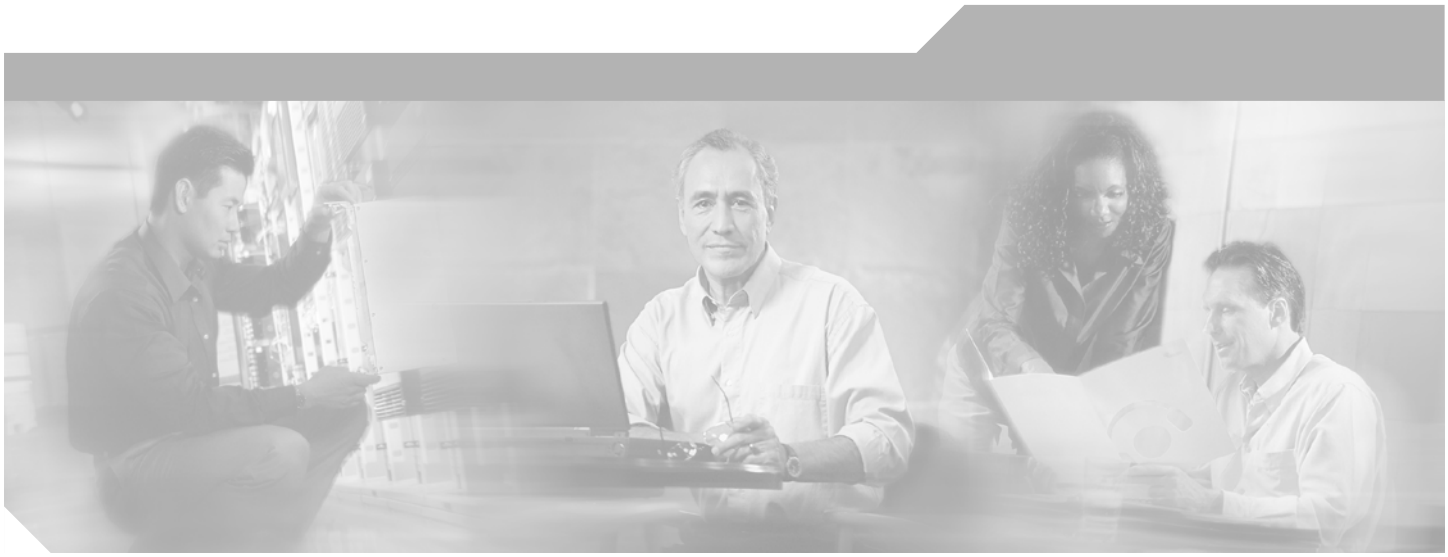


Cisco ONS 15600 SDH Reference Manual

Product and Documentation Release 1.4
February 2004

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

Customer Order Number: DOC-7816212=
Text Part Number: 78-16212-01

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

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

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

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

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

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

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

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

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

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

Cisco ONS 15600 SDH Reference Manual, R1.4

About this Manual

This section explains the objectives, intended audience, and organization of this *Cisco ONS 15600 SDH Reference Manual* and describes the conventions that convey instructions and other information.

This section provides the following information:

Document Objectives

The *Cisco ONS 15600 SDH Reference Manual* provides conceptual information for the Cisco ONS 15600 SDH.

Usethe *Cisco ONS 15600 SDH Reference Manual* in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this *Cisco ONS 15600 SDH Reference Manual*, you should be familiar with Cisco or equivalent optical transmission equipment.

Document Organization

Table 1 Cisco ONS 15600 SDH Reference Guide Chapters

Title	Summary
Chapter 1, "Shelf and Backplane Hardware"	Includes descriptions of the rack, backplane, power and ground, fan-tray assembly, air filter, and card slots.
Chapter 2, "Cards Features and Functions"	Includes descriptions of the Timing and Shelf Controller (TSC), Core Cross Connect (CXC), Synchronous Transport Module (STM)-16 LH, and STM-64 LH cards, as well as card temperature ranges and card compatibility.
Chapter 3, "Card Protection"	Includes optical card protection methods.
Chapter 4, "Cisco Transport Controller Operation"	Includes information about Cisco Transport Controller (CTC) installation, the CTC window, computer requirements, software versions, and database reset and revert.
Chapter 5, "Security and Timing"	Includes user set up and security, and node/network timing.
Chapter 6, "Circuits and Tunnels"	Includes virtual containers (VC4), bidirectional or unidirectional, revertive or nonrevertive, optical, multiple, and path trace circuit information.
Chapter 7, "SDH Topologies"	Includes the SDH configurations used by the ONS 15600 SDH; including MS-SPRings, linear ADMs, subnetwork connection protection rings, and optical bus configurations, as well as information about upgrading optical speeds within any configuration.
Chapter 8, "IP Networking"	Includes IP addressing scenarios and information about IP networking with the ONS 15600 SDH.
Chapter 9, "Performance Monitoring"	Includes performance monitoring statistics for all cards.
Chapter 10, "SNMP"	Explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15600 SDH.
Chapter 11, "Alarm Monitoring and Management"	Explains alarm and event monitoring in the Cisco ONS 15600 SDH.

Related Documentation

Use this *Cisco ONS 15600 SDH Reference Manual, R1.4* in conjunction with the following referenced publications:

- *Cisco ONS 15600 SDH Procedure Guide*
- *Cisco ONS 15600 SDH Troubleshooting Guide*

- *Cisco ONS 15600 SDH TL1 Test Access Guide*

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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 translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Product Safety and Compliance Information* document. This publication describes the international agency compliance and safety information for the Cisco ONS 15600 systems. It also includes translations of the safety warnings that appear in the ONS 15600 system documentation.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

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

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15600 product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

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

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Shelf and Backplane Hardware

This chapter provides a description of Cisco ONS 15600 SDH shelf and backplane hardware. Card and cable descriptions are provided in Chapter 2, "Cards Features and Functions."

To install equipment, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

Note The Cisco ONS 15600 SDH assembly is intended for use with telecommunications equipment only.

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

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

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.**

Warning **Blank faceplates (filler 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, power modules, and faceplates are in place.**

Note The ONS 15600 SDH is designed to comply with Telcordia GR-1089-CORE Type 2 and Type 4 equipment and ETS 300 386-1 and 60950 equipment. Install and operate the ONS 15600 SDH only in environments that do not expose wiring or cabling to the outside plant. Acceptable applications include Central Office Environments (COEs), Electronic Equipment Enclosures (EEEs), Controlled Environment Vaults (CEVs), huts, and Customer Premise Environments (CPEs).

1.1 Installation Overview

The ONS 15600 SDH is a Network Equipment Building System III (NEBS III)-compliant, environmentally hardened shelf assembly that ships as a single shelf in a bay assembly for Release 1.4. The ONS 15600 SDH comes with the power distribution unit (PDU), shelf, fans, and backplane already installed. The front door of the ONS 15600 SDH allows access to the shelf assembly, fan-tray assembly, and cable-management area. The customer access panel (CAP) on the back of the shelf provides access to alarm contacts, external interface contacts, and timing contacts. Power and ground terminals are located on the top left and right sides of the bay.

Caution Voltage to the alarm circuits should not exceed 48 VDC.

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

The ONS 15600 SDH comes mounted in a custom, certified-NEBS-2000 rack. The bay assembly, including the rack, fan trays, and PDU, weighs approximately 500 pounds (226.8 kg) with no cards installed.

ONS 15600 SDH STM-N cards have OGI (Optical Gateway Interface) connectors on the card faceplate; available connector termination types are SC, ST, and FC. Fiber optic cables are routed to the front of the STM-N cards.

The ONS 15600 SDH is powered using –48 VDC power but might range from –40.5 to –72 VDC. Input power is accessible from the sides of the bay, and output power is accessible at the rear of the bay. Cisco supports dual office-power feeds only.

Install the ONS 15600 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 **Ultimate disposal of this product should be handled according to all national laws and regulations.**

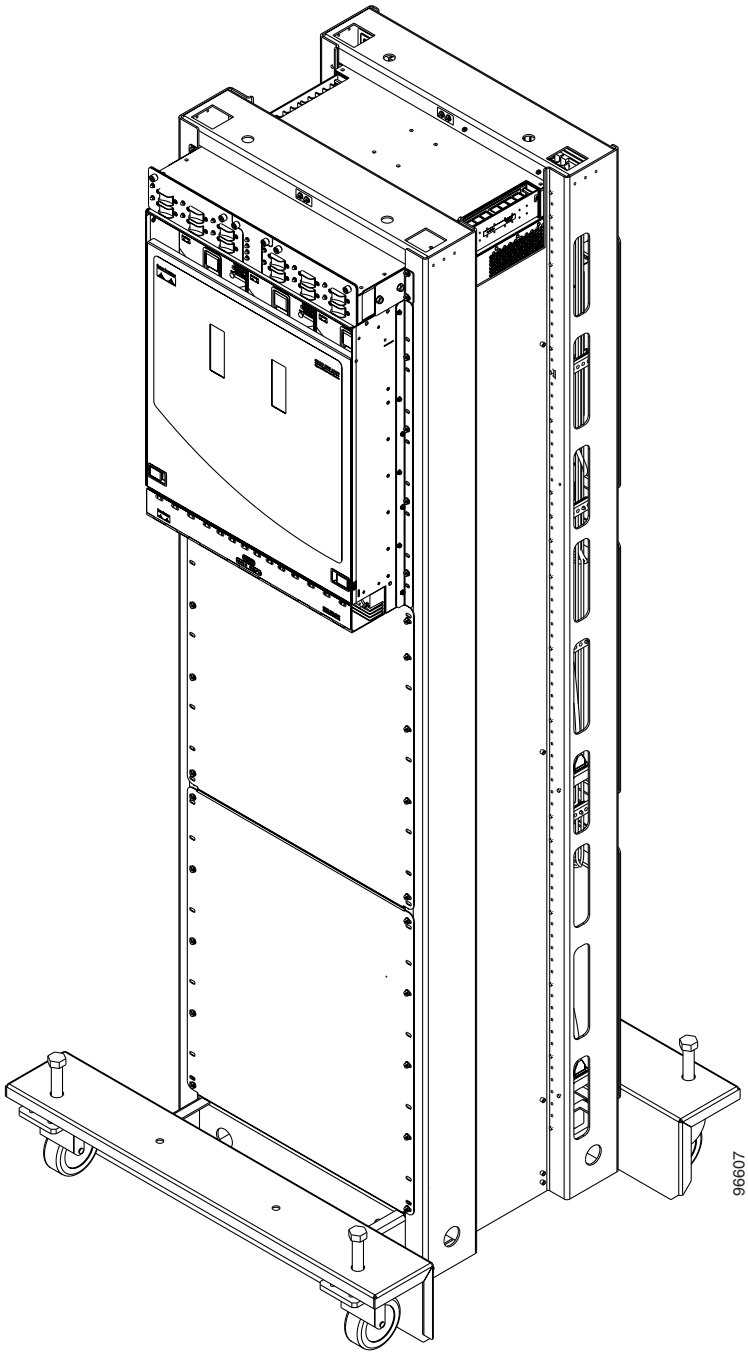
1.2 Bay Installation

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 122°F (50°C). To prevent airflow restriction, allow at least 24 inches (60 cm) of clearance around the ventilation openings.**

Note In this chapter, the terms “ONS 15600 SDH” and “bay assembly” are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, bay assembly refers to the physical steel enclosure that holds the shelves and PDU, and ONS 15600 SDH refers to the entire system, both hardware and software.

To install the ONS 15600 SDH, you must first unpack the bay assembly. Two custom ramps and two dollies are available to assist you with the removal of the bay from the shipping pallet and transportation to the installation location. Figure 1-1 shows the bay assembly with the dollies installed.

Figure 1-1 ONS 15600 SDH with Dollies Installed

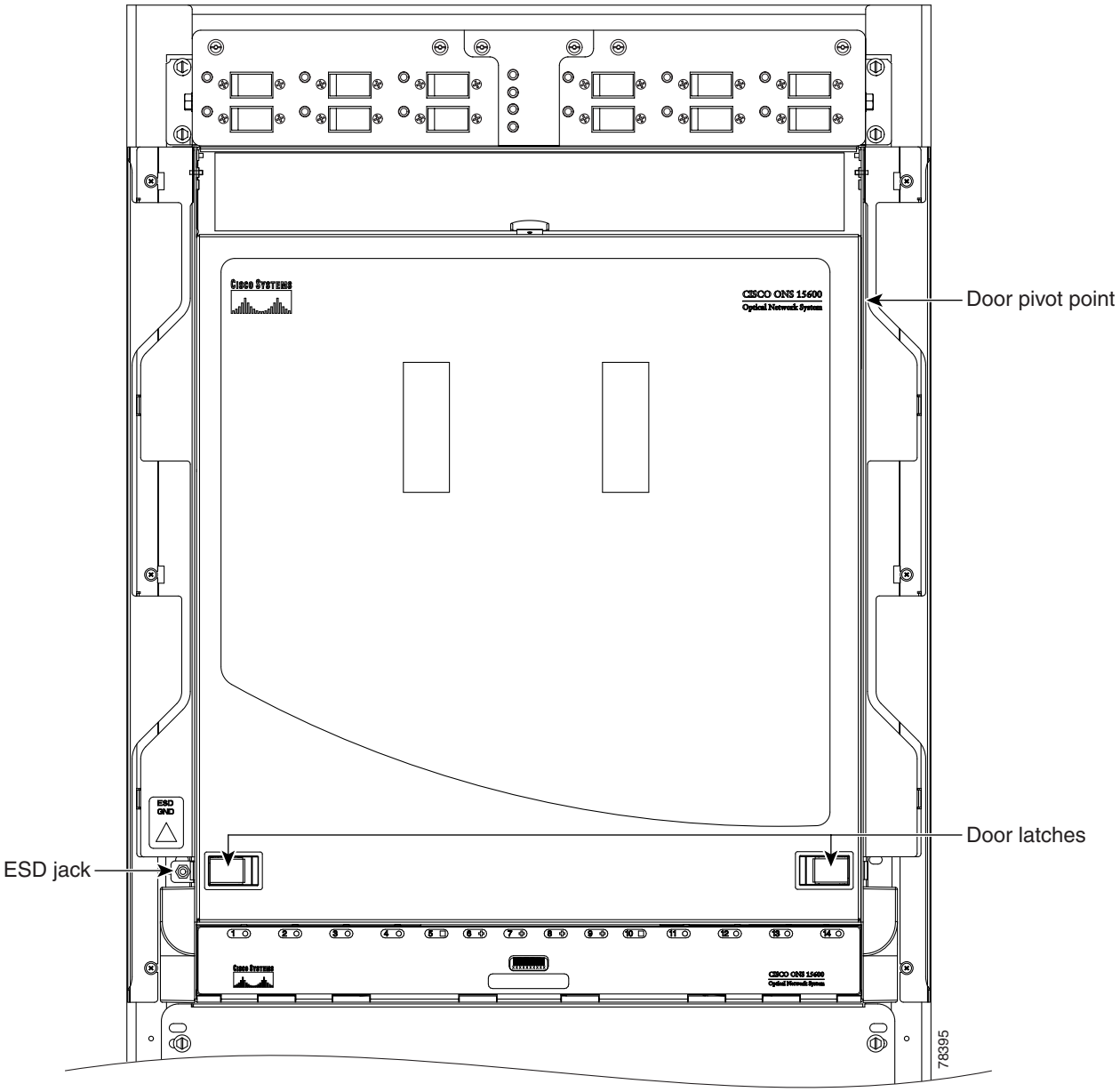


The ONS 15600 SDH shelf measures 25 in. high, 19-9/16 in. wide, and 23 in. deep (63.5 cm by 49.7 cm by 58.3 cm). A maximum of three ONS 15600 SDHs can fit in a custom 7-ft (2.1336-m) equipment rack. The ONS 15600 SDH that ships within a rack is 83-7/8 in. high, 23-5/8 in. wide, and 23-5/8 in. deep (213 cm by 60 cm by 60 cm).

1.3 Front Door

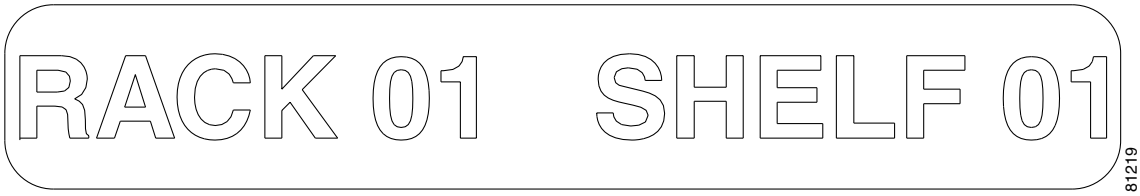
The ONS 15600 SDH features a door to the front compartment that you can open by releasing the latches on the bottom left and right sides of the door. The front door provides access to the shelf, cable-management tray, and fans (Figure 1-2).

Figure 1-2 ONS 15600 SDH Front Door



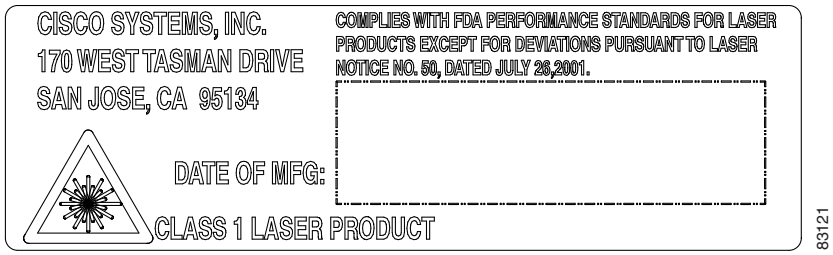
You can remove the front door of the ONS 15600 SDH to provide unrestricted access to the front of the shelf. A label is pasted in a box in the center of the swing-down door that covers the fiber routers (Figure 1-3). This label designates the position of the rack and shelf in a lineup.

Figure 1-3 Bay Label



The front door also has a Class I laser warning (Figure 1-4).

Figure 1-4 Laser Warning Label



1.4 Rear Covers

The ONS 15600 SDH has an optional plastic rear cover that is held in place with six 6-32 x 3/8 inch Phillips screws. This plastic cover provides additional protection for the cables and connectors on the backplane (Figure 1-5).

Figure 1-5 Plastic Rear Cover

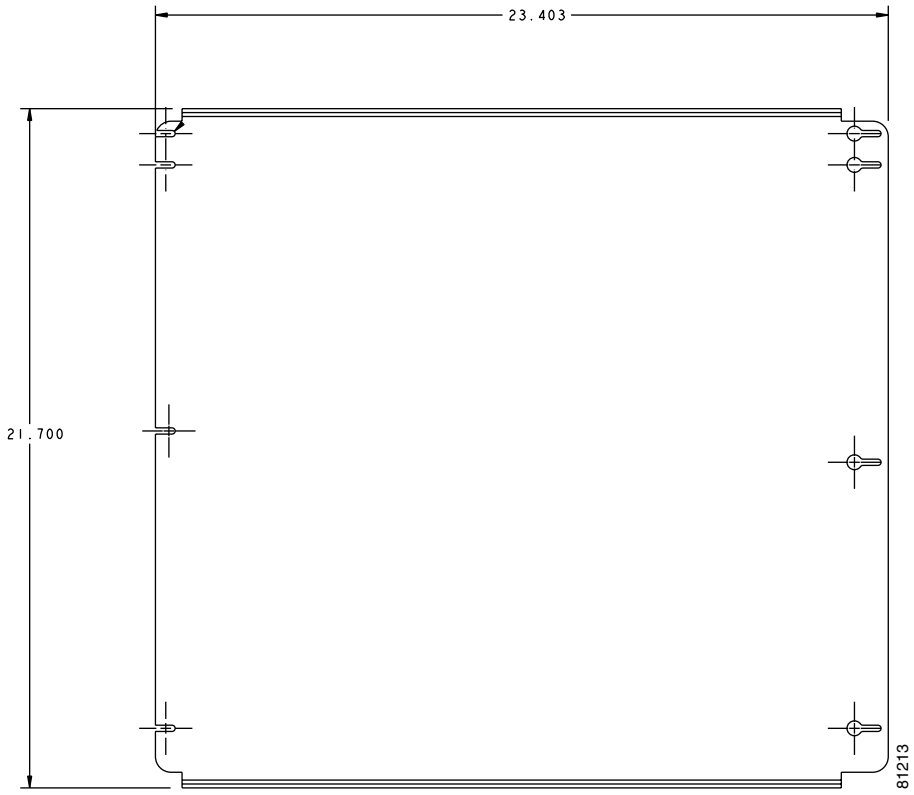
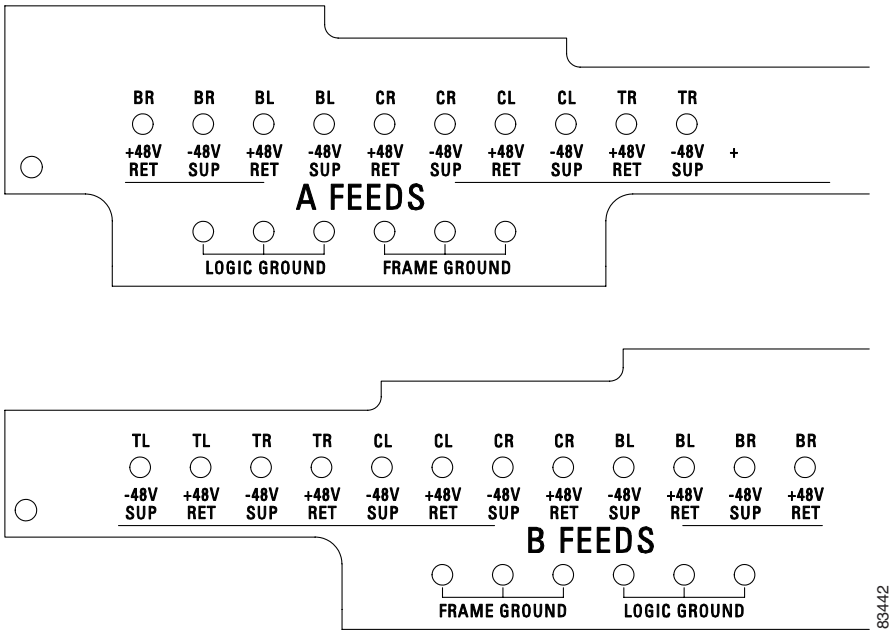


Figure 1-6 shows the bus bar covers.

Figure 1-6 PDU Bus Bar Cover



1.5 Cable Routing

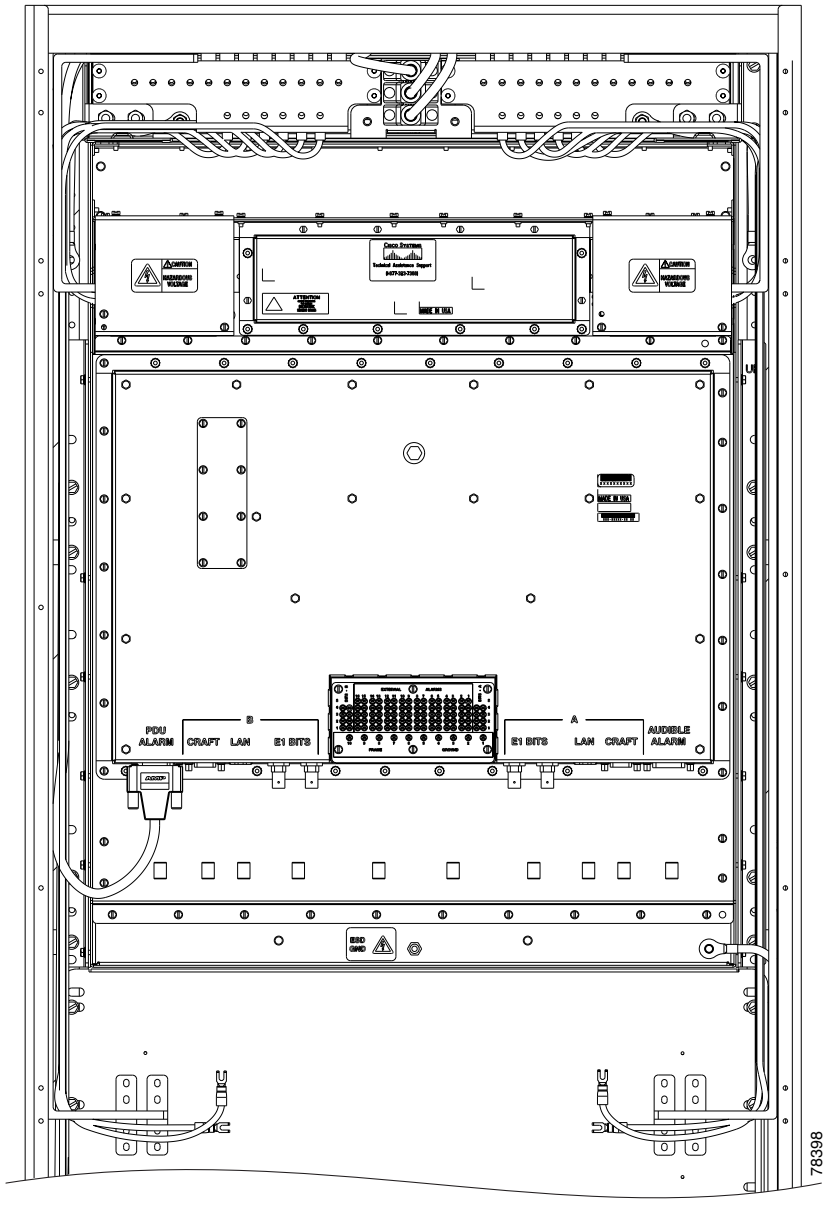
The narrow and wide cable routing modules (CRMs) can be installed on the sides of the bay to manage and contain the optical cables as they are routed away from the bay. You can use both types of fiber routing systems with overhead or under-floor cabling.

1.6 Customer Access Panel

The customer access panel (CAP) is located in the middle of the rear of the shelf. The CAP provides an alarm pin field, timing, and LAN connections. The CAP plugs into the backplane using 2-mm Hard Metric connectors with 752 pins and is held in place with one large captive bolt and multiple screws. Figure 1-7 shows the location of the CAP on the back of the shelf.

Note Only T1 (100 ohm) and E1 (120 ohm) building integrated timing supply (BITS) is supported in Software R1.4.

Figure 1-7 Rear of the ONS 15600 SDH, Including the CAP



The ONS ONS 15600 SDH CAP provides the following:

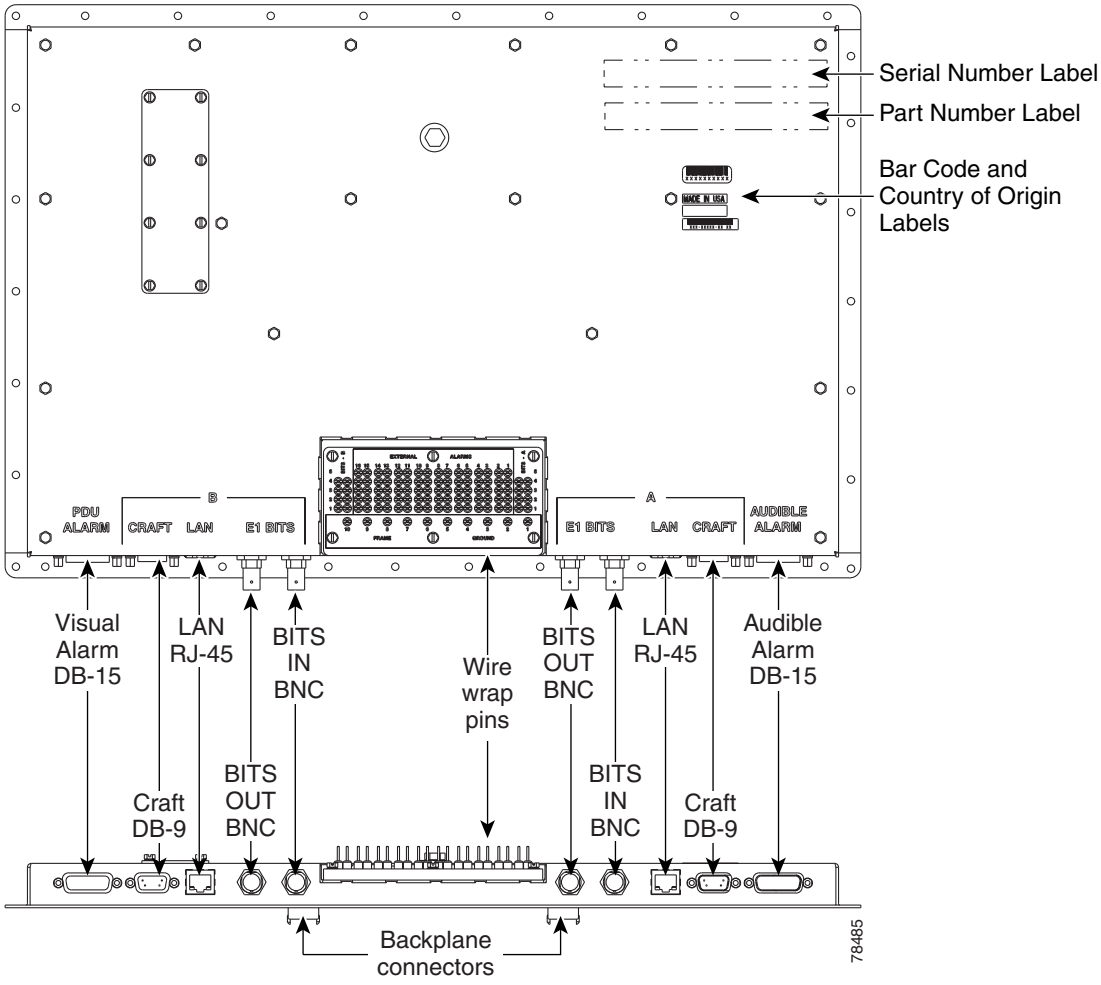
- BITS T1 (100 ohm)/E1 (120 ohm) interfaces via wire-wrap pins.
- Two Ethernet interfaces via RJ-45 connectors with internal transformer isolation.
- An EIA/TIA-232 craft interface via DB-9 connectors. This interface is surge-protected and provides EMI filtering. Two interfaces are provided for redundancy.
- Four audio alarm interfaces via a DB-15 connector that is surge-protected and EMI-filtered. The audio alarm indication is provided by the Timing and Shelf Controller (TSC) card and this interface can receive a signal to disable the audio alarm.

- Four visual alarm interfaces via a DB-15 connector that is surge-protected and EMI-filtered. The visual alarm indication is provided by the TSC card and the signal is connected to the PDU where LEDs indicate the alarm status and severity.
- Environmental (external) alarms and controls (16 inputs and 16 outputs) via wire-wrap pins. The interface is surge-protected and provides isolation by using an opto-isolator for alarm inputs and relays for alarm outputs. By connecting to different wire-wrap pins on the CAP, the alarm outputs can be configured for either normally open (NO) or normally closed (NC) operation. Alarms are initiated by shorting these contacts. The alarm input interface provides a pair of positive and negative wire-wrap pins.

The isolation and termination meet the intrabuilding lightning surge specified in Telcordia GR-1089 and ETS 300 386-1 and 60950. The CAP has –48 VDC monitoring with I^2C interface and nonvolatile memory to store the CAP revision information.

Figure 1-8 shows the CAP faceplate.

Figure 1-8 CAP Faceplate and Connections



If the CAP fails, the node raises an EQPT alarm. You can replace the CAP on an in-service system without affecting traffic. To replace a CAP, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*. Always replace the CAP during a maintenance window.

1.7 Alarm, Timing, LAN, and Craft Pin Connections

Caution Always use the supplied ESD wristband when working with a powered ONS 15600 SDH or any ONS 15600 SDH components. Plug the wristband cable into one of the ESD jacks located on the lower-left outside edge of the bay assembly and at the bottom rear of the shelf.

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.**

The ONS 15600 SDH has a backplane pin field located at the bottom rear of the shelf that is part of the CAP. The CAP provides 0.045 square inch (0.290 square centimeter) wire-wrap pins for enabling alarm inputs and outputs and timing input and output. This section describes the backplane pin field and pin assignments, as well as timing and LAN connections. See the "1.6 Customer Access Panel" section on page 1-8 for more information.

1.7.1 External Alarm and Control Contact Installation

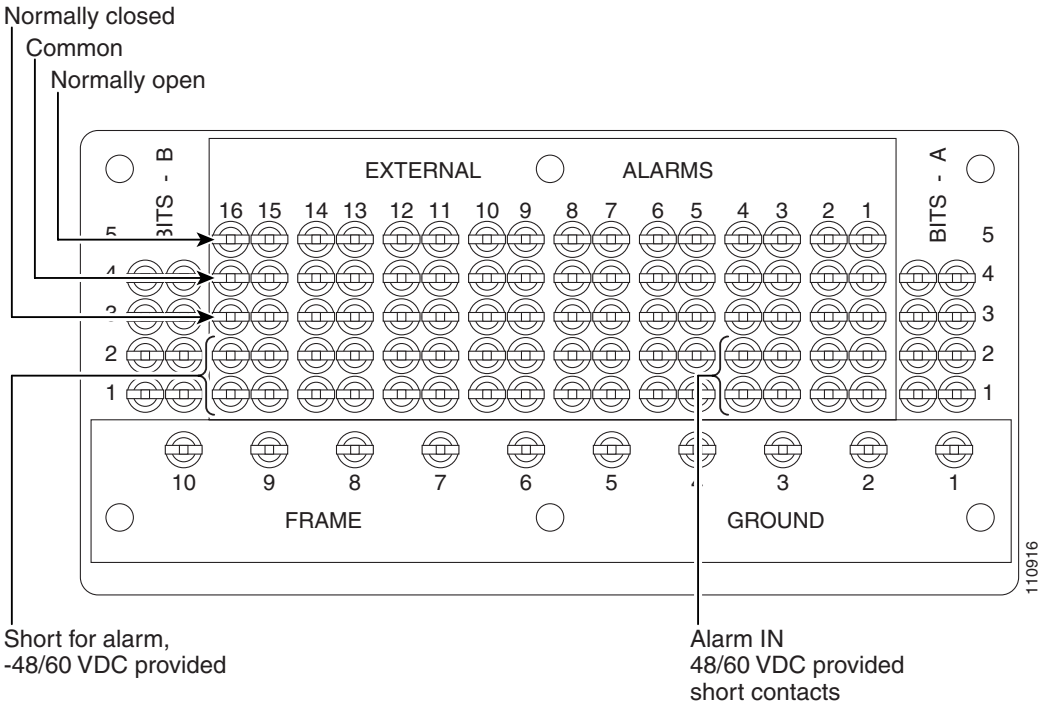
The external (environmental) alarm contacts consist of the wire-wrap pin field and two D-Sub 15s. The alarm pin field supports up to 16 alarm inputs (external alarms) and 16 alarm outputs (external controls). The two D-Sub 15s support four audible alarms, four visual alarms, one alarm cutoff (ACO), a PDU Fail A, and a PDU Fail B.

By connecting to different wire-wrap pins on the CAP, the alarm outputs can be configured for either NO or NC operation (see Figure 1-9). The alarm inputs consist of two wire-wrap pins on the CAP and the alarm outputs consist of three wire-wrap pins.

1.7.1.1 Visual and Audible Alarms

Visual and audible alarm contacts are provisioned as Critical, Major, Minor, and Remote. Figure 1-9 shows alarm pin assignments.

Figure 1-9 Alarm Pin Assignments on the CAP



Visual and audible alarms can be wired to trigger an alarm light at a central alarm collection point when the corresponding contacts are closed.

1.7.1.2 Alarm Cutoff (ACO) and PDU Alarms

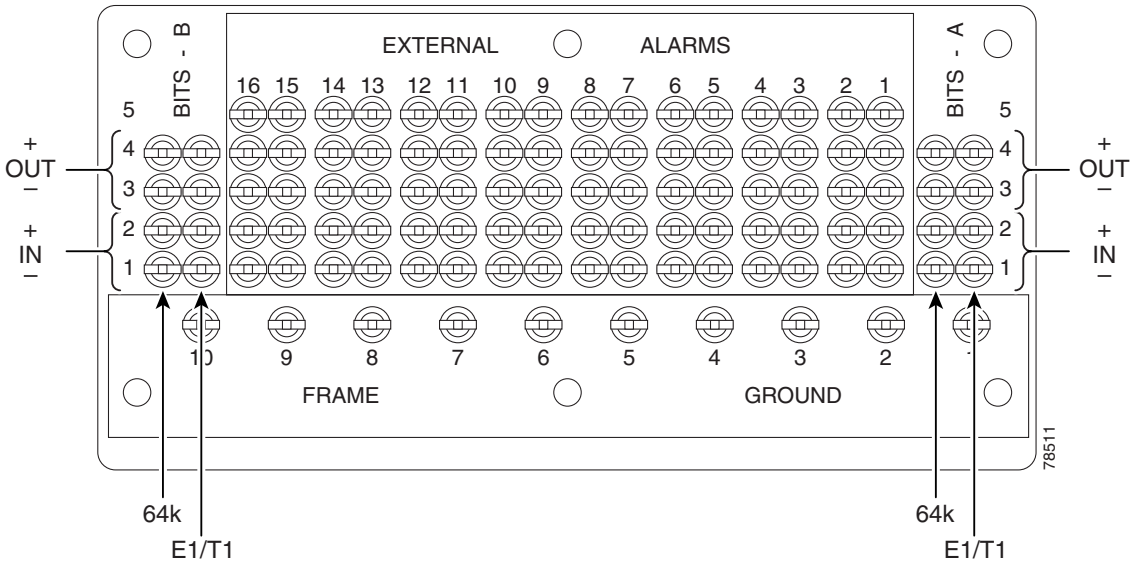
The PDU Alarm connection controls the visual alarm indicators on the front of the PDU. You can also activate the alarm cutoff (ACO) function by pressing the ACO button on the TSC card faceplate. The ACO function extinguishes all audible alarm indications, but the alarm is still raised in Cisco Transport Controller (CTC).

1.7.2 Timing Installation

The ONS 15600 SDH backplane supports two 100-ohm BITS clock pin fields. Figure 1-10 shows the pin assignments for the BITS timing pin fields.

Note Refer to Telcordia SR-NWT-002224 and ITU G.811 for rules about provisioning timing references.

Figure 1-10 BITS Timing Connections on the CAP



1.7.3 LAN Installation

Use a straight-through LAN cable with the LAN port on the ONS 15600 SDH CAP to connect the ONS 15600 SDH to a hub, switch, or a LAN modem for remote access to the node. Use a crossover cable when connecting the CAP to a workstation. You can also use a straight-through or crossover LAN cable with the LAN port on the active TSC faceplate to connect a workstation or to connect the ONS 15600 SDH to the network.

Note Do not use the LAN port on the active TSC for remote monitoring because you will lose connectivity to the node if the other TSC in the shelf becomes the active TSC.

1.7.4 TL1 Craft Interface Installation

To open a TL1 session using the craft interface on a PC, use the RJ-45 port on the active TSC card to access the system using a standard web browser. If a browser is not available, you can access the system using one of the two EIA/TIA-232 ports on the CAP. Each EIA/TIA-232 port supports VT100 emulation so that you can enter TL1 commands directly without using a web browser. Because the CAP EIA/TIA-232 port is set up as a data terminal equipment (DTE) interface, you must use a 3-pair swapping null modem adapter when you are working in a UNIX or PC environment so that the TXD/RXC, DSR/DTR, and CTS/RTS pins are swapped. Use a standard pin D-sub cable when connecting to a PC. Refer to the *Cisco ONS 15600 SDH TL1 Command Guide* for more information.

Note Do not use the LAN port on the active TSC for remote monitoring because you will lose connectivity to the node if the other TSC in the shelf becomes the active TSC.

1.8 Power Distribution Unit

The power distribution unit (PDU) consists of a mounting chassis, A- and B-side power modules, an alarm module, and a rear input/output (I/O) unit. The ONS 15600 SDH PDU has LEDs that alert you to critical, major, minor, and remote alarms on the node. Each module can support three 100 A input power feeds, 48 VDC power load (based on a fully loaded ONS 15600 SDH shelf). The PDU supplies six 50 A power feeds to the shelves. (The PDU provided with the ONS 15600 SDH is capable of supplying power to up to three shelves.)

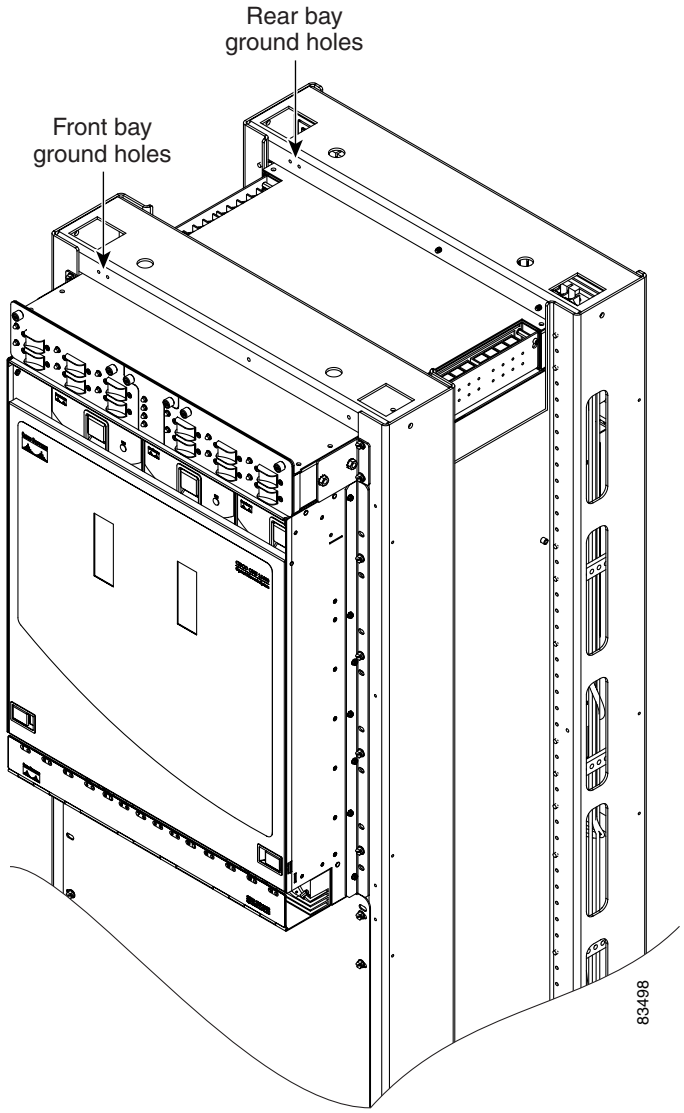
A three-shelf bay at the minimum operational voltage of –36 VDC requires 69 A per feed (207 A total). A three-shelf bay at the nominal operational voltage of –48 VDC requires 52 A per feed (156 A total). Each of the three feeds should be protected by its own 100 A breaker. A bus bar system, rather than wiring, provides a reliable, low resistance path to the ONS 15600 SDH shelf. Figure 1-6 on page 1-8 shows the PDU output covers found at the top rear of the bay.

1.9 Power and Ground Description

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Ground the equipment according to Telcordia and ITU standards or local practices. The ground connection is located on the front of the bay's top horizontal rails. The ONS 15600 SDH provides two #12 tapped holes to accommodate the grounding lug. The lug must be a dual-hole type and rated for at least 125 A capacity. Figure 1-11 shows the front and rear bay ground holes.

Figure 1-11 Front and Rear Bay Ground Holes



The main power connections are made at the PDU side terminals at the top of the bay. To install redundant power feeds, use four power cables and ground cables. For a single power feed, only two power cables and one ground cable (all rated for at least 125 A capacity) are required. Use a conductor with low impedance to ensure circuit overcurrent protection. The ground conductor must have the capability to safely conduct any faulty current that might be imposed.

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

- Red wire for battery connections (–48 VDC)
- Black wire for battery return connections (0 VDC)

The ONS 15600 SDH shelf has redundant –48 VDC power terminals on its backplane. The terminals are labeled A FEEDS and B FEEDS and are located at the top left and right sides of the shelf behind clear plastic covers.

