Cisco ONS 15327 Reference Manual

Product and Documentation Release 3.4
April 2003

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-7815642=
Text Part Number: 78-15642-01

Cisco ONS 15327 Reference Manual

FIGURES

About this Manual

This section explains the objectives, intended audience, and organization of this publication and describes the conventions that convey instructions and other information.

This section provides the following information:

- Document Objectives
- Audience
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Document Objectives

The *Cisco ONS 15327 Reference Manual* provides reference information for the Cisco ONS 15327 system. It contains shelf hardware information, card specifications, and software and topology descriptions. Use this document in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecommunications technician.

Related Documentation

Use the *Cisco ONS 15327 Reference Manual, Release 3.4* in conjunction with the following referenced publications:

- *Cisco ONS 15327 Procedure Guide, Release 3.4*
  Provides installation, turn up, and maintenance procedures for the Cisco ONS 15327

- *Cisco ONS 15327 Troubleshooting Guide, Release 3.4*
  Provides alarm descriptions and troubleshooting procedures, general troubleshooting procedures, and hardware replacement information
- *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide, Release 3.4*
  Provides a comprehensive list of TL1 commands for the ONS 15327 and ONS 15454
- *Release Notes for the Cisco ONS 15327 Release 3.4*
  Provide caveats, closed issues, and new feature information

Where to Find Safety and Warning Information

For safety and warning information, refer to Appendix A "Regulatory and Compliance Requirements." It describes the international agency compliance and safety information for the Cisco ONS 15327. It also includes translations of the safety warnings that appear in the ONS 15327 system documentation.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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

Documentation CD-ROM

Optical networking-related 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.

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 Networking Products MarketPlace:

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, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* 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/go/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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

Shelf Assembly Hardware

This chapter provides a description of Cisco ONS 15327 shelf and backplane hardware. Card and cable descriptions as well as instructions for installing equipment are provided in the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

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

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

Warning **The ONS 15327 is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock, key, or other means of security. A restricted access area is controlled by the authority responsible for the location.**

Warning **The ONS 15327 is suitable for mounting on concrete or other non-combustible surfaces only.**

Note The Cisco ONS 15327 assembly is intended for use with telecommunications equipment only.

Note The ONS 15327 is designed to comply with GR-1089-CORE Type 2 and Type 4. Install and operate the ONS 15327 only in environments that do not expose wiring or cabling to the outside plant. Acceptable applications include Central Office Environments (COEs), Electronic Equipment Enclosures (EEEs), Controlled Environment Vaults (CEVs), huts, and Customer Premise Environments (CPEs).

1.1 Installation Overview

When installed in an equipment rack, the ONS 15327 assembly is typically connected to a fuse and alarm panel that provides centralized alarm connection points and distributed power for the ONS 15327. Fuse and alarm panels are third-party equipment and are not described in this documentation. If you are unsure about the requirements or specifications for a fuse and alarm panel, consult the documentation for that product.

You can mount the ONS 15327 in a 19- or 23-inch rack. Including the fan-tray assembly, the shelf assembly weighs approximately 15 pounds without cards installed and 27 pounds fully loaded. An ONS 15327 is installed in a rack using reversible mounting brackets on each side of the shelf.

You can access the ONS 15327 cards, cables, connectors, power feeds, and fan-tray assembly through the front of the shelf assembly only. The CRIT, MAJ, MIN, and REM alarm LEDs visible on the XTC faceplate indicate whether a Critical, Major, Minor, or Remote alarm is present anywhere on the ONS 15327 assembly. These LEDs help you to determine quickly if any alarms are present on the assembly.

The ONS 15327 is powered using -48 VDC power. Positive and negative power terminals are accessible on the front panel.

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

Note In this chapter, the terms “ONS 15327” and “shelf assembly” are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15327 refers to the entire system, both hardware and software.

Install the ONS 15327 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.**

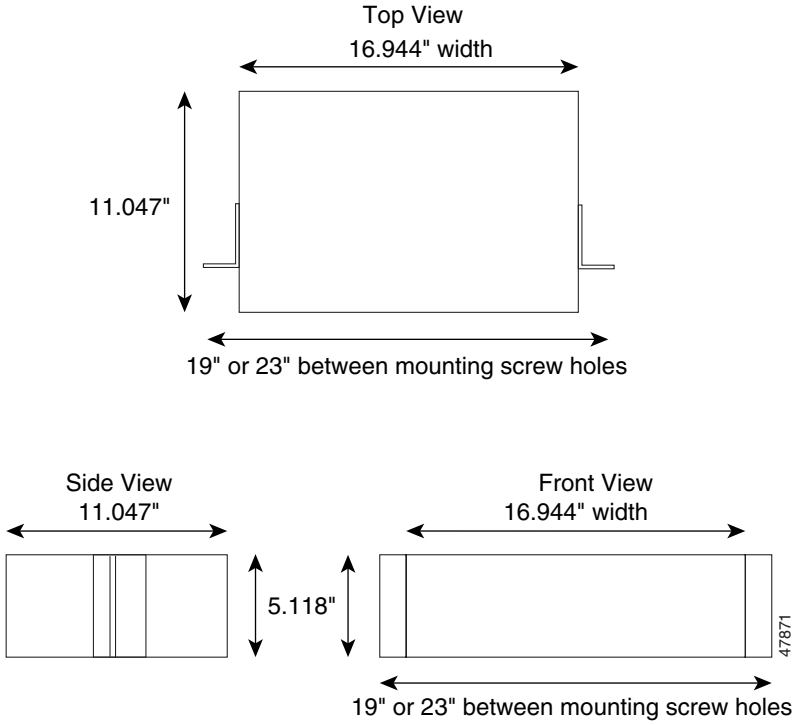
1.2 Rack Installation

Warning **To prevent the equipment from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 131°F (55°C) unless configured for inversion temperature (I-temp). All I-temp rated components are -40°C to +65°C. To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.**

The ONS 15327 is easily mounted in a 19- or 23-inch equipment rack. The shelf assembly projects 2 inches from the front of the rack. It mounts in both EIA-standard and Telcordia-standard racks. The shelf assembly is a total of 17 inches wide with no mounting ears attached. With the mounting ears attached, the shelf assembly is 19 inches wide.

The ONS 15327 measures 5.1 inches high, 19 or 23 inches wide (depending on which way the mounting ears are attached), and 11 inches deep (13 x 48.3 x 28 cm). Figure 1-1 shows the dimensions of the ONS 15327 shelf assembly.

Figure 1-1 ONS 15327 Shelf Assembly Dimensions



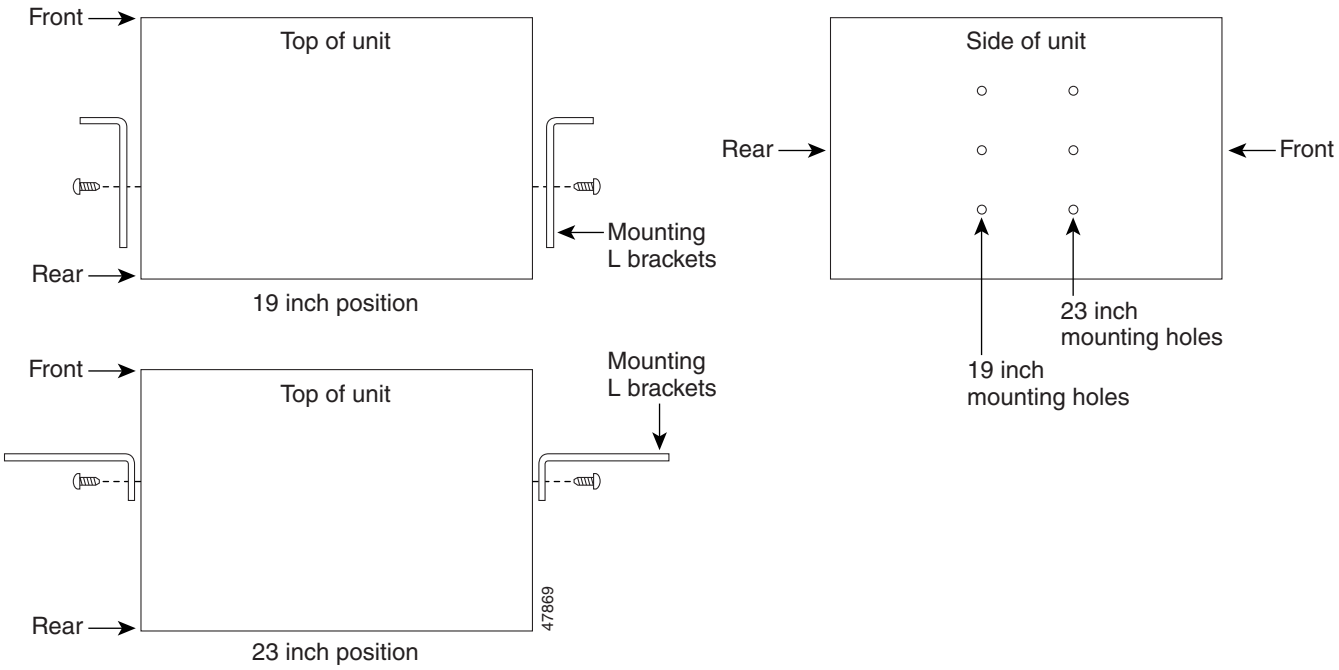
1.2.1 Reversible Mounting Bracket

Caution Use only the fastening hardware provided with the ONS 15327 to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the ONS 15327 in a frame with a non-conductive coating (such as paint, lacquer, or enamel) use either the thread-forming screws provided with the ONS 15327 shipping kit or remove the coating from the threads to ensure electrical continuity.

The shelf assembly comes with mounting brackets that can be reversed for use with a 19- or 23-inch rack (Figure 1-2).

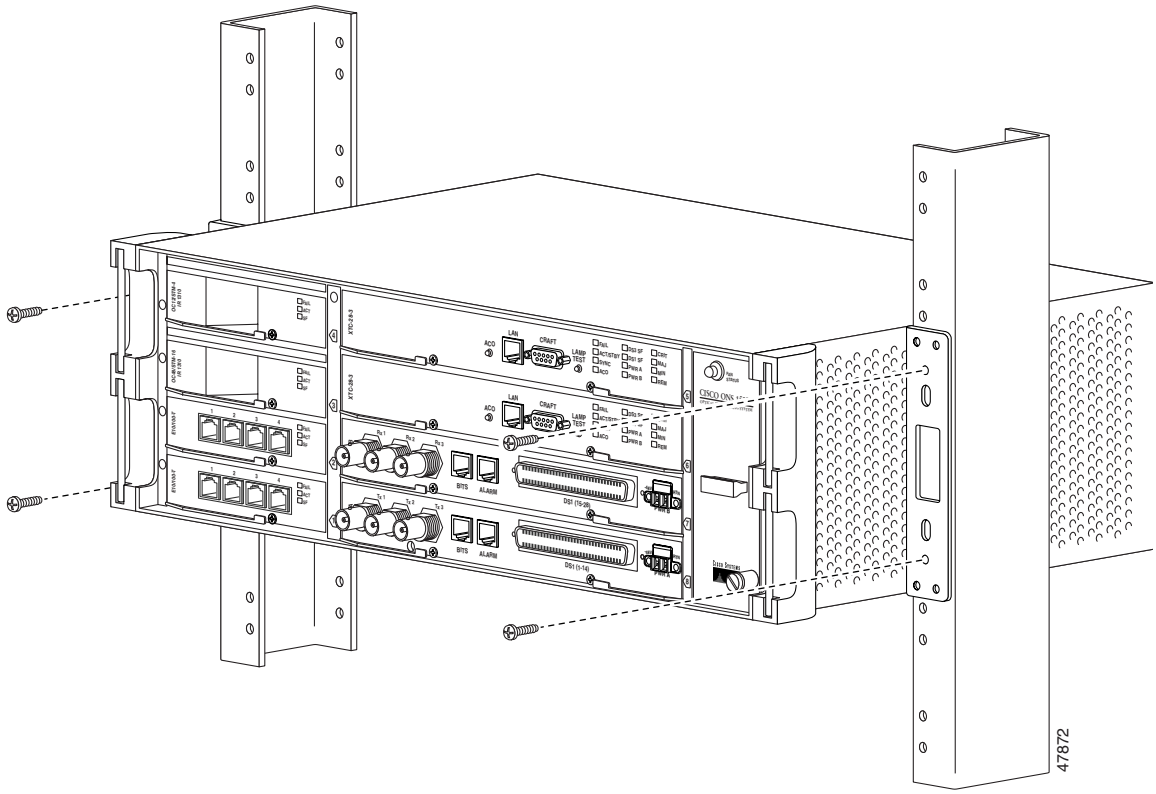
Figure 1-2 Reversing the Mounting Brackets (23-inch Position to 19-inch Position)



1.2.2 Mounting a Single Node

Mounting the ONS 15327 in a rack requires a minimum of 5.2 inches of vertical rack space (plus 1 inch for air flow). To ensure the mounting is secure, use two to four #12-24 mounting screws for each side of the shelf assembly. Figure 1-3 shows the rack mounting position for the ONS 15327.

Figure 1-3 Mounting an ONS 15327 in a Rack



1.2.3 Mounting Multiple Nodes

Most standard seven-foot racks can hold 12 ONS 15327s and a fuse and alarm panel.

1.3 Power and Ground Description

This section describes how to connect the ONS 15327 shelf assembly to the power supply. Terminate the chassis ground to either the office ground or rack ground before you install the power. Use the grounding lug to attach the ground cable to the shelf assembly according to local site practice.

Warning **This equipment must be grounded.**

Warning **When installing the node, you must connect the ground first and disconnect it last.**

Ground one cable to ground the shelf assembly. Terminate the other end of the rack ground cable to ground according to local site practice.

If the system loses power or both XTC cards are reset, you must reset the ONS 15327 clock unless the node has been previously provisioned to use Simple Network Time Protocol (SNTP) to update the clock over the LAN.

Warning **Do not apply power to the ONS 15327 until you complete all installation steps.**

Warning **Before performing any of the following procedures, ensure that the power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

Caution Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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

Use the following wiring conventions:

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

Note Use an external disconnect for service purposes and install it according to local site practice.

The ONS 15327 has redundant -48 VDC power terminals on the Mechanical Interface Cards. The terminals are labeled PWR A and PWR B and are located on the far right-hand side of the MICs if you are facing the shelf assembly. Both MIC A and MIC B must be installed to create redundant power connections.

To install redundant power feeds, use four power cables and one ground cable. For a single power feed, only two power cables and one ground cable are required. Use #12 AWG cable and, to ensure circuit overcurrent protection, use a conductor with low impedance. However, the conductor must have the capability to safely conduct any fault current that might be imposed. Do not use aluminum conductors.

The MIC power connector is shipped with the fastening screws inserted but not tightened. The screws may have tightened due to vibration during shipping. Make sure the screws are loose before attempting to remove the connector.

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

Warning **Connect the unit only to DC power source that complies with the Safety Extra-Low Voltage (SELV) requirements in IEC 60950 based safety standards.**

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

Figure 1-4 shows the MIC power connector being removed.

Figure 1-4 Removing the MIC Power Connector

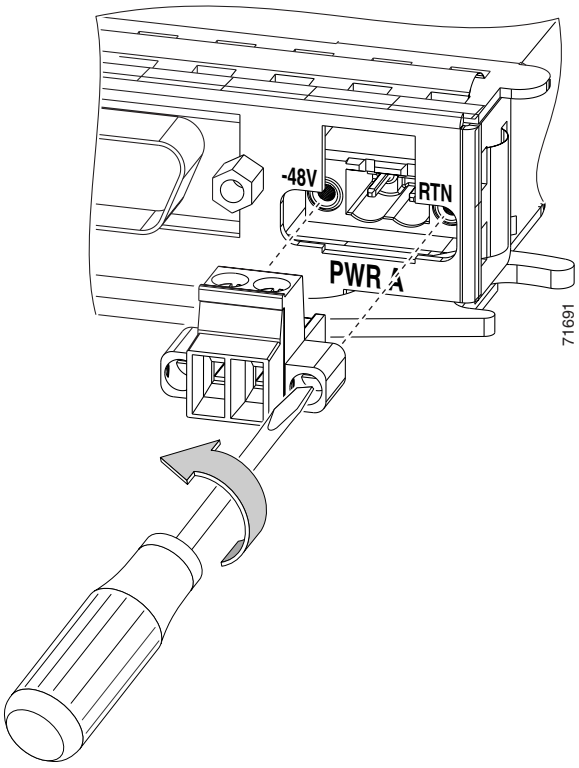


Figure 1-5 shows a power cable being inserted into the MIC power connector.

Figure 1-5 Inserting a Power Cable into the MIC Power Connector

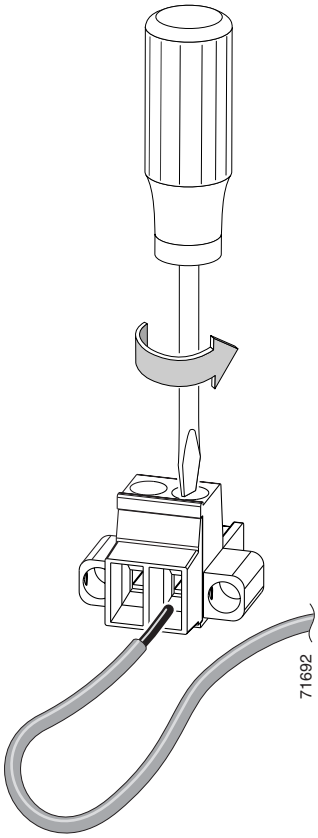


Figure 1-6 shows the MIC power connector being installed.

Figure 1-6 Installing the MIC Power Connector

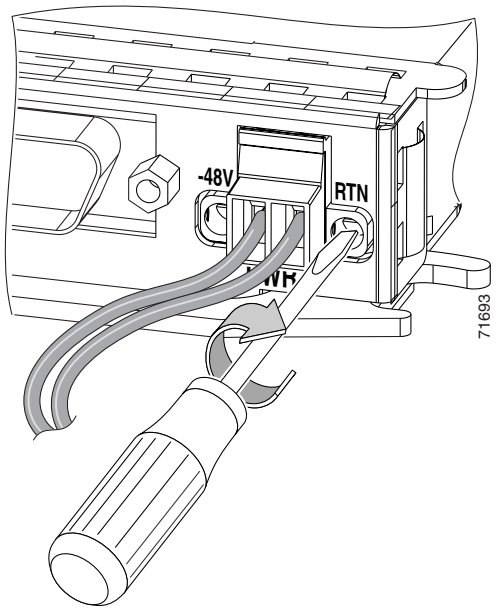
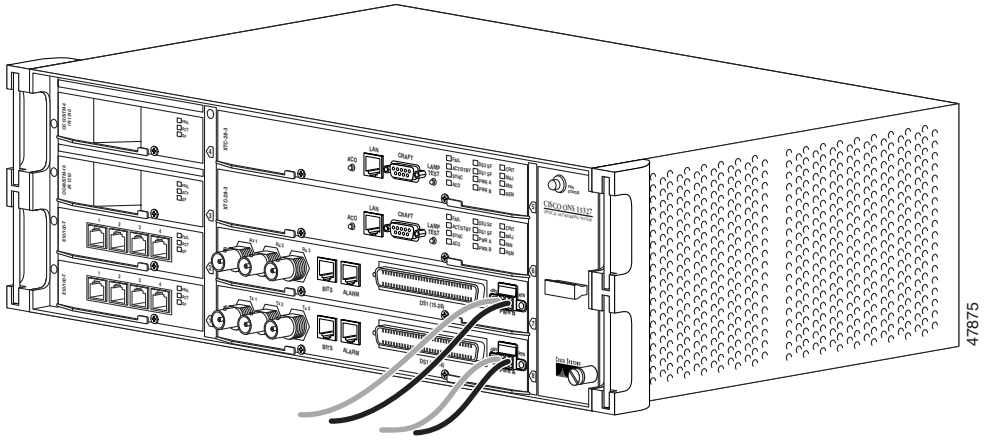


Figure 1-7 shows redundant power connected to an ONS 15327.

Figure 1-7 Redundant Power Connected to an ONS 15327



1.4 Ferrites

Place third-party ferrites on power cables to dampen electromagnetic interference (EMI) from the ONS 15327. Ferrites must be added to meet the requirements of GR 1089. Refer to the ferrite manufacturer documentation for proper use and installation of the ferrites.

1.5 Cable Description and Installation

This section describes fiber-optic, DS-3 (coaxial), DS-1 (Champ), and twisted-pair cables.

1.5.1 Cabling Types

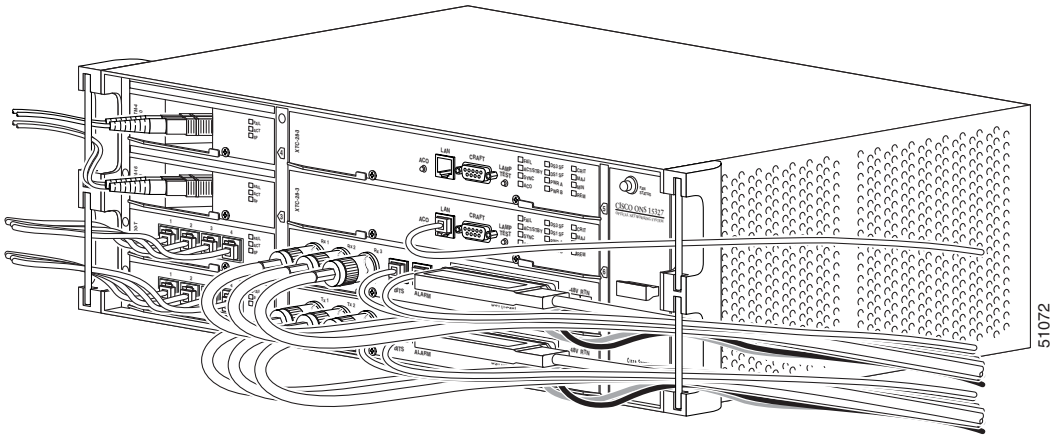
ONS 15327 cables use cable guides at each side of the front of the shelf assembly to economize shelf space and facilitate cable management. The following types of cables are used with the ONS 15327:

- Optical cables: Optical cables connect to the SC connectors on the faceplate of the OC-12 and OC-48 cards and the LC connectors on the OC-3 cards (described in the "Fiber Cable Installation" section on page 1-13). Make sure the fiber cables do not bend excessively; maintaining a proper bend radius prevents damage to the optical cable.
- Coaxial cables: Coaxial cables connect to the MICs on the ONS 15327 using BNC cable connectors. Coaxial cables carry DS-3 traffic to and from the ONS 15327. The ONS 15327 supports up to three transmit and three receive coaxial connectors on each shelf assembly.
- AMP Champ cables: AMP Champ cables connect to MICs on the ONS 15327 using AMP Champ cable connectors. Each Champ connector on the MIC supports one AMP Champ cable connection for a total of two connectors per node. Each Champ connector supports a maximum of 14 DS-1s. See the "DS-1 Cable Installation" section on page 1-15 for more information about the AMP Champ cables and connectors.
- Twisted-pair cables for timing: Twisted-pair cables for timing connect to the BITS ports on the MICs. The twisted-pair cables for timing use RJ-45 connectors. Connecting to the BITS ports requires a BITS clock cable, twisted-pair #22 or #24 shielded AWG wire.
- Category 5 Twisted-Pair cables: Category 5 Twisted-Pair cables connect to the ports on the E-Series Ethernet card, the alarm ports on the MICs, and the LAN port on the XTC cards. The twisted-pair cables use RJ-45 connectors. The Ethernet card ports and the LAN ports use a standard straight-through cable.

1.5.2 Cable Guides

The ONS 15327 has cable guides located on each side of the front of the shelf assembly (see Figure 1-8). The cable guides ensure that the proper bend radius is maintained in the fibers and that all other cables are properly routed. To remove cable guides, take out the screws that anchor them to the side of the shelf assembly.

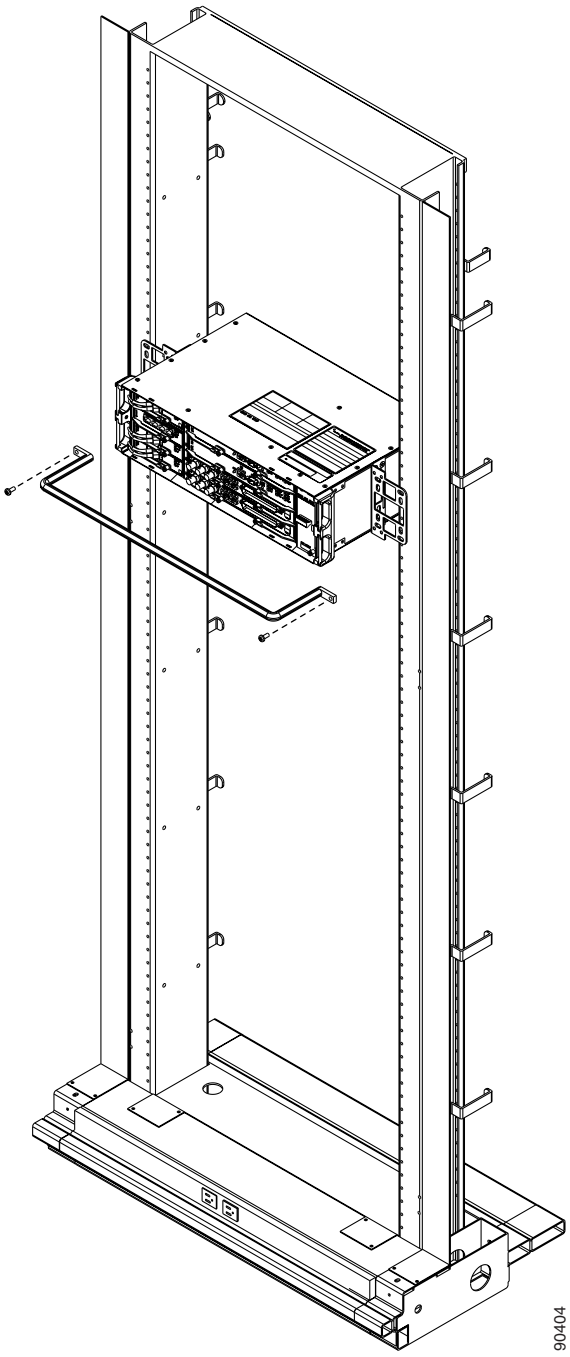
Figure 1-8 Managing Front Panel Cables with Locking Cable Guides



For easier strain relief, you can also use the optional tie-down bar to secure the cables using tie-wraps or other site-specific methods.

Figure 1-9 on page 1-12 shows the tie-down bar, the ONS 15327, and the rack.

Figure 1-9 Tie-Down Bar



1.5.3 Cabling Sequence and Location

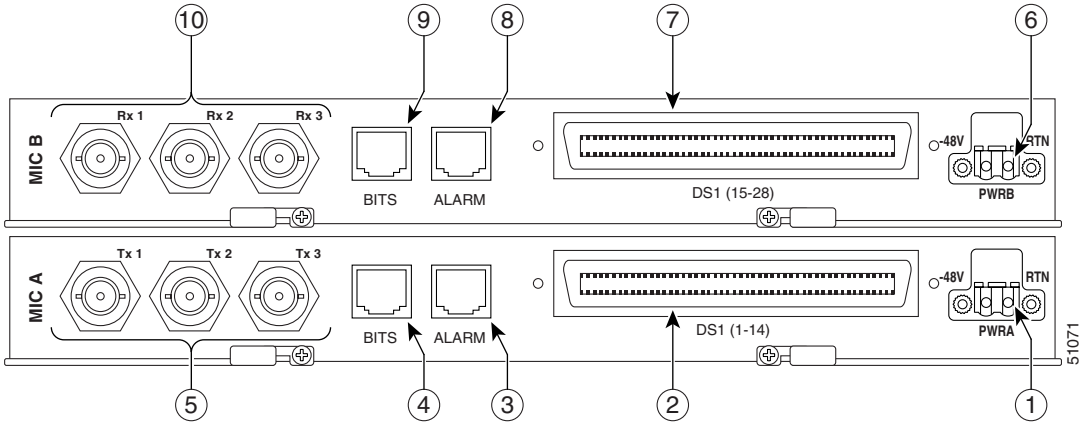
The two cable management considerations are the sequence of cable installation and the location of cable routing. To maintain access to all of the connectors during cable installation, cables must be attached to the MICs in the following order starting with MIC A (the bottom MIC) and repeating for MIC B:

1. Attach power cables
2. Attach DS-1 (Champ) cables
3. Attach Alarm (RJ-45) cables
4. Attach BITS (RJ-45) cables
5. Attach DS-3 (BNC) cables

After attaching all of the cables to the MICs, route the cables out through the bottom right cable guide and snap it closed. Tie wrap the cables according to local site practice. Leave enough slack to remove the fan-tray assembly and fan filter.

You do not need to connect cables for the XTC cards and traffic cards in any particular order. Route XTC cables through the top right cable guide. Route electrical and fiber-optic cables out through the corresponding cable guides on the left side of the shelf assembly. Figure 1-10 shows the order in which you should install cables on the ONS 15327.

Figure 1-10 Cable Installation Sequence



1.5.4 Fiber Cable Installation

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top traffic and XTC slots.

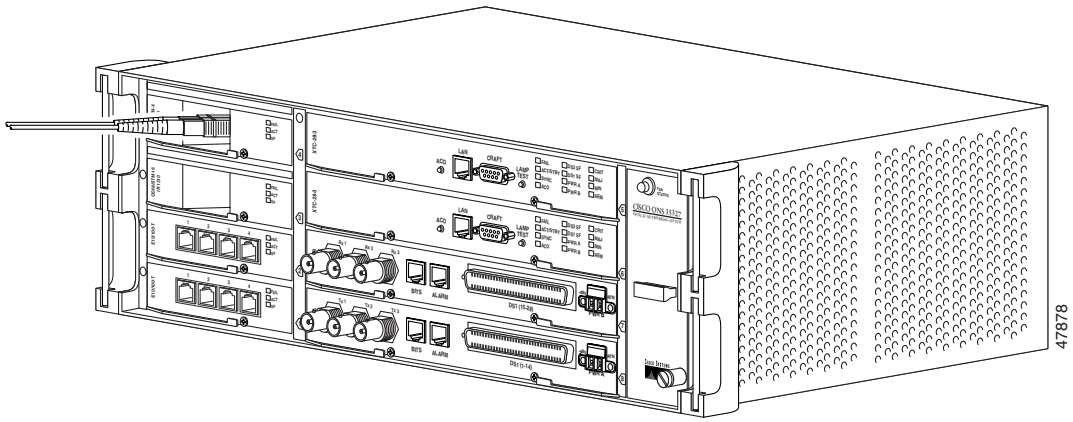
ONS 15327 OC-12 and OC-48 cards have SC connectors and the OC-3 and G1000-2 cards have LC connectors. To install fiber-optic cables in the ONS 15327, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the ONS 15327 cards (see Figure 1-11 on page 1-14). On ONS 15327 OC-12 and OC-48 card ports, the left side connector is the

transmit port and the right side connector is the receive port. Cisco recommends that you label the transmit and receive ports and the working and protection fibers at each end of the fiber span to avoid confusion with cables that are similar in appearance.

Warning **Invisible laser radiation can be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation do not stare into open apertures.**

Note Clean all fiber connectors thoroughly. Dust particles can degrade performance. Put caps on any fiber connectors that you do not use.

Figure 1-11 Installing a Fiber-optic Cable



1.5.5 Coaxial Cable Installation

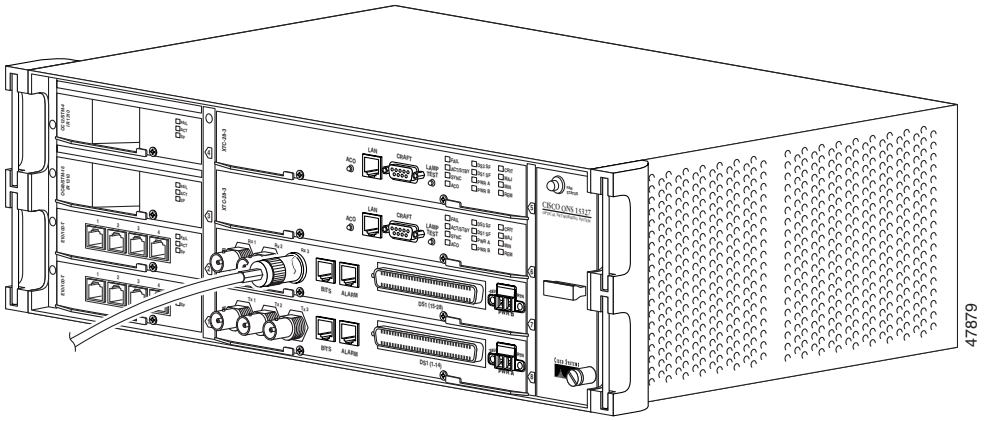
For DS-3 traffic the ONS 15327 uses coaxial cables and connectors. Cisco recommends connecting an RG-59/U cable to a patch panel; RG-59/U cable is designed for long runs of up to 450 feet. Use a compatible straight male BNC connector to connect the cable to the DS-3 ports on the MICs. The transmit (TX) ports on MIC A and the receive (RX) ports on MIC B use the same type of connector.

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

Caution Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Figure 1-12 shows how to connect a coaxial cable to the ONS 15327 MIC.

Figure 1-12 Installing a Coaxial Cable with BNC Connectors



1.5.6 DS-1 Cable Installation

DS-1 ports support AMP Champ connector cabling. Installing AMP Champ connector DS-1 cables requires 64-pin bundled cable connectors with a 64-pin male AMP Champ connector.

Cisco offers these DS-1 cables in various lengths (product # 15327-AMP-WW-30=, 15327-AMP-WW-50=, 15327-AMP-WW-100=, or 15327-AMP-WW-250=, lengths 30, 50, 100, or 250 feet, respectively), including a straight connector for use with the Cisco tie-down bar (product # 15327-TIE-BAR-19= or 15327-TIE-BAR-23= for 19-inch or 23-inch racks, respectively).

You need AMP Champ connector #552285-1 for the plug side and #1-552496-1 for the right-angle shell housing, or their functional equivalents. The corresponding 64-pin female AMP Champ connector on the MIC supports one receive (in) and one transmit (out) for each DS-1 port for the corresponding XTC.

Because each MIC DS-1 connection supports 14 DS-1 ports, only 56 pins (28 pairs) of the 64-pin connector are used. Prepare one 56-wire cable for each DS-1 connection. Table 1-1 shows the pin assignments for the Champ connectors on the ONS 15327 MICs.

Note The shaded area in Table 1-1 corresponds to the white/orange binder group.

Table 1-1 Pin Assignments for Champ Connector

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 yellow/orange	17	49	Rx Ring 1 orange/yellow
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 yellow/green	18	50	Rx Ring 2 green/yellow
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 yellow/brown	19	51	Rx Ring 3 brown/yellow
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 yellow/slate	20	52	Rx Ring 4 slate/yellow
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet

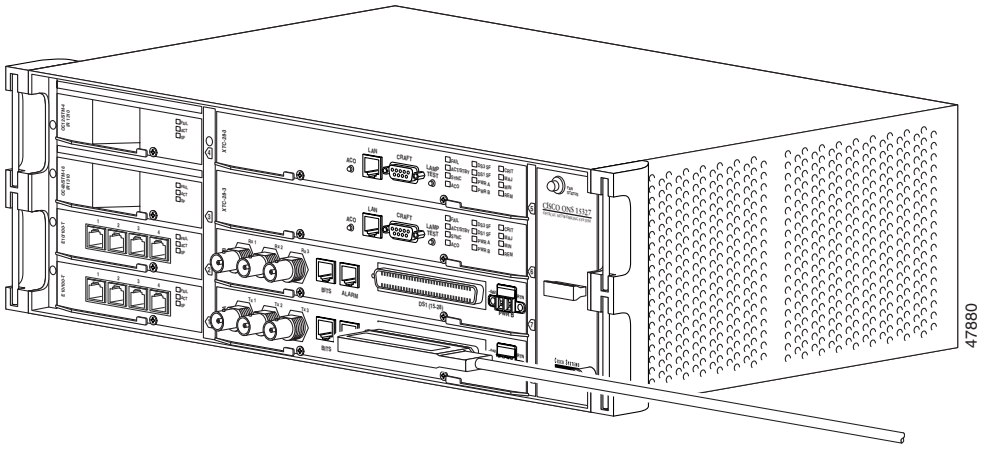
Table 1-1 Pin Assignments for Champ Connector (continued)

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare 0+ N/A	15	47	Tx Spare0- N/A	Rx Spare0+ N/A	31	63	Rx Spare 0- N/A
Tx Spare 1+ N/A	16	48	Tx Spare1- N/A	Rx Spare1+ N/A	32	64	Rx Spare 1- N/A

Note Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top traffic slots and XTC slots.

Figure 1-13 shows DS-1 cable installation.

Figure 1-13 Installing a DS-1 Cable



1.5.7 Alarm Cable Installation

The alarm cables attach to the MICs using twisted-pair cables terminated with an RJ-45 connector on the end that plugs into the ALARM port. The other end of the cable plugs into the alarm-collection equipment. Terminate this end of the cable according to local site practice.

The pins on the ALARM port correspond to the six external alarm inputs and the two external alarm outputs (controls) that you can define using CTC. Alarms 2, 4, and 6 correspond to MIC A and alarms 1, 3, and 5 correspond to MIC B. Alarm output 1 corresponds to MIC B and alarm output 2 corresponds to MIC A. Table 1-2 shows the input alarm pinouts and the corresponding alarm numbers assigned to each MIC port. Table 1-3 shows the output alarm pinouts.

Table 1-2 Alarm Input Pin Assignments

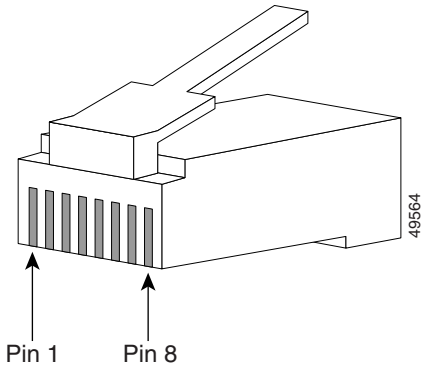
Alarm Input Number (MIC A)	Alarm Input Number (MIC B)	RJ-45 Pin Number	Function
2	1	5	Alarm 2+
		6	Alarm 2–
4	3	3	Alarm 1+
		4	Alarm 1–
6	5	1	Alarm 0+
		2	Alarm 0–

Table 1-3 Alarm (External Control) Output Pin Assignments

Alarm Output Number (MIC A)	Alarm Output Number (MIC B)	RJ-45 Pin Number	Function
2	1	7	Contact+
		8	Contact–

Figure 1-14 shows RJ-45 pin numbering.

Figure 1-14 Pins 1 and 8 on the RJ-45 Connector



1.5.8 BITS Cable Installation

The BITS cables attach to the MICs using BITS clock cable, twisted-pair #22 or #24 shielded AWG wire terminated with an RJ-45 connector on the end that plugs into the BITS port. The other end of the cable plugs into the BITS clock. Terminate this end of the cable according to local site practice.

Each MIC has one BITS input and one BITS output. The BITS inputs and outputs have corresponding pins on the RJ-45 BITS ports. The BITS 1 inputs and outputs are on MIC A and the BITS 2 inputs and outputs are on MIC B. When connecting BITS cable to the ONS 15327, see Table 1-4 for the BITS cable pin assignments. Figure 1-15 on page 1-19 shows the BITS In pins on the RJ-45 connector and Figure 1-16 on page 1-19 shows the BITS Out pins on the RJ-45 connector.

Table 1-4 BITS Cable Pin Assignments

MIC A	MIC B	RJ-45 Pin Number	Function
BITS 1 In	BITS 2 In	3	BITS Input+
		4	BITS Input–
BITS 1 Out	BITS 2 Out	7	BITS Output+
		8	BITS Output–

Figure 1-15 BITS In Pins on the RJ-45 Connector

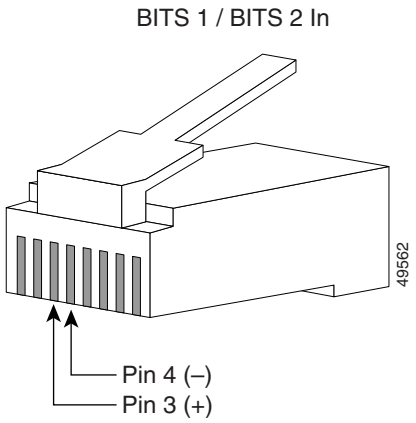
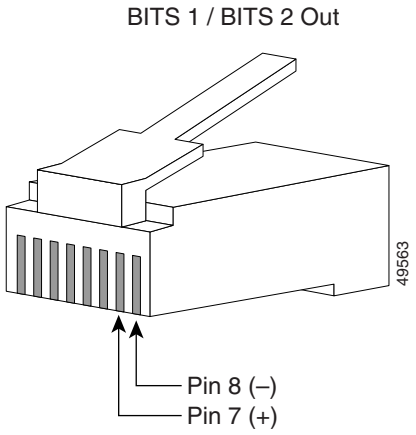


Figure 1-16 BITS Out Pins on the RJ-45 Connector



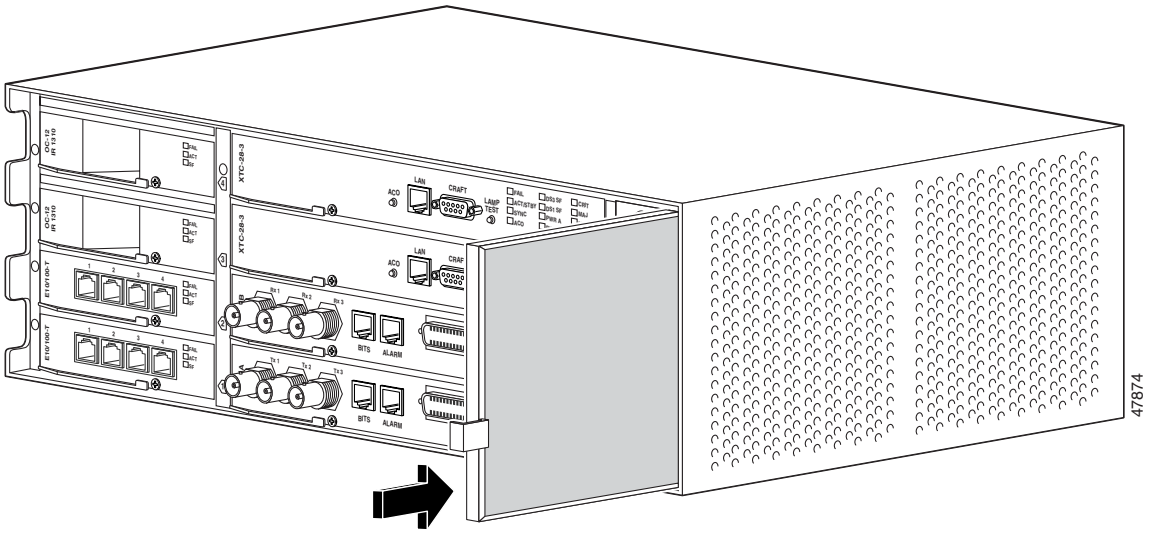
1.6 Fan-Tray Assembly

Facing the front of the ONS 15327, the fan-tray assembly is located on the far right side. The fan-tray assembly is a removable drawer that holds fans and fan-control circuitry for the ONS 15327. After you install the fan-tray assembly, you should not need to remove it unless a fan failure occurs.

The fan-tray assembly has an air filter on the right side of the fan-tray assembly that you can install and remove by hand. Remove and visually inspect this filter every 30 days. For inspection procedures, see the *ONS 15327 Procedure Guide*. Spare filters should be kept in stock. If you are replacing the air filter, you must first move aside the cables that cross in front of it. You must install the air filter with its metal bracing against the fan-tray assembly.

Figure 1-17 on page 1-20 shows the location of the fan tray air filter.

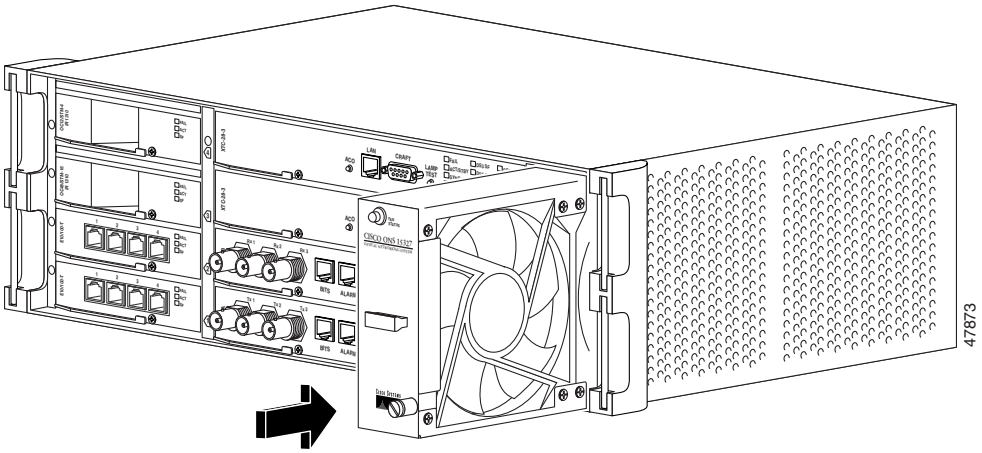
Figure 1-17 Fan-Tray Air Filter



Caution Do not force the fan-tray assembly into place while installing it. Forcing the fan-tray assembly into place can damage the connectors on the fan tray and/or the connectors on the back panel of the shelf assembly.

Figure 1-18 shows the location of the fan-tray assembly.

Figure 1-18 Fan-Tray Assembly



1.7 Alarm Cutoff

Visual and audible alarms are typically wired to trigger an alarm light at a central alarm collection point when the corresponding contacts are closed. The alarm cutoff (ACO) function stops (turns off) the alarm signal being transmitted to the alarm collection point.

To activate the ACO function, press the ACO button on the XTC card faceplate. The ACO button clears all audible alarm indications. After clearing the audible alarm indication, the alarm is still present on the Alarms tab in Cisco Transport Controller (CTC) and appropriate action is needed to clear the alarm. For information about connecting to alarm collection equipment, refer to the *Cisco ONS 15327 Procedure Guide*.

1.8 Timing Installation

The ONS 15327 supports two Building Integrated Timing Supply (BITS) clock interfaces. The physical connection is provided through an RJ-45 connector on each MIC. Two pins on each RJ-45 are used for BITS timing. BITS 1 In (MIC A) and BITS 2 In (MIC B) use pins 3 and 4. BITS 1 Out (MIC A) and BITS 2 Out (MIC B) use pins 7 and 8. The BITS 1 pins support output and input from the first external timing device. The BITS 2 pins perform the identical functions for the second external timing device. Table 1-5 lists the pin assignments for the BITS timing pin fields. For more information about connecting BITS timing to the ONS 15327, refer to the *Cisco ONS 15327 Procedure Guide*.

Table 1-5 External Timing Pin Assignments for BITS

External Device	Contact	RJ-45 Pin	Tip & Ring	Function
First external device (MIC A)	BITS 1 Out	7	Primary ring (–)	Output to external device
	BITS 1 Out	8	Primary tip (+)	Output to external device
	BITS 1 In	3	Secondary ring (–)	Input from external device
	BITS 1 In	4	Secondary tip (+)	Input from external device
Second external device (MIC B)	BITS 2 Out	7	Primary ring (–)	Output to external device
	BITS 2 Out	8	Primary tip (+)	Output to external device
	BITS 2 In	3	Secondary ring (–)	Input from external device
	BITS 2 In	4	Secondary tip (+)	Input from external device

Note Refer to Telcordia SR-NWT-002224 for rules about how to provision timing references.

1.9 Cards and Slots

Caution Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

ONS 15327 cards have electrical plugs at the back that plug into electrical connectors on the shelf assembly backplane. When the ejectors are fully closed, the card plugs into the assembly backplane. Figure 1-19 on page 1-23 shows the slot numbering.

Warning **The optical cards for the ONS 15327 are Class 1 laser products. These products have been tested and comply with Class 1 limits.**

Note DS-1 and DS-3 interfaces are not intended for direct connection to the network. These interfaces should be connected to the network via a CSU/DSU that has the proper certification.

1.9.1 Slot Requirements

The ONS 15327 shelf assembly has eight card slots; four traffic card slots (Slots 1 to 4), two Cross-Connect, Timing and Control (XTC) slots (Slots 5 and 6), and two MIC slots (Slots 7 and 8). The wider slots host the XTC cards and MICs. The narrower slots host Ethernet, OC-3, OC-12, and OC-48 cards.

The XTC slots host both XTC-14 and XTC-28-3 cards. XTC cards are required for system operation. The MIC slots host MIC A and MIC B cards. The MIC slots are keyed to ensure that you install the MICs in the correct slot. Install MIC A in the bottom MIC slot (Slot 8) and MIC B in the top MIC slot (Slot 7). MICs are also required for system operation. Make DS-1 and DS-3 connections using the connectors on the MICs. Refer to Chapter 2, "Card Reference" for more information about ONS 15327 cards.

Table 1-6 lists the number of ports, line rates, connector options, and connector locations for ONS 15327 optical, electrical, and Ethernet interfaces.

