ONS 15454 SDH endpoint node of the hub-and-spoke circuit and repeat Step 1 to Step 3.

Step 5   Click the **Circuits** tab and click **Create**.

Step 6   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.

- Type—Select **VC_HO_PATH_CIRCUIT**.

- Size—Select the circuit size.

- Bidirectional—Leave checked for this circuit (default).

- Number of circuits—Leave set to 1 (default).

- Auto-ranged—Not available.

- State—Choose a service state to apply to the circuit.

    - IS—The circuit is in service.

    - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

    - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

    - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series Ethernet card ports.

- Create cross connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave unchecked.

Step 7   If the circuit will be routed on an SNCP, set the SNCP path selectors.

Step 8   Click **Next**.

Step 9   Provision the circuit source.

    a. From the Node pull-down menu, select one of the hub-and-spoke circuit endpoint nodes. (Either end node can be the circuit source.)

    b. From the Slot pull-down menu, choose the Ethernet card where you enabled the Single-card EtherSwitch in Step 3.

Step 10   Click **Next**.

Step 11   Provision the circuit destination.

    a. From the Node pull-down menu, select the second EtherSwitch circuit endpoint node.

    b. From the Slot pull-down menu, choose the Ethernet card where you enabled the Single-card EtherSwitch in Step 3.

Step 12   Click **Next**.

Step 13   Review the VLANs listed under Available VLANs (Figure 9-16 on page 9-25). If the VLAN you want to use is displayed, go to Step 15. If you need to create a new VLAN, complete the following steps:

    a. Click the **New VLAN** button.

    b. In the New VLAN dialog box, complete the following:

        - VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—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 SDH network supports a maximum of 509 user-provisionable VLANs.

c. Click **OK**.

Figure 9-16   Choosing a VLAN name and ID
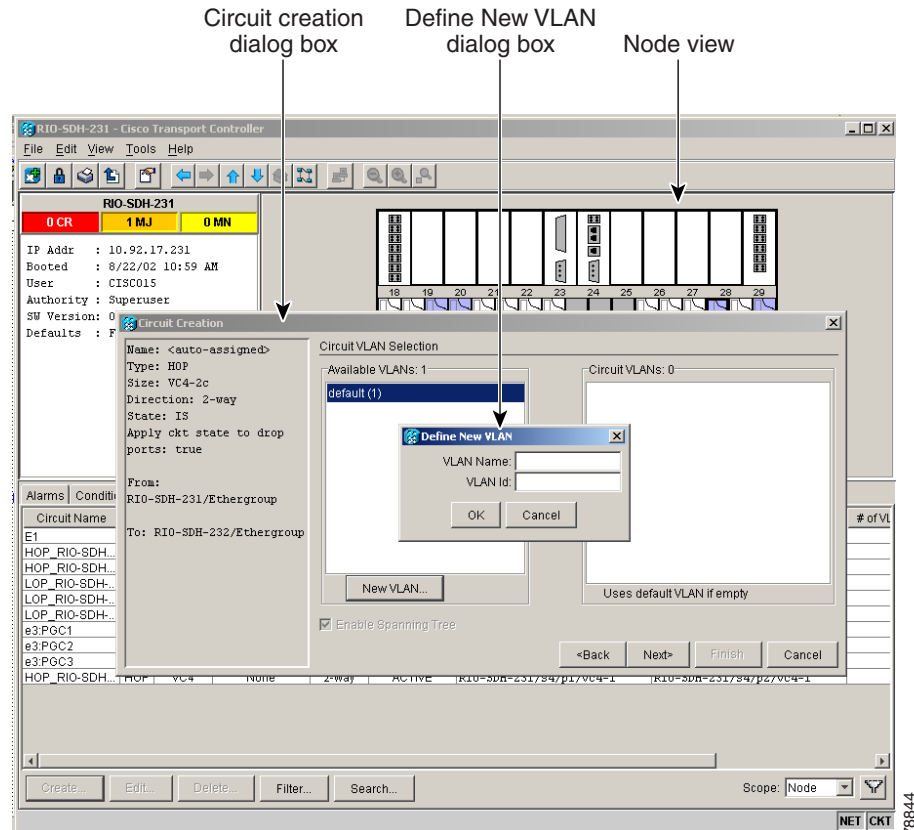
Step 14 Click the VLAN you want to use in the Available VLANs column, then click the Arrow (**>>**) button to move the VLAN to the Circuit VLANs column.

![note icon]

Note Moving the VLAN from Available VLANs to Circuit VLANs forces all the VLAN traffic to use the shared packet ring you are creating.

Step 15 Click **Next.**

Step 16 Confirm that the following information about the hub-and-spoke circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15454 SDH circuit nodes

If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information.

✎
Note   You can also click **Finish**, delete the completed circuit, and start the procedure from the beginning.

Step 17   Click **Finish**.

Step 18   Navigate to an ONS 15454 SDH that will be an endpoint for the second Ethernet circuit.

Step 19   Double-click the Ethernet card that will carry the circuit.

Step 20   Click the **Provisioning > Ether Card** tabs.

Step 21   Under Card Mode, choose **Single-card EtherSwitch** and click **Apply**.

Step 22   From the View menu, choose **Go to Other Node**.

Step 23   In the Select Node dialog box, choose the other endpoint node for the second circuit and repeat Steps 19 to 21 at that node.

Step 24   Click the **Circuits** tab and click **Create**.

Step 25   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.

- Type—Select STS.

- Size—Select the circuit size.

- Bidirectional—Leave checked for this circuit.

- Number of circuits—Leave set to 1 (default).

- Auto-ranged—Not available.

- State—Choose a service state to apply to the circuit.

    – IS—The circuit is in service.

    – OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

    – OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

    – OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Uncheck this box; states cannot be applied to E-Series Ethernet card ports.

- Create cross connects only (TL1-like)—Uncheck this box; it does not apply to Ethernet circuits.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave unchecked.

Step 26   If the circuit will be routed on an SNCP, set the SNCP path selectors.

Step 27   Click **Next.**

Step 28   Provision the circuit source.

    a.   From the Node pull-down menu, select one of the hub-and-spoke circuit endpoint nodes. (Either end node can be the circuit source.)

    b.   From the Slot pull-down menu, choose the Ethernet card where you enabled the Single-card EtherSwitch in Step 21.

Step 29   Click **Next**.

Step 30   Provision the circuit destination.

    a.   From the Node pull-down menu, select the second EtherSwitch circuit endpoint node.

    b.   From the Slot pull-down menu, choose the Ethernet card where you enabled the Single-card EtherSwitch.

Step 31   Click **Next**.

Step 32   Highlight the VLAN that you created for the first circuit and click the Arrow (**>>**) button to move the VLAN(s) from the Available VLANs column to the Selected VLANs column.

Step 33   Click **Next**.

Step 34   Confirm that the following information about the second hub-and-spoke circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15454 SDH circuit nodes

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 35   Click **Finish**.

Step 36   Complete the "Provision E-Series Ethernet Ports" procedure on page 9-11.

Step 37   Complete the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

9.4.4 E-Series Ethernet Manual Cross-Connects

ONS 15454 SDH nodes require end-to-end CTC visibility between nodes for normal provisioning of Ethernet circuits. When other vendors' equipment sits between ONS 15454 SDH nodes, OSI/TARP-based equipment does not allow tunneling of the ONS 15454 SDH TCP/IP-based DCC. To circumvent this lack of continuous DCC, the Ethernet circuit must be manually cross connected (Figure 9-17 on page 9-28) to an VC4 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 follow.

Figure 9-17   Ethernet manual cross-connects
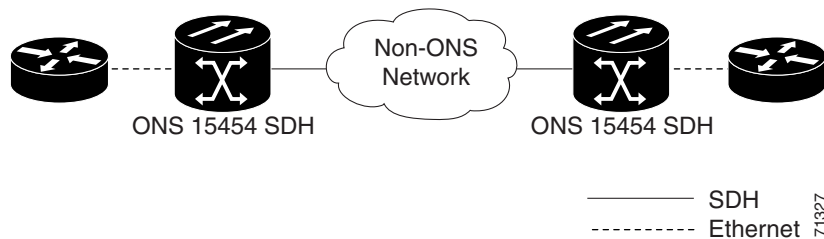
Procedure: Provision an E-Series Single-Card EtherSwitch Manual Cross-Connect

Step 1   From the node view, double-click the Ethernet card that will carry the cross-connect.

> **Note**   In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an STM-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 2   Click the **Provisioning > Ether Card** tabs.

> **Note**   Change card settings only if there are no circuits using this card.

Step 3   Under Card Mode, choose **Single-card EtherSwitch** and click **Apply**.

Step 4   Click the **Circuits** tab and click **Create**.

Step 5   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the cross-connect.

- Type—Select VC_HO_PATH_CIRCUIT.

- Size—Select the cross-connect size. For Single-card EtherSwitch, the available sizes are VC4, VC4-2c and VC4-4c.

- Bidirectional—Leave checked for this cross-connect (default).

- Number of circuits—Leave set to 1 (default).

- Auto-ranged—Not available.

- State—Choose a service state to apply to the circuit.

    - IS—The circuit is in service.

    - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

    - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

    - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Uncheck this box.

- Create cross connects only (TL1-like)—Uncheck this box.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave unchecked.

Step 6   If the circuit carried by the cross-connect will be routed on an SNCP, set the SNCP path selectors.

- 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 you do not choose Revertive, traffic remains on the protect path after the switch.

- Reversion time—If Revertive is checked, choose the reversion time. Click the Reversion time field and select a reversion time from the pull-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.

- SF threshold—Choose from one E-3, one E-4, or one E-5.

- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.

- Switch on PDI-P—Check this box if you want traffic to switch when a VC4 payload defect indicator is received (VC4 circuits only).

Step 7   Click **Next**.

Step 8   Provision the circuit source.

a.   From the Node pull-down menu, choose the cross-connect source node.

b.   From the Slot pull-down menu, choose the Ethernet card where you enabled the Single-card EtherSwitch in Step 3.

Step 9   Click **Next**.

Step 10   Provision the circuit destination.

a.   From the Node pull-down menu, choose the cross-connect circuit source node selected in Step 8. (For Ethernet cross-connects, the source and destination nodes are the same.)

b.   From the Slot pull-down menu, choose the STM-N card that is connected to the non-ONS equipment.

c.   Depending on the STM-N card, choose the port and/or VC4 from the Port and VC4 pull-down menus.

Step 11   Click **Next**.

Step 12   Review the VLANs listed under Available VLANs. If the VLAN you want to use is displayed, go to Step 14. If you need to create a new VLAN, complete the following steps:

a.   Click the **New VLAN** button.

b.   In the New VLAN dialog box, complete the following:

- VLAN Name—Assign an easily identifiable name to your VLAN.

- VLAN ID—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 SDH network supports a maximum of 509 user-provisionable VLANs.

c.   Click **OK**.

Step 13   Click the VLAN you want to use in the Available VLANs column, then click the Arrow (**>>**) button to move the VLAN to the Circuit VLANs column.

Step 14   Click **Next**. The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 15   Confirm that the following information about the Single-card EtherSwitch manual cross-connect is correct.

> ✎
> **Note**   In this task, "circuit" refers to the Ethernet cross-connect.

- Circuit name
- Circuit type
- Circuit size
- VLAN names
- ONS 15454 SDH nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 16   Click **Finish**.

Step 17   Complete the "Provision E-Series Ethernet Ports" procedure on page 9-11.

Step 18   Complete the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

> ✎
> **Note**   The appropriate VC4 circuit must exist in the non-ONS equipment to connect the two VC4 circuits from the ONS 15454 SDH Ethernet manual cross-connect endpoints.

> ⚠
> **Caution**   If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits may have a circuit-size mismatch. For example, a circuit size of VC4-2c might have been configured on the first ONS 15454 SDH while a circuit size of VC4 was configured on the second ONS 15454 SDH. To troubleshoot this occurrence of the CARLOSS alarm, refer to the CARLOSS alarm troubleshooting procedure in the Alarm Troubleshooting chapter of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Procedure: Provision an E-Series Multicard EtherSwitch Manual Cross-Connect

Step 1   From the node view, double-click the Ethernet card where you want to create the cross-connect.

> ✎
> **Note**   In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an STM-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 2   Click the **Provisioning > Ether Card** tabs.

Step 3   Under Card Mode, choose **Multi-card EtherSwitch Group** and click **Apply**.

Step 4   From the View menu, choose **Go to Parent View**.

Step 5   Repeat Steps 1 to 4 for any other Ethernet cards in the ONS 15454 SDH that will carry the circuit.

Step 6   Click the **Circuits** tab and click **Create**.

Step 7   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the source cross connect. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the source cross connect.

- Type—Select **VC_HO_PATH_CIRCUIT**.

- Size—Select the size of the circuit that will be carried by the cross-connect. For Multicard EtherSwitch circuits, the available sizes are VC4 and VC4-2c.

- Bidirectional—Leave checked (default).

- Number of circuits—Leave set to 1 (default).

- Auto-ranged—Not available.

- State—Choose a service state to apply to the circuit.

    – IS—The circuit is in service.

    – OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.

    – OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.

    – OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.

- Apply to drop ports—Uncheck this box.

- Create cross connects only (TL1-like)—Uncheck this box.

- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.

- Protected Drops—Leave unchecked.

Step 8   If the circuit carried by the cross-connect will be routed on an SNCP, set the SNCP path selectors.

- 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 you do not choose Revertive, traffic remains on the protect path after the switch.

- Reversion time—If Revertive is checked, choose the reversion time. Click the Reversion time field and select a reversion time from the pull-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.

- SF threshold—Choose from one E-3, one E-4, or one E-5.

- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.

- Switch on PDI-P—Check this box if you want traffic to switch when a VC4 payload defect indicator is received (VC4 circuits only).

Step 9   Click **Next**.

Step 10   Provision the cross-connect source.

   a. From the Node pull-down menu, select the cross-connect source node.

   b. From the Slot pull-down menu, choose **Ethergroup**.

Step 11   Click **Next**.

Step 12 From the Node pull-down menu under Destination, choose the circuit source node selected in Step 10. (For Ethernet cross-connects, the source and destination nodes are the same.)

The Slot field automatically is provisioned for Ethergroup.

Step 13 Click **Next**.

Step 14 Review the VLANs listed under Available VLANs. If the VLAN you want to use is displayed, go to Step 16. If you need to create a new VLAN, complete the following steps:

   a. Click the **New VLAN** button.

   b. In the New VLAN dialog box, complete the following:

     • VLAN Name—Assign an easily identifiable name to your VLAN.

     • VLAN ID—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 SDH network supports a maximum of 509 user-provisionable VLANs.

   c. Click **OK**.

Step 15 Click the VLAN you want to use in the Available VLANs column, then click the Arrow (**>>**) button to move the VLAN to the Circuit VLANs column.

Step 16 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 17 In the left pane, verify the cross-connect information.

> **Note** In this task, "circuit" refers to the Ethernet cross-connect.

• Circuit name

• Circuit type

• Circuit size

• VLANs

• ONS 15454 SDH nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 18 Click **Finish**.

Step 19 Complete the "Provision E-Series Ethernet Ports" procedure on page 9-11.

Step 20 Complete the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

Step 21 From the View menu, choose **Go to Home View**.

Step 22 Click the **Circuits** tab.

Step 23 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box opens.

Step 24 Click **Drops** and click **Create**.

The Define New Drop dialog box opens.

Step 25 From the Slot menu, choose the STM-N card that links the ONS 15454 SDH to the non-ONS 15454 SDH equipment.

Step 26 From the Port menu, choose the appropriate port.

Step 27   From the VC4 menu, choose the VC4 that matches the VC4 of the connecting non-ONS 15454 SDH equipment.

Step 28   Click **OK**.

Step 29   Confirm the circuit information that displays in the Edit Circuit dialog box and click **Close**.

Step 30   Repeat Steps 2 to 29 at the second ONS 15454 SDH Ethernet manual cross-connect endpoint.

> **Note**   The appropriate VC4 circuit must exist in the non-ONS 15454 SDH equipment to connect the two ONS 15454 SDH Ethernet manual cross-connect endpoints.

> **Caution**   If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits may have a circuit-size mismatch. For example, a circuit size of VC4-2c might have been configured on the first ONS 15454 SDH while a circuit size of VC4 was configured on the second ONS 15454 SDH. To troubleshoot this occurrence of the CARLOSS alarm, refer to the CARLOSS alarm troubleshooting procedure in the Alarm Troubleshooting chapter of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Step 31   Complete the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

9.5 G1000-4 Circuit Configurations

This section explains how to provision G1000-4 point-to-point circuits and Ethernet manual cross-connects. Ethernet manual cross-connects allow you to cross connect individual Ethernet circuits to an VC4 channel on the ONS 15454 SDH optical interface and also to bridge non-ONS SDH network segments.

9.5.1 G1000-4 EtherSwitch Circuits

G1000-4 cards support point-to-point circuit configuration (Figure 9-18). Provisionable circuit sizes are VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c and VC4-16c. Each Ethernet port maps to a unique VC4 circuit on the SDH side of the G1000-4.

Figure 9-18   G1000-4 point-to-point circuit
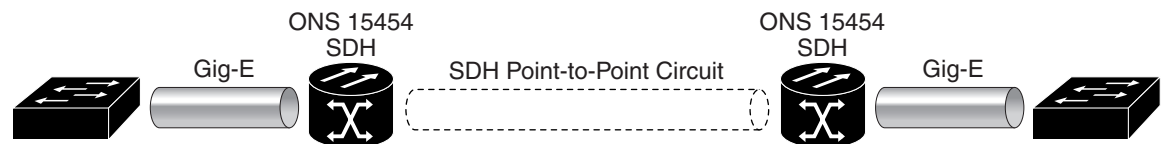
The G1000-4 supports any combination of up to four circuits from the list of valid circuit sizes, however the circuit sizes can add up to no more than VC4-16c. Due to hardware constraints, this card imposes additional restrictions on the combinations of circuits that can be dropped onto a G1000-4 card. These restrictions are transparently enforced by the ONS 15454 SDH, and you do not need to keep track of restricted circuit combinations.

The restriction occurs when a single VC4-8c is dropped on a card. In this instance, the remaining circuits on that card can be another single VC4-8c or any combination of circuits of VC4-4c size or less that add up to no more than VC4-4c (i.e., a total of VC4-16c on the card).

No circuit restrictions are present if VC4-8c circuits are not being dropped on the card. The full VC4-16c bandwidth can be used (for example, using either a single VC4-16c or four VC4-4c circuits).

> **Note** Since the restrictions only apply when VC4-8c circuits are involved but do not apply to two VC4-8c circuits on a card, you can easily minimize the impact of these restrictions. Group the VC4-8c circuits together on a card separate from circuits of other sizes. The grouped circuits can be dropped on other G1000-4 cards on the ONS 15454 SDH.

> **Note** All SDH-side VC4 circuits must be contiguous.

> **Caution** G1000-4 circuits connect with STM-N cards or other G1000-4 cards. G1000-4 cards do not connect with E-series Ethernet cards.

Procedure: Provision a G1000-4 EtherSwitch Circuit

Step 1   From the node view, click the **Circuits** tab and click **Create**.

Step 2   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the circuit.
- Type—Select **VC_HO_PATH_CIRCUIT**.
- *S*ize—Select the circuit size. Valid circuit sizes for a G1000-4 circuit are VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, and VC4-16c.
- Bidirectional—Leave checked for this circuit (default).
- Number of circuits—Leave set to 1 (default).
- State—Choose a service state to apply to the circuit.
  - IS—The circuit is in service.
  - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.
  - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.
  - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.
- Apply to drop ports—Check this box to apply the state chosen in the State field (IS or OOS-MT only) to the Ethernet circuit source and destination ports. You cannot apply OOS-AINS to G1000-4 Ethernet card ports. CTC will apply the circuit state to the ports if the circuit is in full control of the port. If not, a Warning dialog box displays the ports where the circuit state could not be applied. If not checked, CTC will not change the state of the source and destination ports.