Refer to the *Cisco ONS 15600 SDH Procedure Guide* for installation procedures to install 600-mm and 900-mm kick plates when used with narrow cable routing modules (CRMs) and CRMs respectively.

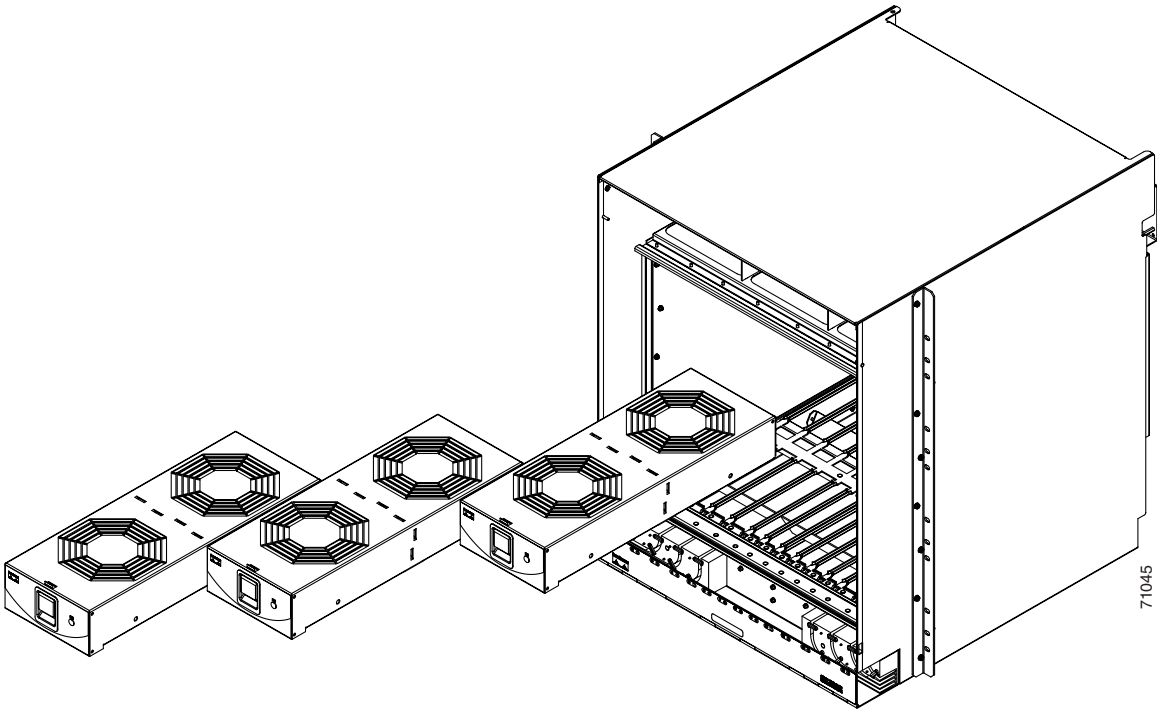
Warning **This product requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

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

1.10 Fan-Tray Assembly

The fan-tray assembly is located at the top of the ONS 15600 SDH shelf front compartment. The fan-tray assembly has three removable drawers that hold two fans each and fan-control circuitry for the ONS 15600 SDH (Figure 1-12). You should only need to access the fans if a fan fails.

Figure 1-12 Fan-Tray Assembly



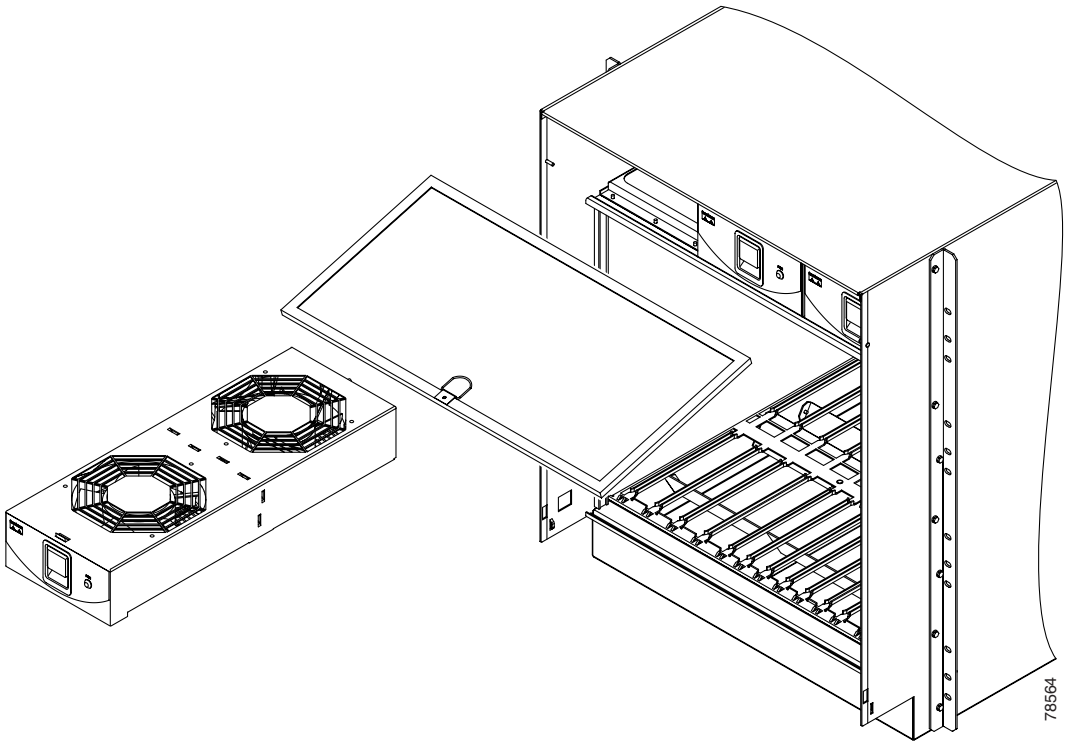
1.10.1 Air Filter

The ONS 15600 SDH contains a disposable air filter that is made of an open-cell polyurethane foam that is flame retardant and fungi resistant. The air filter is located above the three fan trays (Figure 1-13). This disposable filter is not designed to be cleaned. You can order air filter replacements from Cisco (Cisco P/N: 700-13116-xx). Replace this filter at least every 6 months and keep spare filters in stock. Refer to the *Cisco ONS 15600 SDH Troubleshooting Guide* for information about replacing the fan-tray air filter.

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Caution Do not operate an ONS 15600 SDH without a fan-tray air filter. A fan-tray filter is mandatory.

Figure 1-13 Air Filter with One Fan Tray Pulled Out



1.10.2 Fan Speed and Failure

If one or more fans fail on the fan-tray assembly, replace the fan tray where that fan resides. You cannot replace individual fans. The red FAN LED on the front of the fan tray turns on when one or more fans fail. For fan-tray replacement instructions, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*. The red FAN LED clears after you install a working fan tray.

Caution If both fans in the center fan tray are inoperative, you must replace the fan tray within five minutes of failure to avoid affecting traffic because CTC software will shut down one of the Core Cross Connect (CXC) cards.

Caution The ONS 15600 SDH requires at least one working fan in each of the three fan trays. When a single fan in a tray fails, Cisco recommends replacing the tray with a fully working tray as soon as possible.

Note Each fan tray contains two fans. The FAN LED indicates if one or both fans fail in that fan tray.

Fan speed is determined by card temperature sensors that report temperature data to the active TSC card. The sensors measure the input and output air temperature for each card. Fan speed options are low, medium, and high. For example, if a card exceeds permissible operational temperature, the fan speed increases appropriately. At initial turn-up, the default fan speed is high until the node initializes. If both TSC cards fail, the fans automatically shift to high speed. If a single TSC fails, the active TSC still controls the fan speed. Table 1-1 shows the power requirements for an individual fan in a fan tray.

Table 1-1 Power Requirements for an Individual Fan

Condition	Watts	Amps	BTU/Hr
Min. at 48 V (ambient temperature less than 25 degrees C)	12	0.25	41
Max. at 48 V (ambient temperature greater than 25 degrees C)	46	0.95	157

1.11 Cards and Slots

When a card is inserted in a card slot it will contact the shelf backplane but is not fully installed until the ejectors are fully closed.

1.11.1 Card Slot Requirements

The ONS 15600 SDH shelf has 14 card slots numbered sequentially from left to right. Slots 1 to 4 and 11 to 14 are reserved for optical (STM-N) traffic cards. These slots can host any of the ONS 15600 SDH optical cards. Slots 6/7 and 8/9 are dedicated to CXC cards, and Slots 5 and 10 house the TSC cards. Each card is keyed to fit only in an appropriate slot for that card. Unused card slots should be occupied by a filler card (blank faceplate).

Warning **Blank faceplates (filler 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, power modules, and faceplates are in place.**

Caution Do not operate the ONS 15600 SDH with a single TSC card or a single CXC card installed. Always operate the shelf with one active and one redundant standby TSC card and two CXC cards.

Shelf assembly slots have symbols indicating the type of cards that you can install in them. Each ONS ONS 15600 SDH card has a corresponding symbol. The symbol on the card must match the symbol on the slot.

Table 1-2 shows the slot and card symbol definitions.

Table 1-2 Slot and Card Symbols

Symbol Color/Shape	Definition
Orange/Circle	Any optical card (STM-16 and STM-64)
Purple/Square	TSC slot; only install ONS 15600 SDH cards with a square symbol on the faceplate
Green/Cross	CXC slot; only install ONS 15600 SDH cards with a cross symbol on the faceplate

See Chapter 2, "Cards Features and Functions," for more information about ONS 15600 SDH cards.

All physical connections to the optical cards are made through OGI (Optical Gateway Interface) connectors on the card faceplate. Table 1-3 lists the number of ports and the line rates for ONS 15600 SDH optical cards.

Table 1-3 Card Ports and Line Rates

Card	Ports	Line Rate per Port
OC48/STM16 LR/LH 16 Port 1550; OC48/STM16 SR/SH 16 Port 1310	4 physical interfaces; 4 ports per interface, totalling 16 STM-16 ports per card	2488.32 Mbps (VC4-16, VC4-16c)
OC192/STM64 LR/LH 4 Port 1550; OC192/STM64 SR/SH 4 Port 1310	4 physical interfaces; 1 port per interface, totalling 4 STM-64 ports per card	9.95 Gbps (VC4-64, VC4-64c)

1.11.2 OGI Cables

The ONS 15600 SDH faceplate has OGI connectors that terminate in either SC, ST, or FC connectors. Figure 1-14 shows the OGI to SC cable breakout for the STM-16 card.

Figure 1-14 OGI Cable Breakout

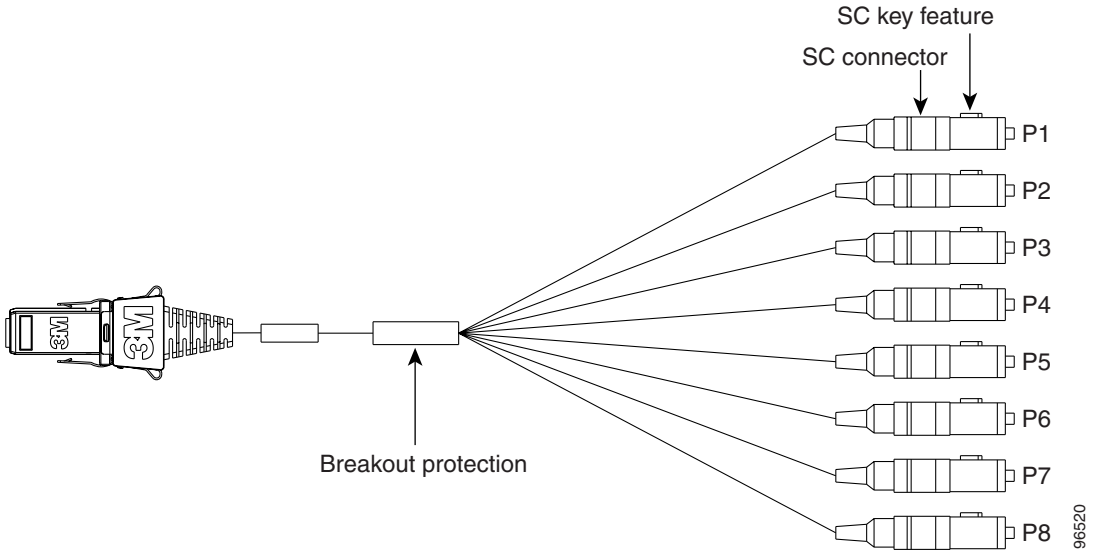
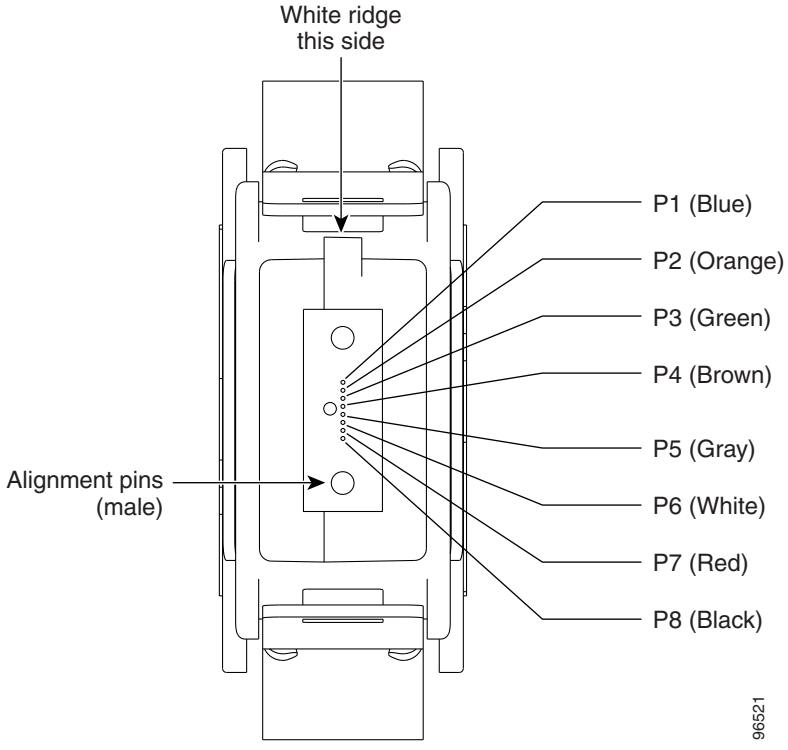


Figure 1-15 show the OGI pin breakout for the STM-16 card.

Figure 1-15 OGI Pin Breakout



1.11.3 Optical Card Cable Routing

The ONS 15600 SDH has a cable-management tray with discrete fiber routing paths for each optical card's cables. Each fiber routing path has a plastic cable latch for securing the cables in the fiber routing path. You can rotate the cable latch into two positions, open or closed; make sure that the cable latch is always completely open before you insert or remove the optical cables. Make sure all fiber-optic cables are disconnected from a card before you remove it.

1.11.4 Card Replacement

To replace an ONS 15600 SDH card with another card of the same type, you do not need to make any changes to the database; remove the old card and replace it with a new card. You can use the CTC Change Card feature to replace a card with a new card while maintaining all existing provisioning. To replace a card with a card of a different type, delete the original card from CTC, physically remove the card, and replace it with the new card.

Caution Removing any active/working card from the ONS 15600 SDH can result in traffic interruption. Use caution when replacing cards and verify that only inactive or standby cards are being replaced. If the active card needs to be replaced, switch it to standby prior to removing the card from the node.

Note An improper removal (IMPROPRMVL) alarm is raised whenever a card pull is performed, unless the card is deleted in CTC first. The alarm will clear after the card replacement is complete.

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.**

Cards Features and Functions

This chapter describes Cisco ONS 15600 SDH card features and functions.

Chapter topics include:

2.1 Common Control Cards

Follow all warnings listed on the equipment or in the documentation.

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.**

Caution When working with cards, wear the supplied ESD wristband to avoid ESD damage to the card. Plug the wristband cable into the ESD jack located on the lower-left outside edge of the shelf assembly.

Caution Do not operate the ONS 15600 SDH with a single TSC card or a single CXC card installed. Always operate the shelf with one active card and one protect card.

2.1.1 Timing and Shelf Controller Card

The Timing and Shelf Controller (TSC) card performs all system timing functions for each ONS 15600 SDH. The TSC card monitors the recovered clocks from each traffic card and two building integrated timing supply (BITS) interfaces for frequency accuracy. The TSC card is provisionable, allowing timing from any optical interface source, a BITS input source, or internal clock source as the system-timing reference. You can provision any of the clock inputs as primary or secondary timing sources, but the ONS 15600 SDH does not support mixed timing references. If you specify external timing references, your options are BITS1, BITS2, and the internal clock sources. If you select line timing, you can specify up to two line ports from which to derive timing, as well as the internal clock

sources. You cannot specify BITS as the primary reference and a line source as the secondary reference. A slow-reference tracking loop allows the TSC to synchronize with the recovered clock and enables holdover if the reference is lost.

The TSC card also provides shelf control related functions. The TSC card has a 100-Mbps Ethernet link to each card on the shelf and monitors the presence of these cards. The TSC provides bulk memory for nonvolatile storage of system software and data and provides EIA/TIA-232 and Ethernet customer interfaces. The TSC card processes and routes line and section data communications channel (DCC) traffic as well as routing the K1, K2, and K3 overhead bytes between traffic (line) cards and Core Cross Connect (CXC) cards. The TSC card controls and monitors the shelf fans and all of the alarm interfaces.

2.1.1.1 TSC Slots and Connectors

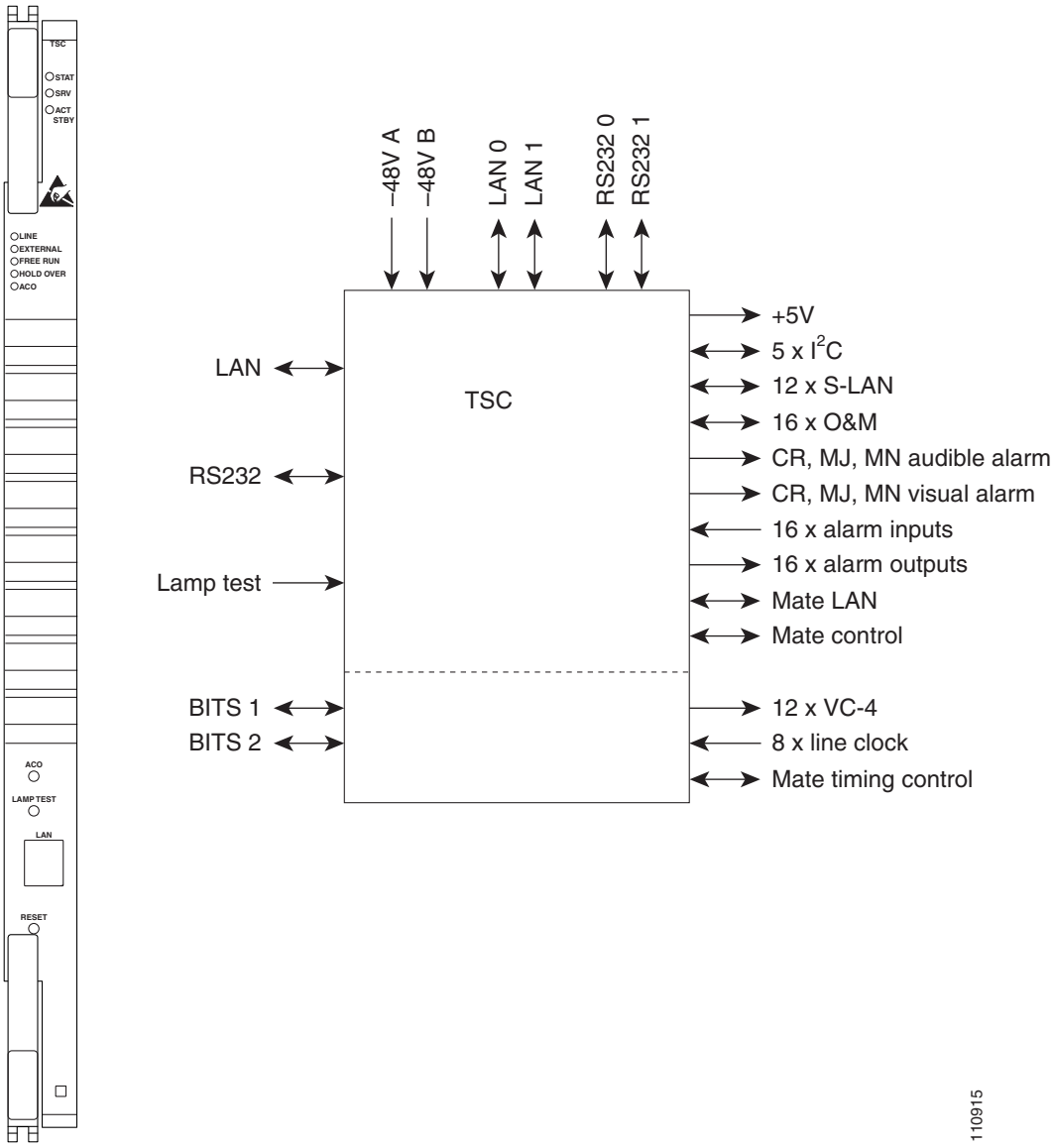
Install TSC cards in Slots 5 and 10 for redundancy. If the active TSC card fails, timing reference and control function switches to the protect TSC card. All TSC card protection switches conform to the Telcordia protection switching standard of equal to or less than 50 ms.

The TSC card features an RJ-45 10/100BaseT LAN port on the faceplate. Two additional RJ-45 10/100BaseT LAN ports and two EIA/TIA-232 DB-9 type craft user interfaces are available via the customer access panel (CAP) on the backplane.

2.1.1.2 TSC Faceplate and Block Diagram

Figure 2-1 shows the TSC card faceplate and a block diagram of the card.

Figure 2-1 TSC Card Faceplate and Block Diagram



2.1.1.3 TSC Card-Level Indicators

Table 2-1 describes the functions of the card-level LEDs on the TSC card faceplate.

Table 2-1 TSC Card-Level Indicators

Indicator LED	Color	Definition
STAT	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED will flash quickly during initialization and slowly during configuration synchronization.
SRV	Green	The service mode of the card; green indicates that the card is in use and off indicates that the card can be removed for service.
ACT/STBY	Green	The ACT/STBY (Active/Standby) LED indicates that the TSC is active (green) or standby (off).

2.1.1.4 TSC Network-Level Indicators

Table 2-2 describes the functions of the network-level LEDs on the TSC card faceplate.

Table 2-2 TSC Network-Level Indicators

Indicator LED	Color	Definition
LINE	Green	Node timing is synchronized to a line timing reference.
EXTERNAL	Green	Node timing is synchronized to an external timing reference.
FREE RUN	Green	Node is not using an external timing reference. Indicated when the timing mode is set to an internal reference or after all external references are lost.
HOLDOVER	Amber	External/line timing references have failed. The TSC has switched to internal timing and the 24-hour holdover period has not elapsed.
ACO	Amber	The alarm cutoff (ACO) push button has been activated. After pressing the ACO button, the amber ACO LED turns on. The ACO button opens the audible closure on the backplane. The ACO state is stopped if a new alarm occurs. After the originating alarm is cleared, the ACO LED and audible alarm control are reset.

2.1.1.5 TSC Push-Button Switches

Table 2-3 describes the functions of the push-button switches on the TSC card faceplate.

Table 2-3 TSC Card Push-Button Switches

Push-Button	Function
ACO	Extinguishes external audible (environmental) alarms. When this button is activated, the amber-colored ACO LED turns on.

Table 2-3 TSC Card Push-Button Switches (continued)

Push-Button	Function
LAMP TEST	Verifies that all the LEDs in the shelf are functioning properly. When this button is activated, all of the front-panel LEDs in the shelf turn on temporarily to verify operation.
RESET	Activates a soft reset of all of the main processor memory on the card. **Note** The RESET button is recessed to prevent accidental activation.

2.1.1.6 TSC Card Specifications

Table 2-4 shows the TSC card specifications.

Table 2-4 TSC Card Specifications

Specification Type	Description
CTC Software	Interface: 10/100BaseT LAN Backplane (CAP) access: RJ-45
TL1 Craft Interface	Speed: 10/100BaseT LAN Front panel access: RJ-45 type connector Backplane access: RJ-45 and EIA/TIA-232 DB-9 type connector
Synchronization	Free running access: Accuracy 4.6 ppm Holdover stability: 3.7 $x10^{-7}$ ppm/day including temperature (< 255 slips in first 24 hours) Reference: External BITS, line, internal
Operating Temperature	23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
Operating Humidity	5 to 95 percent, noncondensing
Dimensions	Height: 16.50 in. (419 mm) Width: 1.07 in. (27 mm) Depth: 18.31 in. (465 mm) Card weight: 4.0 lb (1.81 kg)
Compliance	When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950

2.1.2 Core Cross Connect Card

The Core Cross Connect card (CXC) is the central element for ONS 15600 SDH switching. The CXC card establishes connections and performs time division switching (TDS) at VC-4 and VC4-*N*c levels between ONS 15600 SDH traffic cards.

The CXC card works with the TSC card to maintain connections and set up cross-connects within the ONS 15600 SDH. You establish cross-connect and provisioning information using TL1 or Cisco Transport Controller (CTC). The TSC card stores the proper internal cross-connect information and relays the setup information to the CXC card.

2.1.2.1 CXC Switch Matrix

The switch matrix on each CXC card consists of 2,048 VC4 ports. When creating bidirectional VC4 cross-connects, each cross-connect uses two VC4 ports. This results in 1,024 bidirectional VC4 cross-connects. Any VC4 on any port can be connected to any other port, meaning that the VC4 cross-connections are non blocking. Nonblocking connections allow network operators to connect any VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c payload that is received on an STM-16 or STM-64 interface to any other interface capable of supporting the bandwidth.

The CXC card has 128 input ports and 128 output ports capable of VC4-16. A VC4 on any of the input ports can be mapped to a VC4 output port, thus providing full VC4 time slot assignments (TSA).

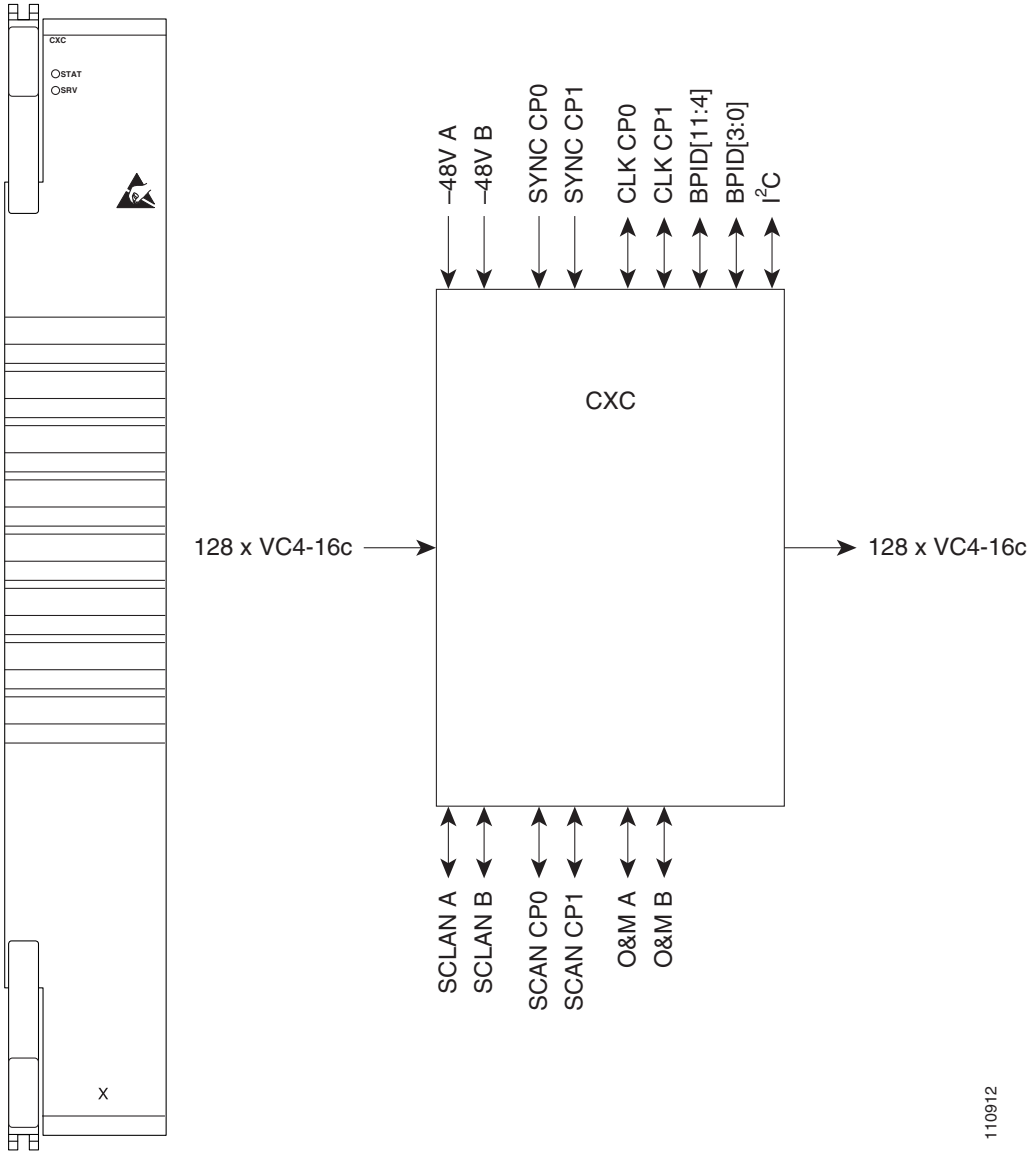
2.1.2.2 CXC Slots and Connectors

Install a CXC card in Slot 6 and a second CXC card in Slot 8 for redundancy. (Slots 7 and 9 are also occupied by the CXC faceplate.) The CXC card has no external interfaces. All CXC card interfaces are provided on the ONS 15600 SDH backplane.

2.1.2.3 CXC Faceplate and Block Diagram

Figure 2-2 shows the CXC card faceplate and a block diagram of the card.

Figure 2-2 CXC Card Faceplate and Block Diagram



2.1.2.4 CXC Card-Level Indicators

Table 2-5 describes the functions of the card-level LEDs on the CXC card faceplate.

Table 2-5 CXC Card-Level Indicators

Indicators LED	Color	Definition
STAT	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED will flash quickly during initialization and flash slowly during configuration synchronization.
SRV	Green	The service mode of the card. Green indicates the card is in use; off indicates that the card can be removed for service.

2.1.2.5 CXC Specifications

Table 2-6 shows the CXC card specifications.

Table 2-6 CXC Card Specifications

Specification Type	Description
Cross-Connect	Connection setup time: 7 microseconds Latency: 0.5 microseconds
Operating Temperature	23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
Operating Humidity	5 to 95 percent, noncondensing
Dimensions	Height: 16.50 in. (419 mm) Width: 2.40 in. (61 mm) Depth: 18.31 in. (465 mm) Card weight: 5.0 lb (2.27 kg)
Compliance	When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950

2.2 Optical Traffic Cards

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.**

2.2.1 OC48/STM16 LR/LH 16 Port 1550 Card

The OC48/STM16 LR/LH 16 Port 1550 card provides 16 long-haul STM-16 ITU-T G.957 L-16.2 compliant signals. The ports operate at the ITU-T G.707 compliant 2488.320 Mbps rate over a single-mode fiber span. The OC48/STM16 LR/LH 16 Port 1550 card has four physical connector adapters with eight fibers per connector adapter. The card supports VC4 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, or VC4-16c signal levels.

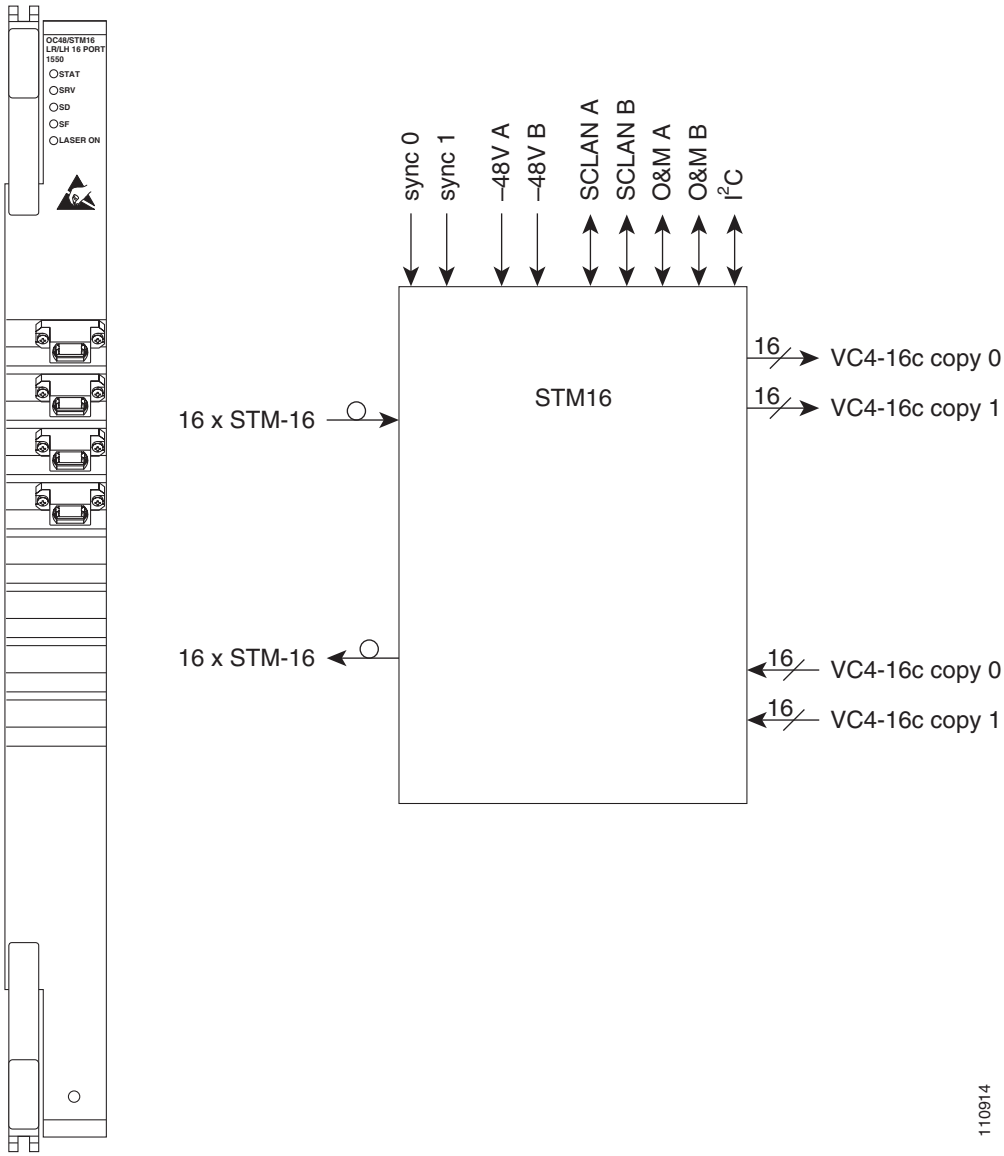
2.2.1.1 OC48/STM16 LR/LH 16 Port 1550 Slots and Connectors

You can install OC48/STM16 LR/LH 16 Port 1550 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI (Optical Gateway Interface) type connector adapters on the faceplate (angled downward), each carrying eight fiber strands (four transmit and four receive).

2.2.1.2 OC48/STM16 LR/LH 16 Port 1550 Faceplate and Block Diagram

Figure 2-3 shows the OC48/STM16 LR/LH 16 Port 1550 faceplate and a block diagram of the card.

Figure 2-3 OC48/STM16 LR/LH 16 Port 1550 Faceplate and Block Diagram



2.2.1.3 OC48/STM16 LR/LH 16 Port 1550 Card-Level Indicators

Table 2-7 describes the functions of the card-level LEDs on the OC48/STM16 LR/LH 16 Port 1550 card.

Table 2-7 OC48/STM16 LR/LH 16 Port 1550 Card-Level Indicators

Indicators	Color	Description
STAT LED	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED will flash quickly during initialization and flash slowly during configuration synchronization.
SRV LED	Green	The service mode of the card; green indicates that the card is in use and off indicates that the card can be removed for service.
LASER ON	Green	The green LASER ON LED indicates that at least one of the card's lasers is active.

2.2.1.4 OC48/STM16 LR/LH 16 Port 1550 Network-Level Indicators

Table 2-8 describes the functions of the network-level LEDs on the OC48/STM16 LR/LH 16 Port 1550 card.

Table 2-8 OC48/STM16 LR/LH 16 Port 1550 Network-Level Indicators

Indicators	Color	Description
SD LED	Blue	The blue SD LED indicates a signal degrade or condition such as a low level signal on at least one of the card's ports.
SF LED	Red	The red SF LED indicates a signal failure or condition such as loss of signal (LOS) or loss of frame alignment, or turns on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off.

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.**

2.2.1.5 OC48/STM16 LR/LH 16 Port 1550 Specifications

Table 2-9 shows the OC48/STM16 LR/LH 16 Port 1550 card specifications.

Table 2-9 OC48/STM16 LR/LH 16 Port 1550 Card Specifications

Specification Type	Description
Line	Bit rate: 2.49 Gbps Code: Scrambled NRZ Fiber: 1550-nm single mode Loopback mode: Facility Connectors: OGI Compliance: Telcordia GR-253-CORE, ITU-T G.707, ITU-T G.957
Transmitter	Max. Transmitter output power: +3 dBm Min. Transmitter output power: –2 dBm Center wavelength: 1500 nm to 1580 nm Nominal wavelength: 1550 nm Transmitter: Distributed feedback (DFB) laser **Note** The CTC Maintenance > Transceiver tab shows the optical power transmitted (OPT) levels. CTC might show OPT levels at 1 dBm more or less than the actual card OPT level.
Receiver	Max. receiver level: –9 dBm Min. receiver level: –28 dBm Receiver: InGaAs APD photodetector Link Loss Budget: 26 dB minimum, with 1 dBm dispersion penalty
Loopback Mode	Facility (Line) **Note** You must use a 19 to 24 dBm (15 to 20 dBm is recommended) fiber attenuator when connecting a fiber loopback to an OC48/STM16 LR/LH 16 Port 1550 card. Never connect a direct fiber loopback.
Operating Temperature	23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
Operating Humidity	5 to 95 percent, noncondensing
Dimensions	Height: 16.50 in. (419 mm) Width: 1.07 in. (27 mm) Depth: 18.31 in. (465 mm) Card weight: 5.0 lb (2.27 kg)
Compliance	Telcordia GR-253, ITU-T G.707, ITU-T G.957 When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products

2.2.1.6 OC48/STM16 LR/LH 16 Port 1550 Card OGI Connector Pinout

Table 2-10 shows the OC48/STM16 LR/LH 16 Port 1550 card OGI connector pinouts.

Table 2-10 OC48/STM16 LR/LH 16 Port 1550 Card OGI Connector Pinout

Connector	OGI Pin and Card Port							
1	1	2	3	4	5	6	7	8
	Transmit 4	Receive 4	Transmit 3	Receive 3	Transmit 2	Receive 2	Transmit 1	Receive 1
2	1	2	3	4	5	6	7	8
	Transmit 8	Receive 8	Transmit 7	Receive 7	Transmit 6	Receive 6	Transmit 5	Receive 5
3	1	2	3	4	5	6	7	8
	Transmit 12	Receive 12	Transmit 11	Receive 11	Transmit 10	Receive 10	Transmit 9	Receive 9
4	1	2	3	4	5	6	7	8
	Transmit 16	Receive 16	Transmit 15	Receive 15	Transmit 14	Receive 14	Transmit 13	Receive 13

2.2.2 OC48/STM16 SR/SH 16 Port 1310 Card

The OC48/STM16 SR/SH 16 Port 1310 card provides 16 short-haul STM-16 ITU-T G.957 I-16 compliant signals. The ports operate at the ITU-T G.707 compliant 2488.320-Mbps rate over a single-mode fiber span. The OC48/STM16 SR/SH 16 Port 1310 card has four physical connector adapters with eight fibers per connector adapter. The card supports VC4 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, or VC4-16c signal levels.

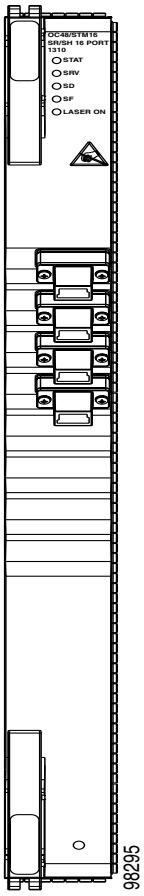
2.2.2.1 OC48/STM16 SR/SH 16 Port 1310 Slots and Connectors

You can install OC48/STM16 SR/SH 16 Port 1310 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI type connector adapters on the faceplate (angled downward), each carrying eight fiber strands (four transmit and four receive).

2.2.2.2 OC48/STM16 SR/SH 16 Port 1310 Faceplate and Block Diagram

Figure 2-4 shows the OC48/STM16 SR/SH 16 Port 1310 faceplate.

Figure 2-4 OC48/STM16 SR/SH 16 Port 1310 Faceplate



2.2.2.3 OC48/STM16 SR/SH 16 Port 1310 Card-Level Indicators

Table 2-11 describes the functions of the card-level LEDs on the OC48/STM16 SR/SH 16 Port 1310 card.

Table 2-11 OC48/STM16 SR/SH 16 Port 1310 Card-Level Indicators

Indicators	Color	Description
STAT LED	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED will flash quickly during initialization and flash slowly during configuration synchronization.
SRV LED	Green	The service mode of the card. Green indicates the card is in use; off indicates that the card can be removed for service.
LASER ON	Green	The green LASER ON LED indicates that at least one of the card's lasers is active.

2.2.2.4 OC48/STM16 SR/SH 16 Port 1310 Network-Level Indicators

Table 2-12 describes the functions of the network-level LEDs on the OC48/STM16 SR/SH 16 Port 1310 card.

Table 2-12 OC48/STM16 SR/SH 16 Port 1310 Network-Level Indicators

Indicators	Color	Description
SD LED	Blue	The blue SD LED indicates a signal degrade or condition such as a low level signal on at least one of the card's ports.
SF LED	Red	The red SF LED indicates a signal failure or condition such as LOS, LOF, or high bit error rate (BER) on at least one of the card's ports. The red SF LED also turns on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off.

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.**

2.2.2.5 OC48/STM16 SR/SH 16 Port 1310 Specifications

Table 2-13 shows the OC48/STM16 SR/SH 16 Port 1310 card specifications.

Table 2-13 OC48/STM16 SR/SH 16 Port 1310 Card Specifications

Specification Type	Description
Line	Bit rate: 2.49 Gbps Code: Scrambled NRZ Fiber: 1310-nm single mode Loopback mode: Facility Connectors: OGI Compliance: Telcordia GR-253, ITU-T G.707, ITU-T G.957
Transmitter	Max. Transmitter output power: –3 dBm Min. Transmitter output power: –10 dBm Center wavelength: 1266 nm to 1360 nm Nominal wavelength: 1310 nm Transmitter: Fabry Perot laser **Note** The CTC Maintenance > Transceiver tab shows the OPT levels. CTC might show OPT levels at 1 dBm more or less than the actual card OPT level.

Table 2-13 OC48/STM16 SR/SH 16 Port 1310 Card Specifications (continued)

Specification Type	Description
Receiver	Max. receiver level: –3 dBm Min. receiver level: –18 dBm Receiver: PIN diode Link Loss Budget: 8 dBm min., with 1 dBm dispersion penalty
Loopback Mode	Facility (Line) **Note** You must use a 3-dBm fiber attenuator when connecting a fiber loopback to an OC48/STM16 SR/SH 16 port 1310 card. Never connect a direct fiber loopback.
Operating Temperature	23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
Operating Humidity	5 to 95 percent, noncondensing
Dimensions	Height: 16.50 in. (419 mm) Width: 1.07 in. (27 mm) Depth: 18.31 in. (465 mm) Card weight: 5.0 lb (2.27 kg)
Compliance	Telcordia GR-253, ITU-T G.707, ITU-T G.957 When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products

2.2.2.6 OC48/STM16 SR/SH 16 Port 1310 Card OGI Connector Pinout

Table 2-14 shows the OC48/STM16 SR/SH 16 Port 1310 card OGI connector pinouts.