Table 1-6 Port Line Rates, Connector Types, and Locations

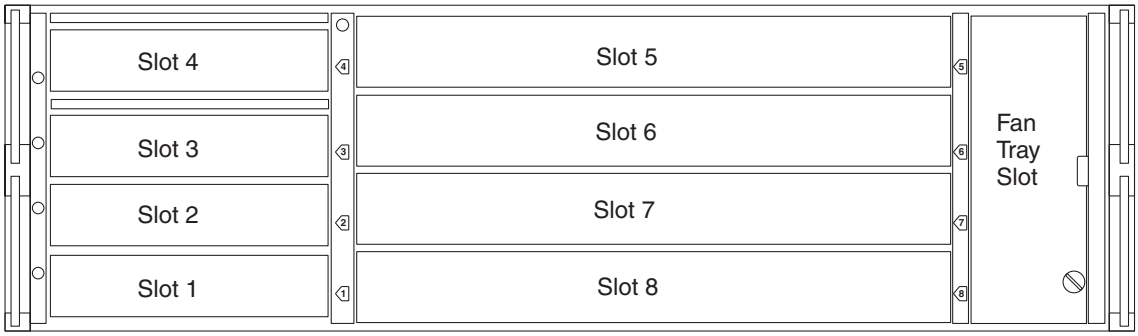
Interface	Ports	Line Rate per Port	Connector Types	Connector Location
DS-1	1–28	1.544 Mbps	CHAMP Connector	MIC faceplate
DS-3	3	44.736 Mbps	BNC	MIC faceplate
E10/100-4	4	10/100 Mbps	RJ-45	E10/100-4 card faceplate
G1000-2	2	1000 Mbps	LC (GBIC)	E1000-2 card faceplate
OC-3 IR 1310	4	155.52 Mbps (STS-3)	LC	OC-3 IR 1310 card faceplate
OC-12 IR 1310	1	622.08 Mbps (STS-12)	SC	OC-12 IR 1310 card faceplate
OC-12 LR 1550	1	622.08 Mbps (STS-12)	SC	OC-12 LR 1550 card faceplate
OC-48 IR 1310	1	2488.32 Mbps (STS-48)	SC	OC-48 IR 1310 card faceplate
OC-48 LR 1550	1	2488.32 Mbps (STS-48)	SC	OC-48 LR 1550 card faceplate

1.9.2 Card Installation

The procedure for installing ONS 15327 cards is slightly different for each card. Before installing any XTC or traffic cards, install at least one MIC and apply power to the shelf assembly. First install MIC A in Slot 8. After successfully connecting the power to MIC A, install MIC B followed by the XTC cards. Install any traffic cards after you have successfully installed and turned up the XTC cards and MICs.

Figure 1-19 shows the location and number of each card slot.

Figure 1-19 ONS 15327 Slot Numbering



Note Because all traffic cards boot from the working XTC card, at least one XTC card must be installed in order to boot any traffic cards.

Warning **Invisible laser radiation can be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation and do not stare into open apertures.**

Figure 1-20 shows XTC card installation.

Figure 1-20 Installing an XTC Card (XTC 28-3)

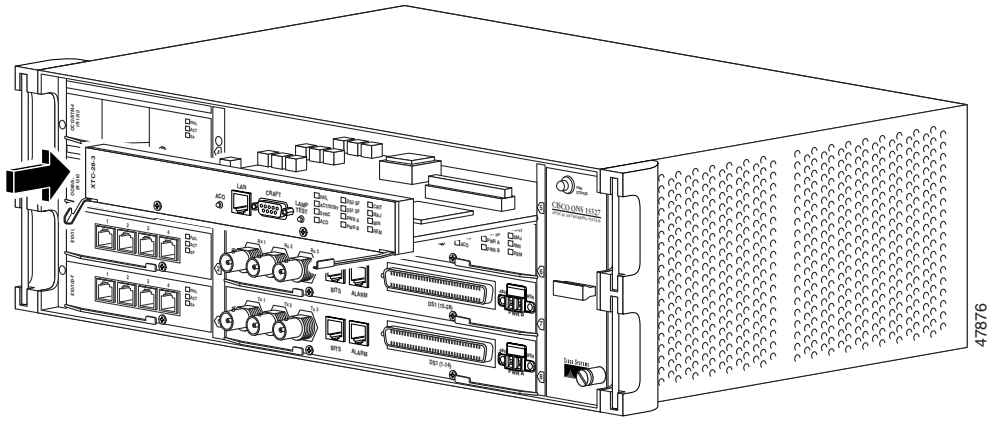
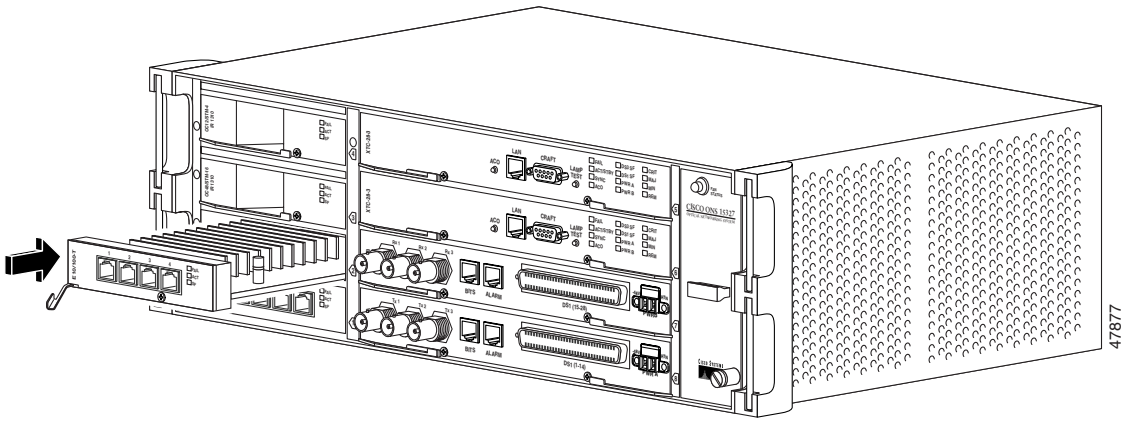


Figure 1-21 shows traffic card installation.

Figure 1-21 Installing a Traffic Card (E10/100-T)



Warning **Install blank faceplates into empty card slots. Blank faceplates serve three functions: They prevent exposure to hazardous voltages and currents inside the ONS 15327 chassis, they eliminate 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 and faceplates are in place.**

1.10 Hardware Specifications

The following sections list the hardware specifications for the ONS 15327 shelf assembly.

1.10.1 Slot Assignments

- Total card slots: 8
- Traffic slots (E10/100-4, G1000-2, OC-3, OC-12, and OC-48): Slots 1– 4
- XTC (Cross Connect, Timing and Control): Slots 5, 6
- MIC (Mechanical Interface Card): Slots 7, 8

1.10.2 Cards

- XTC-14
- XTC-28-3
- MIC A
- MIC B
- E10/100-4
- G1000-2
- OC-3 IR 4 1310
- OC-12 IR 1310

- OC-12 LR 1550
- OC-48 IR 1310
- OC-48 LR 1550

1.10.3 Configurations

- Point-to-point terminal
- Add-drop multiplexer
- Two-fiber UPSR
- Path-protected mesh network (PPMN)
- Two-fiber BLSR (OC-12 and OC-48 cards only)

1.10.4 Cisco Transport Controller

- 10 Base-T
- XTC access: RJ-45 connector

1.10.5 External LAN Interface

- 10 Base-T Ethernet

1.10.6 TL1 Craft Interface

- Speed: 9600 bps
- XTC access: RS-232 DB-9 type connector

1.10.7 Modem Interface

- Hardware flow control
- XTC: RS-232 DB-9 type connector

1.10.8 Alarm Interface

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

1.10.9 Database Storage

- Nonvolatile memory: 96 MB, FLASH memory

1.10.10 BITS Interface

- 2 DS-1 BITS inputs
- 2 derived DS-1 outputs

1.10.11 System Timing

- Stratum 3, compliant with Telcordia GR-253-CORE
- Free running accuracy: ± 4.6 ppm
- Holdover Stability: 3.7 x10 -7 /day, including temperature (< 255 slips in first 24 hours)
- Reference: External BITS, line, internal

1.10.12 Power Specifications

- Input power: -48 VDC
- Power consumption: 260 W (maximum draw w/cards)
- Power Requirements: -42 to -56 VDC
- Power terminals: Removable screw-locking (#12-14 AWG)

1.10.13 Environmental Specifications

- Operating Temperature: 0 to +55 degrees Celsius
- Operating Humidity: 5 - 95%, non-condensing

The FTA is required to fulfill environmental specifications.

1.10.14 Dimensions

- Height: 5.1 inches (13 cm)
- Width:19 or 23 inches (48.3 or 58.4 cm) with mounting ears attached
- Depth: 11 inches (28 cm)
- Weight: 15 lbs., empty (with fan-tray assembly); 27 lbs, maximum

CHAPTER 2

Card Reference

This chapter describes the Cisco ONS 15327 cards. It includes descriptions, hardware specifications, and block diagrams for each card. For installation and turn-up procedures, refer to the *Cisco ONS 15327 Procedure Guide*.

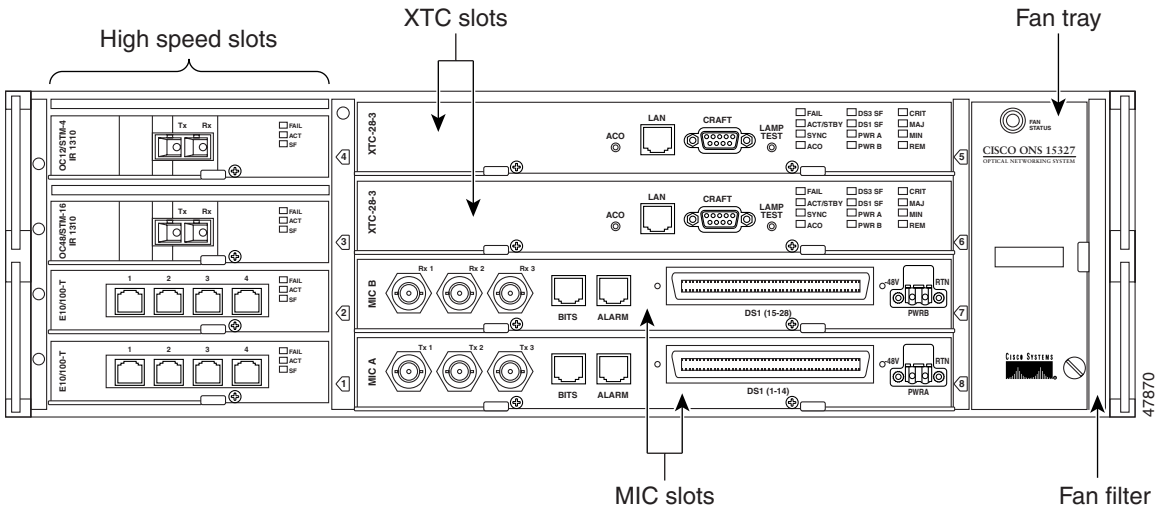
Chapter topics include:

Note The I-Temp symbol is displayed on the faceplate of an I-Temp compliant card. A card without this symbol is C-Temp compliant.

2.1 Overview

The Cisco ONS 15327 uses common control cards, mechanical interface cards, optical cards, and an Ethernet/fast Ethernet card. This overview provides a summary of the cards. Figure 2-1 on page 2-2 shows the ONS 15327 slot assignments.

Figure 2-1 ONS 15327 Slot Assignments



2.1.1 Common Control Cards

The two common control cards are the XTC-28-3 card and the XTC-14 card. Both cards provide timing, control, and digital cross-connect functions. They also provide the EIA/TIA-232 DB9 TL1 connection and RJ-45 LAN connection. The XTC-28-3 provides electrical-tributary circuitry for 28 DS-1s and three DS-3s. The XTC-14 provides electrical-tributary circuitry for 14 DS-1s.

2.1.2 Mechanical Interface Cards

The MICs provide the physical connection points for the DS-1 and DS-3 interfaces on the XTC cards, the redundant power inputs, the alarm inputs and outputs, and the building integrated timing supply (BITS) inputs and outputs.

2.1.3 Optical Cards

The optical cards include the OC3 IR 4 1310, the OC12 IR 1310, the OC12 LR 1550, the OC48 IR 1310, and the OC48 LR 1550. The OC3 IR 4 1310 card provides four intermediate-reach OC-3 interfaces. The OC12 IR 1310 card provides one intermediate- or short-reach OC-12 interface, and the OC12 LR 1550 provides one long-reach OC-12 interface. The OC48 IR 1310 card provides one intermediate-reach OC-48 interface and the OC48 LR 1550 provides one long-reach OC-48 interface.

2.1.4 Ethernet Card

The Ethernet card provides four Layer 2 switched, autosensing, 10/100BaseT Ethernet interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 Mbps per port.

2.1.5 Gigabit Ethernet Card

The Gigabit Ethernet card provides two 1000-Mbps Gigabit Ethernet interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 2000 Mbps per port.

2.2 XTC Cards

This section describes the features and functions of the XTC cards. The ONS 15327 has two XTC cards, the XTC-28-3 and the XTC-14 card.

2.2.1 XTC Card Description

The XTC cards perform system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection and resolution, SONET DCC (data communication channel) termination, system fault detection, and cross-connect maintenance and management for the ONS 15327. The XTC cards also provide the circuitry for the DS-1 and DS-3 interfaces and ensure that the system maintains Telcordia timing requirements.

An XTC card is required to operate the ONS 15327 and can be used in a redundant or nonredundant configuration. Figure 2-2 shows the XTC-28-3 faceplate.

Note You can connect to either the active or standby XTC using the LAN or CRAFT port, but you cannot connect to both cards simultaneously. Connecting to both the active and standby XTC at the same time results in a loss of connectivity.

Figure 2-2 XTC-28-3 Card Faceplate

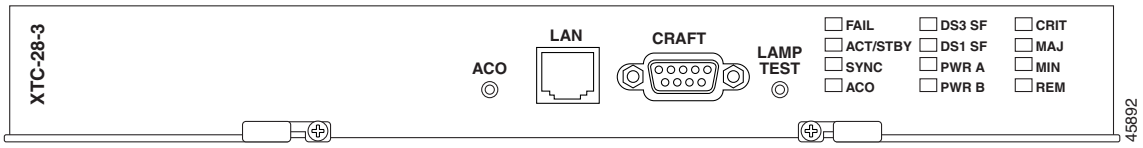
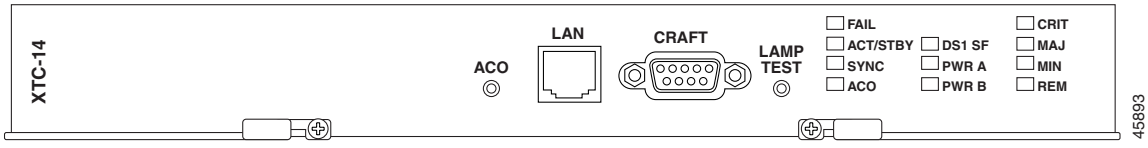


Figure 2-3 shows the XTC-14 faceplate.

Figure 2-3 XTC-14 Card Faceplate



2.2.1.1 XTC Front Panel

The XTC cards have an alarm cutoff (ACO) button, an RJ-45 LAN port, an EIA/TIA-232 TL1 (CRAFT) interface port, and a LAMP TEST button. The XTC-28-3 front panel has 12 LEDs, and the XTC-14 front panel has 11. The following list describes each LED:

- The red FAIL LED indicates an XTC hardware problem. Replace the card if the FAIL LED persists.
- The ACT/STBY (Active/Standby) LED indicates whether the XTC is active and providing timing reference and shelf control (green), or is in standby to the active XTC (amber).
- The green SYNC LED illuminates when the active XTC qualifies a timing reference from the optical facility or an external BITS input.
- The ACO LED indicates that the ACO function has been activated. To activate the ACO, press the ACO button on the front panel.
- The DS3 SF LED (XTC-28-3 only) indicates a signal fail with one or more of the DS-3 interfaces.
- The DS1 SF LED indicates a signal fail with one or more of the DS-1 interfaces.
- The green PWR A and PWR B LEDs illuminate when adequate power voltage is being received by the PWR A and PWR B connections on the MIC cards.
- The CRIT LED illuminates when a critical alarm is present.
- The MAJ LED illuminates when a major alarm is present.
- The MIN LED illuminates when a minor alarm is present.
- The red REM LED illuminates when a remote alarm is present in one or several of the remote terminals, or if an external alarm or condition is present.

2.2.1.2 Support for DS-1 and DS-3

The XTC cards contain the circuitry for connecting DS-1s. The XTC-28-3 also contains the circuitry for connecting DS-3s. The XTC-28-3 supports 28 DS-1s and 3 DS-3s. The XTC-14 supports 14 DS-1s. The DS-1 circuitry on the XTC cards maps each of the received DS-1 signals into VT 1.5s and concatenates these virtual tributaries (VTs) into one STS-1. Full VT 1.5 grooming is supported.

The physical connection points are located on the MIC cards. See the "MIC Description" section on page 2-8 for more information about physical connections.

2.2.1.3 XTC Timing and Control Functionality

The XTC cards combine the timing and control functions into one card. You can install the XTC cards in one or both of the control slots (Slots 5 and 6). XTC cards must be installed in both of the control slots for redundancy. In a nonredundant configuration, you must install the XTC in Slot 6.

The XTC cards support multichannel, high-level data link control (HDLC) processing for the DCC. Up to four DCCs can be routed over the serial communication interface (SCI) and terminated at the XTC card. The XTC cards process ten DCCs to enable remote system management interfaces.

Note ONS 15327 Releases 3.3 and later support DCC tunneling of non-Cisco equipment.

The node database, IP address, and system software are stored in XTC card nonvolatile memory, which allows quick recovery in the event of a power or card failure.

The XTC cards perform all system-timing functions for each ONS 15327. The XTC cards select a recovered clock from optical line cards, a building integrated timing supply (BITS), or an internal Stratum 3 reference as the system-timing reference. You can provision any of the clock inputs as a primary or secondary timing source. A slow-reference tracking loop allows the XTC cards to synchronize to the recovered clock, which provides holdover if the reference is lost.

In a redundant configuration, if the working XTC card fails, traffic switches to the protect XTC card. All XTC protection switches conform to protection switching standards when the bit error rate (BER) counts are not in excess of 1 E-3 and completion time is less than 50 ms.

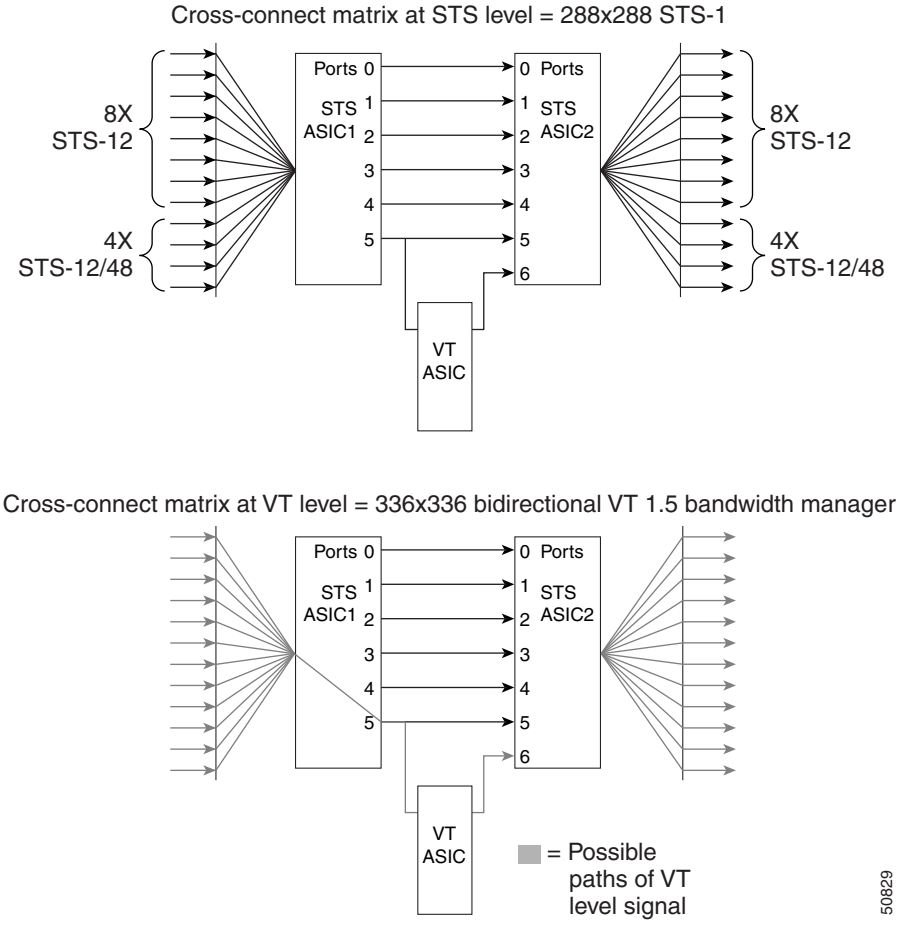
The XTC cards feature an RJ-45 10BaseT LAN port and an EIA/TIA-232 DB9 type craft interface for user interfaces. The craft port runs at 9600 bps.

2.2.1.4 XTC Cross-Connect Functionality

The XTC card is the central element for ONS 15327 switching. It establishes cross connections and performs time-division switching (TDS) at the STS-1 and VT 1.5 level between ONS 15327 traffic cards.

The switch matrix on the XTC card consists of 288 bidirectional ports. When creating bidirectional STS-1 cross-connects, each cross-connect uses two STS-1 ports. This results in 144 bidirectional STS-1 cross-connects. The switch matrix is nonblocking and broadcast supporting. This allows network operators to concentrate or groom low-speed traffic from line cards onto high-speed transport spans and to drop low-speed traffic from transport spans onto line cards. Figure 2-4 shows the cross-connect matrix for the XTC card.

Figure 2-4 Cross-Connect Matrix



The XTC card supports a total of 672 cross-connects with a payload granularity of VT 1.5. The VT functionality supports ring configurations with a mix of VT-capable Cisco transport network elements (NEs) and STS-only capable Cisco transport NEs.

The XTC card provides protection switching control for external and internal VT paths. The card also performs path- and STS-level monitoring and protection switching.

2.2.2 VT Mapping

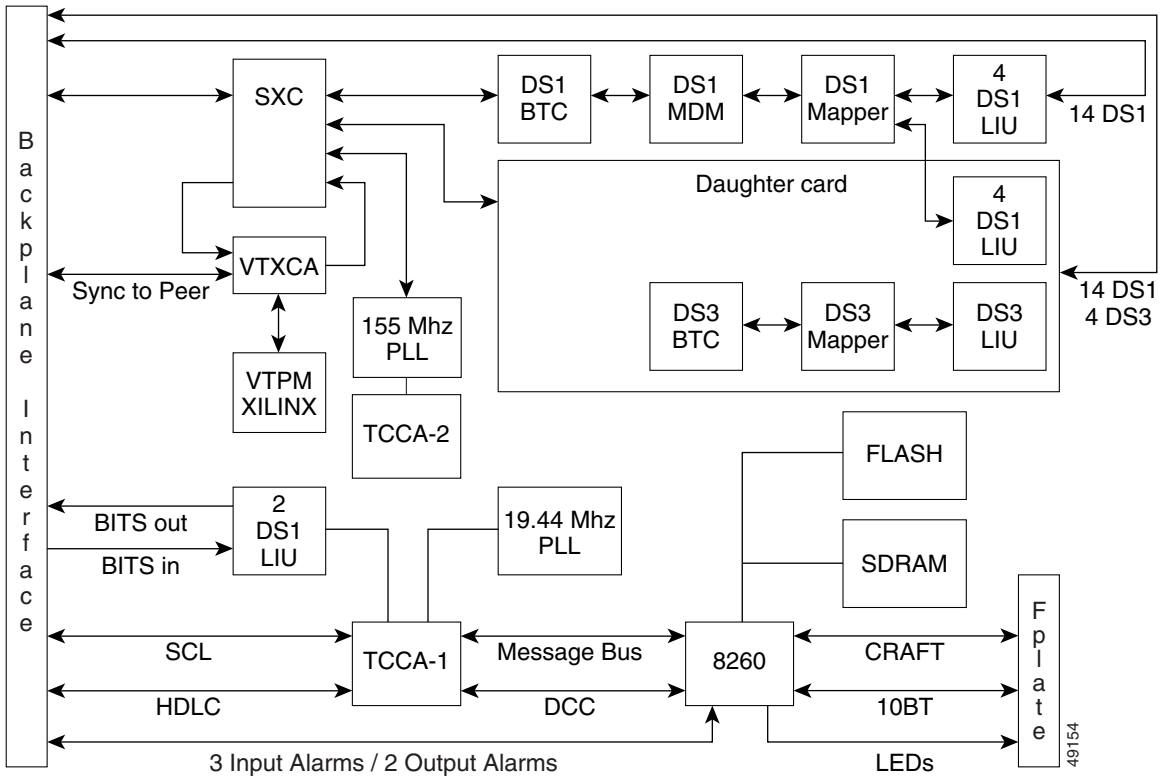
The Cisco ONS 15327 performs VT mapping according to Telcordia GR-253 standards. Table 2-1 shows the VT numbering scheme for the ONS 15327 as it relates to the Telcordia standard.

Table 2-1 VT Mapping

ONS 15327 VT Number	Telcordia Group/VT Number
VT1	Group1/VT1
VT2	Group2/VT1
VT3	Group3/VT1
VT4	Group4/VT1
VT5	Group5/VT1
VT6	Group6/VT1
VT7	Group7/VT1
VT8	Group1/VT2
VT9	Group2/VT2
VT10	Group3/VT2
VT11	Group4/VT2
VT12	Group5/VT2
VT13	Group6/VT2
VT14	Group7/VT2
VT15	Group1/VT3
VT16	Group2/VT3
VT17	Group3/VT3
VT18	Group4/VT3
VT19	Group5/VT3
VT20	Group6/VT3
VT21	Group7/VT3
VT22	Group1/VT4
VT23	Group2/VT4
VT24	Group3/VT4
VT25	Group4/VT4
VT26	Group5/VT4
VT27	Group6/VT4
VT28	Group7/VT4

Figure 2-5 shows the block diagram for the XTC card.

Figure 2-5 XTC Block Diagram



2.2.3 XTC Card (XTC 28-3/XTC-14) Specifications

- CTC software
  - Interface: 10 Base-T LAN
- TL1 craft interface
  - Speed: 9600 baud
  - Front panel access: EIA/TIA-232 DB9 type connector
- Synchronization
  - Stratum 3, per Telcordia GR-253-CORE
  - Free running access: 4.6 ppm accuracy
  - Holdover stability: 3.7 $x10^{-7}$ ppm/day, including temperature (< 255 slips in first 24 hours)
  - Reference: External BITS, line, internal
- Environmental
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 56 W maximum, 1.17 A, 191 BTU/hr

- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 9.375 in. (238.1 mm)
  - Depth: 9.172 in. (233.0 mm)

2.3 Mechanical Interface Cards

This section describes the features and functions of the MICs.

2.3.1 MIC Description

Two MIC cards (MIC A and MIC B) are required to operate the Cisco ONS 15327 if you are using XTC-28-3 cards and/or you need redundant power inputs. The MICs provide power connection points, physical interfaces for DS-1s and DS-3s, and external timing and alarm interfaces.

Figure 2-6 shows the MIC A faceplate. MIC A is keyed so that it can only be installed in Slot 8.

Figure 2-6 MIC A Card Faceplate

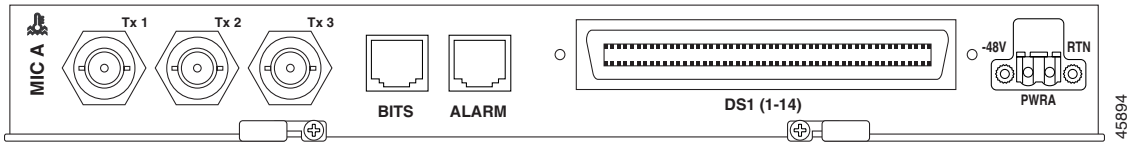
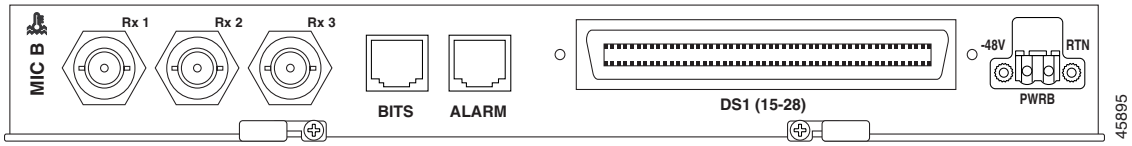


Figure 2-7 shows the MIC-28-3-B faceplate. MIC-B is keyed so that it can only be installed in Slot 7.

Figure 2-7 MIC B Card Faceplate



2.3.1.1 DS-1 Physical Interface

Each MIC uses a 64-pin Champ connector to provide 14 DS-1 interfaces. MIC-28-3-A provides connection to DS-1s 1 to 14, and MIC-28-3-B provides connection to DS-1s 15 to 28. The XTC cards house the electrical tributary circuitry for managing the individual DS-1s.

2.3.1.2 DS-3 Physical Interface

Because transmit (out) and receive (in) interfaces are on different cards, you must install both MICs to use the DS-3 capabilities of the ONS 15327. The DS-3 interfaces use BNC connectors. MIC-28-3-A provides the three transmit (Tx) interfaces and MIC-28-3-B provides the three receive (Rx) interfaces. The XTC-28-3 card houses the electrical-tributary circuitry for managing DS-3s.

2.3.1.3 Power Connection

Each MIC has one –48 VDC power terminal that uses spring terminal block connectors and accepts #12 to #16 AWG wire (the National Electrical Code [NEC] requires #12 to #14 AWG wire). To establish redundant power, install both MICs and connect each one to a power source.

2.3.1.4 External Alarms and Controls

Each MIC has three Form C discrete external alarm inputs and one Form C discrete external control. Connection to the external alarms and controls uses an RJ-45 connector. Two wires of the RJ-45 connector are used for the external control, which defaults to the open position. Six wires of the RJ-45 connector are used for the external alarm input (for additional information, refer to the *Cisco ONS 15327 Procedure Guide*).

In CTC, you can provision the six external alarm inputs (three on each MIC) and the two external controls (one on each MIC). External alarm inputs are typically used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions. They can be set to Alarm on Closure or Alarm on Open. The alarm severity can be set to any of five available levels (Critical, Major, Minor, Not Alarmed, Not Reported). In addition to severity, you can set alarm type and virtual wire for alarm contacts 1 to 4 and define when the alarm is raised. You can assign a 63-character alarm description for display in the alarm log of the CTC. The alarm condition remains until the external input quits driving the contact and you clear the alarm in the CTC. For instructions, refer to the *Cisco ONS 15327 Procedure Guide*.

External controls are typically used to drive visual or audible devices such as bells and lights, but they can control other devices such as generators, heaters, and fans. You can set them to close when the specified alarm condition is triggered; the default condition for output alarms is the open position. The alarm triggering conditions can be any ONS 15327 alarm condition including the user-defined input alarms, severity-based (for example, trigger when any major alarm occurs) alarms, or remote alarms. CTC provisioning of this alarm-to-output-contact association is menu driven and includes alarms and individual alarms within categories. The output contact electrical interface is 50 V, 100 mA. For procedures that provision external controls, refer to the *Cisco ONS 15327 Procedure Guide*.

2.3.1.5 BITS Interface

Each MIC provides connection for one BITS clock input and one BITS clock output using an RJ-45 connector. Both use two wires of the RJ-45 connector.

2.3.2 MIC Specifications

- Environmental
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power Consumption: 4.8 W, 0.1 A, 16.4 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 9.375 in. (238.1 mm)
  - Depth: 9.172 in. (233.0 mm)

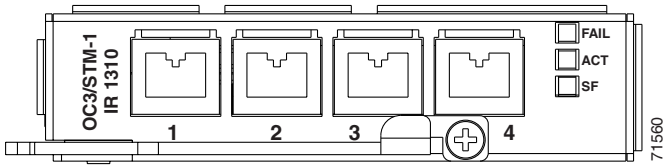
2.4 OC3 IR 4 1310 Card

This section describes the features and functions of the OC3 IR 4 1310 card. For card provisioning, such as changing line and threshold settings, refer to the *Cisco ONS 15327 Procedure Guide*.

2.4.1 OC3 IR 4 1310 Card Description

The OC3 IR 4 1310 card provides four intermediate-reach, Telcordia-compliant, GR-253 SONET OC-3 interfaces per card. The interface operates at 155.52 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1 or STS-3c. Figure 2-8 shows the OC3 IR 4 1310 faceplate.

Figure 2-8 OC3 IR 4 1310 Card Faceplate



You can install the OC3 IR 4 1310 card in any ONS 15327 high-speed card slot. The card can be provisioned as part of a UPSR or a linear add-drop multiplexer (ADM) configuration.The card does not support BLSR. Each port features a 1310 nm laser and contains a transmit and receive connector (labeled, the left-hand connector is the transmit [Tx] port and the right-hand connector is the receive [Rx] port) on the card faceplate. The card uses LC connectors.

The OC3 IR 4 1310 card supports 1+1 unidirectional or bidirectional protection switching. You can provision protection on a per-port basis. See the "Optical Card Protection" section on page 3-2 for more information.

The OC3 IR 4 1310 detects loss of signal (LOS), loss of frame (LOF), loss of pointer (LOP), line alarm indication signal (AIS-L), and line remote defect indication (RDI-L) conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card also counts section and line bit interleaved parity (BIP) errors.

2.4.2 OC3 IR 4 1310 Card-Level Indicators

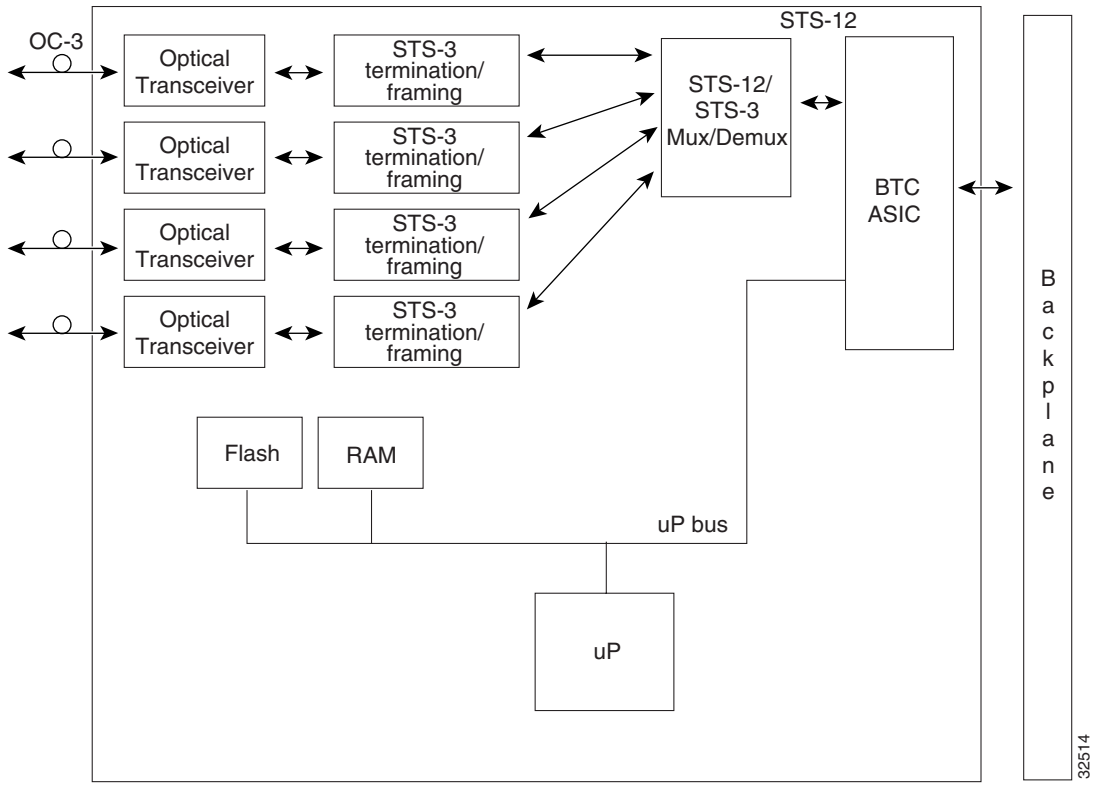
The OC3 IR 4 1310 card has three card-level LED indicators (Table 2-2).

Table 2-2 OC3 IR 4 1310 Card-level Indicators

Card-level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC3 IR 4 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as loss of signal (LOS), loss of frame (LOF), line alarm indication signal (AIS-L), or high bit error rate (BER) on one or more of the card's ports. The amber signal fail (SF) LED also illuminates when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

Figure 2-9 shows the OC3 IR 4 1310 card block diagram.

Figure 2-9 OC3 IR 4 1310 Card Block Diagram



Warning **Invisible laser radiation may be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation, do not stare into open apertures.**

2.4.3 OC3 IR 4 1310 Card Specifications

- Line
  - Bit rate: 155.52 Mbps
  - Code: Scrambled not return to zero (NRZ)
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: LC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Maximum transmitter output power: –8 dBm
  - Minimum transmitter output power: –15 dBm
  - Center wavelength: 1274 nm to 1356 nm

  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: –8 dBm
  - Minimum receiver level: –28 dBm
  - Receiver: InGaAs/InP photo detector
  - Link loss budget: 13 dB
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 14 W, 0.29 A, 48 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

2.5 OC12 IR 1310 Card

This section describes the features and functions of the OC12 IR 1310 card. For card provisioning, refer to the *Cisco ONS 15327 Procedure Guide*.

2.5.1 OC12 IR 1310 Card Description

The OC12 IR 1310 card provides one intermediate- or short-reach, SONET OC-12 interface per card, compliant with Telcordia GR-253. The interface operates at 622.08 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, or STS-12c. Figure 2-10 shows the OC12 IR 1310 faceplate and Figure 2-11 on page 2-13 shows the block diagram.

Figure 2-10 OC12 IR 1310 Card Faceplate

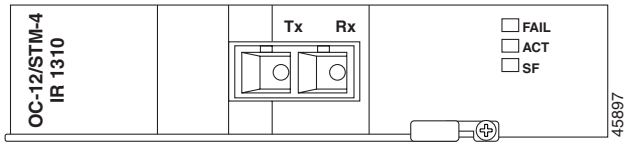
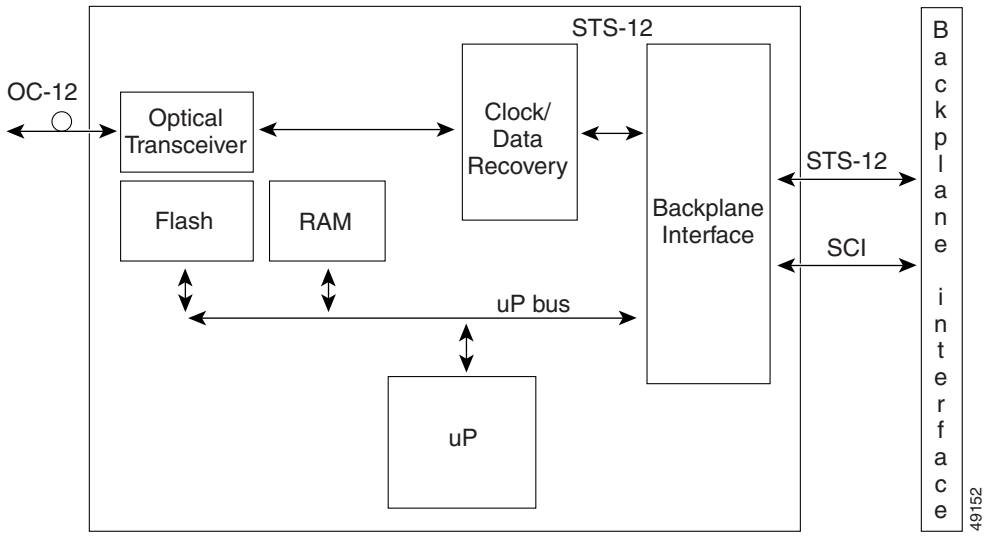


Figure 2-11 OC12 IR 1310 Card Block Diagram



Warning **Invisible laser radiation may be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation, do not stare into open apertures.**

You can install the OC12 IR 1310 card in any ONS 15327 high-speed slot and provision the card as a drop card or span card in a two-fiber BLSR, UPSR, or ADM (linear) configuration.

The OC12 IR 1310 port features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 IR 1310 card uses SC optical connections and supports 1+1 unidirectional and bidirectional protection.

The OC12 IR 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card counts section and line BIT errors.

2.5.2 OC12 IR 1310 Card-Level Indicators

The OC12 IR 1310 card has three card-level LED indicators (Table 2-3).

Table 2-3 OC12 IR 1310 Card-level Indicators

Card-level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC12 IR 1310 card is operational and is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.5.3 OC12 IR 1310 Card Specifications

- Line
  - Bit rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Maximum transmitter output power: –8 dBm
  - Minimum transmitter output power: –15 dBm
  - Center wavelength: 1274 nm to 1356 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: –7 dBm
  - Minimum receiver level: –29 dBm
  - Receiver: InGaAs/InP photo detector
  - Link loss budget: 14 dB
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 14 W, 0.29 A, 48 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

2.6 OC12 LR 1550 Card

This section describes the features and functions of the OC12 LR 1550 card. For card provisioning, refer to the *Cisco ONS 15327 Procedure Guide*.

2.6.1 OC12 LR 1550 Card Description

The OC12 LR 1550 card provides one long-reach, Telcordia-compliant, GR-253 SONET OC-12 interface per card. The interface operates at 622.08 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, or STS-12c. Figure 2-12 shows the OC12 LR 1550 faceplate and Figure 2-13 shows the block diagram.

Figure 2-12 OC12 LR 1550 Card Faceplate

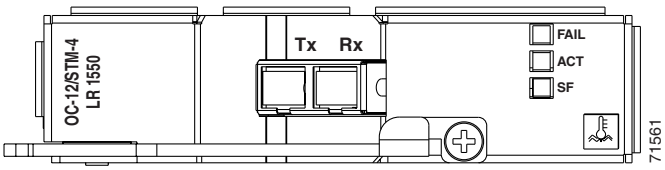
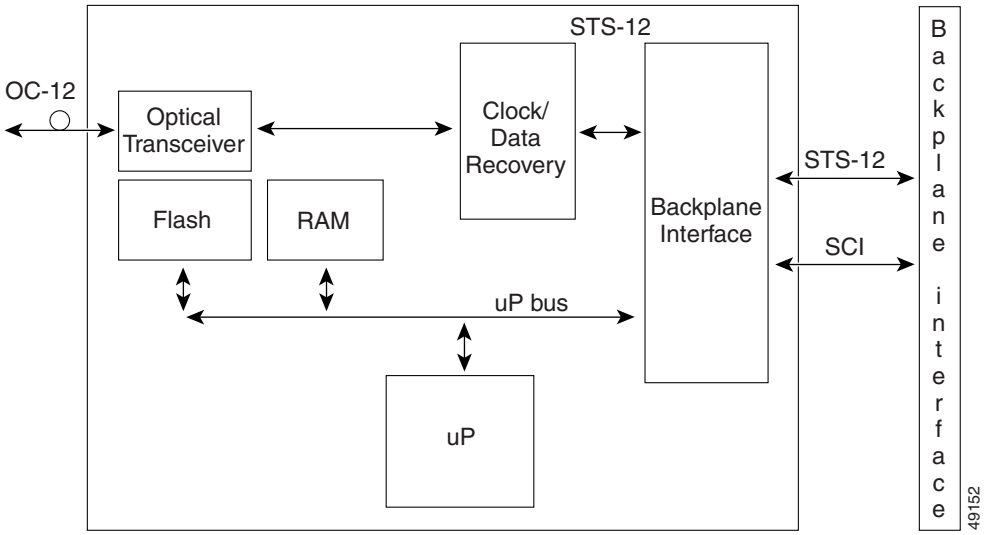


Figure 2-13 OC12 LR 1550 Card Block Diagram



Warning **Invisible laser radiation may be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation, do not stare into open apertures.**

You can install the OC12 LR 1550 card in any ONS 15327 high-speed card slot and provision the card as a drop card or span card in a UPSR or ADM (linear) configurations.

The OC-12 interface features a 1550 nm laser and contains a transmit (Tx) and receive (Rx) connector (labeled) on the card faceplate. The OC12 LR 1550 uses SC connectors. The OC12 LR 1550 card supports 1+1 unidirectional and bidirectional switching.

The OC12 LR 1550 detects loss of signal (LOS), loss of frame (LOF), and loss of pointer (LOP), and line alarm indication signal (AIS-L) conditions (refer to the *Cisco ONS 15327 Troubleshooting Guide* for a complete description of alarm conditions). The OC12 LR 1550 counts path and line BIT errors.

The OC12 LR 1550 extracts the K1 and K2 bytes from the SONET overhead to perform an appropriate protection switch. The DCC bytes are forwarded to the DCC-terminating XTC.

2.6.2 OC12 LR 1550 Card-Level Indicators

The OC12 LR 1550 card has three card-level LED indicators (Table 2-4).

Table 2-4 OC12 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC12 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.6.3 OC12 LR 1550 Card Specifications

- Line
  - Bit rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Maximum transmitter output power: +2 dBm
  - Minimum transmitter output power: –3 dBm
  - Center wavelength: 1480 nm to 1580 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: DFB (distributed feedback) laser
- Receiver
  - Maximum receiver level: –7 dBm
  - Minimum receiver level: –29 dBm
  - Receiver: InGaAs/InP photo detector
  - Link loss budget: 26 dB
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 14 W, 0.29 A, 48 BTU/hr

- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

2.7 OC48 IR 1310 Card

This section describes the features and functions of the OC48 IR 1310 card. For card provisioning, refer to the *Cisco ONS 15327 Procedure Guide*.

2.7.1 OC48 IR 1310 Card Description

The OC48 IR 1310 card provides one intermediate-reach, Telcordia-compliant, GR-253 SONET OC-48 interface per card. Each interface operates at 2488.320 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, STS-12c, or STS-48c. Figure 2-14 shows the OC48 IR 1310 faceplate and Figure 2-15 shows the block diagram.

Figure 2-14 OC48 IR 1310 Card Faceplate

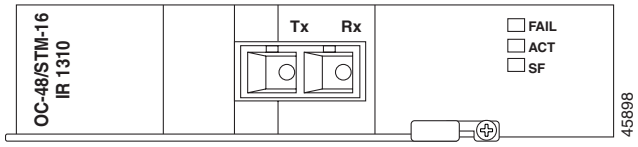
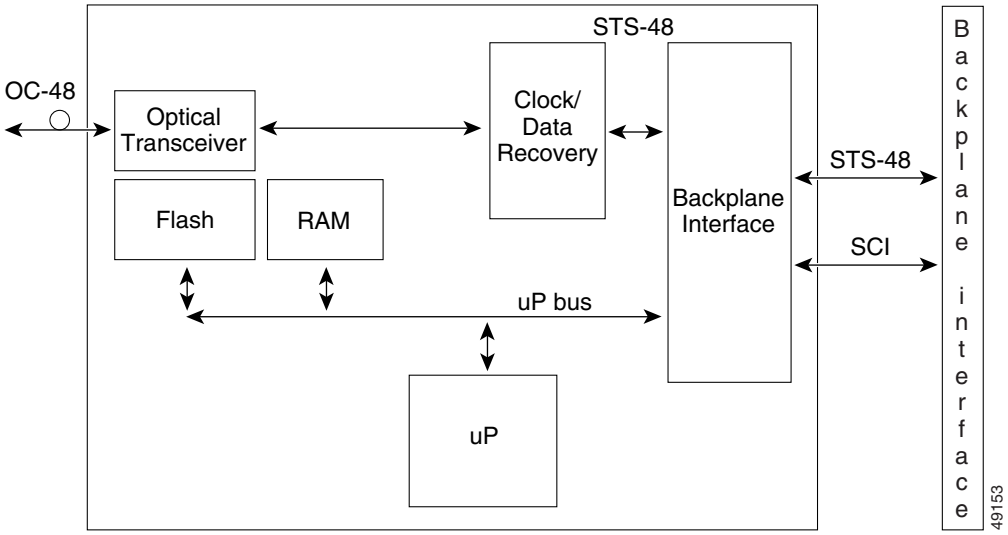


Figure 2-15 OC48 IR 1310 Block Diagram



Warning **Invisible laser radiation may be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation, do not stare into open apertures.**

You can install the OC48 IR 1310 card in any ONS 15327 high-speed card slot and provision the card as a drop or span card in a two-fiber BLSR, UPSR, or in an ADM (linear) configuration.

The OC-48 port features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC48 IR 1310 uses SC connectors. The card supports 1+1 unidirectional and bidirectional protection switching.

The OC48 IR 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card also counts section and line BIT errors.

2.7.2 OC48 IR 1310 Card-Level Indicators

The OC48 IR 1310 card has three card-level LED indicators (Table 2-5).