> **Note**   LOS alarms display if in service (IS) ports are not receiving signals.

- Create cross connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Auto-ranged—Not available.
- Protected Drops—Leave unchecked.

Step 3   If the circuit will be routed on an SNCP, set the SNCP path selectors.

> **Caution**   If you are provisioning a G1000-4 circuit on an SNCP, do not check the **Switch on PDI-P** check box. Checking the **Switch on PDI-P** check box may cause unnecessary SNCP protection switches.

Step 4   Click **Next**.

Step 5   Provision the circuit source.

    a.   From the Node pull-down menu, choose the circuit source node. Either end node can be the point-to-point circuit source.

    b.   From the Slot pull-down menu, choose the slot containing the G1000-4 card that you will use for one end of the point-to-point circuit.

    c.   From the Port pull-down menu, choose a port.

Step 6   Click **Next**.

Step 7   Provision the circuit destination.

    a.   From the Node pull-down menu, choose the circuit destination node.

    b.   From the Slot pull-down menu, choose the slot containing the G1000-4 card that you will use for other end of the point-to-point circuit.

    c.   From the Port pull-down menu, choose a port.

Step 8   Click **Next**. The Circuits window appears.

Step 9   Confirm that the following information about the point-to-point circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 SDH circuit nodes

Step 10   Click **Finish**.

Step 11   If you have not already provisioned the Ethernet card, follow the "Provision G1000-4 Ethernet Ports" procedure on page 9-7.

> **Note**   To change the capacity of a G1000-4 point-to-point circuit, you must delete the original circuit and reprovision a new larger circuit.

9.5.2 G1000-4 Manual Cross-Connects

ONS 15454 SDH nodes require end-to-end CTC visibility between nodes for normal provisioning of Ethernet circuits. When other vendors' equipment sits between ONS 15454 SDH nodes, OSI/TARP-based equipment does not allow tunneling of the ONS 15454 SDH TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit must be manually cross connected (Figure 9-19) to a VC4 channel riding through the non-ONS network. This allows an Ethernet circuit to run from ONS node to ONS node while utilizing the non-ONS network.

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 SDH to allow a circuit to enter and exit an ONS 15454 SDH. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15454 SDH network) to the drop or destination (where traffic exits an ONS 15454 SDH network).

Figure 9-19   G1000-4 manual cross-connects
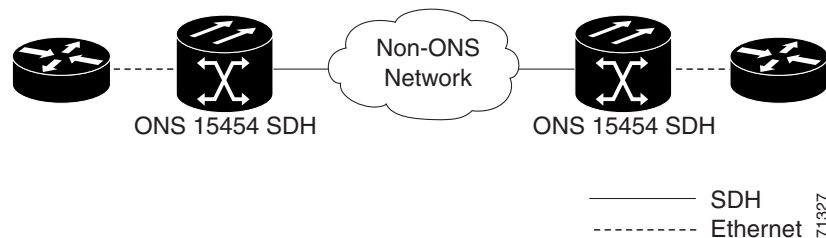
Procedure: Provision a G1000-4 Manual Cross-Connect

Note   In this procedure, cross-connect refers to a circuit connection created within the same node between the Ethernet card and an STM-N card connected to third-party equipment. You create cross-connects at the source and destination nodes so an Ethernet circuit can be routed from source to destination across third-party equipment.

Step 1   From the node view, click the **Circuits** tab and click **Create**.

Step 2   In the Create Circuits dialog box, complete the following fields:

- Name—Assign a name to the source cross-connect. The name can be alphanumeric and up to 48 characters (including spaces). If you leave the field blank, CTC assigns a default name to the source cross-connect.

- Type—Select **VC_HO_PATH_CIRCUIT**.

- Size—Select the size of the circuit that will be carried by the cross-connect. The valid circuit sizes for a G1000-4 circuit are VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, and VC4-16c.

- Bidirectional—Leave checked for this cross-connect (default).

- Number of circuits—Leave set to 1 (default).

- Auto-ranged—Not available.

- State—Choose a service state to apply to the circuit after it is created.
    - IS—The circuit is in service.
    - OOS—The circuit is out of service. Traffic is not passed on the circuit until it is in service.
    - OOS-AINS—(default) The circuit is in service when it receives a valid signal; until then, the circuit is out of service.
    - OOS-MT—The circuit is in a maintenance state. The maintenance state does not interrupt traffic flow; it suppresses alarms and conditions and allows loopbacks to be performed on the circuit. Use OOS-MT for circuit testing or to suppress circuit alarms temporarily. Change the state to IS, OOS, or OOS-AINS when testing is complete.
- Apply to drop ports—Uncheck this box.
- Create cross connects only (TL1-like)—Uncheck this box.
- Inter-domain (UCP) SLA—If the circuit will travel on a UCP channel, enter the service level agreement number. Otherwise, leave the field set to zero.
- Protected Drops—Leave unchecked.

Step 3 If the circuit carried by the cross-connect will be routed on an SNCP, set the SNCP path selectors.

- 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 you do not choose Revertive, traffic remains on the protect path after the switch.
- Reversion time—If Revertive is checked, choose the reversion time. Click the Reversion time field and select a reversion time from the pull-down menu. The range is 0.5 to 12.0 minutes. The default is 5.0 minutes. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared.
- SF threshold—Choose from one E-3, one E-4, or one E-5.
- SD threshold—Choose from one E-5, one E-6, one E-7, one E-8, or one E-9.
- Switch on PDI-P—Check this box if you want traffic to switch when a VC4 payload defect indicator is received (VC4 circuits only).

Step 4 Click **Next**.

Step 5 Provision the circuit source.

  a. From the Node pull-down menu, select the circuit source node.

  b. From the Slot pull-down menu, choose the G1000-4 that will be the cross-connect source.

  c. From the Port pull-down menu, select the cross-connect source port.

Step 6 Click **Next**.

Step 7 Provision the circuit destination.

  a. From the Node pull-down menu, select the cross-connect source node selected in Step 5. (For Ethernet cross connects, the source and destination nodes are the same.)

  b. From the Slot pull-down menu, choose the STM-N card that is connected to the non-ONS equipment.

  c. Depending on the STM-N card, choose the port and/or VC4 from the Port and VC4 pull-down menus.

Step 8 Click **Next**.

Step 9 Verify the cross-connection information.

> ✎
> **Note**   In this task, "circuit" refers to the Ethernet cross-connect.

- Circuit name
- Circuit type
- Circuit size
- ONS 15454 SDH circuit nodes

If the information is not correct, click the **Back** button and repeat the procedure with the correct information.

Step 10   Click **Finish**.

Step 11   You now need to provision the Ethernet ports. For port provisioning instructions, see the "Provision G1000-4 Ethernet Ports" procedure on page 9-7.

Step 12   To complete the procedure, repeat Steps 1 to 10 at the second ONS 15454 SDH.

> ✎
> **Note**   The appropriate STM circuit must exist in the non-ONS equipment to connect the two STMs from the ONS 15454 SDH Ethernet manual cross-connect endpoints.

> ⚠
> **Caution**   If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits may have a circuit-size mismatch. For example, a circuit size of VC4-2c might have been configured on the first ONS 15454 SDH while a circuit size of VC4 was configured on the second ONS 15454 SDH. To troubleshoot this occurrence of the CARLOSS alarm, refer to the CARLOSS alarm troubleshooting procedure in the Alarm Troubleshooting chapter of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

9.6 E-Series 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 SDH. The definition of VLAN ports includes all Ethernet and packet-switched SDH port types. All VLAN IP address discovery, flooding, and forwarding is limited to these ports.

The ONS 15454 SDH IEEE 802.1Q-based VLAN mechanism provides logical isolation of subscriber LAN traffic over a common SDH 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.

9.6.1 E-Series 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 SDH 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 SDH Ethernet port does not support IEEE 802.1Q, the ONS 15454 SDH only uses Q-tags internally. The ONS 15454 SDH associates these Q-tags with specific ports.

With Ethernet devices that do not support IEEE 802.1Q, the ONS 15454 SDH 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 SDH uses the Q-tag attached by the external Ethernet devices. Packets enter the ONS network with an existing Q-tag; the ONS 15454 SDH 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.

To set ports to Tagged and Untag, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-41.

Figure 9-20   Q-tag moving through a VLAN
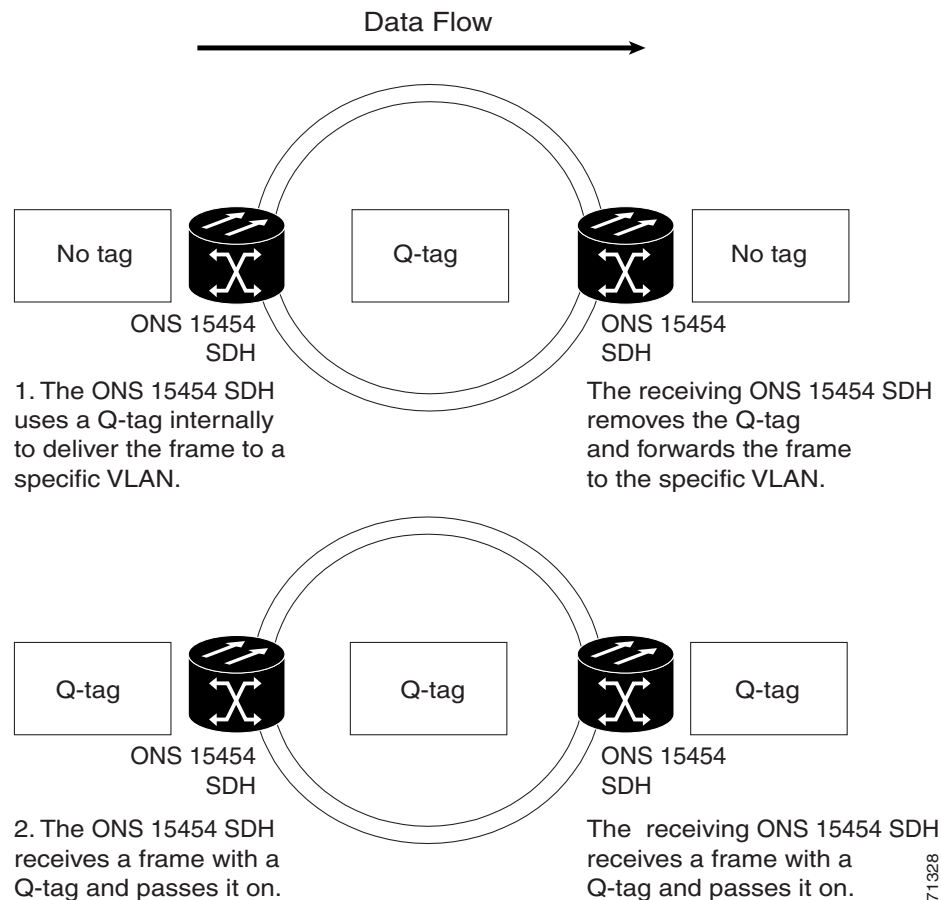
9.6.2 E-Series Priority Queuing (IEEE 802.1Q)

Note   IEEE 802.1Q was formerly titled 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 SDH supports priority queuing. The ONS 15454 SDH takes the eight priorities specified in IEEE 802.1Q and maps them to two queues (Table 9-8). Q-tags carry priority queuing information through the network.

The ONS 15454 SDH 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 9-8   Priority Queuing

User Priority	Queue	Allocated Bandwidth
0,1,2,3	Low	30%
4,5,6,7	High	70%

The priority queueing process is illustrated in Figure 9-21.

Figure 9-21   Priority queuing process

Data Flow

No priority

Priority

ONS 15454
SDH

ONS 15454 SDH maps a frame
with port-based priority using
a Q-tag.

Priority tag
removed

ONS 15454
SDH

The receiving ONS 15454 SDH
removes the Q-tag and
forwards the frame.

Priority

Same
priority

ONS 15454
SDH

ONS 15454 SDH uses a Q-tag to
map a frame with priority and
forwards it on.

Priority

ONS 15454
SDH

The receiving ONS 15454 SDH
receives the frame with a
Q-tag and forwards it.

71329

9.6.3 E-Series VLAN Membership

This section explains how to provision Ethernet ports for VLAN membership. For initial port
provisioning (prior to provisioning VLAN membership) see the "E-Series Port Provisioning" section on
page 9-11.

⚠

Caution   ONS 15454 SDH nodes propagate VLANs whenever a node appears on the same network view of
another node regardless of whether the nodes connect through DCC. For example, if two ONS 15454
SDH nodes without DCC connectivity belong to the same Login Node Group, then whenever CTC gets
launched from within this login node group, VLANs propagate from one to another. This happens even
though the ONS 15454 SDH nodes do not belong to the same SDH ring.

Procedure: Provision Ethernet Ports for VLAN Membership

The ONS 15454 SDH allows you to configure the VLAN membership and Q-tag handling of individual
Ethernet ports on the E-series Ethernet cards.

Step 1   Display the CTC card view for the Ethernet card.

Step 2   Click the **Provisioning > Ether VLAN** tabs (Figure 9-22).

Step 3   To put a port in a VLAN, click the port and choose either **Tagged** or **Untag**. Figure 9-22 on page 9-42 shows Port 1 in the red VLAN and Port 2 through Port 12 in the default VLAN. Table 9-9 shows valid port settings.

Figure 9-22   Configuring VLAN membership for individual Ethernet ports
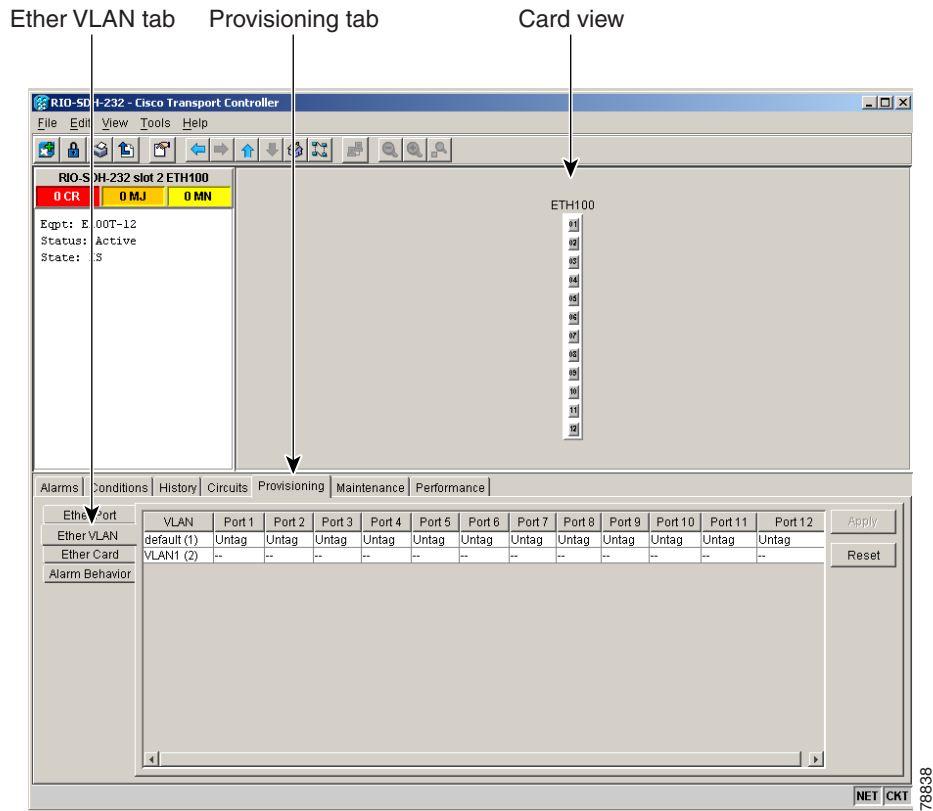
Note   If Tagged is chosen, the attached external devices must recognize IEEE 802.1Q VLANs.

Note   Both ports on individual E1000-2-G cards cannot be members of the same VLAN.

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, that also supports trunking. A trunk port must have tagging (IEEE 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 9-9   Port Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15454 SDH will tag ingress frames and strip tags from egress frames.
Tagged	The ONS 15454 SDH will handle ingress frames according to VLAN ID; egress frames will not have their tags removed.

9.6.4 VLAN Counter

The ONS 15454 SDH displays the number of VLANs used by circuits and the total number of VLANs available for use.

Procedure: Display Available VLANs

Use the following procedure to display the number of available VLANs and the number of VLANs used by circuits.

Step 1   Click the **Circuits** tab and click an existing Ethernet circuit to highlight it.

Step 2   Click **Edit**.

Step 3   Click the **VLANs** tab.

9.7 E-Series Spanning Tree (IEEE 802.1D)

The Cisco ONS 15454 SDH 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 SDH ports. On Ethernet ports, STP is enabled by default, but may be disabled with a check box under the Provisioning > Port tabs at the card-level view. A user can also disable or enable STP on a circuit-by-circuit basis on unstitched Ethernet cards in a point-to-point configuration. However, turning off spanning-tree protection on a circuit-by-circuit basis means that the ONS 15454 SDH system is not protecting the Ethernet traffic on this circuit, and the Ethernet traffic must be protected by another mechanism in the Ethernet network. On SDH 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   STP blocked path
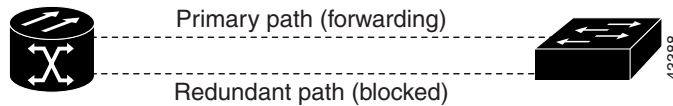
To remove loops, STP defines a tree that spans all the switches in an extended network. STP forces certain redundant data paths into a standby (blocked) state. If one network segment in the STP becomes unreachable, the spanning-tree algorithm reconfigures the spanning-tree topology and reactivates the 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 SDH supports one STP instance per circuit and a maximum of eight STP instances per ONS 15454 SDH.

⚠
Caution   Multiple circuits with spanning-tree protection enabled will incur blocking, if the circuits traverse a common card and use the same VLAN.

9.7.1 E-Series Multi-Instance Spanning Tree and VLANs

The ONS 15454 SDH can operate multiple instances of STP to support VLANs in a looped topology. You can dedicate separate circuits across the SDH ring for different VLAN groups (i.e., one for private TLS service and one for Internet access). Each circuit runs its own STP to maintain VLAN connectivity in a multi-ring environment.

Procedure: Enable E-Series Spanning Tree on Ethernet Ports

Step 1   Display the CTC card view.

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

Step 3   In the left column, find the applicable port number and check the **Stp Enabled** check box to enable STP for that port.

Step 4   Click **Apply**.

9.7.2 E-Series Spanning-Tree Parameters

Default spanning-tree parameters are appropriate for most situations. Contact the Cisco Technical Assistance Center (TAC) before you change the default STP parameters. To obtain a directory of toll-free Cisco TAC telephone numbers for your country, refer to the *Cisco ONS 15454 SDH Product Overview* preference section.

From the node view, click the **Maintenance > Etherbridge > Spanning Trees** tabs to view spanning-tree parameters. Table 9-10 describes spanning-tree parameters.

Table 9-10   Spanning-Tree Parameters

Parameter	Description
BridgeID	ONS 15454 SDH 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 SDH 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.

9.7.3 E-Series Spanning-Tree Configuration

To view the spanning-tree configuration, from the node view click the **Provisioning** > **Etherbridge** tabs. Table 9-11 describes spanning-tree configurations.

Table 9-11   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

9.7.4 E-Series Spanning-Tree Map

The Circuit window shows forwarding spans and blocked spans on the spanning-tree map. To view the E-Series Spanning-Tree Map, on the circuit window (Figure 9-24), double-click an Ethernet circuit.