Table 2-14 OC48/STM16 SR/SH 16 Port 1310 Card OGI Connector Pinout

Connector	OGI Pin and Card Port							
1	1	2	3	4	5	6	7	8
	Transmit 4	Receive 4	Transmit 3	Receive 3	Transmit 2	Receive 2	Transmit 1	Receive 1
2	1	2	3	4	5	6	7	8
	Transmit 8	Receive 8	Transmit 7	Receive 7	Transmit 6	Receive 6	Transmit 5	Receive 5
3	1	2	3	4	5	6	7	8
	Transmit 12	Receive 12	Transmit 11	Receive 11	Transmit 10	Receive 10	Transmit 9	Receive 9
4	1	2	3	4	5	6	7	8
	Transmit 16	Receive 16	Transmit 15	Receive 15	Transmit 14	Receive 14	Transmit 13	Receive 13

2.2.3 OC192/STM64 LR/LH 4 Port 1550 Card

The OC192/STM64 LR/LH 4 port 1550 card provides four long-haul STM-64 ITU-T G.691 L-64.2c (shifted by 4-5 dB) compliant signals. The ports operate at the ITU-T G.707 compliant 9953.28-Mbps rate over a single-mode fiber span. The OC192/STM64 LR/LH 4 port 1550 card has four physical connector adapters with two fibers per connector adapter. The card supports VC4 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c signal levels.

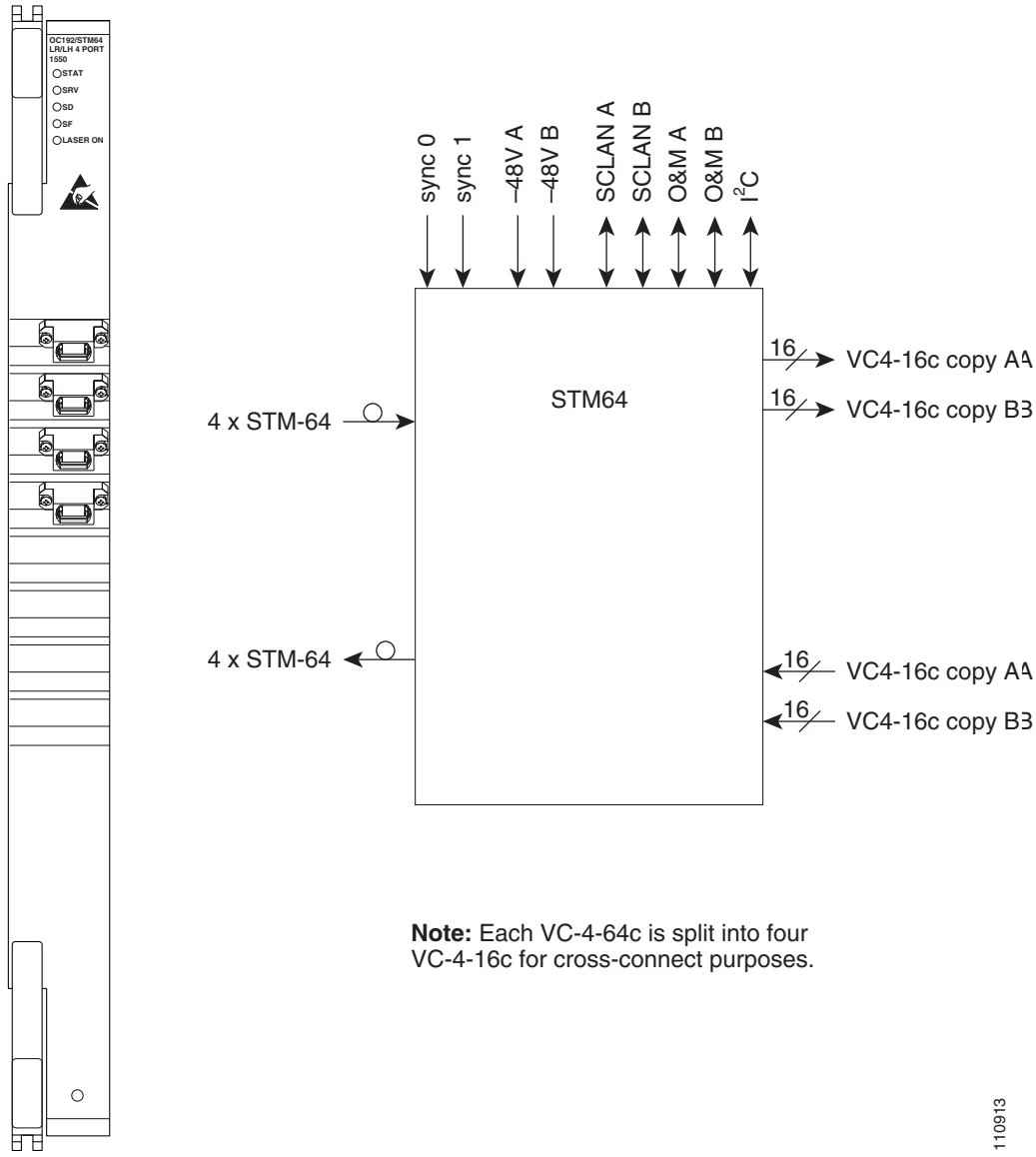
2.2.3.1 OC192/STM64 LR/LH 4 Port 1550 Slots and Connectors

You can install OC192/STM64 LR/LH 4 port 1550 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI type connector adapters on the faceplate (angled downward), carrying two fiber strands (1 transmit and 1 receive). Only one transmit and receive pair is used per connector adapter. On a breakout cable, use Port 3, Fiber 4 (transmit), and Fiber 3 (receive).

2.2.3.2 OC192/STM64 LR/LH 4 Port 1550 Faceplate and Block Diagram

Figure 2-5 shows the OC192/STM64 LR/LH 4 Port 1550 faceplate and a block diagram of the card.

Figure 2-5 OC192/STM64 LR/LH 4 Port 1550 Faceplate and Block Diagram



2.2.3.3 OC192/STM64 LR/LH 4 Port 1550 Card-Level Indicators

Table 2-15 describes the functions of the card-level LEDs on the OC192/STM64 LR/LH 4 Port 1550 card.

Table 2-15 OC192/STM64 LR/LH 4 Port 1550 Card-Level Indicators

Indicators	Color	Description
STAT LED	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the unit if the STAT LED persists. During diagnostics, the LED will flash quickly during initialization and flash slowly during configuration synchronization.
SRV LED	Green	The service mode of the card. Green indicates the card is in use; off indicates that the card can be removed for service.
LASER ON	Green	The green LASER ON LED indicates that at least one of the card's lasers is active.

2.2.3.4 OC192/STM64 LR/LH 4 Port 1550 Network-Level Indicators

Table 2-16 describes the functions of the network-level LEDs on the OC192/STM64 LR/LH 4 Port 1550 card.

Table 2-16 OC192/STM64 LR/LH 4 Port 1550 Network-Level Indicators

Indicators	Color	Description
SD LED	Blue	The blue SD LED indicates a signal degrade or condition such as a low signal level on at least one of the card's ports.
SF LED	Red	The red SF LED indicates a signal failure or condition such as LOS, LOF, or high BERs on at least one of the card's ports. The red SF LED is also on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off.

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.**

2.2.3.5 OC192/STM64 LR/LH 4 Port 1550 Specifications

Table 2-17 shows the OC192/STM64 LR/LH 4 Port 1550 card specifications.

Table 2-17 OC192/STM64 LR/LH 4 Port 1550 Card Specifications

Specification Type	Description
Line	Bit rate: 9.96 Gbps Code: Scrambled NRZ Fiber: 1550-nm single mode
Transmitter	Max. transmitter output power: +7 dBm Min. transmitter output power: +4 dBm Center wavelength: 1530 nm to 1565 nm Nominal wavelength: 1550 nm Transmitter: LN (Lithium Niobate) external modulator transmitter
Receiver	Max. receiver level: –9 dBm Min. receiver level: –22 dBm Receiver: APD/TIA (Avalanche Photo Diode/Trans Impedance Amplifier) Link loss budget: 24 dB min., with no dispersion or 22 dB optical path loss at BER = 1- exp (–12) including dispersion
Loopback Mode	Payload **Note** You must use a 19 to 24 dB (15 to 20 is recommended) fiber attenuator when connecting a fiber loopback to an OC192/STM64 LR/LH 4 Port 1550 card. Never connect a direct fiber loopback.
Connectors	OGI
Operating Temperature	23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
Operating Humidity	5 to 95 percent, noncondensing
Dimensions	Height: 16.50 in. (419 mm) Width: 1.07 in. (27 mm) Depth: 18.31 in. (465 mm) Card weight: 12.0 lb (5.44 kg)
Compliance	Telcordia GR-253, ITU-T G.707, ITU-T G.691 When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products

2.2.3.6 OC192/STM64 LR/LH 4 Port 1550 Card OGI Connector Pinout

Table 2-18 shows the OC192/STM64 LR/LH 4 Port 1550 card OGI connector pinouts.

Table 2-18 OC192/STM64 LR/LH 4 Port 1550 Card OGI Connector Pinout

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

2.2.4 OC192/STM64 SR/SH 4 Port 1310 Card

The OC192/STM64 SR/SH 4 Port 1310 card provides four short-haul STM-64 ITU-T G.691 I-64.1r compliant signals. The ports operate at ITU-T G.707 compliant 9953.28-Mbps rate over a single-mode fiber span. The OC192/STM64 SR/SH 4 port 1310 card has four physical connector adapters with two fibers per connector adapter. The card supports STS-1 payloads and concatenated payloads at VC4, VC4-4c, VC4-8c, VC4-16c, or VC4-64c signal levels.

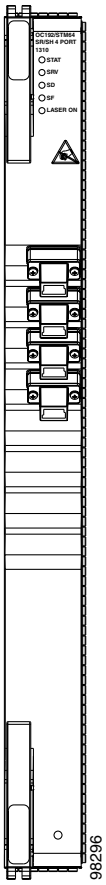
2.2.4.1 OC192/STM64 SR/SH 4 Port 1310 Slots and Connectors

You can install OC192/STM64 SR/SH 4 Port 1310 cards in Slots 1 through 4 and 11 through 14. The card provides four bidirectional OGI type connector adapters on the faceplate (angled downward), carrying two fiber strands (one transmit and one receive). Only one transmit and receive pair is used per connector adapter. On a breakout cable, use Port 3, Fiber 4 (transmit) and Fiber 3 (receive).

2.2.4.2 OC192/STM64 SR/SH 4 Port 1310 Faceplate and Block Diagram

Figure 2-6 shows the OC192/STM64 SR/SH 4 Port 1310 faceplate.

Figure 2-6 OC192/STM64 SR/SH 4 Port 1310 Faceplate



2.2.4.3 OC192/STM64 SR/SH 4 Port 1310 Card-Level Indicators

Table 2-19 describes the functions of the card-level LEDs on the OC192/STM64 SR/SH 4 Port 1310 card.

Table 2-19 OC192/STM64 SR/SH 4 Port 1310 Card-Level Indicators

Indicators	Color	Description
STAT LED	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the unit if the STAT LED persists. During diagnostics, the LED will flash quickly during initialization and flash slowly during configuration synchronization.
SRV LED	Green	The service mode of the card. Green indicates the card is in use; off indicates that the card can be removed for service.
LASER ON	Green	The green LASER ON LED indicates that at least one of the card's lasers is active.

2.2.4.4 OC192/STM64 SR/SH 4 Port 1310 Network-Level Indicators

Table 2-20 describes the functions of the network-level LEDs on the OC192/STM64 SR/SH 4 Port 1310 card.

Table 2-20 OC192/STM64 SR/SH 4 port 1310 Network-Level Indicators

Indicators	Color	Description
SD LED	Blue	The blue SD LED indicates a signal degrade or condition such as a low signal level on at least one of the card's ports.
SF LED	Red	The red SF LED indicates a signal failure or condition such as LOS, LOF, or high BER on at least one of the card's ports. The red SF LED also turns on when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the LED turns off.

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.**

2.2.4.5 OC192/STM64 SR/SH 4 Port 1310 Specifications

Table 2-21 shows the OC192/STM64 SR/SH 4 Port 1310 card specifications.

Table 2-21 OC192/STM64 SR/SH 4 Port 1310 Card Specifications

Specification Type	Description
Line	Bit rate: 9.96 Gbps Code: Scrambled nonreturn to zero (NRZ) Fiber: 1310-nm single mode
Transmitter	Max. transmitter output power: –1 dBm Min. transmitter output power: –6 dBm Center wavelength: 1290 nm to 1330 nm Nominal wavelength: 1310 nm
Receiver	Max. receiver level: –1 dBm Min. receiver level: –11 dBm Link loss budget: 5 dB min., with no dispersion or 4 dB optical path loss at BER = 1– exp (–12) including dispersion
Loopback Mode	Payload **Note** You must use a 3-dBm fiber attenuator when connecting a fiber loopback to an OC192/STM64 SR/SH 4 Port 1310 card. Never connect a direct fiber loopback.
Connectors	OGI

Table 2-21 OC192/STM64 SR/SH 4 Port 1310 Card Specifications (continued)

Specification Type	Description
Operating Temperature	23 to 122 degrees Fahrenheit (–5 to +50 degrees Celsius)
Operating Humidity	5 to 95 percent, noncondensing
Dimensions	Height: 16.50 in. (419 mm) Width: 1.07 in. (27 mm) Depth: 18.31 in. (465 mm) Card weight: 12.0 lb (5.44 kg)
Compliance	Telcordia GR-253, ITU-T G.707, ITU-T G.691 When installed in a system, ONS 15600 SDH cards comply with these safety standards: UL 60950, CSA C22.2 No. 950, EN 60950, IEC 60950 Eye safety compliance: Class 1 (21 CFR 1040.10 and 1040.11) and Class 1 (IEC 60825) laser products

2.2.4.6 OC192/STM64 SR/SH 4 Port 1310 Card OGI Connector Pinout

Table 2-22 shows the OC192/STM64 SR/SH 4 Port 1310 card OGI connector pinouts.

Table 2-22 OC192/STM64 SR/SH 4 Port 1310 Card OGI Connector Pinout

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

2.3 Filler Card

Warning **Blank faceplates (filler 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, power modules, and faceplates are in place.**

The filler card is used to fill unused optical (STM-N) traffic card slots in the ONS 15600 SDH shelf. In Software Release 1.4, the filler card has a card presence indicator (CPI) that allows the shelf to report the presence of the filler card to CTC. The filler card uses dummy backplane connectors and a standard faceplate to secure the card in the empty shelf slot.

Figure 2-7 shows the filler card body and faceplate.

Figure 2-7 ONS 15600 SDH Filler Card

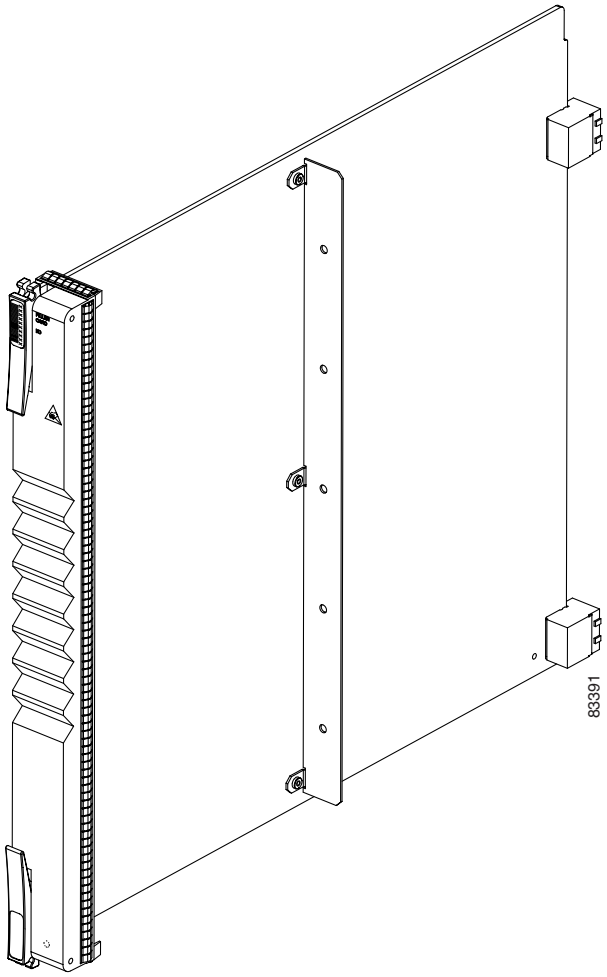


Table 2-23 shows the filler card specifications.

Table 2-23 Filler Card Specifications

Specification Type	Description
Dimensions	Height: 16.50 in. (419 mm)
	Width: 1.07 in. (27 mm)
	Depth: 18.31 in. (465 mm)
	Card weight: 2.5 lb (1.134 kg)

Card Protection

This chapter explains the Cisco ONS 15600 SDH card protection configurations.

Chapter topics include:

3.1 Optical Port Protection

When you set up protection for ONS 15600 SDH cards, you must choose between maximum protection and maximum port availability. The highest protection reduces the number of available ports; the highest port availability reduces the protection. Table 3-1 contrasts port protection with an unprotected scheme.

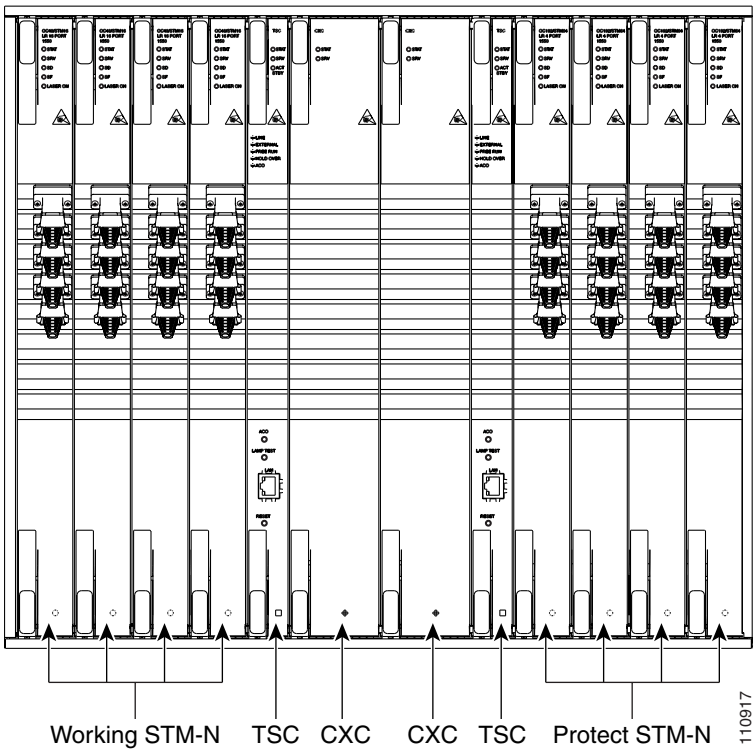
Table 3-1 Port Protection Types

Type	Ports	Description
1+1	Any optical	Pairs a working optical port with a protect optical port. Protect ports must match the line rate of the working ports. For example, Port 1 of an STM-16 card can only be protected by another STM-16 port. Ports do not need to be in adjoining slots. Example of port configuration for protection is, provision the ports/cards in Slots 1 to 4 as working and the ports/cards in Slots 11 to 14 as protect.
Unprotected	Any	Unprotected ports can cause traffic loss if a port fails or incurs a signal error. However, because no ports are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15600 SDH. **Note** If you want to protect traffic you should implement either a subnetwork connection protection (SNCP) or multiplex section-shared protection ring (MS-SPRing) protection scheme.

Note Because there are no electrical cards in the ONS 15600 SDH, 1:1 and 1:N protection is not provided.

Figure 3-1 shows an example of the ONS 15600 SDH in a maximum protection, 1+1 protected configuration.

Figure 3-1 ONS 15600 SDH in a 1+1 Protected Configuration



With 1+1 protection, any number of ports can be assigned to protect corresponding working ports. A working port must be paired with a protect port of the same type, for example, an STM-16 port must be paired with another STM-16 port.

On a multiport card, you can assign one port as a protection port (protecting a corresponding port) and the remaining ports can be working ports. Conversely, you can assign one port as a working port and assign the remaining ports as protection ports.

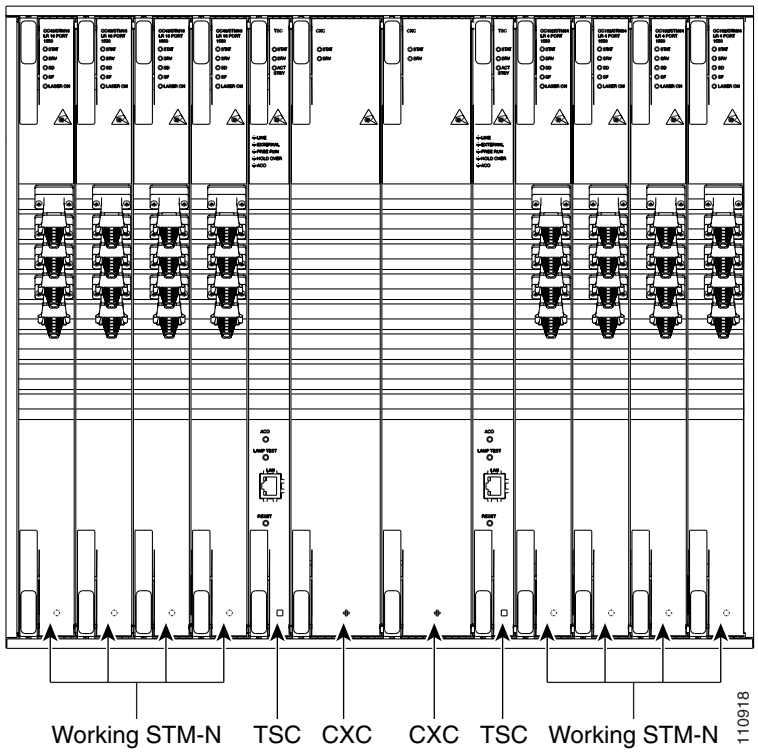
1+1 span protection can be either revertive or nonrevertive. With nonrevertive 1+1 protection, when a span failure occurs and the signal switches from the working port to the protect port, the signal stays switched to the protect port until it is manually switched back. Revertive 1+1 protection automatically switches the signal back to the working port when the failure condition on the working port is cleared.

For more information about protection schemes and how to create and modify them with Cisco Transport Controller (CTC), refer to the *Cisco ONS 15600 Procedure Guide*.

3.2 Unprotected Ports

Unprotected ports are not included in a protection scheme; therefore, a port failure or a signal error can result in data loss if no path level protection (SNCP) exists. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15600 SDH bandwidth. Figure 3-2 shows the ONS 15600 SDH in an unprotected configuration. All ports are in a working state.

Figure 3-2 ONS 15600 SDH in an Unprotected Configuration



3.3 External Switching Commands

The external switching commands on the ONS 15600 SDH are Manual, Force, Lockout, and Lock on.

A Manual switch will switch traffic if the path has an error rate less than the signal degrade. A Force switch will switch traffic even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch has a higher priority than a Manual switch.

Lockouts can only be applied to protect cards and prevent traffic from switching to the protect port under any circumstance. Lockouts have the highest priority. Another way to inhibit protection switching in a 1+1 configuration is to apply a lock on to the working port. A working port with a lock on applied cannot switch traffic to the protect port in the protection group (pair).

Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the Cisco ONS 15600 SDH software interface that is stored on the Timing and Shelf Controller (TSC) card and downloaded to your workstation each time you log into the ONS 15600 SDH. For CTC set up and login information, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

4.1 CTC Software Delivery Methods

Use CTC to provision and administer the ONS 15600 SDH. CTC is a Java application that is installed in two locations:

- ONS 15600 SDH TSC card
- PCs and UNIX workstations that connect to the ONS 15600 SDH

CTC is stored on the TSC card and downloaded to your workstation each time you log into an ONS 15600 SDH.

4.1.1 CTC Software Installed on the TSC Card

CTC software is preloaded on the ONS 15600 SDH TSC cards; therefore, you do not need to install software on the TSC. To upgrade to a newer CTC software version, use the *Cisco ONS 15600 SDH Software Upgrade Guide*.

You can view the software versions that are installed on one ONS 15600 SDH by clicking the Maintenance > Software tabs in node view. Click the tabs in network view to display the software versions installed on all the network nodes.

4.1.2 CTC Software Installed on the PC or UNIX Workstation

When you connect to the ONS 15600 SDH, the TSC card automatically downloads the CTC software to your computer, where it is automatically installed if you have the correct Java Runtime Environment (JRE). The automatic download/installation process ensures that your computer is running the same CTC software version as the TSC you are accessing. The CTC software files are stored in the temporary directory designated by your computer's operating system. You can use the Delete CTC Cache button to remove files stored in the temporary directory. If the files are deleted, they are downloaded the next time you connect to an ONS 15600 SDH. Downloading the Java archive files, called JAR files, for CTC takes several minutes depending on the bandwidth of the connection between your workstation and the ONS 15600 SDH. For example, JAR files downloaded from a modem or an Regenerator Section Data Communication Channels (RSDCC) network link will require more time than JAR files downloaded over a LAN connection.

4.2 CTC Installation Overview

To connect to an ONS 15600 SDH using CTC, enter the ONS 15600 SDH IP address in the URL field of a web browser, such as Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15600 SDH, the following events occur automatically:

Note Each ONS 15600 SDH has a unique IP address that you use to access it. The initial IP address, 192.168.1.2, is the default address for ONS 15600 SDH access and configuration.

1. A CTC launcher applet is downloaded from the TSC to your computer's temporary directory. (If these files are deleted, they are automatically reinstalled the next time you connect to the ONS 15600 SDH.)
2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15600 SDH TSC.
3. If the computer does not have CTC installed, or if the installed release is older than the TSC version, the launcher downloads the CTC program files from the TSC.
4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. If you log into an ONS 15600 SDH that is connected to ONS 15600 SDH nodes with older versions of CTC, or to Cisco ONS 15454 SDH nodes, CTC "element" files are downloaded automatically to enable you to interact with those nodes. You cannot interact with nodes on the network that have a newer software version than the node that you are logged into (the nodes will appear gray in network view). Therefore, always log into nodes with the latest software release.

Each ONS 15600 SDH can handle up to 16 simultaneous CTC sessions. CTC performance might vary depending upon the volume of activity in each session.

Note You can also use TL1 commands to communicate with the ONS 15600 SDH through VT100 terminals and VT100 emulation software, or you can Telnet to an ONS 15600 SDH using TL1 port 3083. See the *Cisco ONS 15600 TL1 Command Guide* for a comprehensive list of TL1 commands.

4.3 PC and UNIX Workstation Requirements

To use CTC with an ONS 15600 SDH, your computer must have a web browser with the correct JRE installed and a modified java.policy file. The correct JRE, Java plugin, and modified java.policy file for the CTC software release are included on the Cisco ONS 15600 SDH software CD.

The requirements depend on the network size. Network size is determined by the following criteria:

- Number of nodes—A small network has 50 nodes or less, a medium network has between 50 and 200 nodes, and a large network has more than 200 nodes.
- Number of circuits—A small network has 6000 circuits or less, a medium network has between 6000 and 12000 circuits, and a large network has over 12000 circuits.

Table 4-1 provides the requirements for PCs and UNIX workstations.

Table 4-1 Computer Requirements for CTC

Area	Requirements	Notes
Processor	• Small networks—Pentium II 300 MHz, UltraSPARC, or equivalent • Medium and large networks—Pentium II 500 MHz P3 processor, UltraSPARC, or equivalent	300 Mhz is the recommended processor speed. You can use computers with a lower processor speed; however, you might experience longer response times and slower performance.
RAM	• Small networks—256 MB • Medium networks—512 MB • Large networks—512 MB or more	—
Hard drive	• Small networks—2 GB • Medium and large networks—10 GB	CTC application files are downloaded from the TSC to your computer's Temp directory. These files occupy 3 to 5 MB of hard drive space.
Operating System	• Small networks—PC: Windows 95, Windows 98, Windows NT 4.0, Windows 2000, or Windows XP; Workstation: Solaris 2.6 or 2.7 • Medium and large networks—PC: Windows 98, Windows NT 4.0, Windows 2000, or Windows XP; Workstation: Ultra 10 Sun running Sun OS 6, 7, or 8	—
Web browser	• PC: Netscape Navigator 4.73 or higher, or Internet Explorer 5.0 (Service Pack 2) or higher • Workstation: Netscape Navigator 4.73 or higher	Netscape Communicator 4.73 (Windows) and 4.76 (UNIX) are installed by the CTC Installation Wizard included on the Cisco ONS 15600 SDH software and documentation CDs.

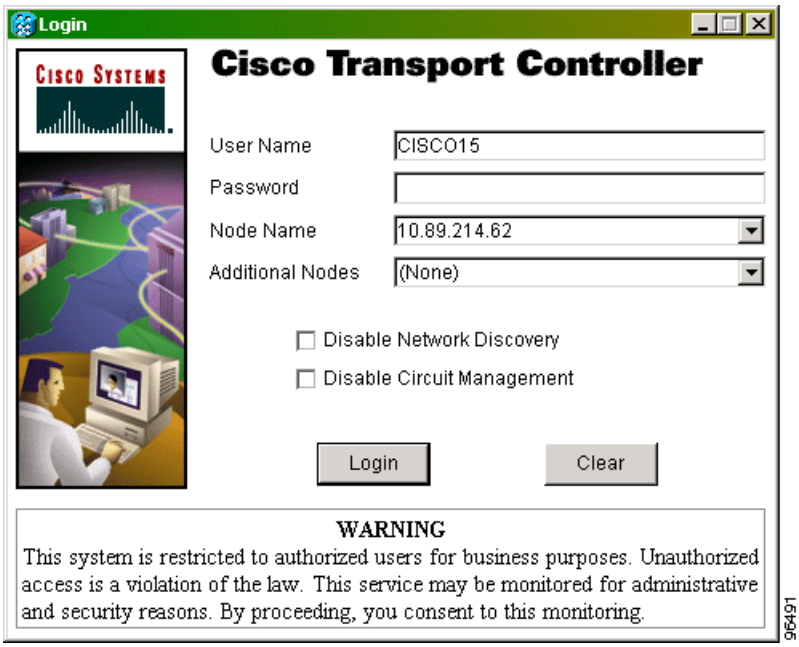
Table 4-1 Computer Requirements for CTC (continued)

Area	Requirements	Notes
Java Runtime Environment	JRE 1.3.1_02	JRE 1.3.1_02 is installed by the CTC Installation Wizard included on the Cisco ONS 15600 SDH software and documentation CDs.
Java.policy file	A java.policy file modified for CTC	The java.policy file is modified by the CTC Installation Wizard included on the Cisco ONS 15600 SDH software and documentation CDs.
Cable	Use a crossover or straight-through LAN (CAT-5) cable to connect: • The ONS 15600 SDH to a hub using the backplane RJ-45 ports, or to connect through a LAN. • The ONS 15600 SDH to a PC using the backplane RJ-45 ports. • The active TSC RJ-45 port to a laptop or hub.	A direct PC-to-ONS 15600 SDH connection means your computer is physically connected to the ONS 15600 SDH. This is most commonly done by connecting a LAN (CAT-5) straight-through cable from your PC to the RJ-45 port on the TSC. However, direct connections include connections to switches or hubs where the ONS 15600 SDH is physically connected. **Note** Use only the active TSC connector for connectivity. If you connect to the standby or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the CAP card so that connection to the ONS 15600 SDH will not be lost during a TSC switch.

4.4 CTC Login

After you have installed CTC, you can log in to a node using your browser. To log in, you must type the node IP address in the URL window. The CTC Login window appears (Figure 4-1).

Figure 4-1 Login Window



The CTC Login window provides the following options to accelerate the login process.

- The Disable Network Discovery option omits the discovery of nodes with DCC connectivity. To access all nodes with DCC connectivity, make sure that Disable Network Discovery is not checked.
- The Disable Circuit Management option omits the discovery of circuits. To view circuits immediately after logging in, make sure that Disable Circuit Management is not checked. However, if disabled, after you have logged in you can click the Circuits tab and CTC will give you the option to enable circuit management.

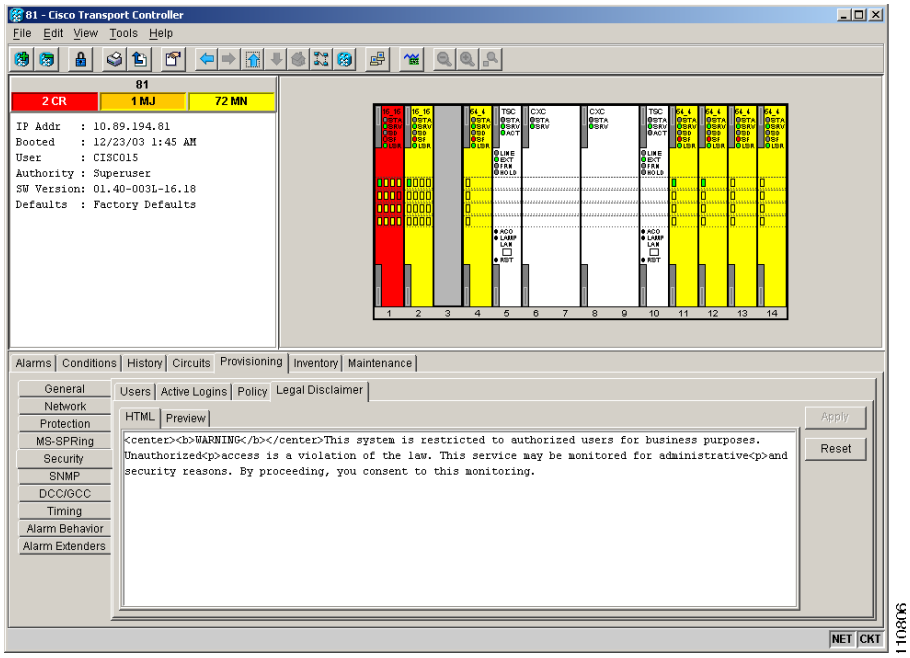
These options are useful if you want to log in to a node to perform a single task, such as placing a card in or out of service, and do not want to wait while CTC discovers DCC connections and circuits.

4.4.1 Legal Disclaimer

The CTC Login window displays a warning message (Figure 4-1).

The ONS 15600 SDH allows a user with Superuser privileges to modify the default login warning message and save it to a node using the Provisioning > Security > Legal Disclaimer > HTML tab (Figure 4-2). The login warning message field allows up to 250 characters of text (1600 characters total, including HTML markup).

Figure 4-2 Legal Disclaimer Tab



4.4.2 Login Node Group

Login node groups display nodes that have only an IP connection. After you are logged into CTC, you can create a login node group from the Edit > Preferences menu. Login groups appear in the Additional Nodes list (Figure 4-1 on page 4-5) on the Login window.

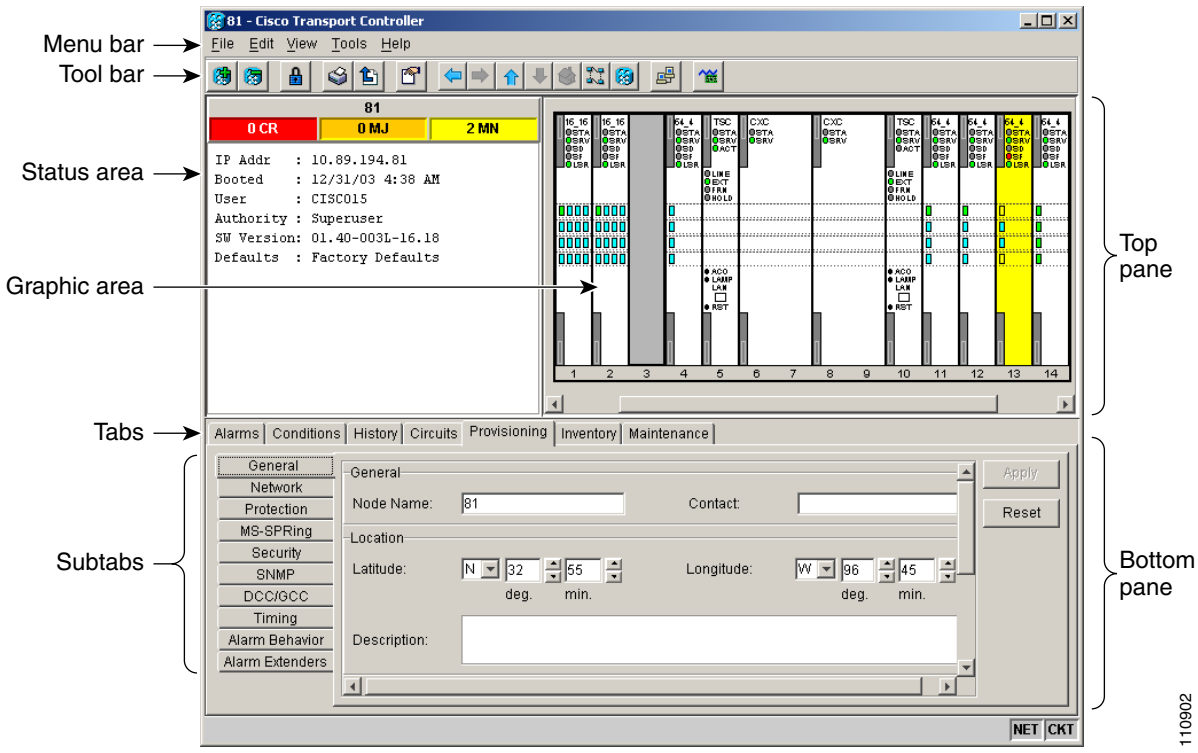
For example, if you logged into Node 1, you would see Node 2 and Node 3 because they have DCC connectivity to Node 1. You would not see Nodes 4, 5, and 6 because DCC connections do not exist. To view all six nodes at once, you create a login node group with the IP addresses of Nodes 1, 4, 5, and 6. Those nodes, and all nodes optically connected to them, appear when you select the login group from the Additional Nodes list on the Login window the next time you log in.

4.5 CTC Window

The CTC window appears after you log into an ONS 15600 SDH. The CTC node view is the first view that appears after you log into an ONS 15600 SDH (Figure 4-3). The login node is the first node displayed, and it is the home view for the session (accessed by choosing View > Go To Home View).

The CTC window includes a menu bar, toolbar, and a top and bottom pane. The top pane displays status information about the selected objects and a graphic of the current view. The bottom pane displays tabs and subtabs, which you use to view ONS 15600 SDH information and perform ONS 15600 SDH provisioning and maintenance. From the default node view window you can display the other two ONS 15600 SDH views: network and card.

Figure 4-3 CTC Window Elements in the Node View (Default Login View)



4.5.1 Node View

Node view allows you to view and manage one ONS 15600 SDH node (Figure 4-3). The status area shows the node name; number of critical (CR), major (MJ), and minor (MN) alarms; IP address; session boot date and time; name of the current logged-in user; and user security level.

4.5.1.1 CTC Card Colors

The graphic area of the CTC window depicts the ONS 15600 SDH shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card, slot, and port. Table 4-2 describes the node view card colors.

Table 4-2 Node View Card Colors

Card Color	Status
Gray	Slot is not provisioned; no card is installed.
Violet	Slot is provisioned; no card is installed (the card immediately changes to yellow because the IMPROPRMVL alarm is raised).
White	Slot is provisioned; a functioning card is installed or booting.
Yellow	Slot is provisioned; a minor alarm condition exists.
Orange	Slot is provisioned; a major alarm condition exists.
Red	Slot is provisioned; a critical alarm exists.

The color of the port in both card and node view indicates the port status. Table 4-3 describes the port colors.

Table 4-3 Node View Card Port Colors

Port Color	State	Description
Cyan	OOS_MT	Port is out of service for maintenance. The maintenance state does not interrupt traffic flow. Alarm reporting is suppressed, but traffic is carried and loopbacks are allowed. Raised fault conditions, whether their alarms are reported or not, can be retrieved on the CTC Conditions tab or by using the TL1 RTRV-COND command. Use OOS_MT for testing or to suppress alarms temporarily. Change the state to IS when testing is complete.
Green	IS	Port is in service. The port will transmit a signal and display alarms; loopbacks are not allowed.

4.5.1.2 Node View Card Shortcuts

If you move your mouse over cards in the graphic, popups display additional information about the card including the card type; card status (active or standby); the type of alarm, such as critical, major, and minor (if any); and the alarm profile used by the card. Right-click a card to reveal a shortcut menu that you can use to open, reset, or delete a card. Right-click an empty slot to preprovision a card (that is, provision a slot before installing the card).

4.5.1.3 Node View Tabs

Table 4-4 lists the tabs and subtabs available in the node view.

Table 4-4 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	Allows you to retrieve a list of standing conditions on the node.	—
History	Provides a history of node alarms including date, type, and severity of each alarm. The Session subtab displays alarms and events for the current session. The Node subtab displays alarms and events retrieved from a fixed-size log on the node.	Session, Node
Circuits	Allows you to create, delete, edit, and reroute circuits.	Circuits, Rolls
Provisioning	Allows you to provision the ONS 15600 SDH node.	General, Network, Protection, MS-SPRing[1], Security, SNMP[2], DCC/GCC[3], Timing, Alarm Behavior, Alarm Extenders

Table 4-4 Node View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Inventory	Provides inventory information (part number, serial number, Common Language Equipment Identification [CLEI] codes) for cards installed in the node. Allows you to delete and reset cards, and provision the user code (a 20-character ASCII string stored in nonvolatile memory so that it is not lost when the unit is moved or stored as a spare).	—
Maintenance	Allows you to perform maintenance tasks for the node.	Database, Protection, Diagnostic, MS-SPRing[1], Software, Timing, Audit, Routing Table, Test Access, Alarm Extenders, Preferred Copy

1. MS-SPRing = multiplex section-shared protection ring
2. SNMP = Simple Network Management Protocol
3. DCC/GCC = data communications channel/general communications channel

4.5.2 Network View

Network view allows you to view and manage ONS 15600 SDH nodes, ONS 15454 SDH nodes that have DCC connections to the node that you logged into, and any login node groups you have selected (Figure 4-4).

Note Nodes with DCC connections to the login node do not display if you selected Disable Network Discovery in the Login dialog box.

To access network view, choose **View > Go To Network View** or click the up arrow in the CTC toolbar.

The graphic area displays a background image with colored node icons. A Superuser can set up the logical network view feature, which enables each user to see the same network view.

The node icon colors indicate the node status (Table 4-5). 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 4-4 Network Displayed in CTC Network View

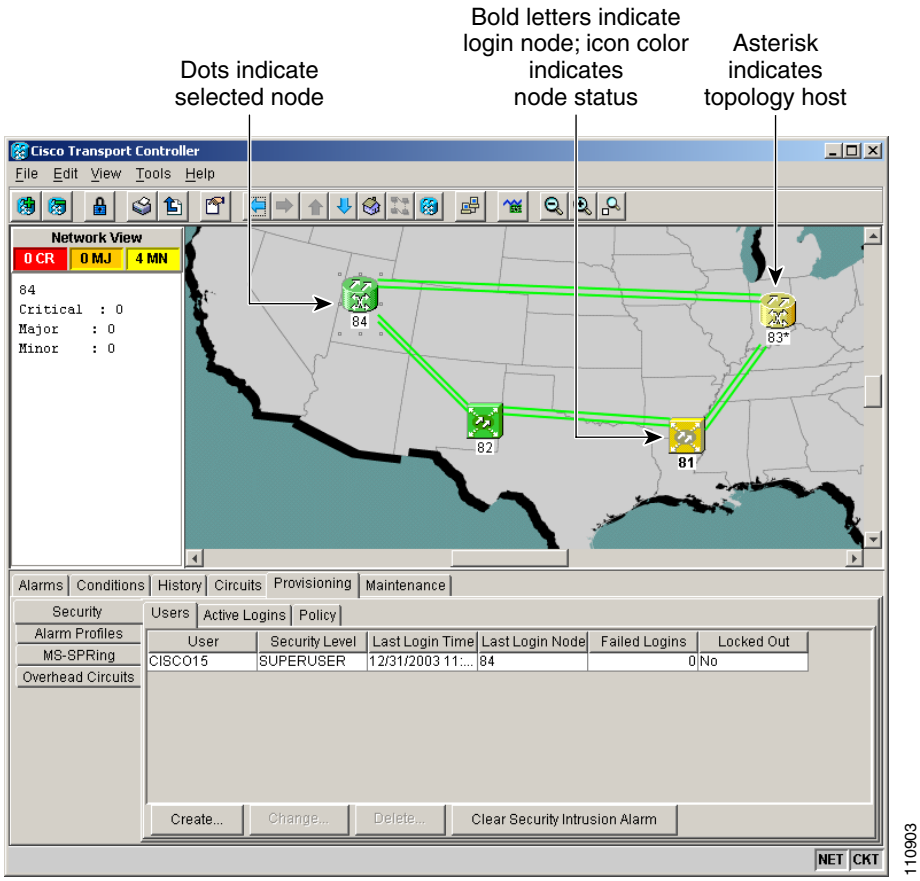


Table 4-5 lists the node status colors.