Table 2-5 OC48 IR 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC48 IR 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF, AIS-L or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.7.3 OC48 IR 1310 Card Specifications

- Line
  - Bit rate: 2488.320 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Maximum transmitter output power: 0 dBm
  - Minimum transmitter output power: –5 dBm
  - Center wavelength: 1280 nm to 1350 nm
  - Nominal wavelength: 1310 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level: 0 dBm
  - Minimum receiver level: –18 dBm

  - Receiver: InGaAs InP photo detector
  - Link loss budget: 13 dB min
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: 32 to 131 degrees Fahrenheit (0 to +55 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 25 W, 0.52 A, 85 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

2.8 OC48 LR 1550 Card

This section describes the features and functions of the OC48 LR 1550 card. For card provisioning, refer to the *Cisco ONS 15327 Procedure Guide*.

2.8.1 OC48 LR 1550 Card Description

The OC48 LR 1550 card provides one intermediate-reach, Telcordia-compliant, GR-253 SONET OC-48 interface per card. Each interface operates at 2488.320 Mbps over a single-mode fiber span and supports VT payloads and nonconcatenated or concatenated payloads for STS-1, STS-3c, STS-6c, STS-12c, or STS-48c. Figure 2-16 shows the OC48 LR 1550 faceplate and Figure 2-17 on page 2-20 shows the block diagram.

Figure 2-16 OC48 LR 1550 Card Faceplate

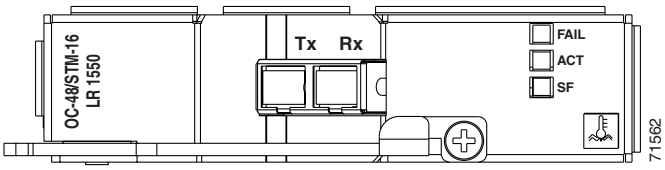
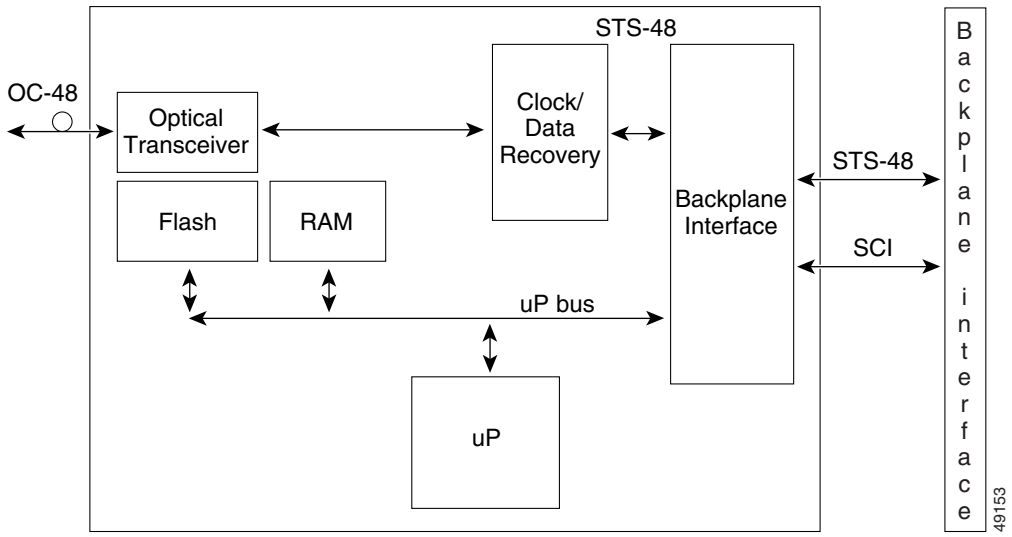


Figure 2-17 OC48 LR 1550 Block Diagram



Warning **Invisible laser radiation may be emitted from the aperture port when no cable is connected. To avoid exposure to laser radiation, do not stare into open apertures.**

You can install the OC48 LR 1550 card in any ONS 15327 high-speed card slot and provision the card as a drop or span card in a two-fiber BLSR, UPSR, or ADM (linear) configuration.

The OC48 LR 1550 port features a 1550-nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The card uses SC connectors, and it supports 1+1 unidirectional and bidirectional protection switching.

The OC48 LR 1550 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a description of these conditions. The card also counts section and line BIT errors.

2.8.2 OC48 LR 1550 Card-Level Indicators

The OC48 LR 1550 card has three card-level LED indicators (Table 2-6).

Table 2-6 OC48 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	Indicates that the OC48 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	Indicates a signal failure or condition such as LOS, LOF or high BERs on the card's port. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. The light turns off when the fibers are properly connected.

2.8.3 OC48 LR 1550 Card Specifications

- Line
  - Bit rate: 2488.320 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550nm single-mode
  - Loopback modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Maximum transmitter output power: +3dBm
  - Minimum transmitter output power: –2 dBm
  - Center wavelength: 1520 nm to 1580 nm
  - Nominal wavelength: 1550 nm
  - Transmitter: Fabry Perot laser
- Receiver
  - Maximum receiver level:–8 dBm
  - Minimum receiver level: –28 dBm
  - Receiver: InGaAs InP photo detector
  - Link loss budget: 26 dB minimum, with 1 dB dispersion penalty
- Environmental
  - Eye safety compliance: Class I
  - Operating temperature: –40 to +149 degrees Fahrenheit (–40 to +65 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 25 W, 0.52 A, 85 BTU/hr
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

2.9 E10/100-4 Card

This section describes the features and functions of the ONS 15327 Ethernet card, called the E10/100-4 card. For card provisioning, refer to the *Cisco ONS 15327 Procedure Guide*.

2.9.1 E10/100-4 Card Description

The E10/100-4 card provides four IEEE 802.3-compliant, 10/100 interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 Mbps per port and 622 Mbps per card. Each port can independently detect the speed of an attached device (autosenses) and automatically connects at the appropriate speed. The ports autoconfigure to operate at either half or full duplex and can determine whether to enable or disable flow control. You can manually set the port speed and duplex mode. The card faceplate and block diagram are shown in Figure 2-18 and Figure 2-19.

Figure 2-18 E10/100-4 Card Faceplate

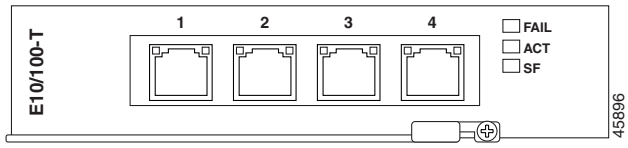
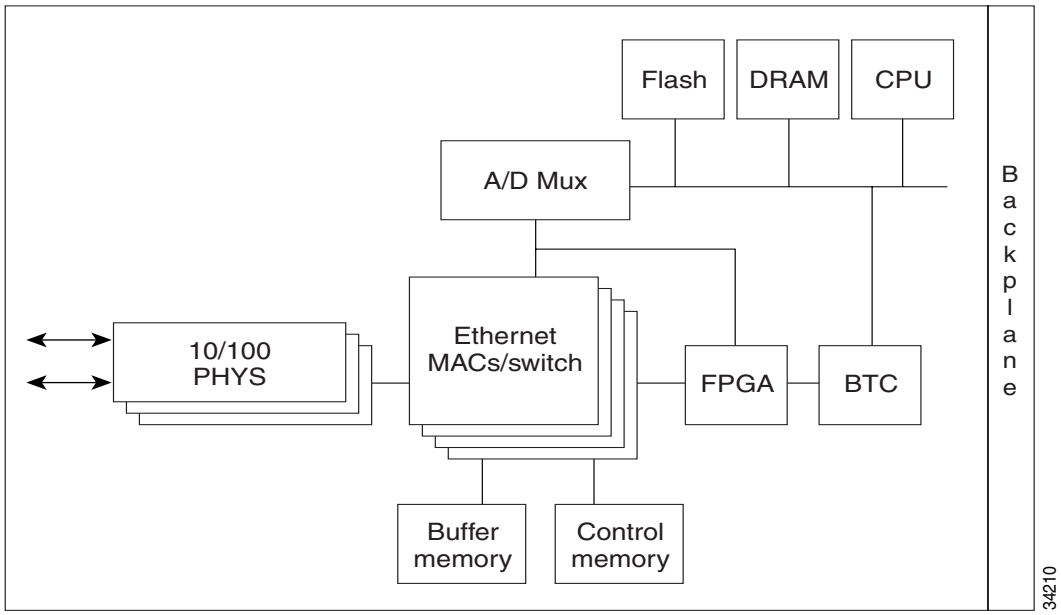


Figure 2-19 E10/100-4 Block Diagram



The E10/100-4 Ethernet card provides high-throughput, low-latency packet switching of Ethernet traffic across a SONET network while providing a greater degree of reliability through SONET "self-healing" protection services. This Ethernet capability enables network operators to provide multiple 10/100 Mbps access drops for high-capacity customer LAN interconnects, Internet traffic, and cable modem traffic aggregation. Efficient transport and coexistence of traditional TDM traffic with packet-switched data traffic is provided.

Each E10/100-4 card supports standards-based, wire-speed, Layer 2, Ethernet switching between its Ethernet interfaces. IEEE 802.1Q-tag and port-based VLANs are supported in order to logically isolate traffic (typically subscribers). Priority queuing is also supported in order to provide multiple classes of service.

You can install the E10/100-4 card in any high-speed slot. Multiple Ethernet cards installed in an ONS 15327 can act as a single switch or multiple switches supporting a variety of SONET port configurations. To create logical SONET ports, provision a number of STS channels to the packet switch entity within the ADM. You can create logical ports with a bandwidth granularity of STS-1. The ONS 15327 can support six STS-1s, two STS-3cs, one STS-6c, or one STS-12c in single-card EtherSwitch mode. It supports three STS-1s or one STS-3c in multicard EtherSwitch mode.

2.9.2 E10/100-4 Card-Level Indicators

The E10/100-4 card faceplate has two card-level LED indicators (Table 2-7).

Table 2-7 E10/100-4 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	Indicates that the card's processor is not ready or catastrophic software failure occurred on the E10/100-4 card. As part of the boot sequence, the FAIL LED is turned on until the software deems the card operational.
Green ACT LED	Provides the operational status of the E10/100-4. When the ACT LED is green it indicates that the E10/100-4 card is active and the software is operational.
SF LED	Not in use.

2.9.3 E10/100-4 Port-Level Indicators

The E10/100-4 card also has four pairs of LEDs (one pair for each port) (Table 2-8) that indicate status, such as signal or equipment failures. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for a complete description of the alarm messages that may be generated when LEDs do not display normal behavior.

Table 2-8 E10/100-4 Port-level Indicators

LED State	Description
Amber	Transmitting and receiving
Solid Green	Idle and link integrity
Green Light Off	Inactive connection or unidirectional traffic

2.9.4 E10/100-4 Card Specifications

- Environmental
  - Operating temperature: 32 to 131 degrees Fahrenheit (0 to +55 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 45 W, 0.95 A, 154 BTU/hr

- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)

2.10 G1000-2 Card

This section describes the features and functions of the ONS 15327 Gigabit Ethernet card, called the G1000-2 card. For card provisioning, refer to the *Cisco ONS 15327 Procedure Guide.*

2.10.1 G1000-2 Card Description

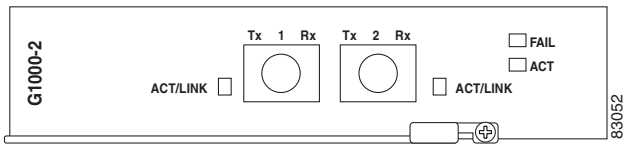
The G1000-2 provides two IEEE 802.3-compliant, 1000 Mbps ports for high-capacity customer LAN interconnections. Each port supports full-duplex operation for a maximum bandwidth of 2000 Mbps per port.

The G1000-2 card uses standard Small-Form-Factor Pluggable (SFP) modules for the optical ports. SFPs are input/output devices that plug into a Gigabit Ethernet port to link the port to the fiber-optic network. Cisco provides two SFP modules: one for short-reach applications and one for long-reach applications. The short-reach model connects to multimode fiber and the long-reach model requires single-mode fiber.

Both SFP modules are offered as separate orderable products: an IEEE 1000BaseSX compliant, 85-nm optical module and an IEEE 1000BaseLX-compliant, 1300-nm optical module. The 850-nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300-nm LX optics are designed for single-mode fiber and distances of up to 10 kilometers.

The card faceplate is shown in Figure 2-20.

Figure 2-20 G1000-2 Card Faceplate



The G1000-2 Gigabit Ethernet card provides high-throughput, low latency transport of Ethernet encapsulated traffic (IP and other Layer 2 or Layer 3 protocols) across a SONET network. Carrier-class Ethernet transport is achieved by hitless (< 50 ms) performance in the event of any failures or protection switches (such as 1+1 APS, UPSR, or BLSR). Full provisioning support is possible via CTC, TL1, or CTM.

The circuit sizes supported are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c and STS-48c.

2.10.2 G1000-2 Card-Level Indicators

The G1000-2 card faceplate has two card-level LED indicators (Table 2-9).

Table 2-9 G1000-2 Card-Level Indicators

Card-Level LEDs	Description
FAIL LED (red)	The red FAIL LED indicates the card's processor is not ready or a catastrophic software failure occurred on the G1000-2 card. As part of the boot sequence, the FAIL LED is turned on, and it turns off if the software is deemed operational. The red FAIL LED blinks, when the card is loading software.
ACT LED (green)	A green ACT LED provides the operational status of the G1000-2. If the ACT LED is green it indicates that the G1000-2 card is active and the software is operational.

2.10.3 G1000-2 Port-Level Indicators

The G1000-2 card also has one bicolor ACT/LINK LED per port. Table 2-10 describes the status that each color represents.

Table 2-10 G1000-2 Port-Level Indicators

Port-Level LED	Description
Off	No link exists to the Ethernet port.
Steady Amber	A link exists to the Ethernet port, but traffic flow is inhibited. For example, an unconfigured circuit, an error on line, or a nonenabled port may inhibit traffic flow.
Solid Green	A link exists to the Ethernet port, but no traffic is carried on the port.
Flashing Green	A link exists to the Ethernet port, and traffic is carried on the port. The LED flash rate reflects the traffic rate for the port.

2.10.4 G1000-2 Card Specifications

- Environmental
  - Operating temperature:

    C-Temp (15327-E1000-2): 32 to 131 degrees Fahrenheit (0 to +55 degrees Celsius)
  - Operating humidity: 5 to 95%, noncondensing
  - Power consumption: 53.50 W, 1.11 A, 182.67 BTU/hr.
- Dimensions
  - Height: 1.080 in. (27.4 mm)
  - Width: 4.280 in. (108.7 mm)
  - Depth: 9.172 in. (233.0 mm)
  - Card weight: 2.1 lb (0.9 kg)
- Compliance

- ONS 15327 cards, when installed in a system, comply with these standards: Safety: UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950
- Eye safety compliance: Class I (21 CFR 1040.10 and 1040.11) and Class 1M (IEC 60825-1 2001-01) laser products

Card Protection

This chapter explains the Cisco ONS 15327 card protection configurations. To provision card protection, refer to the *Cisco ONS 15327 Procedure Guide*. Chapter topics include:

3.1 ONS 15327 Protection Groups

When you set up 1+1 optical protection for ONS 15327 cards, you must choose between maximum protection and maximum slot availability. The highest protection reduces the number of available card slots; the highest slot availability reduces the protection. Table 3-1 shows the protection types that can be set up for ONS 15327 cards.

A 1:1 (electrical) XTC protection group is pre-provisioned on the ONS 15327. The name of the protection group is XTCPROTGRP and it cannot be edited or deleted. Therefore, you only need to create protection for optical cards.

Table 3-1 Card Protection Group Types

Type	Cards	Description
1:1	XTC	Default electrical circuits protection (cannot be changed).
1+1	Any optical	Pairs a working optical port with a protect optical port. Protect ports must match the working ports. For example, Port 1 of an OC-3 card can only be protected by Port 1 of another OC-3 card. Cards do not need to be in adjoining slots.
Unprotected	Any	Unprotected cards can cause signal loss if a card fails or incurs a signal error. However, because no card slots are reserved for protection, unprotected schemes maximize the service available for use on the ONS 15327. Unprotected is the default protection type for optical cards.

3.2 Optical Card Protection

With 1+1 port-to-port protection, ports on the protect card are assigned to protect the corresponding ports on the working card. The working and protect cards do not need to be installed side by side in the node. A working card must be paired with a protect card of the same type, for example, an OC-3 card should be paired with another OC-3 card. The protection takes place on the port level, so any port on the protect card can be assigned to protect the corresponding port on the working card.

For example, on a four-port card, you can assign one port as a protection port on the protect card (protecting the corresponding port on the working card) and leave three ports unprotected. Conversely, you can assign three ports as protection ports and leave one port unprotected.

1+1 span protection can be either revertive or non-revertive. With non-revertive 1+1 protection, when a failure occurs and the signal switches from the working card to the protect card, the signal stays switched to the protect card until it is manually switched back. Revertive 1+1 protection automatically switches the signal back to the working card when the working card comes back online.

For more information, refer to the *Cisco ONS 15327 Procedure Guide*.

3.3 Unprotected Cards

Unprotected optical cards are not included in a protection scheme; therefore, a card failure or a signal error results in lost data. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15327 bandwidth.

3.4 Automatic Protection Switching

Unidirectional switching allows traffic on the transmit and receive fibers to switch independently. With bidirectional switching, transmit and receive lines switch together.

With nonrevertive 1+1 protection, APS switches a signal after a failure from the working card to the protect card and the signal stays switched to the protect card until it is manually switched back. Revertive switching automatically switches the signal back to the working card when the working card comes back online. 1+1 protection is unidirectional and nonrevertive by default; revertive switching is easily provisioned using CTC.

3.5 External Switching Commands

The external switching commands on the ONS 15327 are Manual, Force, and Lockout. 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 (in1+1 configurations) and prevent traffic from switching to the protect port under any circumstance. Lockouts have the highest priority.

Note Force and Manual switches do not apply to a 1:1 protection groups; these ports have a single Switch command.

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). In 1:1 protection groups, working or protect ports can have a lock on.

Cisco Transport Controller Operation

This chapter describes Cisco Transport Controller (CTC), the Cisco ONS 15327 software interface. For CTC set up and login information, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

4.1 CTC Software Delivery Methods

ONS 15327 provisioning and administration is performed using CTC software. CTC is a Java application that is installed in two locations. CTC is stored on the XTC card and downloaded to your workstation each time you log into the ONS 15327.

4.1.1 CTC Software Installed on the XTC Card

CTC software is preloaded on the ONS 15327 XTC cards; therefore, you do not need to install software on the XTC cards. When a new CTC software version is released, follow procedures in the *Cisco ONS 15327 Software Upgrade Guide* to upgrade the ONS 15327 software on the XTC cards.

When you upgrade CTC software, the XTC cards store the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. You can view the software versions that are installed on an ONS 15327 by selecting the Maintenance > Software tabs in node view. Select 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

CTC software is downloaded from the XTC cards and installed on your computer automatically when you connect to the ONS 15327. Downloading the CTC software files automatically ensures that your computer is running the same CTC software version as the XTC cards you are accessing. The CTC files are stored in the temporary directory designated by your computer operating system. You can use the Delete CTC Cache button to remove files stored in the temporary directory. If the files are deleted, they download the next time you connect to an ONS 15327. Downloading the jar files for CTC takes several minutes depending on the bandwidth of the connection between your workstation and the ONS 15327. For example, jar files downloaded from a modem or an SDCC network link will require more time than jar files downloaded over a LAN connection.

4.2 CTC Installation Overview

To connect to an ONS 15327 using CTC, you enter the ONS 15327 IP address in the URL field of a web browser, such as Netscape Navigator or Microsoft Internet Explorer. After connecting to an ONS 15327, the following events occur automatically:

1. A CTC launcher applet is downloaded from the XTC card to your computer.
2. The launcher determines whether your computer has a CTC release matching the release on the ONS 15327 XTC card.
3. If the computer does not have CTC installed, or if the installed release is older than the XTC card version, the launcher downloads the CTC program files from the XTC card.
4. The launcher starts CTC. The CTC session is separate from the web browser session, so the web browser is no longer needed. Always log into nodes having the latest software release. If you log into an ONS 15327 that is connected to ONS 15327s with older versions of CTC, or to Cisco ONS 15454s, CTC "element" files are downloaded automatically to enable you to interact with those nodes. You cannot interact with nodes on the network that have a software version later than the node that you used to launch CTC.

Each ONS 15327 can handle up to four network-level CTC sessions (the login node and its DCC-connected nodes) and one node-level session (login node only) at one time. CTC performance may vary, depending upon the volume of activity in each session.

Note You can also use TL1 commands to communicate with the Cisco ONS 15327 through VT100 terminals and VT100 emulation software, or you can Telnet to an ONS 15327 using TL1 port 3083. See the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide* for a comprehensive list of TL1 commands.

4.3 PC and Unix Workstation Requirements

To use CTC in ONS 15327, your computer must have a web browser with the correct Java Runtime Environment (JRE) installed for the software release in use. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and doc CD. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 4-1 on page 4-3 shows JRE compatibility with ONS software releases.

Table 4-1 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15327 Release 1.0	Yes	No
ONS 15327 Release 1.0.1	Yes	Yes
ONS 15327 Release 3.3	Yes	Yes
ONS 15327 Release 3.4	No	Yes

Requirements for PCs and UNIX workstations are provided in Table 4-2. In addition to Netscape Communicator and the JRE, also included on the ONS 15327 software CD and the ONS 15327 documentation CD are the Java plug-in and modified java.policy file.

Table 4-2 CTC Computer Requirements

Area	Requirements	Notes
Processor	Pentium II 300 MHz, UltraSPARC, or equivalent	300 Mhz is the recommended processor speed. You can use computers with less processor speed; however, you may experience longer response times and slower performance.
RAM	128 MB	—
Hard drive	2 GB recommended; 50 MB space must be available	—
Operating System	• PC: Windows 95, Windows 98, Windows NT 4.0 with Service Pack 6, Windows 2000, or Windows XP • Workstation: Any Solaris release	—
Web browser	• PC: Netscape Navigator 4.73 or higher, 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 15327 software and documentation CDs.
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 15327 software and documentation CDs. If you will connect to an ONS 15327 running Release 2.2.1, you must uninstall JRE 1.3.1 and install JRE 1.2.2_05, then reinstall JRE 1.3.1_02 when you connect to an ONS 15327 running Release 3.4 JRE 1.4 is not supported.

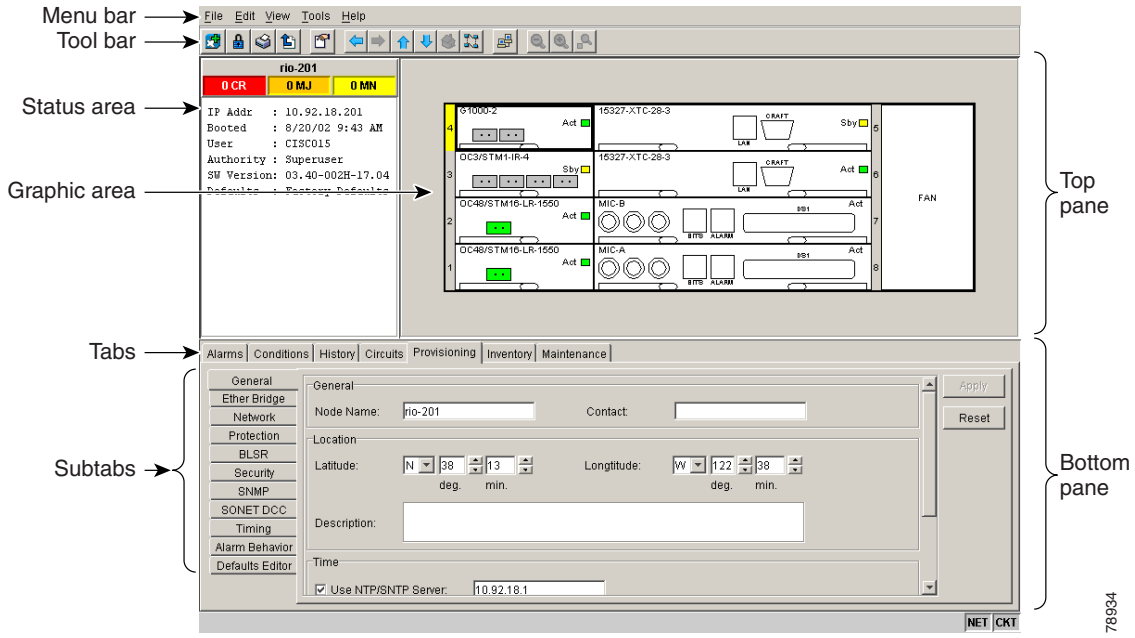
Table 4-2 CTC Computer Requirements (continued)

Area	Requirements	Notes
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 15327 software and documentation CDs.
Cable	User-supplied Category 5 straight-through cable with RJ-45 connectors on each end to connect the computer to the ONS 15327 directly or though a LAN	—

4.4 CTC Window

The CTC window appears after you log into an ONS 15327 (Figure 4-1 on page 4-4). The window includes a menu bar, toolbar, and a top and bottom pane. The top pane displays status information about the selected objects and a graphic of the current view. The bottom pane displays tabs and subtabs, which you use to view ONS 15327 information and perform ONS 15327 provisioning and maintenance. From this window you can display three ONS 15327 views: network, node, and card.

Figure 4-1 Node View (Default Login View)



4.4.1 Node View

The CTC node view, shown in Figure 4-1, is the first view displayed after you log into an ONS 15327. The login node is the first node displayed, and it is the "home view" for the session. Node view allows you to view and manage one ONS 15327 node. The status area shows the node name; IP address; session boot date and time; number of critical (CR), major (MJ), and minor (MN) alarms; the name of the current logged-in user; and security level of the user.

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, which you can use to open, reset, or delete a card. Right-click a slot to preprovision a card slot before installing the card.

The graphic area of the CTC window depicts the ONS 15327 shelf assembly. The colors of the cards in the graphic reflect the real-time status of the physical card and slot (Table 4-3).

Table 4-3 Node View Card and Slot Colors

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

Ports can be assigned one of four states, OOS, IS, OOS_AINS, or OOS_MT. The color of the port in both card and node view indicates the port state. Table 4-4 shows the port colors and their states.

Table 4-4 Node View Card Port Colors

Port Color	State	Description
Gray	OOS	Port is out of service; no signal will be transmitted.
Violet	OOS_AINS	Port is out of service, auto in service. The port will transmit a signal but will suppress alarms. The port will transition to in service (IS) when a signal is received for the amount of time specified in the AINS_SOAK field and no hardware-related alarms, such as Equipment Failure (EQPT) or Improper Removal (IMPROPRMVL) are present on the node.
Cyan	OOS_MT	Port is out of service, maintenance. The port will transmit a signal but alarms are suppressed and loopbacks are allowed. The port will not transition to IS until assigned by the user. Loopbacks are allowed in this port state.
Green	IS	Port is in service. The port will transmit a signal and display alarms; loopbacks are not allowed.

Table 4-5 lists the tabs and subtabs available in the node view.

Table 4-5 Node View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the node and updates them in real time.	—
Conditions	Displays 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	Create, delete, edit, and map circuits.	—
Provisioning	Provision the ONS 15327 node.	General, EtherBridge, Network, Protection, BLSR, Security, SNMP, SONET DCC, Timing, Alarm Behavior, Defaults Editor
Inventory	Provides inventory information (part number, serial number, CLEI codes) for cards installed in the node. Allows you to delete and reset cards.	—
Maintenance	Perform maintenance tasks for the node.	Database, EtherBridge, Protection, BLSR, Software, Overhead XConnect, Diagnostic, Timing, Audit, Routing Table, RIP Routing Table, Test Access

4.4.2 Network View

Network view (Figure 4-2 on page 4-7) allows you to view and manage ONS 15327s that have DCC connections to the node that you logged into and any login node groups you may have selected.

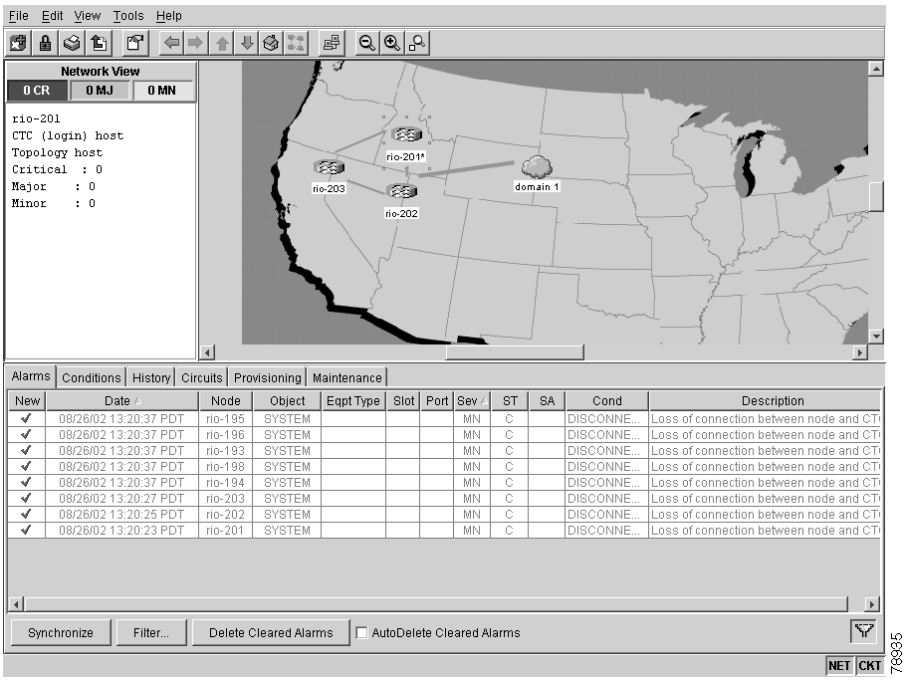
Note Nodes with DCC connections to the login node will not display if you select Disable Network Discovery on the Login dialog box.

The graphic area displays a background image with colored ONS 15327 icons. A Superuser can set up the logical network view feature, which enables each user to see the same network view. The icon colors indicate the node status (Table 4-6 on page 4-7).

The lines show DCC connections between the nodes. DCC connections can be green (active) or gray (fail). The lines can also be solid (circuits can be routed through this link) or dashed (circuits cannot be routed through this link).

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

Figure 4-2 Three-Node Network Displayed in CTC Network View



The node colors shown in network view indicate the status of the node (Table 4-6).

Table 4-6 Node Colors Indicating State in Network View

Color	Alarm Status
Green	No alarms
Yellow	Minor alarms
Orange	Major alarms
Red	Critical alarms
Gray with Unknown#	Node is initializing for the first time. CTC displays Unknown# because CTC has not yet discovered the name of the node

Table 4-7 lists the tabs and subtabs available in the network view.

Table 4-7 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	—

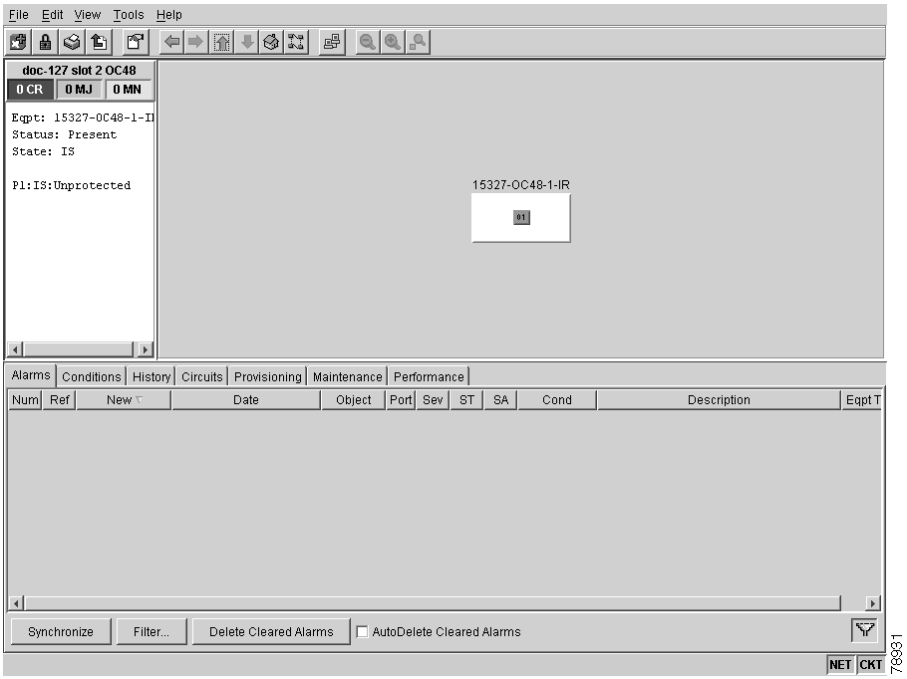
Table 4-7 Network View Tabs and Subtabs (continued)

Tab	Description	Subtabs
Provisioning	Provision security, alarm profiles, BLSR and overhead circuits	Security, Alarm Profiles, BLSR, 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

4.4.3 Card View

Card view displays information about individual ONS 15327 cards. Use this view to perform card-specific maintenance and provisioning (Figure 4-3). A graphic showing the ports on the card appears in the graphic area. The status area displays the node name, slot, number of alarms, card type, equipment type, and either the card status (active or standby), card state (IS, OOS, OOS_AINS, or OOS_MT), or port state (IS, OOS, OOS_AINS, or OOS_MT). The information that appears and the actions you can perform depend on the card.

Figure 4-3 CTC Card View Showing an OC48 IR 1310 Card



Note CTC displays a card view for all ONS 15327 cards except the MIC.

Table 4-8 shows the tabs and subtabs available in card view. The subtabs, fields, and information displayed under each tab depend on the card type selected.

Table 4-8 Card View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the card and updates them in real-time	—
Conditions	Displays a list of standing conditions on the card	—
History	Provides a history of card alarms including date, object, port, and severity of each alarm	Session, Card: The Session subtab displays alarms and events for the current session; the Card subtab displays alarms and events retrieved from a fixed-size log
Circuits	Create, delete, edit, and search circuits	Circuits
Provisioning	Provision an ONS 15327 card	Line, Line Thresholds (different threshold options are available for electrical and optical cards), Elect Path Thresholds, SONET Thresholds, or SONET STS, and Alarm Behavior
Maintenance	Perform maintenance tasks for the card	Loopback, Info, Protection, and J1 Path Trace (Options depend on the card type)
Performance	Perform performance monitoring for the card	—

4.5 XTC Card Reset

You can reset the ONS 15327 XTC card using CTC or by physically reseating the card. Resetting the XTC card reboots the XTC card and reloads the operating system and the application software. Additionally, a reseat temporarily removes power from the XTC card and clears all buffer memory.

You can apply a reset from CTC to either an active or standby XTC card without affecting traffic. If you need to reseat an active XTC card, put the XTC card into standby mode first by performing a reset using CTC.

4.6 XTC Card Database

When dual XTC cards are installed in the ONS 15327, each XTC card hosts a separate database; therefore, the protect card database is available if the database on the working XTC fails. You can also store a backup version of the database on the workstation running CTC. This operation should be part of a regular ONS 15327 maintenance program performed at approximately weekly intervals, and should also be completed when preparing an ONS 15327 for a pending natural disaster, such as a flood or fire.

Note The following parameters are not backed up and restored: node name, IP address, mask and gateway, and IIOP port. If you change the node name and then restore a backed up database with a different node name, the circuits will map to the new node name. Cisco recommends keeping a record of the old and new node names.

4.7 Software Revert

Reverting to Software R2.2.1 or later will load the database without affecting traffic or DCC connectivity. This feature requires dual XTC cards and CTC Software R2.2.1 or later as the protect version.

When you click the Activate button after a software upgrade, the XTC copies the current working database and saves it in a reserved location in the XTC flash memory. If you later need to revert to the original working software load from the protect software load, the saved database installs automatically. You do not need to restore the database manually or recreate circuits.

Tip The revert feature is useful if a maintenance window closes while you are upgrading CTC software. You can revert to the standby software load without losing traffic. When the next maintenance window opens, complete the upgrade and activate the new software load.

Note A revert from a matching maintenance release software load will use the current active database; therefore, no provisioning is lost. All other reverts do restore the database. (A maintenance release has a three-digit release number, for example 2.2.2).

Circuits that were created and provisioning that was performed after a software load is activated (upgraded to a higher software release) will not reinstate with a revert. The database configuration at the time of activation is reinstated after a revert. This does not apply to maintenance reverts (for example 2.2.2 to 2.2.1), because maintenance releases use the same database.

Security and Timing

This chapter provides information about Cisco ONS 15327 user security and SONET timing. To provision security and timing, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

5.1 Users and Security

A CISCO15 ID is provided with the ONS 15327 system. The ID can be used to set up other ONS 15327 users.

Each ONS 15327 can support up to 500 user IDs on one ONS 15327. Each Cisco Transport Controller (CTC) or TL1 user can be assigned one of the following security levels:

- Retrieve—Can retrieve and view CTC information but cannot set or modify parameters.
- Maintenance—Can access only the ONS 15327 maintenance options.
- Provisioning—Can access provisioning and maintenance options.
- Superusers—Can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users.

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

5.1.1 Security Requirements Per Tab in Node View

Table 5-1 shows the actions that each user level can perform in node view.

Table 5-1 ONS 15327 Security Levels—Node View

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	—	Synchronize alarms	X	X	X	X
Conditions	—	Retrieve	X	X	X	X

Table 5-1 ONS 15327 Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
History	Session	Read only	X	X	X	X
	Node	Retrieve alarms/events	X	X	X	X
Circuits	—	Create/edit/delete/filter	—	Partial	X	X
		Search	X	X	X	X
Provisioning	General	Edit	—	—	X	X
	EtherBridge	Spanning trees: edit	—	—	X	X
		Thresholds: create/delete	—	—	X	X
	Network	All	—	—	X	X
	Protection	Create/delete/edit	—	—	X	X
		Browse groups	X	X	X	X
	BLSR	All (BLSR)	—	—	X	X
	Security	Create/delete	—	—	—	X
		Change password	Same user	Same user	Same user	All users
	SNMP	Create/delete/edit	—	—	X	X
		Browse trap destinations	X	X	X	X
	Sonet DCC	Create/delete	—	—	X	X
	Timing	Edit	—	—	X	X
	Alarm Behavior	Edit	—	—	X	X
	Defaults Editor	Edit	—	—	—	X
Inventory	—	Delete	—	X	X	X
		Reset	—	X	X	X

Table 5-1 ONS 15327 Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Maintenance	Database	Backup/restore	—	—	—	X
	EtherBridge	MAC table retrieve	X	X	X	X
		MAC table clear/clear all	—	X	X	X
		Trunk utilization refresh	X	X	X	X
	Protection	Switch/lock out operations	—	X	X	X
	BLSR	BLSR maintenance	—	X	X	X
	Software	Download/upgrade/ activate/revert	—	—	—	X
	Cross-Connect	Delete VT tunnels	—	X	X	X
	Overhead XConnect	Read only	—	—		
	Timing	Edit	—	X	X	X
	Audit	Retrieve	X	X	X	X
	Routing Table	Read only	X	X	X	X
	RIP Routing Table	Refresh	X	X	X	X
	Test Access	Read only	X	X	X	X

5.1.1.1 Security Level Idle Times

Each ONS 15327 CTC or TL1 user can be idle during his or her login session for a specified amount of time before the CTC window is locked. The lockouts prevent unauthorized users from making changes. Higher-level users have shorter default idle periods and lower-level users have longer or unlimited default idle periods, as shown in Table 5-2.

Table 5-2 ONS 15327 Default User Idle Times

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

5.2 Node Timing

SONET timing parameters must be set for each ONS 15327. Each ONS 15327 independently accepts its timing reference from one of three sources:

- The BITS (Building Integrated Timing Supply) pins on the ONS 15327 Mechanical Interface card (MIC)

- An OC-N card installed in the ONS 15327 (the card is connected to a node that receives timing through a BITS source)
- The internal ST3 clock on the XTC card

You can set ONS 15327 timing to one of three modes: external, line, or mixed. If timing is coming from the BITS port, set ONS 15327 timing to external. If the timing comes from an OC-N card, set the timing to line. Typical ONS 15327 networks have the following timing configurations:

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

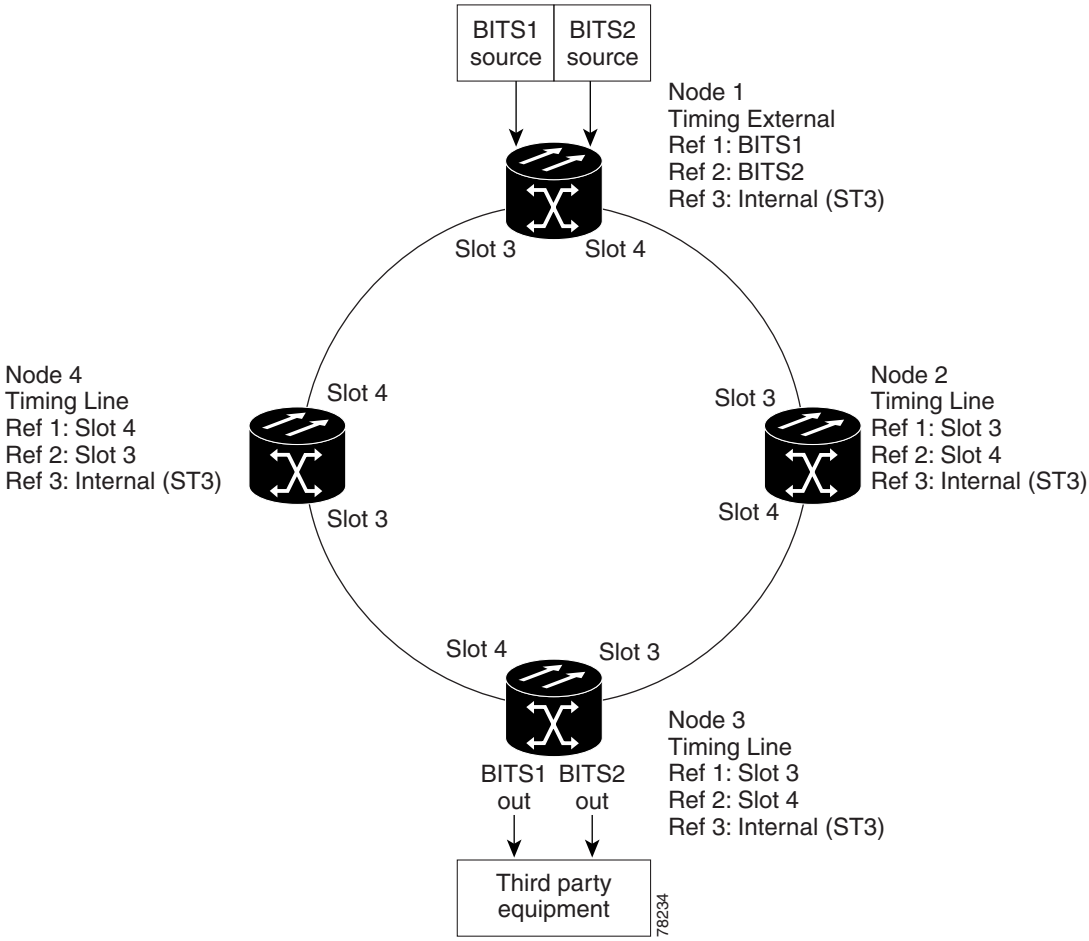
You can set three timing references for each ONS 15327. The first two references are typically two BITS-level sources, or two line-level sources optically connected to a node with a BITS source. The third reference is the internal clock provided on every ONS 15327 XTC card. This clock is a Stratum 3 (ST3). If an ONS 15327 becomes isolated, timing is maintained at the ST3 level.

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

5.2.1 Network Timing Example

Figure 5-1 on page 5-5 shows an example of an ONS 15327 network timing setup. Node 1 is set to external timing. Two references are set to BITS, and the third reference is set to internal. The BITS output pins on the MICs of Node 3 provide timing to outside equipment, such as a Digital Access Line Access Multiplexer.

Figure 5-1 ONS 15327 Timing Example



5.2.2 Synchronization Status Messaging

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

SSM messages are either Generation 1 or Generation 2. Generation 1 is the first and most widely deployed SSM message set. Generation 2 is a newer version. If you enable SSM for the ONS 15327, consult your timing reference documentation to determine which message set to use. Table 5-3 and Table 5-4 on page 5-6 show the Generation 1 and Generation 2 message sets.

Table 5-3 SSM Generation 1 Message Set

Message	Quality	Description
PRS	1	Primary reference source—Stratum 1
STU	2	Sync traceability unknown
ST2	3	Stratum 2

Table 5-3 SSM Generation 1 Message Set (continued)

Message	Quality	Description
ST3	4	Stratum 3
SMC	5	SONET minimum clock
ST4	6	Stratum 4
DUS	7	Do not use for timing synchronization
RES		Reserved; quality level set by user

Table 5-4 SSM Generation 2 Message Set

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

Circuits and Tunnels

This chapter explains Cisco ONS 15327 STS and virtual tributary (VT) circuits and VT and data communications channel (DCC) tunnels. To provision circuits and tunnels, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

6.1 Circuit Properties

On the ONS 15327 you can create unidirectional and bidirectional circuits. For unidirectional path switched ring (UPSR) circuits, you can create revertive or non-revertive circuits. Circuits will route automatically or you can manually route them. With the auto range feature, you do not need to build multiple circuits of the same type individually; the Cisco Transport Controller (CTC) can create additional sequential circuits if you specify the number of circuits you need and build the first circuit.

You can provision circuits either before or after cards are installed if the ONS 15327 slots are provisioned for the card that will carry the circuit. However, circuits will not carry traffic until the cards are installed and the ports and circuit status is in service (IS); out-of-service, auto in-service (OOS-AINS); or out-of-service, maintenance (OOS-MT).

The ONS 15327 Circuits window, which is displayed in network, node, and card view, is where you can view information about circuits, including:

- Name—Name of the circuit. The circuit name can be manually assigned or automatically generated.
- Type—Circuit types are: STS (STS circuit) VT (VT circuit), or VTT (VT tunnel).
- Size—Circuit size. VT circuits are 1.5. STS circuit sizes are 1, 3c, 6c, 9c, 12c, 24c, or 48c.
- Protection—The type of circuit protection.
- Direction—The circuit direction, either two-way or one-way.
- Status—The circuit status. See the "6.1.1 Circuit Status" section on page 6-2.

- Source—The circuit source in the format: node/slot/port “port name”/STS/VT. (Port name will appear in quotes.) Node and slot will always display; port “port name”/STS/VT might display, depending on the source card, circuit type, and whether a name is assigned to the port. If the circuit size is a concatenated size (3c, 6c, 12c, etc.) STSs used in the circuit will be indicated by an ellipsis, for example, “S7..9,” (STSs 7, 8, and 9) or S10..12 (STSs 10, 11, and 12).
- Destination—The circuit destination in same format (node/slot/port “port name”/STS/VT) as the circuit source.
- # of VLANS—The number of VLANS used by an Ethernet circuit.
- # of Spans—The number of inter-node links that constitute the circuit. Right-clicking the column displays a shortcut menu from which you can choose to show or hide circuit span detail.
- State—The circuit state. See the “6.1.1 Circuit Status” section on page 6-2.

6.1.1 Circuit Status

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

Table 6-1 ONS 15327 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 cross-connect or network span; a complete path from source to destination(s) does not exist. 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 flow on a protect path. Network spans are in one of two states: up or down. On CTC circuit and network maps, up spans are displayed as green lines, and down spans are displayed 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 that 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. Therefore, circuits routed on a failed network span will appear as ACTIVE during the current CTC session, but they will appear as INCOMPLETE to users who log in after the span failure.

Table 6-1 ONS 15327 Circuit Status (continued)

Status	Definition/Activity
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.
NOT_UPGRADABLE	A TL1-created circuit or a TL1-like CTC-created circuit is complete but has at least one non-upgradable cross-connect. UPSR_HEAD, UPSR_EN, UPSR_DC, and UPSR_DROP connections are not upgradable, so all unidirectional UPSR 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 non-upgradable cross-connects is missing a cross-connect or circuit span (network link); a complete path from source to destination(s) does not exist.

6.1.2 Circuit States

State is a user-assigned designation that indicates whether the circuit should be in service or out of service. The states that you can assign to circuits are shown in Table 6-2. To carry traffic, circuits must have a status of active and a state of in service (IS), out of service auto in service (OOS_AINS), or out of service maintenance (OOS_MT). The circuit source port and destination port must also be IS, OOS_AINS, or OOS_MT.

Note OOS_AINS and OOS_MT allow a signal to be carried, but alarms are suppressed.

You can assign a state to circuits at two points:

- During circuit creation you assign a state to the circuit on the Create Circuit wizard.
- After circuit creation, you can change a circuit state on the Edit Circuit window.

Table 6-2 Circuit States

State	Definition
IS	In service; able to carry traffic.
OOS	Out of service; unable to carry traffic.

Table 6-2 Circuit States (continued)

State	Definition
OOS-AINS	Out of service, auto in service; 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. VT circuits will change to IS when a signal is received; traffic is carried, but alarms are suppressed and loopbacks are allowed.
OOS-MT	Out of service, maintenance; 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.

PARTIAL is appended to a circuit state whenever all circuit cross-connects are not in the same state. Table 6-3 shows the partial circuit states that can display.

Table 6-3 Partial Circuit States

State	Definition
OOS_PARTIAL	At least one connection is OOS and at least one other is in some other state.
OOS_AINS_PARTIAL	At least one connection is OOS_AINS and at least one other is in IS state.
OOS_MT_PARTIAL	At least one connection is OOS_MT and at least one other is in some other state except OOS.