Figure 9-24   Spanning-tree map on the circuit window
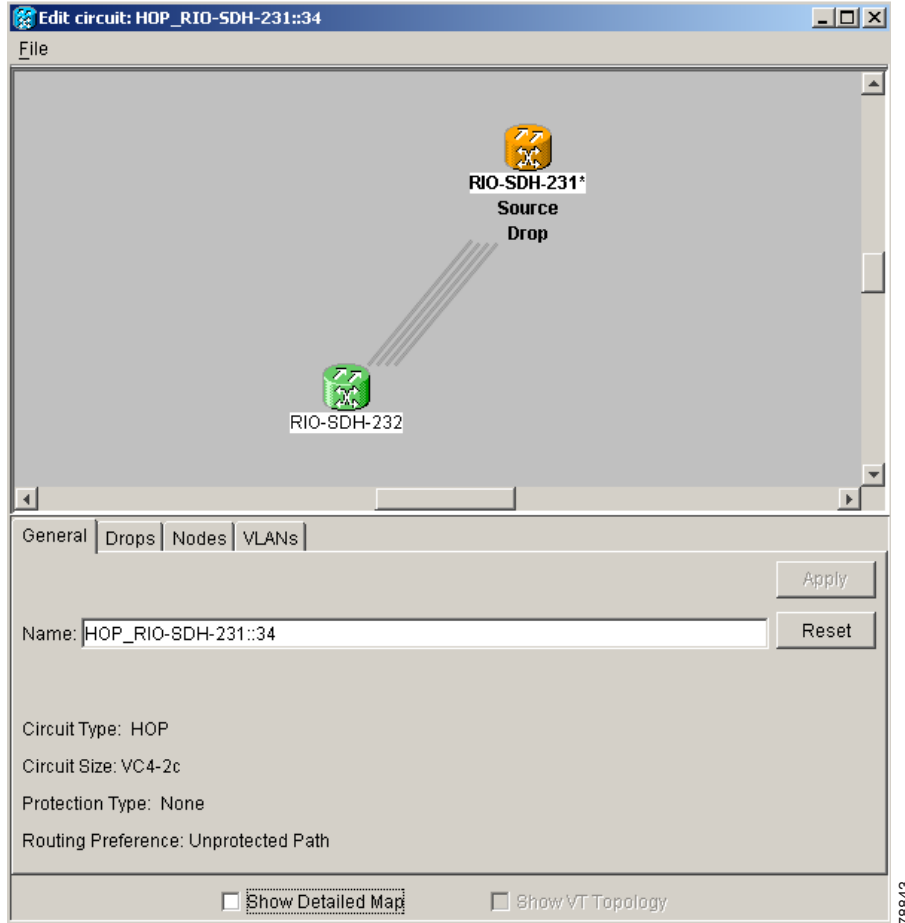
Note   Green represents forwarding spans and purple represents blocked (protect) spans. If you have a packet ring configuration, at least one span should be purple.

9.8 G1000-4 Performance and Maintenance Windows

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 "E-Series Spanning-Tree Parameters" section on page 9-44.

9.8.1 G1000-4 Ethernet Performance Window

CTC provides Ethernet performance information that includes line-level parameters, the amount of port bandwidth used, and historical Ethernet statistics.

9.8.1.1 Statistics Window

The Ethernet statistics window lists Ethernet parameters at the line level. Display the CTC card view for the Ethernet card and click the **Performance > Statistics** tabs to display the window. Figure 9-25 shows the G1000-4 Statistics window. Table 9-12 describes the buttons and drop-down menu in the window. Table 9-13 lists the Ethernet performance monitoring (PM) parameters along with definition of each PM.

Figure 9-25   G1000-4 Statistics window
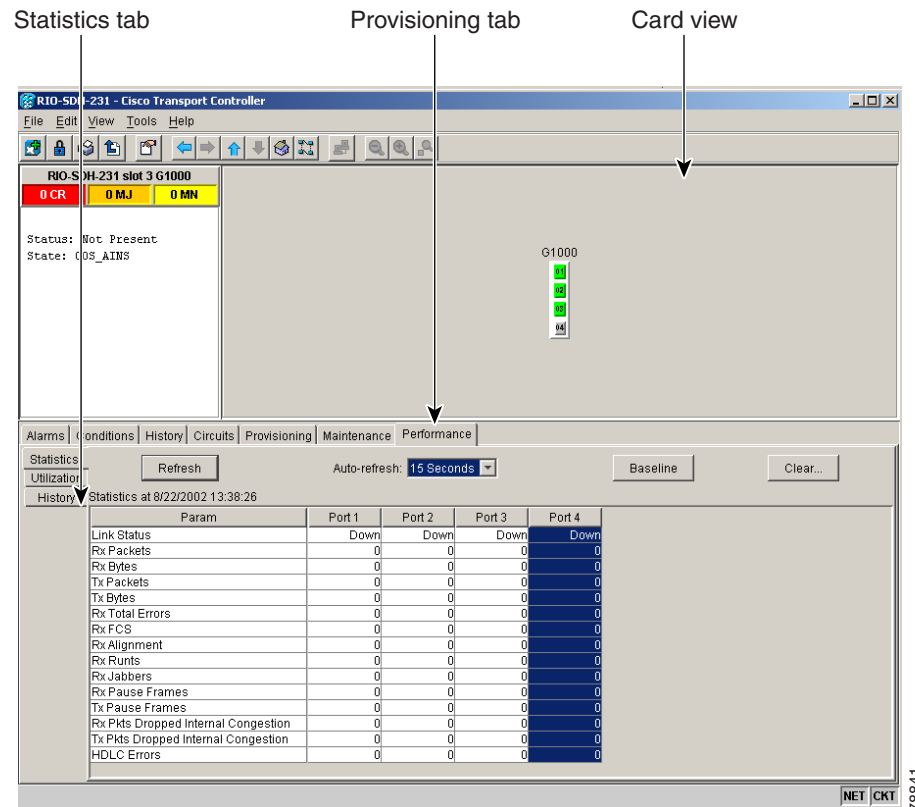
Table 9-12   G1000-4 Statistics Values

Item	Description
Baseline	Clicking Baseline temporarily resets the software counters (in that particular CTC client only) to zero without effecting the actual statistics on the card. From that point on, only the change (delta) in counters is displayed by this CTC. These new baselined counters display only as long as the user displays the Performance pane. If the user navigates to another pane and comes back to the Performance pane, the actual statistics retained by the card display.
Refresh	Manually refreshes the statistics.
Auto-Refresh	Sets a time interval for the automatic refresh of statistics.
Clear	Resets the actual counters on the card to zero; this change is recognized by all management clients.

Note   The CTC automatically refreshes the counter values one time directly after a Baseline operation. If traffic is flowing during a baseline operation, some traffic counts might immediately be observed instead of zero counts.

Note   The Clear button does not cause the G1000-4 card to reset. Provisioning, enabling, or disabling a G1000-4 port does not reset the statistics.

Note   You can apply both the Baseline and the Clear functions to a single port or all ports on the card. To apply Baseline or Clear to a single port, click the port column to highlight the port and click the **Baseline** or **Clear** button.

Table 9-13   Ethernet Parameters

Parameter	Meaning
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; 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	The total number of frames received that are less than 64 bytes in length and have a CRC error.
Rx Jabbers (G-series only)	The total number of frames received that are greater than 1548 bytes in length and have a CRC error.
Rx Giants	Number of packets received that are greater than 1548 bytes in length.
Rx Pause Frames (G-series only)	Number of received Ethernet IEEE 802.3x pause frames.
Tx Pause Frames (G-series only)	Number of transmitted IEEE 802.3x pause frames.
Rx Pkts Dropped Internal Congestion (G-series only)	Number of received packets dropped due to overflow in G1000-4 frame buffer.
Tx Pkts Dropped Internal Congestion (G-series only)	Number of transmit queue drops due to drops in the G1000-4 frame buffer.
HDLC errors (G-series only)	HDLC errors received from SONET/SDH (see note).

Note   The HDLC errors counter should not be used to count the number of frames dropped due to HDLC errors because each frame can get fragmented into several smaller frames during HDLC error conditions and spurious HDLC frames can also generate. If these counters are incrementing at a time when there should be no SDH path problems, it may indicate a problem with the quality of the SDH path. For example, an SDH protection switch causes a set of HLDC errors to generate. The actual values of these counters are less relevant than the fact they are changing.

9.8.1.2 Utilization Window

The Utilization subtab shows the percentage of current and past line bandwidth used by the Ethernet ports. Use this procedure to display values shown on the utilization tab.

Step 1   Display the CTC card view and click the **Performance** > **Utilization** tabs to display the window.

Step 2   From the Interval menu, choose a time segment interval. Valid intervals are 1 minute, 15 minutes, 1 hour, and 1 day.

Step 3   Click **Refresh** to update the data.

9.8.1.3 G-Series Utilization Formula

Line utilization is calculated with the following formula:

((inOctets + outOctets) + (inPkts + outPkts) * 20)) * 8 / 100% interval * maxBaseRate * 2

The interval is defined in seconds. The maxBaseRate is defined by raw bits/second in one direction for the Ethernet port (i.e., 1 Gbps). The maxBaseRate is multiplied by 2 in the denominator to determine the raw bit rate in both directions. The maxBaseRates for STM circuits are provided in Table 9-14.

Table 9-14   maxBaseRates for STM circuits

Circuit Type	maxBaseRate
VC4	155000000
VC4-2c	311000000
VC4-4c	622000000

Note   Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

9.8.1.4 History Window

Use the Ethernet History tab to list past Ethernet statistics.

Step 1   Display the CTC card view and click the **Performance** > **History** tab to view the window.

Step 2   Choose the appropriate port from the Line menu and the appropriate interval from the Interval menu.

Step 3 Click **Refresh** to update the data.

9.8.2 G1000-4 Ethernet Maintenance Window

When a G1000-4 card is installed in the ONS 15454 SDH, the Maintenance tab under the CTC card view reveals a Maintenance window with two subtabs: Loopback and Bandwidth. The Loopback window allows you to put an individual G1000-4 port into a Terminal (inward) loopback. The Bandwidth window displays the amount of current STM bandwidth the card is using. Figure 9-26 shows the Maintenance tab. Table 9-15 describes the columns and buttons in the Maintenance tab.

Figure 9-26   G1000-4 Maintenance tab, including Loopback and Bandwidth tabs
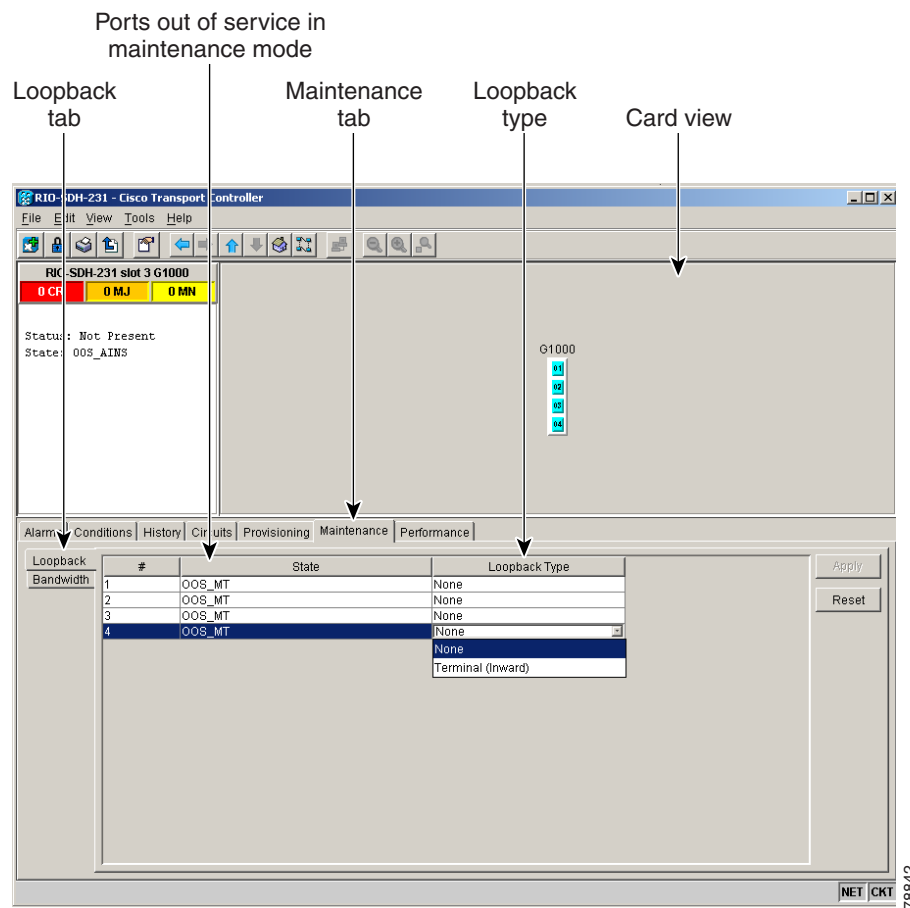
Table 9-15   G1000-4 Maintenance Window Values

Item	Description
Loopback	Displays the Loopback status of the G1000-4 port.
#	Specifies the port number on the G1000-4 card.
Loopback Type	Allows you to configure a port for a Terminal (Inward) loopback or clear the current loopback (none).

Table 9-15   G1000-4 Maintenance Window Values (continued)

Apply	Enables the Loopback configuration on the port.
Bandwidth	Displays the amount of STM bandwidth provisioned for the G1000-4 card.

⚠

Caution   Use Loopback only for the initial test and turn-up of the card and SDH network tests. Do not put the card in Loopback when the G1000-4 ports are in service and attached to a data network. Loopbacks can corrupt the forwarding tables used in data networking.

✎

Note   For more information about using loopbacks with the ONS 15454 SDH, refer to the "Network Tests" section of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

9.8.3 E-Series Ethernet Performance Window

CTC provides Ethernet performance information that includes line-level parameters, the amount of port bandwidth used, and historical Ethernet statistics.

9.8.3.1 Statistics Window

The Ethernet statistics window lists Ethernet parameters at the line level. Table 9-16 defines the parameters. Display the CTC card view for the Ethernet card and click the **Performance > Statistics** tabs to display the window.

The Baseline button resets the statistics values on the Statistics window to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval for automatic refresh of statistics to occur.

The G1000-4 Statistics window also has a Clear button. The Clear button sets the values on the card to zero. Using the Clear button will not cause the G1000-4 to reset.

Table 9-16   Ethernet Parameters

Parameter	Meaning
Link Status	Indicates whether or not 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 FCS error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with alignment errors; alignment errors are received incomplete frames.

Table 9-16   Ethernet Parameters (continued)

Parameter	Meaning
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 (E-series only)	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time causes collisions.
Tx Excessive (E-series only)	Number of consecutive collisions.
Tx Deferred (E-series only)	Number of packets deferred.
Rx Pause Frames (G-series only)	Number of received Ethernet IEEE 802.3x pause frames.
Tx Pause Frames (G-series only)	Number of transmitted IEEE 802.3x pause frames.
Rx Pkts Dropped Internal Congestion (G-series only)	Number of received packets dropped due to overflow in G1000-4 frame buffer.
Tx Pkts Dropped Internal Congestion (G-series only)	Number of transmit que drops due to drops in G1000-4 frame buffer.

9.8.3.2 Line Utilization Window

The Line Utilization window shows the percentage of line, or port, bandwidth used and the percentage used in the past.

Step 1 Display the CTC card view and click the **Performance > Utilization** tabs to display the window.

Step 2 From the Interval menu, choose a time segment interval. Valid intervals are 1 minute, 15 minutes, 1 hour, and 1 day.

Step 3 Click **Refresh** to update the data.

9.8.3.3 E-Series Utilization Formula

Line utilization is calculated with the following formula, see Table 9-17 on page 9-53 for circuit types and the maxBaseRate:

((inOctets + outOctets) + (inPkts + outPkts) * 20)) * 8/100%interval * maxBaseRate * 2

The interval is defined in seconds. The maxBaseRate is defined by raw bits/second in one direction for the Ethernet port (i.e., 1 Gbps). The maxBaseRate is multiplied by 2 in the denominator to determine the raw bit rate in both directions.

Table 9-17   maxBaseRate for STM circuits

Circuit Type	maxBaseRate
VC4	155000000
VC4-2c	311000000
VC4-4c	622000000

Note   Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

9.8.3.4 History Window

The Ethernet History window lists past Ethernet statistics.

Step 1   Display the CTC card view and click the **Performance** tab and **History** subtab to view the window.

Step 2   Choose the appropriate port from the Line menu and the appropriate interval from the Interval menu.

Step 3   Click **Refresh** to update the data. Table 9-16 on page 9-51 defines the listed parameters.

9.8.4 E-Series Ethernet Maintenance Window

Display an E-series Ethernet card in CTC card view and choose the **Maintenance** tab to display MAC address and bandwidth information.

9.8.4.1 MAC Table Window

A MAC address is a hardware address that physically identifies a network device. The ONS 15454 SDH MAC table, also known as the MAC forwarding table, allows you to see all the MAC addresses attached to the enabled ports of an E-series Ethernet card or an E-series 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 SDH and the VLAN, Slot/Port/STM, and circuit that links the ONS 15454 SDH to each MAC address (Figure 9-27).

Figure 9-27   MAC addresses recorded in the MAC table
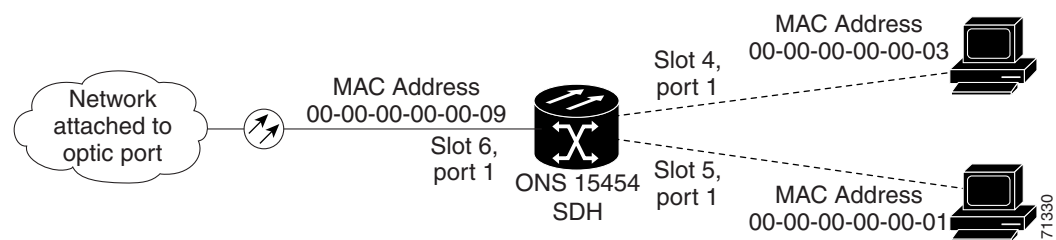
Procedure: Retrieve the MAC Table Information

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 SDH 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.

9.8.4.2 Trunk Utilization Window

The Trunk Utilization window is similar to the Line Utilization window, but Trunk Utilization shows the percentage of circuit bandwidth used rather than the percentage of line bandwidth used.

Step 1   Click the **Maintenance > Ether Bridge > Trunk Utilization** tabs to view the window.

Step 2   Choose a time segment interval from the Interval menu.

> ✎
> **Note**   The percentage shown is the average of ingress and egress traffic.

9.9 Remote Monitoring Specification Alarm Thresholds

The ONS 15454 SDH 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 SDH'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 SDH Troubleshooting and Maintenance Guide*.

Table 9-18 on page 9-55 defines the variables you can provision in CTC. For example, to set the collision threshold, choose **etherStatsCollisions** from the Variable menu.

Table 9-18   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
ifInMulticastPkts	Number of multicast frames received error free
ifInBroadcastPkts	The number of packets, delivered by this sublayer to a higher (sub)layer, that were addressed to a broadcast address at this sublayer
ifInDiscards	The number of inbound packets that were chosen to be discarded, even though no errors had been detected to prevent their being deliverable to a higher-layer 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
ifOutMulticastPkts	Number of multicast frames transmitted error free
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested be transmitted and which packets were addressed to a broadcast address at this sublayer, including those that were discarded or not sent
ifOutDiscards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted
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 FCS test
dot3StatsFCSErrors	Number of frames with framecheck errors, i.e., there is an integral number of octets, but an incorrect 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
dot3StatsCarrierSenseErrors	The number of transmission errors on a particular interface that are not otherwise counted

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

Table 9-18   Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface
etherStatsJabbers	Total number of octets of data (including bad packets) received on the network
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 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 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
receivePauseFrames (G-series only)	The number of received IEEE 802.x pause frames
transmitPauseFrames (G-series only)	The number of transmitted IEEE 802.x pause frames
receivePktsDroppedInternalCongestion (G-series only)	The number of received frames dropped due to frame buffer overflow or other reasons
transmitPktsDroppedInternalCongestion (G-series only)	The number of frames dropped in the transmit direction due to frame buffer overflow or other reasons
txTotalPkts	Total number of transmit packets
rxTotalPkts	Total number of receive packets

Procedure: Create Ethernet RMON Alarm Thresholds

Step 1 From the node view, click the **Provisioning > Etherbridge > Thresholds** tabs.