Table 4-5 Node Status

Color	Alarm Status
Green	No alarms.
Yellow	Highest-level alarm is a minor alarm.
Orange	Highest-level alarm is major alarm.
Red	Highest-level alarm is a critical alarm.
Gray with node name	Node is initializing.
Gray with IP address	Node is initializing; a problem exists with IP routing from node to CTC or your login/password is not provisioned on this node.

Table 4-6 lists the tabs and subtabs available in the network view.

Table 4-6 Network View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the network and updates them in real time.	—
Conditions	Displays a list of standing conditions on the network.	—
History	Provides a history of network alarms including date, type, and severity of each alarm.	—
Circuits	Create, delete, edit, filter, and search for network circuits.	Circuits, Rolls
Provisioning	Provision security, alarm profiles, MS-SPRing, and overhead circuits.	Security, Alarm Profiles, MS-SPRing, Overhead Circuits
Maintenance	Displays the type of equipment and the status of each node in the network; displays working and protect software versions, and allows software to be downloaded.	Software

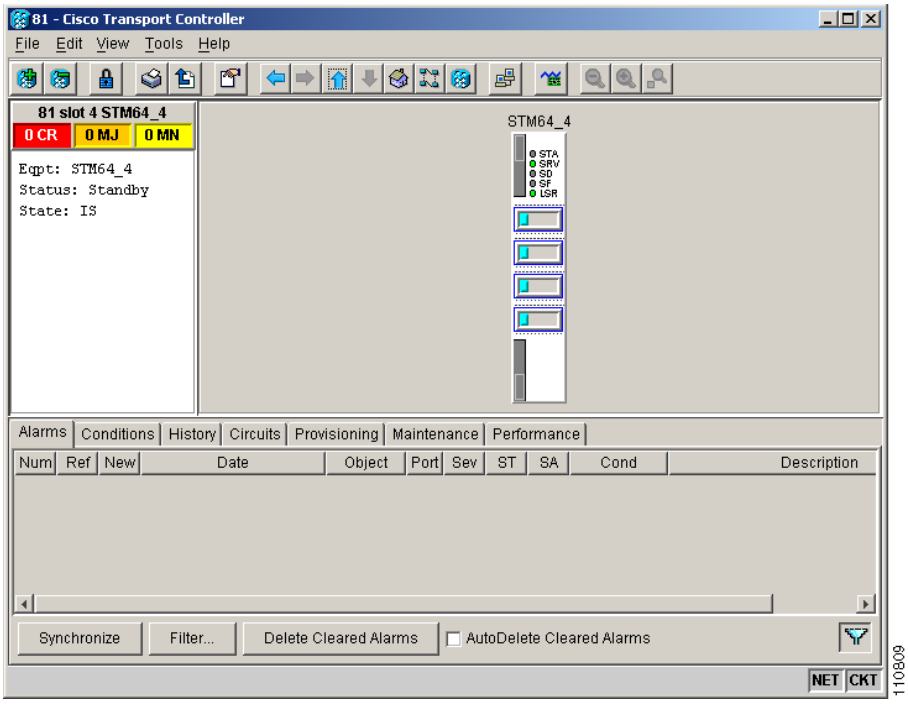
4.5.3 Card View

Card view displays information about individual ONS 15600 SDH cards. Use this window to perform card-specific maintenance and provisioning (Figure 4-5). To access card view, select a card and click the down arrow in the toolbar, or double-click the card.

A graphic of the selected card and ports is shown in the CTC graphic area. The status area displays the node name, slot, card type, number of alarms, equipment type, and the card status (active or standby). The information displayed and the actions you can perform depend on the card.

Note CTC displays a card view for all ONS 15600 SDH cards except the TSC and Core Cross Connect (CXC) cards. Provisioning for these common control cards occurs at the node view; therefore, no card view is necessary.

Figure 4-5 CTC Card View Showing an STM-64 Card



Use the card view tabs and subtabs, shown in Table 4-7, to provision and manage the ONS 15600 SDH. The subtabs, fields, and information displayed under each tab depend on the card type selected.

Table 4-7 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 (displays alarms and events for the current session); Card (displays alarms and events retrieved from a fixed-size log on the card)
Circuits	Create, delete, edit, and search circuits.	Circuits, Rolls
Provisioning	Provision an ONS 15600 SDH card.	MS[1], QoS[2] Thresholds, AU4, and Alarm Behavior
Maintenance	Perform maintenance tasks for the card.	Loopback, Transceiver, Protection, and J1 Path Trace (options depend on the card type)
Performance	Perform performance monitoring for the card.	—

1. MS = Multiplex Section
2. QoS = Quality of Service

4.6 CTC Card Reset

You can reset the ONS 15600 SDH cards by using the hard-reset or soft-reset commands in CTC, or by physically reseating a card (card pull). From the node view, select a card and right-click to open a menu with the hard-reset and soft-reset commands.

A soft reset on the TSC reboots the TSC and reloads the operating system and the application software. A CTC hard reset temporarily removes power from the TSC and clears all buffer memory. You can apply a CTC soft reset to either an active or standby TSC without affecting traffic, but you should only perform a hard reset (or a card pull) on a standby TSC. If you need to perform a CTC hard reset or card pull on an active TSC, put the TSC into standby mode first by performing a soft reset.

A soft reset on an optical card with an active port in a 1+1 protection group will result in a loss of all DCC traffic terminated or tunneled on the active port for the duration of the reset time. A soft reset of an optical card with a standby port in a 1+1 protection group will not affect DCC traffic. A CTC hard reset of an optical card causes a switch to the protect card.

4.7 TSC Card Database

Each TSC card hosts a separate database; therefore, the protect card's database is available if the database on the working TSC fails. After a database change, there might be a 30-second interval before the TSC starts writing the data to the flash drive. If you reset the active TSC immediately after a database change, the change could be lost.

You can also store a backup version of the database on the workstation running CTC. This operation should be part of a regular ONS 15600 SDH maintenance program at approximately weekly intervals and should also be completed when preparing an ONS 15600 SDH for a software upgrade or a pending natural disaster, such as a flood.

Note The Internet Inter-ORB Protocol (IIOP) port is not backed up and restored.

Note The ONS 15600 SDH does not allow you to restore a database from one node to another node. You can install a database from one node to another node by using the Configure Node option on the Maintenance > Database tab.

4.8 Software Load Revert

Before you upgrade to a later software release, you must create a database backup. If you later need to restore the original working software load from the protect software load, CTC displays a prompt requesting the location of the backup. Any provisioning performed with the later software release will be lost when the earlier software release backup is restored.

Note After a software load is activated (upgraded to a later software release), any circuits created and provisioning performed will not reinstate if an older database is restored. The database configuration at the time of activation is reinstated after a revert.

Security and Timing

This chapter provides information about Cisco ONS 15600 SDH user security and timing. To provision security and timing, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

5.1 Users and Security

Each ONS 15600 SDH permits up to 500 Cisco Transport Controller (CTC) or TL1 user IDs. A user ID is assigned one of the following security levels:

- Superuser—Users can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.
- Provisioning—Users can access provisioning and maintenance options.
- Maintenance—Users can access only the ONS 15600 SDH maintenance options.
- Retrieve—Users can retrieve and view CTC information but cannot set or modify parameters.

5.1.1 Security Requirements

Table 5-1 shows the actions that each security level allows in node view.

Table 5-1 ONS 15600 SDH Security Levels—Node View

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize, filter, and delete alarms	X	X	X	X
Conditions	—	Retrieve and filter	X	X	X	X
History	Session	Filter	X	X	X	X
	Node	Retrieve and filter alarms/events	X	X	X	X
Circuits	Circuits	Create/Delete/edit/filter/search/roll	—	—	X	X
	Roll	Complete circuits in the roll pending state	—	—	X	X

Table 5-1 ONS 15600 SDH Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Provisioning	General	Edit	—	—	X	X
	Network	All	—	—	—	X
	Protection	Create/delete/edit	—	—	X	X
		Browse groups	X	X	X	X
	MS-SPRing[1]	All (MS-SPRing)	—	—	X	X
	Security	Create/delete	—	—	—	X
		Change password	Same user	Same user	Same user	All users
	SNMP[2]	Create/delete/edit	—	—	—	X
		Browse trap destinations	X	X	X	X
	DCC/GCC[3]	Create/edit/delete	—	—	—	X
	Timing	Edit	—	—	X	X
	Alarm Behavior	Edit	—	—	X	X
	Alarm Extenders	Edit	—	—	X	X
Inventory	—	Delete	—	—	X	X
		Hard-reset	—	X	X	X
Maintenance	Database	Backup/restore	—	—	—	X
	Protection	Switch/lock out operations	—	X	X	X
	Diagnostic	Retrieve	—	X	X	X
	MS-SPRing	MS-SPRing maintenance	—	—	X	X
	Software	Download/upgrade/activate/revert	—	—	—	X
	Timing	Edit	—	X	X	X
	Audit	Retrieve	—	—	—	X
	Routing Table	Retrieve	X	X	X	X
	Test Access	Read only	X	X	X	X
	Alarm Extenders	Read only	X	X	X	X
	Preferred Copy	Edit	—	—	X	X

1. MS-SPRing = Multiplex Section-Shared Protection Ring
2. SNMP = Simple Network Management Protocol
3. DCC/GCC = Data Communication Channel / General Communication Channel

Table 5-2 shows the actions that each user privilege level can perform in network view.

Table 5-2 ONS 15600 SDH Security Levels—Network View

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize/filter/delete cleared alarms	X	X	X	X
Conditions	—	Retrieve/filter	X	X	X	X
History	—	Filter	X	X	X	X
Circuits	Circuits	Create/delete/edit/filter/search/ roll	—	—	X	X
	Roll	Complete circuits in the roll pending state	—	—	X	X
Provisioning	Security	Users tab: create/change/delete	—	—	—	X
		Active logins tab: logout	—	—	—	X
		Policy tab: change	—	—	—	X
	Alarm Profiles	Load/store/delete	—	—	X	X
		Compare/available/usage	—	X	X	X
	MS-SPRing	All (MS-SPRing)	—	—	X	X
	Overhead Circuits	Edit	—	—	X	X
Maintenance	Software	Download	—	—	X	X

5.1.2 Initial Login

When you log into an ONS 15600 SDH for the first time, you use the CISCO15 user ID, which is provided with every ONS 15600 SDH system. You can use the CISCO15 ID, which has Superuser privileges, to create other ONS 15600 SDH user IDs. For detailed instructions on creating users, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Note When creating a user, a Superuser must add the same user ID and password to each node that a user will access.

5.1.3 Concurrent Logins

Concurrent user ID sessions are allowed on a node, which means that multiple users can log into a node using the same user ID. For example, two or more users can log into a node with the CISCO15 user ID. The default setting is to allow concurrent user ID sessions. If the Superuser provisions a user ID to be active for a single occurrence only, concurrent logins with that user ID are not allowed. A Superuser sets a user ID as single occurrence on the Provisioning > Security > Policy tabs, Single Session per User check box.

5.1.3.1 Idle User Timeout

Each ONS 15600 SDH CTC or TL1 user has a specified amount of time to leave the system idle before the CTC window locks. The CTC lockouts prevent unauthorized users from making changes. Higher-level users have shorter idle times and lower-level users have longer or unlimited default idle periods, as shown in Table 5-3. Superusers can change user idle times on the Provisioning > Security > Policy tabs.

Table 5-3 ONS 15600 SDH User Idle Times

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

5.1.3.2 Superuser Password and Login Privileges

A Superuser can perform ONS 15600 SDH user creation and management tasks from the network or node (default login) view. In network view, a Superuser can add, edit, or delete users from multiple nodes at one time. In node view, a Superuser can only add, edit, or delete users from that node.

Superuser password and login privilege criteria include:

- Privilege level—A Superuser can change the privilege level (such as Maintenance or Provisioning) of a user ID while the user is logged in. The change will become effective the next time the user logs in and will apply to all nodes within the network.
- Login visibility—Superusers can view real-time lists of users who are logged into a node (both CTC and TL1 logins) by retrieving a list of logins by node. A Superuser can also log out an active user.
- Password expiration and reuse settings—Superusers provision password reuse periods (the number of days before a user can reuse a password) and reuse intervals (the number of passwords a user must generate before reusing a password).
- User lockout settings—A Superuser can manually lock out or unlock a user ID.
- Invalid login attempts—A Superuser sets the number of invalid login attempts a user can make before the user ID is locked out. Additionally, the Superuser sets the time interval the user ID is locked out after the user reaches the login attempt limit.

5.1.4 User Audit Trail

The ONS 15600 SDH maintains an audit trail of user actions such as login, logout, and circuit creation or deletion. You can move the log to a local or network drive for later review. The audit log can hold up to 640 entries. The ONS 15600 SDH generates an event to indicate when the log is 80 percent full and another event to indicate that the oldest log entries are being overwritten. To offload the audit log, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

5.2 Node Timing

SDH timing parameters must be set for each ONS 15600 SDH node. Each ONS 15600 SDH independently accepts its timing reference from one of three sources:

- The building integrated timing supply (BITS) pins on the customer access panel (CAP).
- A port on an STM-N card installed in the ONS 15600 SDH. The timing is traceable to a node that receives timing through a BITS source.
- The internal Stratum 3E clock (ST3E) on the TSC card.

You can set ONS 15600 SDH timing to one of two modes: external or line. If the timing comes from BITS, set ONS 15600 SDH timing to external. If the timing comes from an STM-N port, set the timing to line. In typical ONS 15600 SDH networks:

- One node is set to external. The external node derives its timing from a BITS source wired to the BITS backplane pins. The BITS source, in turn, derives its timing from a primary reference source (PRS), such as a Stratum 1 clock or global positioning satellite (GPS) signal.
- Other nodes are set to line. The line nodes derive timing from the externally timed node through the STM-N trunk cards.

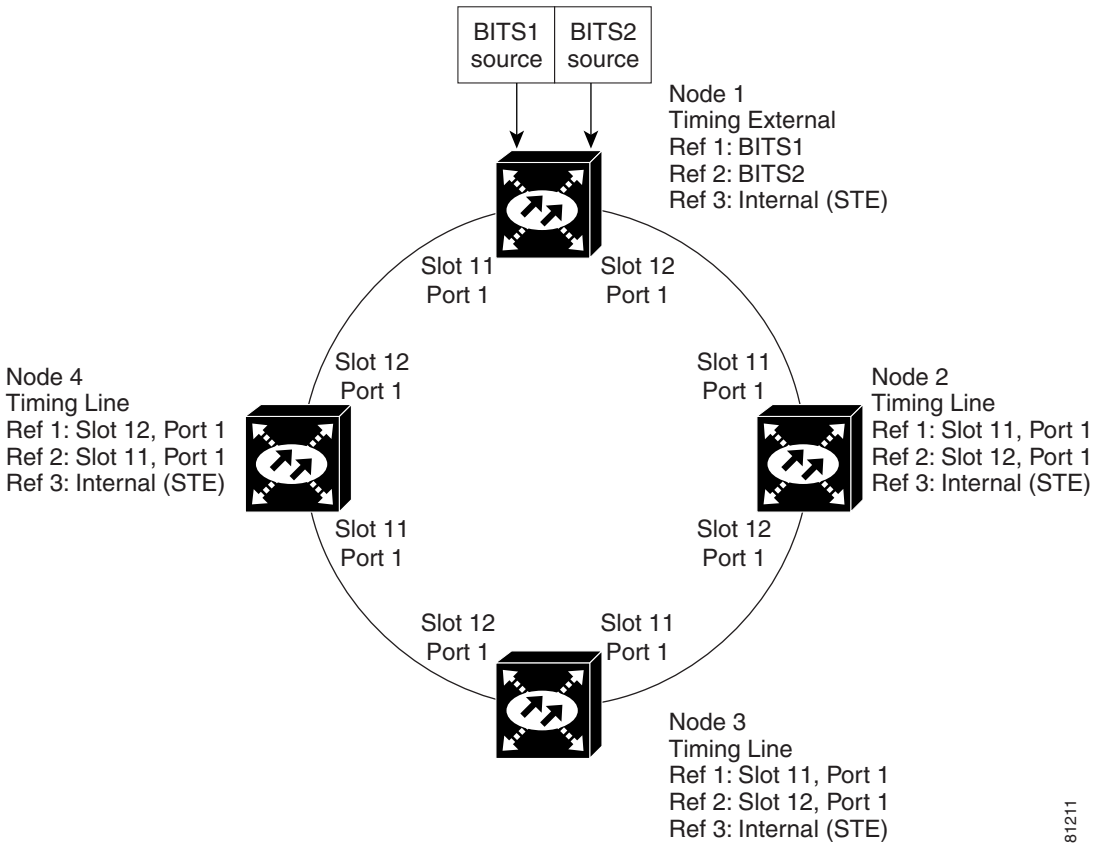
You can set three timing references for each ONS 15600 SDH. The first two references are typically two BITS-level sources, or two line-level sources optically traceable to a node with a BITS source. The third reference is the internal ST3E clock provided on every ONS 15600 SDH TSC card. If an ONS 15600 SDH becomes isolated, the TSC maintains timing at the ST3E level.

5.2.1 Network Timing Example

Figure 5-1 shows an ONS 15600 SDH network timing example. Node 1 is set to external timing. Two timing references are Stratum 1 timing sources wired to the BITS input pins on the Node 1 backplane. The third reference is set to internal clock.

In the example, Slots 11 and 12 of Node 1 contain the trunk (span) cards. Timing at Nodes 2, 3, and 4 is set to line, and the timing references are set to the trunk cards according to the distance from the BITS source. Reference 1 is set to the trunk card closest to the BITS source. At Node 2, Reference 1 is Slot 11/Port 1 because it is connected to Node 1. At Node 4, Reference 1 is set to Slot 12/Port 1 because it is connected to Node 1. At Node 3, Reference 1 could be either trunk card because they are an equal distance from Node 1.

Figure 5-1 ONS 15600 SDH Timing Example



5.2.2 Synchronization Status Messaging

Synchronization status messaging (SSM) is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH MS layer. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

If you enable SSM for the ONS 15600 SDH, consult your timing reference documentation to determine which message set to use. Table 5-4 lists the SSM message set.

Table 5-4 SDH SSM Message Set

Message	Quality	Description
G811	1	Primary reference clock
STU	2	Sync traceability unknown
G812T	3	Transit node clock traceable
G812L	4	Local node clock traceable
SETS	5	Synchronous equipment
DUS	6	Do not use for timing synchronization

Circuits and Tunnels

This chapter explains Cisco ONS 15600 SDH VC4 high-order circuits and data communications channel (DCC) tunnels. To provision circuits and tunnels, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

Note In this chapter, "cross-connect" and "circuit" have the following meanings: cross-connect refers to the connections that occur within a single ONS 15600 SDH to allow a circuit to enter and exit an ONS 15600 SDH. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15600 SDH network) to the destination (where traffic exits an ONS 15600 SDH network).

6.1 Circuit Properties

The ONS 15600 SDH supports unidirectional and bidirectional circuits. Subnetwork connection protection (SNCP) or multiplex section-shared protection ring (MS-SPRing) circuits can be revertive or nonrevertive. Circuits will route automatically or you can manually route them. The autorange feature eliminates the need to build circuits of the same type individually; Cisco Transport Controller (CTC) can create up to five sequential circuits. You must specify the number of circuits that you need and build the first circuit.

You can provision circuits at either of the following points:

- Before cards are installed. The ONS 15600 SDH allows you to provision slot and circuits before installing the traffic cards. However, circuits will not carry traffic until the cards are installed, the circuit status is In Service (IS), and the port status is IS or Out of Service-Maintenance (OOS-MT).

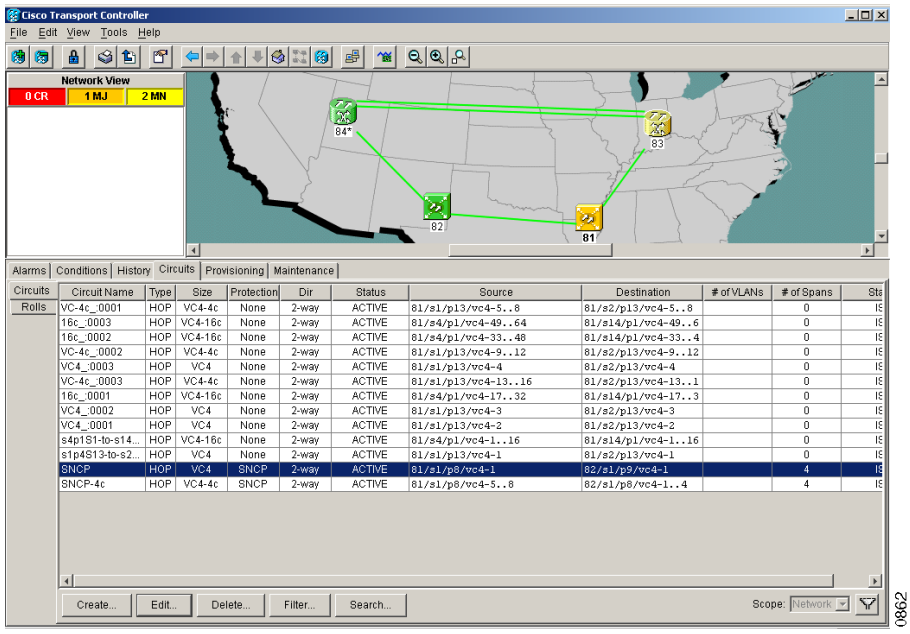
- Cards are installed and their ports are in service. Circuits will carry traffic as soon as the signal is received.

The ONS 15600 SDH Circuits window (Figure 6-1), which is available from network, node, and card view, is where you can view information about circuits, including:

- Name—The name of the circuit (user-assigned or automatically generated).
- Type—For the ONS 15600 SDH, the circuit type is VC4 (VC4 circuit).
- Size—VC4 circuit sizes can be VC4, VC4-2c, VC4-3c, VC4-4c, VC4-8c, VC4-16c, or VC4-64c.
- Protection—The protection type; see the "6.1.2 Circuit Protection Types" section on page 6-4.
- Direction—The circuit direction, either two-way or one-way.
- Status—The circuit status; for details, see the "6.1.1 Circuit Status" section on page 6-3.
- Source—The circuit source in the format *node/slot/port/VC4*.
- Destination—The circuit destination in the format *node/slot/port/VC4*.
- # of VLANS—The number of VLANs used by an Ethernet circuit (future use for the ONS 15600 SDH).
- # of Spans—The number of internode links that compose the circuit.
- State—The circuit state. The ONS 15600 SDH Release 1.4 does not support a full state model. As a result, you cannot change the circuit state; it is always IS.

Note You cannot set up low-order (VC3 and VC12) circuits to terminate on an ONS 15600 SDH node. However, you can create both VC4 and low-order circuits that have an ONS 15454 SDH source and destination with an ONS 15600 SDH as a pass-through node. For information on low-order circuit creation and tunneling, refer to the circuit chapters in the *Cisco ONS 15454 SDH Reference Manual*. Note that you cannot mix protection schemes, for example, 1+1 to SNCP. Acceptable schemes are unprotected to unprotected, 1+1 to 1+1, MS-SPRing to MS-SPRing, and SNCP to SNCP.

Figure 6-1 ONS 15600 SDH Circuit Window in Network View



6.1.1 Circuit Status

The circuit statuses that appear in the Circuit window Status column are generated by CTC based on an assessment of conditions along the circuit path. Table 6-1 lists the statuses that can appear in the Status column.

Table 6-1 ONS 15600 SDH Circuit Status

Status	Definition/Activity
CREATING	CTC is creating a circuit.
ACTIVE	CTC created a circuit. All components are in place and a complete path exists from circuit source to destination.
DELETING	CTC is deleting a circuit.
INCOMPLETE	A CTC-created circuit is missing a connection or circuit span (network link), a complete path from source to destination(s) does not exist, or a MAC address change occurred on one of the circuit nodes and the circuit is in need of repair. (In the ONS 15454 SDH, the MAC address resides on the alarm interface panel [AIP]; in the ONS 15600 SDH, the MAC address resides on the backplane EEPROM.) In CTC, circuits are represented using cross-connects and network spans. If a network span is missing from a circuit, the circuit status is INCOMPLETE. However, an INCOMPLETE status does not necessarily mean a circuit traffic failure has occurred because traffic might be on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans appear as green lines (Figure 6-1 on page 6-2) and down spans appear as gray lines. If a failure occurs on a network span during a CTC session, the span remains on the network map but its color changes to gray to indicate the span is down. If you restart your CTC session while the failure is active, the new CTC session cannot discover the span and its span line will not appear on the network map. Subsequently, circuits routed on a network span that goes down will appear as ACTIVE during the current CTC session, but they will appear as INCOMPLETE to users who log in after the span failure.
UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit is complete and has upgradable cross-connects. A complete path from source to destination(s) exists. The circuit can be upgraded.
INCOMPLETE_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit with upgradable cross-connects is missing a cross-connect or circuit span (network link), and a complete path from source to destination(s) does not exist. The circuit cannot be upgraded until missing components are in place.

Table 6-1 ONS 15600 SDH Circuit Status (continued)

Status	Definition/Activity
NOT_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit is complete but has at least one nonupgradable cross-connect. SNCP_HEAD, SNCP_EN, SNCP_DC, and SNCP_DROP connections are not upgradable so all unidirectional SNCP circuits created with TL1 are not upgradable.
INCOMPLETE_NOT_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit with one or more nonupgradable cross-connects is missing a cross-connect or circuit span (network link); a complete path from source to destination(s) does not exist.
ROLL_PENDING	Roll is awaiting completion or cancellation. When a roll is in the ROLL PENDING state, you can complete a manual roll and cancel an automatic or manual roll.

6.1.2 Circuit Protection Types

The Protection column on the Circuit window shows the card (MS) and SDH topology (AU4) protection used for the entire circuit path. Table 6-2 lists the protection type indicators that you will see in this column.

Table 6-2 Circuit Protection Types

Protection Type	Description
—	Circuit protection is not applicable.
2F MS-SPRing	The circuit is protected by a 2-fiber MS-SPRing.
SNCP	The circuit is protected by an SNCP.
1+1	The circuit is protected by a 1+1 protection group.
Protected	The circuit is protected by diverse SDH topologies, for example a MS-SPRing and an SNCP, or an SNCP and 1+1.
Unprot (black)	The circuit is not protected.
Unprot (red)	A circuit created as a fully protected circuit is no longer protected due to a system change, such as a traffic switch.
Unknown	Circuit protection types appear in the Protection column only when all circuit components are known, that is, when the circuit status is ACTIVE or UPGRADABLE. If the circuit is in some other status, the protection type appears as “unknown.”

6.1.3 Viewing Circuit Information on the Edit Circuit Window

When Show Detailed Map is checked on the Edit Circuit window, you can view information about ONS 15600 SDH circuits. Routing information includes:

- Circuit direction (unidirectional or bidirectional)
- The nodes and VC4s that the circuit traverses, including slots and port numbers

- The circuit source and destination points
- Open Shortest Path First (OSPF) area IDs
- Link protection (SNCP, unprotected, MS-SPRing, 1+1) and bandwidth (STM-N)

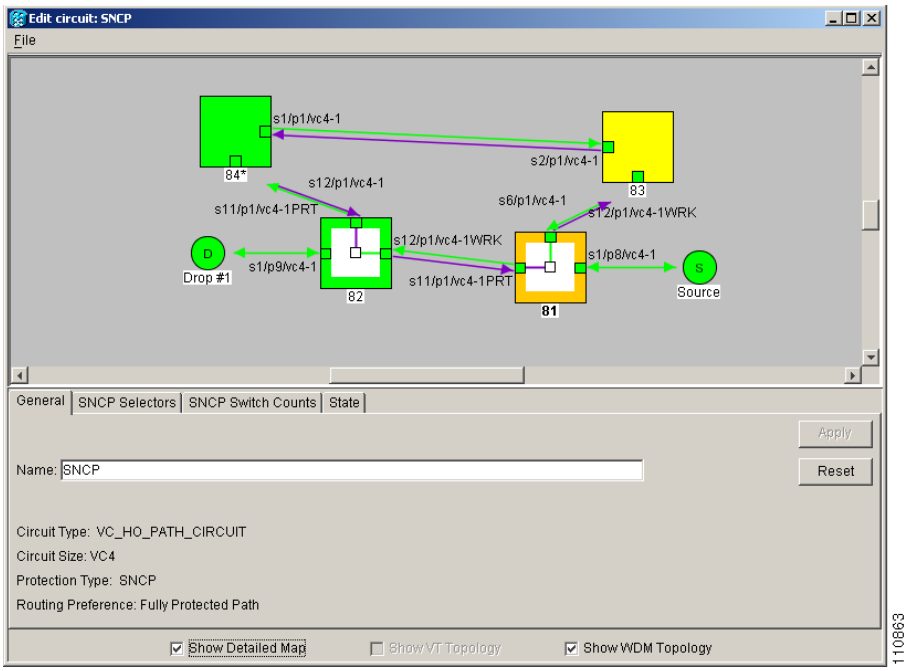
For MS-SPRings, the detailed map shows the number of MS-SPRing fibers and the MS-SPRing ring ID. For SNCPs, the map shows the active and standby paths from circuit source to destination, and it also shows the working and protect paths.

Alarms and states can also be viewed on the circuit map, including:

- Alarm states of nodes on the circuit route
- Number of alarms on each node organized by severity
- Port service states on the circuit route
- Alarm state/color of most severe alarm on port
- Loopbacks
- Path trace states
- Path selector states

Figure 6-2 shows a bidirectional VC4 circuit routed on an SNCP.

Figure 6-2 SNCP Circuit on the Edit Circuits Window



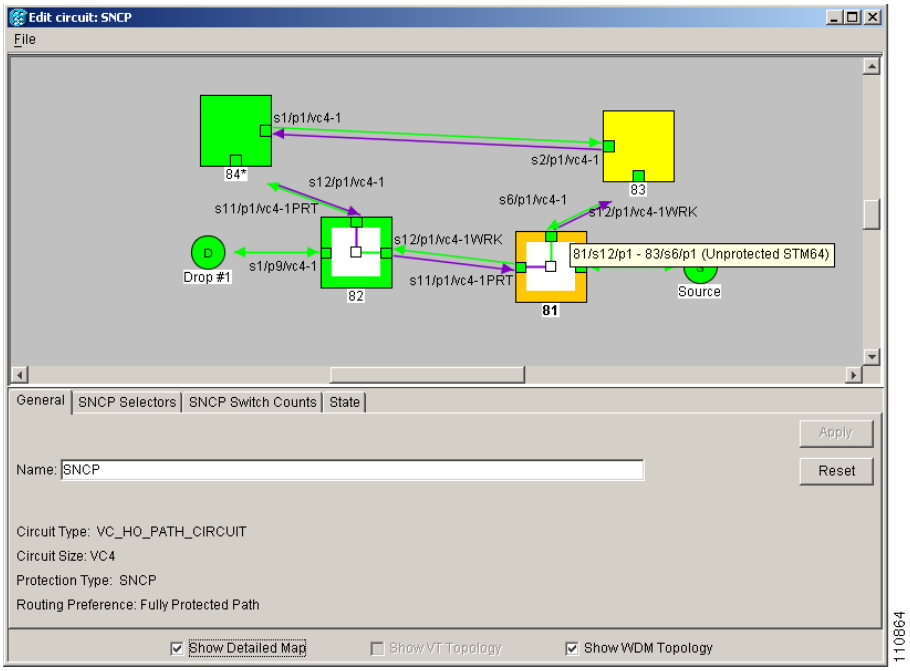
By default, the working path is indicated by a green, bidirectional arrow, and the protect path is indicated by a purple, bidirectional arrow. Source and destination ports are shown as circles with an S and D, respectively. Port status is indicated by colors, shown in Table 6-3.

Table 6-3 Port State Color Indicators

Port Color	State
Green	IS
Light blue	OOS-MT

Figure 6-3 shows a popup for an SNCP span. The detailed circuit map also provides popup span information for MS-SPRings.

Figure 6-3 Detailed Circuit Map Showing Span Information



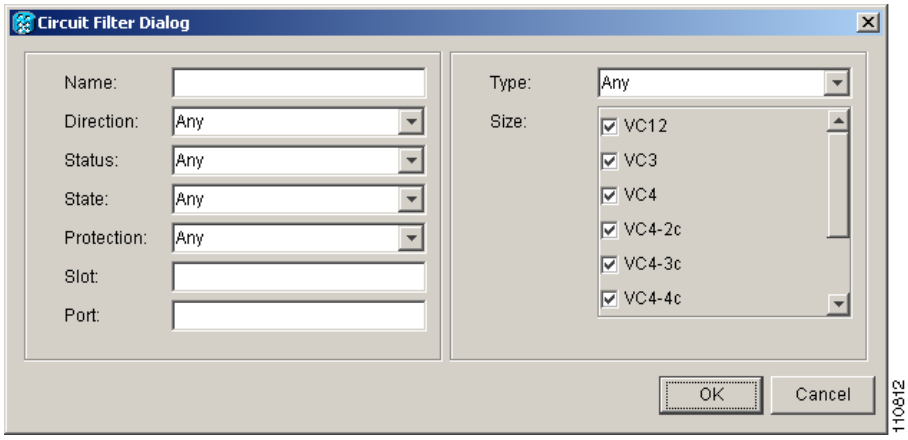
In addition to providing circuit information, the detailed circuit map allows you to add a drop and initiate a path trace:

- To add a drop to a circuit, right-click a unidirectional circuit destination node and choose from the menu.
- To initiate a path trace, right-click a port containing a path trace capable card and choose from the menu.

6.1.4 Circuit Filter

The ONS 15600 SDH will support up to 2048 VC4 circuits. The Circuit Filter feature allows you to reduce the number of circuits that appear on the Circuits window (Figure 6-4). You can specify certain filter criteria, such as name, direction, and state; only the circuits that match the criteria will appear on the Circuits window.

Figure 6-4 Filtering Circuits



6.2 DCC Tunnels

SDH provides four DCCs for network element Operation, Administration, Maintenance, and Provisioning (OAM&P): one on the SDH regenerator section (RS) layer (DCC1) and three on the SDH multiplex section (MS) layer (DCC2, DCC3, DCC4). The ONS 15600 SDH uses the RS DCC for ONS 15600 SDH management and provisioning.

You can use the three MS DCCs and the RS DCC (when not used for ONS 15600 SDH DCC terminations) to tunnel third-party SDH equipment across ONS 15600 SDH networks. A DCC tunnel endpoint is defined by slot, port, and DCC, where DCC can be either the RS DCC or one of the MS DCCs. You can link MS DCCs to MS DCCs and link RS DCCs to RS DCCs. You can also link a RS DCC to a MS DCC and a MS DCC to a RS DCC. To create a DCC tunnel, connect the tunnel endpoints from one ONS 15600 SDH optical port to another.

Table 6-4 lists the DCC tunnels that you can create.

Table 6-4 DCC Tunnels

DCC	SDH Layer	SDH Bytes
DCC1	RS	D1 to D3
DCC2	MS	D4 to D6
DCC3	MS	D7 to D9
DCC4	MS	D10 to D12

When you create DCC tunnels, keep the following guidelines in mind:

- Each ONS 15600 SDH can have up to 64 DCC tunnel connections.
- A RS DCC that is terminated cannot be used as a DCC tunnel endpoint.
- A RS DCC that is used as an DCC tunnel endpoint cannot be terminated.
- All DCC tunnel connections are bidirectional.

6.3 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 to the source. The ONS 15600 SDH supports either of the following:

- Up to 2048 1:2 nonblocking broadcast connections
- Up to 682 1:*N* nonblocking broadcast connections (where *N* is less than or equal to 8)

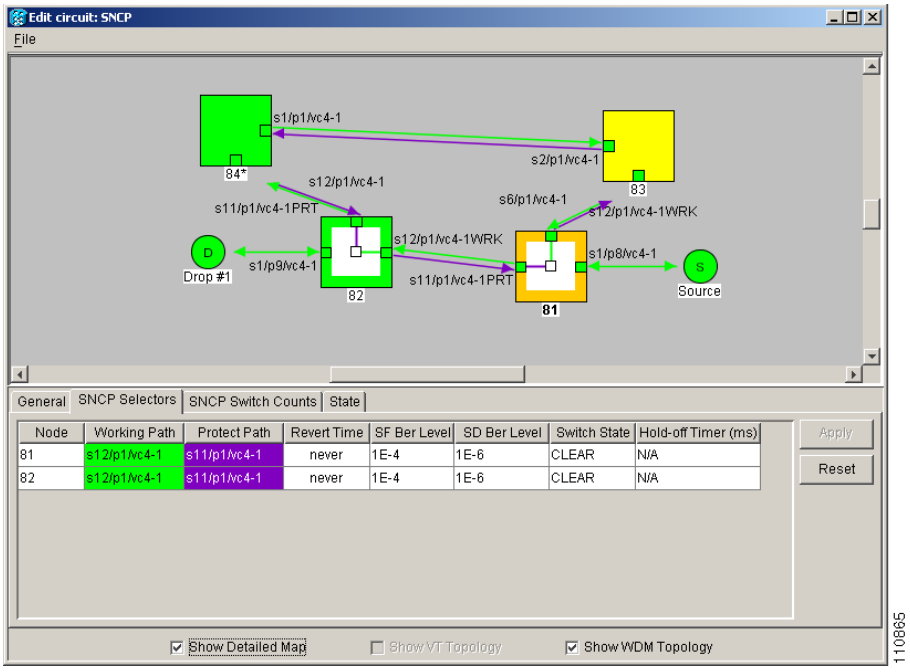
When you create a unidirectional circuit, the card that does not have its backplane receive (Rx) input terminated with a valid input signal generates a loss of service (LOS) alarm. To mask the alarm, create an alarm profile suppressing the LOS alarm and apply the profile to the port that does not have its Rx input terminated.

6.4 SNCP Circuits

Use the Edit Circuits window to change SNCP selectors and switch protection paths (Figure 6-5). In the SNCP Selectors tab, you can:

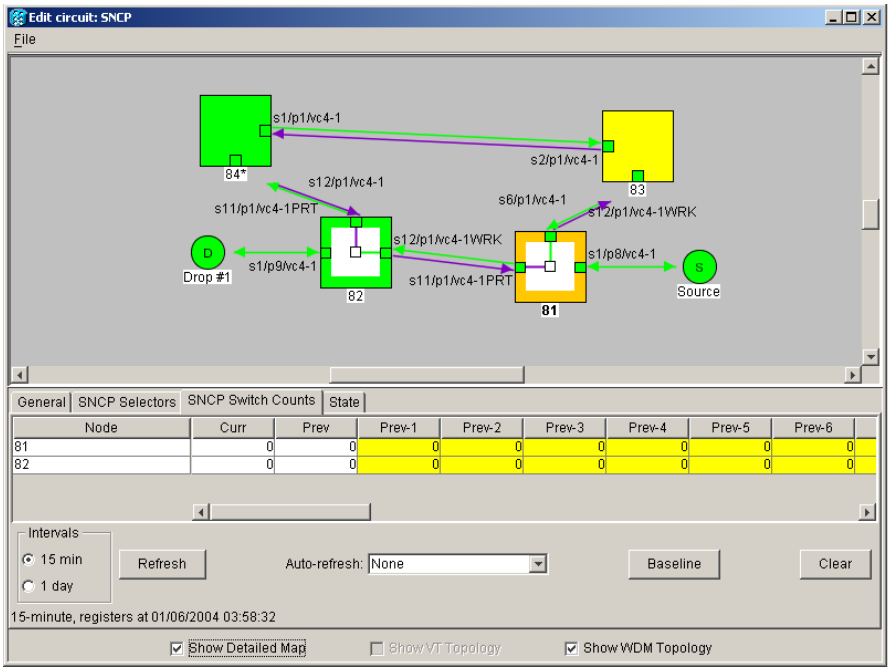
- View the SNCP circuit's working and protection paths
- Edit the reversion time
- Edit the signal fail/signal degrade thresholds

Figure 6-5 Editing SNCP Selectors



On the SNCP Switch Counts tab, you can view switch counts for the selectors (Figure 6-6).

Figure 6-6 Viewing SNCP Switch Counts



6.5 Path Trace

The SDH J1 Path Trace is a repeated, fixed-length string that includes 64 or 16 consecutive J1 bytes. You can use the string to monitor interruptions or changes to circuit traffic. Table 6-5 lists the ONS 15600 SDH cards that support path trace. Cards not listed in the table do not support the J1 byte.

Table 6-5 ONS 15600 SDH Cards Supporting J1 Path Trace

Card	Receive	Transmit
OC48/STM16 SR/SH 16 Port 1310	Yes	Yes
OC48/STM16 LR/LH 16 Port 1550	Yes	Yes
OC192/STM64 SR/SH 4 Port 1310	Yes	Yes
OC192/STM64 LR/LH 4 Port 1550	Yes	Yes

The J1 path trace transmits a repeated, fixed-length string. If the string received at a circuit drop port does not match the string the port expects to receive, an alarm is raised.

The ONS 15600 SDH supports manual J1 path trace monitoring to detect and report the contents of the 64-byte VC4 path trace message (nonterminated) for the designated VC4 path. You can also modify the expected path trace message. The ONS 15600 SDH does not support path trace auto mode or allow you to modify a transmitted path trace message.

The ONS 15600 SDH can also monitor a 16-byte ITU pattern.

6.6 Automatic Circuit Routing

If you select automatic routing during circuit creation, CTC routes the circuit by dividing the entire circuit route into segments based on protection schemes. 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 scheme, and each protection scheme is protected in a specific fashion (virtual SNCP or 1+1).

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.
- If you do not choose Fully Path Protected during circuit creation, circuits can still contain protected segments. Because circuit routing always selects the shortest path, one or more segments might have protection. CTC does not look at link (segment) protection while computing a path for unprotected circuits.
- Circuit routing will not use links that are out of service. If you want all links to be considered for routing, do not create circuits when a link is out of service.
- Circuit routing computes the shortest path when you add a new drop to an existing circuit.

6.6.1 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:

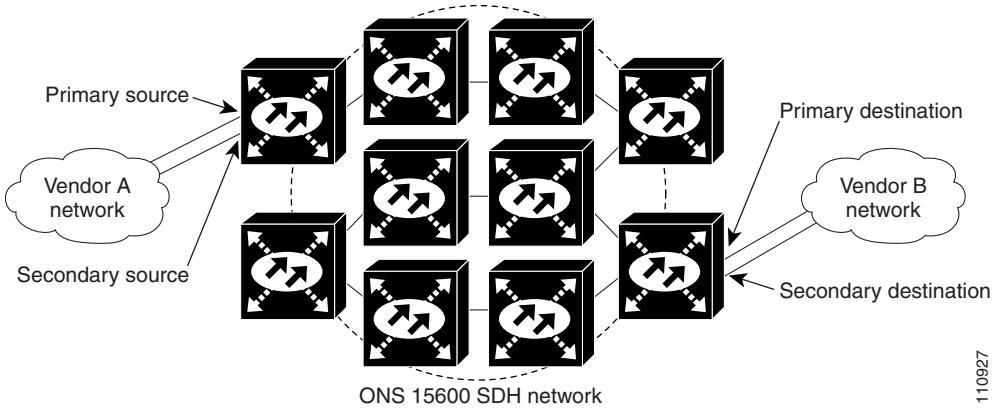
- The link has sufficient bandwidth to support the circuit.
- The link does not change the protection characteristics of the path.