PARTIAL states can occur during automatic or manual transitions. Some cross-connects transition to IS, while others are OOS_AINS. PARTIAL can appear during a manual transition caused by an abnormal event such as a CTC crash, communication error, or one of the cross-connects could not be changed. Refer to the *Cisco ONS 15327 Troubleshooting Guide* for troubleshooting procedures.

Circuits do not use the soak timer for transitional states, but ports do. When provisioned as OOS-AINS, the ONS 15327 monitors a circuit's cross-connects for an error-free signal. It changes the state of the circuit from OOS-AINS to IS or to AINS-partial as each cross-connect assigned to the circuit path is completed. This allows you to provision a circuit using TL1, verify its path continuity, and prepare the port to go into service when it receives an error-free signal for the time specified in the port soak timer. Two common examples of state changes you will see when provisioning DS-1 and DS-3 circuits using CTC are as follows:

- When provisioning VT1.5 circuits and VT tunnels as OOS-AINS, the circuit state transitions to IS shortly after the circuits are created with the circuit source and destination ports are IS, OOS_AINS, or OOS_MT. The source and destination ports on the VT1.5 circuits remain in OOS-AINS state until an alarm-free signal is received for the duration of the soak timer. When the soak timer expires, the VT1.5 source port and destination port states change to IS.
- When provisioning STS circuits as OOS-AINS, the circuit and source and destination ports are OOS-AINS. As soon as an alarm-free signal is received the circuit state changes to IS and the source and destination ports remain OOS-AINS for the duration of the soak timer. After the port soak timer expires, STS source and destination ports change to IS.

6.1.3 Circuit Protection Types

The Protection column on the Circuit window shows the card (line) and SONET topology (path) protection used for the entire circuit path. Table 6-4 shows the protection type indicators that you will see in this column.

Table 6-4 Circuit Protection Types

Protection Type	Description
—	The circuit has no protection.
2F BLSR	The circuit is protected by a two-fiber bidirectional line switched ring (BLSR).
UPSR	The circuit is protected by a UPSR.
1+1	The circuit is protected by a 1+1 protection group.
protected	The circuit is protected by diverse SONET topologies, for example, a BLSR and a UPSR, or a UPSR and 1+1.
2F-PCA	The circuit is routed on a protection channel access path on a two-fiber BLSR. PCA circuits are unprotected.
PCA	The circuit is routed on a protection channel access path on two-fiber BLSRs. PCA circuits are unprotected.
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 display 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, protection type appears as “unknown.”

6.1.4 Edit Circuits Window

Use the Edit Circuits window to view general circuit information, create monitor circuits, change UPSR selectors and UPSR protection paths, and change a circuit state. For UPSR circuits, you can also:

- View the UPSR circuit’s working and protection paths
- Edit the reversion time
- Edit the Signal Fail/Signal Degrade thresholds
- Change payload defect indication path (PDI-P) settings
- Perform maintenance switches on the circuit selector
- View switch counts for the selectors

From the Edit Circuits window you can display a detailed circuit map by checking Show Detailed Map. The detailed map allows you to view information about ONS 15327 circuits graphically. Routing information that appears includes:

- Circuit direction (unidirectional/bidirectional)
- The nodes, STSs, and VTs through which circuit passes including slots and port numbers
- The circuit source and destination points

- OSPF Area IDs
- Link protection (UPSR, unprotected, BLSR, 1+1) and bandwidth (OC-N)

For BLSRs, the detailed map shows the number of BLSR fibers and the BLSR Ring ID. For UPSRs, 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 selectors states

By default, the working path on the detailed circuit map 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. Port states are indicated by colors, shown in Table 6-5.

Table 6-5 Port State Color Indicators

Port Color	State
Green	IS
Gray	OOS
Purple	OOS_AINS
Light blue	OOS_MT

Notation within the squares on each node indicate switches and other conditions. Move the mouse cursor over nodes, ports, and spans to see tooltips with information including the number of alarms on a node (organized by severity), a port's state of service (for example, in-service, out-of-service), and the protection topology.

Right-click a node, port, or span on the detailed circuit map to initiate certain circuit actions:

- Right-click a unidirectional circuit destination node to add a drop to the circuit.
- Right-click a port containing a path trace capable card to initiate the path trace.
- Right-click a UPSR span to change the state of the path selectors in the UPSR circuit.

6.2 Manage VT1.5 Bandwidth

The ONS 15327 XTC card performs port-to-port, time-division multiplexing (TDM). Because VT1.5 multiplexing is STS-based, understanding how VT1.5 circuits use the XTC VT matrix resources is necessary to avoid unexpected depletion of the VT matrix capacity. The key VT matrix principles are as follows:

- The VT matrix has 24 logical STS ports. All VT1.5 multiplexing is achieved through these logical STS ports.

- Each VT matrix STS port has capacity for 28 VT1.5s. Therefore, the VT matrix has a capacity for 672 VT1.5 terminations.
- Because each logical STS termination on the VT matrix can carry 28 VT1.5s, the VT matrix capacity is 672 VT 1.5s (24 times 28).

The XTC card can map up to 24 STSs for VT1.5 traffic. Because one STS can carry 28 VT1.5s, the XTC card can terminate up to 672 VT1.5s or 336 VT1.5 cross-connects. However, to terminate 336 VT1.5 cross-connects:

- Each STS mapped for VT1.5 traffic must carry 28 VT1.5 circuits. If you assign each VT1.5 circuit to a different STS, the XTC card VT1.5 cross-connect capacity will be reached after you create 12 VT1.5 circuits.
- ONS 15327s must be in a BLSR. Source and drop nodes in UPSR or 1+1 (linear) protection have capacity for only 224 VT1.5 cross-connects because an additional STS is used for the protect path.

6.3 VT Tunnels

To maximize XTC VT1.5 cross-connect resources, you can tunnel VT1.5 circuits through ONS 15327 nodes. VT1.5 tunnels do not use VT matrix capacity at ONS 15327 pass-through nodes, thereby freeing the XTC card cross-connect resources for other VT1.5 circuits.

6.4 DCC Tunnels

SONET provides four DCCs for network element operations, administration, maintenance, and provisioning: one on the SONET Section layer (DCC1) and three on the SONET Line layer (DCC2, DCC3, DCC4). The ONS 15327 uses the Section DCC for ONS 15327 management and provisioning.

You can use the three Line DCCs and the Section DCC (when not used for ONS 15327 DCC terminations) to tunnel third-party SONET equipment across ONS 15327 networks. A DCC tunnel end-point is defined by Slot, Port, and DCC, where DCC can be either the Section DCC or one of the Line DCCs. You can link a Section DCC to an Line DCC and a Line DCC to a Section DCC. You can also link Line DCCs to Line DCCs and link Section DCCs to Section DCCs. To create a DCC tunnel, you connect the tunnel endpoints from one ONS 15327 optical port to another.

Table 6-6 on page 6-7 shows the DCC tunnels that you can create.

Table 6-6 DCC Tunnels

DCC	SONET Layer	SONET Bytes	OC-3, OC-12, OC-48
DCC1	Section	D1 to D3	Yes
DCC2	Line	D4 to D6	Yes
DCC3	Line	D7 to D9	Yes
DCC4	Line	D10 to D12	Yes

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

- Each ONS 15327 can have up to 32 DCC tunnel connections.
- Each ONS 15327 can have up to 10 Section DCC terminations.
- A section DCC that is terminated cannot be used as a DCC tunnel endpoint.

- A section DCC that is used as a DCC tunnel endpoint cannot be terminated.
- All DCC tunnel connections are bidirectional.

6.5 BLSR Protection Channel Circuits

You can provision circuits to carry traffic on BLSR protection channels when conditions are fault-free. Traffic routed on BLSR protection channels, called extra traffic, has lower priority than the traffic on the working channels and is unprotected. During ring or span switches, protection channel circuits are preempted and squelched. For example, in an OC-48 BLSR, STSs 25-48 can carry extra traffic when no ring switches are active, but protection channel circuits on these STSs are preempted when a ring switch occurs. When the conditions that caused the ring switch are remedied and the ring switch is removed, protection channel circuits are restored if the BLSR is provisioned as revertive.

Provisioning traffic on BLSR protection channels is performed during circuit provisioning. The protection channel check box appears whenever Fully Protected Path is unchecked on the circuit creation wizard. Refer to the *Cisco ONS 15327 Procedure Guide* for more information.

6.6 Path Trace

The SONET J1 Path Trace is a repeated, fixed-length string comprised of 64 consecutive J1 bytes. You can use the string to monitor interruptions or changes to circuit traffic. Table 6-7 shows the ONS 15327 cards that support path trace.

Table 6-7 ONS 15327 Cards Capable of Path Trace

J1 Function	Cards
Transmit and receive	XTC (DS-1) G1000-4
Receive only	OC3 IR 4 1310 OC12 IR 1310, OC12 LR 1550 OC48 IR 1310, OC48 LR 1550

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

- Automatic—The receiving port assumes that the first J1 string it receives is the baseline J1 string.
- Manual—The receiving port uses a string that you manually enter as the baseline J1 string.

SONET Topologies

This chapter explains Cisco ONS 15327 SONET topologies. To provision topologies, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

7.1 Bidirectional Line Switched Rings

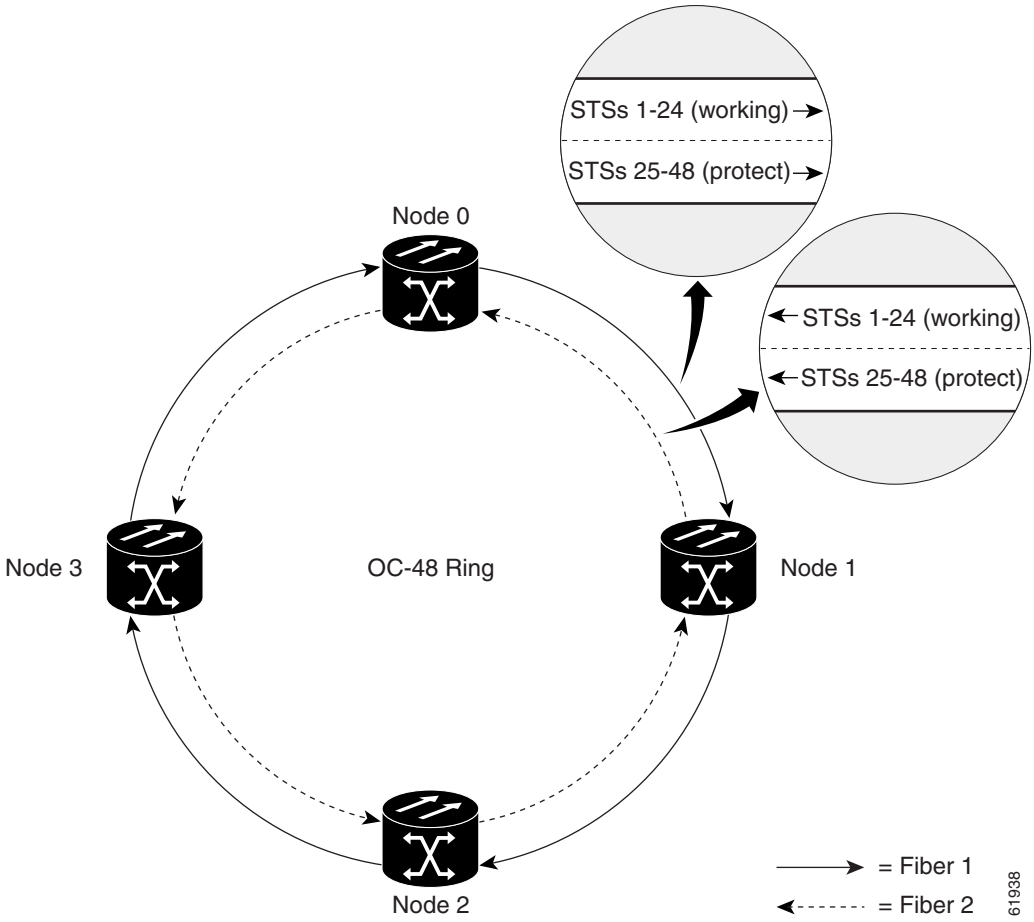
One ONS 15327 can support two concurrent BLSRs each BLSR can have up to 32 ONS 15327s. Because the working and protect bandwidths must be equal, you can create only OC-12, or OC-48 BLSRs. For information about BLSR protection channels, see the "BLSR Protection Channel Circuits" section on page 6-8.

Note For best performance, BLSRs should have one LAN connection for every ten nodes in the BLSR.

7.1.1 BLSR Functionality

The Cisco ONS 15327 supports two-fiber BLSRs (the ONS 15454 also supports four-fiber BLSRs); each fiber in a two-fiber BLSR is divided into working and protect bandwidths. For example, in an OC-48 BLSR (Figure 7-1 on page 7-2), STSs 1 to 24 carry the working traffic, and STSs 25 to 48 are reserved for protection. Working traffic (STSs 1 to 24) travels in one direction on one fiber and in the opposite direction on the second fiber. The Cisco Transport Controller (CTC) circuit routing routines calculate the "shortest path" for circuits based on many factors, including user requirements, traffic patterns, and distance. For example, in Figure 7-1, 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 on Fiber 2 through Node 3 and Node 2. Traffic from Node 0 to Node 2 (or Node 1 to Node 3) can be routed on either fiber, depending on circuit provisioning requirements and traffic loads.

Figure 7-1 Four-Node BLSR



The SONET K1, K2, and K3 bytes carry the information that governs BLSR protection switches. Each BLSR node monitors the K bytes to determine when to switch the SONET signal to an alternate physical path. The K bytes communicate failure conditions and actions taken between nodes in the ring.

If a break occurs on one fiber, working traffic targeted for a node beyond the break switches to the protect bandwidth on the second fiber. The traffic travels in 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 7-2 on page 7-3 shows a traffic pattern sample on a four-node BLSR.

Figure 7-2 Four-Node BLSR Traffic Pattern Example

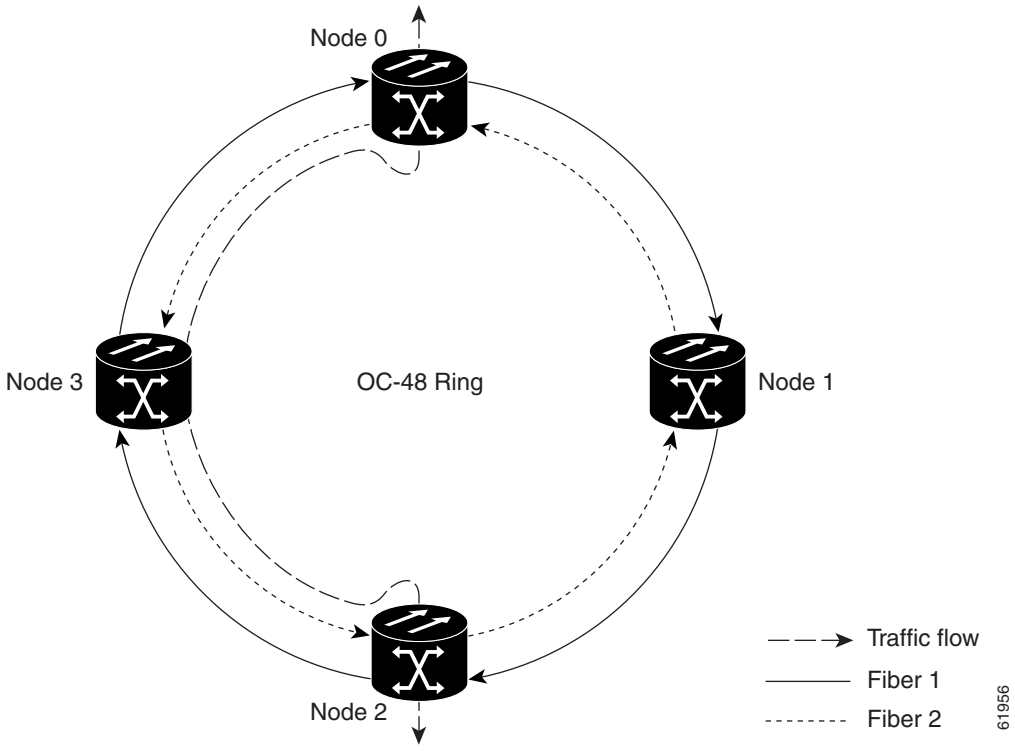
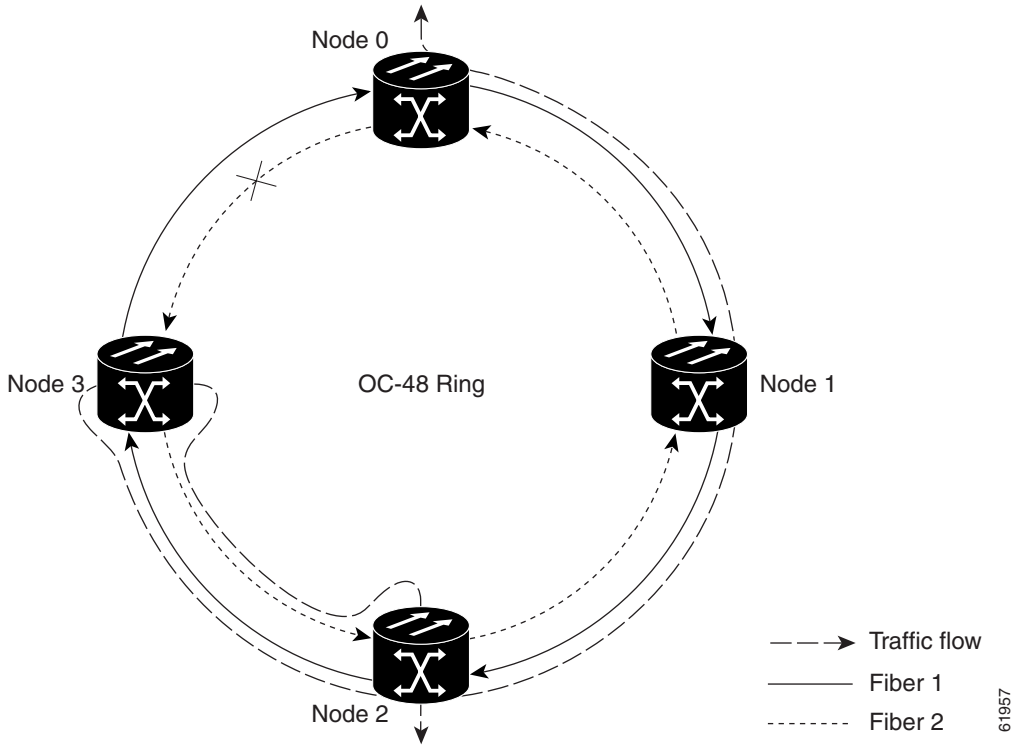


Figure 7-3 on page 7-4 shows how traffic is rerouted following a line break between Node 0 and Node 3.

- All circuits originating on Node 0 carried traffic to Node 2 on Fiber 2 are switched to the protect bandwidth of Fiber 1. For example, a circuit carrying traffic on STS-1 on Fiber 2 is switched to STS-25 on Fiber 1. A circuit carried on STS-2 on Fiber 2 is switched to STS-26 on Fiber 1. Fiber 1 carries the circuit to Node 3 (the original routing destination). Node 3 switches the circuit back to STS-1 on Fiber 2 where it is routed to Node 2 on STS-1.
- Circuits originating on Node 2 that normally carried traffic to Node 0 on Fiber 1 are switched to the protect bandwidth of Fiber 2 at Node 3. For example, a circuit carrying traffic on STS-2 on Fiber 1 is switched to STS-26 on Fiber 2. Fiber 2 carries the circuit to Node 0 where the circuit is switched back to STS-2 on Fiber 1 and then dropped to its destination.

Figure 7-3 Four-Node BLSR Traffic Pattern Following a Line Break



7.1.2 BLSR Bandwidth

BLSR nodes can terminate traffic coming from either side of the ring. Therefore, BLSRs are suited for distributed node-to-node traffic applications such as interoffice networks and access networks.

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

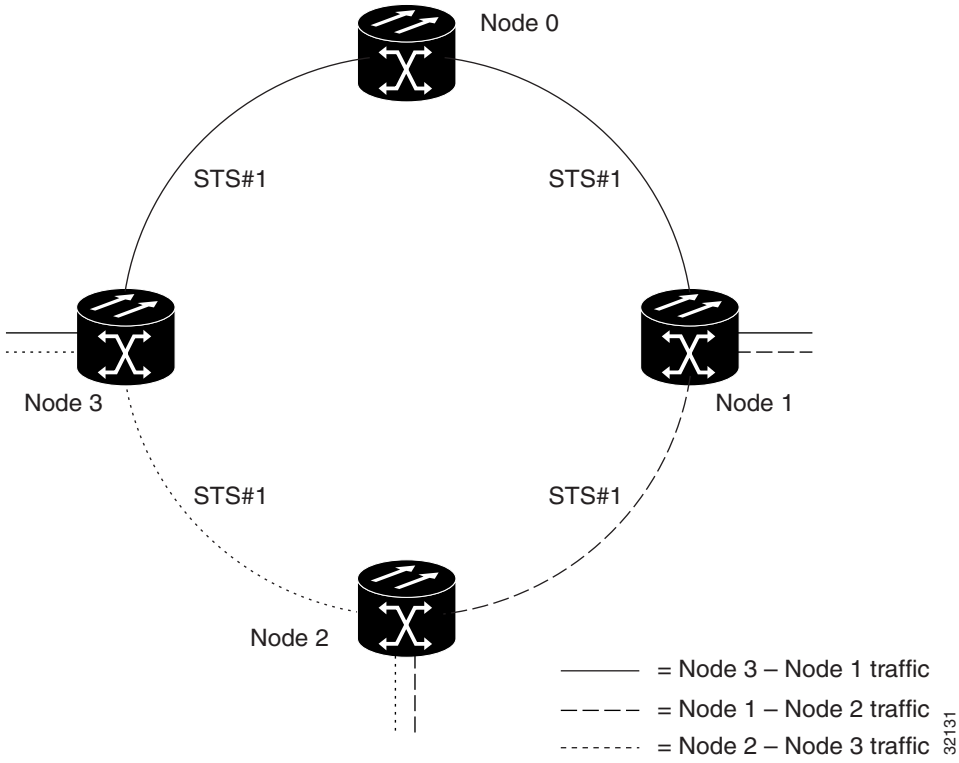
Table 7-1 BLSR Capacity

OC Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
OC-12	STS1-6	STS 7-12	6 x N[1] - PT[2]
OC-48	STS 1-24	STS 25-48	24 x N - PT

1. N equals the number of ONS 15327 nodes configured as BLSR nodes.
2. PT equals the number of STS-1 circuits passed through ONS 15327 nodes in the ring (capacity can vary depending on the traffic pattern).

Figure 7-4 on page 7-5 shows an example of BLSR bandwidth reuse. The same STS 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 7-4 BLSR Bandwidth Reuse



7.1.3 BLSR Application Example

Figure 7-5 on page 7-6 shows a BLSR implementation example. A regional long-distance network connects to other carriers at Node 0. Traffic is delivered to the service provider's major hubs.

- Carrier 1 delivers two DS-3s over one OC-3 spans to Node 0. Carrier 2 provides two DS-3s directly. Node 0 receives the signals and delivers them around the ring to the appropriate node.
- The ring also brings 14 DS-1s back from each remote site to Node 0. Intermediate nodes serve these shorter regional connections.
- The ONS 15327 OC-3 card supports a total of four OC-3 ports so that two additional OC-3 spans can be added at little cost.

Figure 7-5 Five-Node BLSR

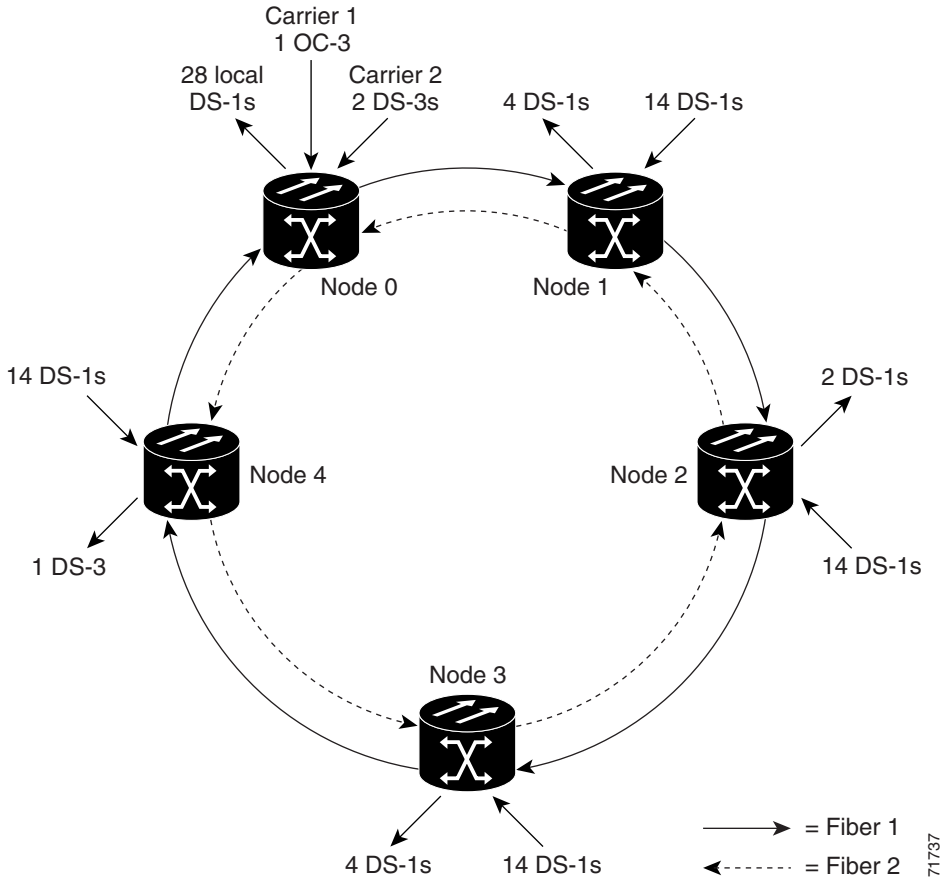


Figure 7-6 shows the shelf assembly layout for Node 0, which has no free slots.

Figure 7-6 Shelf Assembly Layout for Node 0 in Figure 7-5

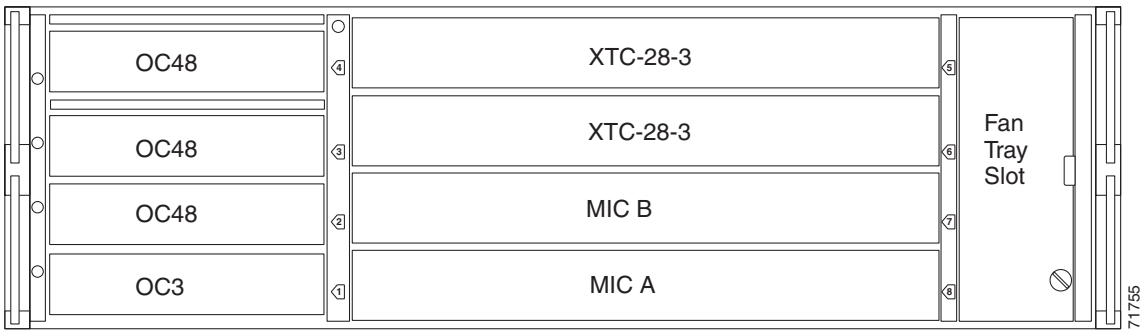
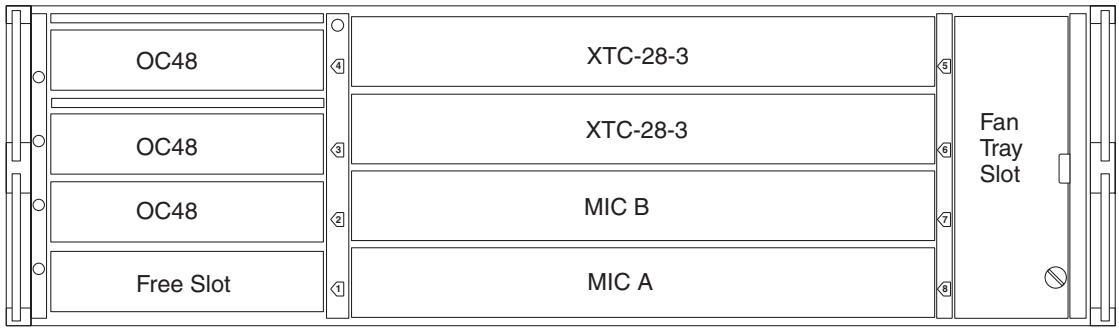


Figure 7-7 on page 7-7 shows the shelf assembly layout for the remaining sites in the ring. In this BLSR configuration, an additional three DS-3s at Nodes 1, 2, 3, and 4 can be activated. Each site has free slots for future traffic needs.

Figure 7-7 Shelf Assembly Layout for Nodes 1 – 4 in Figure 7-5

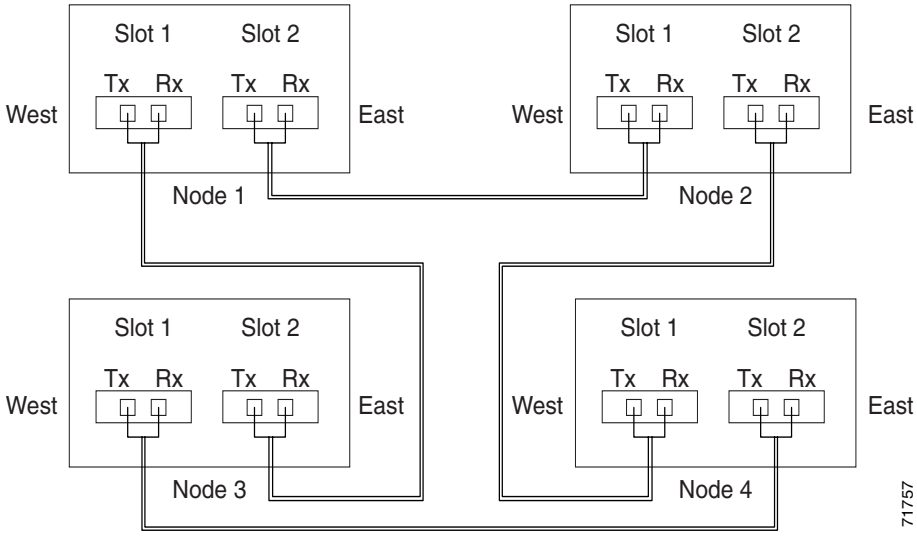


7.1.4 BLSR Fiber Connections

Plan your fiber connections and use the same plan for all BLSR nodes. For example, make the east port the farthest slot to the right and the west port the farthest slot to the left. Plug fiber connected to an east port at one node into the west port on an adjacent node. Figure 7-8 shows fiber connections for a BLSR with trunk (span) cards in Slot 1 (west) and Slot 2 (east). See the *Cisco ONS 15327 Procedure Guide* for fiber connection procedures.

Note Always plug the transmit (Tx) connector of an OC-N card at one node into the receive (Rx) connector of an OC-N card at the adjacent node. Cards will display an SF LED when Tx and Rx connections are mismatched.

Figure 7-8 Connecting Fiber to a Four-Node, Two-Fiber BLSR



7.2 Unidirectional Path Switched Rings

UPSRs provide duplicate fiber paths around the ring. Working traffic flows in one direction and protection traffic flows in the opposite direction. If a problem occurs with the working traffic path, the receiving node switches to the path coming from the opposite direction.

CTC automates ring configuration. UPSR traffic is defined within the ONS 15327 on a circuit-by-circuit basis. If a path-protected circuit is not defined within a 1+1 or BLSR line protection scheme and path protection is available and specified, CTC uses UPSR as the default.

A UPSR circuit requires two DCC-provisioned optical spans per node. UPSR circuits can be created across these spans until their bandwidth is consumed.

Because each traffic path is transported around the entire ring, UPSRs are best suited for networks where traffic concentrates at one or two locations and is not widely distributed. UPSR capacity is equal to its bit rate. Services can originate and terminate on the same UPSR, or they can be passed to an adjacent access or interoffice ring for transport to the service-terminating location.

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

7.2.1 UPSR Bandwidth

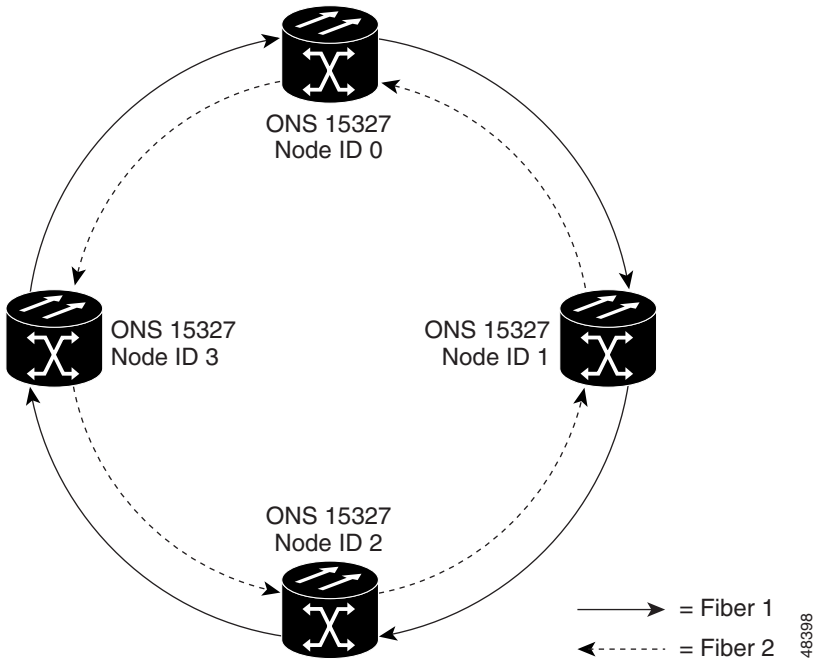
The span bandwidth consumed by a UPSR circuit is two times the circuit bandwidth, because the circuit is duplicated. The cross-connection bandwidth consumed by a UPSR circuit is three times the circuit bandwidth at the source and destination nodes only. The cross-connection bandwidth consumed by an intermediate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

The UPSR circuit limit is the sum of the optical bandwidth containing 10 section data communications channels (SDCCs) divided by two if you are using redundant XTC cards. The spans can be of any bandwidth from OC-3 to OC-48. The circuits can be of any size from VT1.5 to 48c.

7.2.2 UPSR Application Example

Figure 7-9 on page 7-9 shows a basic UPSR configuration. If Node ID 0 sends a signal to Node ID 2, the working signal travels on the working traffic path through Node ID 1. The same signal is also sent on the protect traffic path through Node ID 3.

Figure 7-9 Basic Four-Node UPSR



If a fiber break occurs (Figure 7-10 on page 7-10), Node ID 2 switches its active receiver to the protect signal coming through Node ID 3.

Figure 7-10 UPSR with a Fiber Break

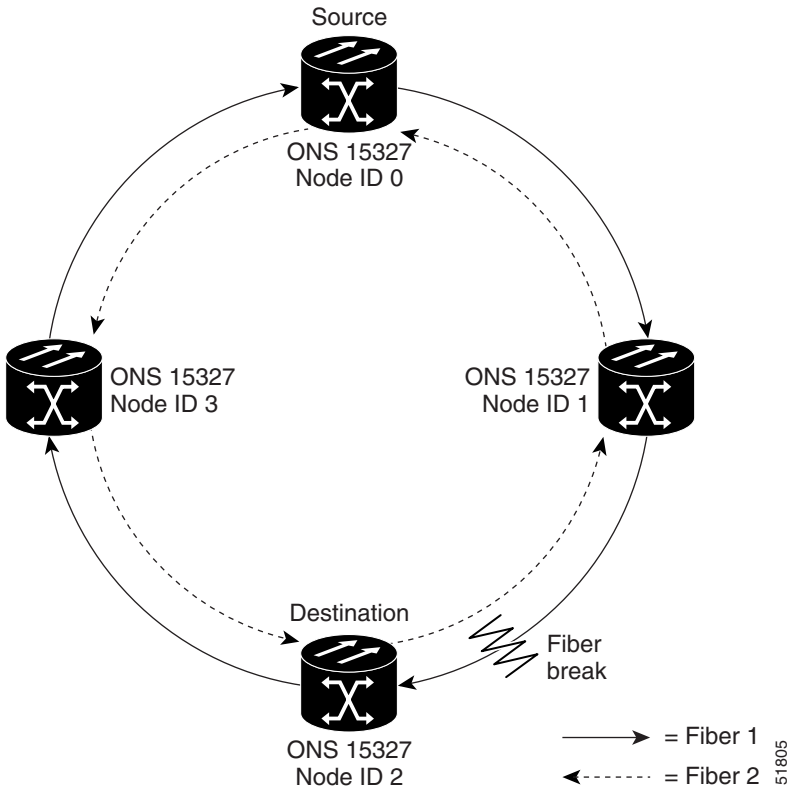
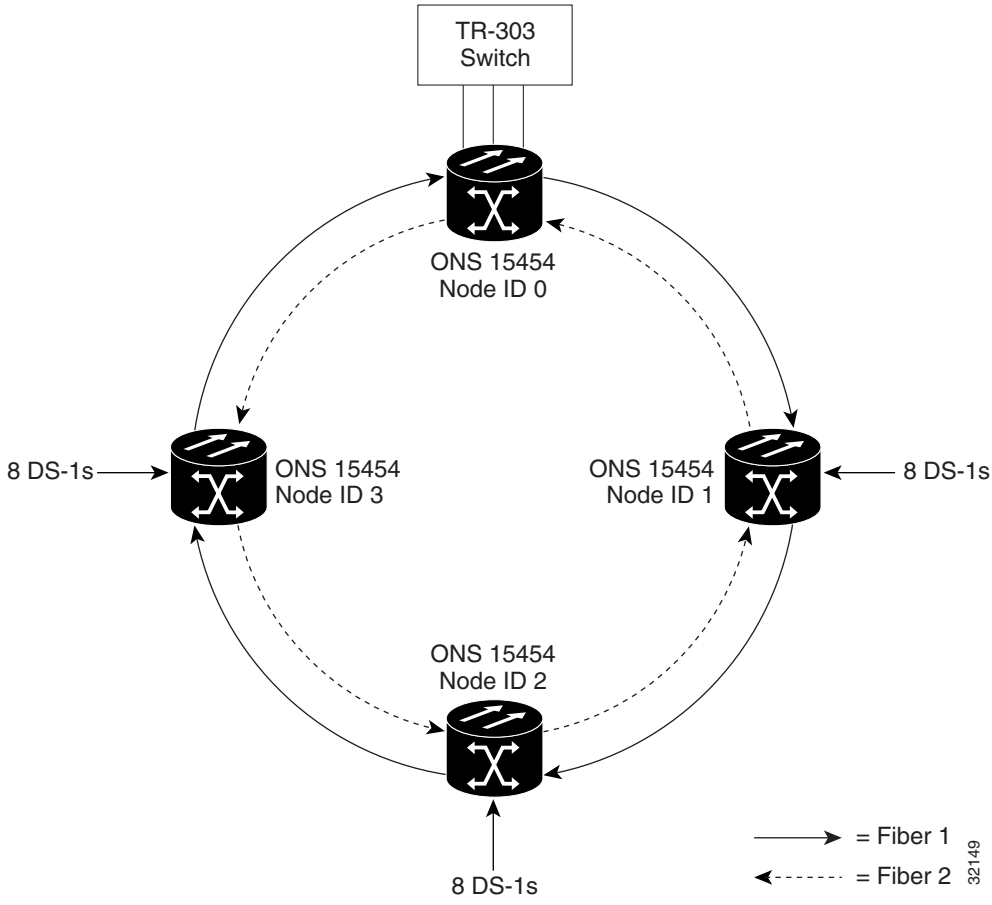


Figure 7-11 on page 7-11 shows a common UPSR application. OC-3 optics provide remote switch connectivity to a host TR-303 switch. In the example, each remote switch requires eight DS-1s to return to the host switch. Figure 7-12 on page 7-11 and Figure 7-13 on page 7-12 show the shelf layout for each site.

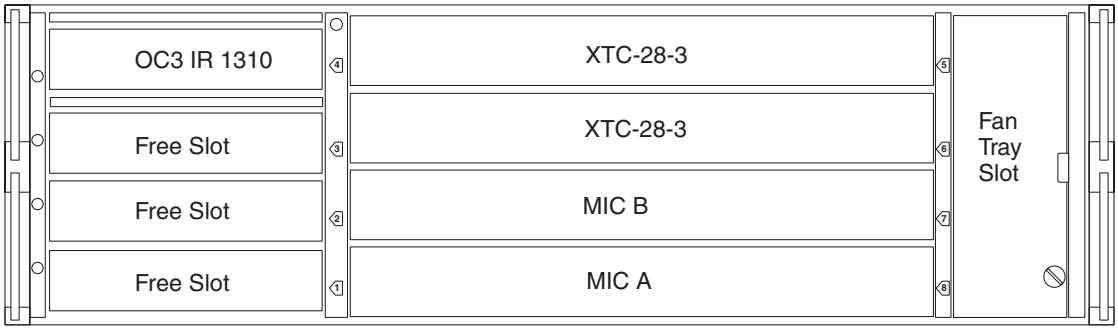
Figure 7-11 Four-Port OC-3 UPSR



Node ID 0 has two XTC-28-3 cards to provide 28 active DS-1 ports. The other sites only require XTC-14 cards to handle the 14 DS-1s to and from the remote switch. You can use the other half of each ONS 15327 shelf assembly to provide support for a second or third ring to other existing or planned remote sites.

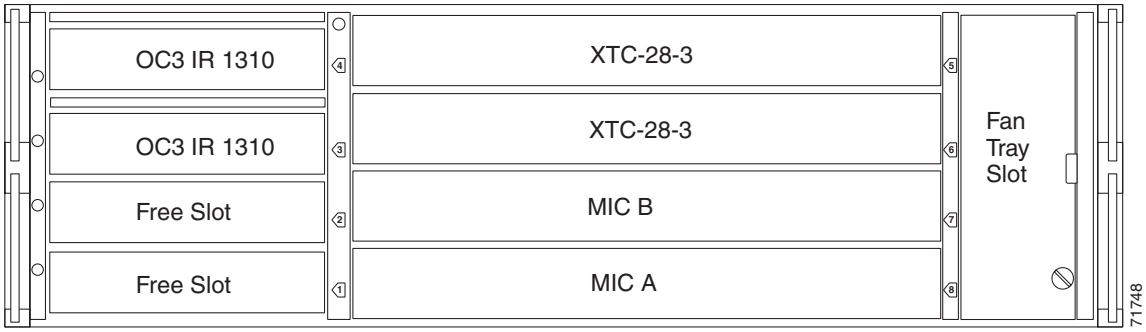
In the OC-3 UPSR sample, Node ID 0 contains two XTC 28-3 cards and two OC3 IR 4 1310 cards. Two free slots can be provisioned with cards or left empty. Figure 7-12 shows the shelf setup for these cards.

Figure 7-12 Layout of Node ID 0 in the OC-3 UPSR Example in Figure 7-11



In the Figure 7-11 example, Nodes IDs 1, 2, and 3 each contain two XTC cards and two OC3 IR 4 1310 cards. Two free slots exist. They can be provisioned with other cards or left empty. Figure 7-13 shows the shelf assembly setup for this configuration sample.

Figure 7-13 Layout of Node IDs 1—3 in the OC-3 UPSR Example in Figure 7-11



7.3 Subtending Rings

The ONS 15327 supports up to ten SONET SDCCs. Table 7-2 shows the SONET rings that can be created on each ONS 15327 node using redundant XTC cards.

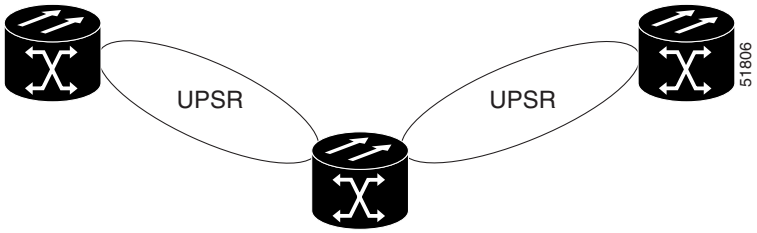
Table 7-2 ONS 15327 Rings with Redundant XTC Cards

Ring Type	Maximum rings per node
BLSRs	2
UPSR	5[1]

1. See the "Unidirectional Path Switched Rings" section on page 7-8

Subtending rings reduce the number of nodes and cards required and reduce external shelf-to-shelf cabling. Figure 7-14 shows an ONS 15327 with two subtending rings.

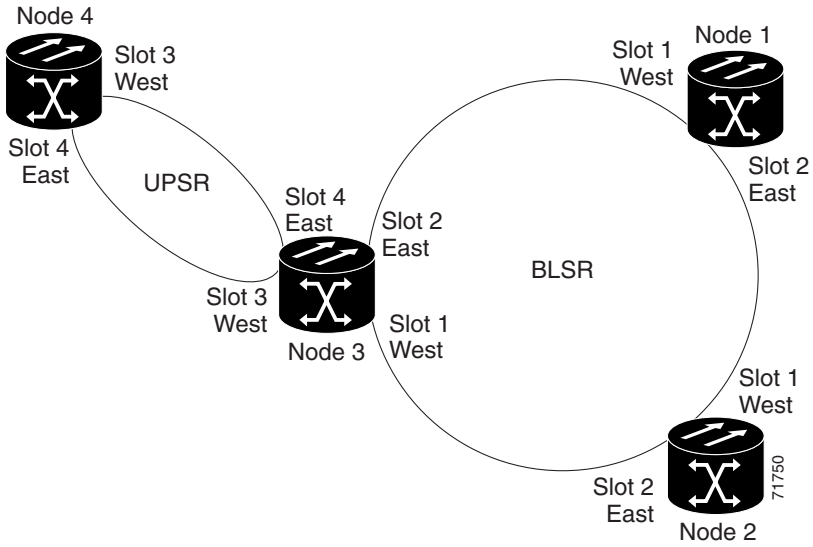
Figure 7-14 ONS 15327 with Two Subtending UPSRs



7.3.1 Subtending Ring Examples

Figure 7-15 shows a UPSR subtending from a BLSR. In this example, Node 3 is the only node serving both the BLSR and UPSR. OC-N cards in Slots 1 and 2 serve the BLSR, and OC-N cards in Slots 3 and 4 serve the UPSR.

Figure 7-15 UPSR Subtending from a BLSR

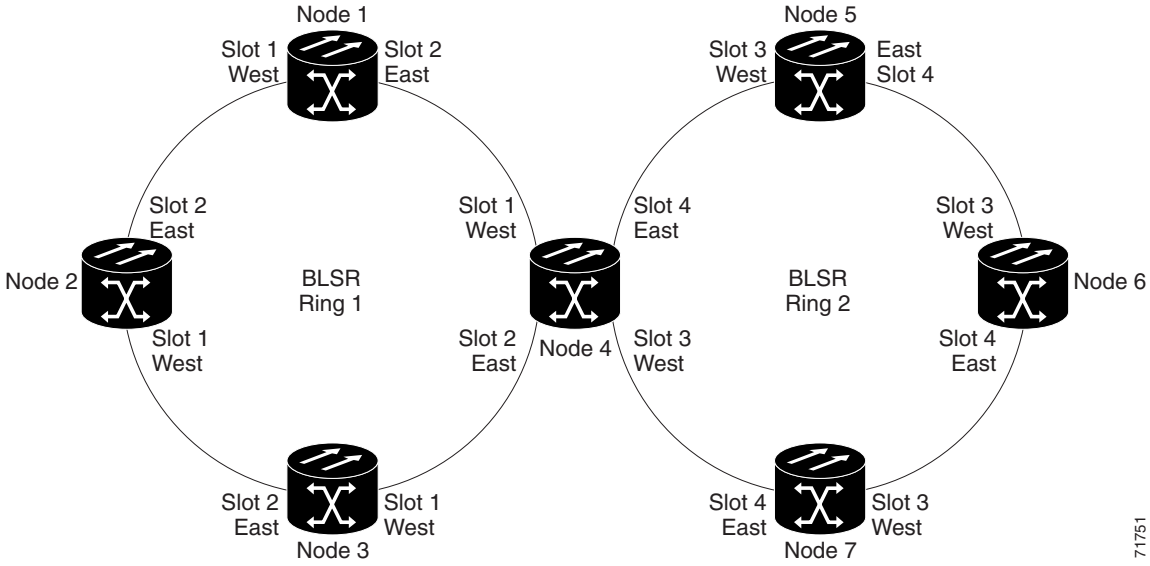


The ONS 15327 can support two BLSRs on the same node. This capability allows you to deploy an ONS 15327 in applications requiring SONET digital cross connect systems (DCSs) or multiple SONET add/drop multiplexers (ADMs).

Figure 7-16 on page 7-14 shows two BLSRs shared by one ONS 15327. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7. Two BLSR rings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 1 and 2, and Ring 2 uses cards in Slots 3 and 4.

Note Nodes in different BLSRs can have the same node ID.

Figure 7-16 BLSR Subtending from a BLSR



After subtending two BLSRs, you can route circuits from nodes in one ring to nodes in the second ring. For example, in Figure 7-16 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.