Step 2 Click **Create**.

The Create Ether Threshold dialog box opens (Figure 9-28).

Figure 9-28 Creating Ethernet RMON thresholds
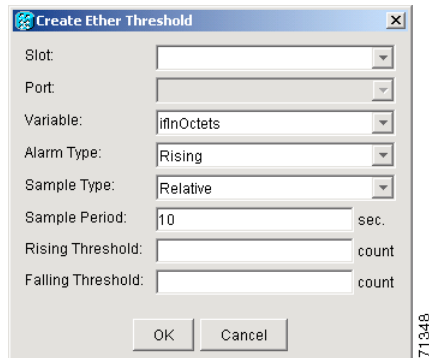
Step 3   In the Slot field, choose the appropriate Ethernet card.

Step 4   In the Port field, choose the appropriate port on the Ethernet card.

Step 5   In the Variable field, choose the variable. Table 9-18 lists and defines the Ethernet threshold variables available in this field.

Step 6   In the Alarm Type field, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 7   In the Sample Type field, 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 8   Type in an appropriate number of seconds in the Sample Period field.

Step 9   Type in the appropriate number of occurrences in the Rising Threshold field.

> **Note**   For a rising type of alarm to be raised, the measured value must move 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 raise an alarm.

Step 10   Type in the appropriate number of occurrences in the Falling Threshold field. 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 large number of events.

Step 11   Click **OK** 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, refer to the Alarm Troubleshooting chapter of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide*.

Table 10-1   Alarm Monitoring and Management Topics

Alarm Monitoring and Management Topics
10.1 Overview, page 10-2
10.2 Viewing ONS 15454 SDH Alarms, page 10-2
10.3 Using Alarm Profiles, page 10-10
10.4 Suppressing Alarms, page 10-16

Table 10-2   Alarm Monitoring and Management Procedures

Alarm Monitoring and Management Procedures
Procedure: View Affected Circuits for a Specific Alarm, page 10-5
Procedure: View Alarm Counts on a Specific Slot and Port, page 10-10
Procedure: Create an Alarm Profile, page 10-11
Procedure: Apply an Alarm Profile at the Card View, page 10-15
Procedure: Apply an Alarm Profile at the Node View, page 10-16
Procedure: Suppress Alarms, page 10-17

10.1 Overview

CTC detects and reports SDH alarms generated by the Cisco ONS 15454 SDH and the larger SDH network. You can use CTC to monitor and manage alarms at card, node, or network levels and view alarm counts on the LCD front panel. Default alarm severities conform to the ITU-T G.783 standard, but you can reset severities to customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard ITU categories employed by ONS nodes, see the *Cisco ONS 15454 SDH Maintenance and Troubleshooting Guide.*

Note   ONS 15454 SDH alarms can also be monitored and managed through a network management system (NMS).

10.2 Viewing ONS 15454 SDH Alarms

At the card, node, or network CTC view, click the **Alarms** tab to display the alarms for that card, node, or network. Table 10-3 lists the tab's column headings and the information recorded in each column. Figure 10-1 shows how to view ONS 15454 SDH alarms in CTC.

Table 10-3   Alarms Column Descriptions

Column	Description
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.)
New	Indicates a new alarm. To change this status, check either the Synchronize Alarms or the Delete Cleared Alarms check box, or reset the active TCC-I 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.
Eqpt 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), or NR (not reported).
ST	Status: R (raised), C (clear), or T (transient).
SA	When checked, indicates a service-affecting alarm.
Cond	The alarm name. These are defined alphabetically in the Alarm Troubleshooting chapter of the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide.*
Description	Description of the alarm.

Figure 10-1   Viewing alarms in the CTC node view

Alarms display in one of five background colors, listed in Table 10-4, 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 10-4   Color Codes for Alarms, Conditions, and Events

Color	Description
Red	Critical Alarm (CR)
Orange	Major Alarm (MJ)
Yellow	Minor Alarm (MN)
Magenta	Condition (NA)
Blue	Condition (NR)
White	Cleared alarm or event (CL)

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

10.2.1 Controlling Alarm Display

You can control the display of the alarms on the Alarms tab. Table 10-5 shows the actions you can perform from the Alarms tab.

Table 10-5   Alarm Display

Button or Check Box	Action
Synchronize button	Causes CTC to retrieve a current alarm summary for the node. This is optional, since CTC updates the Alarms tab automatically as raise/clear messages arrive from the node. It is useful in the case when messages may have been lost.
Delete Cleared Alarms button	Deletes cleared alarms and transient messages from the CTC display when they are not needed for long-term information or later troubleshooting.
Filter button	Filters alarm parameters chosen in the Filter dialog box when alarm filtering is enabled Not enforced when alarm filtering is disabled.
AutoDelete Cleared Alarms check box	If checked, CTC automatically deletes cleared alarms from the display.

10.2.2 Viewing Alarm-Affected Circuits

You can view which ONS 15454 SDH circuits are affected by a specific alarm. Figure 10-2 illustrates the Select Affected Circuits option.

Figure 10-2   Selecting the Affected Circuits option

Procedure: View Affected Circuits for a Specific Alarm

Purpose	This procedure allows you to view affected circuits for a specific alarm
Prerequisite Procedures	ONS 15454 SDH installed and provisioned
Onsite/Remote	Onsite or remote

Step 1   Under the Alarms tab, right-click the row of an active alarm.

The Select Affected Circuit option appears.

Step 2   Click **Select Affected Circuits**.

The Circuits window appears with affected circuits highlighted (Figure 10-3).

Figure 10-3   Highlighted (selected) circuit

10.2.3 Using the Conditions Tab

The Conditions tab displays retrieved fault conditions. A fault is a problem detected by ONS 15454 SDH 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 or not this particular fault currently exists on the ONS 15454 SDH. Fault conditions include all existing conditions, whether the severity is that of an alarm (Critical, Major or Minor) or a condition (Not Reported or Not Alarmed). See the trouble notifications information in the *Cisco ONS 15454 SDH Troubleshooting and Maintenance Guide* for more information about the classifications for alarms and conditions.

Displaying all existing fault conditions is helpful while troubleshooting the ONS 15454 SDH. The Conditions tab does not adhere to ITU guidelines for reporting alarms, events, and conditions. Alarm reporting under the Alarms tab is ITU-compliant.

10.2.3.1 Retrieving and Displaying Conditions

At the node view, click the **Conditions** tab and the **Retrieve Conditions** button to retrieve the current set of all existing fault conditions from the ONS 15454 SDH, as maintained by the alarm manager. Figure 10-4 illustrates the fault conditions retrieved under the Conditions tab. 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 tab

10.2.3.2 Conditions Column Descriptions

Table 10-6 lists the tab's column headings and the information recorded in each column.

Table 10-6   Conditions Column Descriptions

Column	Information Recorded
Date	Date and time of the alarm
Node	Node where the condition occurred (displays in network view only)
Object	TL1 access identifier (AID) for the alarmed object
Eqpt Type	Card type in this slot

Table 10-6   Conditions Column Descriptions (continued)

Column	Information Recorded
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), or NR (not reported)
SA	When checked, indicates a service-affecting alarm
Cond	The condition name
Description	Description of the condition

10.2.4 Controlling Conditions Display

You can control the display of the conditions on the Conditions tab. Table 10-7 shows the actions you can perform from the Conditions tab.

Table 10-7   Conditions Display

Button or Check Box	Action
Retrieve button	Retrieves all conditions as maintained by the alarm manager.
Filter button	Filters alarm parameters chosen in the Filter dialog box when alarm filtering is enabled. Not enforced when alarm filtering is disabled.
Exclude Same Root Cause check box	If checked, allows conditions that are caused by the same event (such as AIS, which accompanies many alarms such as LOS) to be excluded from display.

10.2.5 Viewing History

The History tab displays historical alarm message data. It also displays event messages, 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 History > Session tab presents alarm messages and event messages that have occurred during the current CTC session.

- The History > Node tab shows the alarm messages that have occurred on the node since CTC installation (Figure 10-5) and alarm messages that have occurred for the current login session (Figure 10-6). A summary of alarm messages and event messages can also be shown. The ONS 15454 SDH can store up to 640 critical alarm raise/clear messages, 640 major alarm raise/clear messages, 640 minor alarm raise/clear messages, and 640 event-level raise/clear/transient messages. When any of these limits is reached, the ONS 15454 SDH discards the oldest alarms and events in that category.

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

Figure 10-5   Viewing node alarms reported since CTC software installation

Figure 10-6   Viewing alarms for the CTC session
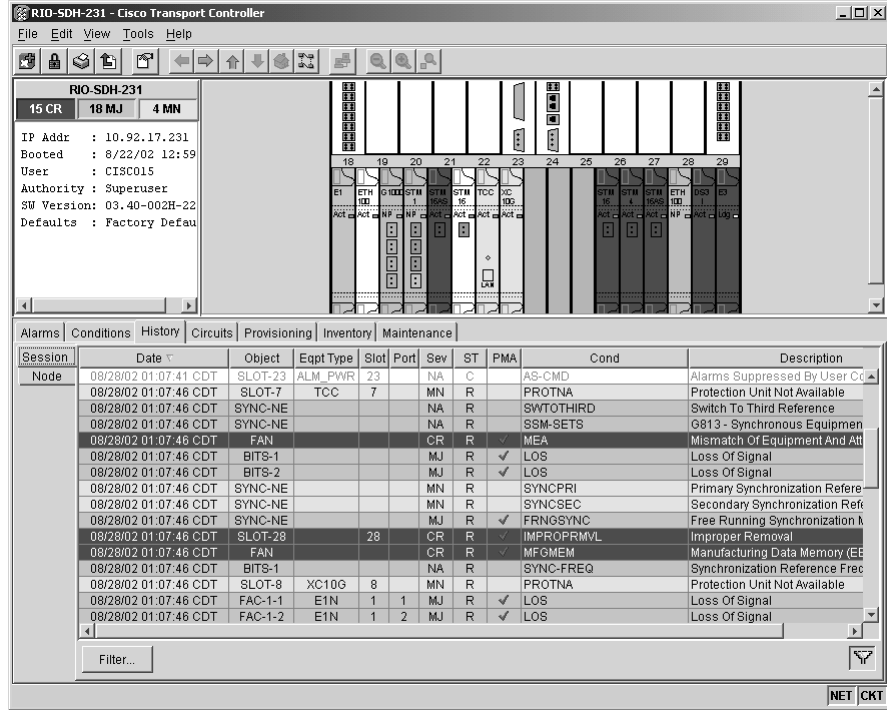
10.2.6 Viewing Alarms on the LCD

The Critical, Major, and Minor alarm LEDs on the fan-tray assembly front panel indicate whether a critical, major, or minor alarm exists on the ONS 15454 SDH. These LEDs are viewable through the front door so that you can quickly determine whether 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 10-7 illustrates the LCD panel.

Figure 10-7   Front LCD panel
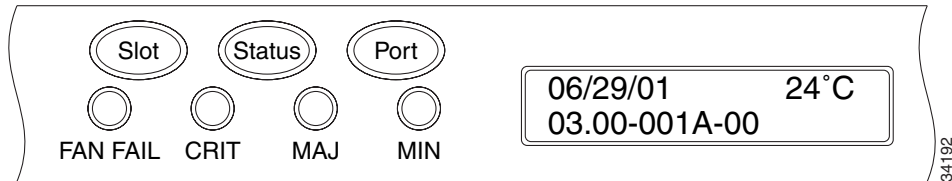
Procedure: View Alarm Counts on a Specific Slot and Port

Purpose	View alarm counts on a specific slot and port
Tools/Equipment	Computer, configured for CTC
Prerequisite Procedures	ONS 15454 SDH operational; CTC running
Onsite/Remote	Onsite or remote

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 10-7 shows the LCD panel.

10.3 Using Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15454 SDH 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 ITU-T G.783 settings, and the Inherited profile, which sets all alarm severities to transient (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 10-8). A default alarm profile (in the Default column) is preprovisioned for every alarm. Default alarm profiles are loaded clicking Node/Profile Ops > Load > From Node > Default > OK. 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 10-8   Alarm profiles window showing the alarm type conditions of the listed alarms
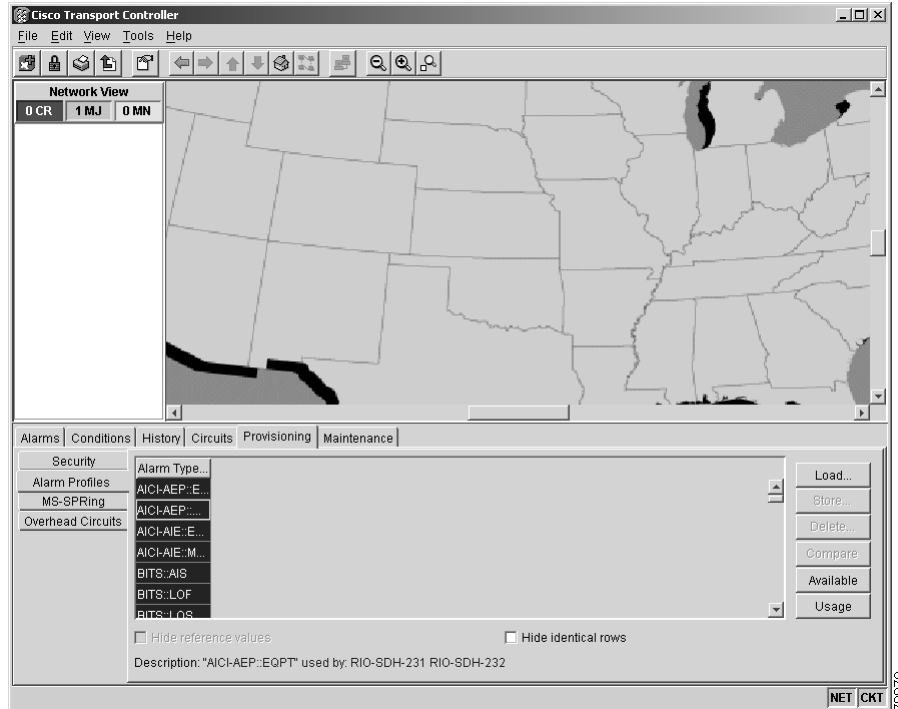
Procedure: Create an Alarm Profile

Purpose	Create alarm profile
Tools/Equipment	Computer, configured for CTC
Prerequisite Procedures	ONS 15454 SDH operational; CTC running
Onsite/Remote	Onsite or remote

Step 1   Display the CTC network view.

Step 2   Click the **Provisioning > Alarm Profiles** tabs.

Step 3   To load a stored profile from another node:

   a.   Click **Load**.

   b.   Highlight the node name you are logged into under Node Names and highlight **Default** under Profile Names.

   c.   Click **OK**.

Step 4   To create a new profile by cloning the default profile:

   a.   Right-click anywhere in the Default column to display the Profile Editing shortcut menu.

   b.   Choose **Clone** from the shortcut menu. (You can also clone any other profiles that appear under the Available button, except Inherited.)

   c.   In the Clone Profile Default dialog box, enter a name in the *New Profile Name* field.

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

d. Click **OK**.

A new alarm profile (named inStep c) is created. This profile duplicates the severities of the default profile and is added as a new column on the far right side.

Step 5 Modify the alarm profile to customize it.

a. In the new alarm profile column, click a row that contains the alarm severity you want to change.

b. From the drop-down list, 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 **Store**.

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 in the Available dialog box. Click **Available** to access the dialog box.

Note   The Alarm Profile is not effective on the node until selected in the node view Provisioning > Alarm Behavior tab Node Profile drop-down list, or on a card until it is selected in the slot drop-down list.

10.3.2 Alarm Profile Menus

The Alarm Profiles tab displays six alarm profile buttons. Table 10-8 lists and describes each of the alarm profile buttons.

Table 10-8   Alarm Profile Buttons

Button	Description
Load	Loads a profile to a node or a file
Store	Saves profiles on a node (or nodes) or in a file
Delete	Deletes profiles from a node
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

10.3.3 Alarm Profile Editing

Table 10-9 lists and describes the five profile editing options available when you right-click in an alarm profile column.

Table 10-9   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

10.3.4 Alarm Severity Option

You change or assign alarm severity using a menu. To view this menu, click the alarm you want to change in its alarm profile column. Seven severity levels appear in a drop-down list for the alarm:

- CR: Critical
- MJ: Major
- MN: Minor
- NR: Not reported
- NA: Not alarmed
- TR: Transient
- UNSET: Unset/Unknown (not normally used)

Transient and Unset only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

10.3.5 Row Display Options

In addition to check boxes displayed in the Alarm Profile tabs, the Alarm Behavior tab displays two check boxes at the bottom of the screen: Hide reference values and Hide identical rows. The Hide reference values check box highlights alarms with nondefault severities by clearing alarm cells with default severities. The Hide identical rows check box hides rows of alarms that contain the same severity for each profile.

10.3.6 Applying Alarm Profiles

In CTC card view, the Alarm Behavior tab displays the alarm profiles of the selected card. In node view, the Alarm Behavior tab displays alarm profiles for the node. A node-level alarm profile applies to all cards in the node except those that have their own profiles. Many card-level alarm profiles apply to all ports on the card, except for those that have their own profiles.

At the node level, you can apply profile changes on a card-by-card basis or set a profile for the entire node. Figure 10-9 shows the profile of an STM-4 card being changed to Inherited at the node view.

Figure 10-9   Node view of an STM-4 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 10-10 shows the affected STM-4 card; notice that the CTC shows Parent Card Profile: Inherited.

Figure 10-10 Card view of an STM-4 alarm profile
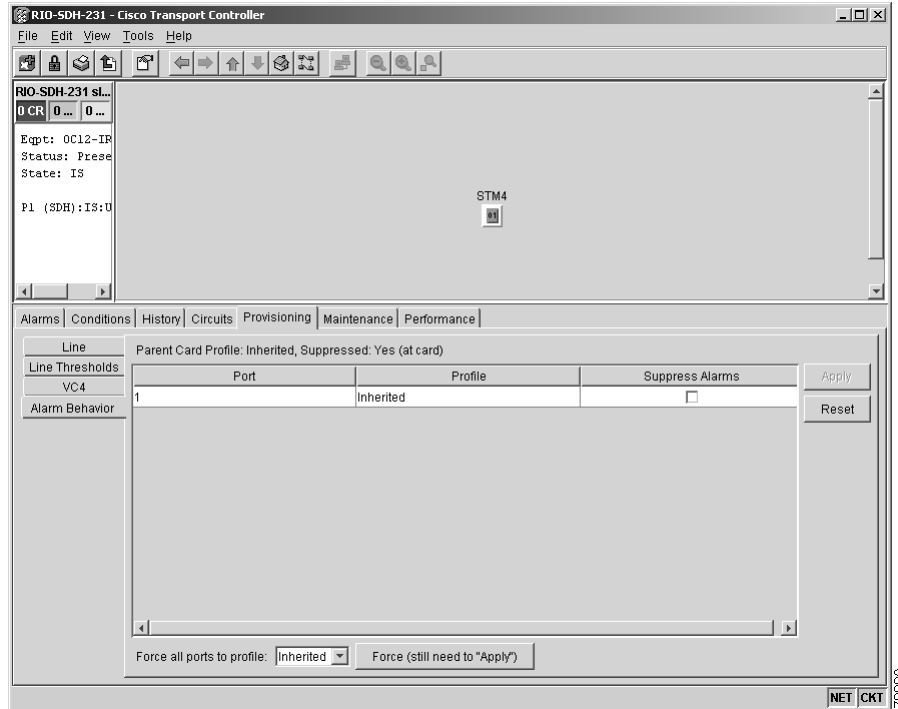
Procedure: Apply an Alarm Profile at the Card View

Purpose	Apply alarm profile at card view
Tools/Equipment	Computer, configured for CTC
Prerequisite Procedures	ONS 15454 SDH operational; CTC running
Onsite/Remote	Onsite or remote

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-by-port basis:

    a. Click the appropriate row under the Profile column for the port desired.

    b. Choose the appropriate profile from the drop-down list.