If CTC cannot find a link that meets these requirements, an error appears.

6.6.2 Secondary Sources and Drops

CTC supports secondary sources and drops. Secondary sources and drops typically interconnect two networks containing equipment from different vendors, as shown in Figure 6-7. Traffic is protected while it traverses a network of ONS 15600 SDH nodes.

Figure 6-7 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 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 VC4 connections.

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 15600 SDH network. If you check the Fully Path Protected option during circuit creation, traffic is protected within the ONS 15600 SDH network. At the destination, another SNCP connection is created to bridge traffic from the ONS 15600 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.

6.7 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 VC4 on each link along the route

CTC imposes the following rules on manual routes:

- All circuits in a shared packet ring should have links with a direction that flows from source to destination.
- If you enabled Fully Protected Path, choose a diverse protect (alternate) path for every unprotected segment.
- For a node that has an SNCP selector based on the links chosen, the input links to the SNCP selectors cannot be 1+1 protected. The same rule applies at the SNCP bridge.

If Fully Protected Path is chosen, CTC verifies that the route selection is protected at all segments. A route can have multiple protection schemes with each scheme protected by a different mechanism.

Table 6-6 summarizes the available bidirectional connections. Any other combination is invalid and will generate an error.

Table 6-6 Bidirectional VC4 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

Table 6-7 summarizes the available unidirectional connections. Any other combination is invalid and will generate an error.

Table 6-7 Unidirectional VC4 Circuits

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
—	2	1	—	SNCP head end
2	—	—	1+	SNCP drop and continue

6.8 Constraint-Based Circuit Routing

When you create circuits, you can choose Fully Protected Path to protect the circuit from source to destination. The protection mechanism used depends on the path that CTC calculates for the circuit. If the network is comprised entirely of 1+1 links, or the path between source and destination can be entirely protected using 1+1 links, no Extended SNCP Mesh Networks protection is used.

If Extended SNCP Mesh Networks protection is needed to protect the path, set the level of node diversity for the Extended SNCP Mesh Networks 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 Networks scheme 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 Networks scheme in the complete path.
- Link Diversity Only—Creates only a link diverse path for each Extended SNCP Mesh Networks scheme.

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 achieve the following results:

- 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 use less bandwidth. 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 used only during the primary path computation and only for Extended SNCP Mesh Networks segments. The alternate path is computed normally; CTC uses excluded nodes/links when finding all primary and alternate paths on Extended SNCP Mesh Networks.

6.9 Bridge and Roll

The Bridge and Roll wizard reroutes live traffic without interrupting service. The bridge process takes traffic from a designated “roll from” facility and establishes a cross connect to the designated “roll to” facility. After the bridged signal at the receiving end point is verified, the roll process creates a new cross-connect to receive the new signal. After the roll completes, the original cross-connects are released. You can use the bridge and roll feature for maintenance functions such as card or facility replacement, or for load balancing.

Note To perform bridge and roll, you should be logged into an ONS 15600 SDH node. If you are logged into an ONS 15454 SDH node, you should log out. When you log in, clear the cache and reload CTC from an ONS 15600 SDH node.

6.9.1 Roll States

Table 6-8 lists the roll states.

Table 6-8 Roll States

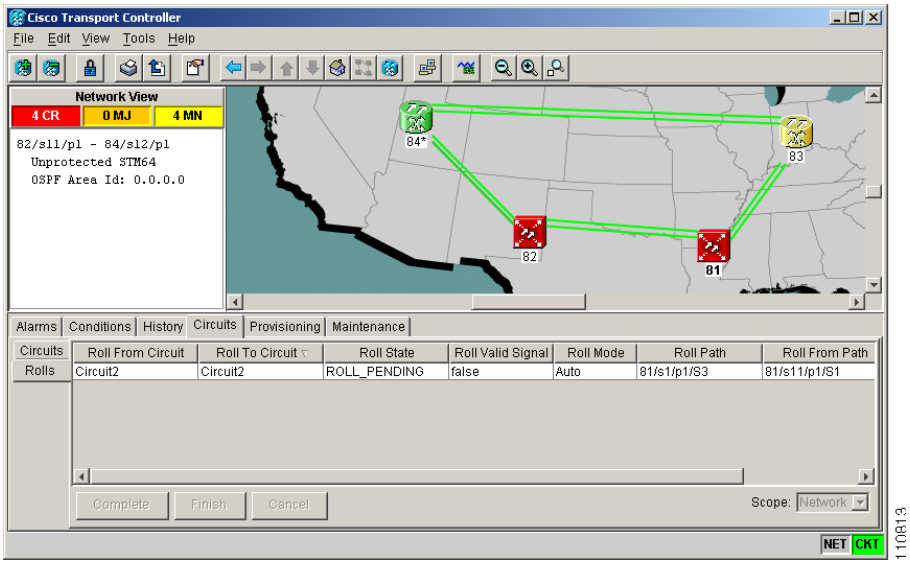
State	Description
ROLL_PENDING	Roll is awaiting completion or cancellation.
ROLL_CANCELLED	Roll has been canceled.

Note You can only reroute circuits in the Active state. You cannot reroute circuits that are in the Roll Pending state.

6.9.2 Roll Window

The Rolls window lists information about a rolled circuit before the roll process is complete. You can access the Rolls window by clicking the Circuits > Rolls tabs in either network or node view. Figure 6-8 shows the Rolls window.

Figure 6-8 Rolls Window



The Rolls window options include:

- Roll From Circuit is the circuit that has connections that will no longer be used after the roll process is complete.
- Roll To Circuit identifies the circuit that will carry the traffic after the roll process is complete. The Roll To Circuit will be the same as the Roll From Circuit if a single circuit is involved in a roll.
- Roll State shows the values described in Table 6-8.
- Roll Mode indicates whether the roll is automatic or manual. CTC implements roll mode at the cross-connect level, which means it applies to connections within a single ONS 15600 SDH.
  - Automatic—When a valid signal is received on the new path, CTC completes the roll on the node automatically. You can cancel an automatic roll only when the Roll Valid Signal value is false. One-way source rolls are always automatic.
  - Manual—You must complete a manual roll after a valid signal is received. You can cancel a manual roll at any time. One-way destination rolls are always manual.
- Roll Path indicates the fixed point of the roll object.
- Roll From Path indicates the path (VC4) that is being rerouted.
- Roll To Path indicates the new path where the Roll From Path is rerouted.
- Use the Complete button to terminate a manual roll. You can do this when a manual roll is in a ROLL_PENDING state and you have not yet completed the roll or have not cancelled its sibling roll.
- Use the Finish button to complete the circuit processing of a roll. It changes the circuit state from ROLL_PENDING to ACTIVE.

- Use the Cancel button to cancel the selected roll. You can cancel a manual roll at anytime; you can cancel an automatic roll only if the Roll Valid Signal is false.

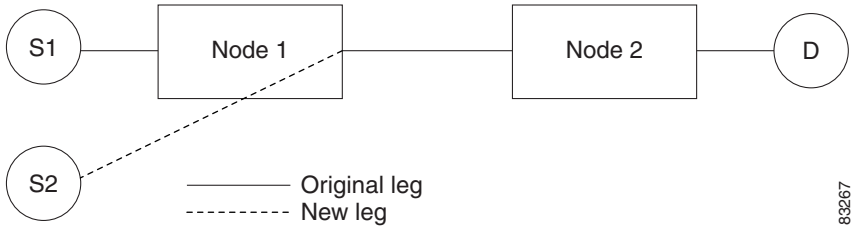
6.9.3 Single and Dual Rolls

Circuits have an additional layer of roll types, single and dual. A single roll on a circuit is a roll on one of its cross-connections. Use a single roll to:

- Change either the source or destination of a selected circuit (Figure 6-9 and Figure 6-10, respectively).
- Roll a segment of the circuit onto another chosen circuit (Figure 6-11). This roll also results in a new destination.

In Figure 6-9, you can select any available VC4 on Node 1 for a new source.

Figure 6-9 Single Source Roll



In Figure 6-10, you can select any available VC4 on Node 2 for a new destination.

Figure 6-10 Single Destination Roll

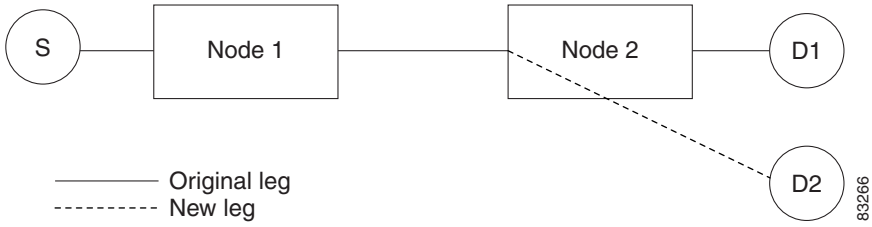
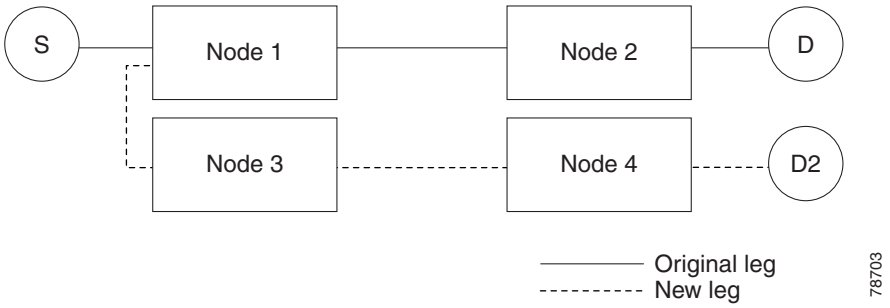


Figure 6-11 shows one circuit rolling onto another circuit. The new circuit has cross-connections on Node 1, Node 3, and Node 4. CTC deletes the cross-connection on Node 2 after the roll.

Figure 6-11 Single Roll from One Circuit to Another Circuit



A dual roll involves two cross-connections. It allows you to reroute intermediate segments of a circuit, but keep the original source and destination. You can perform a dual roll on a single circuit or two circuits. When rolling two cross-connections using the CTC Bridge and Roll wizard, you can choose an existing circuit or create a new circuit. The created circuit is designated with the same name as the original circuit with the suffix _ROLL**.

Several constraints exist for dual rolls:

- You must complete or cancel both cross-connects rolled in a dual roll. You cannot complete one roll and cancel the other roll.
- When a Roll To circuit is involved in the dual roll, the first roll must roll onto the source of the Roll To circuit and the second roll must roll onto the destination of the Roll To circuit.

Figure 6-12 illustrates a dual roll on the same circuit.

Figure 6-12 Dual Roll on the Same Circuit

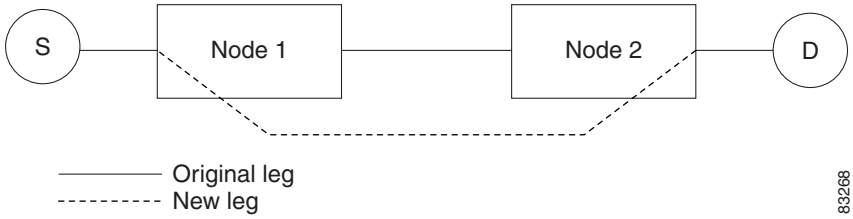
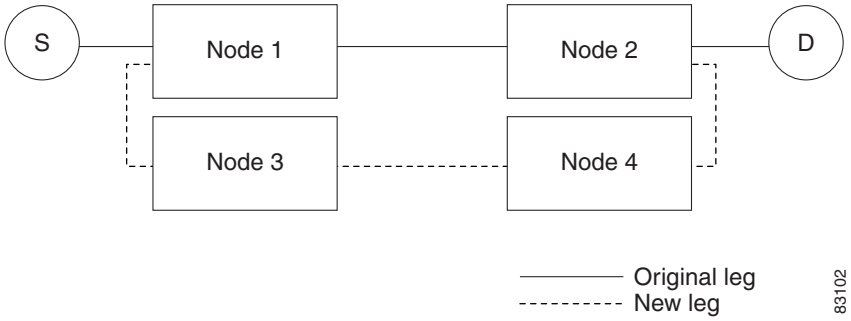


Figure 6-13 illustrates a dual roll involving two circuits.

Figure 6-13 Dual Roll on Two Circuits



6.9.4 Circuit Bridge and Roll Restrictions

Several restrictions apply when using the bridge and roll feature to reroute traffic using two circuits:

- DCC must be enabled on the circuits involved in a roll before roll creation.
- A maximum of two rolls can exist between any two circuits.
- If two rolls are involved between two circuits, both rolls must be on the original circuit. The second circuit should not carry live traffic. The two rolls loop from the second circuit back to the original circuit. The roll mode of the two rolls must be identical (either automatic or manual).
- If a single roll exists on a circuit, you must roll the connection onto the source or the destination of the second circuit and not an intermediate node in the circuit.

6.9.5 Protected Circuits

CTC allows you to roll the working or protect path regardless of which is active. You can upgrade an unprotected circuit to a fully protected circuit or downgrade a 1+1-protected circuit to an unprotected circuit.

When using bridge and roll on SNCP circuits, you can roll the source or destination or both path selectors in a dual roll. However, you cannot roll a single path selector.

You can also perform bridge and roll on MS-SPRing circuits.

SDH Topologies

This chapter explains Cisco ONS 15600 SDH topologies. To provision topologies, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

The ONS 15600 SDH usually operates as a hub node in networks that include ONS 15454 SDH nodes. Single nodes are installed at geographic locations where several ONS 15454 SDH topologies converge. A single ONS 15600 SDH node might be a part of several ONS 15454 SDH rings/networks.

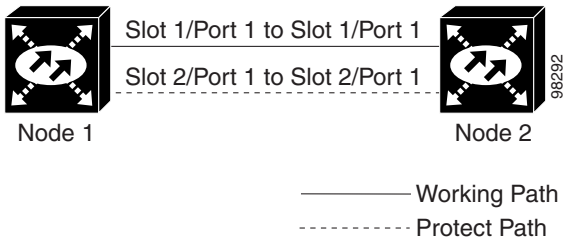
To avoid errors during network configuration, Cisco recommends that you draw the complete ONS 15600 SDH topology on paper (or electronically) before you begin the physical implementation. A sketch ensures that you have adequate slots, cards, and fibers to complete the topology.

7.1 Linear ADM Configurations

You can configure ONS 15600 SDH nodes as a line of add/drop multiplexers (ADMs) by configuring one STM-N port as the working path and a second port as the protect path. Unlike rings, point-to-point (two node configurations) and linear (three node configurations) ADMs require that the STM-N ports at each node are in 1+1 Linear Multiplex Section Protection (LMSP) to ensure that a break to the working path automatically routes traffic to the protect path.

Figure 7-1 shows two ONS 15600 SDH nodes in a point-to-point ADM configuration. Working traffic flows from Slot 1/Port 1 at Node 1 to Slot 1/Port 1 at Node 2. You create the protect path by creating a 1+1 LMSP configuration with Slot 1/Port 1 and Slot 2/Port 1 at Nodes 1 and 2.

Figure 7-1 Point-to-Point ADM Configuration



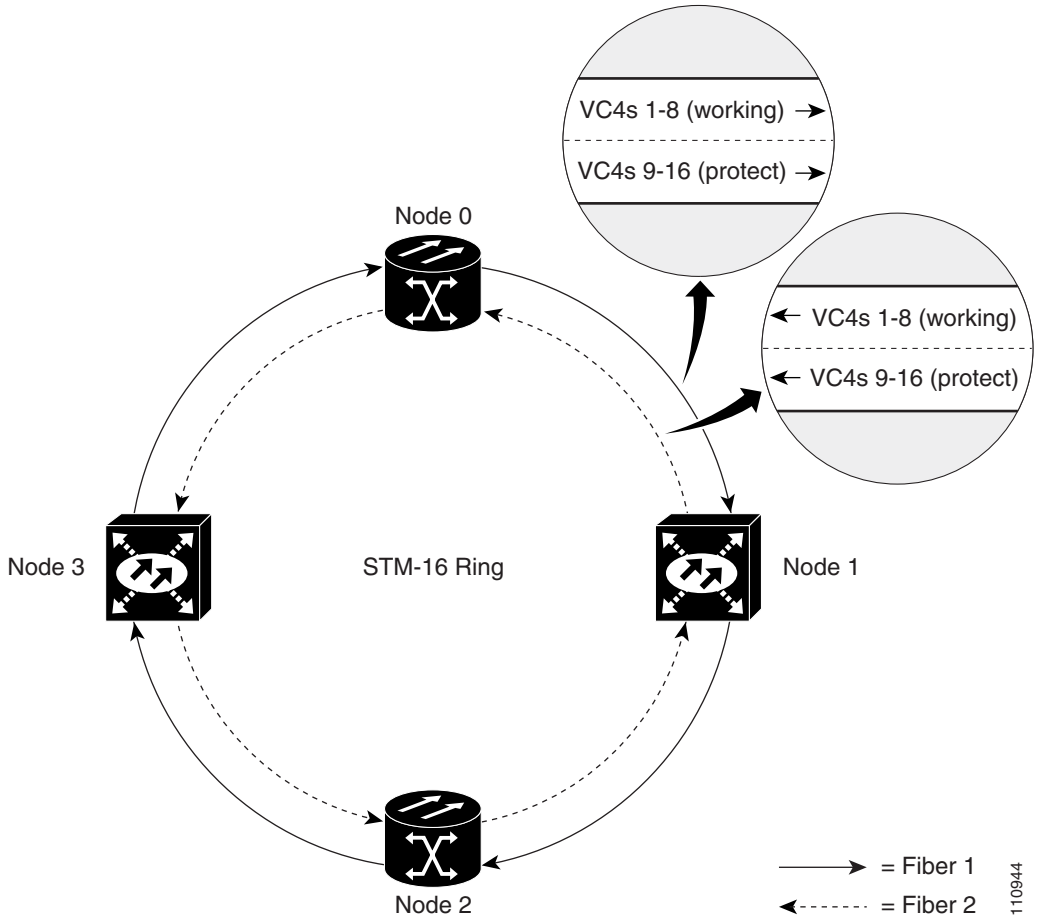
7.2 Multiplex Section-Shared Protection Rings

The ONS 15600 SDH can support 16 concurrent two-fiber multiplex section-shared protection rings (MS-SPRings). Each MS-SPRing can support up to 24 ONS 15600 SDH nodes. Because the working and protect bandwidths must be equal, you can create only STM-16 or STM-64 MS-SPRings.

Note For best performance, MS-SPRings should have one LAN connection for every ten nodes in the MS-SPRing.

In two-fiber MS-SPRings, each fiber is divided into working and protect bandwidths. For example, in an STM-16 MS-SPRing, VC4s 1 to 8 carry the working traffic, and VC4s 9 to 16 are reserved for protection (Figure 7-2). Working traffic (VC4s 1 to 8) travels in one direction on one fiber and in the opposite direction on the second fiber. CTC circuit routing routines calculate the shortest path for circuits based on many factors, including user requirements, traffic patterns, and distance. For example, in Figure 7-2, circuits going from Node 0 to Node 1 will typically travel on Fiber 1, unless that fiber is full, in which case circuits will be routed to 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 7-2 Four-Node, Two-Fiber MS-SPRing



The SDH K1, K2, and K3 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 targeted for a node beyond the break switches to the protect bandwidth on the second fiber. The traffic travels in a reverse direction on the protect bandwidth until it reaches its destination node. At that point, traffic is switched back to the working bandwidth.

Figure 7-3 shows a traffic pattern sample on a four-node, two-fiber MS-SPRing.

Figure 7-3 Four-Node, Two-Fiber MS-SPRing Traffic Pattern Sample

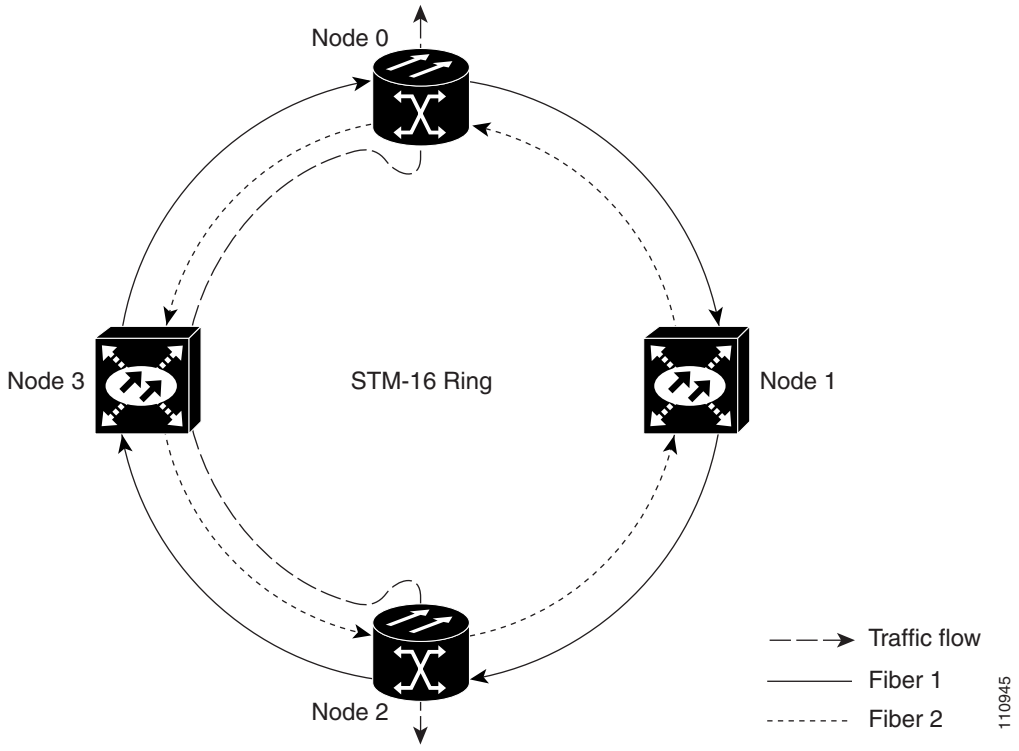
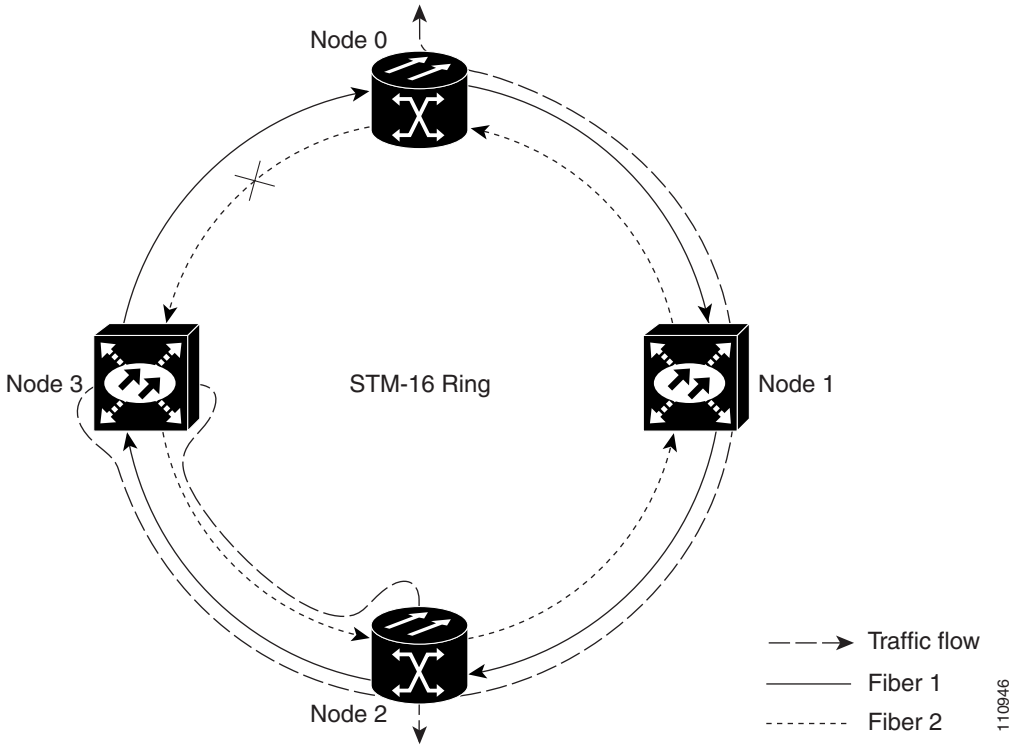


Figure 7-4 shows how traffic is rerouted following a line break between Node 0 and Node 3.

- All circuits originating on Node 0 that carried traffic to Node 2 on Fiber 2 are switched to the protect bandwidth of Fiber 1. For example, a circuit carrying traffic on VC4-1 on Fiber 2 is switched to VC4-9 on Fiber 1. A circuit carried on VC4-1 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 normally carry traffic to Node 0 on Fiber 1 switch to the protect bandwidth of Fiber 2 at Node 3. For example, a circuit carrying traffic on VC4-1 on Fiber 1 switches to VC4-10 on Fiber 2. Fiber 2 carries the circuit to Node 0 where the circuit switches back to VC4-2 on Fiber 1 and is then dropped to its destination.

Figure 7-4 Four-Node, Two-Fiber MS-SPRing Traffic Pattern Following Line Break



7.2.1 MS-SPRing Bandwidth

MS-SPRing nodes can terminate traffic coming 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.

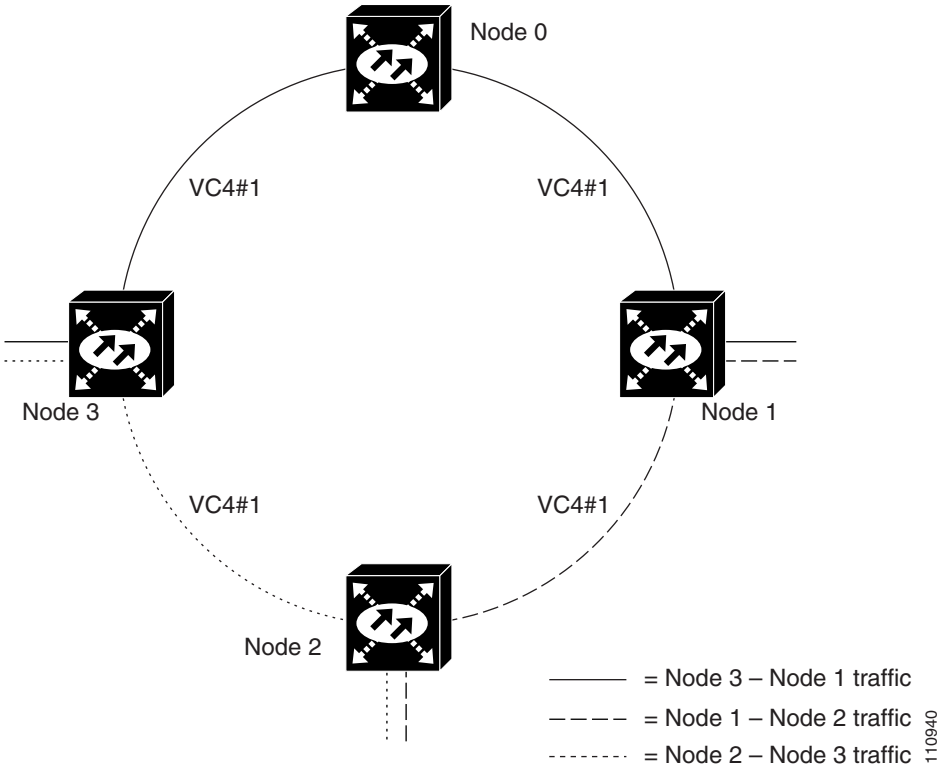
MS-SPRings allow bandwidth to be reused around the ring and can carry more traffic than a network with traffic flowing through one central hub. MS-SPRings can also carry more traffic than an SNCP operating at the same STM-N rate. Table 7-1 shows the bidirectional bandwidth capacities of two-fiber MS-SPRings. The capacity is the STM-N rate divided by two, multiplied by the number of nodes in the ring minus the number of pass-through VC4 circuits.

Table 7-1 Two-Fiber MS-SPRing Capacity

STM Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
STM-16	VC4 1-8	VC4 9-16	8 x N – PT
STM-64	VC4 1-32	VC4 33-64	32 x N – PT

Figure 7-5 shows an example of MS-SPRing bandwidth reuse. The same VC4 carries three different traffic sets simultaneously on different spans around the ring: one set from Node 3 to Node 1, another set from Node 1 to Node 2, and another set from Node 2 to Node 3.

Figure 7-5 MS-SPRing Bandwidth Reuse

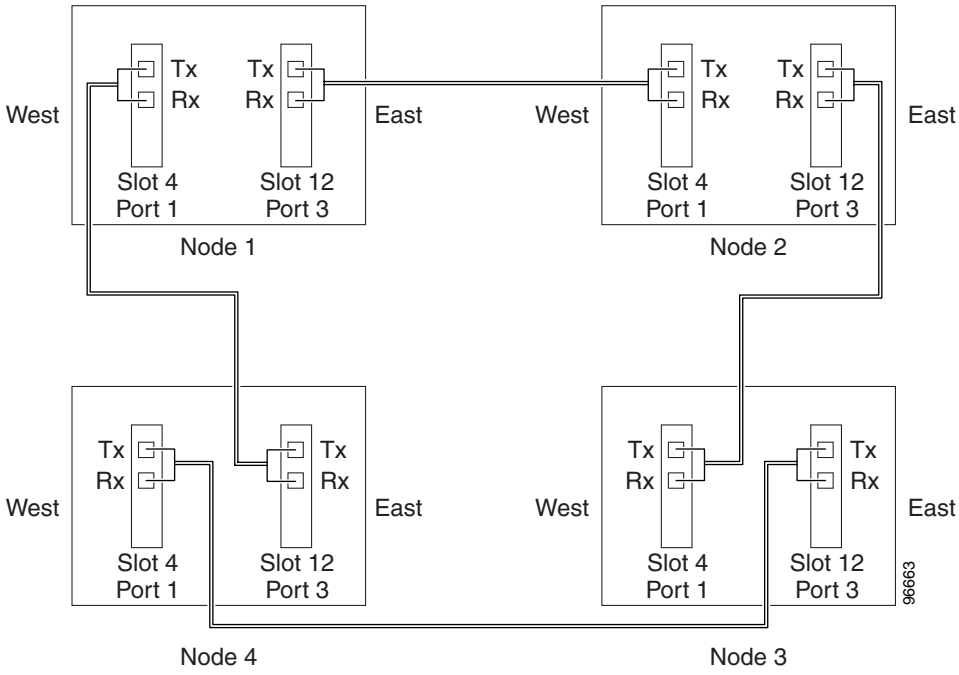


7.2.2 MS-SPRing Fiber Connections

Plan your fiber connections and use the same plan for all MS-SPRing nodes. For example, make the east port the farthest slot to the right and the west port the farthest slot to the left. Plug fiber connected to an east port at one node into the west port on an adjacent node. Figure 7-6 shows fiber connections for a two-fiber MS-SPRing with trunk (span) cards in Slot 4 (west) and Slot 12 (east). Refer to the *Cisco ONS 15600 SDH Procedure Guide* for fiber connection procedures.

Note Always plug 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. Cards display an SF LED when Tx and Rx connections are mismatched.

Figure 7-6 Connecting Fiber to a Four-Node, Two-Fiber MS-SPRing



7.3 Subnetwork Connection Protection

Subnetwork connection protection (SNCP) rings provide duplicate fiber paths around the ring. Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs in the working traffic path, the receiving node switches to the path coming from the opposite direction.

CTC automates ring configuration. SNCP traffic is defined within the ONS 15600 SDH on a circuit-by-circuit basis. If a path-protected circuit is not defined within a 1+1 LMSP or MS-SPRing line protection scheme and path protection is available and specified, CTC uses SNCP as the default. You can set up a maximum of 64 STM-16 SNCPs or 16 STM-64 SNCPs for each ONS 15600 SDH node.

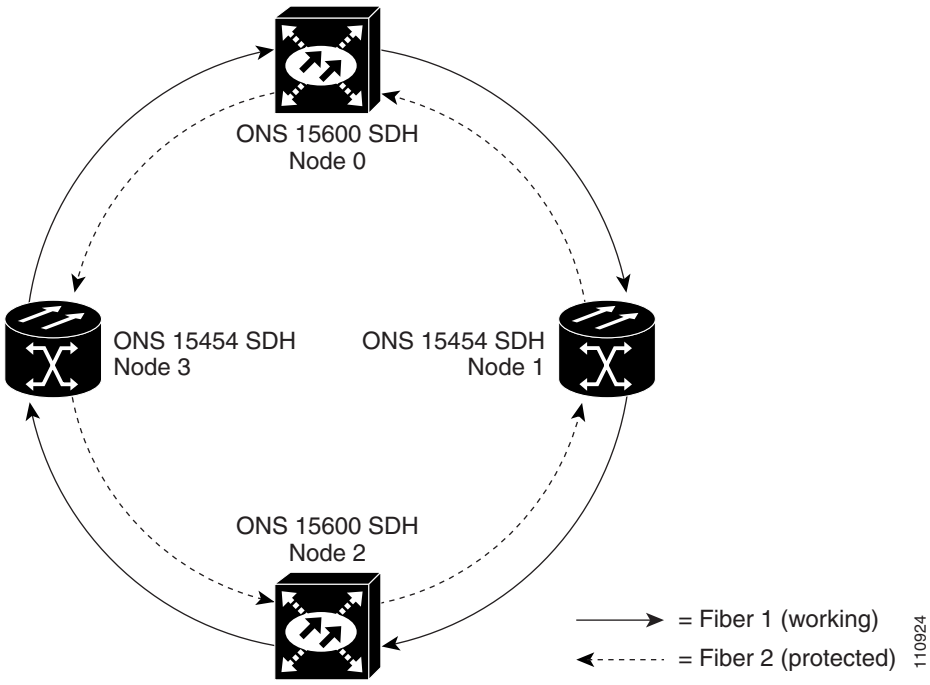
A SNCP circuit requires two data communications channel (DCC)-provisioned optical spans per node. SNCP circuits can be created across these spans until their bandwidth is consumed.

Note If a SNCP circuit is created manually by TL1, DCCs are not needed; therefore, SNCP circuits are limited by the cross-connection bandwidth, or the span bandwidth, but not by the number of DCCs.

The span bandwidth consumed by a SNCP circuit is two times the circuit bandwidth, since the circuit is duplicated. The cross-connection bandwidth consumed by a SNCP circuit is three times the circuit bandwidth at the source and destination nodes only. The cross-connection bandwidth consumed by an intermediate node has a factor of one.

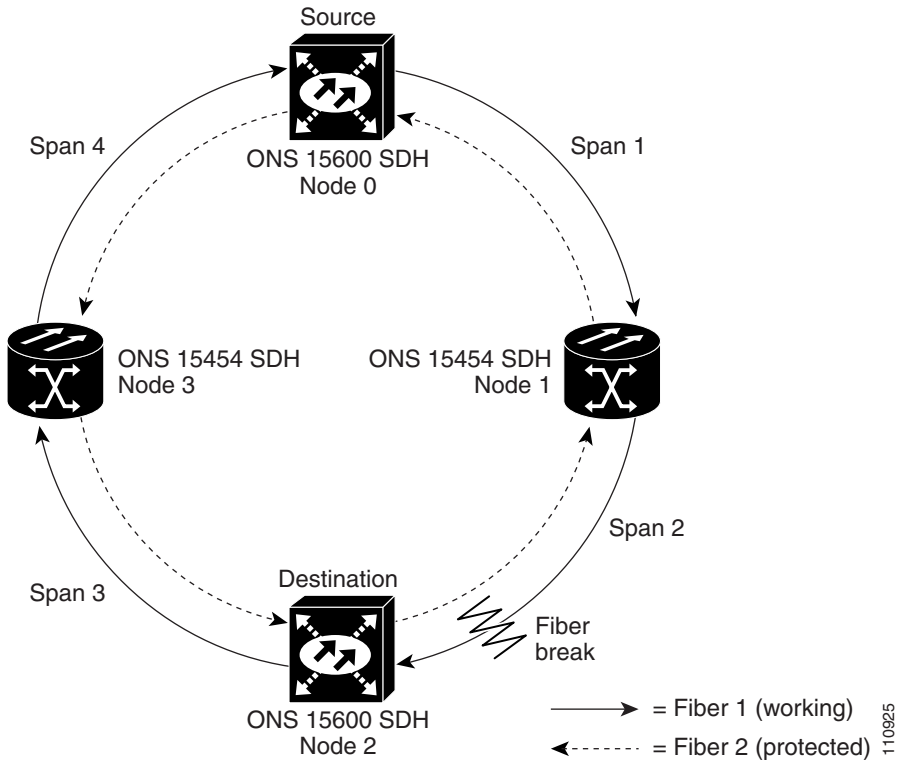
Figure 7-7 shows a basic SNCP configuration. If Node 0 sends a signal to Node 2, the working signal travels on the working traffic path through Node 1. The same signal is also sent on the protect traffic path through Node 3.

Figure 7-7 Basic Four-Node SNCP



If a fiber break occurs, Node 2 switches its active receiver to the protect signal coming through Node 3 (Figure 7-8).

Figure 7-8 SNCP with a Fiber Break



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 capacity is equal to its bit rate. Services can originate and terminate on the same SNCP, or they can be passed to an adjacent access or interoffice ring for transport to the service-terminating location.

7.4 Subtending Rings

Subtending rings reduce the number of nodes and cards required and reduce external shelf-to-shelf cabling. The ONS 15600 SDH supports ten concurrent rings. Figure 7-9 shows an ONS 15600 SDH with multiple subtending rings.

Figure 7-9 ONS 15600 SDH with Multiple Subtending Rings

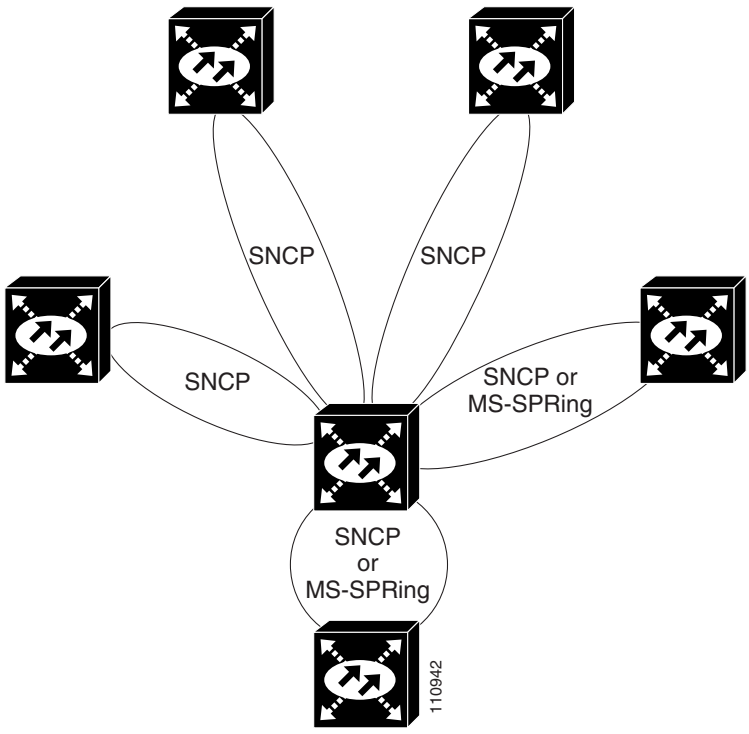
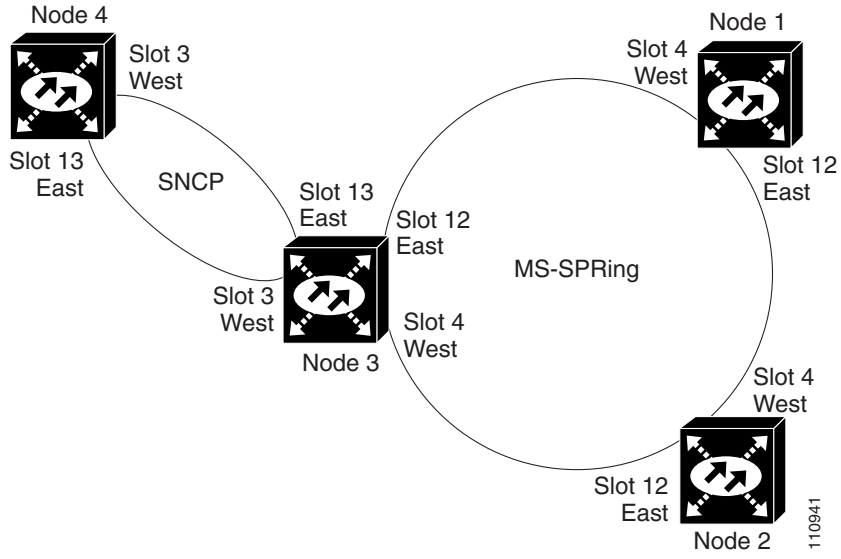


Figure 7-10 shows an SNCP subtending from an MS-SPRing. In this example, Node 3 is the only node serving both the MS-SPRing and SNCP. STM-N cards in Slots 4 and 12 serve the MS-SPRing, and STM-N cards in Slots 3 and 13 serve the SNCP.

Figure 7-10 SNCP Subtending from an MS-SPRing

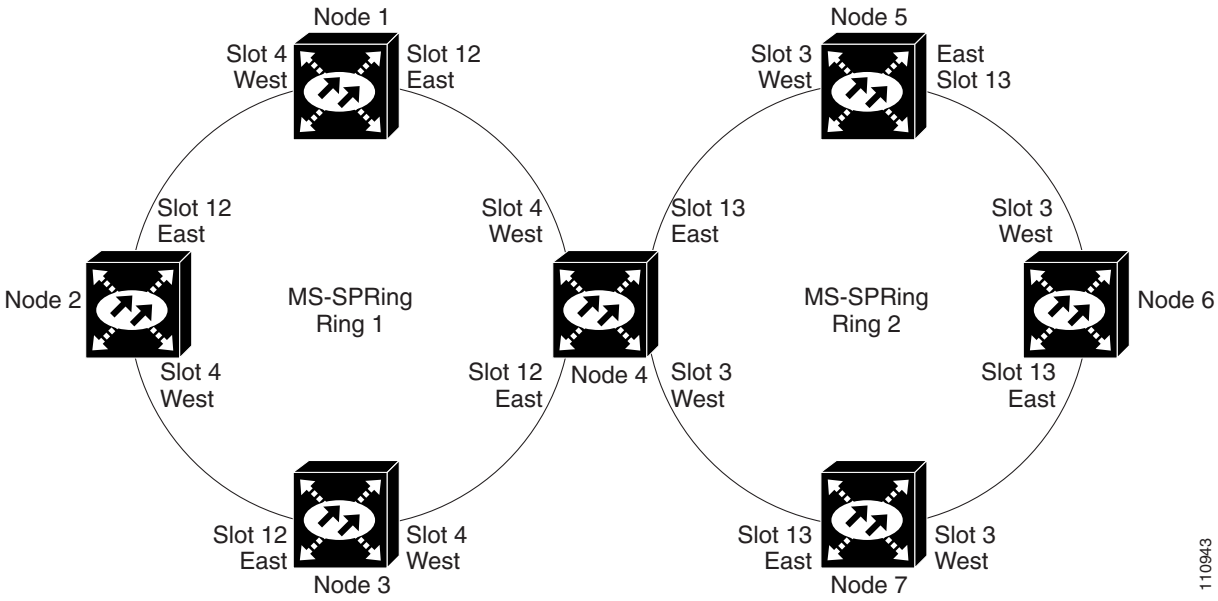


The ONS 15600 SDH can support 16 MS-SPRings on the same node. This capability allows you to deploy an ONS 15600 SDH in applications requiring SDH digital cross-connect systems (DCSs) or multiple SDH ADMs.