7.3.2 Connecting ONS 15327 Nodes and ONS 15454 Nodes

You can install ONS 15327 nodes into a network comprised entirely of ONS 15327 nodes or into a network that has a mix of ONS 15327 and ONS 15454 nodes. The ONS 15327 interoperates with the ONS 15454 in linear, UPSR, and 2-fiber BLSR configurations. Because connection procedures for both types of nodes are the same (for example, adding or dropping nodes from a UPSR or linear configuration, or creating DCCs), follow the instructions in the *Cisco ONS 15327 Procedure Guide* whenever you make connections between ONS 15454 and ONS 15327 nodes. Figure 7-17 shows a basic linear or UPSR connection between ONS 15327 and ONS 15454 nodes.

Figure 7-17 Linear or UPSR Connection between ONS 15454 and ONS 15327 Nodes

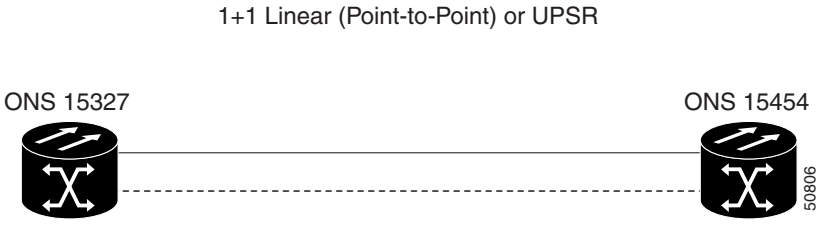
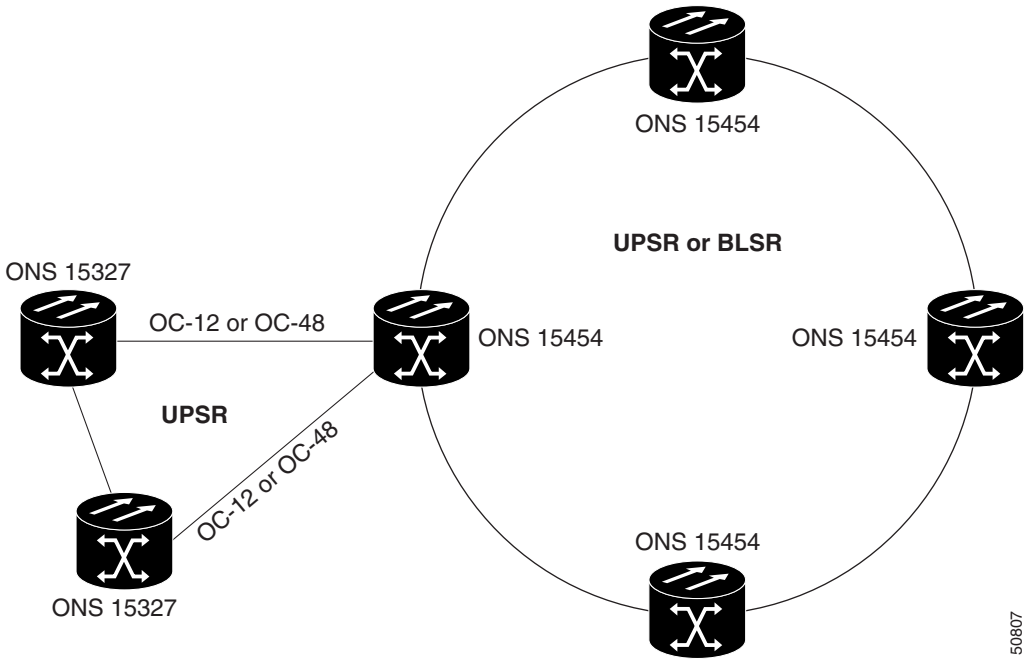


Figure 7-18 on page 7-15 shows a ring of ONS 15327s subtended from a ring of ONS 15454s.

Figure 7-18 ONS 15327 Ring Subtended from an ONS 15454 Ring

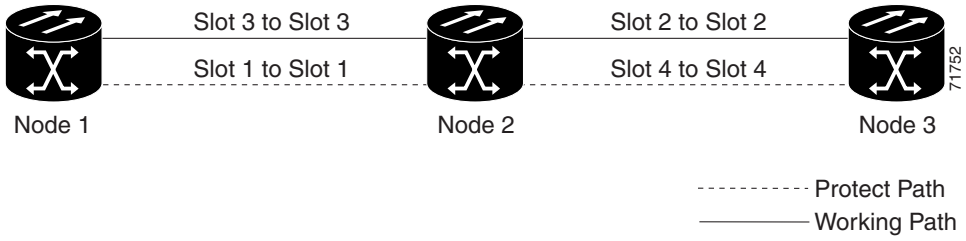


7.4 Terminal Point-to-Point and Linear ADM Configurations

You can configure ONS 15327s in a terminal point-to-point network (2 nodes) or as a line of add/drop multiplexers (ADMs) (3 or more nodes) by configuring one set of OC-N cards as the working path and a second set as the protect path. Unlike rings, terminal and linear ADMs require that the OC-N cards at each node be in 1+1 protection to ensure that a break to the working line is automatically routed to the protect line.

Figure 7-19 shows three ONS 15327s in a linear ADM configuration. Working traffic flows from Slot 3/Node 1 to Slot 3/Node 2, and from Slot 2/Node 2 to Slot 2/Node 3. You create the protect path by placing Slot 3 in 1+1 protection with Slot 1 at Nodes 1 and 2, and Slot 2 in 1+1 protection with Slot 4 at Nodes 2 and 3.

Figure 7-19 Linear ADM Configuration



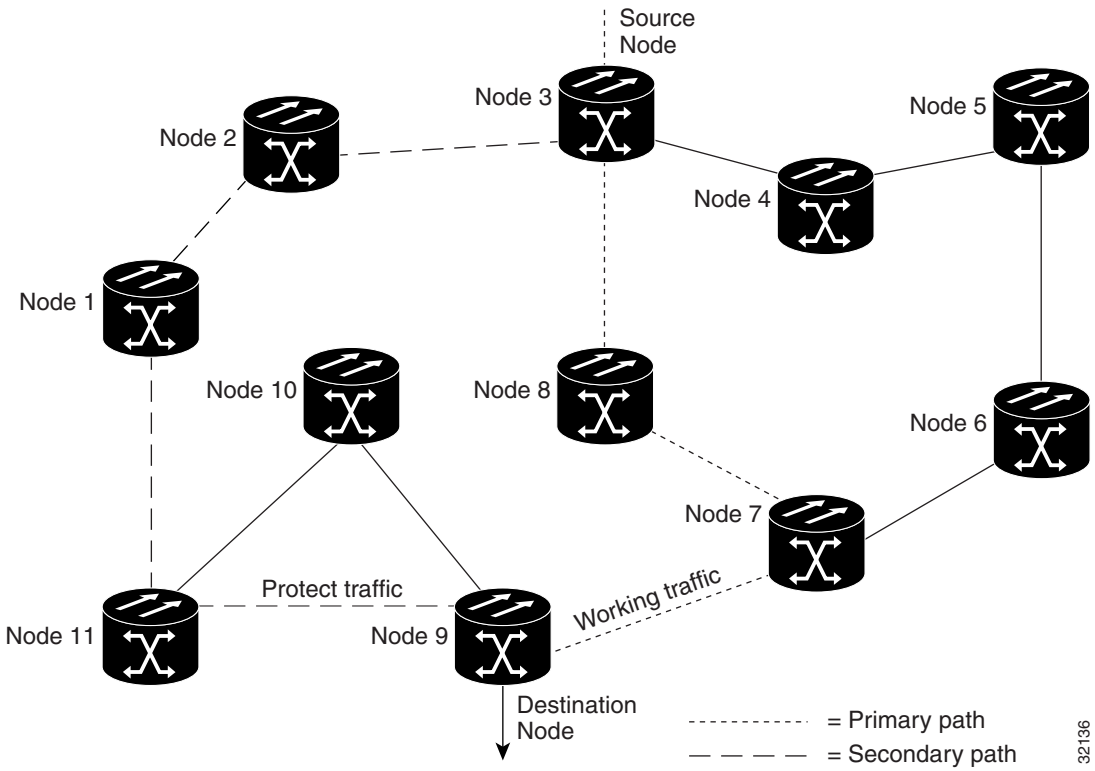
7.5 Path-Protected Mesh Networks

In addition to single BLSRs, UPSRs and terminal point-to-point or linear ADMs, you can extend ONS 15327 traffic protection by creating path-protected mesh networks (PPMNs). PPMNs include multiple ONS 15327 SONET topologies and extend the protection provided by a single UPSR to the meshed architecture of several interconnecting rings. In a PPMN, circuits travel diverse paths through a network of single or multiple meshed rings. When you create circuits, you can have CTC automatically route circuits across the PPMN, or you can manually route them. You can also choose levels of circuit protection. For example, if you choose full protection, CTC creates an alternate route for the circuit in addition to the main route. The second route follows a unique path through the network between the source and destination and sets up a second set of cross-connections.

For example, in Figure 7-20, a circuit is created from Node 3 to Node 9. CTC determines that the shortest route between the two nodes passes through Node 8 and Node 7, shown by the dotted line, and automatically creates cross-connections at Nodes 3, 8, 7, and 9 to provide the primary circuit path.

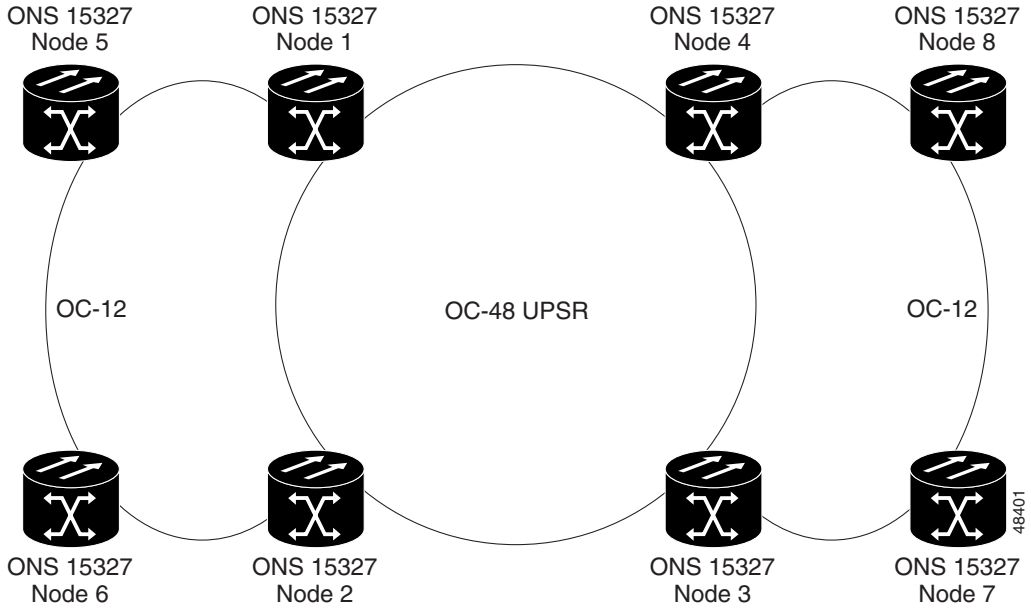
If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 which, in this example, passes through Nodes 2, 1, and 11. Cross-connections are automatically created at Nodes 3, 2, 1, 11, and 9, shown by the dashed line. If a failure occurs on the primary path, traffic switches to the second circuit path. In this example, Node 9 switches from the traffic coming in from Node 7 to the traffic coming in from Node 11 and service resumes. The switch occurs within 50 ms.

Figure 7-20 Path-Protected Mesh Network



PPMN also allows spans with different SONET speeds to be mixed together in "virtual rings." Figure 7-21 on page 7-17 shows Nodes 1, 2, 3, and 4 in a standard OC-48 ring. Nodes 5, 6, 7, and 8 link to the backbone ring through OC-12 fiber. The "virtual ring" formed by Nodes 5, 6, 7, and 8 uses both OC-48 and OC-12 cards.

Figure 7-21 PPMN Virtual Ring



7.6 Four Node Configurations

You can link multiple ONS 15327s using their OC-N cards (also known as creating a fiber-optic bus) to accommodate more access traffic than a single ONS 15327 can support. For example, to drop more than 28 DS-1s or 3 DS-3s (the maximum that can be aggregated in a single node), you can link the nodes but not merge multiple nodes into a single ONS 15327. You can link nodes with OC-12 or OC-48 fiber spans as you would link any other two network nodes. The nodes can be grouped in one facility to aggregate more local traffic.

7.7 Optical Speed Upgrades

A span is the optical fiber connection between two ONS 15327 nodes. In a span (optical speed) upgrade, the transmission rate of a span is upgraded from a lower to a higher OC-N signal but all other span configuration attributes remain unchanged. With multiple nodes, a span upgrade is a coordinated series of upgrades on all nodes in the ring or protection group.

To perform a span upgrade, the higher-rate optical card must replace the lower-rate card in the same slot. All spans in the network must be upgraded. The protection configuration of the original lower-rate optical card (BLSR, UPSR, and 1+1) is retained for the higher-rate optical card.

When performing span upgrades on a large number of nodes, Cisco recommends that you upgrade all spans in a network consecutively and in the same maintenance window. Until all spans are upgraded, mismatched card types will be present.

Cisco recommends using the Span Upgrade Wizard to perform span upgrades. Although you can also use the manual span upgrade procedures, the manual procedures are mainly provided as error recovery for the wizard. The Span Upgrade Wizard and the manual span upgrade procedures require at least two

technicians (one at each end of the span) who can communicate with each other during the upgrade. Upgrading a span is non-service affecting and will cause no more than three switches, each of which is less than 50 ms in duration.

Note Span upgrades do not upgrade SONET topologies, for example, a 1+1 group to a BLSR. See the *Cisco ONS 15327 Procedure Guide* for topology upgrade procedures.

7.7.1 Span Upgrade Wizard

The Span Upgrade Wizard automates all steps in the manual span upgrade procedure (BLSR, UPSR, and 1+1). The wizard can upgrade both lines of a 1+1 group; the wizard upgrades UPSRs and BLSRs one line at a time. The Span Upgrade Wizard requires that spans have DCCs enabled.

The Span Upgrade Wizard provides no way to back out of an upgrade. In the case of an error, you must exit the wizard and initiate the manual procedure to either continue with the upgrade or back out of it. To continue with the manual procedure, examine the standing conditions and alarms to identify the stage in which the wizard failure occurred.

7.7.2 Manual Span Upgrades

Manual span upgrades are mainly provided as error recovery for the Span Upgrade Wizard, but they can be used to perform span upgrades. You can perform a manual span upgrade on a BLSR, UPSR, and on a 1+1 protection group.

Downgrading can be performed to back out of a span upgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate card type and install a lower-rate card. You cannot downgrade if circuits exist on the STSs that will be removed (the higher STSs).

IP Networking

This chapter provides seven scenarios showing Cisco ONS 15327s in common IP network configurations. The chapter does not provide a comprehensive explanation of IP networking concepts and procedures. For IP set up instructions, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

Note To connect ONS 15327s to 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 15327s can be connected in many different ways within an IP environment:

- They can be connected to LANs through direct connections or a router.
- IP subnetting can create ONS 15327 login node groups, which allow you to provision non-DCC connected nodes in a network.
- Different IP functions and protocols can be used to achieve specific network goals. For example, Proxy Address Resolution Protocol (ARP) enables one LAN-connected ONS 15327 to serve as a gateway for ONS 15327s that are not connected to the LAN.
- You can create static routes to enable connections among multiple CTC sessions with ONS 15327s that reside on the same subnet but have different destination IP addresses.
- If ONS 15327s are connected to OSPF networks, ONS 15327 network information is automatically communicated across multiple LANs and WANs.
- The ONS 15327 proxy server controls the visibility and accessibility between CTC computers and ONS 15327 element nodes.

8.2 IP Addressing Scenarios

ONS 15327 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 15327s in IP networks.

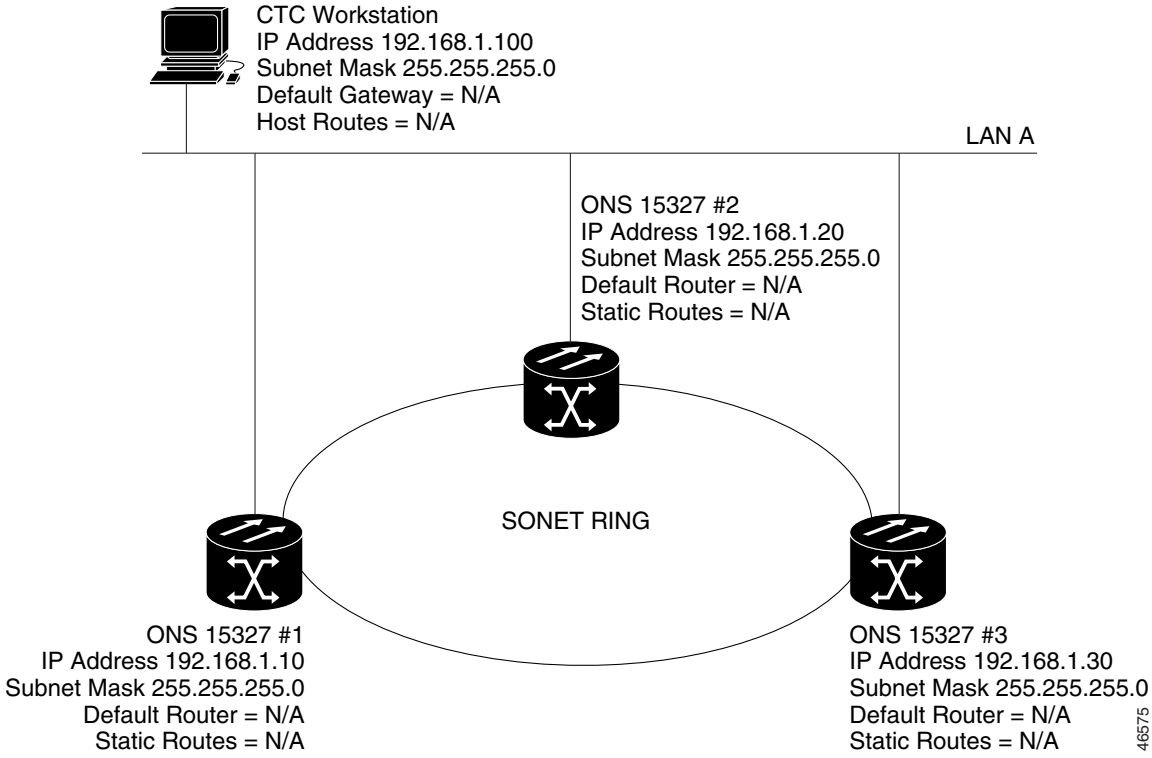
Table 8-1 General ONS 15327 IP Troubleshooting Checklist

Item	What to check
Link integrity	Verify that link integrity exists between: • CTC computer and network hub/switch • ONS 15327s (wire-wrap pins or RJ-45 port) and network hub/switch • Router ports and hub/switch ports
ONS 15327 hub/switch ports	Verify connectivity. If connectivity problems occur, set the hub or switch port that is connected to the ONS 15327 to 10 Mbps half-duplex.
Ping	Ping the node to test connections between computers and ONS 15327s.
IP addresses/subnet masks	Verify that ONS 15327 IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify that ONS 15327 optical trunk ports are in service; DCC is enabled on each trunk port.

8.2.1 Scenario 1: CTC and ONS 15327s on the Same Subnet

Scenario 1 shows a basic ONS 15327 LAN configuration (Figure 8-1 on page 8-3). The ONS 15327s and CTC computer reside on the same subnet. All ONS 15327s connect to LAN A, and all ONS 15327s have DCC connections.

Figure 8-1 Scenario 1: CTC and ONS 15327s on the Same Subnet

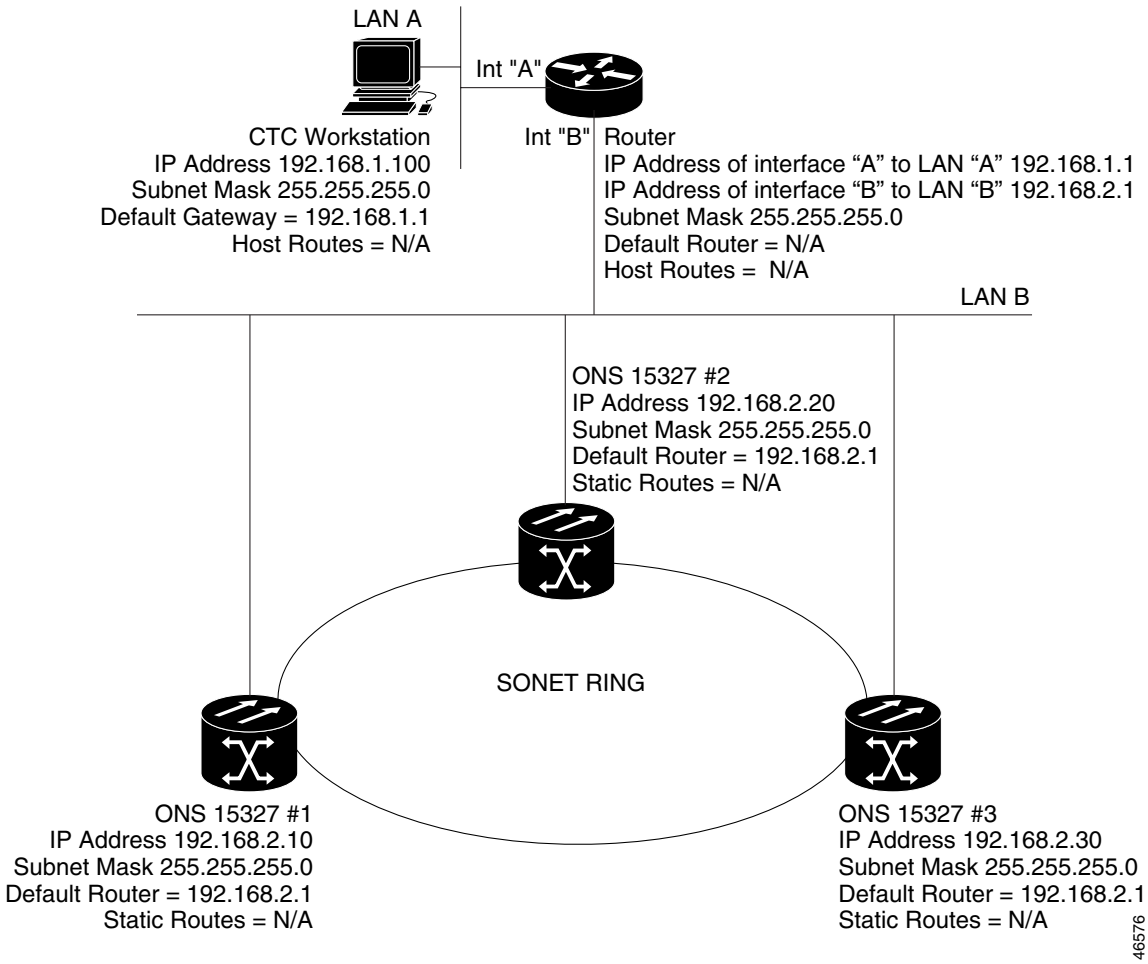


8.2.2 Scenario 2: CTC and ONS 15327s Connected to a Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 8-2 on page 8-4). The ONS 15327s 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 Figure 8-2 on page 8-4, a DHCP server is not available.

Figure 8-2 Scenario 2: CTC and ONS 15327s Connected to Router

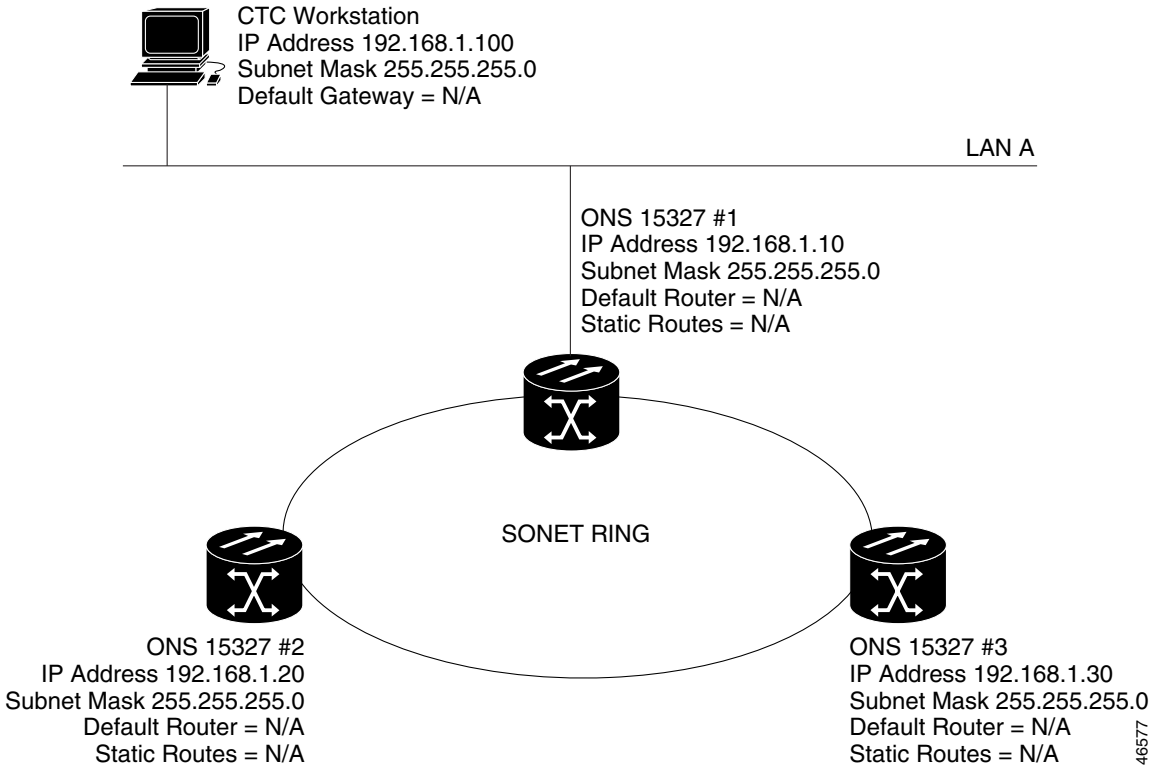


8.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15327 Gateway

Scenario 3 is similar to Scenario 1, but only one ONS 15327 (Node 1) connects to the LAN (Figure 8-3 on page 8-5). Two ONS 15327s (Nodes 2 and 3) connect to ONS 15327 #1 through the SONET DCC. Because all three ONS 15327s are on the same subnet, Proxy ARP enables Node 1 to serve as a gateway for Nodes 2 and 3.

Note This scenario assumes all CTC connections are to Node 1. If you connect a laptop to either Nodes 2 or 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, you will need to create static routes (see Scenario 5) or enable the ONS 15327 proxy server (see Scenario 7).

Figure 8-3 Scenario 3: Using Proxy ARP



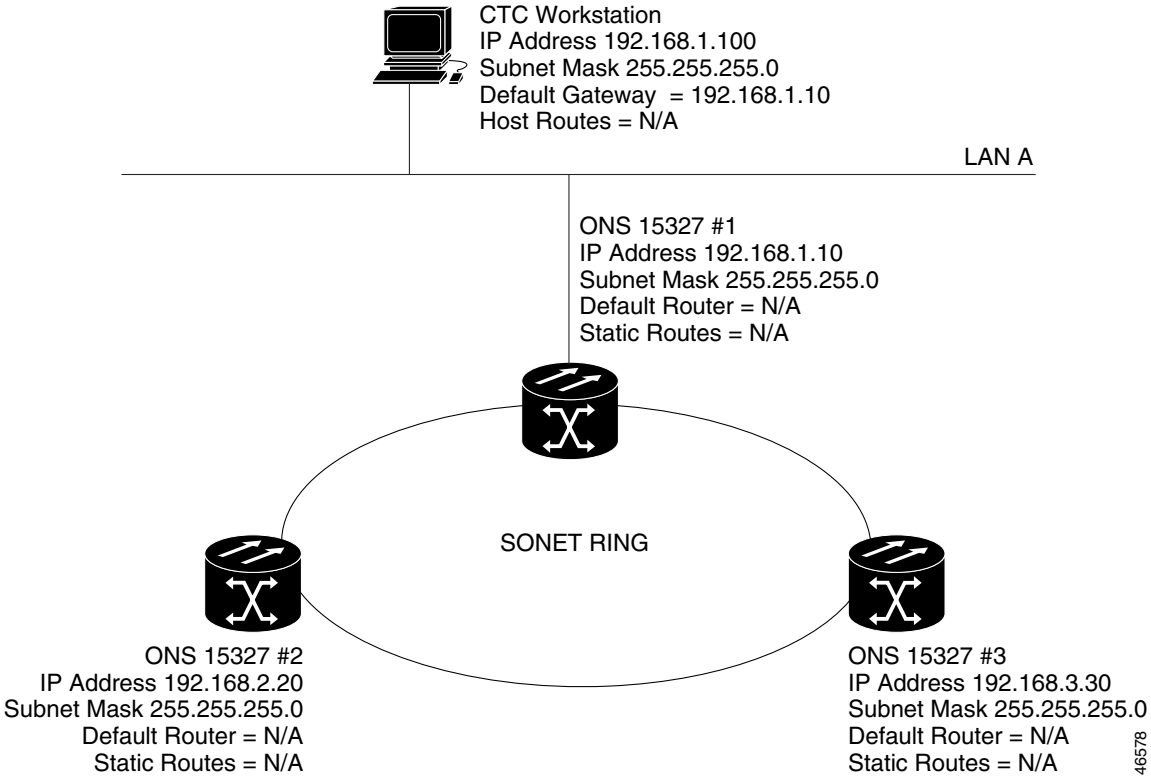
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of 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 15327 to respond to the ARP request for ONS 15327s that are not connected to the LAN. (ONS 15327 proxy ARP requires no user configuration.) The DCC-connected ONS 15327s must reside on the same subnet. When a LAN device sends an ARP request to an ONS 15327 that is not connected to the LAN, the gateway ONS 15327 returns its MAC address to the LAN device. The LAN device then sends the datagram for the remote ONS 15327 to the MAC address of the proxy ONS 15327. The proxy ONS 15327 uses its routing table to forward the datagram to the non-LAN ONS 15327.

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 on page 8-6). Node 1 and the CTC computer are on subnet 192.168.1.0. Proxy ARP is not used because the network includes different subnets. In order for the CTC computer to communicate with Nodes 2 and 3, Node 1 is entered as the default gateway on the CTC computer.

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



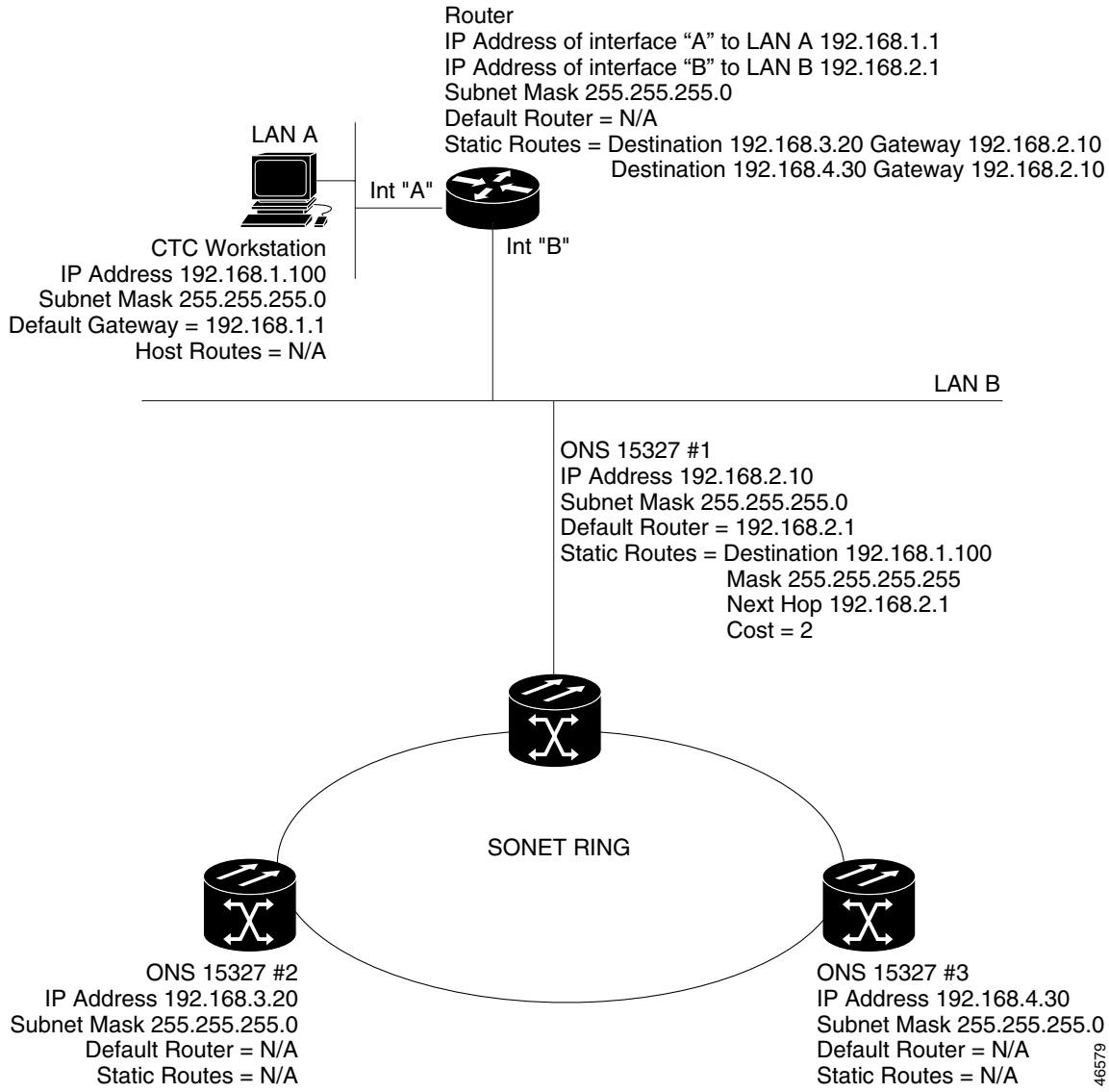
8.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15327s to CTC sessions on one subnet that are connected by a router to ONS 15327s 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 15327s residing on the same subnet.

In Figure 8-5 on page 8-7, 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 15327s residing on different subnets are connected through Node 1 to the router through interface B. Because Nodes 2 and 3 are on different subnets, proxy ARP does not enable Node 1 as a gateway. To connect to CTC computers on LAN A, a static route is created on Node 1.

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

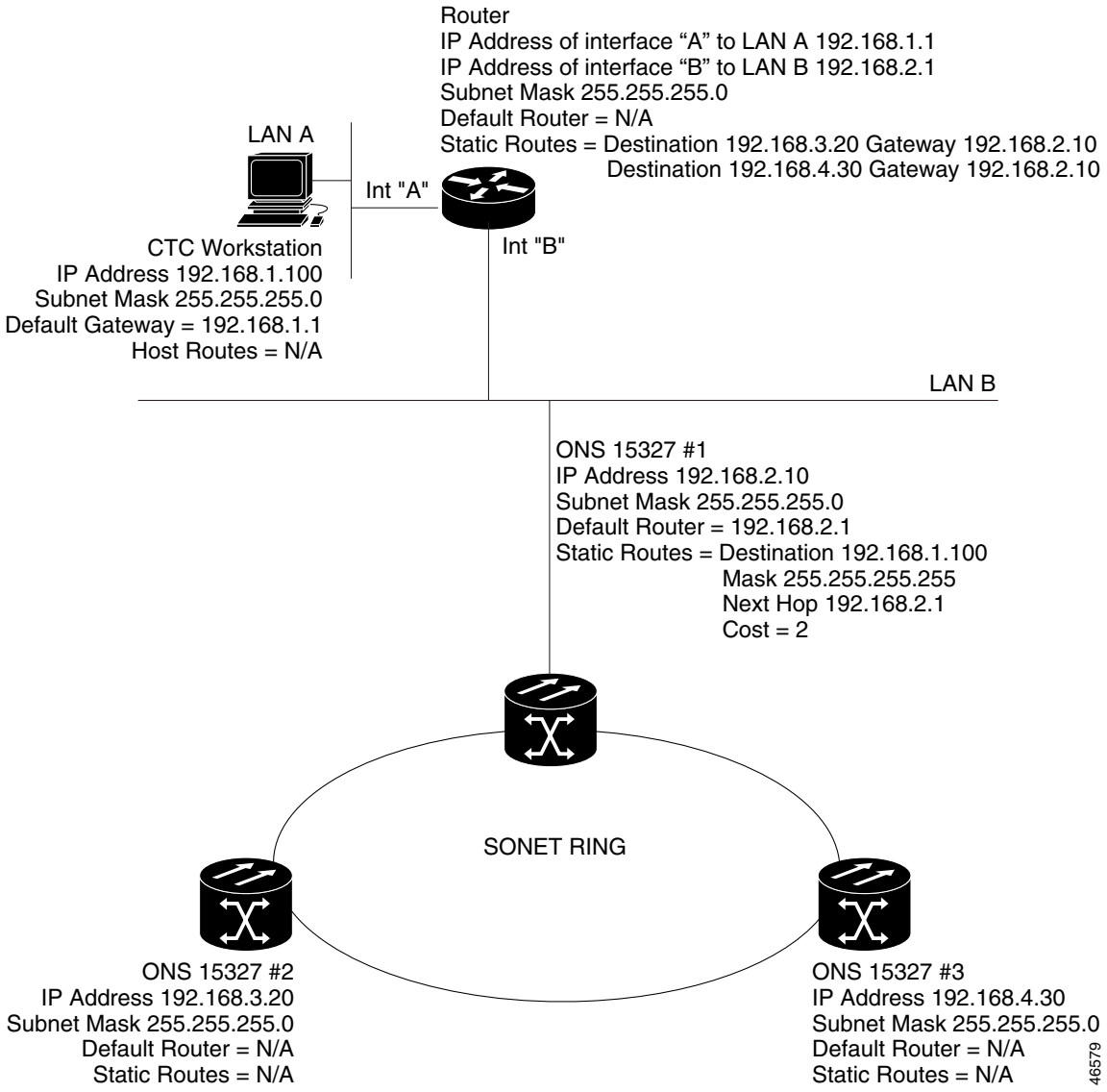


The destination and subnet mask entries control access to the ONS 15327s:

- If a single CTC computer is 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 toa router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 8-6 on page 8-8 shows an example.

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

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



8.2.6 Scenario 6: Using OSPF

Open Shortest Path First (OSPF) is a link state Internet routing protocol. Link state protocols use a "hello protocol" to monitor their links with adjacent routers and to test the status of their links to their neighbors. Link state protocols advertise their directly-connected networks and their active links. Each link state router captures the link state "advertisements" and puts them together to create a topology of the entire network or area. From this database, the router calculates a routing table by constructing a shortest path tree. Routes are recalculated when topology changes occur.

The ONS 15327 uses OSPF protocol in internal ONS 15327 networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15327 so that the ONS 15327 topology is sent to OSPF routers on a LAN. Advertising the ONS 15327 network topology to LAN routers eliminates the need to enter static routes for ONS 15327 subnetworks manually.

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 an ONS 15327 OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID in decimal format to the ONS 15327 network. Coordinate the area ID number assignment with your LAN administrator. All DCC-connected ONS 15327s should be assigned the same OSPF area ID.

Figure 8-7 shows a network enabled for OSPF.

Figure 8-7 Scenario 6: OSPF Enabled

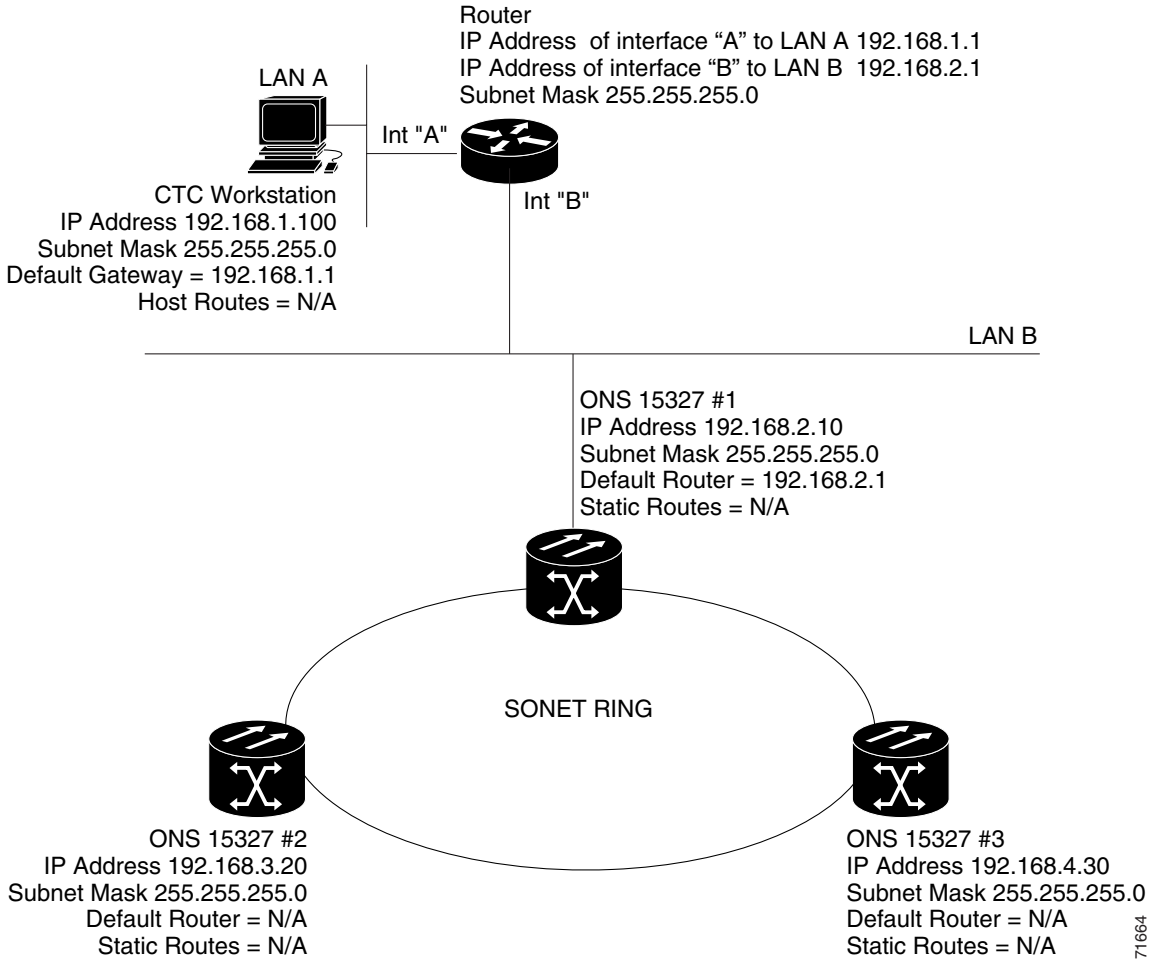
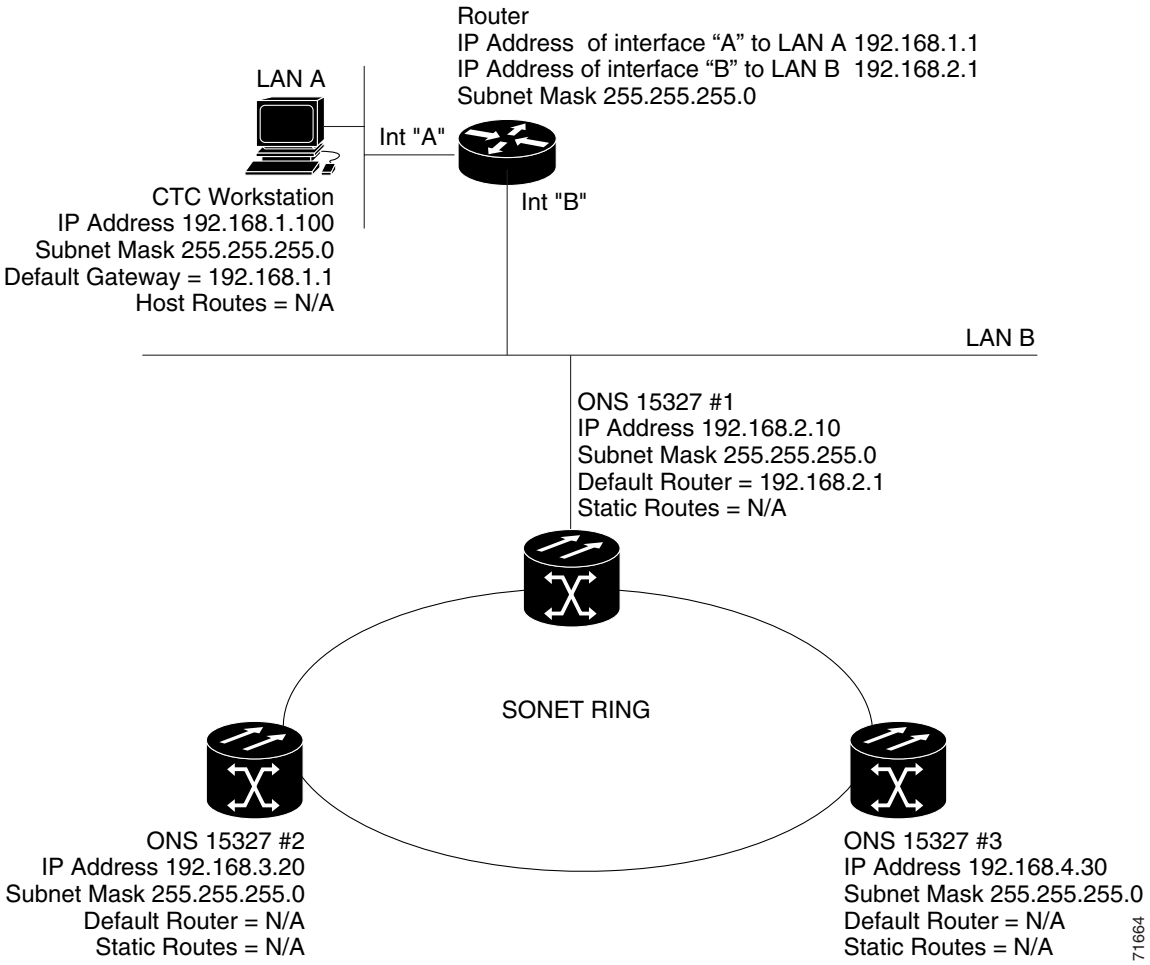


Figure 8-8 on page 8-10 shows the same network without OSPF. Static routes must be manually added to the router for CTC computers on LAN A to communicate with Nodes 2 and 3 because these nodes reside on different subnets.

Figure 8-8 Scenario 6: OSPF Not Enabled



8.2.7 Scenario 7: Provisioning the ONS 15327 Proxy Server

The ONS 15327 proxy server is a set of functions that allows you to network ONS 15327s in environments where visibility and accessibility between ONS 15327s 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 access the same ONS 15327s while preventing the field technicians from accessing the NOC LAN. To provision proxy server, one ONS 15327 is provisioned as a gateway NE (GNE) and the other ONS 15327s are provisioned as end NEs (ENEs). The GNE tunnels connections between CTC computers and ENEs, which provides management capability while preventing access for non-ONS 15327 management purposes.

The ONS 15327 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 8-14 and Table 8-4 on page 8-15) depend on whether the packet arrives at the ONS 15327 DCC or XTC 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 15327 creates an entry in its ARP table. The ARP entry allows the ONS 15327 to reply to an address over the local Ethernet so craft technicians can connect to ONS 15327s without changing the IP addresses of their computers.
- Processes SNTP/NTP requests. Element ONS 15327 NEs can derive time-of-day from an SNTP/NTP LAN server through the GNE.
- Process SNMPv1 traps. The GNE receives SNMPv1 traps from the ENE and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15327 proxy server is provisioned using three check boxes on the Provisioning > Network > General tabs:

- Enable Proxy—When enabled, the ONS 15327 serves as a proxy for connections between CTC clients and ONS 15327s that are DCC-connected to the proxy ONS 15327. The CTC client establishes connections to DCC-connected nodes through the proxy node. The CTC client can connect to nodes that it cannot directly contact from its host. If Enable Proxy is off, the node does not proxy for any CTC clients, although any established proxy connections will continue until the CTC client exits.