    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 from the drop-down list.

    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

Purpose	Apply alarm profile at node view
Tools/Equipment	Computer, configured for CTC
Prerequisite Procedures	ONS 15454 SDH operational; CTC running
Onsite/Remote	Onsite or remote

Step 1   In CTC, display the node view.

Step 2   Click the **Provisioning > Alarm Behavior** tabs.

Step 3   To apply profiles on a card basis:

   a.   Click the Profile column for the card desired.

   b.   Choose the appropriate profile from the drop-down list.

   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 from the drop-down list.

   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 not-reported (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 sessions are open, you will suppress the alarms in all other open sessions.

Procedure: Suppress Alarms

Purpose	Suppressing alarms
Tools/Equipment	Computer, configured for CTC
Prerequisite Procedures	ONS 15454 SDH operational; CTC running
Onsite/Remote	Onsite or remote

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 for the entire node.

Step 2 Check the *Suppress Alarms* check box in the row of the card or port you want to suppress. Figure 10-11 shows the Suppress Alarms column check box for cards.

Figure 10-11 Suppress Alarms check box

Step 3 Click **Apply**.

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

Note When you uncheck the Suppress Alarms check box and click Apply, the node sends out autonomous messages to raise any actively suppressed alarms.

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454 SDH.

Table 11-1   SNMP Topics

SNMP Topics
11.1 SNMP Overview, page 11-1
11.2 SNMP Basic Components, page 11-2
11.3 SNMP Support, page 11-3
11.4 SNMP Management Information Bases, page 11-5
11.5 SNMP Traps, page 11-6
11.6 SNMP Community Names, page 11-8
11.7 SNMP Remote Network Monitoring, page 11-9

Table 11-2   SNMP Procedure

SNMP Procedure
Procedure: Set Up SNMP Support, page 11-3

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 SDH 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 electrical, SDH, and Ethernet technologies. SNMP allows limited management of the ONS 15454 SDH by a generic SNMP manager, for example HP OpenView Network Node Manager (NNM) or Open System Interconnection (OSI) NetExpert.

The Cisco ONS 15454 SDH 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 SDH. Figure 11-1 illustrates a basic network managed by SNMP.

Figure 11-1   Basic network managed by SNMP
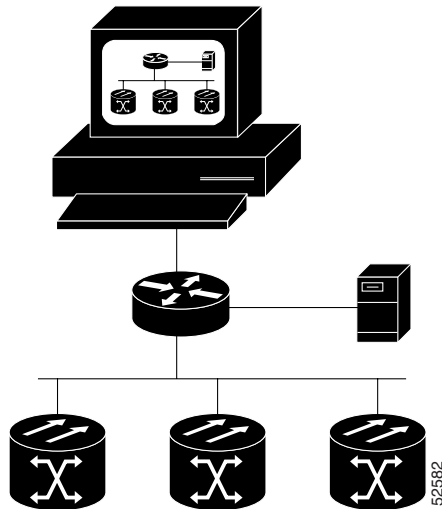
11.2 SNMP Basic Components

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 SDH.

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   SNMP agent gathering data from an MIB and sending traps to the manager
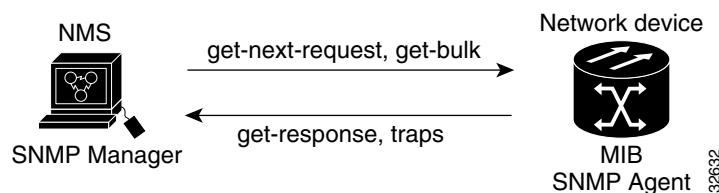
A management system such as HP OpenView executes applications that monitor and control managed devices. Management systems provide the bulk of the processing and memory resources required for network management. One or more management systems must exist on any managed network. Figure 11-3 illustrates the relationship between the three key SNMP components.

Figure 11-3   Primary SNMP components

Managed Devices
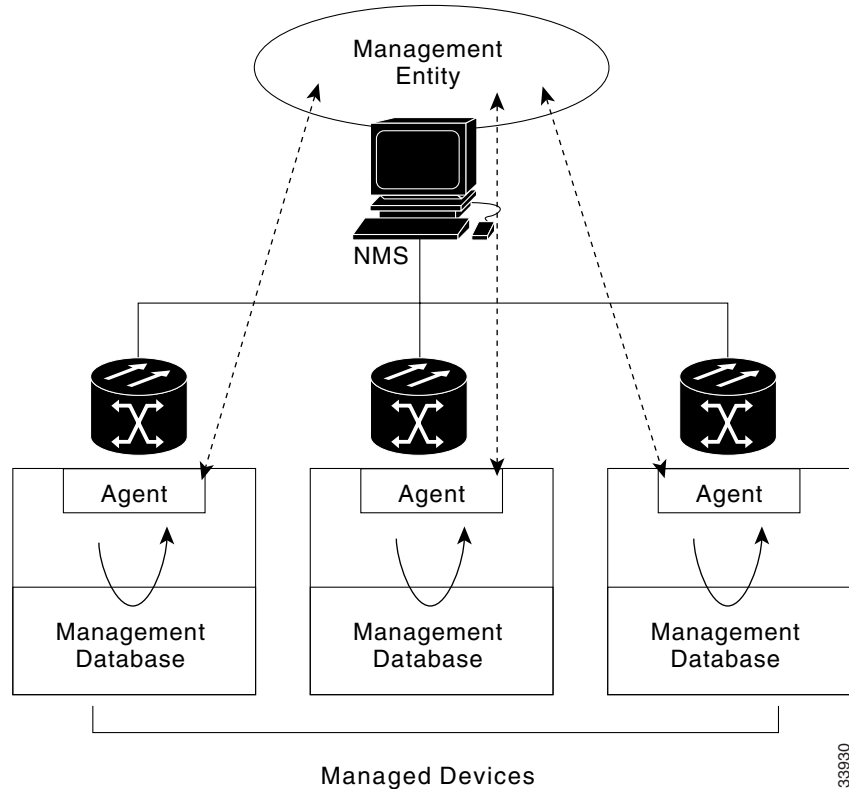
11.3 SNMP Support

The ONS 15454 SDH supports SNMPv1 and SNMPv2c traps and get requests. The SNMP MIBs in the ONS 15454 SDH 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 SDH multiplexers.

Purpose	Use this procedure to set up SNMP trap support on the ONS 15454 SDH
Tools/Equipment	—
Prerequisite Procedures	—
Onsite/Remote	Onsite/Remote

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 window.

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 to either **SNMPv1** or **SNMPv2**.

Refer to your NMS documentation to determine whether to use SNMP version 1 (v1) or SNMP version 2 (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 window (Figure 11-5).

Figure 11-5   Viewing trap destinations
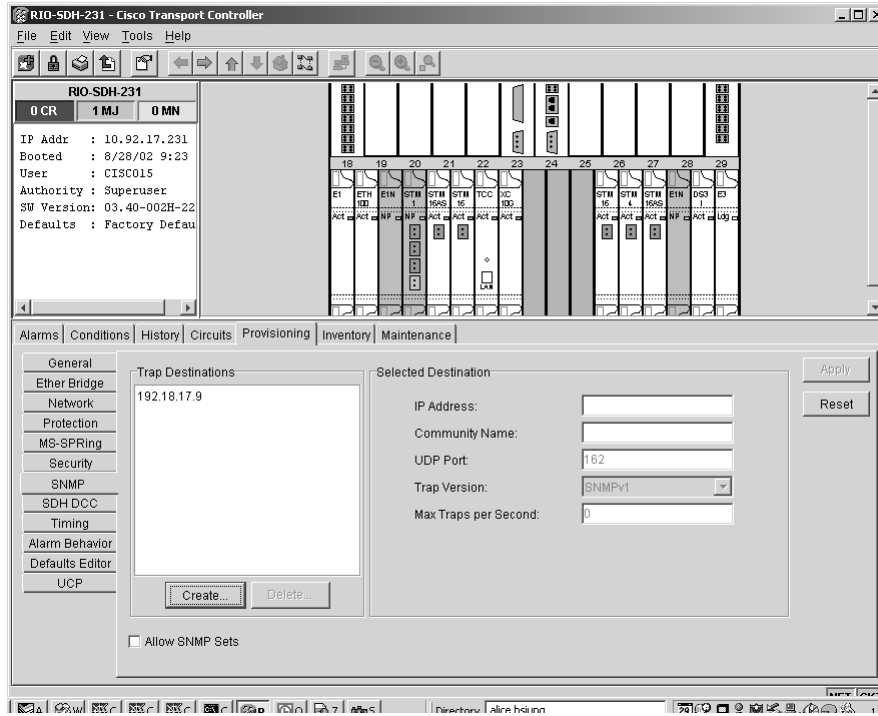
11.4 SNMP Management Information Bases

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 SDH SNMP agent communicates with an SNMP management application using SNMP operations. Table 11-3 describes these messages.

Table 11-3   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 11-3   SNMP Message Types (continued)

Operation	Description
get-bulk-request	Similar to a get-next-request, but fills the get-response with up to the max-repetition number of get-next interactions.
trap	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). Table 11-4 lists the IETF standard MIBs implemented in the ONS 15454 SDH SNMP agent.

The ONS 15454 SDH MIBs are included on the software CD that ships with the ONS 15454 SDH. 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 SDH MIBs, call the Technical Assistance Center (TAC). To obtain a directory of toll-free Cisco TAC telephone numbers for your country, refer to the *Cisco ONS 15454 SDH Product Overview* preference section.

Table 11-4   IETF Standard MIBs Implemented in the ONS 15454 SDH SNMP Agent

RFC#	Module Name	Title/Comments
1213 +1907	RFC1213-MIB, SNMPV2-MIB	MIB-II from RFC1213 with enhancement from RFC1907 for SNMPv2
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 SDH can receive SNMP requests from a number of SNMP managers and send traps to eleven trap receivers. The ONS 15454 SDH generates all alarms and events as SNMP traps.

The ONS 15454 SDH 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 SDH also generates a trap for each alarm when the alarm condition clears.

Each SNMP trap contains eleven variable bindings for the ONS 15454 SDH, listed in Table 11-5.

Table 11-5   SNMP Trap Variable Bindings for ONS 15454 SDH

Number	Name	Description
1	cerent454AlarmTable	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	cerent454AlarmIndex	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	cerent454AlarmObjectType	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	cerent454AlarmSlotNumber	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	cerent454AlarmPortNumber	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	cerent454AlarmLineNumber	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	cerent454AlarmObjectIndex	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	cerent454AlarmType	This variable provides the exact alarm type.
9	cerent454AlarmState	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	cerent454AlarmTimeStamp	This variable gives the time when the alarm occurred. The value is the number of ticks that has lapsed since 1/1/1970.
11	cerent454AlarmObjectName	This variable gives the TL1-style user-visible name which uniquely identifies an object in the system.

The ONS 15454 SDH supports the generic and IETF traps listed in Table 11-6.

Table 11-6   Traps Supported in the ONS 15454 SDH

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 (extended 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 (extended 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 SDH incorporates RMON to allow network operators to monitor the Ethernet cards. For more information on Ethernet RMONs, see the "Remote Monitoring Specification Alarm Thresholds" section on page 9-54. 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. CTC also monitors the five RMON groups implemented by the ONS 15454 SDH.

ONS 15454 SDH RMON implementation is based on the IETF-standard MIB Request for Comment (RFC)1757. The ONS 15454 SDH 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 SDH 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 SDH implements the logTable as specified in RFC 1757.

Circuit Routing

This appendix provides an in-depth explanation of ONS 15454 SDH circuit routing and VC low-order path tunneling in mixed protection or meshed environments, such as the network shown in Figure A-1. For circuit creation and provisioning procedures, see Chapter 6, "Circuits and Tunnels."

Figure A-1   Multiple protection domains
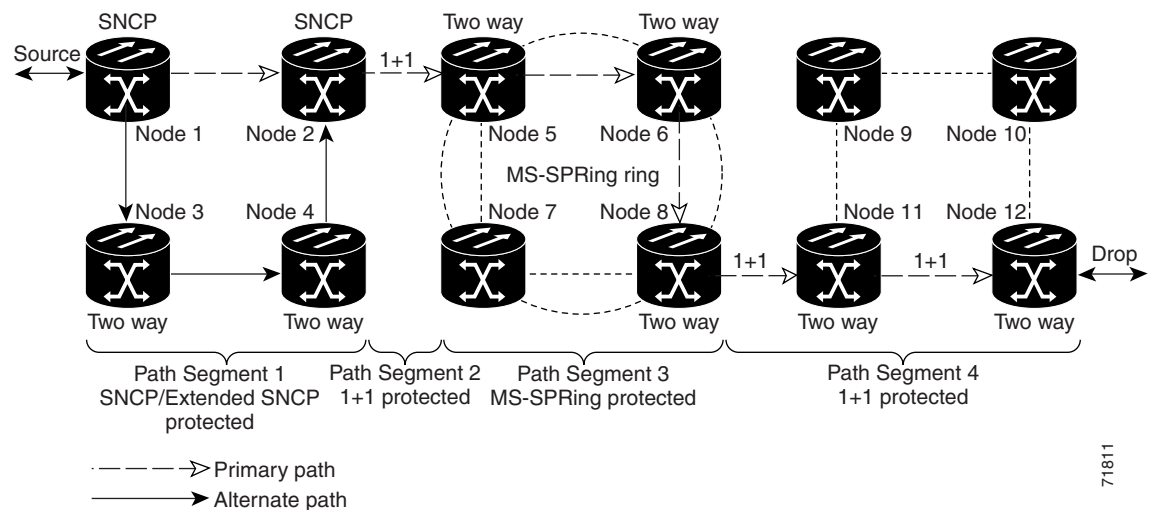
Automatic Circuit Routing

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 SNCP fashion. Each path segment is a separate protection domain, and each protection domain is protected in a specific fashion (virtual SNCP, MS-SPRing, or 1+1).

Circuit Routing Characteristics

The following list provides principles and characteristics of automatic circuit routing:

- Circuit routing tries to use the shortest path within the user-specified or network-specified constraints. VC low-order path tunnels are preferable for VC high-order path circuits because VC low-order path tunnels are considered shortcuts when CTC calculates a circuit path in extended SNCP mesh networks.

- If you do not choose the Fully Protected Path option 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.

- For 1+1 and MS-SPRing, if a link is down, a fully protected circuit will be provisioned. The working route uses the link that is up (short or long path), and the protect route uses the link that is down. SNCP circuit routing will not use links that are down. If you want all links to be considered for routing while creating an SNCP ring, 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.

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 MS-SPRing.

If CTC cannot find a link that meets these requirements, it displays an error.

The same logic applies to VC high-order path circuits on VC low-order path tunnels. Circuit routing typically favors VC low-order path tunnels because, based on topology maintained by circuit routing, VC low-order path tunnels are shortcuts between a given source and destination. If the VC low-order path tunnel in the route is full (no more bandwidth), CTC asks whether you want to create an additional VC low-order path 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 15454 SDHs.

Figure A-2   Secondary sources and drops
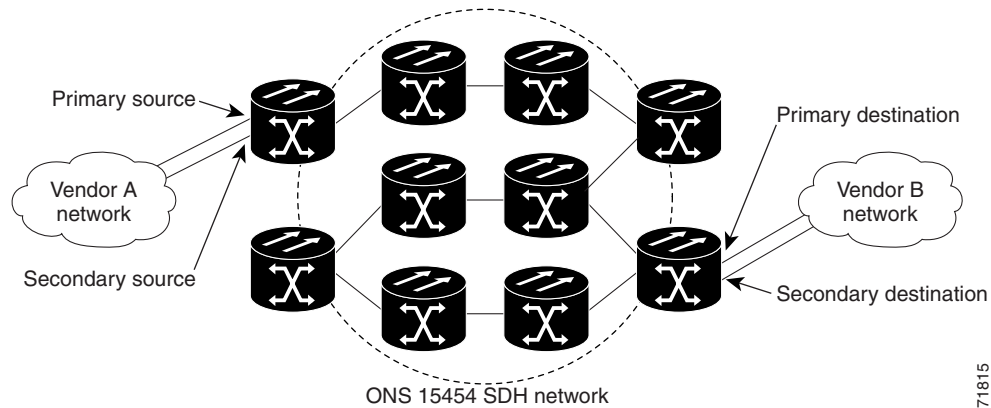
Several rules apply to secondary sources and drops:

- 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.
- Secondary sources and destinations are permitted only for regular VC connections (not for VC low-order path tunnels and Multicard EtherSwitch circuits).
- For point-to-point (straight) Ethernet circuits, only SDH VC4 endpoints can be specified as multiple sources or drops.

For bidirectional circuits, CTC creates an SNCP connection at the source node that allows traffic to be selected from one of the two sources on the ONS 15454 SDH network. If you check the Fully Protected Path option during circuit creation, traffic is protected within the ONS 15454 SDH network. At the destination, another SNCP connection is created to bridge traffic from the ONS 15454 SDH 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, an SNCP 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 VC 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 SNCP segments.

CTC imposes the following rules on manual routes:

- You cannot create manual low-order path circuits (DS3i or E3 cards).
- 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 on page A-1).

- If you enabled the Fully Protected Path option, choose a diverse protect (alternate) path for every unprotected segment (see Figure A-3). The dashed line with the white arrowhead shows the primary path and the solid lines with the black arrowhead shows the alternate path.

Figure A-3   Alternate paths for virtual SNCP segments
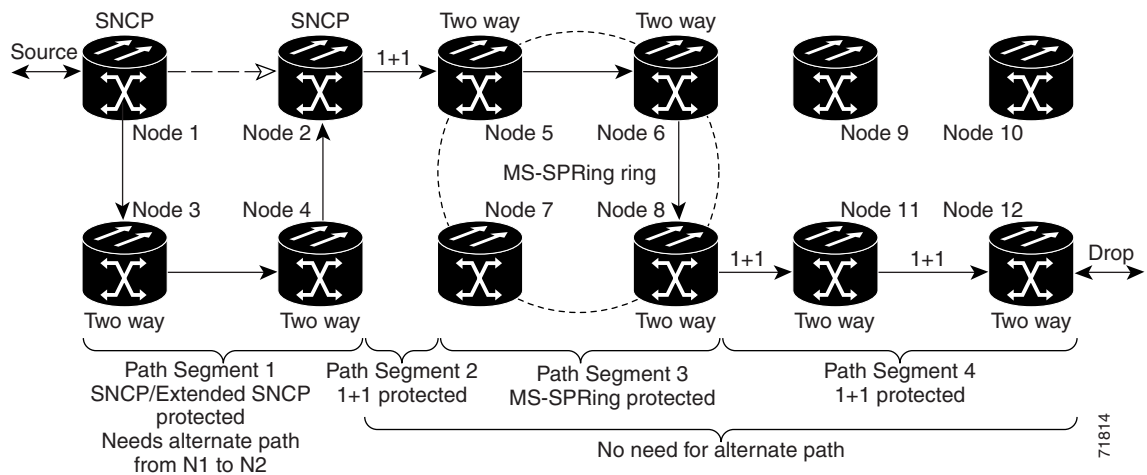
- For Multicard EtherSwitch circuits, the Fully Protected Path option is ignored. Each high-order path circuit must be manually selected to complete a packet ring.

- For a node that has an SNCP selector based on the links chosen, the input links to the SNCP selectors cannot be 1+1 or MS-SPRing protected (see Figure A-4 on page A-5). The same rule applies at the SNCP bridge.

Note   The dashed line with the white arrowhead shows the primary path and the solid lines with the black arrowhead shows the alternate path.