Figure 7-11 shows two MS-SPRings shared by one ONS 15600 SDH. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7. Two MS-SPRings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 4 and 12, and Ring 2 uses cards in Slots 3 and 13.

Note Nodes in different MS-SPRings can have the same or different node IDs.

Figure 7-11 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 7-11 you can route a circuit from Node 1 to Node 7. The circuit would normally travel from Node 1 to Node 4 to Node 7. If fiber breaks occur, for example between Nodes 1 and 4 and Nodes 4 and 7, traffic is rerouted around each ring: in this example, Nodes 2 and 3 in Ring 1 and Nodes 5 and 6 in Ring 2.

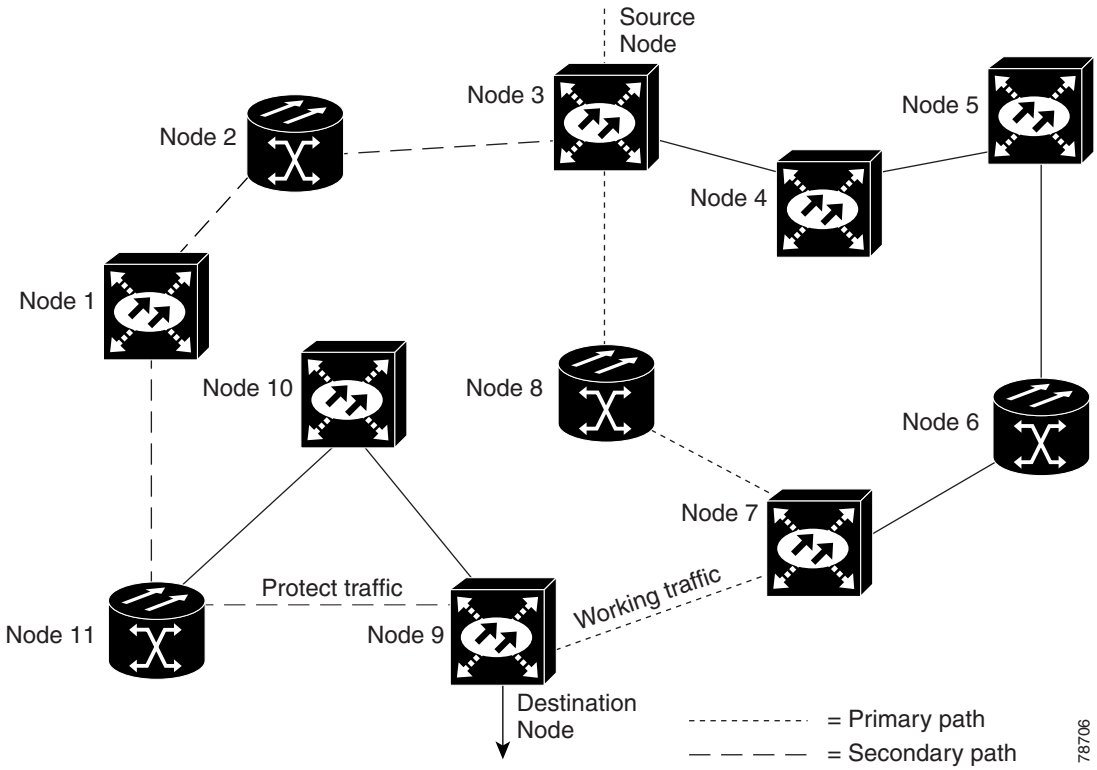
7.5 Extended SNCP Mesh Networks

In addition to single MS-SPRings, SNCPs, and ADMs, you can extend ONS 15600 SDH traffic protection by creating extended SNCP mesh networks. Extended SNCP rings include multiple ONS 15600 SDH topologies and extend the protection provided by a single SNCP to the meshed architecture of several interconnecting rings.

In an extended SNCP ring, circuits travel diverse paths through a network of single or multiple meshed rings. When you create circuits, CTC automatically routes circuits across the Extended SNCP ring, 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 7-12, a circuit is created from Node 3 to Node 9. CTC determines that the shortest route between the two nodes passes through Node 8 and Node 7, shown by the dotted line, and automatically creates cross-connections at Nodes 3, 8, 7, and 9 to provide the primary circuit path.

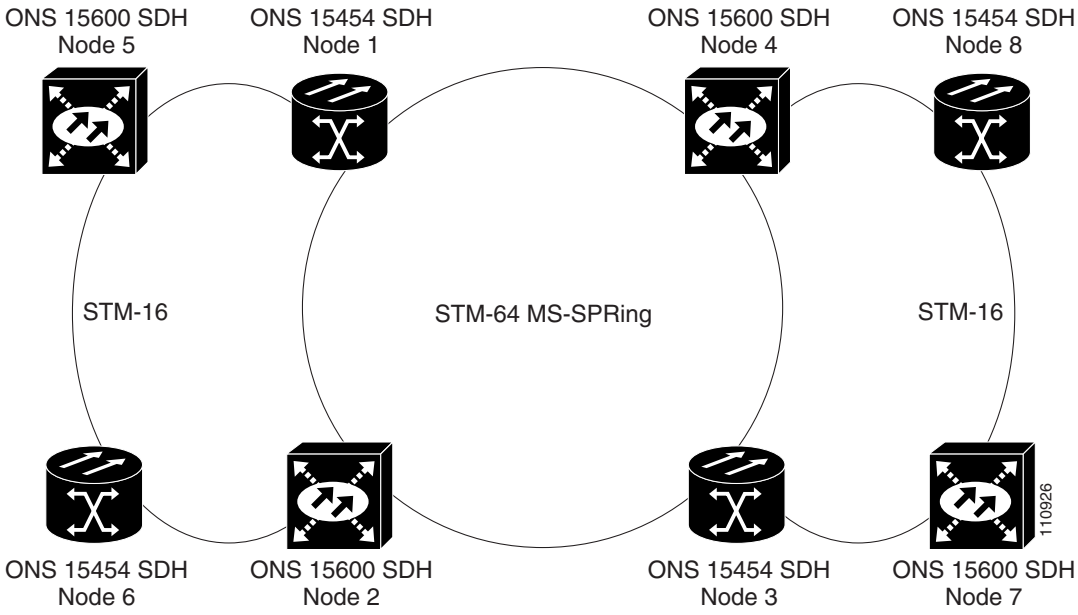
Figure 7-12 Extended SNCP Mesh Network



If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 that 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 fiber from Node 7 to the fiber from Node 11 and service resumes. The switch occurs within 50 ms.

Extended SNCP rings also allow spans of different SDH line rates to be mixed together in virtual rings. Figure 7-13 shows Nodes 1, 2, 3, and 4 in an STM-64 ring.

Figure 7-13 Extended SNCP Virtual Ring



IP Networking

This chapter provides seven scenarios showing Cisco ONS 15600 SDH nodes in common IP network configurations. The chapter does not provide a comprehensive explanation of IP networking concepts and procedures.

For IP setup instructions, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

Note To set up ONS 15600 SDH nodes within an IP network, you must work with a LAN administrator or other individual at your site who has IP networking training and experience.

8.1 IP Networking Overview

ONS 15600 SDH nodes can be connected in many different ways within an IP environment:

- You can connect ONS 15600 SDH nodes and LANs through direct connections or a router.
- IP subnetting can create ONS 15600 SDH node groups, which allow you to provision nodes in a network that are connected using the data communications channel (DCC).
- Different IP functions and protocols allow you to achieve specific network goals. For example, Proxy Address Resolution Protocol (ARP) enables one LAN-connected ONS 15600 SDH to serve as a gateway for ONS 15600 SDH nodes that are not connected to the LAN.
- You can create static routes to enable connections among multiple Cisco Transport Controller (CTC) sessions with ONS 15600 SDH nodes that reside on the same subnet but have different destination IP addresses.
- If ONS 15600 SDH nodes are connected to Open Shortest Path First (OSPF) networks, ONS 15600 SDH network information is automatically communicated across multiple LANs and WANs.

8.2 ONS 15600 SDH IP Addressing Scenarios

ONS 15600 SDH IP addressing generally has seven common scenarios or configurations. Use the scenarios as building blocks for more complex network configurations. Table 8-1 provides a general list of items to check when setting up ONS 15600 SDH nodes in IP networks.

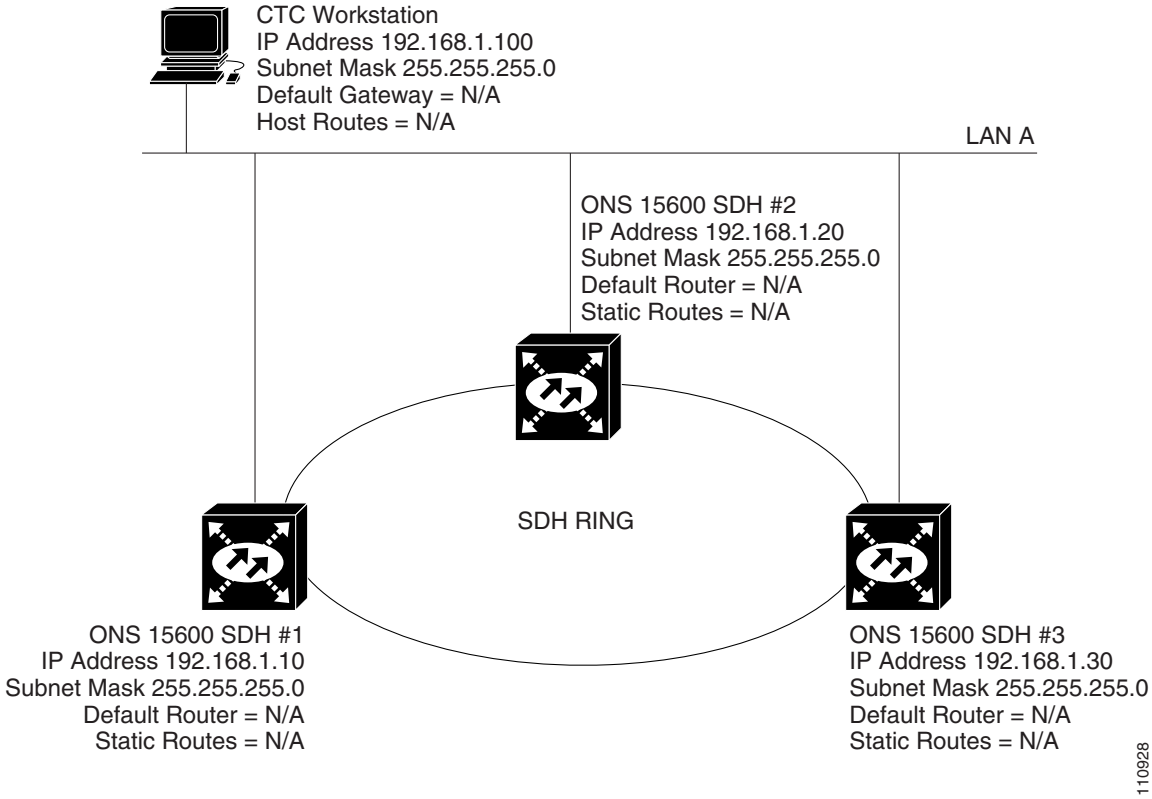
Table 8-1 General ONS 15600 SDH IP Troubleshooting Checklist

Item	What to Check
Link integrity	Verify that link integrity exists between: • CTC computer and network hub/switch • ONS 15600 SDH nodes (backplane ports or active Timing and Shelf Controller [TSC] port) and network hub/switch • Router ports and hub/switch ports
ONS 15600 SDH hub/switch ports	If connectivity problems occur, set the hub or switch port that is connected to the ONS 15600 SDH to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15600 SDH nodes.
IP addresses/subnet masks	Verify that ONS 15600 SDH IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15600 SDH optical trunk ports are in service and that DCC is enabled on each trunk port.

8.2.1 Scenario 1: CTC and ONS 15600 SDH Nodes in the Same Subnet

Scenario 1 shows a basic ONS 15600 SDH LAN configuration (Figure 8-1). The ONS 15600 SDH nodes and CTC computer reside on the same subnet. All ONS 15600 SDH nodes connect to LAN A, and all ONS 15600 SDH nodes have DCC connections.

Figure 8-1 Scenario 1: CTC and ONS 15600 SDH Nodes on Same Subnet

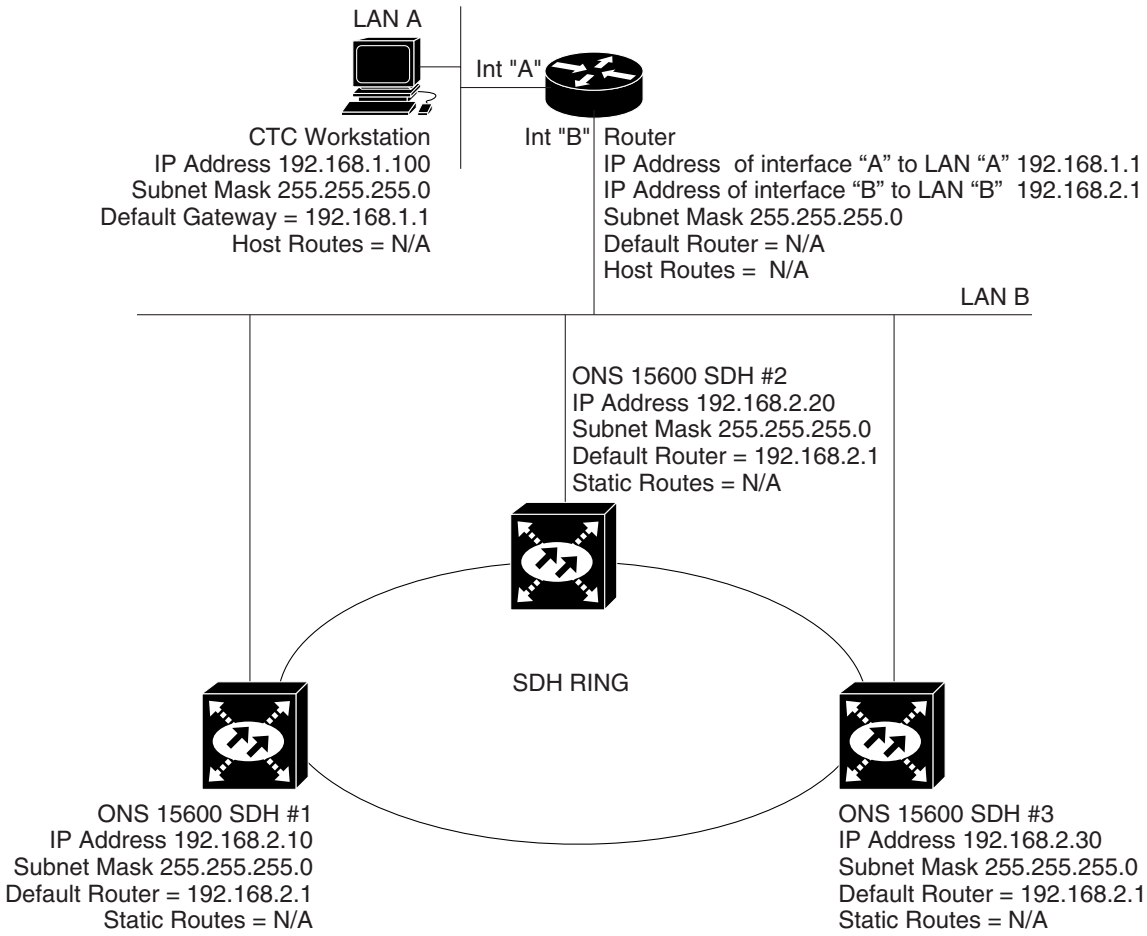


8.2.2 Scenario 2: CTC and ONS 15600 SDH Nodes Connected to Router

In Scenario 2, the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 8-2). The ONS 15600 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 Dynamic Host Configuration Protocol (DHCP), the default gateway and IP address are assigned automatically. In the Figure 8-2 example, a DHCP server is not available.

Figure 8-2 Scenario 2: CTC and ONS 15600 SDH Nodes Connected to Router

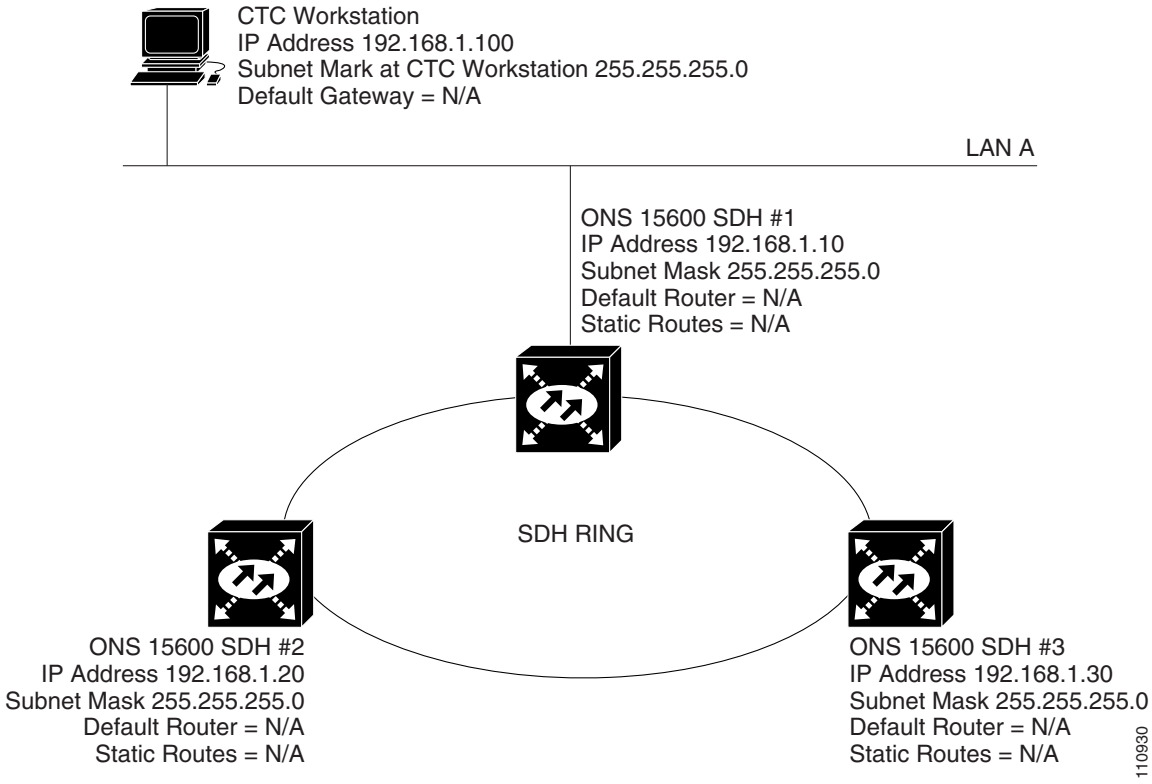


8.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15600 SDH Gateway

Scenario 3 is similar to Scenario 1, but only one ONS 15600 SDH (Node 1) connects to the LAN (Figure 8-3). Two ONS 15600 SDH nodes (Nodes 2 and 3) connect to Node 1 through the SDH DCC. Because all three ONS 15600 SDH nodes are on the same subnet, Proxy ARP enables Node 1 to serve as a gateway for Nodes 2 and 3.

Note This scenario assumes that all CTC connections are to Node 1. If you connect a laptop to either Node 2 or Node 3, network partitioning will occur; neither the laptop or the CTC computer will be able to see all nodes. If you want laptops to connect directly to end network elements (ENEs), you will need to create static routes (see the "8.2.5 Scenario 5: Using Static Routes to Connect to LANs" section on page 8-6) or enable the ONS 15600 SDH proxy server (see the "8.2.7 Scenario 7: Provisioning the ONS 15600 SDH Proxy Server" section on page 8-11).

Figure 8-3 Scenario 3: Using Proxy ARP



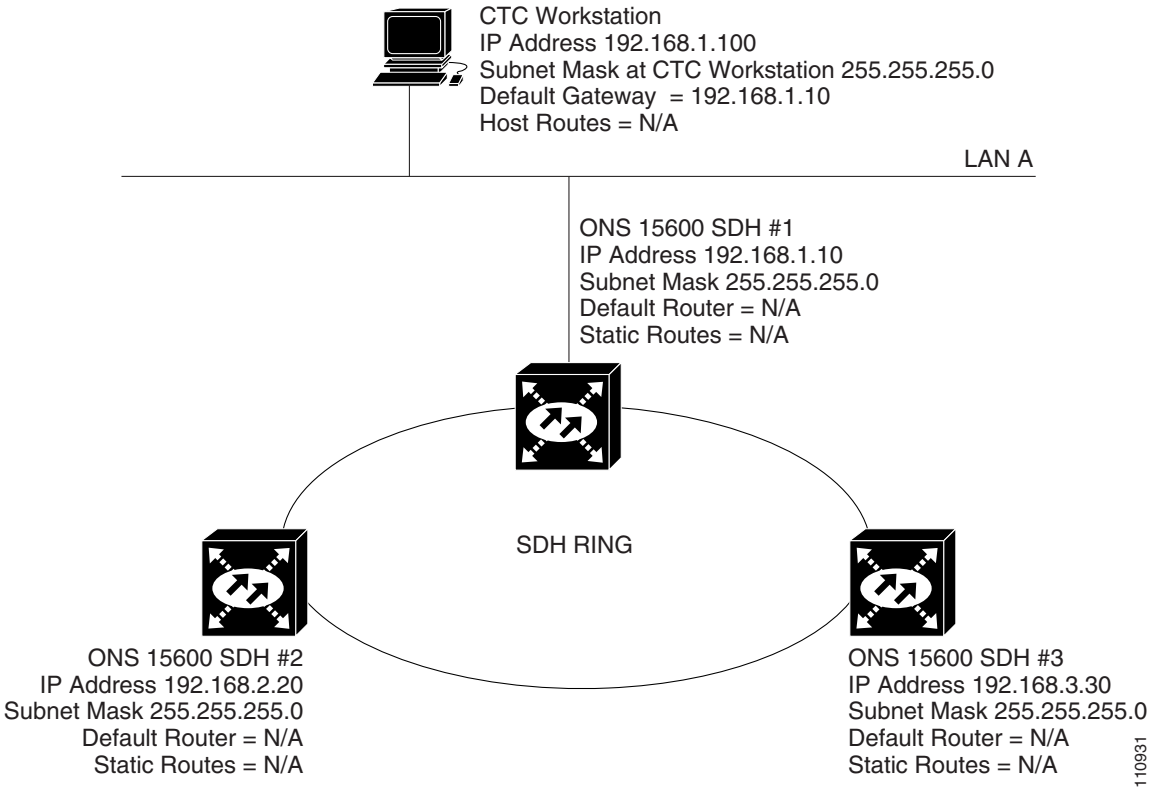
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called the ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one 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 15600 SDH to respond to the ARP request for ONS 15600 SDH nodes that are not connected to the LAN. (ONS 15600 SDH Proxy ARP requires no user configuration.) For this response to occur, the DCC-connected ONS 15600 SDH nodes must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15600 SDH that is not connected to the LAN, the gateway ONS 15600 SDH returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15600 SDH to the MAC address of the proxy ONS 15600 SDH. The proxy ONS 15600 SDH uses its routing table to forward the datagram to the non-LAN ONS 15600 SDH.

8.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but Nodes 2 and 3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 8-4). Node 1 and the CTC computer are on subnet 192.168.1.0. For the CTC computer to communicate with Nodes 2 and 3, you would enter Node 1 as the default gateway on the CTC computer.

Figure 8-4 Scenario 4: Default Gateway on a CTC Computer



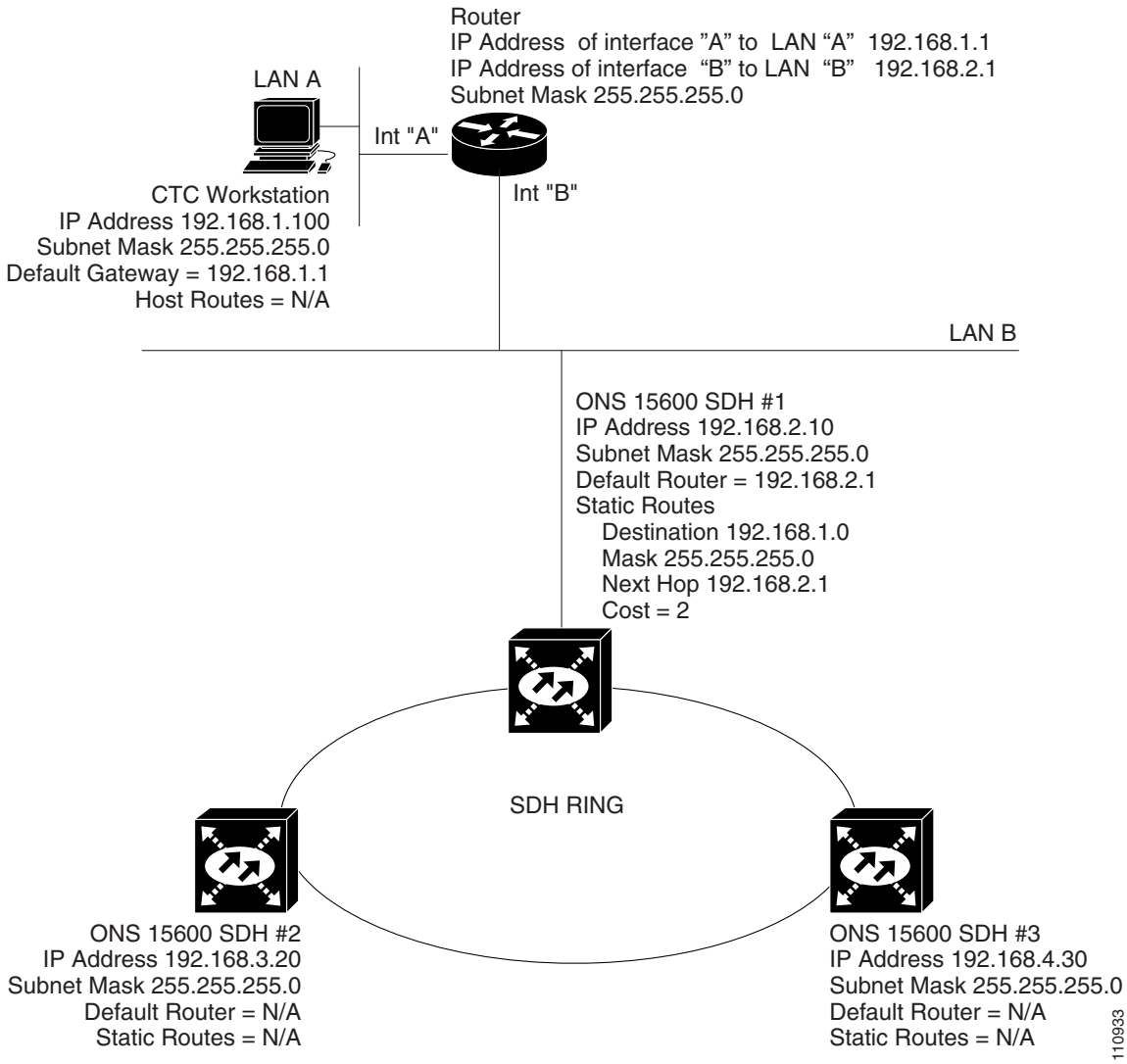
8.2.5 Scenario 5: Using Static Routes to Connect to LANs

Use static routes for the following two reasons:

- To connect ONS 15600 SDH nodes to CTC sessions on one subnet connected by a router to ONS 15600 SDH nodes residing on another subnet. (These static routes are not needed if OSPF is enabled. Scenario 6 shows an OSPF example.)
- To enable multiple CTC sessions among ONS 15600 SDH nodes residing on the same subnet.

In Figure 8-5, 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 15600 SDH nodes residing on subnet 192.168.2.0 are connected through Node 1 to the router through interface B. To connect to CTC computers on LAN A, you would create a static route on Node 1.

Figure 8-5 Scenario 5: Static Route with One CTC Computer Used as a Destination

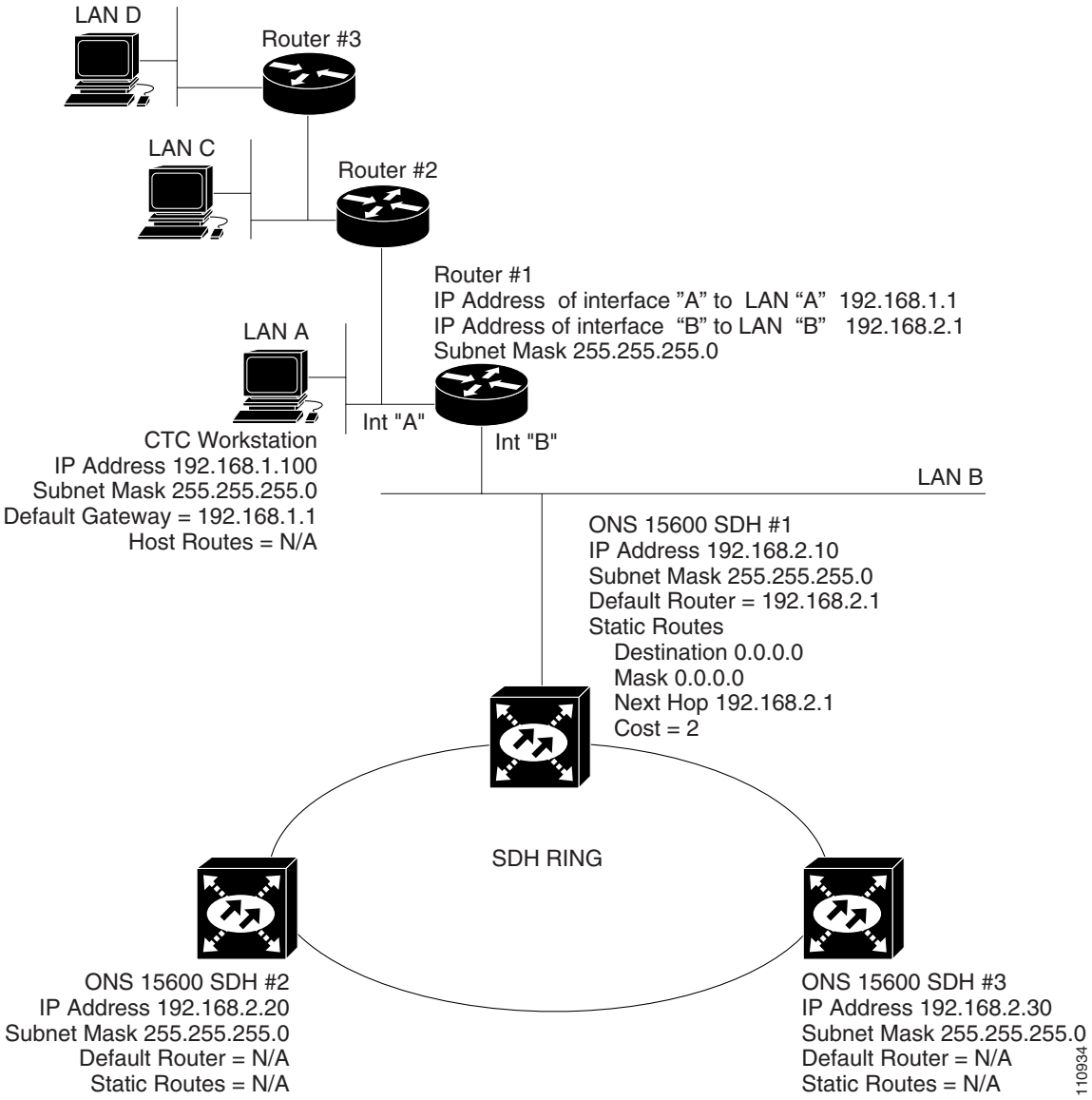


The destination and subnet mask entries control access to the ONS 15600 SDH nodes:

- If a single CTC computer will be connected to a router, enter the complete CTC host route IP address as the destination with a subnet mask of 255.255.255.255.
- If CTC computers on a subnet are connected to a 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 are connected to router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 8-6 shows an example.

The IP address of router interface B is entered as the next hop (the next router that a packet traverses to reach its destination), and the cost (number of hops from source to destination) is 2.

Figure 8-6 Scenario 5: Static Route with Multiple LAN Destinations



8.2.6 Scenario 6: Using OSPF

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 their links with their neighbors. Link state protocols advertise their directly connected networks and their active links. Each link state router captures the link state advertisements (LSAs) 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. The router continuously recalculates to capture ongoing topology changes.

ONS 15600 SDH nodes use the OSPF protocol in internal ONS 15600 SDH networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15600 SDH nodes so that the ONS 15600 SDH topology is sent to OSPF routers on a LAN. Advertising the

ONS 15600 SDH network topology to LAN routers means you do not need to manually enter static routes for ONS 15600 SDH subnetworks. Figure 8-7 shows the same network enabled for OSPF. When you are logged into an ONS 15600 SDH node, CTC does not allow both a DCC interface and a LAN interface in the same nonzero OSPF area.

Figure 8-7 Scenario 6: OSPF Enabled

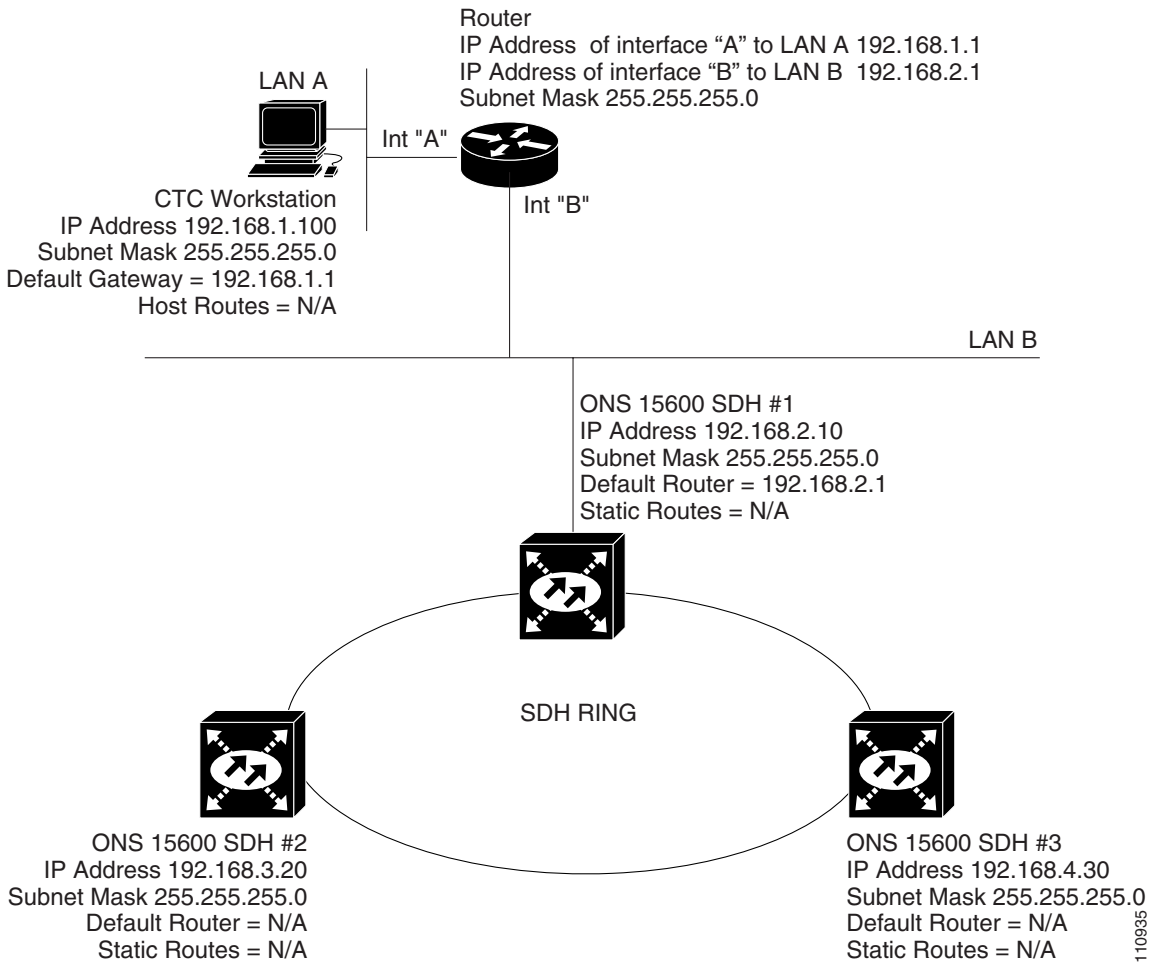
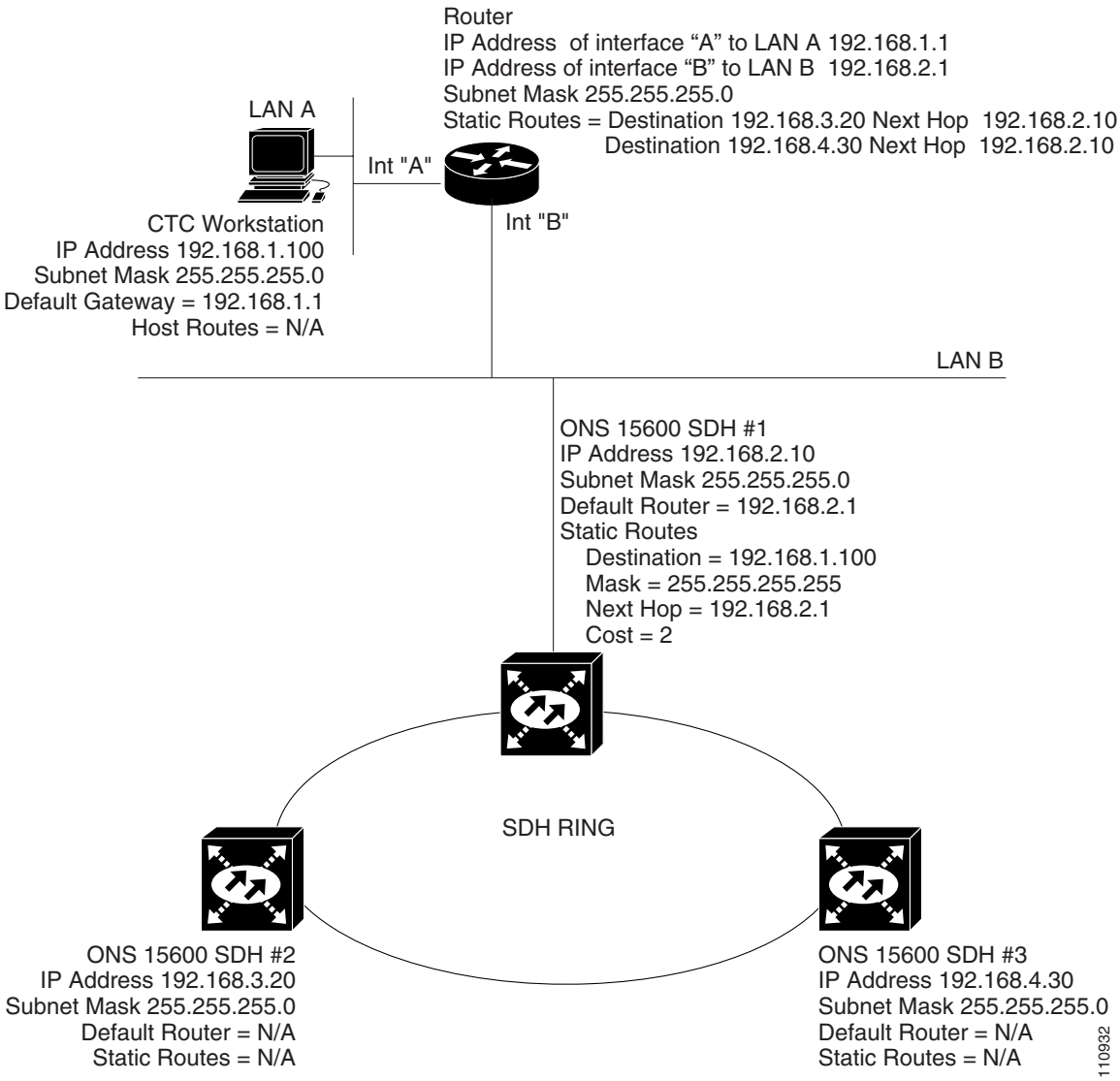


Figure 8-8 shows the same network without OSPF. Static routes must be manually added to the router in order for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

Figure 8-8 Scenario 6: OSPF Not Enabled



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 15600 SDH OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15600 SDH network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15600 SDH nodes should be assigned the same OSPF area ID.

The ONS 15600 SDH supports the multiple OSPF area feature, which allows the ability to configure and support multiple OSPF areas in each DCC-connected topology. A node is in a single OSPF area if all of its DCC or LAN interfaces are in the same OSPF area, while a node is in multiple OSPF areas if it has DCC or LAN interfaces in two or more OSPF areas. If the 15600 SDH has interfaces (DCC or LAN) in multiple OSPF areas, at least one ONS 15600 SDH interface (DCC or LAN) must be in the backbone area 0.

If multiple ONS 15600 SDH nodes and routers are connected to the same LAN in OSPF backbone area 0 and a link between two routers breaks, the backbone OSPF area 0 could divide into multiple gateway network elements (GNEs). If this occurs, the CTC session connected to Router 1 will not be able to communicate with the ONS 15600 SDH connected to Router 2. To resolve, you must repair the link between the routers or provide another form of redundancy in the network. This is standard behavior for an OSPF network.

Note To create OSPF virtual links, OSPF must be enabled on the LAN.

Note Cisco recommends limiting the number of link-state packets (LSPs) that will be forwarded over the DCC interfaces.

8.2.7 Scenario 7: Provisioning the ONS 15600 SDH Proxy Server

The ONS 15600 SDH proxy server is a set of functions that allows you to configure ONS 15600 SDH nodes in environments where visibility and accessibility between ONS 15600 SDH nodes and CTC computers must be restricted. For example, you can set up a network so that field technicians and network operating center (NOC) personnel can both access the same ONS 15600 SDH nodes while preventing the field technicians from accessing the NOC LAN. To do this, one ONS 15600 SDH is provisioned as a GNE and the other ONS 15600 SDH nodes are provisioned as ENEs. The GNE ONS 15600 SDH tunnels connections between CTC computers and ENE ONS 15600 SDH nodes, providing management capability while preventing access for non-ONS 15600 SDH management purposes.

The ONS 15600 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 8-3 on page 8-15 and Table 8-4 on page 8-16) depend on whether the packet arrives at the ONS 15600 SDH DCC or TSC 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 15600 SDH creates an entry in its ARP table. The ARP entry allows the ONS 15600 SDH to reply to an address over the local Ethernet so craft technicians can connect to ONS 15600 SDH nodes without changing the IP addresses of their computers.
- Processes Simple Network Time Protocol/Network Time Protocol (SNTP/NTP) requests. Element ONS 15600 SDH NEs can derive time-of-day from an SNTP/NTP LAN server through the GNE ONS 15600 SDH.
- Process SNMPv1 traps. The GNE ONS 15600 SDH receives SNMPv1 traps from the ENE ONS 15600 SDH nodes and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15600 SDH proxy server is provisioned using three check boxes on the Provisioning > Network > General tab (see Figure 8-9):

- Enable Proxy—When enabled, the ONS 15600 SDH serves as a proxy for connections between CTC clients and ONS 15600 SDH nodes that are DCC-connected to the proxy ONS 15600 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 proxy for any CTC clients, although any established proxy connections continue until the CTC client exits.

Note If you launch CTC on a node through a network address translation (NAT) or port address translation (PAT) router and that node does not have proxy enabled, your CTC session will start as expected; however, CTC will never receive alarm updates and will disconnect and reconnect every two minutes. If the proxy is accidentally disabled, you can still enable the proxy during a reconnect cycle and recover your ability to manage the node, even through a NAT/PAT firewall.