Note If you launch CTC against a node through a NAT/PAT router and that node does not have proxy server enabled, your CTC session will start and initially appear error free. However CTC will never receive alarm updates and will disconnect and reconnect every two minutes. If the proxy is accidentally disabled, it is still possible to 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 enabled, the ONS 15327 does not install or advertise default or static routes. CTC computers can communicate with the ONS 15327 using the XTC craft port, but they cannot communicate directly with any other DCC-connected ONS 15327.
- Enable Firewall—If selected, the node prevents IP traffic from being routed between the DCC and the LAN port. The ONS 15327 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 on page 8-12 shows an ONS 15327 proxy server implementation. A GNE is connected to a central office LAN and to ENEs. 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 ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

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

Figure 8-9 ONS 15327 Proxy Server with GNE and ENEs on the Same Subnet

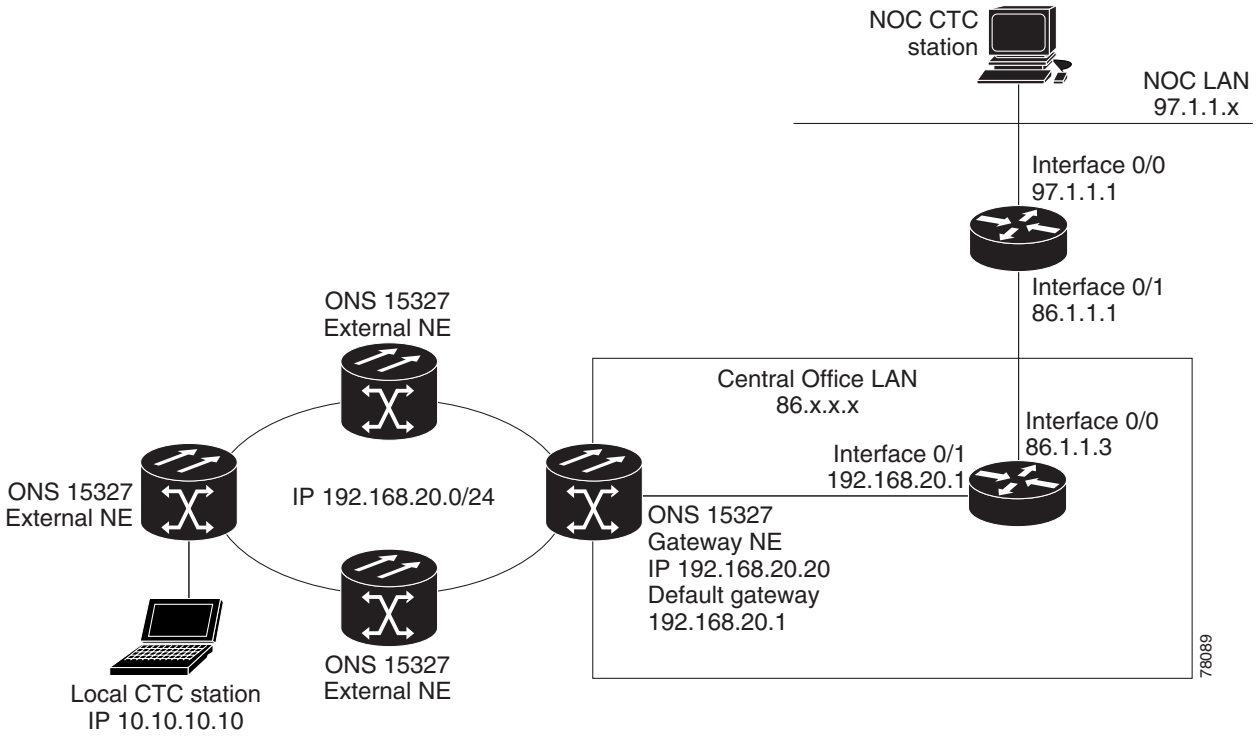


Table 8-2 shows recommended settings for ONS 15327 GNEs and ENEs in the configuration shown in Figure 8-9.

Table 8-2 ONS 15327 Gateway and Element NE Settings

Setting	ONS 15327 Gateway NE	ONS 15327 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 ONS 15327 GNE IP address
SNMP (if used)	SNMPv1 trap destinations	Set SNMPv1 trap destinations to ONS 15327 GNE

Figure 8-10 on page 8-13 shows the same proxy server implementation with ONS 15327 ENEs on different subnets. In this example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 8-2 on page 8-12.

Figure 8-10 Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on Different Subnets

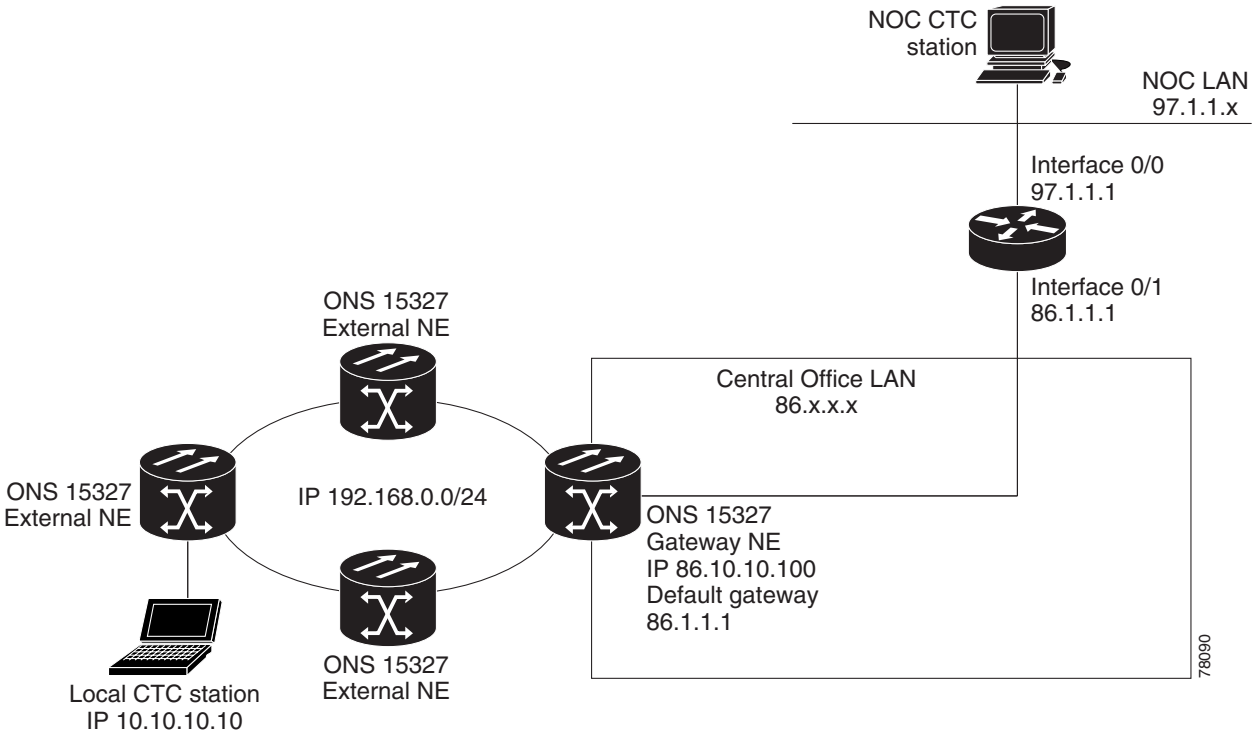


Figure 8-11 on page 8-14 shows the implementation with ONS 15327 ENEs in multiple rings. In this example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 8-2 on page 8-12.

Figure 8-11 Scenario 7: ONS 15327 Proxy Server with ENEs on Multiple Rings

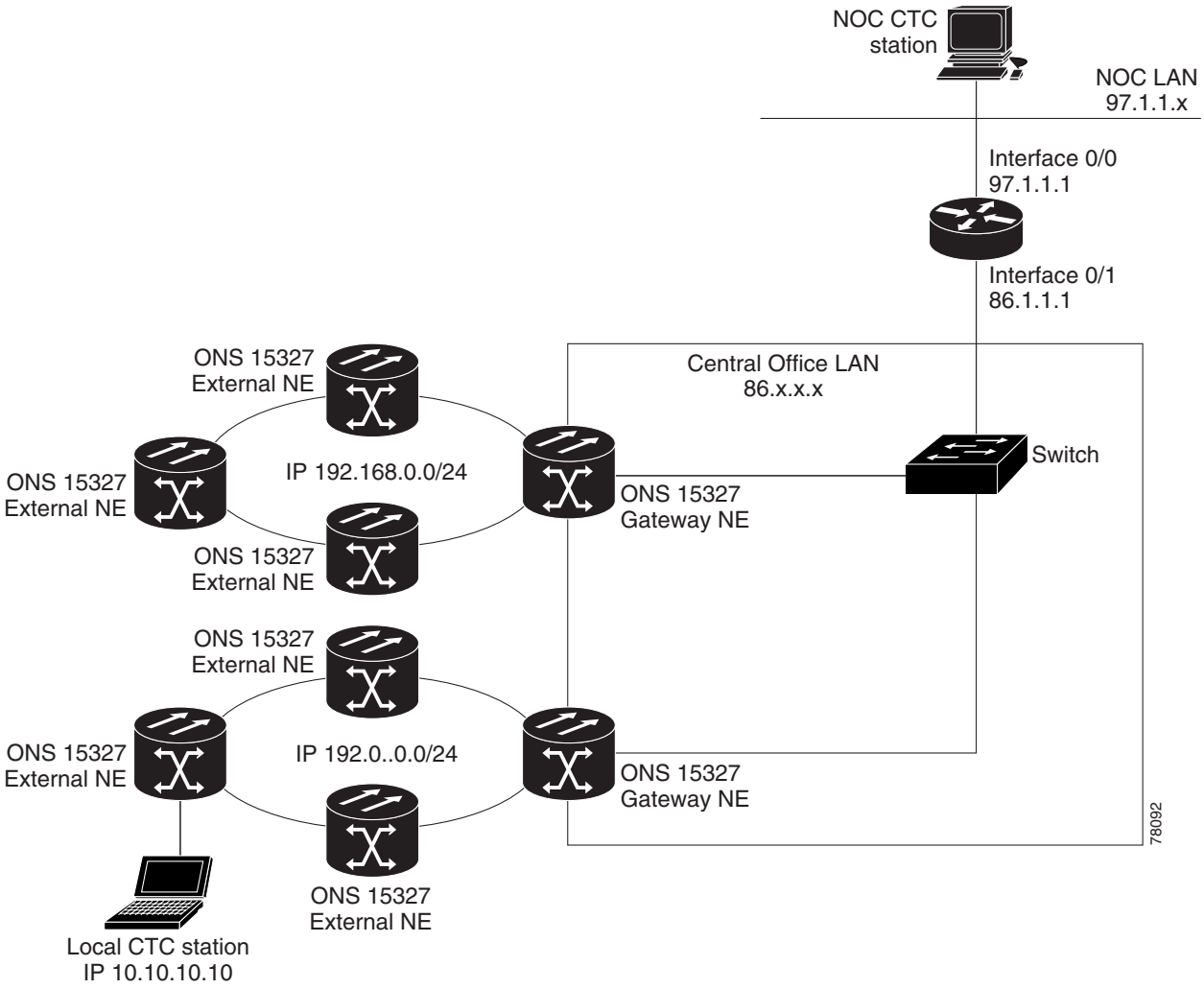


Table 8-3 shows the rules the ONS 15327 follows to filter packets when Enable Firewall is enabled.

Table 8-3 Proxy Server Firewall Filtering Rules

Packets arriving at:	Are accepted if the IP destination address is:
XTC ethernet interface	• The ONS 15327 shelf itself • The ONS 15327'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 15327 itself • Any destination that is connected through another DCC interface • Within the 224.0.0.0/8 network

Table 8-4 shows additional rules that apply if the packet addressed to the ONS 15327 is discarded. Rejected packets are silently discarded.

Table 8-4 Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15327

Packets Arrive At	Accepted	Rejected
XTC Ethernet Interface	• All User Datagram Protocol (UDP) packets except those in the Rejected column	• UDP packets addressed to the SNMP trap relay port (391) are rejected
DCC Interface	• All UDP packets • All TCP packets except those in the Rejected column • OSPF packets • Internet Control Message Protocol (ICMP) packets	• TCP packets addressed to the telnet port are rejected • TCP packets addressed to the proxy server port are rejected • All packets other than UDP, TCP, OSPF, ICMP

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

1. All DCC-connected ONS 15327s on the same Ethernet segment must have the same Craft Access Only setting. Mixed values will produce unpredictable results, and may leave some nodes unreachable through the shared Ethernet segment.
2. All DCC-connected ONS 15327s on the same Ethernet segment must have the same Enable Firewall setting. Mixed values will produce unpredictable results. Some nodes may become unreachable.
3. If you check Enable Firewall, always check Enable Proxy. If Enable Proxy is unchecked, CTC will not be able to see nodes on the DCC side of the ONS 15327.
4. If Craft Access Only is checked, check Enable Proxy. If Enable Proxy is not checked, CTC will not be able to see nodes on the DCC side of the ONS 15327.

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

- Disconnect the craft computer from the unreachable ONS 15327. Connect to the ONS 15327 through another ONS 15327 in the network that has a DCC connection to the unreachable ONS 15327.
- Disconnect the Ethernet cable from the unreachable ONS 15327. Connect a CTC computer directly to the ONS 15327.

8.3 Routing Table

ONS 15327 routing information is displayed on the Maintenance > Routing Table tabs. 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 the listed route has been used.

- Interface—Shows the ONS 15327 interface used to access the destination. Values are:
  - cpm0—The ONS 15327 Ethernet interface, that is, the RJ-45 jack and the LAN pin on the XTC card.
  - pdcc0—An SDCC interface, that is, an OC-N trunk card identified as the SDCC termination.
  - lo0—A loopback interface.

Table 8-5 shows sample routing entries for an ONS 15327.

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 15327 Ethernet interface is used to reach the gateway.

Entry #2 shows the following:

- Destination (172.20.214.0) is the destination network IP address.
- Mask (255.255.255.0) is a 24-bit mask, meaning all addresses within the 172.20.214.0 subnet can be a destination.
- Gateway (172.20.214.92) is the gateway address. All outbound traffic belonging to this network is sent to this gateway.
- Interface (cpm0) indicates that the ONS 15327 Ethernet interface is used to reach the gateway.

Entry #3 shows the following:

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

Entry #4 shows the following:

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

Entry #5 shows a DCC-connected node that is accessible through a node that is not directly connected:

- Destination (172.20.214.94) is the destination host IP address.
- Mask (255.255.255.255) is a 32-bit mask, meaning only the 172.20.214.94 address is a destination.
- Gateway (172.20.214.93) indicates that the destination host is accessed through a node with IP address 172.20.214.93.
- Interface (pdcc0) indicates that a SONET SDCC interface is used to reach the gateway.

8.4 External Firewalls

Table 8-6 shows the ports that are used by the XTC.

Table 8-6 Ports Used by the XTC

Port	Function
0	Never used
21	FTP control
23	TELNET
80	HTTP
111	rpc (not used; but port is in use)
513	rlogin (not used; but port is in use)
=<1023	Default CTC listener ports
1080	Proxy server
2001-2017	I/O card telnet
2018	DCC processor on active XTC
2361	TL1
3082	TL1
3083	TL1
5001	BLSR server port
5002	BLSR client port
7200, 7209, 7210	SNMP input port
9100	EQM port
9101	EQM port 2
9401	TCC boot port
9999	Flash manager
10240-12288	Proxy client
57790	Default TCC listener port

8.4.1 Access Control List Example With Proxy Server Not Enabled

The following access control list (ACL) examples show a firewall configuration when the Proxy Server feature is not enabled. In the example, the CTC workstation address is 192.168.10.10 and the ONS 15327 address is 10.10.10.100. The firewall is attached to the GNE, so the inbound path is CTC to the GNE and the outbound path is from the GNE to CTC. The CTC CORBA Standard constant is 683 and the TCC CORBA Default TCC Fixed (57790).

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15327 using http (port 80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 57790
access-list 100 remark *** allows CTC communication with the 15327 GNE (port 57790) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 established
access-list 100 remark *** allows ACKs back from CTC to the 15327 GNE ***
access-list 101 remark *** Outbound ACL, NE -> CTC ***
access-list 101 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 eq 683
access-list 101 remark *** allows alarms etc., from the 15327 (random port) to the CTC workstation
(port 683) ***
access-list 100 remark
access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established
access-list 101 remark *** allows ACKs from the 15327 GNE to CTC ***
```

8.4.2 Access Control List Example With Proxy Server Enabled

The following ACL examples show a firewall configuration when the Proxy Server feature is enabled. As with the first example, the CTC workstation address is 192.168.10.10 and the ONS 15327 address is 10.10.10.100. The firewall is attached to the GNE, so the inbound path is CTC to the GNE and the outbound path is from the GNE to CTC. CTC CORBA Standard constant (683) and TCC CORBA Default TCC Fixed (57790).