Figure A-4   Mixing 1+1 or MS-SPRing protected links with an SNCP
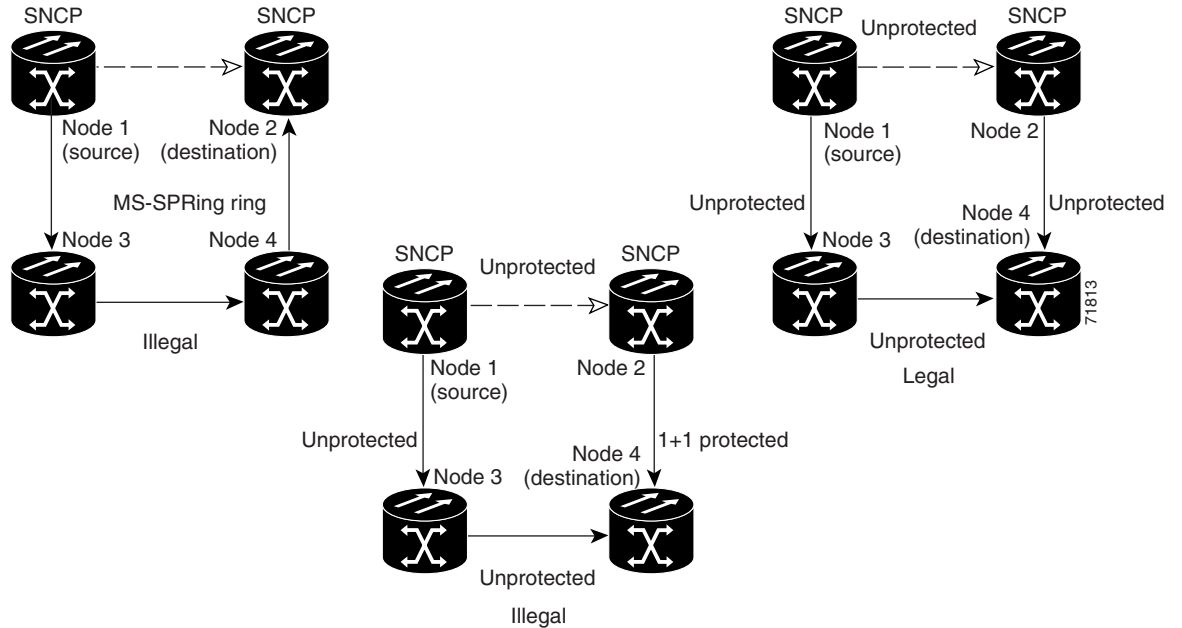
- Choose the links of Multicard EtherSwitch circuits in a shared packet ring to route from source to destination and back to source (see Figure A-5). Otherwise, a route (set of links) chosen with loops is invalid.

Figure A-5   Ethernet shared packet ring routing
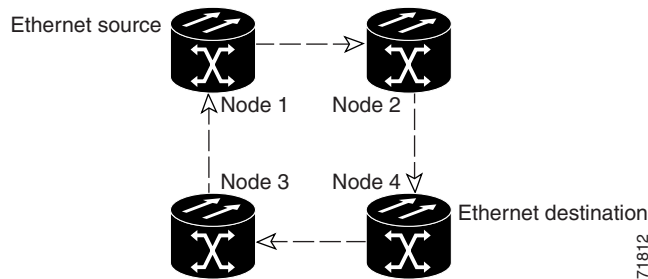
- Multicard EtherSwitch circuits can have virtual SNCP segments if the source or destination is not in the SNCP domain. This restriction also applies after circuit creation; therefore, if you create a circuit with SNCP segments, Ethernet node drops cannot exist anywhere on the SNCP segment (see Figure A-6 on page A-6).

Note   The dashed line with the white arrowhead shows the primary path and the solid lines with the black arrowhead shows the alternate path.

Figure A-6   Ethernet and SNCP
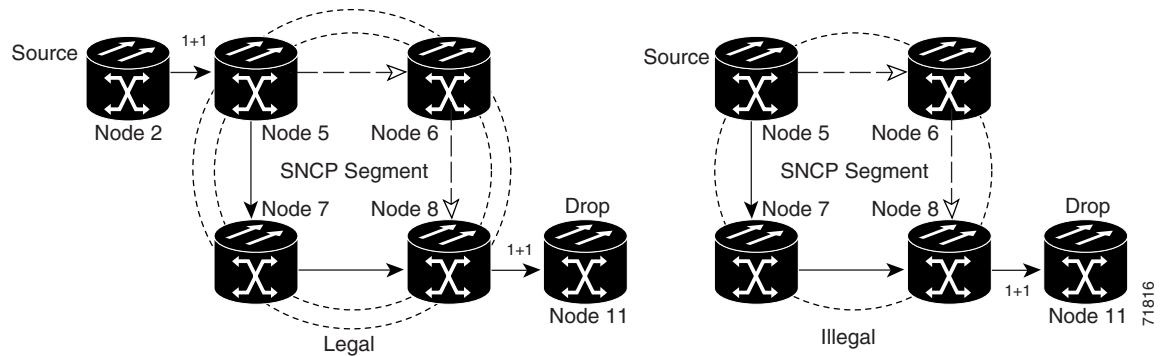
- VC low-order path tunnels cannot be an endpoint of an SNCP segment. An SNCP segment endpoint is where the SNCP selector resides.

If the Fully Protected Path option 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.

Table A-1, Table A-2, Table A-3, and Table A-4 summarize the available node connections. Any other combination is invalid and will generate an error.

Table A-1   Bidirectional VC/Regular Multicard EtherSwitch/Point-to-Point (straight) Ethernet Circuits

No. of Inbound Links	No. of Outbound Links	No. of Sources	No. of Drops	Connection Type
—	2	1	—	SNCP
2	—	—	1	SNCP
2	1	—	—	SNCP
1	2	—	—	SNCP
1	—	—	2	SNCP
—	1	2	—	SNCP
2	2	—	—	Double SNCP
2	—	—	2	Double SNCP
—	2	2	—	Double SNCP
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 VC Circuit

No. of Inbound Links	No. of Outbound Links	No. of Sources	No. of Drops	Connection Type
1	1	—	—	One way
1	2	—	—	SNCP head end

Table A-2   Unidirectional VC Circuit (continued)

No. of Inbound Links	No. of Outbound Links	No. of Sources	No. of Drops	Connection Type
—	2	1	—	SNCP head end
2	—	—	1+	SNCP drop and continue

Table A-3   Multicard Group Ethernet Shared Packet Ring Circuit

No. of Inbound Links	No. of Outbound Links	No. of Sources	No. of Drops	Connection Type
At intermediate nodes only				
2	1	—	—	SNCP
1	2	—	—	SNCP
2	2	—	—	Double SNCP
1	1	—	—	Two way
At source or destination nodes only				
1	1	—	—	Ethernet

Table A-4   Bidirectional VC Low-Order Path Tunnels

No. of Inbound Links	No. of Outbound Links	No. of Sources	No. of Drops	Connection Type
At intermediate nodes only				
2	1	—	—	SNCP
1	2	—	—	SNCP
2	2	—	—	Double SNCP
1	1	—	—	Two way
At source nodes only				
—	1	—	—	VC low-order path tunnel end point
At destination nodes only				
1	—	—	—	VC low-order path tunnel end point

Although virtual SNCP segments are possible in VC low-order path tunnels, VC low-order path tunnels are still considered unprotected. If you need to protect VC high-order path circuits, either use two independent VC low-order path tunnels that are diversely routed or use a VC low-order path tunnel that is routed over only 1+1 or MS-SPRing links (or a mix of both link types).

Constraint-Based Circuit Routing

When you create circuits, you can choose the Fully Protected Path option to protect the circuit from source to destination. The protection mechanism used depends on the path that CTC calculates for the circuit. If the network is comprised entirely of MS-SPRing and/or 1+1 links, or the path between source and destination can be entirely protected using 1+1 and/or MS-SPRing links, no extended SNCP mesh network (virtual SNCP) protection is used.

If virtual SNCP (extended SNCP mesh network) protection is needed to protect the path, set the level of node diversity for the extended SNCP mesh network portions of the complete path on the Circuit Creation dialog box.

- Nodal Diversity Required—Ensures that the primary and alternate paths of each extended SNCP mesh network domain in the complete path have a diverse set of nodes.

- Nodal Diversity Desired—CTC looks for a node diverse path; if a node diverse path is not available, CTC finds a link diverse path for each extended SNCP mesh network domain in the complete path.

- Link Diversity Only—Creates only a link diverse path for each extended SNCP mesh network 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 used less. By selecting a required node and/or a link, you force CTC to use (or not use) an element, resulting in more efficient 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 extended SNCP mesh network domains/segments. The alternate path is computed normally; CTC uses excluded nodes/links when finding all primary and alternate paths on extended SNCP mesh networks.

A P P E N D I X   **B**

Regulatory Compliance and Safety Information

Regulatory Compliance

The ONS 15454 SDH meets the regulatory compliance and safety approval requirements listed in Table B-1.

Table B-1   Standards

Discipline	Country	Specification
EMC Emissions (Class A)	Global	CISPR22/EN55022 Class A Radiated Emissions 30-1000 MHz and Conducted Emissions 0.15-30 MHz
		EN300386/2000 Conducted Emissions 0.02-30 MHz
		AS/NZS 3548 Incorporating Amendments 1 and 2
		VCCIV-3/2000.04
		47 CFR 15 Subpart B
EMC Immunity	Global	EN61000-4-2 Level 4, Electrostatic discharge immunity
		EN61000-4-3 Level 3, Radiated susceptability
		EN61000-4-4 Level 2, Electrical fast transient/burst immunity
		EN61000-4-5 1kV (L-L)/1kV (L-G) Surges
		EN61000-4-6 Level 3, Conducted susceptability
Safety	Global	IEC 60950
		EN 60950
		UL 60950
		CSA-C22.2 No. 60950
		TS 001
		AS/NZS 3260

Table B-1   Standards (continued)

Discipline	Country	Specification
Environmental	USA	Cisco Mechanical Environmental Design and Qualification Guideline ENG-3396
	European Union	ETS 300 019 Class 3.1E for Operation
		ETS 300 019 Class 2.3 for Transport
		ETS 300 019 Class 1.1 for Storage
Telecom	European Union	Directive 1999/5/EC
	Australia	AS/ACIF S016:2001, for DS3 and E1 cards
		TS-026, for optical interfaces
	Singapore	IDA TS DLCN 1:2000

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。

Translated Safety Warnings

This document contains the translated warnings that are required in Cisco hardware installation guides and user guides. These warnings are required in hardware documentation to comply with the regulatory agency requirements of other countries.

The translated safety warnings are listed in the following order:

1. English
2. Dutch
3. Finnish
4. French
5. German
6. Italian
7. Norwegian

8. Portuguese

9. Spanish

10. Swedish

Electrical Circuitry Warning

Warning   This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the "Regulatory Compliance and Safety Information" section in this document.

Waarschuwing   Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het gedeelte Regulatory Compliance and Safety Information (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen in dit document.

Varoitus   Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät tämän asiakirjan Regulatory Compliance and Safety Information -osasta (määräysten noudattaminen ja tietoa turvallisuudesta).

Attention   Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez la section Regulatory Compliance and Safety Information (Conformité aux règlements et consignes de sécurité) de ce document.

Warnung   Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Abschnitt "Regulatory Compliance and Safety Information" (Informationen zu behördlichen Vorschriften und Sicherheit) in diesem Dokument.

Avvertenza   Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nella documento Regulatory Compliance and Safety Information (Conformità alle norme e informazioni sulla sicurezza) nel presente documento.

■ **Translated Safety Warnings**

Advarsel	**Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i avsnittet Regulatory Compliance and Safety Information (Overholdelse av forskrifter og sikkerhetsinformasjon) i dette dokumentet.**
Aviso	**Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte a secção Regulatory Compliance and Safety Information (Informação de Segurança e Disposições Reguladoras) neste documento.**
¡Advertencia!	**Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar la sección titulada Regulatory Compliance and Safety Information (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que aparece en este documento.**
Varning!	**Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Om du vill se översättningar av de varningar som visas i denna publikation, se avsnittet "Efterrättelse av föreskrifter och säkerhetsinformation" i detta dokument.**

Installation Warning

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.**

Short-Circuit Protection Warning

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

Waarschuwing **Voor dit product moet kortsluitbeveiliging (overstroombeveiliging) deel uitmaken van de installatie in het gebouw. De installatie moet voldoen aan de nationale en lokale bedradingvoorschriften.**

Varoitus **Tämä tuote vaatii suojauksen oikosulkuja (ylivirtaa) vastaan osana asennusta rakennukseen. Asenna ainoastaan kansallisten ja paikallisten johdotussäännösten mukaisesti.**

Attention **La protection de ce produit contre les courts-circuits (surtensions) doit être assurée par la configuration électrique du bâtiment. Vérifiez que l'installation a lieu uniquement en conformité avec les normes de câblage en vigueur au niveau national et local.**

Warnung **Für dieses Produkt ist eine Kurzschlußsicherung (Überstromsicherung) erforderlich, die als Teil der Gebäudeinstallation zur Verfügung gestellt wird. Die Installation sollte nur in Übereinstimmung mit den nationalen und regionalen Vorschriften zur Verkabelung erfolgen.**

Figyelem! **A termékhez kötelező rövidzárlat (túláram) elleni védelmet használni, amelyet az épület kábelezésének részeként kell biztosítani. Csak az országos és helyi kábelezési elõírásoknak megfelelõen helyezhetõ üzembe.**

Avvertenza **Questo prodotto richiede una protezione contro i cortocircuiti, da fornirsi come parte integrante delle dotazioni presenti nell'edificio. Effettuare l'installazione rispettando le Norme CEI pertinenti.**

Advarsel **Dette produktet krever beskyttelse mot kortslutninger (overspenninger) som en del av installasjonen. Bare installer utstyret i henhold til nasjonale og lokale krav til ledningsnett.**

Aviso **Este produto requer proteção contra curto-circuitos (sobreintensidade de corrente), que deve estar instalada nos edifícios. Instale apenas de acordo com as normas de instalação elétrica nacionais e locais.**

Advertencia **Este producto necesita estar conectado a la protección frente a cortacircuitos (sobretensiones) que exista en el edificio. Instálelo únicamente en conformidad con las regulaciones sobre cableado, tanto locales como nacionales, a las que se tenga que atener.**

Varning! **Denna produkt kräver att kortslutningsskydd (överström) tillhandahålles som en del av byggnadsinstallationen. Installera bara i enlighet med nationella och lokala kabeldragningsbestämmelser.**

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.

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。

Backplane Voltage Warning

Warning	Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.
Waarschuwing	Er is gevaarlijke spanning of energie aanwezig op de achterplaat wanneer het systeem bediend wordt. Wees voorzichtig bij het onderhoud.
Varoitus	Kun laite on toiminnassa, taustalevyyn muodostuu vaarallista jännitettä. Ole varovainen huoltaessasi laitetta.
Attention	Lorsque le système est en fonctionnement, des tensions électriques circulent sur le fond de panier. Prendre des précautions lors de la maintenance.
Warnung	Wenn das System in Betrieb ist, treten auf der Rückwandplatine gefährliche Spannungen oder Energien auf. Vorsicht bei der Wartung.
Figyelem!	A rendszer mûködése közben veszélyes feszültség vagy energia van jelen a hátlapon. Karbantartás közben óvatosan járjon el!
Avvertenza	Quando il sistema è in funzione, il pannello posteriore è sotto tensione pericolosa. Prestare attenzione quando si lavora sul sistema.
Advarsel	Farlig spenning er til stede på bakpanelet når systemet kjøres. Utvis forsiktighet under service.
Aviso	Há presença de voltagem perigosa ou de energia na placa traseira quando o sistema está em operação. Tenha cuidado ao fazer a manutenção.
¡Advertencia!	Cuando el sistema está en funcionamiento, el voltaje del plano trasero es peligroso. Tenga cuidado cuando lo revise.
Varning!	Farlig spänning föreligger på bakplattan när systemet körs. Var försiktig vid service.

Rack Installation Warning

Warning	The chassis should be mounted on a rack that is permanently affixed to the building.
Waarschuwing	Het chassis moet gemonteerd worden op een rek dat blijvend aan het gebouw is vastgezet.
Varoitus	Asennuspohja on asennettava pysyvästi rakennukseen kiinnitettyyn telineeseen.
Attention	Le châssis doit être installé sur une étagère fixée au bâtiment de manière permanente.

Cisco ONS 15454 SDH Installation and Operations Guide, R3.4

Warnung	**Das Chassis sollte auf einem Gestell angebracht werden, das fest im Gebäude verankert ist.**
Figyelem!	**A gépházat az épülethez állandó kötéssel rögzített rackbe kell felszerelni.**
Avvertenza	**Il telaio deve essere montato su un rack affrancato alla struttura dell'edificio.**
Advarsel	**Kabinettet må monteres på et stativ som er permanent festet til gulvet.**
Aviso	**O chassis deve ser montado em um rack permanentemente fixo ao chão.**
¡Advertencia!	**El chasis debe montarse en un bastidor que esté fijado permanentemente al edificio.**
Varning!	**Chassit ska monteras i ett rack som är permanent fastsatt vid byggnaden.**

Chassis Warning—Rack-Mounting and Servicing

Warning   **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Waarschuwing   **Om lichamelijk letsel te voorkomen wanneer u dit toestel in een rek monteert of het daar een servicebeurt geeft, moet u speciale voorzorgsmaatregelen nemen om ervoor te zorgen dat het toestel stabiel blijft. De onderstaande richtlijnen worden verstrekt om uw veiligheid te verzekeren:**

- Dit toestel dient onderaan in het rek gemonteerd te worden als het toestel het enige in het rek is.
- Wanneer u dit toestel in een gedeeltelijk gevuld rek monteert, dient u het rek van onderen naar boven te laden met het zwaarste onderdeel onderaan in het rek.
- Als het rek voorzien is van stabiliseringshulpmiddelen, dient u de stabilisatoren te monteren voordat u het toestel in het rek monteert of het daar een servicebeurt geeft.

Varoitus   **Kun laite asetetaan telineeseen tai huolletaan sen ollessa telineessä, on noudatettava erityisiä varotoimia järjestelmän vakavuuden säilyttämiseksi, jotta vältytään loukkaantumiselta. Noudata seuraavia turvallisuusohjeita:**

- Jos telineessä ei ole muita laitteita, aseta laite telineen alaosaan.

- Jos laite asetetaan osaksi täytettyyn telineeseen, aloita kuormittaminen sen alaosasta kaikkein raskaimmalla esineellä ja siirry sitten sen yläosaan.

- Jos telinettä varten on vakaimet, asenna ne ennen laitteen asettamista telineeseen tai sen huoltamista siinä.

Attention   **Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel :**

- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.

- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.

- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

Warnung   **Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:**

- Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.

- Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.

- Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.

Avvertenza   **Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un supporto, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive vengono fornite per garantire la sicurezza personale:**

- Questa unità deve venire montata sul fondo del supporto, se si tratta dell'unica unità da montare nel supporto.

- Quando questa unità viene montata in un supporto parzialmente pieno, caricare il supporto dal basso all'alto, con il componente più pesante sistemato sul fondo del supporto.

- Se il supporto è dotato di dispositivi stabilizzanti, installare tali dispositivi prima di montare o di procedere alla manutenzione dell'unità nel supporto.

Advarsel   **Unngå fysiske skader under montering eller reparasjonsarbeid på denne enheten når den befinner seg i et kabinett. Vær nøye med at systemet er stabilt. Følgende retningslinjer er gitt for å verne om sikkerheten:**

- Denne enheten bør monteres nederst i kabinettet hvis dette er den eneste enheten i kabinettet.

- Ved montering av denne enheten i et kabinett som er delvis fylt, skal kabinettet lastes fra bunnen og opp med den tyngste komponenten nederst i kabinettet.