- Craft Access Only—When this option is enabled, the ONS 15600 SDH does not install or advertise default or static routes. CTC computers can communicate with the ONS 15600 SDH using the TSC craft port, but they cannot communicate directly with any other DCC-connected ONS 15600 SDH.
- Enable Firewall—When this option is enabled, the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15600 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 8-9 Proxy Server Gateway Settings

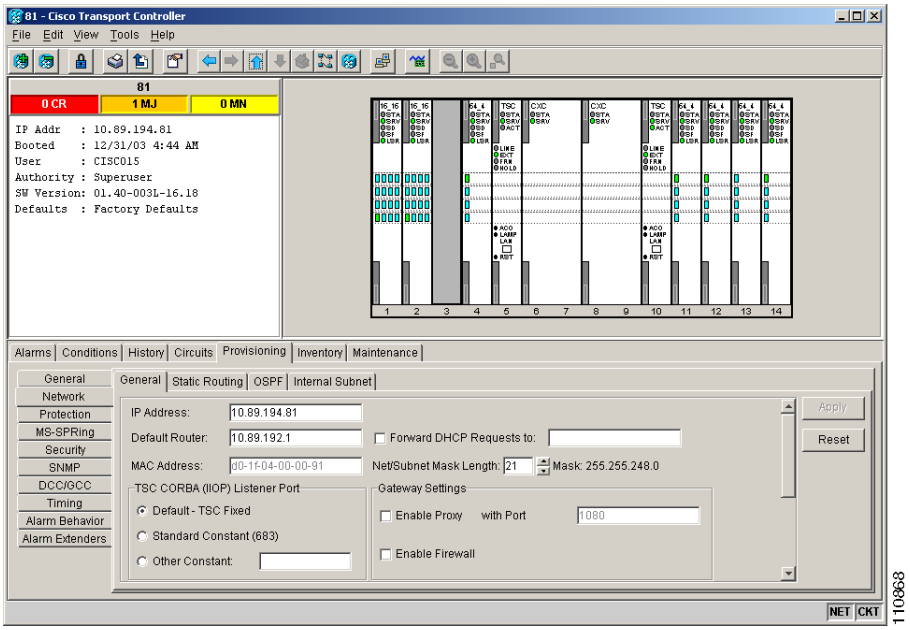


Figure 8-10 shows an ONS 15600 SDH proxy server implementation. A GNE ONS 15600 is connected to a central office LAN and to ENE ONS 15600 SDH nodes. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ONS 15600 SDH ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

In the example, the ONS 15600 SDH GNE is assigned an IP address within the central office LAN and is physically connected to the LAN through its LAN port. ONS 15600 SDH ENEs are assigned IP addresses that are outside the central office LAN and given private network IP addresses. If the ONS 15600 SDH ENEs are colocated, the craft LAN ports could be connected to a hub. However, the hub should have no other network connections.

Figure 8-10 Scenario 7: ONS 15600 SDH Proxy Server with GNE and ENEs on the Same Subnet

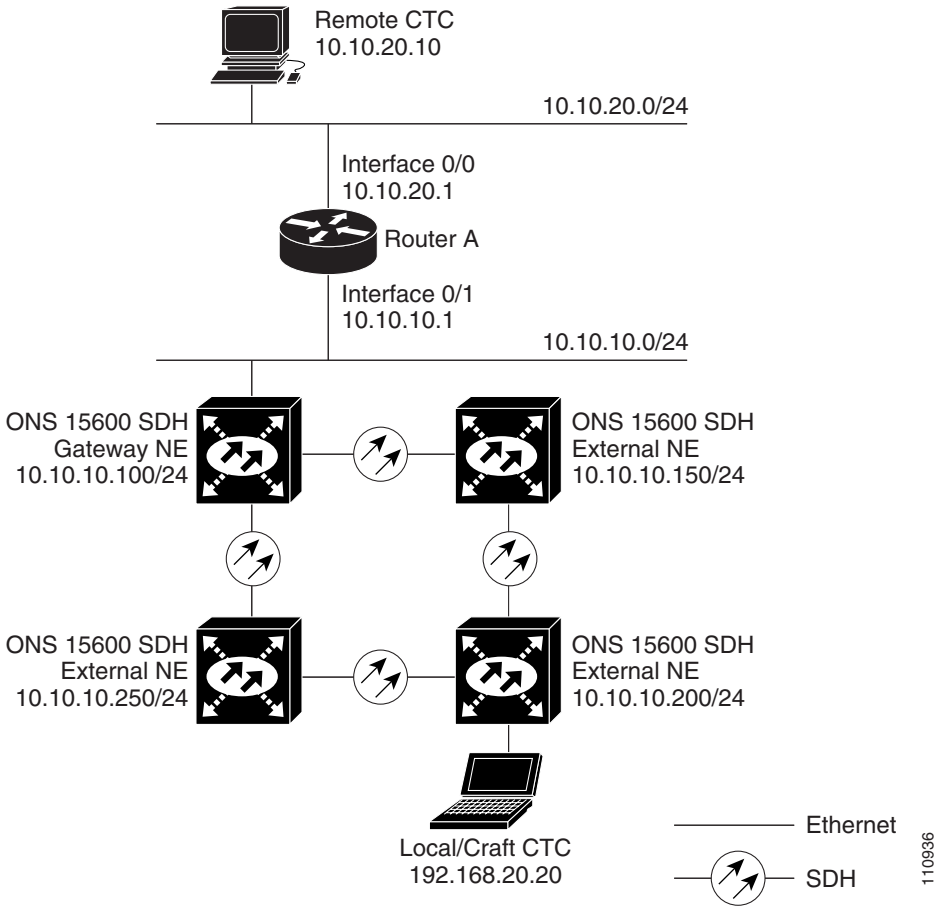


Table 8-2 shows recommended settings for ONS 15600 SDH GNEs and ENEs in the configuration shown in Figure 8-10.

Table 8-2 ONS 15600 SDH Gateway and Element NE Settings

Setting	ONS 15600 SDH Gateway NE	ONS 15600 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	Set to the ONS 15600 SDH GNE IP address.
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15600 GNE, port 391.

Figure 8-11 shows the same proxy server implementation with ONS 15600 SDH ENEs on different subnets. The ONS 15600 SDH GNEs and ENEs are provisioned with the settings shown in Table 8-2.

Figure 8-11 Scenario 7: ONS 15600 SDH Proxy Server with GNE and ENEs on Different Subnets

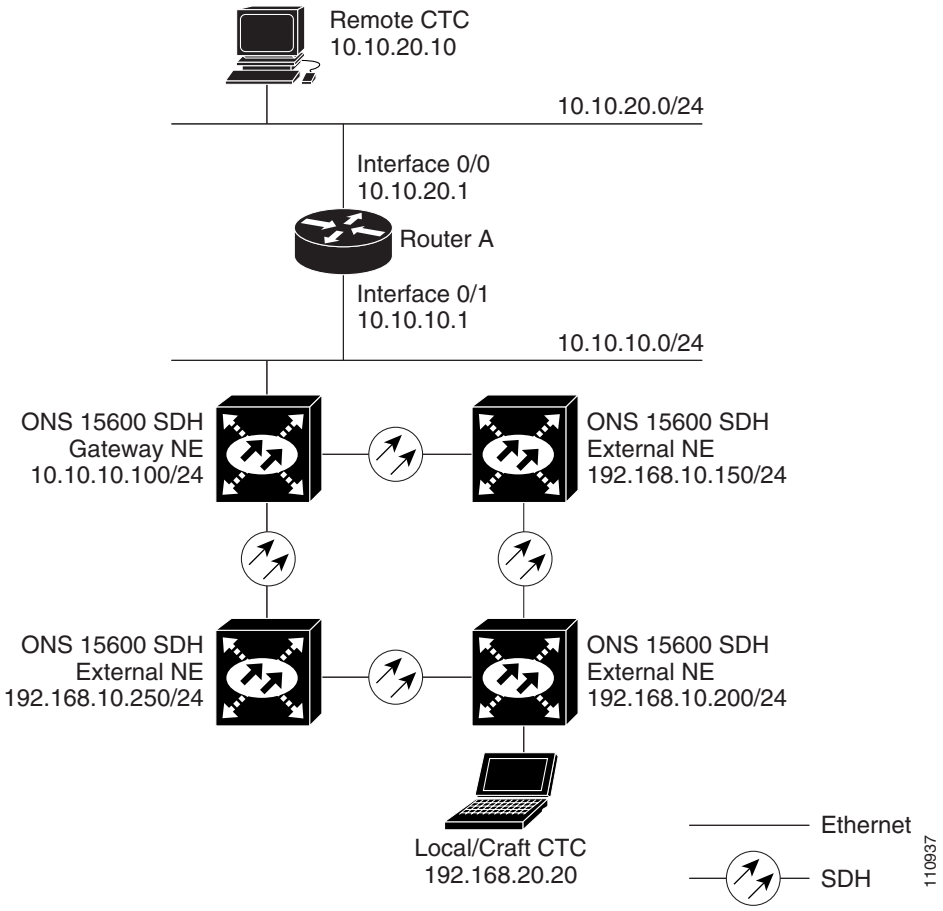
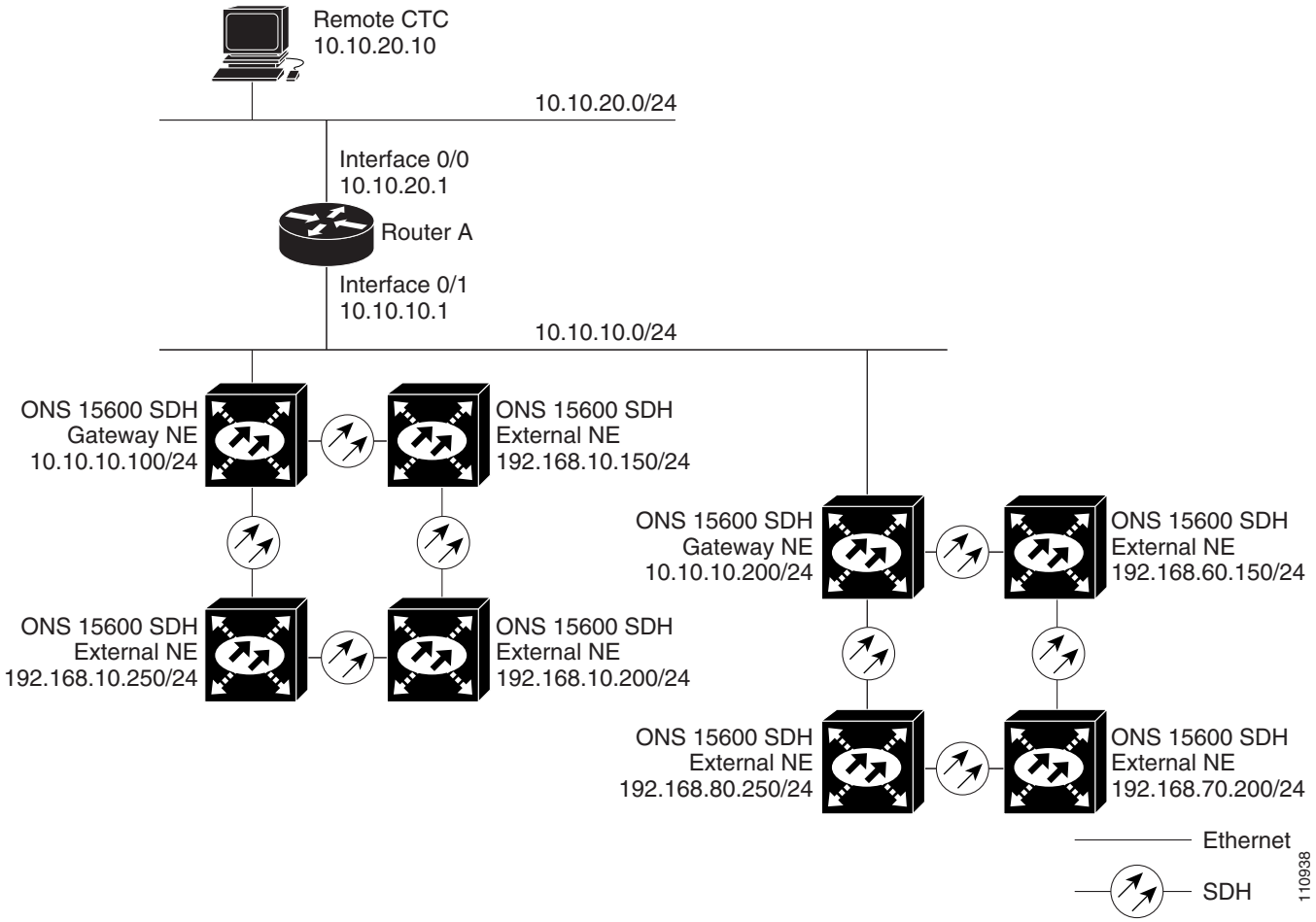


Figure 8-12 shows the Figure 8-11 implementation with ONS 15600 SDH ENEs in multiple rings. The ONS 15600 GNEs and ENEs are provisioned with the settings shown in Table 8-2.

Figure 8-12 Scenario 7: ONS 15600 SDH Proxy Server With ENEs on Multiple Rings



8.2.7.1 Firewall Enabled

Table 8-3 shows the rules the ONS 15600 SDH users to filter packets when the firewall is enabled.

Table 8-3 Proxy Server Firewall Filtering Rules

Packets Arriving At:	Are Accepted if the IP Destination Address Is:
TSC Ethernet Interface	• The ONS 15600 SDH itself • The ONS 15600 SDH's subnet broadcast address • Within the 224.0.0.0/8 network (reserved network used for standard multicast messages) • Subnet mask = 255.255.255.255
DCC Interface	• The ONS 15600 SDH itself • Any destination connected through another DCC interface • Within the 224.0.0.0/8 network

The rules in Table 8-4 are applied if a packet is addressed to the ONS 15600 SDH. Rejected packets are discarded.

Table 8-4 Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15600 SDH

Packets Arrive At:	Accepted	Rejected
TSC Ethernet Interface	• All user datagram protocol (UDP) packets except those in the Rejected column	• UDP packets addressed to the SNMP trap relay port (391)
DCC Interface	• All UDP packets • All TCP packets except those in the Rejected column • OSPF packets • Internet control message protocol (ICMP) packets	• TCP packets addressed to the Telnet port • TCP packets addressed to the proxy server port • All packets other than UDP, TCP, OSPF, and ICMP

If an ONS 15600 SDH or CTC computer resides behind a firewall that uses port filtering, you must enable an Internet Inter-ORB Protocol (IIOP) port on the ONS 15600 SDH and/or CTC computer, depending on whether one or both devices reside behind a firewall. You can enable an IIOP port on the Provisioning > Network > General tabs in CTC.

Figure 8-13 shows ONS 15600 SDH nodes in a protected network and the CTC computer in an external network. For the computer to access the ONS 15600 SDH nodes, you must provision the IIOP listener port specified by your firewall administrator on the ONS 15600 SDH. The ONS 15600 SDH sends the port number to the CTC computer during the initial contact between the devices using HTTP. After the CTC computer obtains the ONS 15600 SDH IIOP port, the computer opens a direct session with the node using the specified IIOP port.

Figure 8-13 Nodes Behind a Firewall

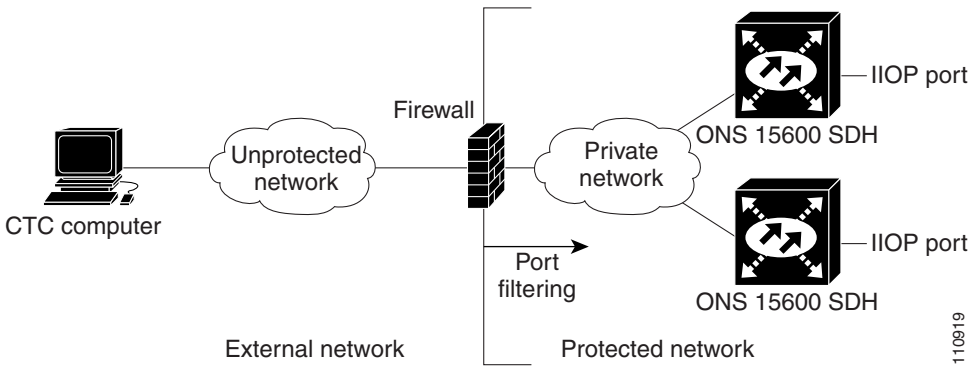
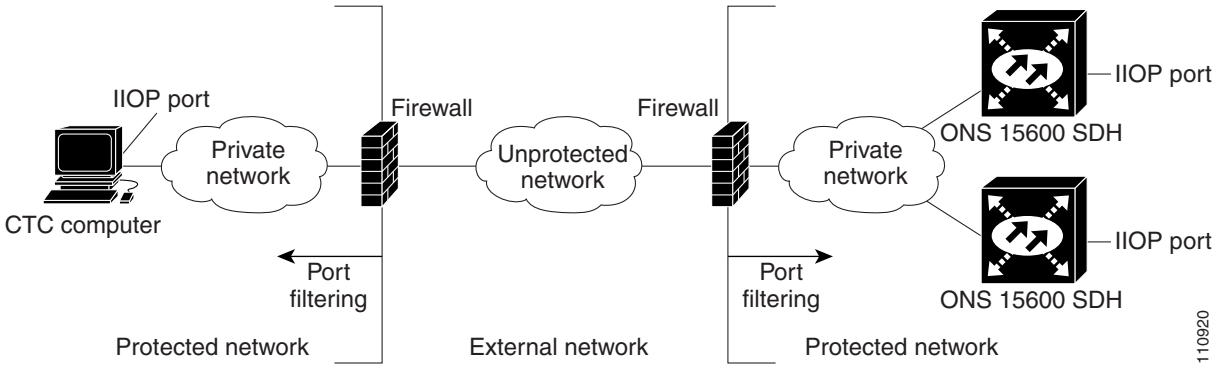


Figure 8-14 shows a CTC computer and ONS 15600 SDH nodes behind firewalls. For the computer to access the ONS 15600 SDH, you must provision the IIOP port on the CTC computer and on the ONS 15600 SDH. Each firewall can use a different IIOP port. For example, if the CTC computer firewall uses IIOP port 4000 and the ONS 15600 SDH firewall uses IIOP port 5000, provision IIOP port 4000 for the CTC computer and provision IIOP port 5000 for the ONS 15600 SDH.

Figure 8-14 CTC Computer and ONS 15600 SDH Nodes Residing Behind Firewalls



8.2.7.2 Proxy Server Implementation Guidelines

If you implement the proxy server, keep the following cases in mind:

1. All DCC-connected ONS 15600 SDH nodes on the same Ethernet segment must have the same Craft Access Only setting in CTC. Mixed values will produce unpredictable results, and might leave some nodes unreachable through the shared Ethernet segment.
2. All DCC-connected ONS 15600 SDH nodes on the same Ethernet segment must have the same Enable Firewall setting in CTC. Mixed values will produce unpredictable results. Some nodes might become unreachable.
3. If you select Enable Firewall in CTC, always select Enable Proxy. If Enable Proxy is not selected, CTC will not be able to see nodes on the DCC side of the ONS 15600 SDH.
4. If Craft Access Only is enabled, select Enable Proxy. If Enable Proxy is not selected, CTC is not able to see nodes on the DCC side of the ONS 15600 SDH.

If nodes become unreachable in cases 1, 2, and 3, correct the setting by performing one of the following:

- Disconnect the craft computer from the unreachable ONS 15600 SDH. Connect to the ONS 15600 SDH through another network ONS 15600 SDH that has a DCC connection to the unreachable ONS 15600 SDH.
- Disconnect the Ethernet cable from the unreachable ONS 15600 SDH. Connect a CTC computer directly to the ONS 15600 SDH.

8.3 Routing Table

ONS 15600 SDH routing information appears on the Maintenance > Routing Table tabs (Figure 8-15). 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 15600 SDH interface used to access the destination.
  - cpm0—The Ethernet management interface.

- pdcc—A section data communications channel (SDCC) interface, that is, an STM-N trunk (span) card identified as the SDCC termination (0 to 128).
- lo0—A loopback interface.
- pend0—The RJ-45 jack on the TSC.
- motfcc0—Interface on the TSC that connect the TSC to all other cards except the other TSC.
- hdlc0—Connects the two TSC cards together; traffic cards forward DCC packets over the motfcc0 Ethernet interface.

Figure 8-15 Viewing the ONS 15600 SDH Routing Table

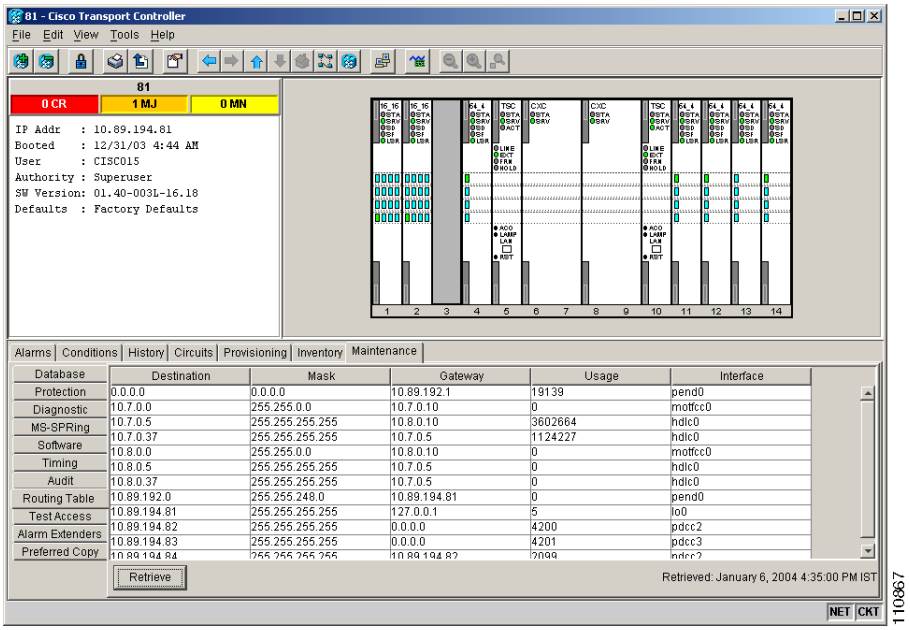


Table 8-5 shows sample routing entries for an ONS 15600 SDH.

Table 8-5 Sample Routing Table Entries

Entry	Destination	Mask	Gateway	Interface
1	0.0.0.0	0.0.0.0	172.20.214.1	cpm0
2	172.20.214.0	255.255.255.0	172.20.214.92	cpm0
3	172.20.214.92	255.255.255.255	127.0.0.1	lo0
4	172.20.214.93	255.255.255.255	0.0.0.0	pdcc0
5	172.20.214.94	255.255.255.255	172.20.214.93	pdcc0

Entry 1 shows the following:

- Destination (0.0.0.0) is the default route entry. All undefined destination network or host entries on this routing table will be mapped to the default route entry.
- Mask (0.0.0.0) is always 0 for the default route.
- Gateway (172.20.214.1) is the default gateway address. All outbound traffic that cannot be found in this routing table or is not on the node's local subnet will be sent to this gateway.

- Interface (cpm0) indicates that the ONS 15600 SDH Ethernet management interface is used to reach the gateway.

Entry 2 shows the following:

- Destination (172.20.214.0) is the destination network IP address.
- Mask (255.255.255.0) is a 24-bit mask, meaning all addresses within the 172.20.214.0 subnet can be destinations.
- 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 15600 SDH Ethernet management interface is used to reach the gateway.

Entry 3 shows the following:

- Destination (172.20.214.92) is the destination host IP address.
- Mask (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.92 address is a destination.
- Gateway (127.0.0.1) is a loopback address. The host directs network traffic to itself using this address.
- Interface (lo0) indicates that the local loopback interface is used to reach the gateway.

Entry 4 shows the following:

- Destination (172.20.214.93) is the destination host IP address.
- Mask (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.93 address is a destination.
- Gateway (0.0.0.0) means the destination host is directly attached to the node.
- Interface (pdcc0) indicates that a 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 the IP address 172.20.214.93.
- Interface (pdcc0) indicates that a SDH SDCC interface is used to reach the gateway.

Performance Monitoring

Use performance monitoring (PM) parameters to gather, store, threshold, and report performance data for early detection of problems. This chapter defines PM parameters and concepts for Cisco ONS 15600 SDH optical cards.

You can find additional PM information Telcordia GR-1230-CORE, GR-820-CORE, and GR-253 CORE, in ITU-T G.826, G.827, G.828, G.829, M2101, and M2102, and in the ANSI document titled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

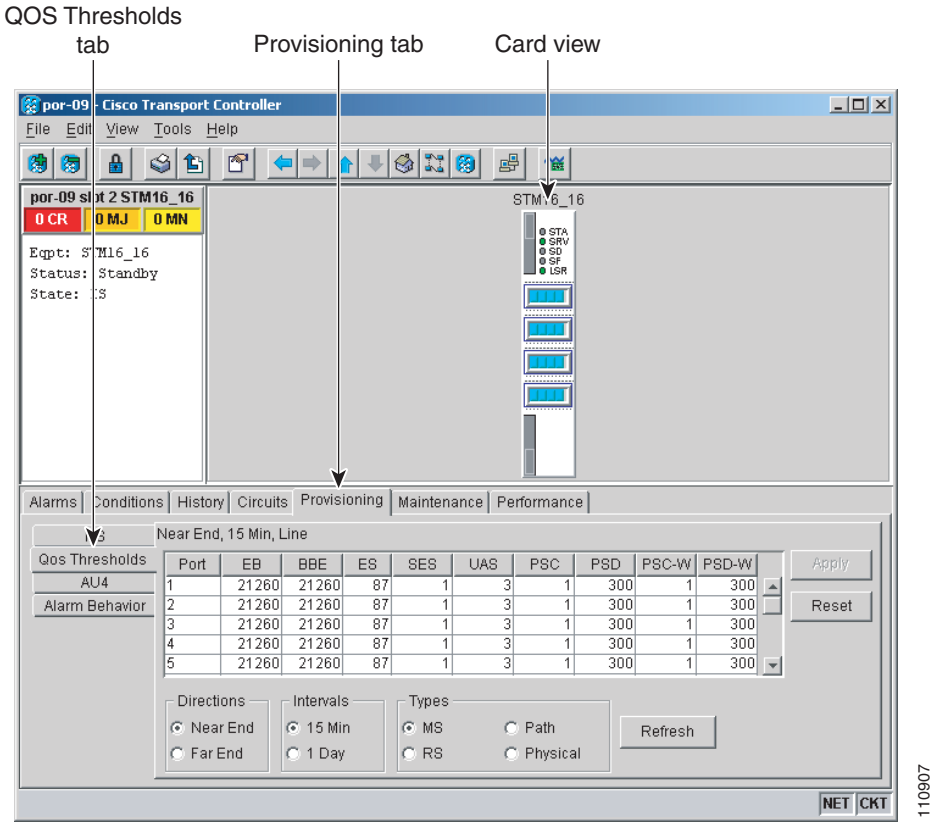
Chapter topics include:

9.1 Threshold Performance Monitoring

Thresholds are used to set error levels for each PM. You can program PM threshold ranges from the Provisioning > QoS Thresholds tabs on the Cisco Transport Controller (CTC) card view. To provision card thresholds, such as Regenerator Section, Multiplex Section, and High Order Path thresholds, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and sent to CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the performance monitoring parameter is disabled. Figure 9-1 shows the Provisioning > QoS Thresholds tabs for an OC-48/STM-16 card.

Figure 9-1 QoS Thresholds Tab for Setting Threshold Values



Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical VC4 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

9.2 Intermediate-Path Performance Monitoring

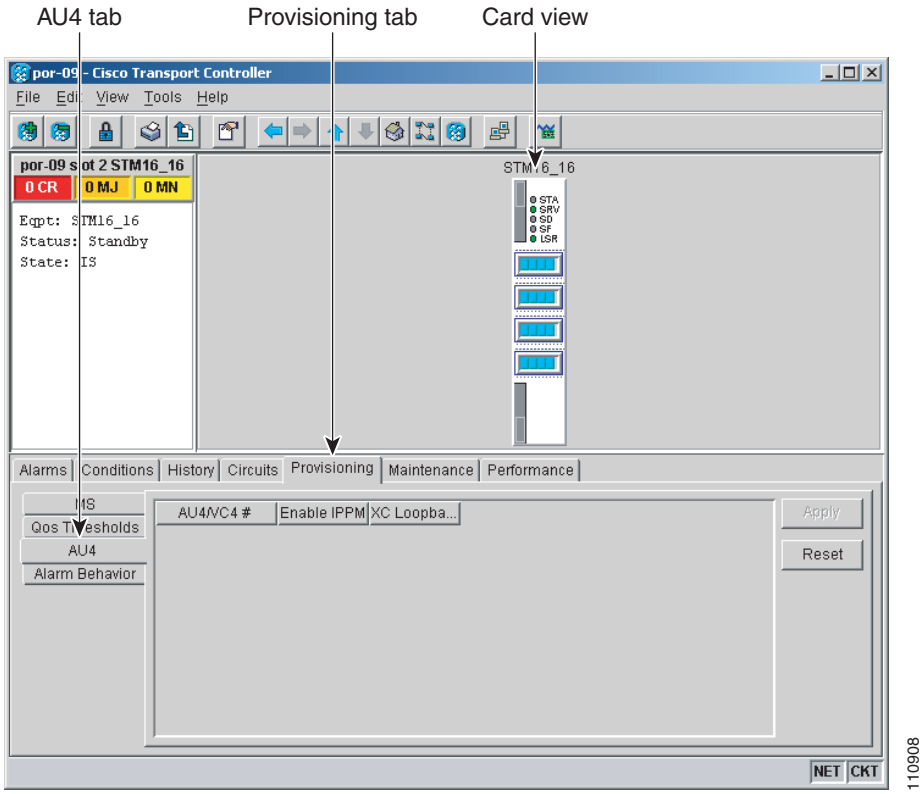
Intermediate-path performance monitoring (IPPM) allows a nonterminating node to transparently monitor a constituent channel of an incoming transmission signal. ONS 15600 SDH networks only use line terminating equipment (LTE), not path terminating equipment (PTE). Table 9-1 shows ONS 15600 SDH cards that are considered LTE.

Table 9-1 Line Terminating Traffic Cards

Line Terminating Equipment
OC48/STM16 SR/SH 16 Port 1310
OC48/STM16 LR/LH 16 Port 1550
OC192/STM64 SR/SH 4 Port 1310
OC192/STM64 LR/LH 4 Port 1550

Figure 9-2 shows the Provisioning > AU4 tabs for an STM-16 card.

Figure 9-2 AU4 Tab for Enabling IPPM



Software Release 1.0 and later allows LTE cards to monitor near-end path PM data on individual VC4 payloads by enabling IPPM. After enabling IPPM on provisioned VC4 ports, service providers can monitor large amounts of VC4 traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on VC4 paths that have IPPM enabled, and TCAs are raised only for PM parameters on the selected IPPM paths. The monitored IPPMs are VC4 HP-EB, VC4 HP-ES, VC4 HP-SES, VC4 HP-UAS, and VC4 HP-BBE. The following ratio parameters are provided: VC4 HP-BBER, VC4 HP-ESR, and VC4 HP-SESR. To enable IPPM, refer to the *Cisco ONS 15600 Procedure Guide*.

The ONS 15600 SDH performs IPPM by examining the overhead in the monitored path and reading all of the near-end path performance monitoring parameters in the incoming transmission direction. The IPPM process allows the path overhead to pass bidirectionally through the node completely unaltered.

For detailed information about specific performance monitoring parameters, see the "9.4 Optical Card Performance Monitoring" section on page 9-5.

9.3 Pointer Justification Count

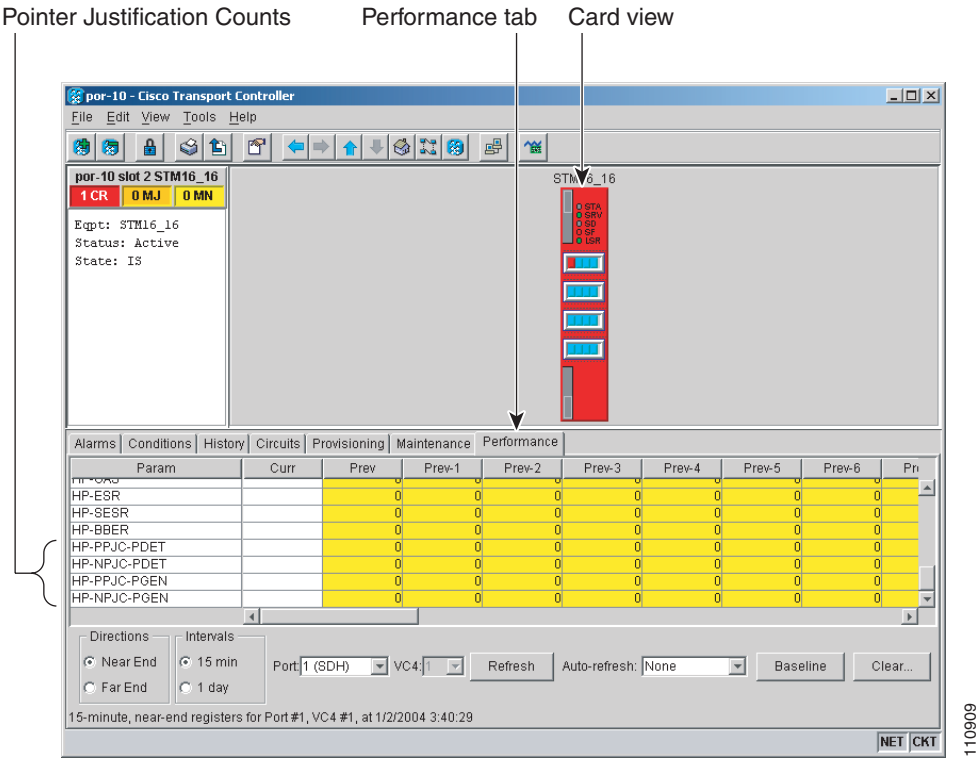
Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing differences on SDH networks. When a network is not synchronized, frequency and phase variations occur on the transported signal. Excessive frequency and phase variations can cause terminating equipment to slip. These variations also cause 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, which causes data to be transmitted again.

Pointers align the phase variations in VC4 and TU payloads. The VC4 payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the VC4 Virtual Container (VC) called the J1 byte. A small number of pointer justification counts per day is not cause for concern. If the pointer justification count continues to rise or becomes large, action must be taken to correct the problem.

Figure 9-3 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.

Figure 9-3 Viewing Pointer Justification Count Parameters



PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications depending on the specific PM name. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications depending on the specific PM name.

A consistent 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. Positive pointer adjustments occur when the frame rate of the VC is too slow in relation to the rate of the VC4.

For pointer justification count definitions, see the "9.4 Optical Card Performance Monitoring" section on page 9-5. In CTC, the PM count fields for PPJC and NPJC appear white and blank unless IPPM is enabled.

Note PPJC-Pgen and NPJC-Pgen correspond to the "PJE+" and "PJE–" pointer justification counters required by the ITU-T.

9.4 Optical Card Performance Monitoring

The following sections define performance monitoring parameters for the OC-48/STM16 and OC-192/STM64 optical cards.

9.4.1 OC-48/STM16 and OC-192/STM64 Card Performance Monitoring Parameters

Figure 9-4 shows where overhead bytes detected on the application-specific integrated circuits (ASICs) produce performance monitoring parameters for the OC-48/STM16 and OC-192/STM64 optical cards.

Figure 9-4 PM Read Points on the OC-48/STM16 and OC-192/STM64 Cards

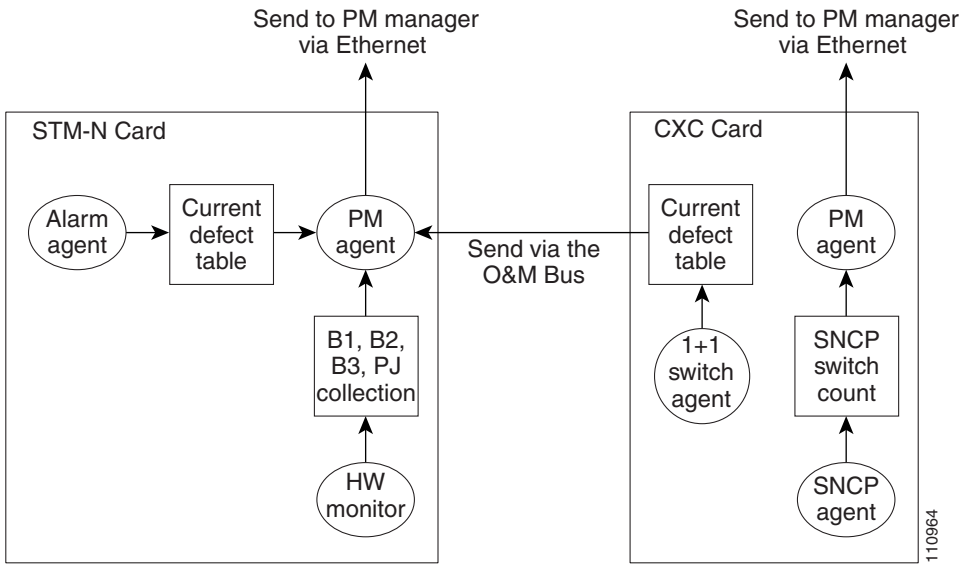


Table 9-2 defines the near-end regenerator section layer PMs.

Table 9-2 Near-End Regenerator Section Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition	Default TCA Value[1]
RS-EB	Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within the block.	10000 (15 Min) 100000 (1 Day)
RS-BBE	Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of RS-SES.	10000 (15 Min) 100000 (1 Day)

Table 9-2 Near-End Regenerator Section Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards (continued)

Parameter	Definition	Default TCA Value[1]
RS-ES	Regenerator Section Errored Seconds (RS-ES) indicates the count of number of seconds when at least one RS-layer EDC error was detected or a Loss Of Signal (LOS) defect was present.	500 (15 Min) 5000 (1 Day)
RS-SES	Regenerator Section Severely Errored Seconds (RS-SES) is a count of seconds where K or more EDC RS-layer errors were detected or an LOS defect was present.	500 (15 Min) 5000 (1 Day)

1. The default TCA value might vary depending your system configuration and specific requirements.

Table 9-3 defines the near-end and far-end multiplex section layer PMs.

Table 9-3 Near-End and Far-End Multiplex Section Layer Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition	Default TCA Value[1]
MS-EB	Multiplex Section Errored Block (MS-EB). Near-End MS-EB indicates that one or more bits are in error (EDC error) within a block. Far-End MS-EB indicates that one or more MS-REI (Multiplex Section-Remote Error Indication) occurs in a block.	21260 (15 Min) STM16 85040 (15 Min) STM64 212600 (1 Day) STM16 850400 (1 Day) STM64
MS-BBE	Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an MS-SES.	21260 (15 Min) STM16 85040 (15 Min) STM64 212600 (1 Day) STM16 850400 (1 Day) STM64
MS-ES	Multiplex Section Errored Seconds (MS-ES). A Near-End MS-ES indicates the count of the number of seconds when at lease one MS-layer EDC error was detected or one defect MS-AIS (Multiplex Section-Alarm Indication Signal) occurred. A Far-End MS-ES indicates the count of the number of seconds when at least on MS-REI (Multiplex Section-Remote Error Indication) was detected or one MS-RDI (Multiplex Section Remote Defect Indication) occurred.	87 (15 Min 864 (1 Day)

Table 9-3 Near-End and Far-End Multiplex Section Layer Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards (continued)

Parameter	Definition	Default TCA Value[1]
MS-SES	Multiplex Section Severely Errored Seconds (MS-SES). A Near-End MS-SES is a count of the number of seconds when K (see G.826-G.829 ITU-T) or more EDC MS-layer errors were detected or MS-AIS occurred. (See ITU-T G.829 for further details.) A Far-End MS-SES is a count of the number of seconds when at least K EBs (Errored Blocks0 derived from MS-REI or MS-RDI occurred. (See ITU-T G.829 for further details.)	1 (15 Min) 4 (1 Day)
MS-UAS	Near-End/Far-End Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section is 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.	3 (15 Min) 10 (1 Day)

1. The default TCA value might vary depending your system configuration and specific requirements.

Table 9-4 defines the near-end SDH Path H-Byte PMs.

Table 9-4 Near-End SDH Path H-Byte Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition	Default TCA Value[1]
PPJC-Pdet	Positive Pointer Justification Count, VC4 Path Detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SDH signal.	60 (15 Min) 5760 (1 Day)
NPJC-Pdet	VC4 Path Detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SDH signal.	60 (15 Min) 5760 (1 Day)
PPJC-Pgen	Positive Pointer Justification Count, VC4 Path Generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the VC with the local clock.	60 (15 Min) 5760 (1 Day)
NPJC-Pgen	Negative Pointer Justification Count, VC4 Path Generated (PPJC-Pgen) is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the VC with the local clock.	60 (15 Min) 5760 (1 Day)

1. The default TCA value might vary depending your system configuration and specific requirements.

For information about troubleshooting SNCP switch counts, refer to the *Cisco ONS 15600 SDH Troubleshooting Guide*. For information about creating circuits with protection switching, see Chapter 6, "Circuits and Tunnels."

Table 9-5 defines the near-end protection switching PMs.

Table 9-5 Near-End Protection Switching Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition	Default TCA Value[1]
MS-PSC (1+1 protection)	In a 1 + 1 protection scheme for a working card, Multiplex Section Protection Switch 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 reverts 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 reverts to the protection card. The MS-PSC PM is only applicable if revertive line-level protection switching is used.	1 (15 Min) 5 (1 Day)
MS-PSD	For an active protection line, Multiplex Section Protection Switch 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 counts on the active protect line.	300 (15 Min) 600 (1 Day)
MS-PSC-W	For a working line in a two-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.	1 (15 Min) 5 (1 Day)
MS-PSD-W	For a working line in a two-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.	300 (15 Min) 600 (1 Day)

1. The default TCA value might vary depending on your system configuration and specific requirements.

SDH path performance monitoring parameters increment only if IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring" section on page 9-2.

Table 9-6 defines the near-end and far-end SDH high order path PMs.

Table 9-6 Near-End and Far-End SDH Path Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition	Default TCA Value[1]
HP-EB	High Order Path Errored Block (HP-EB). Near-End HP-EB indicates that one or more bits are in error within a block. Far-End HP-EB indicates that one or more HP-REI occurs in aa block.	25 (15 Min) VC4 75 (15 Min) VC4-4c and greater 250 (1 Day) VC4 750 (1 Day) VC4-4c and greater
HP-BBE	High Order Path Background Block Error (HP-BBE). A Near-End/Far-End HP-BBE indicates an errored block not occurring as part of an HP-SES.	25 (15 Min) 250 (1 Day)

Table 9-6 Near-End and Far-End SDH Path Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards (continued)

Parameter	Definition	Default TCA Value[1]
HP-ES	High Order Path Errored Seconds (HP-ES) A Near-End HP-ES indicates the count of the number of seconds when at least one path-layer EDC error was detected or one among AU-LOP (Administration Unit-Loss of Power), AU-AIS (Administration unit-Alarm Indication Signal, HP-TIM (High Order Path-Trace Identifier Mismatch), or HP-UNEQ (High Order Path-Unequipped) defects occurred. (See ITU-T G.826 for further details.) A Far-End HP-ES indicates the count of the number of seconds when at least one HP-REI was detected or an HP-RDI (High Order Path-Remote Defect Indication) defect occurred.	20 (15 Min) VC4 60 (15 Min) VC4-4c and greater 200 (1 Day) VC4 600 (1 Day) VC4-4c and greater
HP-SES	High Order Path Severely Errored Seconds (HP-SES). A Near-End HP-SES is a count of the seconds when K (2400) or more EDC HP-layer errors were detected or one among AU-LOP, AU-AIS, HP-TIM or HP-UNEQ defect occurred. (See ITU-T G.826 for further details.) A Far-End HP-SES is a count of the seconds when at least K (2400) EBs (Errored Blocks) derived from HP-REI errors were detected or an HP-RDI defect occurred. (See ITU-T G.829 for further details.) HP-SES is a subset of HP-ES.	3 (15 Min) 7 (1 Day)
HP-UAS	Near-End/Far-End High Order Path Unavailable Seconds (VC4 HP-UAS) is a count of the seconds when the high order (HO) path (VC4) was unavailable. An HO 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.	10 (15 Min) 10 (1 Day)
HP-ESR	Near-End/Far-End 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	Near-End/Far-End High Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of HP-SES to total seconds in available time during a fixed measurement interval.	—
HP-BBER	Near-End/Far-End High Order Path Background Block Error Ratio (HP-BBER) is the ratio of Background Block Errors (HP-BBE) to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during HP-SESs.	—

1. The default TCA value might vary depending your system configuration and specific requirements.

9.4.2 Physical Layer Parameters

The ONS 15600 SDH retrieves the optical power received (OPR), optical power transmitted (OPT), and laser bias current (LBC) from the line card and stores these values with the PM counts for the 15-minute and 1-day periods. You can retrieve current OPR, OPT, and LBC values for each port by displaying the card view in CTC and clicking the Maintenance > Transceiver tabs.