```
access-list 100 remark *** Inbound ACL, CTC -> NE ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq www
access-list 100 remark *** allows initial contact with the 15327 using http (port 80) ***
access-list 100 remark
access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 eq 1080
access-list 100 remark *** allows CTC communication with the 15327 GNE proxy server (port
1080) ***
```

access-list 100 remark

access-list 100 permit tcp host 192.168.10.10 host 10.10.10.100 established

access-list 100 remark *** allows ACKs from CTC to the 15327 GNE ***

access-list 101 remark *** Outbound ACL, NE -> CTC ***

access-list 101 remark

access-list 101 permit tcp host 10.10.10.100 eq 1080 host 192.168.10.10

access-list 101 remark *** allows alarms and other communications from the 15327 (proxy server) to the CTC workstation

(port 683) ***

access-list 100 remark

access-list 101 permit tcp host 10.10.10.100 host 192.168.10.10 established

access-list 101 remark *** allows ACKs from the 15327 GNE to CTC ***

Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, threshold, and report performance data for early detection of problems. In this chapter, PM parameters and concepts are defined for both electrical cards and optical cards in the Cisco ONS 15327.

For information about enabling and viewing PM parameters, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

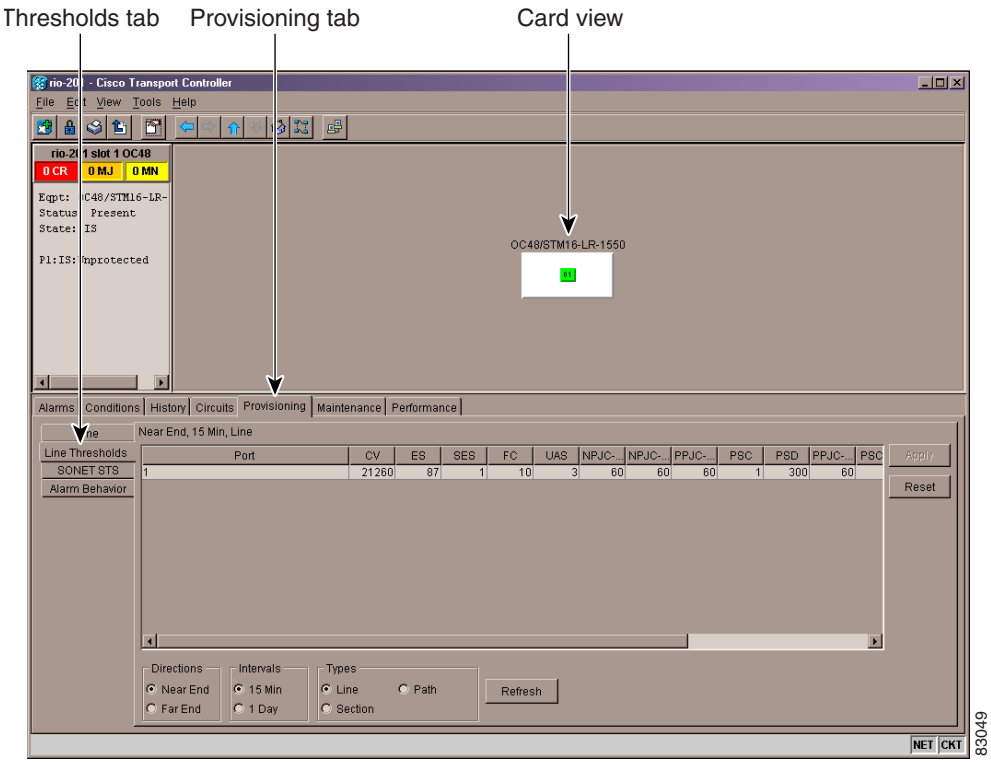
Note Additional PM parameter information can also be found under digital transmission surveillance in Telcordia's GR-1230-CORE, GR-820-CORE, and GR-253-CORE documents and in the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

9.1 Threshold Reference

Thresholds are used to set error levels for each PM parameter. You can program PM parameter threshold ranges from the Provisioning > Line Thresholds tabs on the card view. For procedures on provisioning card thresholds, such as line, path, and SONET thresholds, refer to the *Cisco ONS 15327 Procedure Guide*.

During the accumulation cycle, if the current value of a PM 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 PM parameter is disabled. Figure 9-1 on page 9-2 shows the Provisioning > Line Thresholds tabs for an OC-48 card.

Figure 9-1 Line 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 DS1 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

9.2 Intermediate-Path Performance Monitoring Reference

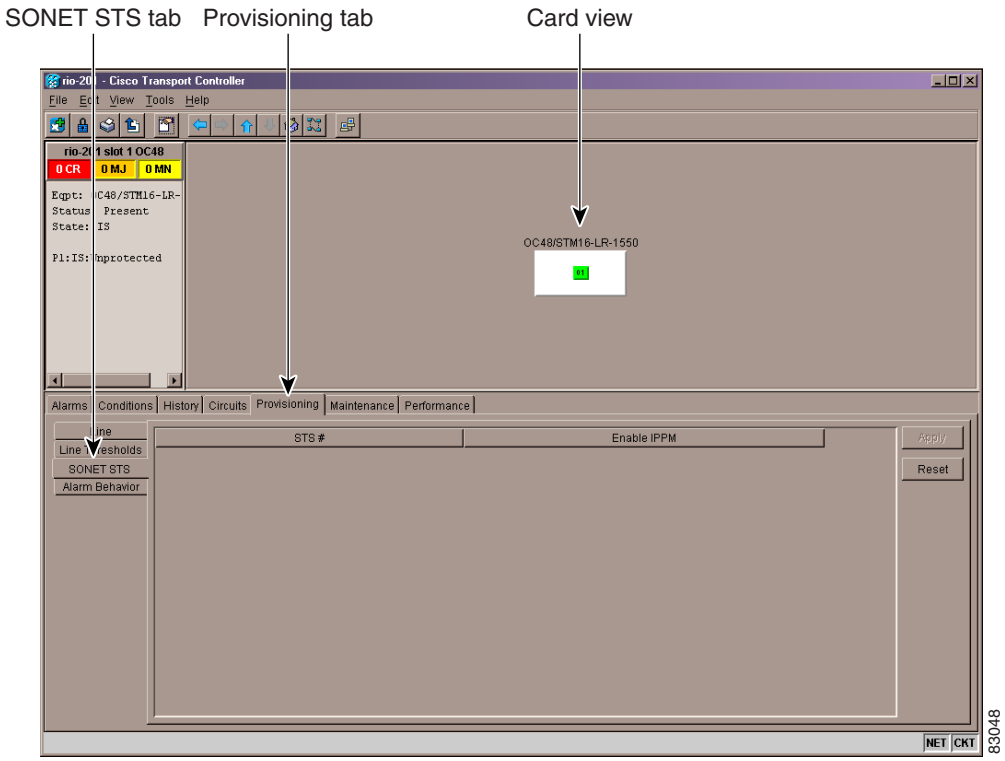
Intermediate-path performance monitoring (IPPM) allows transparent monitoring of a constituent channel of an incoming transmission signal by a node that does not terminate that channel. Many large ONS 15327 networks only use line terminating equipment (LTE) not path terminating equipment (PTE). Table 9-1 shows ONS 15327 cards that are considered LTEs.

Table 9-1 Traffic Cards that Terminate the Line, Called LTEs

Line Terminating Equipment	
XTC-14	XTC-28-3
OC3 IR 1310	OC12 IR 1310
OC12 LR 1550	OC48 IR 1310
OC48 LR 1550	

Figure 9-2 on page 9-3 shows the Provisioning > SONET STS tabs for enabling IPPM on an OC-48 card.

Figure 9-2 SONET STS Tab for Enabling IPPM



Software Release 3.0 and later allows LTE cards to monitor near-end PM parameter data on individual STS payloads by enabling IPPM. After enabling IPPM provisioning on the line card, service providers can monitor large amounts of STS traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on STS paths which have IPPM enabled, and TCAs are raised only for PM parameters on the selected IPPM paths. The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P.

Note Far-end IPPM is not supported. However, SONET path PM parameters can be monitored by logging into the far-end node directly.

The ONS 15327 performs IPPM by examining the overhead in the monitored path and by reading all of the near-end path PM parameters in the incoming direction of transmission. The IPPM process allows the path signal to pass bidirectionally through the node completely unaltered.

For detailed information about specific PM parameters, locate the card name in the following sections and review the appropriate definition.

9.3 Pointer Justification Count Reference

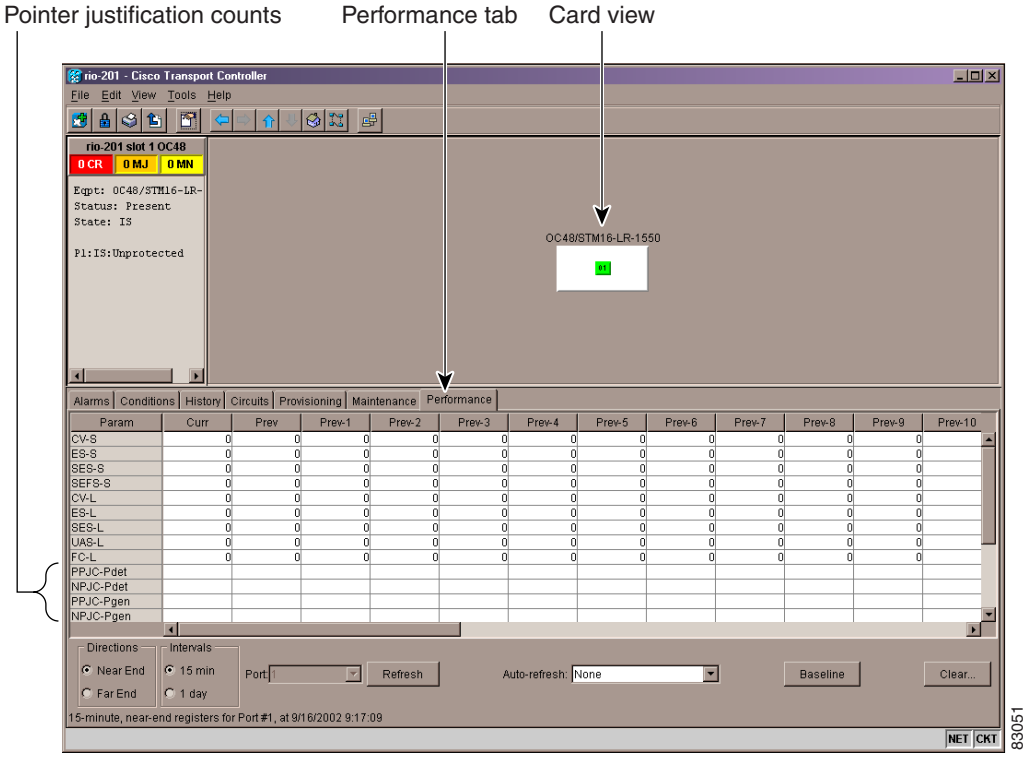
Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks. When a network is out of synch, jitter and wander occurs on the transported signal. Excessive wander can cause terminating equipment to slip. It also causes slips at the SDH and plesiochronous digital hierarchy (PDH) boundaries.

Slips cause different effects in service. Voice service has intermittent audible clicks. Compressed voice technology has short transmission errors or dropped calls. Fax machines lose scanned lines or experience dropped calls. Digital video transmission has distorted pictures or frozen frames. Encryption service loses the encryption key causing data to be transmitted again.

Pointers provide a way to align the phase variations in STS and virtual tributary (VT) payloads. The STS payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the STS synchronous payload envelope (SPE) called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

Figure 9-3 shows pointer justification count parameters in the Performance Monitoring window. You can enable positive pointer justification count (PPJC) and negative pointer justification count (NPJC) performance monitoring parameters for LTE cards. See Table 9-1 on page 9-2 for a list of Cisco ONS 15327 LTE cards.

Figure 9-3 Viewing Pointer Justification Count Parameters



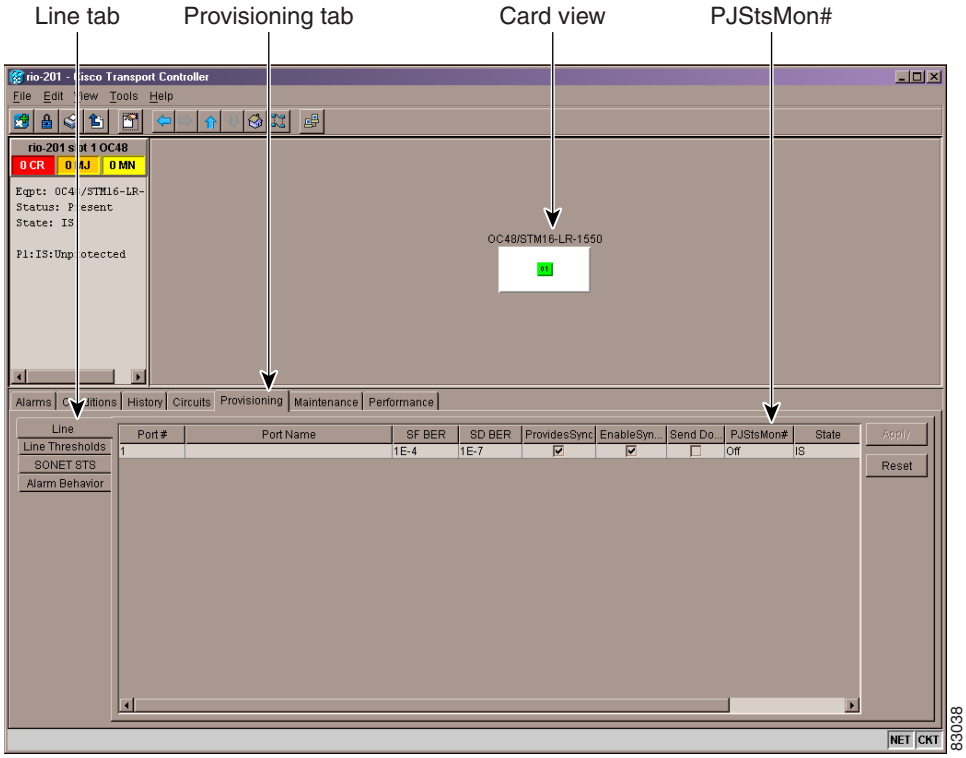
There are PPJC and NPJC parameters. PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications depending on the specific PM parameter.

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 SPE is too slow in relation to the rate of the STS 1.

For pointer justification count definitions, depending on the cards in use, see the "9.6.1 OC-3 Card Performance Monitoring Parameters" section on page 9-18, the "9.6.2 OC-12 Card Performance Monitoring Parameters" section on page 9-24, or the "9.6.3 OC-48 Card Performance Monitoring Parameters" section on page 9-29.

In CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tabs. Figure 9-4 shows the PJStsMon# menu on the Provisioning window.

Figure 9-4 Line Tab for Enabling Pointer Justification Count Parameters



9.4 Performance Monitoring for Electrical Cards

The following sections define performance monitoring parameters for the XTC-14 and XTC-28-3 electrical cards.

9.4.1 XTC DS1 Performance Monitoring Parameters

Figure 9-5 on page 9-6 shows the signal types that support near-end and far-end PM parameters.

Figure 9-5 Monitored Signal Types for the XTC Card DS-1 Ports

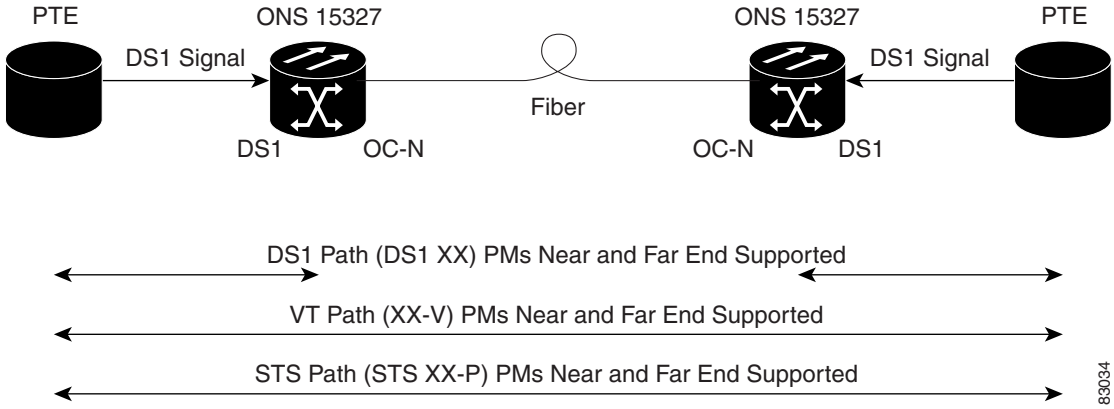
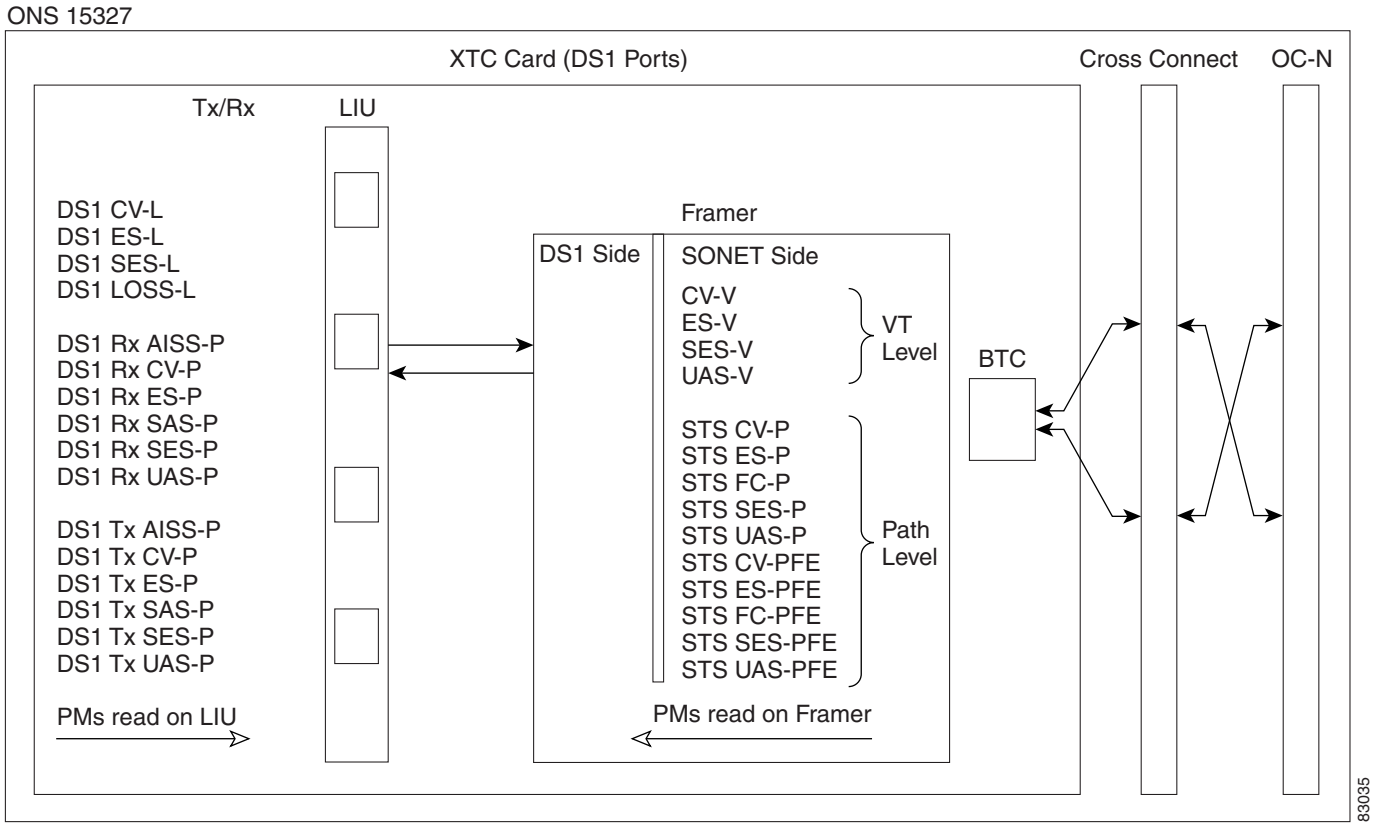


Figure 9-6 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the XTC card DS-1 ports.

Note The XX in Figure 9-5 represents all PM parameters listed in Figure 9-6 with the given prefix and/or suffix.

Figure 9-6 PM Parameter Read Points on the XTC Card DS-1 Ports



The PM parameters for the XTC card DS-1 ports are described in Table 9-2 through Table 9-8 on page 9-11.

Table 9-2 DS-1 Line PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
DS1 CV-L	Line Code Violation (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
DS1 ES-L	Line Errored Seconds (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (loss of signal) on the line.
DS1 SES-L	Line Severely Errored Seconds (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ ≥ 1544) and/or defects on the line.
DS1 LOSS-L	Line Loss of Signal Seconds (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Note Under the Provisioning > Threshold tab, the XTC cards have user-defined thresholds for the DS-1 receive (Rx) path PM parameters. In the Threshold tab they are displayed as Code Violation (CV), Errored Seconds (ES), Severely Errored Seconds (SES), Unavailable Seconds (UAS), Alarm Indication Signal (AIS), and Seconds Frame/Alarm Indication Signal (SAS) without the Rx prefix.

Table 9-3 DS-1 Receive Path PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
DS1 Rx AISS-P	Receive Path Alarm Indication Signal (Rx AISS-P) means that an alarm indication signal occurred on the receive end of the path. This parameter is a count of seconds containing one or more Alarm Indication Signal (AIS) defects.
DS1 Rx CV-P	Receive Path Code Violation (Rx CV-P) means that a coding violation occurred on the receive end of the path. For DS-1 ESF paths, this parameter is a count of detected CRC-6 errors. For the DS-1 SF paths, the Rx CV-P parameter is a count of detected frame-bit errors (FE).
DS1 Rx ES-P	Receive Path Errored Seconds (Rx ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths on the receive end of the signal. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more Severely Errored Frame (SEF) or AIS defects. For DS1-SF paths, the Rx ES-P parameter is a count of one-second intervals containing one or more FE events, or one or more CS events, or one or more SEF or AIS defects.
DS1 Rx SAS-P	Receive Path Severely Errored Seconds Frame/Alarm Indication Signal (Rx SAS-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the receive end of the signal.

Table 9-3 DS-1 Receive Path PM Parameters for the XTC Card DS-1 Ports (continued)

Parameter	Definition
DS1 Rx SES-P	Receive Path Severely Errored Seconds (Rx SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths on the receive end of the signal. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more SEF or AIS defects occurred. For DS1-SF paths, a SES is a second containing either the occurrence of four FEs or one or more SEF or AIS defects.
DS1 Rx UAS-P	Receive Path Unavailable Seconds (Rx UAS-P) is a count of one-second intervals when the DS-1 path is unavailable on the receive end of the signal. The DS-1 path is unavailable at the onset of 10 consecutive seconds that qualify as SESs, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES-Ps. The ten seconds with no SES-Ps are excluded from unavailable time.

Note Under the Performance tab, the displayed DS1 Tx path PM parameter values are based on calculations performed by the card and therefore have no user-defined thresholds. The tab is labeled Elect[rical] Path Threshold.

Table 9-4 DS-1 Transmit Path PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
DS1 Tx AIS-P	Transmit Path Alarm Indication Signal (Tx AIS-P) means that an alarm indication signal occurred on the transmit end of the path. This parameter is a count of seconds containing one or more AIS defects.
DS1 Tx CV-P	Transmit Path Code Violation (Tx CV-P) means that a coding violation occurred on the transmit end of the path. For DS-1 ESF paths, this parameter is a count of detected CRC-6 errors. For the DS-1 SF paths, the Tx CV-P parameter is a count of detected FEs.
DS1 Tx ES-P	Transmit Path Errored Seconds (Tx ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths on the transmit end of the signal. For DS-1 ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more SEF or AIS defects. For DS-1 SF paths, the Tx ES-P parameter is a count of one-second intervals containing one or more FE events, or one or more CS events, or one or more SEF or AIS defects.
DS1 Tx SAS-P	Transmit Path Severely Errored Seconds Frame/Alarm Indication Signal (Tx SAS-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the transmit end of the signal.

Table 9-4 DS-1 Transmit Path PM Parameters for the XTC Card DS-1 Ports (continued)

Parameter	Definition
DS1 Tx SES-P	Transmit Path Severely Errored Seconds (Tx SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths on the transmit end of the signal. For the DS-1 ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more SEF or AIS defects occurred. For DS-1 SF paths, a SES is a second containing either the occurrence of four FEs or one or more SEF or AIS defects.
DS1 Tx UAS-P	Transmit Path Unavailable Seconds (Tx UAS-P) is a count of one-second intervals when the DS-1 path is unavailable on the transmit end of the signal. The DS-1 path is unavailable at the onset of 10 consecutive seconds that qualify as SESs, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SESs. The ten seconds with no SESs are excluded from unavailable time.

Table 9-5 VT Path PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
CV-V	Code Violation VT Layer (CV-V) is a count of the bit interleaved parity (BIP) errors detected at the VT path layer. Up to two BIP errors can be detected per VT superframe, with each error incrementing the current CV-V second register.
ES-V	Errored Seconds VT Layer (ES-V) is a count of the seconds when at least one VT Path BIP error was detected. An Alarm Indication Signal VT Layer (AIS-V) defect (a lower-layer, traffic-related, near-end defect) or a Loss of Pointer VT Layer (LOP-V) defect can also cause an ES-V.
SES-V	Severely Errored Seconds VT Layer (SES-V) is a count of seconds when K (600) or more VT Path BIP errors were detected. SES-V can also be caused by an Alarm Indication Signal VT Layer (AIS-V) defect (a lower-layer, traffic-related, near-end defect) or a Loss of Pointer VT layer (LOP-V) defect.
UAS-V	Unavailable Second VT Layer (UAS-V) is a count of the seconds when the VT path is considered unavailable. A VT path becomes unavailable at the onset of ten consecutive seconds that qualify as SES-Vs, and continues to be unavailable until the onset of ten consecutive seconds occur that do not qualify as SES-Vs.

Table 9-6 Far-End VT Path PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
CV-VFE	Far-End VT Path Coding Violations (CV-VFE) is a count of the number of BIP errors detected by the far-end VT path terminating equipment (PTE) and reported back to the near-end VT PTE using the VT layer remote error indication (REI-V) in the VT path overhead. Only one BIP error can be indicated per VT superframe using the REI-V bit. The current CV-VFE second register is incremented for each BIP error indicated by the incoming REI-V.
ES-VFE	Far-End VT Path Errored Seconds (ES-VFE) is a count of the seconds when at least one VT path BIP error was reported by the far-end VT PTE, or a one-bit VT layer remote defect indication (RDI-V) defect is present.
SES-VFE	Far-End VT Path Severely Errored Seconds (SES-VFE) is a count of the seconds when K (600) or more VT path BIP errors were reported by the far-end VT PTE or a one-bit RDI-V defect was present.
UAS-VFE	Far-End VT Path Unavailable Seconds (UAS-VFE) is a count of the seconds when the VT path is unavailable at the far-end. A VT path is considered unavailable at the onset of ten consecutive seconds that qualify as SES-VFEs, and continues to be considered unavailable until the onset of 10 consecutive seconds that do not qualify as SES-VFEs.

Table 9-7 Near-End SONET Path PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (STS CV-P) is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame, with each error incrementing the current CV-P second register.
STS ES-P	Near-End STS Path Errored Seconds (STS ES-P) is a count of the seconds when at least one STS path BIP error was detected. An path-layer alarm indicator signal (AIS-P) defect (a lower-layer, traffic-related, near-end defect) or a path-layer loss of pointer (LOP-P) defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (STS FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a path-layer unequipped (UNEQ-P), or a path-layer trace identifier mismatch (TIM-P) failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.

Table 9-7 Near-End SONET Path PM Parameters for the XTC Card DS-1 Ports (continued)

Parameter	Definition
STS SES-P	Near-End STS Path Severely Errored Seconds (STS SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the one-second intervals when the STS path is unavailable. An STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ps. The ten seconds with no SES-Ps are excluded from unavailable time.

Table 9-8 Far-End SONET Path PM Parameters for the XTC Card DS-1 Ports

Parameter	Definition
STS CV-PFE	Far-End STS Path Coding Violations (STS CV-PFE) is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame, with each error incrementing the current CV-P second register.
STS ES-PFE	Far-End STS Path Errored Seconds (STS ES-PFE) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.
STS FC-PFE	Far-End STS Path Failure Counts (STS FC-PFE) is a count of the number of far-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-PFE	Far-End STS Path Severely Errored Seconds (STS SES-PFE) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS SES-PFE.
STS UAS-PFE	Far-End STS Path Unavailable Seconds (UAS-PFE) is a count of the one-second intervals when the STS path is unavailable. An STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-PFEs. The ten seconds with no SES-PFEs are excluded from unavailable time.

9.4.2 XTC DS3 Card Performance Monitoring Parameters

Figure 9-7 on page 9-12 shows the signal types that support near-end and far-end PM parameters.

Figure 9-7 Monitored Signal Types for the XTC Card DS-3 Ports

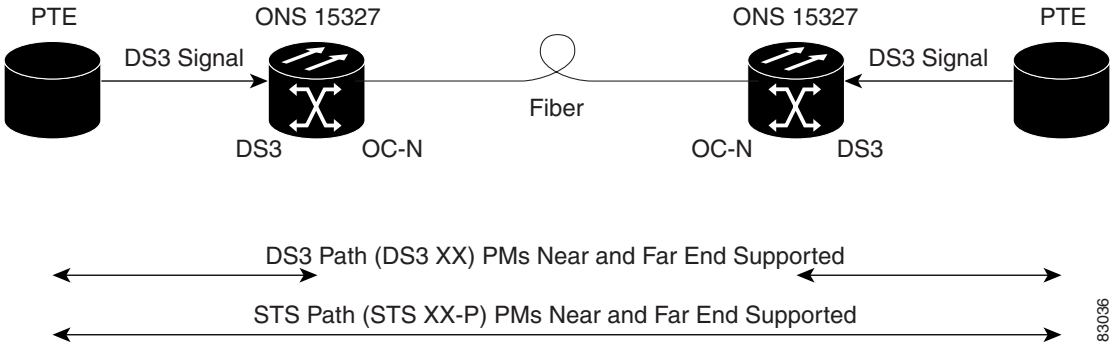
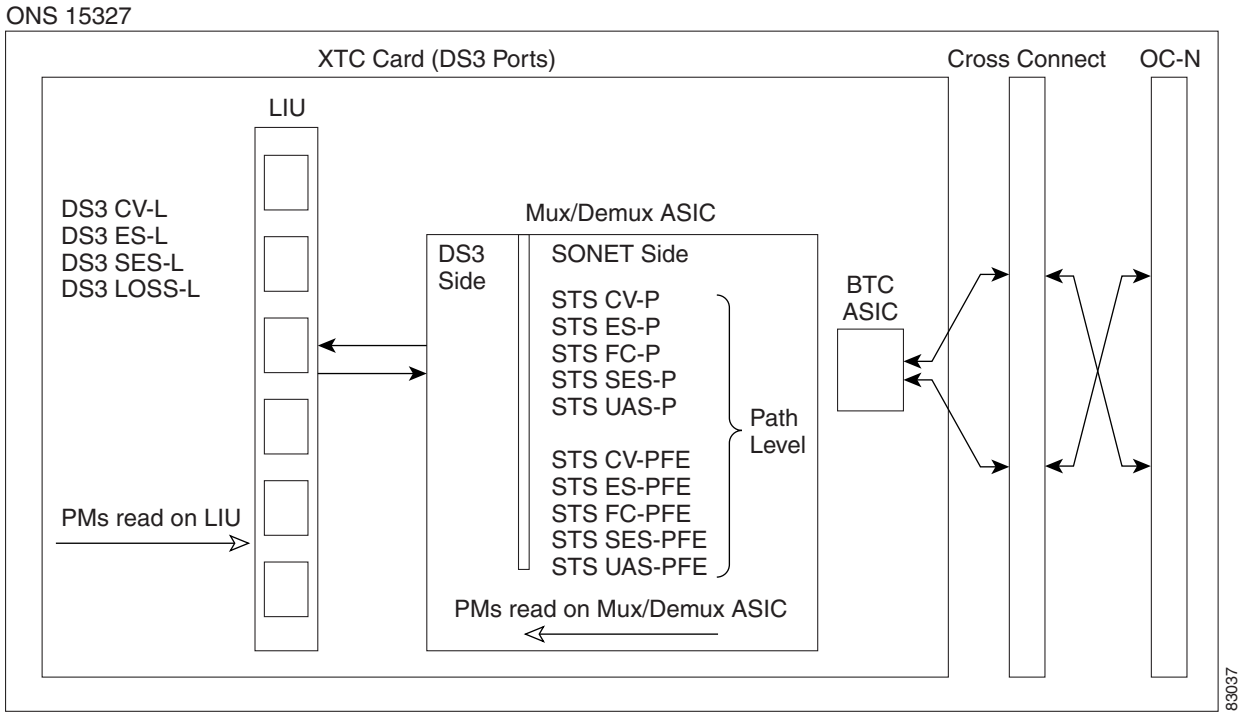


Figure 9-8 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the XTC card DS-3 ports.

Note The XX in Figure 9-7 represents all PM parameters listed in Figure 9-8 with the given prefix and/or suffix.

Figure 9-8 PM Parameter Read Points on the XTC Card DS-3 Ports



The PM parameters for the XTC card DS-3 ports are described in Table 9-9 through Table 9-11 on page 9-13.

Table 9-9 Near-End DS3 Line PM Parameters for the XTC Card DS-3 Ports

Parameter	Definition
DS3 CV-L	CV-L indicates the number of coding violations occurring on the line. This parameter is a count of BPVs and EXZs occurring over the accumulation period.
DS3 ES-L	ESL is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (loss of signal) on the line.
DS3 SES-L	SES-L is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
DS3 LOSS-L	LOSS-L is a count of one-second intervals containing one or more LOS defects.

Table 9-10 Near-End SONET Path PM Parameters for the XTC Card DS-3 Ports

Parameter	Definition
STS CV-P	STS CV-P is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	STS ES-P is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	STS FC-P is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	STS SES-P is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	STS UAS-P is a count of the one-second intervals when the STS path is unavailable. An STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ps. The ten seconds with no SES-Ps are excluded from unavailable time.

Table 9-11 Far-End SONET Path PM Parameters for the XTC Card DS-3 Ports

Parameter	Definition
STS CV-PFE	STS CV-PFE is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-PFE	STS ES-PFE is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.

Table 9-11 Far-End SONET Path PM Parameters for the XTC Card DS-3 Ports (continued)

Parameter	Definition
STS FC-PFE	STS FC-PFE is a count of the number of far-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-PFE	STS SES-PFE is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS SES-PFE.
STS UAS-PFE	STS UAS-PFE is a count of the one-second intervals when the STS path is unavailable. An STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-PFEs. The ten seconds with no SES-PFEs are excluded from unavailable time.

9.5 Performance Monitoring for Ethernet Cards

The following sections define performance monitoring parameters and definitions for the E-Series and G-Series Ethernet cards.

9.5.1 E-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The E-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

9.5.1.1 E-Series Ethernet Statistics Window

The Ethernet Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh will occur.

Table 9-12 defines the E-Series Ethernet card statistics parameters.

Table 9-12 E-Series Ethernet Statistics Parameters

Parameter	Meaning
Link Status	Indicates whether or not link integrity is present; up means present and down means not present
Rx Packets	Number of packets received since the last counter reset
Rx Bytes	Number of bytes received since the last counter reset
Tx Packets	Number of packets transmitted since the last counter reset
Tx Bytes	Number of bytes transmitted since the last counter reset

Table 9-12 E-Series Ethernet Statistics Parameters (continued)

Parameter	Meaning
Rx Total Errors	Total number of receive errors
Rx FCS	Number of packets with a frame check sequence (FCS) error; FCS errors indicate frame corruption during transmission
Rx Alignment	Number of packets with alignment errors; alignment errors are received incomplete frames
Rx Runts	Number of packets received that are less than 64 bytes in length
Rx Giants	Number of packets received that are greater than 1518 bytes in length for untagged interfaces and greater than 1522 bytes for tagged interfaces
Tx Collisions	Number of transmit packets that are collisions. The port and the attached device transmitting at the same time caused collisions
Tx Late Collisions	Number of frames that were not transmitted because they encountered a collision outside of the normal collision window. Normally, late collision events should occur only rarely, if at all
Tx Excessive Collisions	Number of consecutive collisions
Tx Deferred	Number of packets deferred

9.5.1.2 E-Series Ethernet Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as 100 Full, which is the mode setting configured on the E-Series port. However, if the E-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the E-Series and the peer Ethernet device attached directly to the E-Series port.

The Utilization window provides an Interval menu, that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100 % interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100 % interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits/second in one direction for the Ethernet port (that is, 1 Gbps). Table 9-13 shows the maxBaseRates for E-Series Ethernet cards.

Table 9-13 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note The E-Series Ethernet card is a Layer 2 device or switch and supports Trunk Utilization statistics. The trunk utilization statistics are similar to the line utilization statistics, but show the percentage of circuit bandwidth used rather than the percentage of line bandwidth used. The trunk utilization statistics are accessed via the card view Maintenance tab.

9.5.1.3 E-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window will display the statistics for each port for the number of previous time intervals as shown in Table 9-14. The listed parameters are defined in Table 9-12.

Table 9-14 Ethernet History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24-hours)	7 previous time intervals

9.5.2 G-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The G-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

9.5.2.1 G-Series Ethernet Statistics Window

The Ethernet Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh will occur. The G-Series Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the G-Series card.

Table 9-15 defines the G-Series Ethernet card Statistics parameters.

Table 9-15 G-Series Ethernet Statistics Parameters

Parameter	Meaning
Time Last Cleared	A time stamp indicating the last time statistics were reset
Link Status	Indicates whether or not the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present and down means not present
Rx Packets	Number of packets received since the last counter reset
Rx Bytes	Number of bytes received since the last counter reset
Tx Packets	Number of packets transmitted since the last counter reset

Table 9-15 G-Series Ethernet Statistics Parameters (continued)

Parameter	Meaning
Tx Bytes	Number of bytes transmitted since the last counter reset
Rx Total Errors	Total number of receive errors
Rx FCS	Number of packets with a FCS error; FCS errors indicate frame corruption during transmission
Rx Alignment	Number of packets with received incomplete frames
Rx Runts	Total number of frames received that are less than 64 bytes in length and have a CRC error
Rx Jabbers	Total number of frames received that exceed the1548-byte maximum and contain CRC errors
Rx Pause Frames	Number of received Ethernet IEEE 802.3z pause frames
Tx Pause Frames	Number of transmitted IEEE 802.3z pause frames
Rx Pkts Dropped Internal Congestion	Number of received packets dropped due to overflow in G-Series frame buffer
Tx Pkts Dropped Internal Congestion	Number of transmit queue drops due to drops in the G-Series frame buffer
HDLC errors	HDLC errors received from SONET/SDH)[1]

1. Do not use the HDLC errors counter to count the number of frames dropped because of HDLC errors, because each frame can fragment into several smaller frames during HDLC error conditions and spurious HDLC frames can also be generated. If HDLC error counters are incrementing when no SONET path problems should be present, it might indicate a problem with the quality of the SONET path. For example, a SONET protection switch generates a set of HLDC errors. But the actual values of these counters are less significant than the fact they are changing.

9.5.2.2 G-Series Ethernet Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as 100 Full, which is the mode setting configured on the G-Series port. However, if the G-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the G-Series and the peer Ethernet device attached directly to the G-Series port.

The Utilization window provides an Interval menu, that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100 % interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100 % interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits/second in one direction for the Ethernet port (that is, 1 Gbps). Table 9-16 shows the maxBaseRates for G-Series Ethernet cards.

Table 9-16 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note Unlike the E-Series, the G Series card does not have a display of trunk utilization statistics, because the G-Series card is not a Layer 2 device or switch.

9.5.2.3 G-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window will display the statistics for each port for the number of previous time intervals as shown in Table 9-17. The listed parameters are defined in Table 9-15 on page 9-16.

Table 9-17 Ethernet History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

9.6 Performance Monitoring for Optical Cards

The following sections define performance monitoring parameters and definitions for the OC-3, OC-12, and OC-48 cards.

9.6.1 OC-3 Card Performance Monitoring Parameters

Figure 9-9 shows the signal types that support near-end and far-end PM parameters. Figure 9-10 on page 9-19 shows where overhead bytes detected on the ASICs produce PM parameters for the OC-3 card.

Figure 9-9 Monitored Signal Types for the OC-3 Card

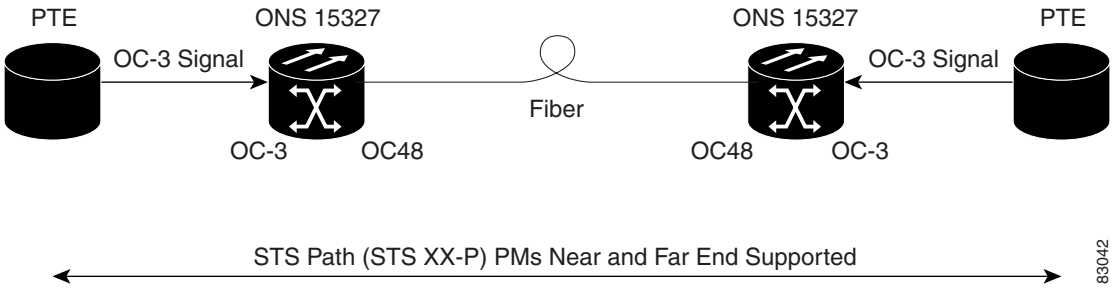
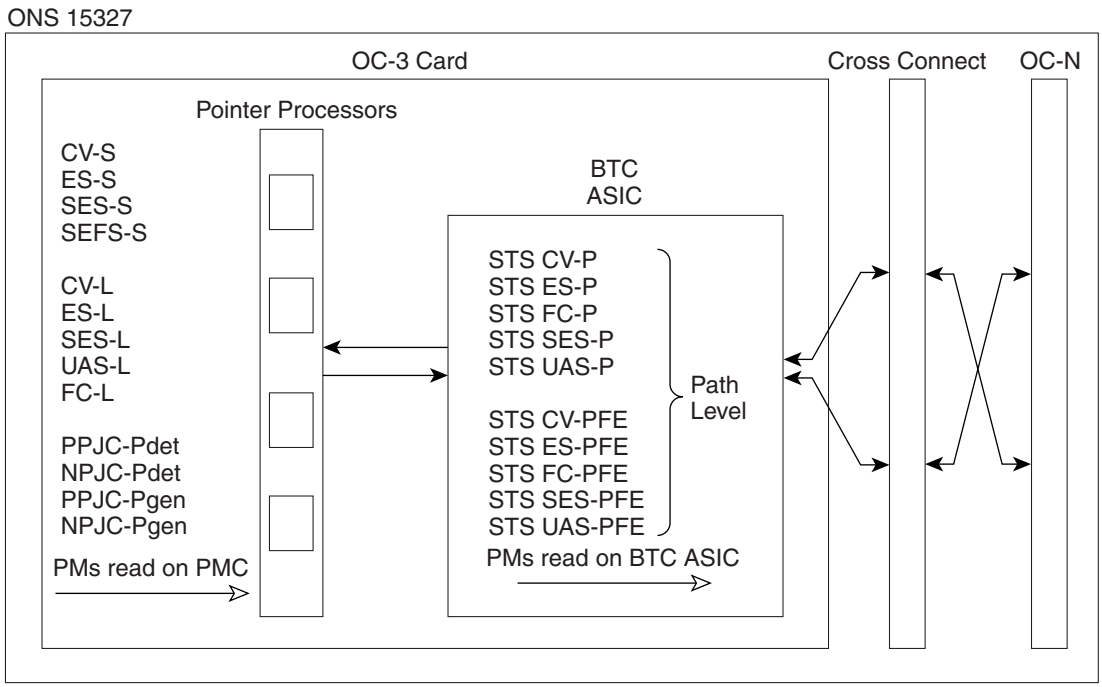


Figure 9-10 PM Parameter Read Points on the OC-3 Card



Note For PM locations relating to protection switch counts, see the Telcordia GR-253-CORE document.

The PM parameters for the OC-3 cards are described in Table 9-18 through Table 9-24 on page 9-23.

Table 9-18 Near-End Section PM Parameters for the OC-3 Card

Parameter	Definition
CV-S	CV-S is a count of BIP errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame, with each error incrementing the current CV-S second register.
ES-S	SES-S is a count of the number of seconds when at least one section-layer BIP error was detected or a SEF or LOS defect was present.
SES-S	SES-S is a count of the seconds when K (see Telcordia GR-253-CORE for value) or more section-layer BIP errors were detected or a SEF or LOS defect was present.
SEFS-S	SEFS-S is a count of the seconds when a SEF defect was present. A SEF defect is expected to be present during most seconds when a LOS or LOF defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect.

Table 9-19 Near-End Line Layer PM Parameters for the OC-3 Card

Parameter	Definition
CV-L	CV-L is a count of BIP errors detected at the line layer (that is, using the B2 bytes in the incoming SONET signal). Up to 8 x *n* BIP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	ES-L is a count of the seconds when at least one line-layer BIP error was detected or an AIS-L defect was present.
SES-L	SES-L is a count of the seconds when K (see Telcordia GR-253-CORE for values) or more line-layer BIP errors were detected or an AIS-L defect was present.
UAS-L	UAS-L is a count of the seconds when the line is considered unavailable. A line becomes unavailable at the onset of ten consecutive seconds that qualify as SES-Ls, and continues to be unavailable until the onset of ten consecutive seconds occur that do not qualify as SES-Ls.
FC-L	FC-L is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure is declared or when a lower-layer, traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.

Note For information about troubleshooting UPSR switch counts, refer to the *Cisco ONS 15327 Troubleshooting Guide*. For information about creating circuits that perform a switch, refer to the *Cisco ONS 15327 Procedure Guide*.

Table 9-20 Near-End Protection-Switching PM Parameters for the OC-3 Cards

Parameter	Definition
PSC (1+1 protection)	In a 1+1 protection scheme for a working card, Protection Switching Count (PSC) is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM parameter is only applicable if revertive line-level protection switching is used. **Note** BLSR is not supported on the OC-3 card; therefore, the Protection Switching Count-Working (PSC-W), Protection Switching Count-Span (PSC-S), and Protection Switching Count-Ring (PSC-R) PM parameters do not increment.
PSD	Protection Switching Duration (PSD) applies to the length of time, in seconds, that service is carried on another line. For a working line, PSD is a count of the number of seconds that service was carried on the protection line. For the protection line, PSD is a count of the seconds that the line was used to carry service. The PSD PM parameter is only applicable if revertive line-level protection switching is used. **Note** BLSR is not supported on the OC-3 card; therefore, the Protection Switching Duration-Working (PSD-W), Protection Switching Duration-Span (PSD-S), and Protection Switching Duration-Ring (PSD-R) PM parameters do not increment.

Note In CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tabs. See the "9.3 Pointer Justification Count Reference" section on page 9-4.

Table 9-21 Near-End SONET Path H-Byte PM Parameters for the OC-3 Card

Parameter	Definition
PPJC-Pdet	PPJC-Pdet is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	NPJC-Pdet is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	PPJC-Pgen is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	NPJC-Pgen is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.

Table 9-22 Far-End Line Layer PM Parameters for the OC-3 Card

Parameter	Definition
CV-LFE	CV-LFE is a count of BIP errors detected by the far-end LTE and reported back to the near-end LTE using the REI-L indication in the line overhead. For SONET signals at rates below OC-48, up to 8 x *n* BIP errors per STS-N frame can be indicated using the Line remote error indication (REI-L). For OC-48 signals, up to 255 BIP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each BIP error indicated by the incoming REI-L.
ES-LFE	ES-LFE is a count of the seconds when at least one line-layer BIP error was reported by the far-end LTE or a Line remote defect indication (RDI-L) defect was present.
SES-LFE	SES-LFE is a count of the seconds when K (see Telcordia GR-253-CORE for values) or more line-layer BIP errors were reported by the far-end LTE or an RDI-L defect was present.
UAS-LFE	UAS-LFE is a count of the seconds when the line is unavailable at the far end. A line becomes unavailable at the onset of ten consecutive seconds that qualify as SES-LFEs, and continues to be unavailable until the onset of ten consecutive seconds occur that do not qualify as SES-LFEs.
FC-LFE	FC-LFE is a count of the number of far-end line failure events. A failure event begins when RFI-L failure is declared, and it ends when the Line remote fault indication (RFI-L) failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

Note SONET path PM parameters do not count unless IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring Reference" section on page 9-2.

Table 9-23 Near-End SONET Path PM Parameters for the OC-3 Card

Parameter	Definition
STS CV-P	STS CV-P is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	STS ES-P is a count of the seconds when one or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	STS FC-P is a count of the number of near-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.

Table 9-23 Near-End SONET Path PM Parameters for the OC-3 Card (continued)

Parameter	Definition
STS SES-P	STS SES-P is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	STS UAS-P is a count of the seconds when the STS path is considered unavailable. An STS path becomes unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ps.

Note SONET path PM parameters do not count unless IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring Reference" section on page 9-2.

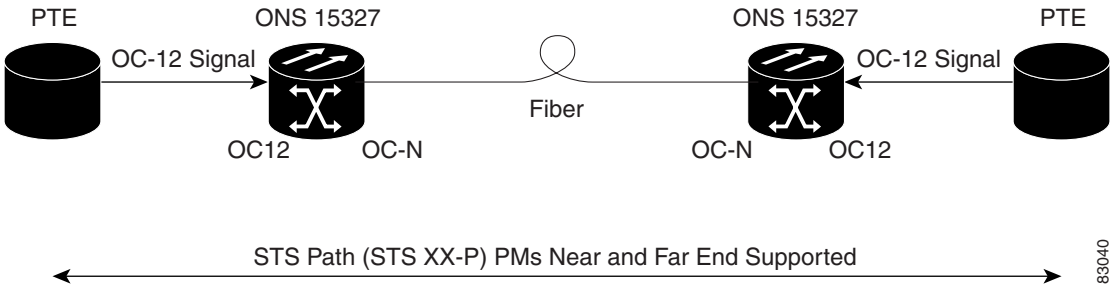
Table 9-24 Far-End SONET Path PM Parameters for the OC-3 Card

Parameter	Definition
STS CV-PFE	STS CV-PFE is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-PFE	STS ES-PFE is a count of the seconds when one or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.
STS FC-PFE	STS FC-PFE is a count of the number of far-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-PFE	STS SES-PFE is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS SES-PFE.
STS UAS-PFE	STS UAS-PFE is a count of the seconds when the STS path is considered unavailable. An STS path becomes unavailable at the onset of ten consecutive seconds that qualify as SES-PFEs, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-PFEs.

9.6.2 OC-12 Card Performance Monitoring Parameters

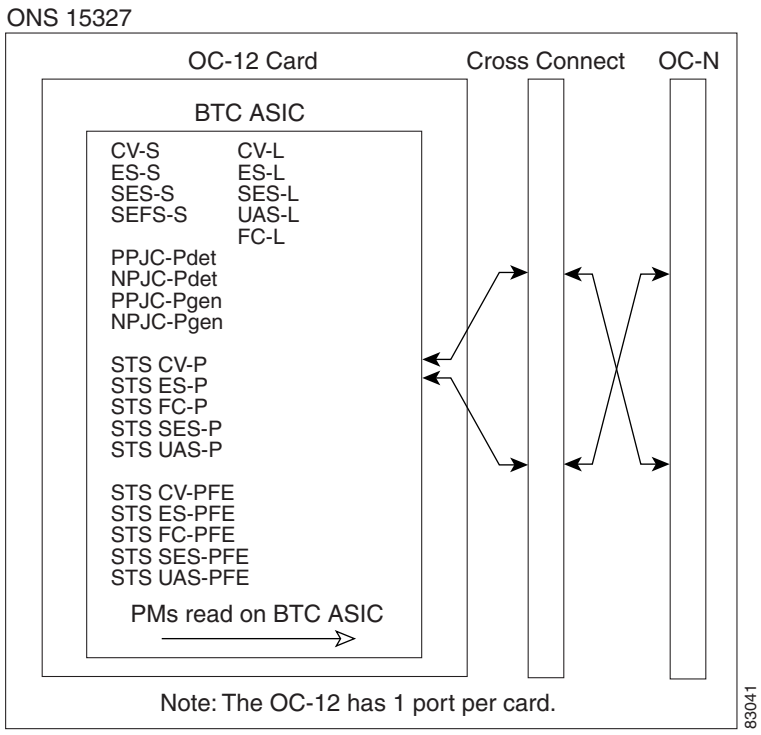
Figure 9-11 shows the signal types that support near-end and far-end PM parameters. Figure 9-12 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-12 cards.

Figure 9-11 Monitored Signal Types for the OC-12 Cards



Note PM parameters on the protect STS are not supported for BLSR. The XX in Figure 9-11 represents all PM parameters listed in Figure 9-12 with the given prefix and/or suffix.

Figure 9-12 PM Parameter Read Points on the OC-12 Cards



Note For PM locations relating to protection switch counts, see the Telcordia GR-1230-CORE document.

The PM parameters for the OC-12 cards are described in Table 9-25 through Table 9-31 on page 9-28.

Table 9-25 Near-End Section PM Parameters for the OC-12 Cards

Parameter	Definition
CV-S	CV-S is a count of BIP errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.
ES-S	ES-S is a count of the number of seconds when at least one section-layer BIP error was detected or a SEF or LOS defect was present.
SES-S	SES-S is a count of the seconds when K (see Telcordia GR-253 for value) or more section-layer BIP errors were detected or a SEF or LOS defect was present.
SEFS-S	SEFS-S is a count of the seconds when a SEF defect was present. An SEF defect is expected to be present during most seconds when a LOS or LOF defect is present. However, there may be situations when the SEFS-S parameter is only incremented based on the presence of an SEF defect.

Table 9-26 Near-End Line Layer PM Parameters for the OC-12 Cards

Parameter	Definition
CV-L	CV-L is a count of BIP errors detected at the line layer (that is, using the B2 bytes in the incoming SONET signal). Up to 8 x N BIP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	ES-L is a count of the seconds when at least one line-layer BIP error was detected or an AIS-L defect was present.
SES-L	SES-L is a count of the seconds when K (see Telcordia GR-253 for values) or more line-layer BIP errors were detected or an AIS-L defect was present.
UAS-L	UAS-L is a count of the seconds when the line is unavailable. A line becomes unavailable at the onset of ten consecutive seconds that qualify as SES-Ls, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ls.
FC-L	FC-L is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure or a lower-layer traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.

Note In CTC, the count fields for Positive Point Justification Count (PPJC) and Negative Pointer Justification Count (NPJC) PM parameters appear white and blank unless they are enabled on the **Provisioning > Line** tabs. See the "9.3 Pointer Justification Count Reference" section on page 9-4.

Table 9-27 Near-End SONET Path H-byte PM Parameters for the OC-12 Cards

Parameter	Definition
PPJC-Pdet	PPJC-Pdet is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	NPJC-Pdet is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	PPJC-Pgen is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	NPJC-Pgen is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.

Note For information about troubleshooting UPSR switch counts, refer to the *Cisco ONS 15327 Troubleshooting Guide*. For information about creating circuits that perform a switch, refer to the *Cisco ONS 15327 Procedure Guide*.

Table 9-28 Near-End Protection-Switching PM Parameters for the OC-12 Cards

Parameter	Definition
PSC (BLSR)	For a protect line in a two-fiber ring, PSC refers to the number of times a protection switch has occurred either to a particular span's line protection or away from a particular span's line protection. Therefore, if a protection switch occurs on a two-fiber BLSR, the PSC of the protection span to which the traffic is switched will increment, and when the switched traffic returns to its original working span from the protect span, the PSC of the protect span will increment again.
PSC (1+1 protection)	In a 1+1 protection scheme for a working card, PSC is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM parameter is only applicable if revertive line-level protection switching is used.
PSD	For an active protection line in a two-fiber BLSR, PSD is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. PSD increments on the active protect line and PSD-W increments on the failed working line.

Table 9-28 Near-End Protection-Switching PM Parameters for the OC-12 Cards (continued)

Parameter	Definition
PSC-W	For a working line in a two-fiber BLSR, PSC-W is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line and PSC increments on the active protect line.
PSD-W	For a working line in a two-fiber BLSR, PSD-W is a count of the number of seconds that service was carried on the protection line. PSD-W increments on the failed working line and PSD increments on the active protect line.

Note SONET path PM parameters do not count unless IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring Reference" section on page 9-2.

Table 9-29 Near-End SONET Path PM Parameters for the OC-12 Cards

Parameter	Definition
STS CV-P	STS CV-P is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	STS ES-P is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	STS FC-P is a count of the number of near-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	STS SES-P is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	STS UAS-P is a count of one-second intervals when the STS path is unavailable. An STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds occur that do not qualify as SES-Ps. The ten seconds with no SES-Ps are excluded from unavailable time.

Table 9-30 Far-End Line Layer PM Parameters for the OC-12 Card

Parameter	Definition
CV-LFE	CV-LFE is a count of BIP errors detected by the far-end LTE and reported back to the near-end LTE using the REI-L indication in the line overhead. For SONET signals at rates below OC-48, up to 8 x N BIP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 BIP errors per STS-N frame can be indicated. The current CV-LFE second register is incremented for each BIP error indicated by the incoming REI-L.
ES-LFE	ES-LFE is a count of the seconds when at least one line-layer BIP error was reported by the far-end LTE or an RDI-L defect was present.
SES-LFE	SES-LFE is a count of the seconds when K (see Telcordia GR-253-CORE for values) or more line-layer BIP errors were reported by the far-end LTE or an RDI-L defect was present.
UAS-LFE	UAS-LFE is a count of the seconds when the line is considered unavailable at the far end. A line is considered unavailable at the onset of ten consecutive seconds that qualify as SES-LFEs, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-LFEs.
FC-LFE	FC-LFE is a count of the number of far-end line failure events. A failure event begins when RFI-L failure is declared and ends when the RFI-L failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

Note SONET path PM parameters do not count unless IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring Reference" section on page 9-2.

Table 9-31 Far-End SONET Path PM Parameters for the OC-12 Card

Parameter	Definition
STS CV-PFE	STS CV-PFE is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-PFE	STS ES-PFE is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.
STS FC-PFE	STS FC-PFE is a count of the number of far-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.

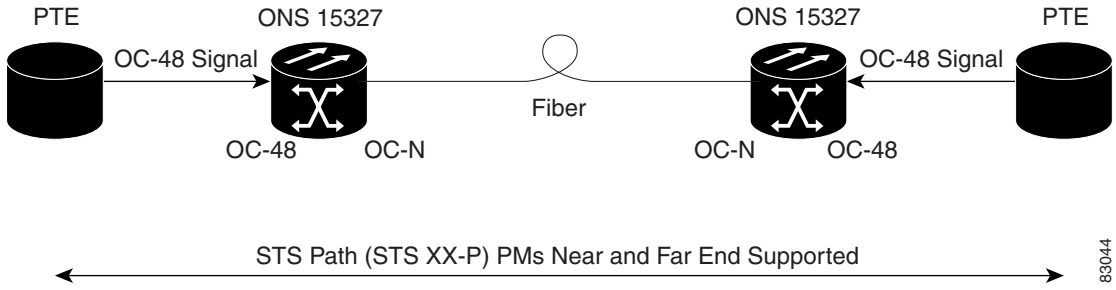
Table 9-31 Far-End SONET Path PM Parameters for the OC-12 Card (continued)

Parameter	Definition
STS SES-PFE	STS SES-PFE is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS SES-PFE.
STS UAS-PFE	STS UAS-PFE is a count of one-second intervals when the STS path is unavailable. An STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-PFEs, and continues to be unavailable until the onset of ten consecutive seconds occur that do not qualify as SES-PFEs. The ten seconds with no SES-PFEs are excluded from unavailable time.

9.6.3 OC-48 Card Performance Monitoring Parameters

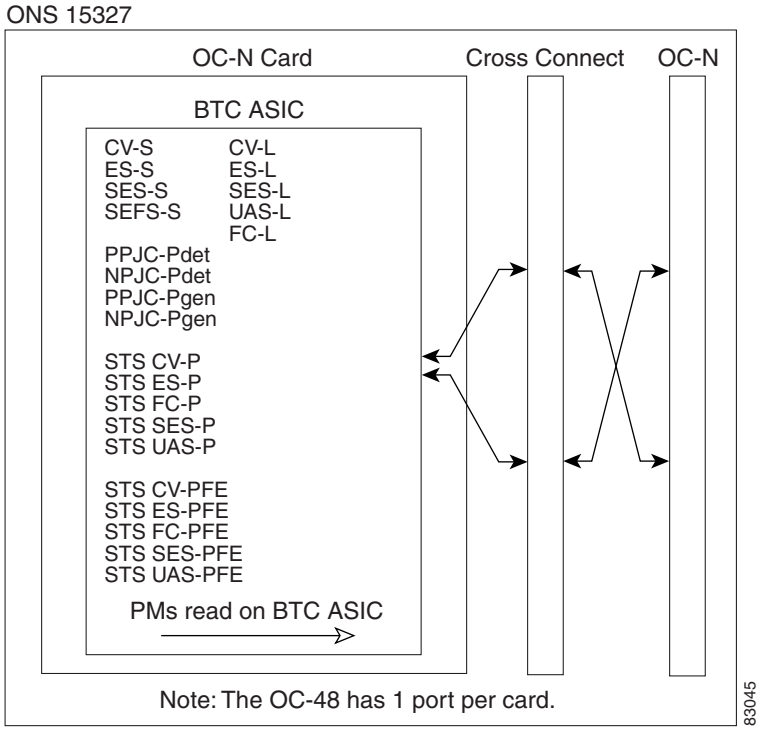
Figure 9-13 shows the signal types that support near-end and far-end PM parameters. Figure 9-14 on page 9-30 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-48 cards.

Figure 9-13 Monitored Signal Types for the OC-48 Cards



Note PM parameters on the protect STS are not supported for BLSR. The XX in Figure 9-13 represents all PM parameters listed in Figure 9-14 on page 9-30 with the given prefix and/or suffix.

Figure 9-14 PM Parameter Read Points on the OC-48 Cards



Note For PM locations relating to protection switch counts, see the Telcordia GR-1230-CORE document.

The PM parameters for the OC-48 cards are described in Table 9-32 through Table 9-38 on page 9-34.

Table 9-32 Near-End Section PM Parameters for the OC-48 Cards

Parameter	Definition
CV-S	CV-S is a count of BIP errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.
ES-S	ES-S is a count of the number of seconds when at least one section-layer BIP error was detected or a SEF or LOS defect was present.
SES-S	SES-S is a count of the seconds when K (see Telcordia GR-253 for value) or more section-layer BIP errors were detected or a SEF or LOS defect was present.
SEFS-S	SEFS-S is a count of the seconds when a SEF defect was present. An SEF defect is expected to be present during most seconds when a LOS or LOF defect is present. However, there may be situations when the SEFS-S parameter is only incremented based on the presence of an SEF defect.

Table 9-33 Near-End Line Layer PM Parameters for the OC-48 Cards

Parameter	Definition
CV-L	CV-L is a count of BIP errors detected at the line layer (that is, using the B2 bytes in the incoming SONET signal). Up to 8 x *n* BIP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	ES-L is a count of the seconds when at least one line-layer BIP error was detected or an AIS-L defect was present.
SES-L	SES-L is a count of the seconds when K (see Telcordia GR-253 for values) or more line-layer BIP errors were detected or an AIS-L defect was present.
UAS-L	UAS-L is a count of the seconds when the line is considered unavailable. A line becomes unavailable at the onset of ten consecutive seconds that qualify as SES-Ls, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ls.
FC-L	FC-L is a count of the number of near-end line failure events. A failure event begins when an AIS-L failure or a lower-layer, traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.

Note In CTC, the count fields for Positive Point Justification Count (PPJC) and Negative Pointer Justification Count (NPJC) PM parameters appear white and blank unless they are enabled on the Provisioning > Line tabs. See the "9.3 Pointer Justification Count Reference" section on page 9-4.

Table 9-34 Near-End SONET Path H-byte PM Parameters for the OC-48 Cards

Parameter	Definition
PPJC-Pdet	PPJC-Pdet is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	NPJC-Pdet is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	PPJC-Pgen is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	NPJC-Pgen is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.

Note For information about troubleshooting UPSR switch counts, refer to the *Cisco ONS 15327 Troubleshooting Guide*. For information about creating circuits that perform a switch, refer to the *Cisco ONS 15327 Procedure Guide*.

Table 9-35 Near-End Protection-Switching PM Parameters for the OC-48 Cards

Parameter	Definition
PSC (BLSR)	For a protect line in a two-fiber ring, PSC refers to the number of times a protection switch has occurred either to a particular span's line protection or away from a particular span's line protection. Therefore, if a protection switch occurs on a two-fiber BLSR, the PSC of the protection span to which the traffic is switched will increment, and when the switched traffic returns to its original working span from the protect span, the PSC of the protect span will increment again.
PSC (1+1 protection)	In a 1+1 protection scheme for a working card, PSC is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM parameter is only applicable if revertive line-level protection switching is used.
PSD	For an active protection line in a two-fiber BLSR, PSD is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. PSD increments on the active protect line and PSD-W increments on the failed working line.
PSC-W	For a working line in a two-fiber BLSR, PSC-W is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line and PSC increments on the active protect line.
PSD-W	For a working line in a two-fiber BLSR, PSD-W is a count of the number of seconds that service was carried on the protection line. PSD-W increments on the failed working line and PSD increments on the active protect line.

Note SONET path PM parameters do not count unless IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring Reference" section on page 9-2.

Table 9-36 Near-End SONET Path PM Parameters for the OC-48 Cards

Parameter	Definition
STS CV-P	STS CV-P is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-P	STS ES-P is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.

Table 9-36 Near-End SONET Path PM Parameters for the OC-48 Cards (continued)

Parameter	Definition
STS FC-P	STS FC-P is a count of the number of near-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	STS SES-P is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS SES-P.
STS UAS-P	STS UAS-P is a count of the one-second intervals when the STS path is unavailable. The STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-Ps, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ps. The ten seconds with no SES-Ps are excluded from available time.

Table 9-37 Far-End Line Layer PM Parameters for the OC-48 Cards

Parameter	Definition