- Hvis kabinettet er utstyrt med stabiliseringsutstyr, skal stabilisatorene installeres før montering eller utføring av reparasjonsarbeid på enheten i kabinettet.

Aviso   **Para se prevenir contra danos corporais ao montar ou reparar esta unidade numa estante, deverá tomar precauções especiais para se certificar de que o sistema possui um suporte estável. As seguintes directrizes ajudá-lo-ão a efectuar o seu trabalho com segurança:**

- Esta unidade deverá ser montada na parte inferior da estante, caso seja esta a única unidade a ser montada.

- Ao montar esta unidade numa estante parcialmente ocupada, coloque os itens mais pesados na parte inferior da estante, arrumando-os de baixo para cima.

- Se a estante possuir um dispositivo de estabilização, instale-o antes de montar ou reparar a unidade.

¡Advertencia!   **Para evitar lesiones durante el montaje de este equipo sobre un bastidor, o posteriormente durante su mantenimiento, se debe poner mucho cuidado en que el sistema quede bien estable. Para garantizar su seguridad, proceda según las siguientes instrucciones:**

- Colocar el equipo en la parte inferior del bastidor, cuando sea la única unidad en el mismo.

- Cuando este equipo se vaya a instalar en un bastidor parcialmente ocupado, comenzar la instalación desde la parte inferior hacia la superior colocando el equipo más pesado en la parte inferior.

- Si el bastidor dispone de dispositivos estabilizadores, instalar éstos antes de montar o proceder al mantenimiento del equipo instalado en el bastidor.

Varning!   **För att undvika kroppsskada när du installerar eller utför underhållsarbete på denna enhet på en ställning måste du vidta särskilda försiktighetsåtgärder för att försäkra dig om att systemet står stadigt. Följande riktlinjer ges för att trygga din säkerhet:**

- Om denna enhet är den enda enheten på ställningen skall den installeras längst ned på ställningen.

- Om denna enhet installeras på en delvis fylld ställning skall ställningen fyllas nedifrån och upp, med de tyngsta enheterna längst ned på ställningen.

- Om ställningen är försedd med stabiliseringsdon skall dessa monteras fast innan enheten installeras eller underhålls på ställningen.

Installation and Replacement Warning

Warning	**When installing or replacing the unit, the ground connection must always be made first and disconnected last.**
Waarschuwing	**Bij installatie of vervanging van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.**
Varoitus	**Laitetta asennettaessa tai korvattaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.**
Attention	**Lors de l'installation ou du remplacement 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 oder beim Austauschen der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.**
Figyelem!	**A készülék üzembe helyezése és cserélése közben mindig a földelés vezetékét kell elsõként csatlakoztatni és azt kell utolsóként leválasztani.**
Avvertenza	**In fase di installazione o sostituzione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.**
Advarsel	**Når enheten installeres eller byttes, må jordledningen alltid tilkobles først og frakobles sist.**
Aviso	**Ao instalar ou substituir a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.**
¡Advertencia!	**Al instalar o sustituir el equipo, conecte siempre la toma de tierra al principio y desconéctela al final.**
Varning!	**Vid installation eller utbyte av enheten måste jordledningen alltid anslutas först och kopplas bort sist.**

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.

Grounded Equipment Warning

⚠ Warning	This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
Waarschuwing	Deze apparatuur hoort geaard te worden Zorg dat de host-computer tijdens normaal gebruik met aarde is verbonden.
Varoitus	Tämä laitteisto on tarkoitettu maadoitettavaksi. Varmista, että isäntälaite on yhdistetty maahan normaalikäytön aikana.
Attention	Cet équipement doit être relié à la terre. S'assurer que l'appareil hôte est relié à la terre lors de l'utilisation normale.
Warnung	Dieses Gerät muß geerdet werden. Stellen Sie sicher, daß das Host-Gerät während des normalen Betriebs an Erde gelegt ist.
Avvertenza	Questa apparecchiatura deve essere collegata a massa. Accertarsi che il dispositivo host sia collegato alla massa di terra durante il normale utilizzo.
Advarsel	Dette utstyret skal jordes. Forviss deg om vertsterminalen er jordet ved normalt bruk.
Aviso	Este equipamento deverá estar ligado à terra. Certifique-se que o host se encontra ligado à terra durante a sua utilização normal.
¡Advertencia!	Este equipo debe conectarse a tierra. Asegurarse de que el equipo principal esté conectado a tierra durante el uso normal.
Varning!	Denna utrustning är avsedd att jordas. Se till att värdenheten är jordad vid normal användning.

Installation Warning

Warning	**Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**
Waarschuwing	**Deze apparatuur mag alleen worden geïnstalleerd, vervangen of hersteld door bevoegd geschoold personeel.**
Varoitus	**Tämän laitteen saa asentaa, vaihtaa tai huoltaa ainoastaan koulutettu ja laitteen tunteva henkilökunta.**
Attention	**Il est vivement recommandé de confier l'installation, le remplacement et la maintenance de ces équipements à des personnels qualifiés et expérimentés.**
Warnung	**Das Installieren, Ersetzen oder Bedienen dieser Ausrüstung sollte nur geschultem, qualifiziertem Personal gestattet werden.**
Avvertenza	**Questo apparato può essere installato, sostituito o mantenuto unicamente da un personale competente.**
Advarsel	**Bare opplært og kvalifisert personell skal foreta installasjoner, utskiftninger eller service på dette utstyret.**
Aviso	**Apenas pessoal treinado e qualificado deve ser autorizado a instalar, substituir ou fazer a revisão deste equipamento.**
¡Advertencia!	**Solamente el personal calificado debe instalar, reemplazar o utilizar este equipo.**
Varning!	**Endast utbildad och kvalificerad personal bör få tillåtelse att installera, byta ut eller reparera denna utrustning.**

Supply Circuit Warning

Warning	**Care must be given to connecting units to the supply circuit so that wiring is not overloaded.**
Waarschuwing	**Let erop dat de toestellen op voedingscircuits worden aangesloten zonder het vermogen van de bedrading te overschrijden.**
Varoitus	**Laiteyksiköt on yhdistettävä huolellisesti syöttöpiiriin niin, että johdot eivät ole ylikuormitettuja.**
Avertissement	**Veillez à bien connecter les unités au circuit d'alimentation afin de ne pas surcharger les connections.**

Achtung   **Beim Anschließen der Geräte an das Stromnetz ist darauf zu achten, daß die Schaltverbindungen nicht überlastet werden.**

Avvertenza   **Fare attenzione quando si collegano le unità al circuito di alimentazione, per non sovraccaricare i cablaggi.**

Advarsel   **Vær nøye med å koble enheter til strømforsyningskretsen slik at ledningene ikke overbelastes.**

Aviso   **Deverá ter precaução ao ligar unidades ao circuito de fornecimento de energia, para não sobrecarregar a instalação.**

¡Atención!   **Poner mucho cuidado al conectar los equipos al circuito de alimentación a fin de no sobrecargar el cableado.**

Varning   **Var noga vid anslutning av enheter till matarströmkretsen så att ledningarna inte överbelastas.**

Disconnect Device Warning

⚠

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

Waarschuwing   **Er moet een gemakkelijk toegankelijke, tweepolige stroomverbreker opgenomen zijn in de vaste bedrading.**

Varoitus   **Kiinteään johdotukseen on liitettävä kaksinapainen kytkinlaite, johon on helppo päästä käsiksi.**

Attention   **Un disjoncteur bipolaire facile d'accès doit être intégré dans le câblage fixe.**

Warnung   **Die feste Verdrahtung muß eine leicht zugängliche, zweipolige Trennvorrichtung enthalten.**

Avvertenza   **Nei cablaggi fissi va incorporato un sezionatore a due poli facilmente accessibile.**

Advarsel   **En lett tilgjengelig, topolet frakoblingsenhet må være innebygd i det faste ledningsnettet.**

Aviso   **Deverá incorporar-se um dispositivo de desconexão de dois pólos de acesso fácil, na instalação eléctrica fixa.**

¡Advertencia!   **El cableado fijo debe incorporar un dispositivo de desconexión de dos polos y de acceso fácil.**

Varning!   **En lättillgänglig tvåpolig frånkopplingsenhet måste ingå i den fasta kopplingen.**

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.

Faceplates and Cover Panels Warning

⚠

Warning   **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

Waarschuwing   **Lege vlakplaten en afdekpanelen vervullen drie belangrijke functies: ze voorkomen blootstelling aan gevaarlijke voltages en stroom binnenin het frame, ze bevatten elektromagnetische storing (EMI) hetgeen andere apparaten kan verstoren en ze leiden de stroom van koellucht door het frame. Het systeem niet bedienen tenzij alle kaarten, vlakplaten en afdekkingen aan de voor- en achterkant zich op hun plaats bevinden.**

Varoitus   **Tyhjillä tasolaikoilla ja suojapaneeleilla on kolme tärkeää käyttötarkoitusta: Ne suojaavat asennuspohjan sisäisille vaarallisille jännitteille ja sähkövirralle altistumiselta; ne pitävät sisällään elektromagneettisen häiriön (EMI), joka voi häiritä muita laitteita; ja ne suuntaavat tuuletusilman asennuspohjan läpi. Järjestelmää ei saa käyttää, elleivät kaikki tasolaikat, etukannet ja takakannet ole kunnolla paikoillaan.**

Attention   **Ne jamais faire fonctionner le système sans que l'intégralité des cartes, des plaques métalliques et des panneaux avant et arrière ne soient fixés à leur emplacement. Ceux-ci remplissent trois fonctions essentielles : ils évitent tout risque de contact avec des tensions et des courants dangereux à l'intérieur du châssis, ils évitent toute diffusion d'interférences électromagnétiques qui pourraient perturber le fonctionnement des autres équipements, et ils canalisent le flux d'air de refroidissement dans le châssis.**

Warnung   **Blanke Faceplates und Abdeckungen haben drei wichtigen Funktionen: (1) Sie schützen vor gefährlichen Spannungen und Strom innerhalb des Chassis; (2) sie halten elektromagnetische Interferenzen (EMI) zurück, die andere Geräte stören könnten; (3) sie lenken den kühlenden Luftstrom durch das Chassis. Das System darf nur betrieben werden, wenn alle Karten, Faceplates, Voder- und Rückabdeckungen an Ort und Stelle sind.**

Figyelem!   **Az előlapok és burkolópanelek három fontos funkciót töltenek be: biztosítják a veszélyes feszültségű és áramerősségű területek érintésvédelmét; elnyelik a más berendezések működésében működési zavarokat okozó elektromágneses interferenciát (EMI); a gépházon belül terelik a hűtőlevegőt. Csak úgy működtesse a rendszert, ha minden kártya, lemez, elülső és hátulsó burkolat a helyén van.**

Avvertenza   **Le piattaforme bianche e i panelli di protezione hanno tre funzioni importanti: Evitano l'esposizione a voltaggi e correnti elettriche pericolose nello chassis, trattengono le interferenze elettromagnetiche (EMI) che potrebbero scombussolare altri apparati e dirigono il flusso di aria per il raffreddamento attraverso lo chassis. Non mettete in funzione il sistema se le schede, le piattaforme, i panelli frontali e posteriori non sono in posizione.**

Advarsel   **Blanke ytterplater og deksler sørger for tre viktige funksjoner: de forhindrer utsettelse for farlig spenning og strøm inni kabinettet; de inneholder elektromagnetisk forstyrrelse (EMI) som kan avbryte annet utstyr, og de dirigerer luftavkjølingsstrømmen gjennom kabinettet. Betjen ikke systemet med mindre alle kort, ytterplater, frontdeksler og bakdeksler sitter på plass.**

Aviso   **As faces furadas e os painéis de protecção desempenham três importantes funções: previnem contra uma exposição perigosa a voltagens e correntes existentes no interior do chassis; previnem contra interferência electromagnética (EMI) que poderá danificar outro equipamento; e canalizam o fluxo do ar de refrigeração através do chassis. Não deverá operar o sistema sem que todas as placas, faces, protecções anteriores e posteriores estejam nos seus lugares.**

¡Advertencia!   **Las placas frontales y los paneles de relleno cumplen tres funciones importantes: evitan la exposición a niveles peligrosos de voltaje y corriente dentro del chasis; reducen la interferencia electromagnética (EMI) que podría perturbar la operación de otros equipos y dirigen el flujo de aire de enfriamiento a través del chasis. No haga funcionar el sistema a menos que todas las tarjetas, placas frontales, cubiertas frontales y cubiertas traseras estén en su lugar.**

Varning!   **Tomma framplattor och skyddspaneler har tre viktiga funktioner: de förhindrar att personer utsätts för farlig spänning och ström som finns inuti chassit; de innehåller elektromagnetisk interferens (EMI) som kan störa annan utrustning; och de styr riktningen på kylluftsflödet genom chassit. Använd inte systemet om inte alla kort, framplattor, fram- och bakskydd är på plats.**

Product Disposal Warning

Warning   **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Waarschuwing   **Het uiteindelijke wegruimen van dit product dient te geschieden in overeenstemming met alle nationale wetten en reglementen.**

Varoitus   **Tämä tuote on hävitettävä kansallisten lakien ja määräysten mukaisesti.**

Attention   **La mise au rebut ou le recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environnement. Renseignez-vous auprès de l'organisme compétent.**

Warnung   **Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.**

Avvertenza   **Lo smaltimento di questo prodotto deve essere eseguito secondo le leggi e regolazioni locali.**

Advarsel   **Endelig kassering av dette produktet skal være i henhold til alle relevante nasjonale lover og bestemmelser.**

Aviso   **Deitar fora este produto em conformidade com todas as leis e regulamentos nacionais.**

¡Advertencia!   **Al deshacerse por completo de este producto debe seguir todas las leyes y reglamentos nacionales.**

Varning!   **Vid deponering hanteras produkten enligt gällande lagar och bestämmelser.**

Wrist Strap Warning

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.**

Waarschuwing   **Draag tijdens deze procedure aardingspolsbanden om te vermijden dat de kaart beschadigd wordt door elektrostatische ontlading. Raak het achterbord niet rechtstreeks aan met uw hand of met een metalen werktuig, omdat u anders een elektrische schok zou kunnen oplopen.**

Varoitus   **Käytä tämän toimenpiteen aikana maadoitettuja rannesuojia estääksesi kortin vaurioitumisen sähköstaattisen purkauksen vuoksi. Älä kosketa taustalevyä suoraan kädelläsi tai metallisella työkalulla sähköiskuvaaran takia.**

Attention   **Lors de cette procédure, toujours porter des bracelets antistatiques pour éviter que des décharges électriques n'endommagent la carte. Pour éviter l'électrocution, ne pas toucher le fond de panier directement avec la main ni avec un outil métallique.**

Warnung   **Zur Vermeidung einer Beschädigung der Karte durch elektrostatische Entladung während dieses Verfahrens ein Erdungsband am Handgelenk tragen. Bei Berührung der Rückwand mit der Hand oder einem metallenen Werkzeug besteht Elektroschockgefahr.**

Avvertenza   **Durante questa procedura, indossare bracciali antistatici per evitare danni alla scheda causati da un'eventuale scarica elettrostatica. Non toccare direttamente il pannello delle connessioni, né con le mani né con un qualsiasi utensile metallico, perché esiste il pericolo di folgorazione.**

Advarsel   **Bruk jordingsarmbånd under prosedyren for å unngå ESD-skader på kortet. Unngå direkte berøring av bakplanet med hånden eller metallverktøy, slik at di ikke får elektrisk støt.**

Aviso   **Durante este procedimento e para evitar danos ESD causados à placa, use fitas de ligação à terra para os pulsos. Para evitar o risco de choque eléctrico, não toque directamente na parte posterior com a mão ou com qualquer ferramenta metálica.**

¡Advertencia!   **Usartiras conectadas a tierra en las muñecas durante este procedimiento para evitar daños en la tarjeta causados por descargas electrostáticas. No tocar el plano posterior con las manos ni con ninguna herramienta metálica, ya que podría producir un choque eléctrico.**

Varning!   **Använd jordade armbandsremmar under denna procedur för att förhindra elektrostatisk skada på kortet. Rör inte vid baksidan med handen eller metallverktyg då detta kan orsaka elektrisk stöt.**

Installation Warning

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.

Waarschuwing Deze uitrusting dient geïnstalleerd en onderhouden te worden door onderhoudspersoneel zoals gedefinieerd door AS/NZS 3260. Als deze uitrusting onjuist op een stopcontact voor algemeen gebruik wordt aangesloten kan dit gevaarlijk zijn. De telecommunicatielijnen dienen ontkoppeld te worden 1) voordat de stekker naar de hoofdstroomtoevoer eruit wordt genomen en/of 2) terwijl de behuizing open is.

Varoitus Huoltohenkilöstön on asennettava ja huollettava tämä laite AS/NZS 3260:n määräysten mukaisesti. Laitteen virheellinen kytkeminen yleispistorasiaan voi aiheuttaa vaaratilanteita. Tietoliikennejohdot on irrotettava 1) ennen kuin päävirtaliitin irrotetaan pistorasiasta ja/tai 2) kun kotelo on auki.

Attention Cet équipement ne doit être installé et entretenu que par du personnel d'entretien comme défini par la réglementation AS/NZS 3260. Un branchement incorrect de cet équipement à une prise de courant peut créer une situation dangereuse. Les lignes de télécommunications doivent être déconnectées 1) avant de débrancher le connecteur d'alimentation principal et/ou 2) lorsque le boîtier est ouvert.

Warnung Dieses Gerät ist nur von ausgebildetem Personal zu installieren und zu warten (lt. Definition in AS/NZS 3260). Fälschliches Anschließen des Geräts an eine normale Steckdose könnte gefährlich sein. Die Telekommunikationsleitungen dürfen 1) beim Herausziehen des Netzsteckers und/oder 2) bei geöffnetem Gehäuse nicht angeschlossen sein.

Avvertenza Questo apparecchio deve essere installato e mantenuto in efficienza esclusivamente da personale tecnico che soddisfi i requisiti specificati nelle norme AS/NZS 3260. Un collegamento errato di questo apparecchio ad una presa di uso generale può essere pericoloso. Le linee di telecomunicazione vanno scollegate sia prima di scollegare la spina dell'alimentazione di rete sia prima di aprire l'involucro (non ricollegarle finché non si chiude l'involucro).

Advarsel Dette utstyret må monteres og vedlikeholdes av vedlikeholdspersonell i henhold til AS/NZS 3260. Feilaktig tilkopling av dette utstyret til et vanlig strømuttak kan medføre fare. Telekommunikasjonslinjene må være frakoplet 1) før strømledningen trekkes ut av kontakten og/eller 2) mens huset er åpent.

Aviso A instalação e a manutenção deste equipamento devem ser realizadas por pessoal da assistência, conforme definido na norma AS/NZS 3260. A ligação incorrecta deste equipamento a uma tomada de utilização geral poderá ser perigosa. As linhas de telecomunicações têm de estar desligadas 1) antes de desligar a ligação à corrente principal e/ou 2) enquanto a caixa estiver aberta.