The physical layer performance parameters consist of normalized and nonnormalized values of LBC, OPT, and OPR. Table 9-7 defines the nonnormalized values.

Table 9-7 Nonnormalized Transceiver Physical Optics for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition
Nonnormalized LBC (mA)[1]	The actual operating value of laser bias current (mA) for the specified card port.
Nonnormalized OPT (dBm)[1]	The actual operating value of optical power transmitted (dBm) for the specified card port.
Nonnormalized OPT (dBm)[2]	The actual operating value of optical power received (dBm) for the specified card port.

1. This value should be somewhat consistent from port to port and cannot be configured.
2. This value will vary from port to port because of received optical signal power differences. This value can be configured by calibrating the nominal value to the initial receive power level when the port is put in service.

The normalized physical layer performance parameters are represented as a percentage of the nominal operating value, with 100 representing the nominal value. Table 9-8 defines the normalized physical layer performance parameters.

Table 9-8 Physical Optics Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards

Parameter	Definition	Default TCA Value
LBC (1)[1]	Laser bias current (LBC) is represented by the percentage of the normal (100%) laser bias current of the laser on the card port. The high laser bias current (LBC-HIGH) threshold is the percentage of the normal laser bias current when a high current TCA occurs. The low laser bias current (LBC-LOW) threshold is the percentage of the normal laser bias current when a low current TCA occurs.	200 (LBC-HIGH) 20 (LBC-LOW)

Table 9-8 Physical Optics Performance Monitoring Parameters for the OC-48/STM16 and OC-192/STM64 Cards (continued)

Parameter	Definition	Default TCA Value
OPT	Optical power transmitted (OPT) is represented by the percentage of the normal (100%) optical transmit power of the laser on the card port. The high optical power transmitted (OPT-HIGH) threshold is the percentage of the normal transmit optical power when a high transmit power TCA occurs. The low optical power transmitted (OPT-LOW) threshold is the percentage of the normal transmit optical power when a low transmit power TCA occurs.	120 (OPT-HIGH) 80 (OPT-LOW)
OPR	Optical power received (OPR) is represented by the percentage of the normal optical receive power of the card port. The high optical power received (OPR-HIGH) threshold is the percentage of the calibrated receive optical power when a high receive power TCA occurs. The low optical power received (OPR-LOW) threshold is the percentage of the calibrated receive optical power when a low receive power TCA occurs.	200 (OPR-HIGH) 50 (OPR-LOW)

1. As stated in Telcordia GR-253-CORE, the LBC (TCA) PM value is not appropriate for use with some optical transmitter technologies. Such is the case for Cisco's uncooled SR optical transmitters. The default LBC TCA provides safe operating parameter for both of Cisco's cooled and uncooled transmitters.

To set the threshold values for LBC, OPT, and OPR, and to reset the OPR nominal value for future calculation, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

CHAPTER 10

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15600 SDH.

For SNMP setup information, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

Chapter topics include:

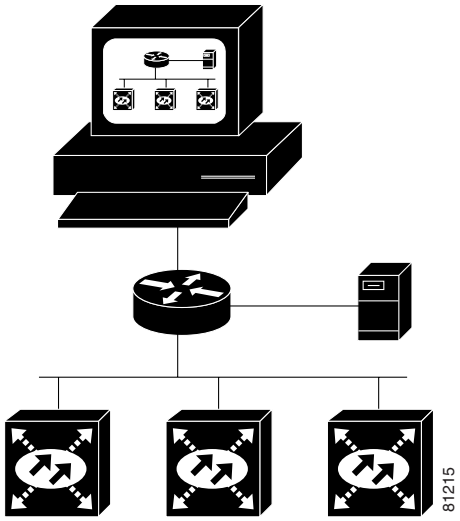
10.1 SNMP Overview

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 15600 SDH uses SNMP to provide asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for generic read-only management of SDH technologies. SNMP allows limited management of the ONS 15600 SDH by a generic SNMP manager, for example HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert.

The Cisco ONS 15600 SDH supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). The two versions share many features, but SNMPv2c includes additional protocol operations. SNMP Version 3 is acceptable, but not required. This chapter describes both versions and explains how to configure SNMP on the ONS 15600 SDH. Figure 10-1 illustrates a basic network managed by SNMP.

Figure 10-1 Basic Network Managed by SNMP

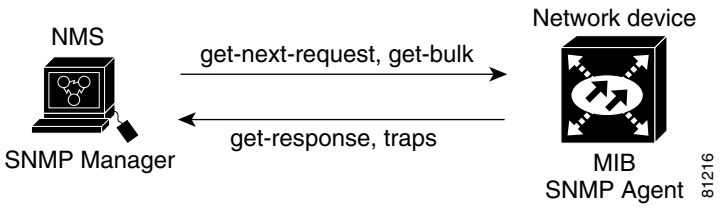


10.2 SNMP Basic Components

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 15600 SDH.

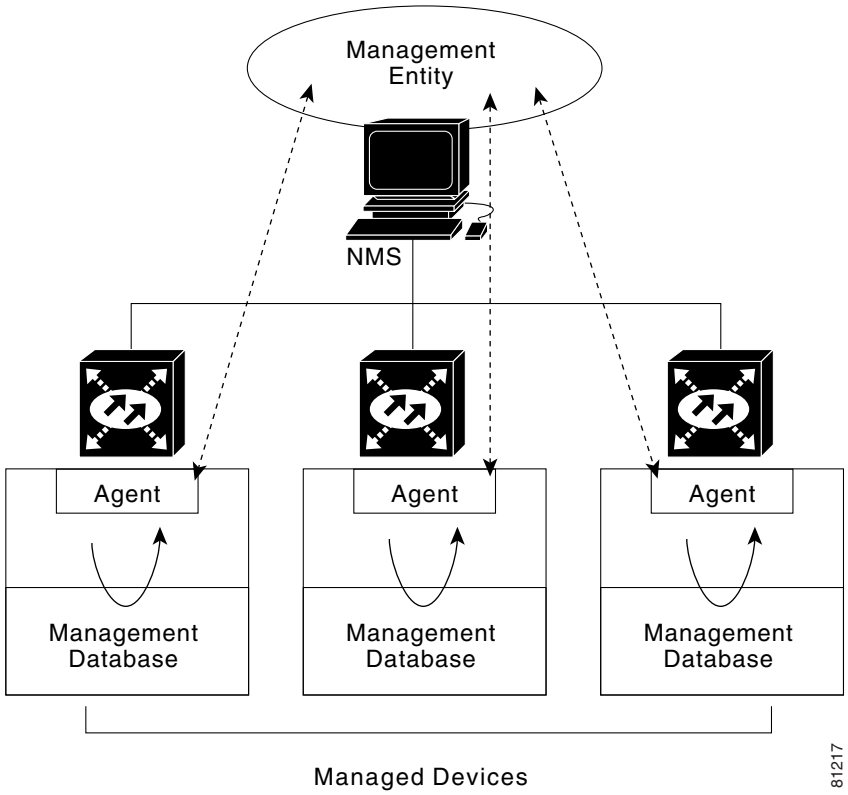
An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the MIB, which is the repository for device parameter and network data. The agent can also send traps, or notifications of certain events, to the manager. Figure 10-2 illustrates these SNMP operations.

Figure 10-2 SNMP Agent Gathering Data from a 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 10-3 illustrates the relationship between the three key SNMP components.

Figure 10-3 Example of the Primary SNMP Components



10.3 SNMP Support

The ONS 15600 SDH supports SNMPv1 and SNMPv2c traps and get requests. The SNMP MIBs in the ONS 15600 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. To set up SNMP, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

10.4 SNMP Management Information Bases

A MIB is a hierarchically organized collection of information. Network management protocols such as SNMP access MIBs. MIBs consist of managed objects and are identified by object identifiers.

The ONS 15600 SDH SNMP agent communicates with an SNMP management application using SNMP messages. Table 10-1 describes these messages.

Table 10-1 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request.
trap	Indicates that an event has occurred. A trap is an unsolicited message sent by an SNMP agent to an SNMP manager.

A managed object (also 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 10-2 lists the IETF standard MIBs implemented in the ONS 15600 SDH SNMP Agent.

The ONS 15600 SDH MIBs are included on the software CD that ships with the ONS 15600 SDH. Compile these MIBs in the following sequence. If you do not follow the sequence, one or more MIB files might not compile.

1. CERENT-GLOBAL-REGISTRY.mib
2. CERENT-TC.mib
3. CERENT-454-MIB.mib
4. CERENT-GENERIC-MIB.mib

If you cannot compile the ONS 15600 SDH MIBs, contact the Cisco Technical Assistance Center (TAC). For contact information, see the "Obtaining Technical Assistance" section on page -xxi.

Table 10-2 IETF Standard MIBs Implemented in the ONS 15600 SNMP Agent

RFC#	Module Name	Title/Comments
1213 +1907	RFC1213-MIB, SNMPV2-MIB	MIB-II from RFC1213 with enhancement from RFC1907 for v2
1253	OSPF-MIB	Open Shortest Path First
1493	BRIDGE-MIB	Bridge/Spanning Tree (SNMPv1 MIB)
2737	ENTITY-MIB	Entity MIB using SMI[1] v2 (version II)
2233	IF-MIB	Interface evolution (enhances MIB-II)
2358	Etherlike-MIB	Ethernet-like interface (SNMPv2 MIB)
2558	SDH-MIB	SDH
2674	P-BRIDGE-MIB, Q-BRIDGE-MIB	P-Bridge and Q-Bridge MIB

1. SMI = Structure of Management Information

10.5 SNMP Traps

The ONS 15600 SDH can receive SNMP requests from a number of SNMP managers and send traps to ten trap receivers. The ONS 15600 SDH generates all alarms and events as SNMP traps.

The ONS 15600 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, VC4, 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 15600 SDH also generates a trap for each alarm when the alarm condition clears.

Table 10-3 lists the SNMP trap variable bindings.

Table 10-3 SNMP Trap Variable Bindings for the ONS 15600 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 listed after 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.

Table 10-3 SNMP Trap Variable Bindings for the ONS 15600 SDH (continued)

Number	Name	Description
10	cerent454AlarmTimeStamp	This variable gives the time when the alarm occurred.
11	cerent454AlarmObjectName	This variable gives the TL1-style user-visible name which uniquely identifies an object in the system.

Table 10-4 lists the generic and IETF traps for the ONS 15600 SDH.

Table 10-4 Traps Supported in the ONS 15600 SDH

Trap	From RFC No.	Description
ColdStart	RFC1213-MIB	Agent up, cold start.
WarmStart	RFC1213-MIB	Agent up, warm start.
NewRoot	RFC1493/ BRIDGE-MIB	The 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.
risingAlarm	RFC1757	The SNMP trap that is generated when an alarm entry crosses the rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC1757	The SNMP trap that is generated when an alarm entry crosses the falling threshold and generates an event that is configured for sending SNMP traps.

10.6 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination dialog box (see the "10.3 SNMP Support" section on page 10-3). 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.

Alarm Monitoring and Management

This chapter explains how to manage alarms with Cisco Transport Controller (CTC), which includes:

To troubleshoot specific alarms, see the *Cisco ONS 15600 SDH Troubleshooting Guide*.

11.1 Overview

CTC detects and reports SDH alarms generated by the Cisco ONS 15600 SDH and the larger SDH network. You can use CTC to monitor and manage alarms in the card, node, or network level. Default alarm severities conform to the ITU-T G.783 standard, but you can reset alarm severities in customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard Telcordia categories employed by ONS nodes, see the *Cisco ONS 15600 SDH Troubleshooting Guide*.

Note ONS 15600 SDH alarms can also be monitored and managed through a network management system (NMS).

11.2 Alarms, Conditions, and History

In the card, node, or network-level CTC view, click the Alarms tab to display the alarms for that card, node or network. The Alarms window shows alarms in conformance to ITU-T G.783. This means that if a network problem causes two alarms, such as loss of frame (LOF) and loss of signal (LOS), CTC only shows the LOS alarm in this window because it supersedes the LOF.

Table 11-1 describes in the information in the Alarms window.

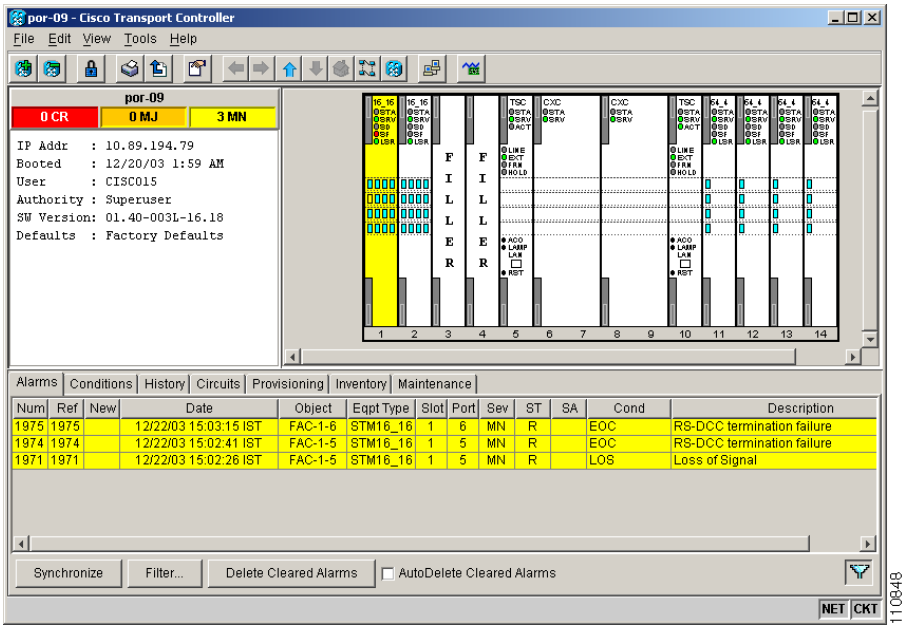
Table 11-1 Alarms Column Descriptions

Column	Information Recorded
Num	A count of incrementing alarm messages (hidden by default)
Ref	Reference number assigned to a cleared alarm (hidden by default)
New	Indicates a new alarm if checked[1]
Date	Date and time of the alarm
Object	TL1 access identifier (AID) for the alarmed object
Eqpt Type	Card type in this slot
Slot	Slot where the alarm occurred (appears in the network view and node view)
Port	Port where the alarm occurred
Sev	Severity level: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR)
ST	Status: Raised (R), Clear (C), Transient (T)
SA	When checked, indicates a service-affecting alarm
Cond	Error message/alarm name; alphabetically defined in the *Cisco ONS 15600 SDH Troubleshooting Guide*
Description	Description of the alarm
Node	Node where the alarm occurred (only displayed in network view)

1. The user can click the Synchronize button to acknowledge the new alarm. Clicking the Delete Cleared Alarms button only deletes cleared alarm on the window.

Figure 11-1 shows the CTC node view Alarms window.

Figure 11-1 Viewing Alarms in CTC Node View



Alarms and conditions appear in one of five background colors, listed in Table 11-2, to communicate severity.

Table 11-2 Color Codes for Alarms and Conditions

Color	Description
Red	Critical alarm
Orange	Major alarm
Yellow	Minor alarm
Magenta (pink)	Event (NA)
Blue	Condition (NR)
White	Cleared alarm or event (CL)

Software Release 1.4 has more numbered synchronous transfer module (STM) and Virtual Container (VC) alarm object identifiers based upon the object IDs. The numbering of the monitored (MON) object that tripped the alarm is in the format VC4-<*Slot*>-<*Port*>-<*VC_within_port*>. For example, with a VC4, Slot 6, Port 1, and VC4 6, the VC AID would be VC4-6-1-6.

11.2.1 Alarm Window

Table 11-3 shows the actions you can perform in the Alarms window.

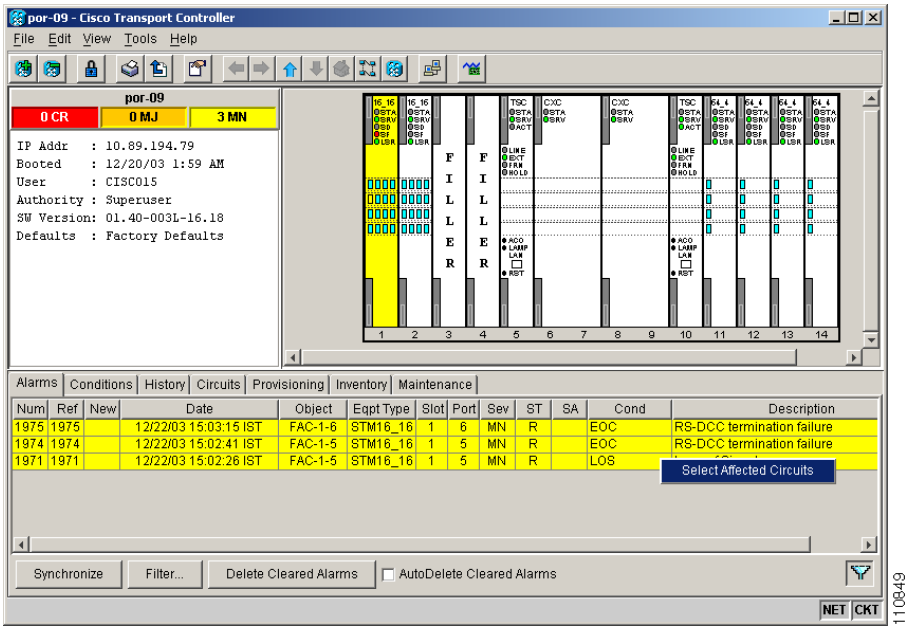
Table 11-3 Alarm Window

Button	Action
Filter	Allows you to change the display on the Alarms window to show only alarms that meet a certain severity level, occur in a specified time frame, and/or reflect specific appear on the window. If you enable the Filter feature by clicking the Filter icon button in one CTC view, such as node view, it is enabled in the others as well (card view and network view).
Synchronize	Updates the alarm display. Although CTC displays alarms in real time, the Synchronize button verifies that CTC and the ONS 15600 SDH agree on current alarms. This is particularly useful during provisioning or troubleshooting.
Delete Cleared Alarms	Deletes alarms that have been cleared.
AutoDelete Cleared Alarms	If checked, CTC automatically deletes cleared alarms.

11.2.2 Alarm-Affected Circuits

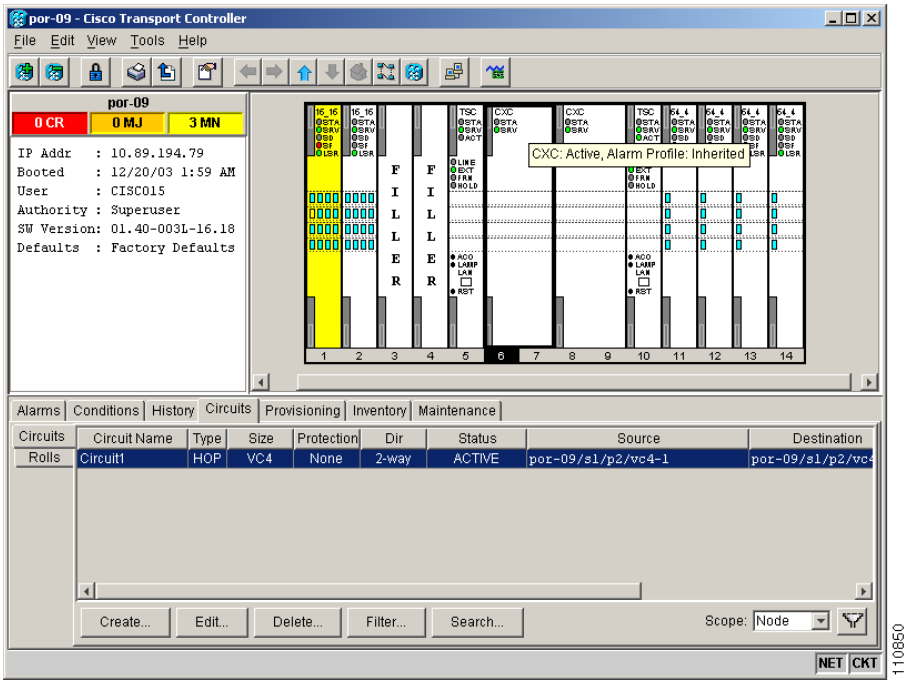
You can determine which ONS 15600 SDH circuits are affected by a specific alarm by positioning the cursor over the alarm in the Alarm window and right-clicking. A shortcut menu appears (Figure 11-2).

Figure 11-2 Select the Affected Circuits Option for an Alarm



When the user selects the Select Affected Circuits option, the Circuits window appears to show the circuits that are affected by the alarm (Figure 11-3).

Figure 11-3 Alarm-Affected Circuit Appears



11.2.3 Conditions Window

The Conditions window displays retrieved fault conditions. A condition is a fault or status detected by ONS 15600 SDH hardware or software. When a condition occurs and continues for a minimum period of time, CTC raises a condition, which is a flag showing that this particular condition currently exists on the ONS 15600 SDH.

The Conditions window shows all conditions that occur, including those that are superseded by alarms. For instance, if a network problem causes two alarms, such as LOF and LOS, CTC shows both the LOF and LOS conditions in this window. Having all conditions visible can be helpful when troubleshooting the ONS 15600 SDH. If you want to retrieve conditions that obey a root-cause hierarchy (that is, LOS supersedes and replaces LOF), you can exclude the same root causes.

Fault conditions include reported alarms and not-reported or not-alarmed conditions. See the trouble notifications information in the *Cisco ONS 15600 SDH Troubleshooting Guide* for more information about alarm and condition classifications.

11.2.4 Conditions Window Actions

Table 11-4 shows the actions you can perform in the Conditions window.

Table 11-4 Conditions Display

Button	Action
Retrieve	Retrieves the current set of all existing fault conditions, as maintained by the alarm manager, from the ONS 15600 SDH.
Filter	Allows you to change the Conditions window display to only show the conditions that meet a certain severity level or occur in a specified time. For example, you can set the filter so that only critical conditions display on the window. There is a Filter icon button on the lower-right of the window that allows you to enable or disable the filter feature.

The current set of all existing conditions maintained by the alarm manager appears when you click the Retrieve button. The set of conditions retrieved is relative to the view. For example, if you click the button in the node view, node-specific conditions appear (Figure 11-4). If you click the Retrieve button in the network view, all conditions for the network (including ONS 15600 SDH nodes and other connected nodes such as ONS 15454) appear, and the card view shows only card-specific conditions.

Figure 11-4 Viewing Conditions in the Conditions Window

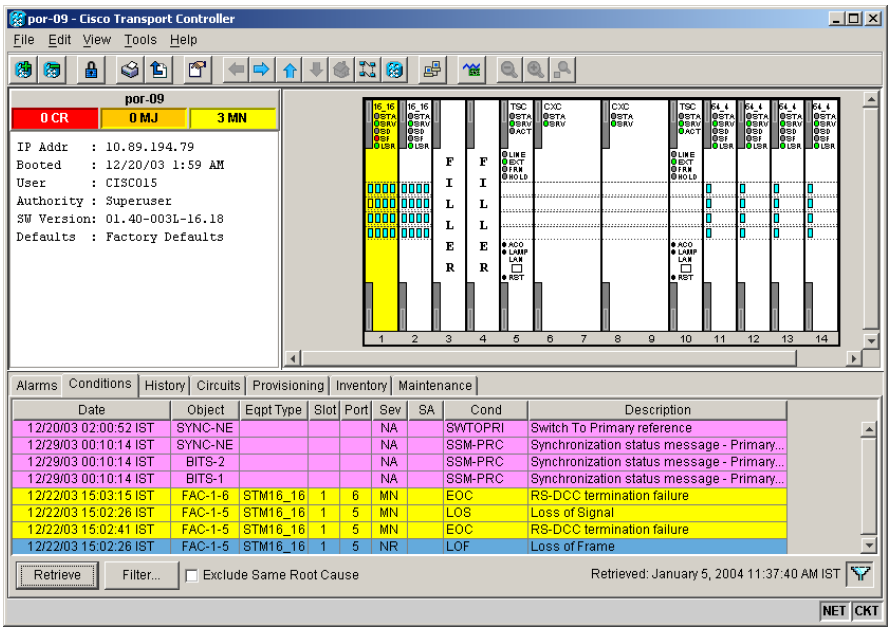


Table 11-5 lists the Conditions window column headings and the information recorded in each column.

Table 11-5 Conditions Column Description

Column	Information Recorded
Date	Date and time of the condition.
Object	TL1 AID for the alarmed object.
Eqpt Type	Card type in this slot (only displayed in the network view and node view).
Slot	Slot where the condition occurred (only displayed in the network view and node view).
Port	Port where the condition occurred.
Sev	Severity level: CR, MJ, MN, NA, NR.
SA	When checked, indicates a service-affecting alarm.
Cond	Condition name; these names are alphabetically listed and defined in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15600 SDH Troubleshooting Guide*.
Description	Description of the condition.
Node	Node where the condition occurred (only displayed in network view).

11.2.5 History Window

The History window displays historical alarm data. It also displays conditions, which are not-alarmed activities such as timing changes and threshold crossings. For example, protection-switching events or performance-monitoring threshold crossings appear here. The ONS 15600 SDH can store up to 3,000 total alarms and conditions: 750 critical alarms, 750 major alarms, 750 minor alarms, and 750 conditions. When the limit is reached, the ONS 15600 SDH begins replacing the oldest items. The History window presents several alarm history views:

- The History > Session window appears in network view, node view, and card view (Figure 11-5). It shows alarms and conditions that have occurred during the current user CTC session.
- The History > Node window appears only in node view. It shows the alarms and conditions that have occurred on the node since CTC software was originally activated for that node.
- The History > Card window appears only in the card view. It shows the alarms and conditions that have occurred on the card since CTC software was installed on the node.

Note In the Preference dialog General tab, the Maximum History Entries value only applies to the Session window.

Tip Double-click an alarm in the History window to display the corresponding view. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Figure 11-5 Viewing All Alarms Reported for Current Session

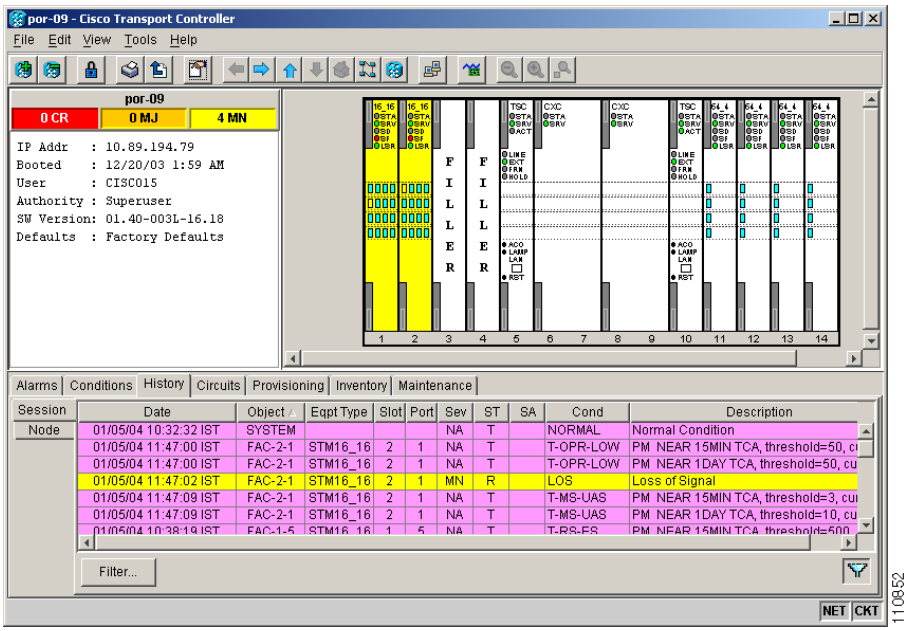


Table 11-6 describes the information in the History window.

Table 11-6 History Column Description

Column	Information Recorded
Date	Date and time of the alarm.
Object	TL1 AID for the alarmed object.
Sev	Severity level: CR, MJ, MN, NA, NR.
Eqpt Type	Card type in this slot (only displays in network view and node view).
ST	Status: R (Raised), C (Cleared), T (Transient).
Description	Description of the condition.
Port	Port where the condition occurred.
Cond	Condition name.
Slot	Slot where the condition occurred (only displays in network view and node view).
SA	When checked, indicates a service-affecting alarm.

11.2.6 Alarm History Actions

You can retrieve and view the history of alarms and conditions, as well as transients (passing notifications of processes as they occur) in the CTC history window. The information in this window is specific to the view where it is shown (that is, network history in the network view, node history in the node view, and card history in the card view).

The node and card history views are each divided into two tabs. In node view, when you click the Retrieve button, you can see the history of alarms, conditions, and transients that have occurred on the node in the History > Node window, and the history of alarms, conditions, and transients that have occurred on the node during your login session in the History > Session window. When you retrieve the

card history, you can see the history of alarms, conditions, and transients on the card in the History > Card window, or a history of alarms, conditions, and transients that have occurred during your login session in the History > Session window.

You can also filter the severities and occurrence period in these history windows, but you cannot filter out not-reported conditions or transients.

11.3 Alarm Profiles

The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15600 SDH ports, cards, or nodes. A created alarm profile can be applied to any node on the network. Alarm profiles can be saved to a file and imported elsewhere in the network, but the profile must be stored locally on a node before it can be applied to the node, cards, or ports.

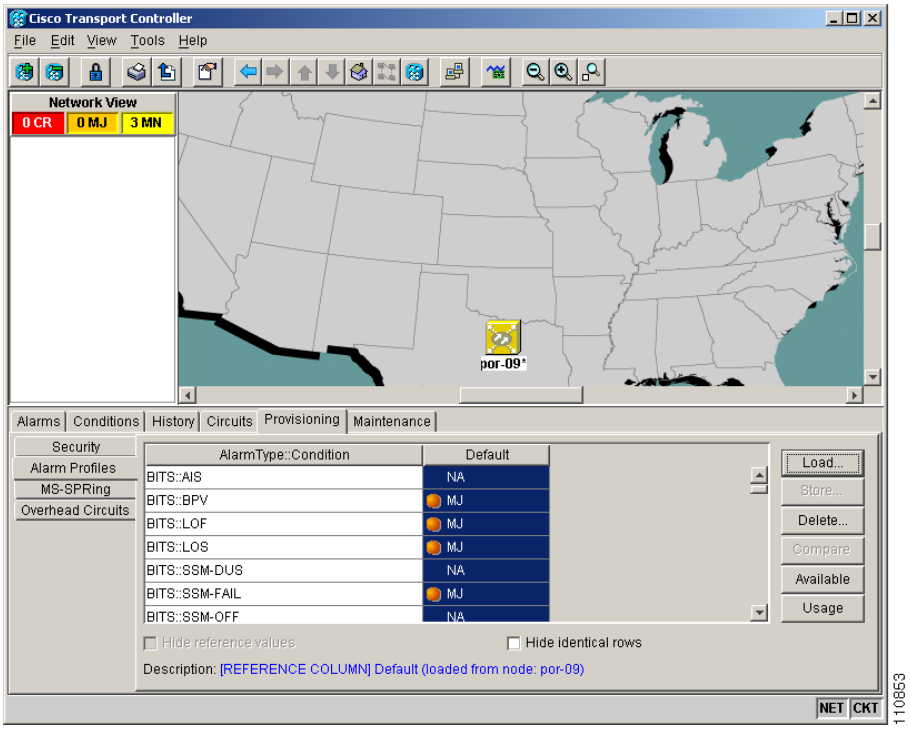
CTC can store up to ten active alarm profiles at any time to apply to the node. Custom profiles can take eight of these active profile positions, and two are reserved by CTC. The reserved Default profile contains ITU-T G.783 severities. The reserved Inherited profile allows port alarm severities to be governed by the card-level severities or card alarm severities to be determined by the node-level severities.

If one or more alarm profiles have been stored as files from elsewhere in the network onto the local PC or server hard drive where CTC resides, you can utilize as many profiles as you can physically store by deleting and replacing them locally in CTC so that only eight are active at any given time.

11.3.1 Alarm Profile Window

Alarm profiles are created in the network view using the Provisioning > Alarm Profiles tabs (Figure 11-6). A default alarm profile (in the Default column) is preprovisioned for every alarm. After loading the default profile on the node, you can use the Clone feature to create new profiles based on the default alarm profile. After the new profile is created, the Alarm Profiles window shows the default profile and the new profile.

Figure 11-6 Alarm Profiles Window Showing the Default Profiles of Listed Alarms



11.3.2 Alarm Profile Buttons

The Alarm Profiles window has six buttons on the right side. Table 11-7 describes each of the alarm profile buttons.

Table 11-7 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 (individual alarms that are not configured equivalently between profiles).
Available	Displays all profiles available on each node.
Usage	Displays all entities (nodes and alarm subjects) present in the network and which profiles contain the alarm (can be printed).

11.3.3 Alarm Profile Editing

Table 11-8 describes the five profile-editing options available when you right-click an alarm item in the profile column (such as Default).

Table 11-8 Alarm Profile Editing Options

Button	Description
Store	Saves a profile in a node or in a file.
Rename	Changes a profile name.
Clone	Creates a new profile that contains the same alarm severity settings as the profile being cloned.
Reset	Restores a profile to its previous state or to the original state (if it has not yet been applied).
Remove	Removes a profile from the table editor.

11.3.4 Alarm Severity Option

To change or assign alarm severity, left-click the alarm severity you want to change in the alarm profile column. Seven severity levels appear for the alarm:

- Not-reported (NR)
- Not-alarmed (NA)
- Minor (MN)
- Major (MJ)
- Critical (CR)
- UNSET: Unset/Unknown (not normally used)
- Transient (T)

Transient and Unset only appear in alarm profiles. They do not appear when you view alarms, history, or conditions.

11.3.5 Row Display Options

In the network view, the Alarm Profiles window has two check boxes at the bottom of the window:

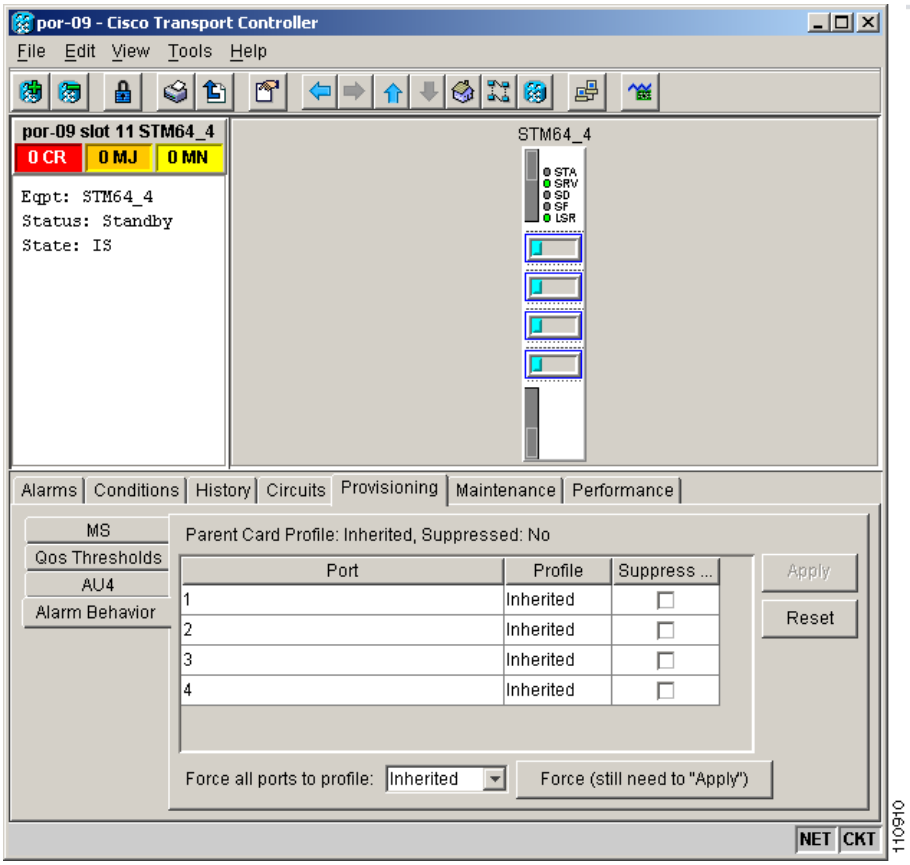
- Hide values matching profile Default—Highlights alarms with nondefault severities by clearing alarm cells with default severities (disabled in Software Release 1.4.).
- Hide identical rows—Hides rows of alarms that contain the same severity for each profile.

11.3.6 Alarm Profile Applications

In CTC node view, the Alarm Behavior window displays alarm profiles for the node, and in card view the Alarm Behavior window displays the alarm profiles for the selected card. Alarm profiles form a hierarchy. A node-level alarm profile applies to all cards in the node except cards that have their own profiles. A card-level alarm profile applies to all ports on the card except ports 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. At the card-level view, you can apply profile changes on a port-by-port basis for all ports on that card. Figure 11-7 shows the STM64 L4 1550 card view of an alarm profile.

Figure 11-7 Alarm Profile on the STM64 L4 1550 Card



11.4 Alarm Filter

Alarm display can be filtered to keep particular alarm severities, or alarms that occur between certain dates, from appearing in the Alarms window (Figure 11-2 on page 11-4). You can set the parameters of the filter by clicking the Filter button at the bottom-left of the Alarms window. You can turn the filter on or off by clicking the Filter icon button at the bottom-right of the window. CTC retains your filter activation setting. For example, if you turn the filter on and then log out, CTC makes the filter active the next time your user ID is activated.

11.5 Alarm Suppression

The ONS 15600 SDH has suppression options that prevent node, slot, chassis, or port alarms from appearing in the Alarms window. Suppression changes the entity alarm to Not-Reported, so suppressed alarms are shown in the Conditions window. The suppressed alarms are shown with their other visual characteristics (service-affecting status and color-coding) in the window. These alarms do not appear in the History window or in any other clients.

In node view, you can suppress all alarms for a node, one or more card slots, fan slots, noncard objects such as the chassis, or the customer access panel (CAP). In the card view, you can suppress alarms on a port-by-port basis. All alarms for the entity are suppressed. For example, if you click the Suppress Alarms check box in node view, all node alarms appear in the Conditions window rather than the Alarms window. If you suppress alarms for one or more slots or ports, alarms for those entities appear in the Conditions window.

Note Use alarm suppression with caution. If multiple CTC or TL1 sessions are open, suppressing the alarms in one session suppresses the alarms in all other open sessions.

11.6 External Alarms and Controls

External alarm inputs are used for external sensors such as open doors and flood sensors, temperature sensors, and other environmental conditions. External control outputs allow you to drive external visual or audible devices such as bells and lights. They can control other devices such as generators, heaters, and fans.

You provision external alarms and controls in the node view Provisioning or Maintenance > Alarm Extenders window. Up to 16 external alarm inputs and 16 external controls are available. The external input/output contacts are located on the CAP attached to the ONS 15600 SDH backplane.

11.6.1 External Alarm Input

You can provision each alarm input separately. Provisionable characteristics of external alarm inputs include:

- Alarm type
- Alarm severity (CR, MJ, MN, NA, or NR)
- Alarm-trigger setting (open or closed)
- Virtual wire associated with the alarm
- CTC alarm log description (up to 63 characters)

11.6.2 External Control Output

You can provision each alarm output separately. Provisionable characteristics of alarm outputs include:

- Control type
- Trigger type (alarm or virtual wire)
- Description for CTC
- Closure setting (manually or by trigger). If you provision the output closure to be triggered, the following characteristics can be used as triggers:
  - Local NE alarm severity—A chosen alarm severity (for example, major) and any higher-severity alarm (in this case, critical) causes output closure
  - Remote NE alarm severity—Similar to local NE alarm severity trigger setting, but applies to remote alarms

- Virtual wire entities—You can provision an alarm that is input to a virtual wire to trigger an external control output

11.6.3 Virtual Wires for External Alarms in Mixed Networks

Virtual wires route external alarms to one or more alarm collection centers in a network. External alarms can be assigned to virtual wires in the ONS 15600 SDH-only network or in mixed networks containing ONS 15600s, ONS 15454s, and ONS 15327s. You can view virtual wires in the CTC node view Maintenance > Alarm Extenders > Virtual Wires window.

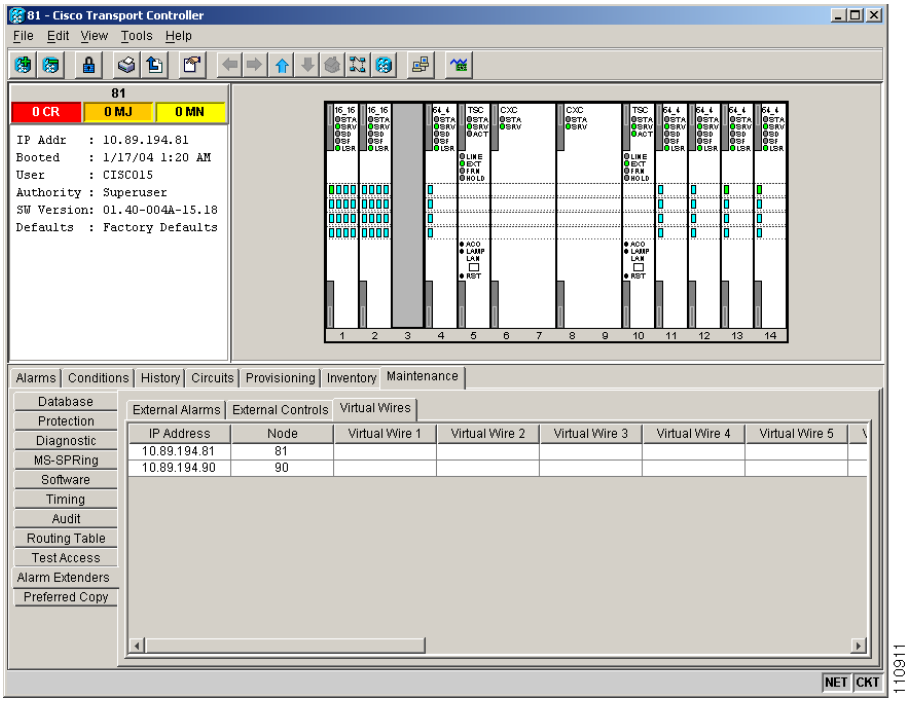
When using virtual wires, you can:

- Assign different external devices to the same virtual wire.
- Assign virtual wires as the trigger type for different external controls.

The ONS 15600 SDH supports 16 virtual wires.

Figure 11-8 shows an ONS 15600 SDH Virtual Wires window with a DCC connection to an ONS 15454 node. The ONS 15600 SDH Virtual Wires window shows 10 virtual wire columns, but 16 are available. The first 12 are available for other ONS 15600 SDHs. Only the last four are available for the ONS 15454, because it can only support four virtual wires.

Figure 11-8 Virtual Wires Seen from an ONS 15600 SDH



11.7 Audit Trail

The ONS 15600 SDH keeps a human-readable audit trail of all system actions, such as circuit creation or deletion, and security events such as login and logouts. You can archive this log in text form on a PC or network. Access the log by clicking the Maintenance > Audit tabs. The log capacity is 640 entries; when this limit is reached, the oldest entries are overwritten with new events. When the log is 80 percent full, an AUD-LOG-LOW condition is raised. When the log is full and entries are being overwritten, an AUD-LOG-LOSS condition occurs.

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W