¡Advertencia!   **Este equipo se debe instalar y mantener solamente por personal de servicio, según definido por AS/NZS 3260. La conexión incorrecta de este equipo a una toma o receptáculo de tipo general podría resultar peligrosa. Las líneas de telecomunicaciones deben desconectarse 1) antes de desenchufar el conector principal de energía y 2) mientras la caja esté abierta.**

Varning!   **Denna utrustning måste installeras och underhållas av servicepersonal enligt AS/NZS 3260. Felaktig anslutning av denna utrustning till ett vanligt vägguttag kan medföra fara. Teleledningarna måste kopplas ifrån innan väggkontakten dras ut och/eller innan höljet tas av.**

Short-Circuit Protection Warning

Warning   **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

Waarschuwing   **Voor dit product moet kortsluitbeveiliging (overstroombeveiliging) deel uitmaken van de installatie in het gebouw. De installatie moet voldoen aan de nationale en lokale bedradingvoorschriften.**

Varoitus   **Tämä tuote vaatii suojauksen oikosulkuja (ylivirtaa) vastaan osana asennusta rakennukseen. Asenna ainoastaan kansallisten ja paikallisten johdotussäännösten mukaisesti.**

Attention   **La protection de ce produit contre les courts-circuits (surtensions) doit être assurée par la configuration électrique du bâtiment. Vérifiez que l'installation a lieu uniquement en conformité avec les normes de câblage en vigueur au niveau national et local.**

Warnung   **Für dieses Produkt ist eine Kurzschlußsicherung (Überstromsicherung) erforderlich, die als Teil der Gebäudeinstallation zur Verfügung gestellt wird. Die Installation sollte nur in Übereinstimmung mit den nationalen und regionalen Vorschriften zur Verkabelung erfolgen.**

Avvertenza   **Questo prodotto richiede una protezione contro i cortocircuiti, da fornirsi come parte integrante delle dotazioni presenti nell'edificio. Effettuare l'installazione rispettando le Norme CEI pertinenti.**

Advarsel   **Dette produktet krever beskyttelse mot kortslutninger (overspenninger) som en del av installasjonen. Bare installer utstyret i henhold til nasjonale og lokale krav til ledningsnett.**

Aviso   **Este produto requer proteção contra curto-circuitos (sobreintensidade de corrente), que deve estar instalada nos edifícios. Instale apenas de acordo com as normas de instalação elétrica nacionais e locais.**

Advertencia   **Este producto necesita estar conectado a la protección frente a cortacircuitos (sobretensiones) que exista en el edificio. Instálelo únicamente en conformidad con las regulaciones sobre cableado, tanto locales como nacionales, a las que se tenga que atener.**

Varning!   **Denna produkt kräver att kortslutningsskydd (överström) tillhandahålles som en del av byggnadsinstallationen. Installera bara i enlighet med nationella och lokala kabeldragningsbestämmelser.**

Installation and Replacement Warning

Warning	**When installing or replacing the unit, the ground connection must always be made first and disconnected last.**
Waarschuwing	**Bij installatie of vervanging van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.**
Varoitus	**Laitetta asennettaessa tai korvattaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.**
Attention	**Lors de l'installation ou du remplacement 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 oder beim Austauschen der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.**
Avvertenza	**In fase di installazione o sostituzione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.**
Advarsel	**Når enheten installeres eller byttes, må jordledningen alltid tilkobles først og frakobles sist.**
Aviso	**Ao instalar ou substituir a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.**
¡Advertencia!	**Al instalar o sustituir el equipo, conecte siempre la toma de tierra al principio y desconéctela al final.**
Varning!	**Vid installation eller utbyte av enheten måste jordledningen alltid anslutas först och kopplas bort sist.**

Overheating Prevention Warning

Warning	**To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C).**
Waarschuwing	**Om te voorkomen dat het systeem oververhit raakt, dient u het systeem niet te gebruiken in een ruimte waar de maximaal aanbevolen omgevingstemperatuur van 40°C wordt overschreden.**
Varoitus	**Jotta järjestelmä ei kuumentuisi liikaa, sitä ei saa käyttää alueella, jonka lämpötila ylittää suositellun maksimiympäristölämpötilan 40°C.**
Attention	**Pour éviter toute surchauffe du système, il est recommandé de maintenir une température ambiante inférieure à 40°C.**

Warnung	Um das System vor Überhitzung zu schützen, vermeiden Sie dessen Verwendung in einer Gegend, in der die Umgebungstemperatur das empfohlene Maximum von 40°C überschreitet.
Avvertenza	Per evitare che il sistema si surriscaldi, non utilizzatelo in una zona dove la temperatura ambiente ecceda la temperatura massima raccomandata di 40°C (104°F).
Advarsel	For å hindre at systemet blir overopphetet, må det ikke brukes i et område der temperaturen overstiger den maksimalt anbefalte temperaturen på 40°C.
Aviso	Para evitar o sobreaquecimento do sistema, não o utilize em áreas que excedam a temperatura ambiente máxima recomendada de 40°C (104°F).
¡Advertencia!	Para impedir que el sistema se caliente, no lo utilice en zonas en las que la temperatura ambiente llegue a los 40°C (104°F).
Varning!	Förhindra att systemet blir överhettat genom att inte använda det på en plats där den rekommenderade omgivningstemperaturen överstiger 40°C.

Laser Radiation Warning

⚠ Warning	Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.
Waarschuwing	Losgekoppelde of losgeraakte glasvezels of aansluitingen kunnen onzichtbare laserstraling produceren. Kijk niet rechtstreeks in de straling en gebruik geen optische instrumenten rond deze glasvezels of aansluitingen.
Varoitus	Irrotetuista kuiduista tai liittimistä voi tulla näkymätöntä lasersäteilyä. Älä tuijota säteitä tai katso niitä suoraan optisilla välineillä.
Attention	Les fibres ou connecteurs débranchés risquent d'émettre des rayonnements laser invisibles à l'œil. Ne regardez jamais directement les faisceaux laser à l'œil nu, ni d'ailleurs avec des instruments optiques.
Warnung	Unterbrochene Fasern oder Steckerverbindungenkönnen unsichtbare Laserstrahlung abgeben.. Blicken Sie weder mit bloßem Auge noch mit optischen Instrumenten direkt in Laserstrahlen.
Avvertenza	Le fibre ottiche ed i relativi connettori possono emettere radiazioni laser. I fasci di luce non devono mai essere osservati direttamente o attraverso strumenti ottici.
Advarsel	Det kan forekomme usynlig laserstråling fra fiber eller kontakter som er frakoblet. Stirr ikke direkte inn i strålene eller se på dem direkte gjennom et optisk instrument.
Aviso	Radiação laser invisível pode ser emitida de conectores ou fibras desconectadas. Não olhe diretamente para os feixes ou com instrumentos ópticos.

■ **Translated Safety Warnings**

¡Advertencia! **Es posible que las fibras desconectadas emitan radiación láser invisible. No fije la vista en los rayos ni examine éstos con instrumentos ópticos.**

Varning! **Osynlig laserstrålning kan avges från frånkopplade fibrer eller kontaktdon. Rikta inte blicken in i strålar och titta aldrig direkt på dem med hjälp av optiska instrument.**

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).**

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.**

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).**

DC Power SELV Requirement Warning

Warning   **The DC power supply systems (main, redundant, and service battery power supply systems) must be compliant with safety extra low voltage (SELV) requirements in accordance with IEC 60950 and UL 60950.**

Waarschuwing   **De toevoersystemen van de gelijkstroom (hoofdtoevoersystemen, redundante en toevoersystemen voor de servicebatterij) dienen te voldoen aan de SELV (safety extra low voltage) vereisten in overeenstemming met IEC 60950 en UL 60950.**

Varoitus   **Tasavirtavoimaverkkojen (pää-, varmennus- ja käyttöakkuvirtajärjestelmät) on noudatettava suojattuja erittäin alhaisia jännitteitä (SELV) koskevia vaatimuksia standardien IEC 60950 ja UL 60950 mukaisesti.**

Attention   **Les systèmes d'alimentation en courant continu (systèmes principal, de secours et d'alimentation électrique d'entretien sur piles) doivent être conformes aux critères SELV (Safety Extra Low Voltage) tels qu'ils sont définis dans les normes IEC 60950 et UL 60950.**

Warnung   **Die Systeme für die Gleichstromversorgung (Haupt-, redundante und Wartungsbatterie-Stromversorgungssysteme) müssen den Anforderungen für besonders niedrige Spannungen (SELV) nach den Richtlinien IEC 60950 und UL 60950 entsprechen.**

Avvertenza   **I sistemi di alimentazione CC (sistema principale, di riserva e di alimentazione della batteria di servizio) devono essere conformi ai requisiti delle tensioni di sicurezza a basso voltaggio (SELV, Safety Extra Low Voltage) in conformità alle norme IEC 60950 e UL 60950.**

Advarsel   **Likestrømsystemet (hovedledning, redundant og strøm fra servicebatterisystemet) må samsvare med sikkerhets-lavspenning (SELV)-kravene i henhold til IEC 60950 og UL 60950.**

Aviso   **Os sistemas de fonte de alimentação CC (sistemas de fontes de alimentação principal, redundante e de bateria de serviço) devem ser compatíveis com os requisitos SELV (safety extra low voltage, tensão de segurança extra baixa) de acordo com as normas IEC 60950 e UL 60950.**

¡Advertencia!   **Los sistemas de suministro de alimentación de CC (sistemas de alimentación principal, redundante y de batería de servicio) deben cumplir los requerimientos de voltaje de seguridad extra bajo (SELV) de conformidad con IEC 60950 y UL 60950.**

Varning!   **Matarsystemen för likström (huvud-, tilläggs- och servicebatterisystem) måste följa kraven för SELV (safety extra low voltage) i enlighet med IEC 60950 och UL 60950.**

Numerics

1:1 protection

An electrical card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot (DS-1 and DS-3 speeds). 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 to the working card.

1+1 protection

An optical (OC-N) card protection scheme that pairs a single working port/card with a single dedicated protect port/card. All OC-N cards can use this protection type (OC-3, OC-12, OC-48, and OC-192 speeds).

1:N protection

An electrical card protection scheme that allows a single protect card to provide protection for several working cards (DS-1 and DS-3 speeds). If a 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 to the working card.

10BaseT

Standard 10 Mbps local area network over unshielded twisted pair copper wire.

100BaseT

Standard 100 Mbps local ethernet network.

100BaseTX

Specification of 100BaseT that supports full duplex operation.

A

Access drop

Points where network devices can access the network.

ACO

Alarm cutoff.

Active card

A card that is working or carrying traffic. A card provisioned as working can be an active card or, after a protection switch, a protect card can be an active card.

ACT/STBY

Active/Standby.

Address mask

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the portion that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

ADM

(Add/drop multiplexers). Linear ADMs allow signals to be added to a SONET span or dropped from a SONET span. An ADM has three or more nodes.

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.

AIC

Alarm Interface Controller.

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. See also *TID*.

AIP

Alarm Interface Panel.

AIS

Alarm Indication Signal.

AIS-L

Line Alarm Indication Signal.

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.

ANSI

American National Standards Institute.

APS

(Automatic Protection Switching). SONET switching mechanism that routes traffic from working lines to protect lines if a line card failure or fiber cut occurs.

ARP

Address Resolution Protocol.

APSB

Alarm Protection Switching Byte.

ATAG

(Autonomous Message Tag). ATAG is used for TL1 message sequencing. See also *CTAG*.

ATM

Asynchronous Transfer Mode.

AWG

American Wire Gauge

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.

Backbone

The part of the network that carries the heaviest traffic or joins LANs together.

BER

(Bit Error Rate). Ratio of received bits that contain errors.

BIC

Backplane Interface Connector.

BIP

Bit Interleaved Parity.

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. See also *UPSR*.

Blue band

Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 SDH operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

BNC

Bayonet Neill-Concelman (coaxial cable bayonet-locking connector).

BPDU

Bridge Protocol Data Unit.

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. See also *MAC address*.

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. See also *MAC address.*

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. See also *SONET.*

CAT 5

Category 5 (cabling).

CCITT

Comité Consultatif International Télégraphique et Téléphoniques. (Formerly ITU.)

CEO

Central Office Environment.

CEV

Controlled Environment Vaults.

CLEI

Common Language Equipment Identifier code.

CLNP

Correctionless Network Protocol.

cm

Centimeter.

CMIP

Common Management Information Protocol.

COE

Central Office Environment.

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.

CORBA

Common Object Request Broker Architecture.

CPE

Customer Premise Environments.

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. See also *ATAG*.

CTC

(Cisco Transport Controller). A Java-based graphical user interface (GUI) that allows operations, administration, maintenance, 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 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 SDCC or LDCC. See also *LDCC* and *SDCC*.

DCN

Data Communications Network.

DCS

Distributed Communications System.

Default router

If the ONS 15454 must communicate with a device on a network to which the ONS 15454 is not connected, packets are sent to this router to be distributed.

Demultiplex

To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. Compare *Multiplexing.*

Destination

The endpoint where traffic exits an ONS 15454 network. Endpoints can be paths (STS or STS/VT for optical card endpoints), ports (for electrical circuits, such as DS1, VT, DS3, STS), or cards (for circuits on DS1 and Ethernet cards). See also STS, and *VT.*

DRAM

Dynamic Random-Access Memory.

Drop

See *Destination*.

DS-1

Digital Signal Level One.

DS1-14

Digital Signal Level One (14 ports).

DS1N-14

Digital Signal Level One (N-14 ports).

DS-3

Digital Signal Level Three.

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). 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.

EFCA

Electrical Facility Connection Assembly.

EFT

Electrical Fast Transient/Burst.

EIA

(Electrical Interface Assemblies). Provides backplane connection points for the DS-1, DS-3, and EC-1 cards.

ELR

Extended Long Reach.

EMC

Electromagnetic compatibility.

EMI

(Electromagnetic Interference). Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

EML

Element Manager Layer.

EMS

Element Management System.

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

(Engineered Orderwire). A permanently connected voice circuit between selected stations for technical control purposes.

ERDI

Enhanced Remote Defect Indicator.

ES

Errored Seconds.

ESD

Electrostatic Discharge.

ESF

Extended Super Frame.

Ethernet switch

A type of Ethernet LAN device that increases 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.

ETSI

European Telecommunications Standards Institute.

Extended SNCP

(Extended Subnetwork Connection Protection). Extended SNCP extends the protection scheme of a subnetwork connection protection ring (SNCP) beyond the basic ring configuration to the meshed architecture of several interconnecting rings. See *SNCP*.

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.*

FC

Failure count.

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.

FE

Frame Bit Errors.

FG1

Frame Ground #1 (pins are labeled "FG1," "FG2," etc.)

FMEC

Front Mount Electrical Connection.

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.

FSB

Field Service Bulletin.

G

Gateway

An electronic repeater device that intercepts and steers electrical signals from one network to another.

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.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GR-153-CORE

General Requirements #253 Council of Registrars.

GR-1089

General Requirements #1089.

GUI

Graphical User Interface.

H

Hard reset

The physical removal and insertion of a TCC+ card, also known as reseating a card or performing 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

IEC
1. 1. InterExchange Carrier.
2. 2. International Electrotechnical Commission.

IEEE

Institute of Electrical and Electronics Engineers.

IETF

Internet Engineering Task Force.

Input alarms

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

I/O

Input/Output.

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.

IPPM

Intermediate-Path Performance Monitoring.

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.

ITU-T

International Telecommunication Union - Telecommunication Standards Sector.

J

JRE

Java Runtime Environment.

K

K bytes

Automatic protection-switching bytes 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.

LDCC

Line Data Communication Channel.

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 terminating equipment (LTE)

Refers to line cards which terminate the line signal in the ONS 15454.

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 has link integrity if it is intact.

LOF

Loss of Frame.

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.

LOP

Loss of Pointer.

LOS

Loss of Signal.

LOW

(Local Orderwire). A communications circuit between a technical control center and selected terminal or repeater locations.

LTE

Line Terminating Equipment.

LVDS

Low-Voltage Differential Signal.

M

MAC

Media Access Control.

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.

Mbps

Megabits per second.

MBps

Megabytes per second.

MHz

Megahertz.

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.

MIME

Multipurpose Internet Mail Extensions.

MS

Multiplex Section.

MS-FERF

Multiplex Section Far-end Receive Failure.

MSP

Multiplex Section Protection.

MS-SPRing

(Multiplex Section Shared Protection Ring.) SDH ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically rerouted onto the protection fiber.

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 signals to be transmitted simultaneously across a single physical channel. Compare *Demultiplex*.

Mux/Demux

Multiplexer/Demultiplexer.

Muxed

Multiplexed. See *Multiplexing*.

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.

NEBS

Network Equipment-Building Systems.

NEL

Network Element Layer.

Network number

Part of an IP address that specifies the network where the host belongs.

NML

Network Management Layer.

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.

O

OAM&P

(Operations, Administration, Maintenance, and Provisioning). Provides the facilities and personnel required to manage a network.

OC

Optical carrier.

OOS AS

Out of Service Assigned.

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. See *Local orderwire*.

OSI

Open Systems Interconnection.

OSPF

Open Shortest Path First.

OSS

Operations Support System.

OSS/NMS

Operations Support System/Network Management System.

Output contacts (controls)

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).

PCM

Pulse Code Modulation.

PCMCIA

Personal Computer Memory Card International Association.

PCN

Product Change Notice(s).

PDI-P

STS Payload Defect Indication - Path.

Ping

(Packet internet grouper). ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

Pointer justification

In SONET, the mechanism used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks.

POP

Point of Presence.

PM

Performance Monitoring.

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.

Protect card

A card in a protection pair or scheme that is provisioned as a protect card to the working card. If the working card fails, the protect card becomes active. See also *working card.*

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.*

PSC

Protection-Switching Count.

PSD

Protection-Switching Duration.

PTE

Path-Terminating Equipment.

Q

Queue

In routing, a backlog of packets waiting to be forwarded over a router interface.

R

RAM

Random Access Memory.

RDI-L

Remote Defect Indication - Line.

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 SDH operate on wavelengths between 1547.72nm and 1560.61nm.

RES

Reserved.

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 (traffic) 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.

RJ-45

Registered Jack #45 (8-pin).

RMA

Return Materials Authorization.

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.

RS-232

Recommended Standard #232 (ANSI Electrical Interface for Serial Communication).

Rx

Receive.

S

SCI

Serial Communication Interface.

SCL

System Communications Link.

SDCC

Section Data Communication Channel.

SDH

(Synchronous Digital Hierarchy). European standard that defines a set of rate and format standards that are transmitted using optical signals over fiber. SDH is similar to SONET, with a basic SDH rate of 155.52 Mbps. Compare *SONET*.

SEF

Severely Errored Frame.

SELV

Safety Extra-Low Voltage.

SES

Severely Errored Seconds.

SF

Super Frame.

SML

Service Management Layer.

SMF

Single Mode Fiber.

SNCP

(Subnetwork Connection Protection Ring). Path-switched SDH 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.

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 TCC+ 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). See also *STS* and *VT*.

Span

An optical path between two nodes.

Spanning tree

A 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

(Synchronous 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*.

Standby card

A card that is not active or carrying traffic. A standby card can be a protect card or, after a protection switch, a working card can be a standby card.

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

1. 1. Shielded Twisted Pair.

2. 2. 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 and STA*.

STS

(Synchronous Transport Signal, used generically when speaking of SONET signals.)

STS-1

(Synchronous Transport Signal Level 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*.

SWS

SONET WAN switch.

SXC

SONET Cross Connect ASIC.

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*.

TAC

Technical Assistance Center.

Tag

Identification information, including a number plus other information.

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). 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.

TDS

Time-Division Switching.

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. See also *AID*.

TL1

Transaction Language 1.

TLS

(Transparent LAN Service). Provides private network service across a SONET backbone.

TMN

Telecommunications Management Network.

Transponder

Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength. See also *DWDM*.

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. See also *CTM*.

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*.

TSA

Time-Slot Assignment.

TSI

Time-Slot Interchange.

Tunneling

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme.

Tx

Transmit.

U

UAS

Unavailable Seconds.

UDP/IP

User Datagram Protocol/Internet Protocol.

UID

User Identifier.

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. See also *BLSR*.

Upstream

Set of frequencies used to send data from a subscriber to the head end.

UTC

Universal-Time Coordinated.

UTP

Unshielded Twisted Pair.

V

VDC

Volts Direct Current.

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. See also *Tributary.*

VT1.5

Virtual Tributary that equals 1.544 Mbps.

VT layer

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.

W

W

Watts.

WAN

Wide Area Network.

Working card

A card that is provisioned as an active, primary card. Traffic cards in a protection pair are provisioned as working or protect See also *Protect card.*

X

XC

Cross Connect

XCVT

Cross Connect Virtual Tributary.

X.25

Protocol providing devices with direct connections to a packet-switched network.