CV-LFE	CV-LFE is a count of BIP errors detected by the far-end LTE and reported back to the near-end LTE using the REI-L indication in the line overhead. For SONET signals at rates below OC-48, up to 8 x N BIP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 BIP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each BIP error indicated by the incoming REI-L.
ES-LFE	ES-LFE is a count of the seconds when at least one line-layer BIP error was reported by the far-end LTE or an RDI-L defect was present.
SES-LFE	SES-LFE is a count of the seconds when K (see Telcordia GR-253-CORE for values) or more line-layer BIP errors were reported by the far-end LTE or an RDI-L defect was present.
UAS-L	UAS-L is a count of the seconds when the line is considered unavailable at the far end. A line becomes unavailable at the onset of ten consecutive seconds that qualify as SES-LFEs, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-LFEs.
FC-L	FC-L is a count of the number of far-end line failure events. A failure event begins when RFI-L failure is declared and ends when the RFI-L failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

Note SONET path PM parameters do not count unless IPPM is enabled. For additional information, see the "9.2 Intermediate-Path Performance Monitoring Reference" section on page 9-2.

Table 9-38 Far-End SONET Path PM Parameters for the OC-48 Cards

Parameter	Definition
STS CV-PFE	STS CV-PFE is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
STS ES-PFE	STS ES-PFE is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.
STS FC-PFE	STS FC-PFE is a count of the number of far-end STS path failure events. A failure event begins with an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports RDI-P for that path. The failure event ends when these failures are cleared.
STS SES-PFE	STS SES-P is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS SES-PFE.
STS UAS-PFE	STS UAS-PFE is a count of the one-second intervals when the STS path is unavailable. The STS path is unavailable at the onset of ten consecutive seconds that qualify as SES-PFEs, and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-PFEs. The ten seconds with no SES-PFEs are excluded from available time.

CHAPTER 10

Ethernet Operation

The Cisco ONS 15327 integrates Ethernet into a SONET time-division multiplexing (TDM) platform. The ONS 15327 supports E-Series and G-Series Ethernet cards. For Ethernet card specifications, see Chapter 2, "Card Reference." For step-by-step Ethernet card circuit configuration procedures, refer to the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

10.1 G-Series Application

The G-Series card (G1000-2) reliably transports Ethernet and IP data across a SONET backbone. The G-Series card maps up to two Gigabit Ethernet interfaces onto a SONET transport network and provides scalable and provisionable transport bandwidth at signal levels up to STS-48c per card. The G-Series card provides line rate forwarding for all Ethernet frames (unicast, multicast, and broadcast) and can be configured to support Jumbo frames (defined as a maximum of 10,000 bytes). The G-series card incorporates features optimized for carrier-class applications such as:

- High Availability (including hitless (< 50 ms) performance under software upgrades and all types of SONET/SDH equipment protection switches)
- Hitless reprovisioning
- Support of Gigabit Ethernet traffic at full line rate
- Full TL1-based provisioning capability (refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide* for G-Series TL1 provisioning commands)

The G-Series card allows an Ethernet private line service to be provisioned and managed very much like a traditional SONET line. G-Series card applications include providing carrier-grade transparent LAN services (TLS), 100 Mbps Ethernet private line services (when combined with an external 100 Mb Ethernet switch with Gigabit uplinks), and high-availability transport for applications such as storage over MAN/WANs. The card maps a single Ethernet port to a single STS circuit. You can independently map the two ports on the G-Series card to any combination of STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c circuit sizes, provided the sum of the circuit sizes that terminate on a card do not exceed STS-48c.

To support a Gigabit Ethernet port at full line rate, an STS circuit with a capacity greater or equal to 1 Gbps (bidirectional 2 Gbps) is needed. An STS-24c is the minimum circuit size that can support a Gigabit Ethernet port at full line rate.

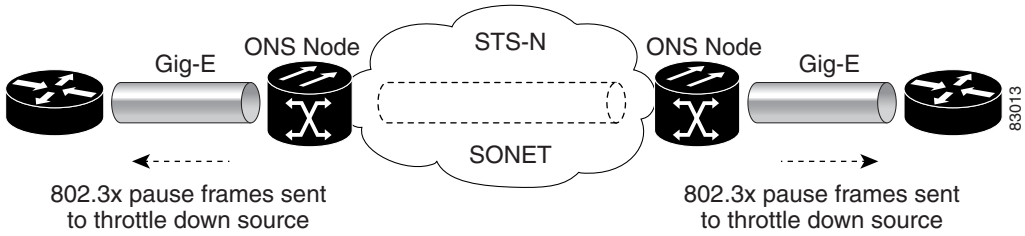
The G-Series card transmits and monitors the SONET J1 Path Trace byte in the same manner as ONS 15327 OC-N cards.

Note G-Series encapsulation is standard high-level data link control (HDLC) framing over SONET/SDH as described in RFC 1622 and RFC 2615 with the point-to-point (PPP) protocol field set to the value specified in RFC 1841.

10.1.1 G-Series Example

Figure 10-1 shows an example of a G-Series application. In this example, data traffic from the Gigabit Ethernet port of a high-end router travels across the ONS 15327 point-to-point circuit to the Gigabit Ethernet port of another high-end router.

Figure 10-1 Data Traffic on G-Series Point-To-Point Circuit



The G-Series card carries any Layer 3 protocol that can be encapsulated and transported over Gigabit Ethernet, such as IP or IPX. The data is transmitted on the Gigabit Ethernet fiber into the standard Small Form-factor Pluggable (SFP) modules on a G-Series card. The G-Series card transparently maps Ethernet frames into the SONET payload by multiplexing the payload onto a SONET OC-N card. When the SONET payload reaches the destination node, the process is reversed and the data is transmitted from the standard Cisco SFP in the destination G-Series card onto the Gigabit Ethernet fiber.

The G-Series card discards certain types of erroneous Ethernet frames rather than transport them over SONET. Erroneous Ethernet frames include corrupted frames with CRC errors and under-sized frames that do not conform to the minimum 64-byte length Ethernet standard. The G-Series card forwards valid frames unmodified over the SONET network. Information in the headers is not affected by the encapsulation and transport. For example, packets with formats that include IEEE 802.1Q information will travel through the process unaffected.

10.1.2 802.3z Flow Control and Frame Buffering

The G-Series supports 802.3z flow control and frame buffering to reduce data traffic congestion. To prevent over-subscription, 512 KB of buffer memory is available for the receive and transmit channels on each port. When the buffer memory on the Ethernet port nears capacity, the ONS 15327 uses 802.3z flow control to transmit a pause frame to the source at the opposite end of the Gigabit Ethernet connection.

The pause frame instructs the source to stop sending packets for a specific period of time. The sending station waits the requested time before sending more data. Figure 10-1 on page 10-2 illustrates pause frames being sent and received by ONS 15327s and attached switches.

With Software R4.0 and later, the G-Series card has symmetric flow control and proposes symmetric flow control when auto-negotiating flow control with attached Ethernet devices. Symmetric flow control allows the G-Series to respond to pause frames sent from external devices and send pause frames to external devices. Prior to Software R4.0, flow control on the G-Series card was asymmetric, meaning the card sent pause frames and discarded received pause frames.

This flow-control mechanism matches the sending and receiving device throughput to that of the bandwidth of the STS circuit. For example, a router might transmit to the Gigabit Ethernet port on the G-Series. This particular data rate may occasionally exceed 622 Mbps, but the ONS 15327 circuit assigned to the G-Series port might be only STS-12c (622.08 Mbps). In this example, the ONS 15327 sends out a pause frame and requests that the router delay its transmission for a certain period of time. With flow control and a substantial per-port buffering capability, a private line service provisioned at less than full line rate capacity (STS-24c) is efficient because frame loss can be controlled to a large extent.

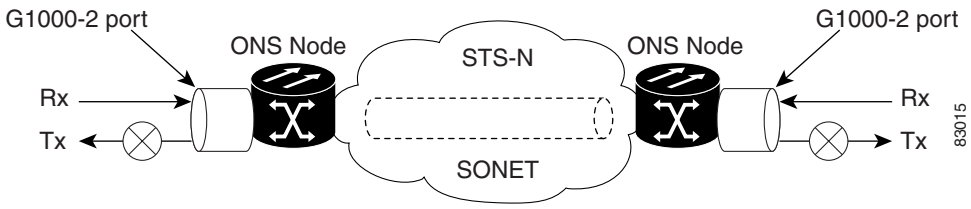
Note External Ethernet devices with auto-negotiation that are configured to interoperate with G-Series cards running releases prior to release 4.0 do not need to change auto-negotiation settings when interoperating with G-Series cards running release 4.0 and later.

Note With a G-Series card, you can only enable flow control on a port if auto-negotiation is enabled on the device attached to that port.

10.1.3 Ethernet Link Integrity Support

The G-Series supports end-to-end Ethernet link integrity (see Figure 10-2). This capability is integral to providing an Ethernet private line service and correct operation of Layer 2 and Layer 3 protocols on the attached Ethernet devices. End-to-end Ethernet link integrity essentially means that if any part of the end-to-end path fails the entire path fails. Failure of the entire path is ensured by turning off the transmit lasers at each end of the path. The attached Ethernet devices recognize the disabled transmit laser as a loss of carrier and consequently an inactive link.

Figure 10-2 End-to-end Ethernet Link Integrity Support



Note Some network devices can be configured to ignore a loss of carrier condition. If a device configured to ignore a loss of carrier condition attaches to a G-Series card at one end, alternative techniques (such as use of Layer 2 or Layer 3 keep-alive messages) are required to route traffic around failures. The response time of such alternate techniques is typically much longer than techniques that use link state as indications of an error condition.

Note Enabling or disabling port-level flow control on the test set or other Ethernet device attached to the G-Series port can affect the transmit (Tx) laser and result in unidirectional traffic flow.

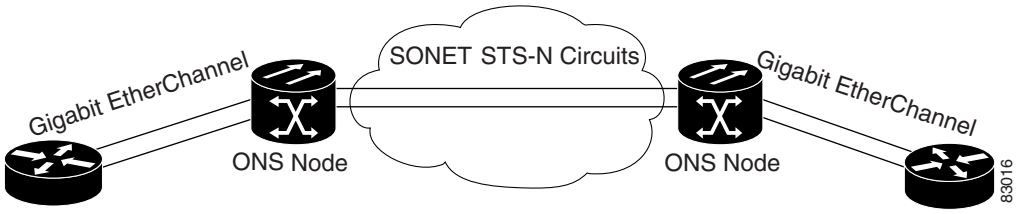
As shown in Figure 10-2 on page 10-3, a failure at any point of the path causes the G-Series card at each end to disable its transmit (Tx) laser, which causes the devices at both ends to detect a link down. If one of the Ethernet ports is administratively disabled or set in loopback mode, the port is considered a failure for the purposes of end-to-end link integrity because the end-to-end Ethernet path is unavailable. The port failure also disables both ends of the path.

10.1.4 Gigabit EtherChannel/802.3ad Link Aggregation

The end-to-end Ethernet link integrity feature can be used in combination with Gigabit EtherChannel capability on attached devices. The combination provides an Ethernet traffic restoration scheme that has a faster response time than alternate techniques such as spanning tree rerouting, yet is more bandwidth efficient because spare bandwidth does not need to be reserved.

The G-Series supports all forms of link aggregation technologies including Gigabit EtherChannel (GEC), which is a Cisco proprietary standard, and the IEEE 802.3ad standard. The end-to-end link integrity feature of the G-Series allows a circuit to emulate an Ethernet link. This allows all flavors of Layer 2 and Layer 3 rerouting to work correctly with the G-Series. Figure 10-3 illustrates G-Series GEC support.

Figure 10-3 G-Series Gigabit EtherChannel (GEC) Support



Although the G-Series card does not actively run GEC, it supports the end-to-end GEC functionality of attached Ethernet devices. If two Ethernet devices running GEC connect through G-Series cards to an ONS 15327 network, the ONS 15327 SONET side network is transparent to the EtherChannel devices. The EtherChannel devices operate as if they are directly connected to each other. Any combination of G-Series parallel circuit sizes can be used to support GEC throughput.

GEC provides line-level active redundancy and protection (1:1) for attached Ethernet equipment. It can also bundle parallel G-Series data links together to provide more aggregated bandwidth. STP operates as if the bundled links are one link and permits GEC to utilize these multiple parallel paths. Without GEC, STP permits only a single non-blocked path. GEC can also provide G-Series card-level protection or redundancy because it can support a group of ports on different cards (or different nodes) so that if one port or card has a failure, traffic is rerouted over the other port or card.

10.2 E-Series Application

The E-Series cards (E10/100-4) incorporate Layer 2 switching, whereas the G-Series card is a straight mapper card. E-Series cards support virtual local area networks (VLANs), IEEE 802.1Q, STP, and IEEE 802.1D.

10.2.1 E-Series Modes

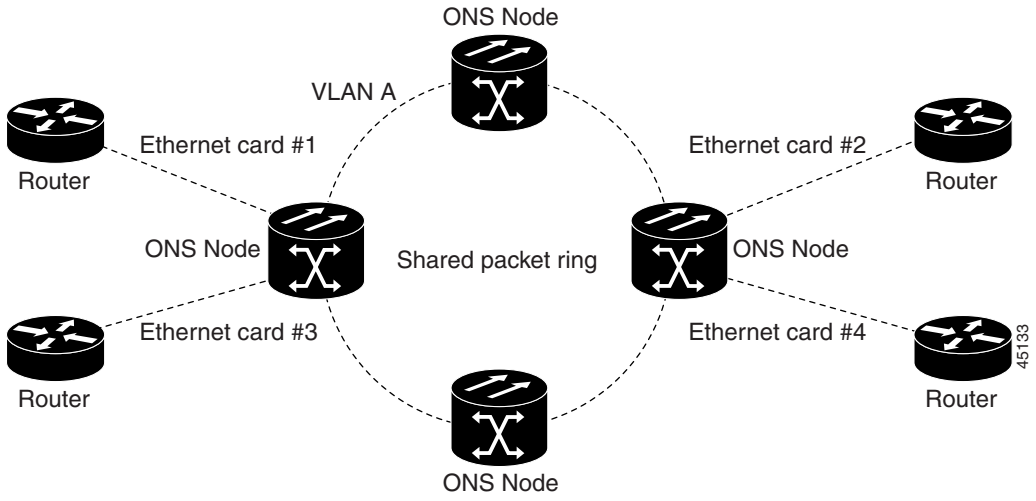
An E-Series card operates in one of three modes: Multicard EtherSwitch Group, Single-card EtherSwitch, or Port-mapped. Within an ONS 15327 containing multiple E-Series cards, each E-Series card can operate in any of the three separate modes. At the Ethernet card view in CTC, click the Provisioning > Ether Card tabs to reveal the card modes.

Note Port-mapped mode eliminates issues inherent in other E-Series modes and detailed in the field notice, "E-Series Ethernet Line Card Packet Forwarding Limitations."

10.2.1.1 E-Series Multicard EtherSwitch Group

Multicard EtherSwitch Group provisions two or more Ethernet cards to act as a single Layer 2 switch. It supports one STS-3c shared packet rings or three STS-1 shared packet rings. Each multicard switch may connect up to a total of STS-3c in SONET circuits. When provisioned as an add or drop node of a shared packet ring circuit, the effective bandwidth doubles, supporting STS-3c in each direction of the ring. Figure 10-4 illustrates a Multicard EtherSwitch configuration.

Figure 10-4 Multicard EtherSwitch Configuration

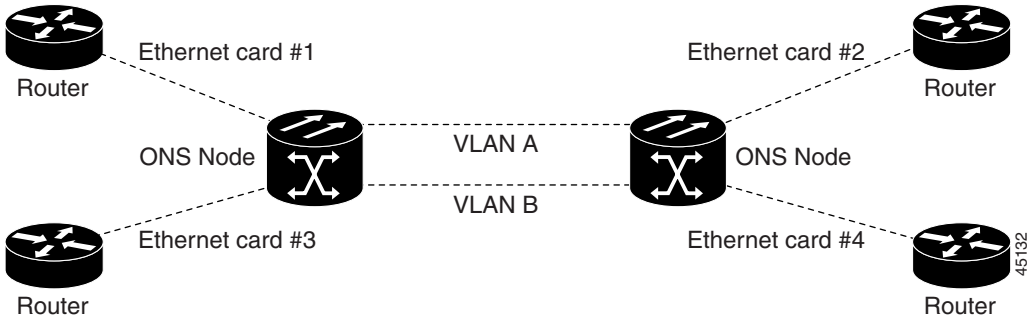


Caution Whenever you terminate two STS-3c multicard EtherSwitch circuits on an Ethernet card and later delete the first circuit, delete the remaining STS-3c circuit before you provision an STS-1 circuit to the card. If you attempt to create an STS-1 circuit after only deleting the first STS-3c circuit, the STS-1 circuit will not work, but no alarms will indicate this condition. To avoid this situation, delete the second STS-3c before creating an STS-1 circuit.

10.2.1.2 E-Series Single-card EtherSwitch

Single-card EtherSwitch allows each Ethernet card to remain a single switching entity within the ONS 15327 shelf. This option allows STS-12c worth of bandwidth between two Ethernet circuit endpoints. Figure 10-5 on page 10-6 illustrates a Single-card EtherSwitch configuration.

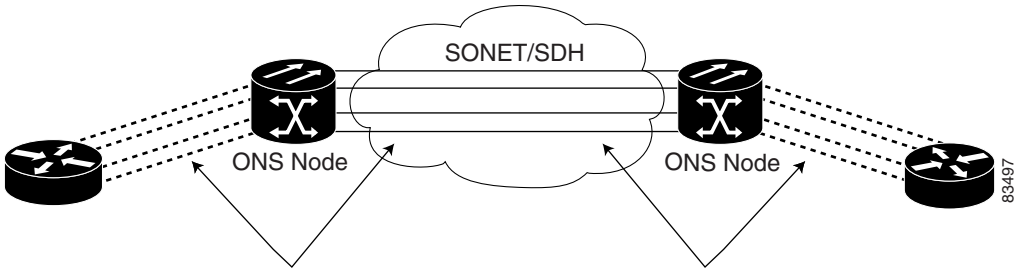
Figure 10-5 Single-card EtherSwitch Configuration



10.2.1.3 Port-Mapped (Linear Mapper)

Port-mapped mode, also referred to as linear mapper, configures the E-Series card to map a specific E-Series Ethernet port to one of the STS circuits on the card (see Figure 10-6). Port-mapped mode ensures Layer 1 transport has low latency for unicast, multicast, and mixed traffic. Ethernet and Fast Ethernet on the E10/100-4 card operate at line-rate speed. Ethernet frame sizes up to 1522 bytes are also supported, which allows transport of 802.1Q tagged frames. The larger maximum frame size of Q-in-Q frames, 802.1Q in 802.1Q wrapped frames, are not supported.

Figure 10-6 E-Series Mapping Ethernet Ports to SONET STS Circuits



Port-mapped mode disables Layer 2 functions supported by the E-Series in Single-card and Multicard mode, including STP, VLANs, and MAC address learning. It significantly reduces the service-affecting time for cross-connect and TCC+/TCC2 card switches.

Port-mapped mode does not support VLANs in the same manner as multicard and single-card mode. The ports of E-Series cards in multicard and single-card mode can join specific VLANs. E-Series cards in port-mapped mode do not have this Layer 2 capability and only transparently transport external VLANs over the mapped connection between ports. An E-Series card in port-mapped mode does not inspect the tag of the transported VLAN, so a VLAN range of 1 through 4096 can be transported in port-mapped mode.

Port-mapped mode also allows the creation of STS circuits between any two E-Series cards, including the E10/100-4 and, on the Cisco ONS 15454, the E1000-G and E100G-12 cards. Port-mapped mode does not allow an E-Series cards to connect to the G-Series cards or the ONS 15454 ML-Series cards.

10.2.2 E-Series 802.3z Flow Control

The E10/100-4 supports 802.3z symmetrical flow control and proposes symmetric flow control when auto-negotiating with attached Ethernet devices. For flow control to operate, both the E-Series port and the attached Ethernet device must be set to auto-negotiation (AUTO) mode. The flow-control mechanism allows the E-Series to respond to pause frames sent from external devices and send pause frames to external devices. Flow control matches the sending and receiving device throughput to that of the bandwidth of the STS circuit.

Note To enable flow control between an E-Series in port mapped mode and a SmartBits test set, manually set bit 5 of the MII register to 0 on the SmartBits test set. To enable flow control between an E-Series in port mapped mode and an Ixia test set, select Enable the flow control in the properties menu of the attached Ixia port.

10.2.3 E-Series VLAN Support

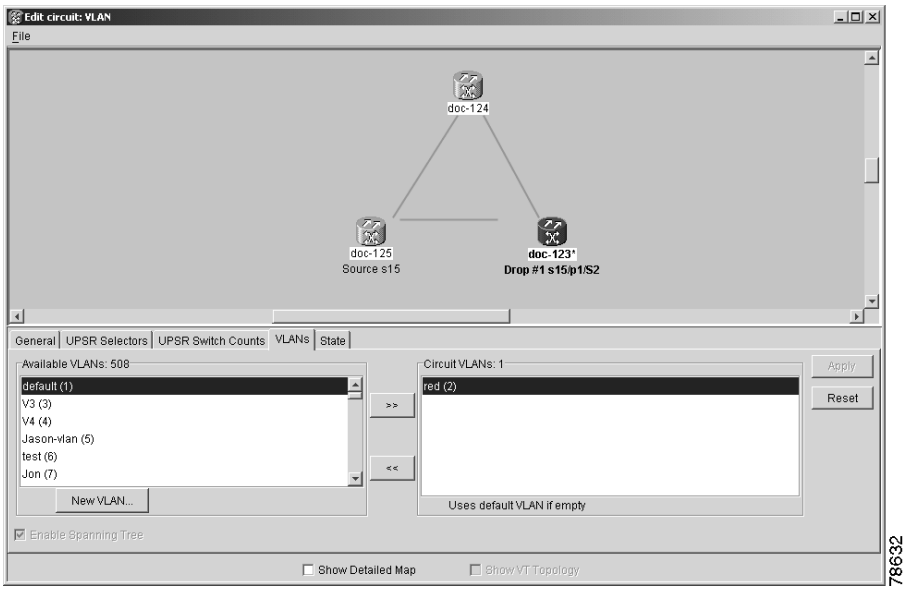
Users can provision up to 509 VLANs per network with the CTC software. Specific sets of ports define the broadcast domain for the ONS 15327. The definition of VLAN ports includes all Ethernet and packet-switched SONET port types. All VLAN IP address discovery, flooding, and forwarding is limited to these ports.

The ONS 15327 802.1Q-based VLAN mechanism provides logical isolation of subscriber LAN traffic over a common SONET transport infrastructure. Each subscriber has an Ethernet port at each site, and each subscriber is assigned to a VLAN. Although the subscriber's VLAN data flows over shared circuits, the service appears to the subscriber as a private data transport.

Note Port-mapped mode does not support VLANs.

The number of VLANs used by circuits and the total number of VLANs available for use appears in CTC on the VLAN counter (see Figure 10-7 on page 10-8).

Figure 10-7 Edit Circuit Dialog Featuring Available VLANs



10.2.4 E-Series Q-Tagging (IEEE 802.1Q)

E-Series cards in single-card and multicard mode support IEEE 802.1Q. IEEE 802.1Q allows the same physical port to host multiple 802.1Q VLANs. Each 802.1Q VLAN represents a different logical network. E-Series cards in port-mapped mode transport IEEE 802.1Q tags (Q-tags), but do not remove or add these tags.

The ONS 15327 works with Ethernet devices that support IEEE 802.1Q and those that do not support IEEE 802.1Q. If a device attached to an ONS 15327 Ethernet port does not support IEEE 802.1Q, the ONS 15327 uses Q-tags internally only. The ONS 15327 associates these Q-tags with specific ports.

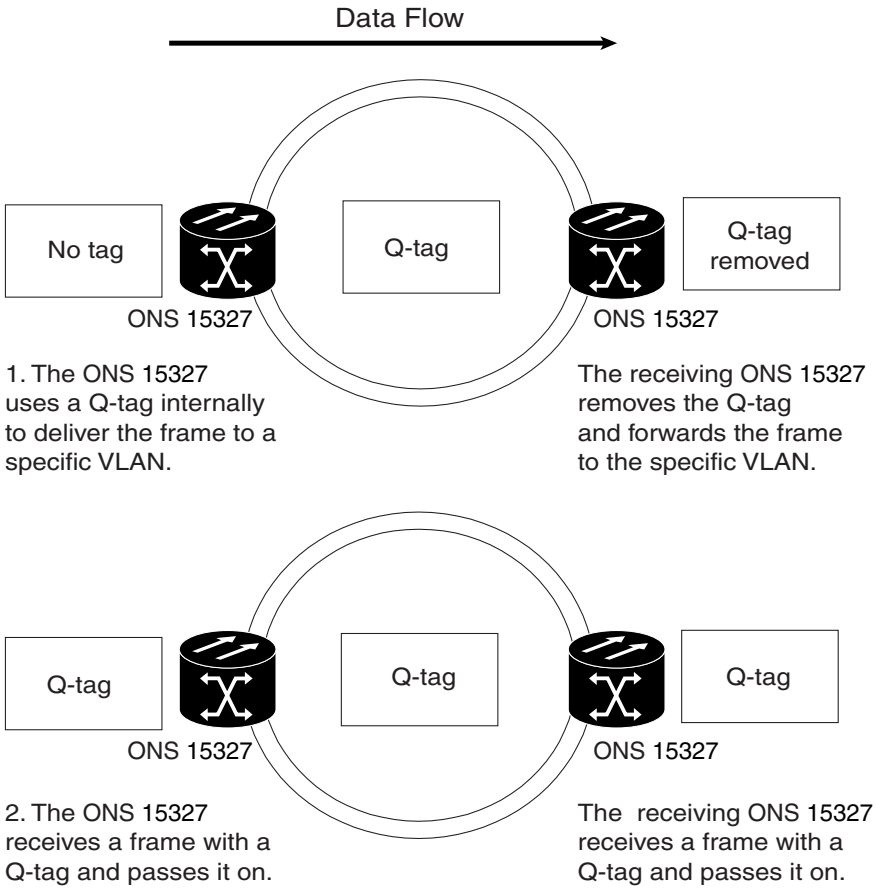
With Ethernet devices that do not support IEEE 802.1Q, the ONS 15327 takes non-tagged Ethernet frames that enter the ONS network and uses a Q-tag to assign the packet to the VLAN associated with the ONS network's ingress port. The receiving ONS node removes the Q-tag when the frame leaves the ONS network (to prevent older Ethernet equipment from incorrectly identifying the 8021.Q packet as an illegal frame). The ingress and egress ports on the ONS network must be set to Untag for the removal to occur. Untag is the default setting for ONS ports. Example 1 in Figure 10-8 on page 10-9 illustrates Q-tag use only within an ONS network.

The ONS 15327 uses the Q-tag attached by the external Ethernet devices that support IEEE 802.1Q. Packets enter the ONS network with an existing Q-tag; the ONS 15327 uses this same Q-tag to forward the packet within the ONS network and leaves the Q-tag attached when the packet leaves the ONS network. The entry and egress ports on the ONS network must be set to Tagged for this process to occur. Example 2 in Figure 10-8 on page 10-9 illustrates the handling of packets that both enter and exit the ONS network with a Q-tag.

For more information about setting ports to Tagged and Untag, refer to the *Cisco ONS 15327 Procedure Guide*.

Caution ONS 15327s propagate VLANs whenever a node appears on the network view of another node, regardless of whether the nodes are in the same SONET network or connected through DCC. For example, if two ONS 15327s without DCC connectivity belong to the same login node group, VLANs propagate between the two ONS 15327s. VLAN propagation happens even though the ONS 15327s do not belong to the same SONET ring.

Figure 10-8 Q-Tag Moving through VLAN



10.2.5 E-Series Priority Queuing (IEEE 802.1Q)

Networks without priority queuing handle all packets on a first-in-first-out basis. Priority queuing reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. The ONS 15327 supports priority queuing. The ONS 15327 maps the eight priorities specified in IEEE 802.1Q to two queues, low priority and high priority (see Table 10-1 on page 10-10). Q-tags carry priority queuing information through the network.

The ONS 15327 uses a "leaky bucket" algorithm to establish a weighted priority (not a strict priority). A weighted priority gives high-priority packets greater access to bandwidth, but does not totally preempt low-priority packets. During periods of network congestion, roughly 70% of bandwidth goes to the high-priority queue and the remaining 30% goes to the low-priority queue. A network that is too congested will drop packets.

Note IEEE 802.1Q was formerly IEEE 802.1P.

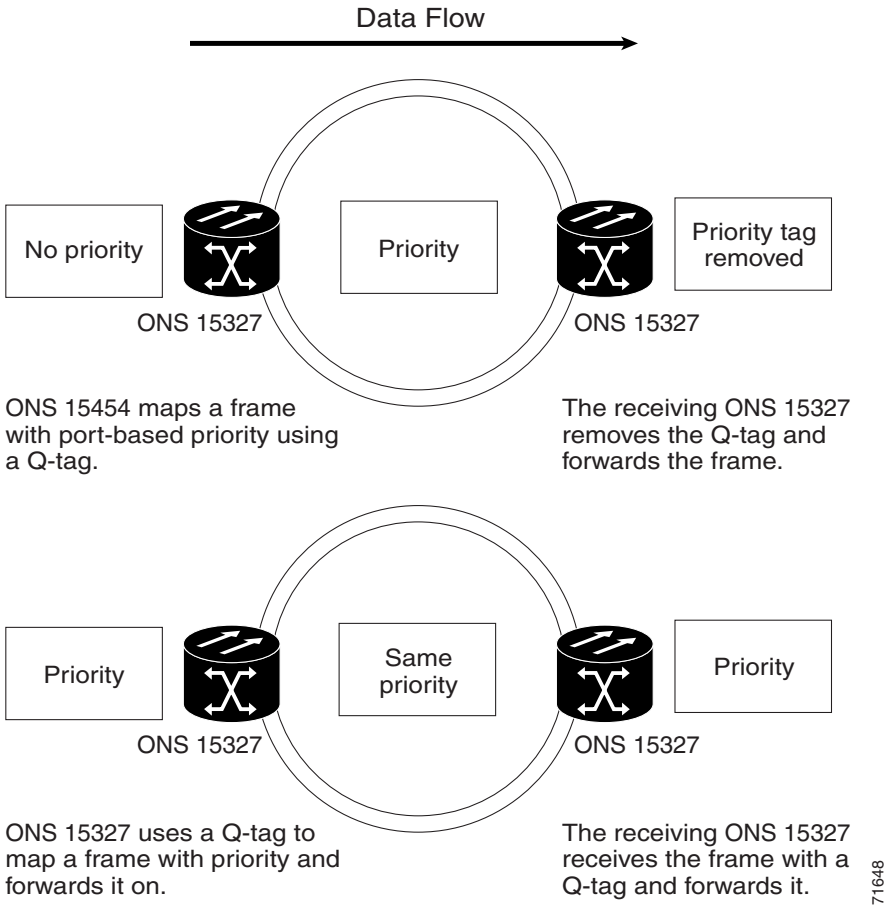
Note E-Series cards in port-mapped mode and G-Series cards do not support priority queuing (IEEE 8021.Q).

Table 10-1 E-Series Card User Priority Queuing

User Priority	Queue	Allocated Bandwidth
0, 1, 2, 3	Low	30%
4, 5, 6, 7	High	70%

Figure 10-9 shows the E-Series priority queuing process.

Figure 10-9 E-Series Priority Queuing Process



10.2.6 E-Series Spanning Tree (IEEE 802.1D)

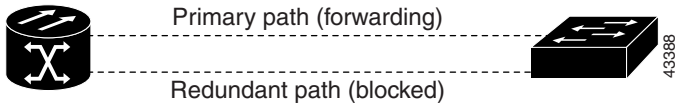
The Cisco ONS 15327 operates spanning tree protocol (STP) according to IEEE 802.1D, when an Ethernet card is installed. The E-Series card supports common STPs on a per circuit basis up to a total of eight STP instances. It does not support per-VLAN STP. In single-card mode, STP can be disabled or enabled on a per circuit basis during circuit creation. Disabling STP will preserve the number of available STP instances.

STP operates over all packet-switched ports including Ethernet and OC-N ports. On Ethernet ports, STP is enabled by default but may be disabled. A user can also disable or enable STP on a circuit-by-circuit basis on unstitched Ethernet cards in a point-to-point configuration. However, turning off STP protection on a circuit-by-circuit basis means that the ONS 15327 system is not protecting the Ethernet traffic on this circuit, and the Ethernet traffic must be protected by another mechanism in the Ethernet network. On OC-N interface ports, the ONS 15327 activates STP by default, and STP cannot be disabled.

The Ethernet card can enable STP on the Ethernet ports to create redundant paths to the attached Ethernet equipment. STP connects cards so that both equipment and facilities are protected against failure.

STP detects and eliminates network loops. When STP detects multiple paths between any two network hosts, STP blocks ports until only one path exists between any two network hosts (Figure 10-10). The single path eliminates possible bridge loops. This is crucial for shared packet rings, which naturally include a loop.

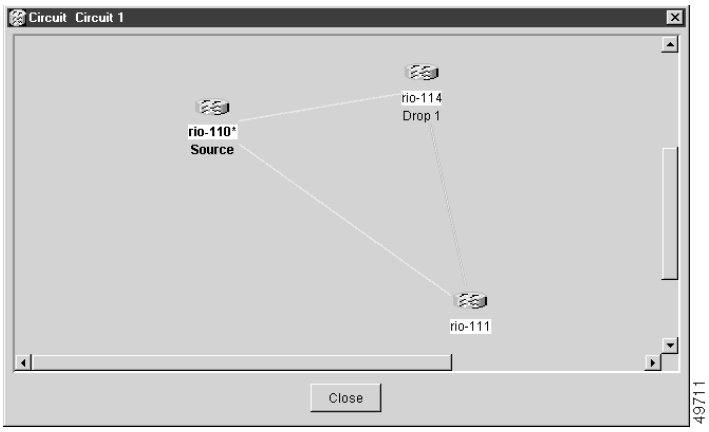
Figure 10-10 STP Blocked Path



To remove loops, STP defines a tree that spans all the switches in an extended network. STP forces certain redundant data paths into a standby (blocked) state. If one network segment in the STP becomes unreachable, the STP algorithm reconfigures the STP topology and reactivates the blocked path to reestablish the link. STP operation is transparent to end stations, which do not discriminate between connections to a single LAN segment or to a switched LAN with multiple segments. The ONS 15327 supports one STP instance per circuit and a maximum of eight STP instances per ONS 15327.

The Circuit window shows forwarding spans and blocked spans on the spanning tree map (see Figure 10-11 on page 10-12).

Figure 10-11 Spanning Tree Map on the Circuit Window



Note Green represents forwarding spans and purple represents blocked (protect) spans. If you have a packet ring configuration, at least one span should be purple.

Caution Multiple circuits with STP protection enabled will incur blocking, if the circuits traverse a common card and uses the same VLAN.

Note E-Series Port-mapped mode does not support STP (IEEE 8021.D).

10.2.6.1 E-Series Multi-Instance Spanning Tree and VLANs

The ONS 15327 can operate multiple instances of STP to support VLANs in a looped topology. You can dedicate separate circuits across the SONET ring for different VLAN groups. Each circuit runs its own STP to maintain VLAN connectivity in a multiring environment.

10.2.6.2 Spanning Tree on a Circuit-by-Circuit Basis

You can also disable or enable STP on a circuit-by-circuit basis on single-card Etherswitch E-Series cards in a point-to-point configuration. This feature allows customers to mix spanning tree protected circuits with unprotected circuits on the same card. It also allows two single-card Etherswitch E-Series cards on the same node to form an intranode circuit.

10.2.6.3 E-Series Spanning Tree Parameters

Default STP parameters on Table 10-2 on page 10-13 are appropriate for most situations. Contact the Cisco Technical Assistance before you change the default STP parameters. See the "Obtaining Technical Assistance" section on page xxi for TAC contact information.

Table 10-2 Spanning Tree Parameters

Parameter	Description
BridgeID	ONS 15327 unique identifier that transmits the configuration bridge protocol data unit (BPDU); the bridge ID is a combination of the bridge priority and the ONS 15327 MAC address
TopoAge	Amount of time in seconds since the last topology change
TopoChanges	Number of times the STP topology has been changed since the node booted up
DesignatedRoot	Identifies the STP designated root for a particular STP instance
RootCost	Identifies the total path cost to the designated root
RootPort	Port used to reach the root
MaxAge	Maximum time that received-protocol information is retained before it is discarded
HelloTime	Time interval, in seconds, between the transmission of configuration BPDUs by a bridge that is the spanning tree root or is attempting to become the spanning tree root
HoldTime	Minimum time period, in seconds, that elapses during the transmission of configuration information on a given port
ForwardDelay	Time spent by a port in the listening state and the learning state

10.2.6.4 E-Series Spanning Tree Configuration

To view the spanning tree configuration (see Table 10-3), at the node view click the Provisioning > Etherbridge > Spanning Trees tabs.

Table 10-3 Spanning Tree Configuration

Column	Default Value	Value Range
Priority	32768	0 to 65535
Bridge max age	20 seconds	6 to 40 seconds
Bridge Hello Time	2 seconds	1 to 10 seconds
Bridge Forward Delay	15 seconds	4 to 30 seconds

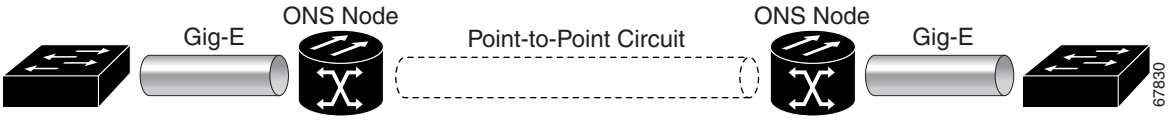
10.3 G-Series Circuit Configurations

This section explains G-Series point-to-point circuits and manual cross-connects. Ethernet manual cross-connects allow you to cross connect individual Ethernet circuits to an STS channel on the ONS 15327 optical interface and also to bridge non-ONS SONET network segments.

10.3.1 G-Series Point-to-Point Ethernet Circuits

G-Series cards support point-to-point circuit configurations (see Figure 10-12 on page 10-14). Provisionable circuit sizes are STS-1, STS-3c, STS-6c, STS-9c, STS-12c, STS-24c, and STS-48c. Each Ethernet port maps to a unique STS circuit of the G-Series card.

Figure 10-12 G-Series Point-to-Point Circuit



The G-Series supports any combination of up to four circuits from the list of valid circuit sizes; however, the circuit sizes can add up to no more than 48 STSs.

Caution G-Series cards do not connect with E-Series cards.

Note The G-Series uses STS cross-connects only. No VT level cross-connects are used.

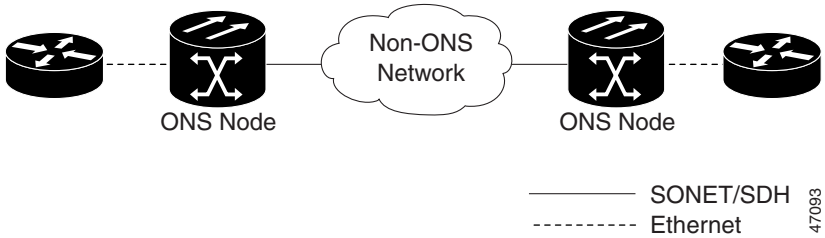
Note All SONET side STS circuits must be adjacent to one another.

10.3.2 G-Series Manual Cross-Connects

ONS 15327s require end-to-end CTC visibility between nodes for normal provisioning of Ethernet circuits. When other vendors' equipment sits between ONS 15327s, OSI/TARP-based equipment does not allow tunneling of the ONS 15327 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit must be manually cross connected to an STS channel using the non-ONS network. Manual cross-connects allows an Ethernet circuit to run from ONS node to ONS node while utilizing the non-ONS network (see Figure 10-13).

Note In this chapter, "cross-connect" and "circuit" have the following meanings: Cross-connect refers to the connections that occur within a single ONS 15327 to allow a circuit to enter and exit an ONS 15327. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15327 network) to the drop or destination (where traffic exits an ONS 15327 network).

Figure 10-13 G-Series Manual Cross-Connects



10.4 E-Series Circuit Configurations

Ethernet circuits can link ONS nodes through point-to-point (straight), shared packet ring, or hub and spoke configurations. Two nodes usually connect with a point-to-point configuration. More than two nodes usually connect with a shared packet ring configuration or a hub-and-spoke configuration. Ethernet manual cross-connects allow you to cross connect individual Ethernet circuits to an STS channel on the ONS 15327 optical interface and also to bridge non-ONS SONET network segments. For step-by-step procedures to configure E-Series circuits, refer to the *Cisco ONS 15327 Procedure Guide*.

Note Before making Ethernet connections, choose an STS-1, STS-3c, STS-6c, or STS-12c circuit size.

Note To make an STS-6c or STS-12c Ethernet circuit, Ethernet cards must be configured in single-card EtherSwitch or port-mapped mode. Multicard mode does not support STS-6c or STS-12c Ethernet circuits.

10.4.1 ONS 15454 and ONS 15327 Ethernet Circuit Combinations

The following table shows the Ethernet circuit combinations available in ONS 15454 E-Series cards and ONS 15327 E-Series cards.

Table 10-4 ONS 15454 and ONS 15327 Ethernet Circuit Combinations

15327 Single-Card	15327 Port-mapped	15327 Multicard	15454 E-Series Single-Card	15454 E-Series Port-Mapped	15454 E-Series Multicard
six STS-1s	six STS-1s	three STS-1s	one STS 12c	one STS 12c	six STS-1s
two STS 3cs	two STS 3cs	one STS 3c	two STS 6cs	two STS 6cs	two STS 3cs
one STS 6c	one STS 6c		one STS 6c and two STS 3cs	one STS 6c and two STS 3cs	one STS 6c
one STS 12c	one STS 12c		one STS 6c and six STS-1s	one STS 6c and six STS-1s	
			four STS 3cs	four STS 3cs	
			two STS 3cs and six STS-1s	two STS 3cs and six STS-1s	
			twelve STS-1s	twelve STS-1s	

10.4.2 E-Series Point-to-Point Ethernet Circuits

The ONS 15327 can set up a point-to-point (straight) Ethernet circuit as Single-card, Port-mapped or Multicard circuit. Multicard EtherSwitch limits bandwidth to STS-3c of bandwidth between two Ethernet circuit points, but allows adding nodes and cards and making a shared packet ring (see Figure 10-14 on page 10-16). Single-card EtherSwitch and Port-mapped mode allows a full STS-12c of bandwidth between two Ethernet circuit endpoints (see Figure 10-15 on page 10-16).

Figure 10-14 Multicard EtherSwitch Point-to-point Circuit

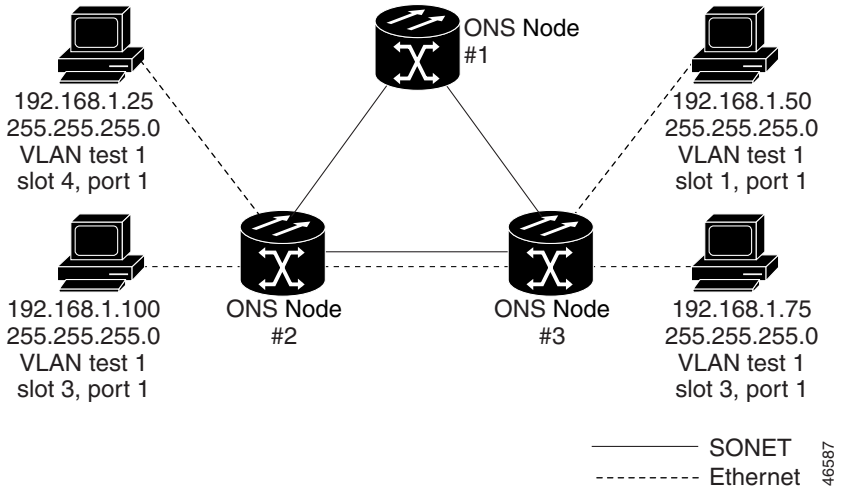
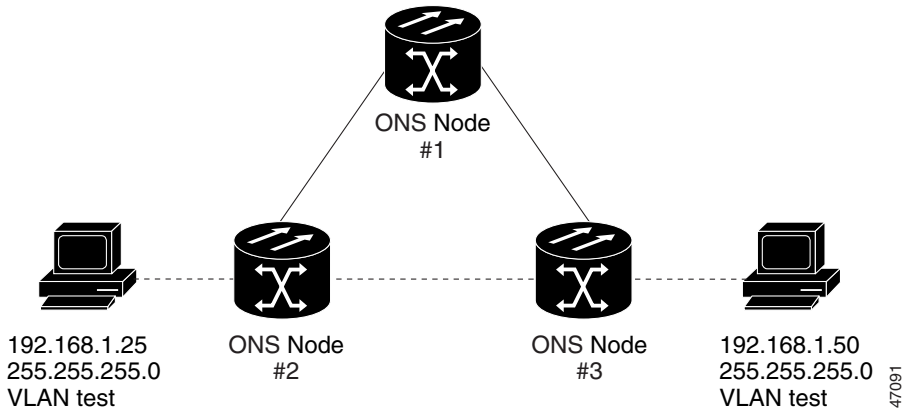


Figure 10-15 Single-card EtherSwitch or Port-mapped Point-to-point Circuit

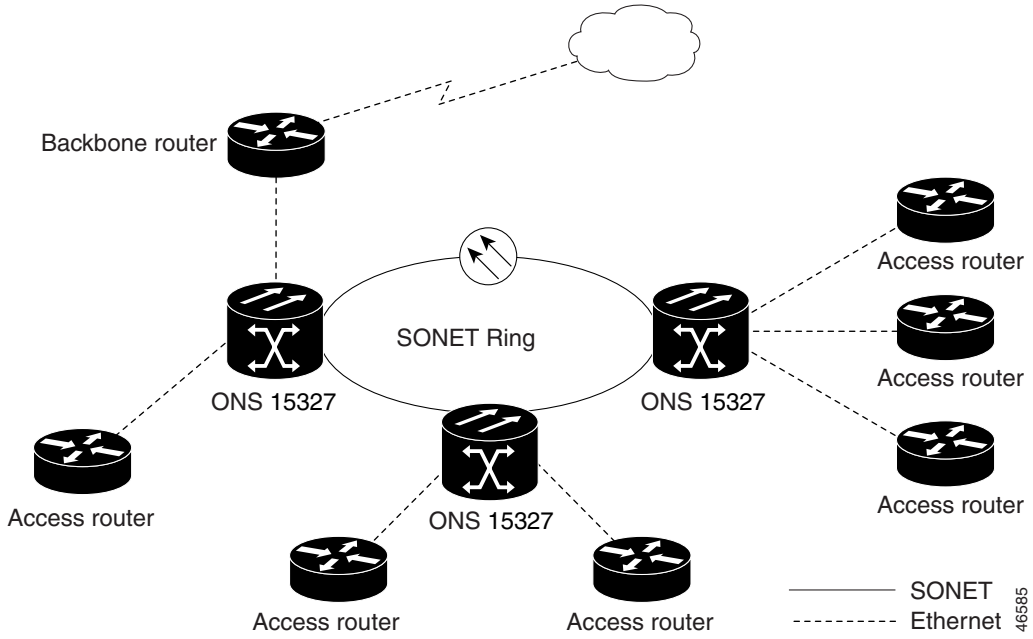


Note A Port-mapped point-to-point circuit does not contain a VLAN.

10.4.3 E-Series Shared Packet Ring Ethernet Circuits

A shared packet ring allows additional nodes, besides the source and destination nodes, access to an Ethernet STS circuit. The E-Series card ports on the additional nodes can share the circuit's VLAN and bandwidth. Figure 10-16 on page 10-17 illustrates a shared packet ring. Your network architecture may differ from the example.

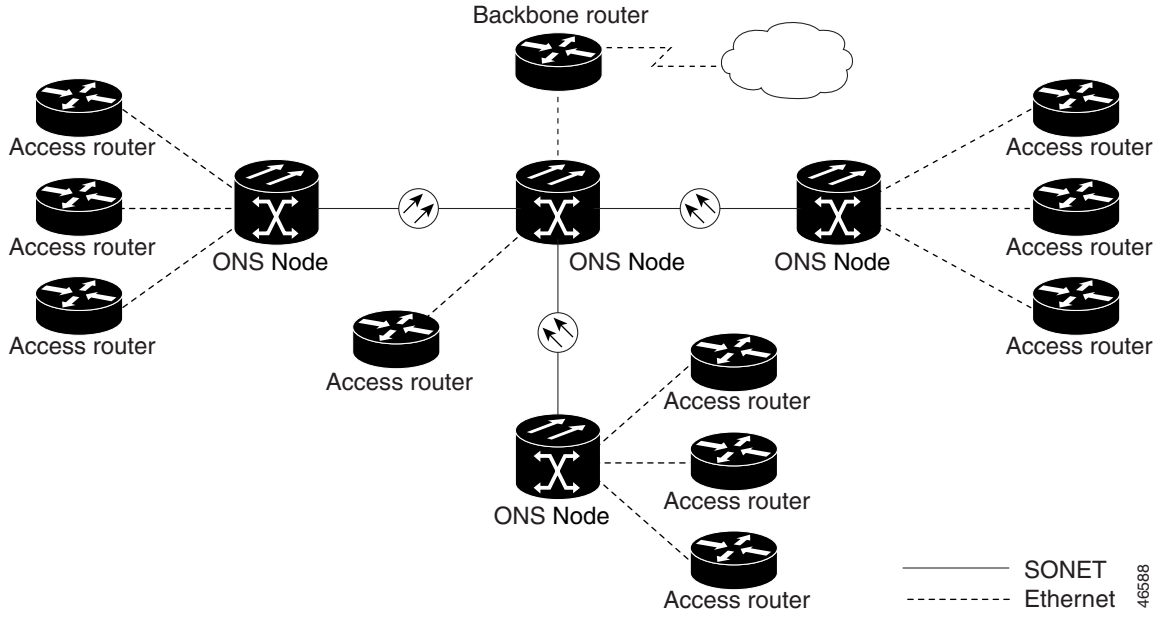
Figure 10-16 Shared Packet Ring Ethernet Circuit



10.4.4 E-Series Hub and Spoke Ethernet Circuit Provisioning

The hub and spoke configuration connects point-to-point circuits (the spokes) to an aggregation point (the hub). In many cases, the hub links to a high-speed connection and the spokes are Ethernet cards. Figure 10-17 on page 10-18 illustrates a hub and spoke ring. Your network architecture may differ from the example.

Figure 10-17 Hub And Spoke Ethernet Circuit



10.4.5 E-Series Ethernet Manual Cross-Connects

ONS 15327s require end-to-end CTC visibility between nodes for normal provisioning of Ethernet circuits. When other vendors' equipment sits between ONS 15327s, OSI/TARP-based equipment does not allow tunneling of the ONS 15327 TCP/IP-based DCC. To circumvent this lack of continuous DCC, the Ethernet circuit must be manually cross connected to an STS channel using the non-ONS network. The manual cross-connect allows an Ethernet circuit to run from ONS node to ONS node utilizing the non-ONS network.

Note In this chapter, "cross-connect" and "circuit" have the following meanings: Cross-connect refers to the connections that occur within a single ONS 15327 to allow a circuit to enter and exit an ONS 15327. Circuit refers to the series of connections from a traffic source (where traffic enters the ONS 15327 network) to the drop or destination (where traffic exits an ONS 15327 network).

10.5 Remote Monitoring Specification Alarm Thresholds

The ONS 15327 features Remote Monitoring (RMON) that allows network operators to monitor the health of the network with a Network Management System (NMS).

One of the ONS 15327's RMON MIBs is the Alarm group, which consists of the alarmTable. An NMS uses the alarmTable to find the alarm-causing thresholds for network performance. The thresholds apply to the current 15-minute interval and the current 24-hour interval. RMON monitors several variables, such as Ethernet collisions, and triggers an event when the variable crosses a threshold during that time interval. For example, if a threshold is set at 1000 collisions and 1001 collisions occur during the 15-minute interval, an event triggers. CTC allows you to provision these thresholds for Ethernet statistics.

Note Table 10-5 defines the variables you can provision in CTC. For example, to set the collision threshold, choose etherStatsCollisions from the Variable menu.

Table 10-5 Ethernet Threshold Variables (MIBs)

Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInMulticastPkts	Number of multicast frames received error free (not supported by E-Series)
ifInBroadcastPkts	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer (not supported by E-Series)
ifInDiscards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol (not supported by E-Series)
iflnErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
ifOutMulticastPkts	Number of multicast frames transmitted error free (not supported by E-Series)
ifOutBroadcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent (not supported by E-Series)
ifOutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted (not supported by E-Series)
dot3statsAlignmentErrors	Number of frames with an alignment error, that is, the length is not an integral number of octets and the frame cannot pass the Frame Check Sequence (FCS) test
dot3StatsFCSErrors	Number of frames with framecheck errors, that is, there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrame	Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	Number of times the first transmission was delayed because the medium was busy

Table 10-5 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
dot3StatsExcessiveCollision	Number of frames where transmissions failed because of excessive collisions
dot3StatsLateCollision	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsFrameTooLong	Number of received frames that were larger than the maximum size permitted
dot3StatsCarrierSenseErrors	The number of transmission errors on a particular interface that are not otherwise counted (not supported by E-Series)
dot3StatsSQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface (not supported by E-Series)
etherStatsJabbers	Total number of Octets of data (including bad packets) received on the network
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets)
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 to 172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 to 255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 to 511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 to 1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 to 1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length

Table 10-5 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
receivePauseFrames	The number of received 802.x pause frames (not supported by E-Series)
transmitPauseFrames	The number of transmitted 802.x pause frames (not supported by E-Series)
receivePktsDroppedInternalCongestion	The number of received frames dropped because of frame buffer overflow and other reasons (not supported by E-Series)
transmitPktsDroppedInternalCongestion	The number of frames dropped in the transmit direction because of frame buffer overflow and other reasons (not supported by E-Series)
txTotalPkts	Total number of transmit packets (not supported by E-Series)
rxTotalPkts	Total number of receive packets (not supported by E-Series)

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15327. For SNMP set up information, refer to the *Cisco ONS 15327 Procedure Guide*.

Chapter topics include:

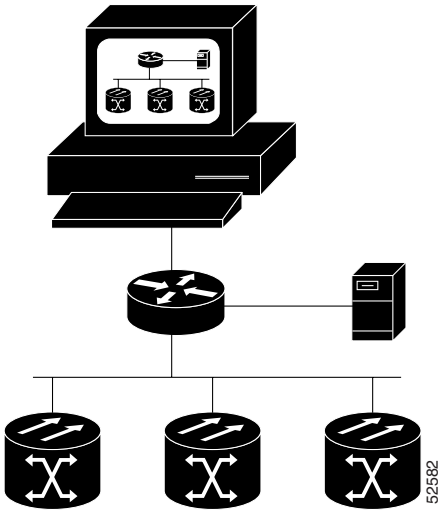
11.1 SNMP Overview

SNMP is an application-layer communication protocol that allows network devices to exchange management information. SNMP enables network administrators to manage network performance, find and solve network problems, and plan network growth.

The ONS 15327 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 DS-1, DS-3, SONET, and Ethernet technologies. SNMP allows limited management of the ONS 15327 by a generic SNMP manager, for example HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert.

The Cisco ONS 15327 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both versions share many features, but SNMPv2c includes additional protocol operations. This chapter describes both versions and explains how to configure SNMP on the ONS 15327. Figure 11-1 on page 11-2 illustrates a basic network managed by SNMP.

Figure 11-1 Basic Network Managed by SNMP

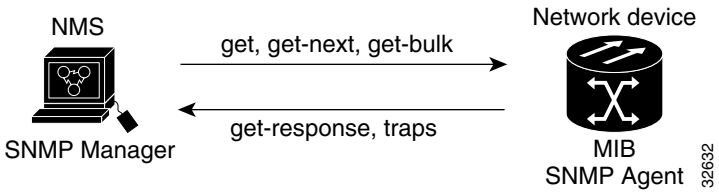


11.2 SNMP Basic Components

An SNMP-managed network consists of three primary components: managed devices, agents, and management systems. A managed device is a network node that contains an SNMP agent and resides on an SNMP-managed network. Managed devices collect and store management information and use SNMP to make this information available to management systems that use SNMP. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and network elements such as an ONS 15327.

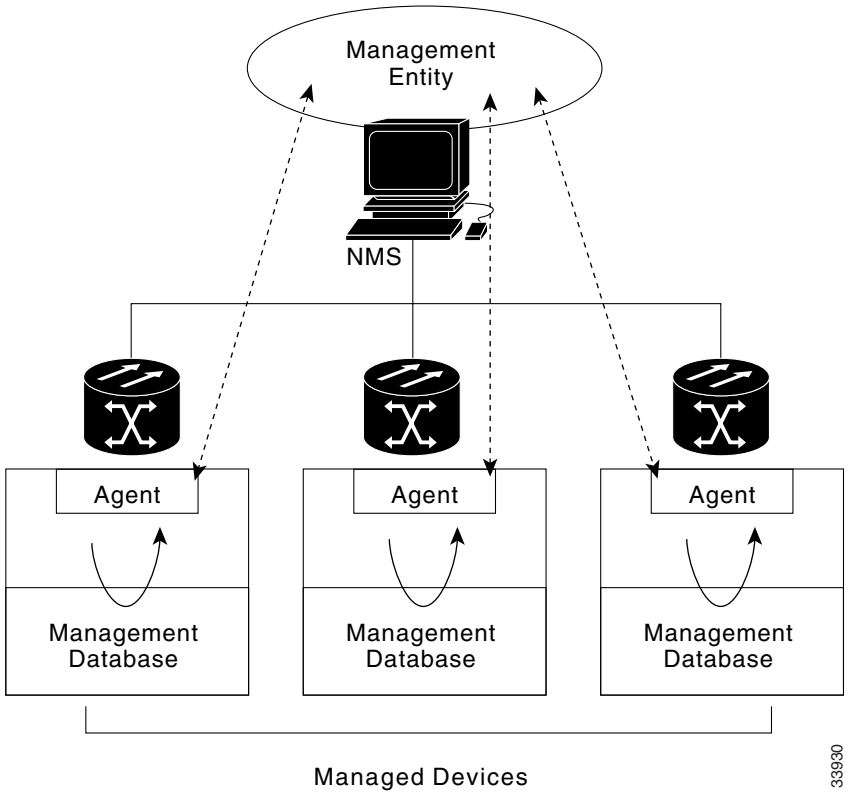
An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the MIB, which is the repository for device parameter and network data. The agent can also send traps, which are notifications of certain events (such as changes), to the manager. Figure 11-2 illustrates these SNMP operations.

Figure 11-2 SNMP Agent Gathering Data from an MIB and Sending Traps to the Manager



A management system such as HP OpenView executes applications that monitor and control managed devices. Management systems provide the bulk of the processing and memory resources required for network management. One or more management systems must exist on any managed network. Figure 11-3 on page 11-3 illustrates the relationship between the three key SNMP components.

Figure 11-3 Example of the Primary SNMP Components



11.3 SNMP Support

The ONS 15327 supports SNMP v1 and v2c traps and get requests. The SNMP MIBs in the ONS 15327 define alarms, traps, and status. Through SNMP, NMS applications can query a management agent using a supported MIB. The functional entities include Ethernet switches and SONET multiplexers. Refer to the *Cisco ONS 15327 Procedure Guide* for procedures to set up or change SNMP settings.

11.4 SNMP Management Information Bases

A MIB is a hierarchically organized collection of information. It consists of managed objects and is identified by object identifiers. Network-management protocols, such as SNMP, are able to access to MIBs. The ONS 15327 SNMP agent communicates with an SNMP management application using SNMP messages. Table 11-1 on page 11-4 describes these messages.

Table 11-1 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	The reply to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Similar to a get-next-request, but this operation fills the get-response with up to the max-repetition number of get-next interactions.
set-request	Set-request processing is enabled to provide remote network monitoring (RMON) MIB.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that an event has occurred.

A managed object (sometimes called a MIB object) is one of any specific characteristics of a managed device. Managed objects consist of one or more object instances (variables). Table 11-3 lists the IETF standard MIBs implemented in the ONS 15327 SNMP Agent.

The ONS 15327 MIBs in Table 11-2 are included on the software CD that ships with the ONS 15327. Compile these MIBs in the following order. If you do not follow the order, one or more MIB files might not compile. If you cannot compile the ONS 15327 MIBs, contact the Technical Assistance Center (TAC). See the "Obtaining Technical Assistance" section on page xxi.

Table 11-2 ONS 15327 Proprietary MIBs

MIB#	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-454.mib (for ONS 15454 only)
4	CERENT-GENERIC.mib (for ONS 15327 only)

Table 11-3 lists the IETF standard MIBs implemented in the ONS 15327.

Table 11-3 IETF Standard MIBs Implemented in the ONS 15327 SNMP Agent

RFC#	Module Name	Title/Comments
—	IANAifType-MIB.mib	Internet Assigned Numbers Authority (IANA) ifType
1213 1907	RFC1213-MIB-rfc1213.mib, SNMPV2-MIB-rfc1907.mib	Management Information Base for Network Management of TCP/IP-based internets: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1253	RFC1253-MIB-rfc1253.mib	Open Shortest Path First (OSPF) Version 2 Management Information Base

Table 11-3 IETF Standard MIBs Implemented in the ONS 15327 SNMP Agent (continued)

RFC#	Module Name	Title/Comments
1493	BRIDGE-MIB-rfc1493.mib	Definitions of Managed Objects for Bridges This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network (LAN) segments.
1757	RMON-MIB-rfc1757.mib	Remote Network Monitoring Management Information Base
2737	ENTITY-MIB-rfc2737.mib	Entity MIB (Version 2)
2233	IF-MIB-rfc2233.mib	The Interfaces Group MIB using SMIv2
2358	EtherLike-MIB-rfc2358.mib	Definitions of Managed Objects for the Ethernet-like Interface Types
2493	PerfHist-TC-MIB-rfc2493.mib	Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
2495	DS1-MIB-rfc2495.mib	Definitions of Managed Objects for the DS-1, E-1, DS-2 and E-2 Interface Types
2496	DS3-MIB-rfc2496.mib	Definitions of Managed Object for the DS-3/E-3 Interface Type
2558	SONET-MIB-rfc2558.mib	Definitions of Managed Objects for the SONET/SDH Interface Type
2674	P-BRIDGE-MIB-rfc2674.mib Q-BRIDGE-MIB-rfc2674.mib	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions

11.5 SNMP Traps

The ONS 15327 can receive SNMP requests from a number of SNMP managers and send traps to eleven trap receivers. The ONS 15327 generates all alarms and events as SNMP traps.

The ONS 15327 generates traps containing an object ID that uniquely identifies the alarm. An entity identifier uniquely identifies the entity that generated the alarm (slot, port, STS, VT, BLSR, STP, etc.). The traps give the severity of the alarm (critical, major, minor, event, etc.) and indicate whether the alarm is service affecting or non-service affecting. The traps also contain a date/time stamp that shows the date and time the alarm occurred. The ONS 15327 also generates a trap for each alarm when the alarm condition clears.

Each SNMP trap contains eleven variable bindings listed in Table 11-4.

Table 11-4 SNMP Trap Variable Bindings for ONS 15454

Number	Name	Description
1	sysUpTime	The first variable binding in the variable binding list of an SNMPv2-Trap-PDU.
2	snmpTrapOID	The second variable binding in the variable binding list of an SNMPv2-Trap-PDU.
3	cerentNodeTime	This variable gives the time that an event occurred.

Table 11-4 SNMP Trap Variable Bindings for ONS 15454 (continued)

Number	Name	Description
4	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.
5	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.
6	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.
7	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.
8	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.
9	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.
10	cerent454AlarmObjectName	This variable gives the TL1-style user-visible name which uniquely identifies an object in the system.

Table 11-5 lists the variable bindings for the ONS 15327.

Table 11-5 SNMP Trap Variable Bindings Used in ONS 15327

Number	Name	Description
1	sysUpTime	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	snmpTrapID	This variable uniquely identifies each entry in an alarm table. When an alarm in the alarm table clears, the alarm indexes change for each alarm located subsequent to the cleared alarm.
3	cerentNodeTime	This variable gives the time that an event occurred.
4	cerentGenericAlarmState	This variable specifies alarm severity and service-affecting status. Severities are minor, major and critical. Service- affecting statuses are service-affecting and non-service affecting.

Table 11-5 SNMP Trap Variable Bindings Used in ONS 15327 (continued)

Number	Name	Description
5	cerentGenericAlarmObjectType	This variable provides the entity type that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
6	cerentGenericAlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of the objects in each table; if the alarm is interface related, this is the index of the interfaces in the interface table.
7	cerentGenericAlarmSlotNumber	This variable indicates the slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
8	cerentGenericAlarmPortNumber	This variable provides the port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
9	cerentGenericAlarmLineNumber	This variable provides the object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
10	cerentGenericAlarmObjectName	This variable gives the TL1-style user-visible name which uniquely identifies an object in the system.

The ONS 15327 supports the generic and IETF traps listed in Table 11-6.

Table 11-6 IETF Traps Supported in the ONS 15327

Trap	From RFC# MIB	Description
coldStart	RFC1907-MIB	Agent up, cold start
warmStart	RFC1907-MIB	Agent up, warm start
authenticationFailure	RFC1907-MIB	Community string does not match
newRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree
topologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking
entConfigChange	RFC2737/ ENTITY-MIB	The entLastChangeTime value has changed
dsx1LineStatusChange	RFC2495/ DS1-MIB	A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (such as, DS-3), no traps for the DS-1 are sent.

Table 11-6 IETF Traps Supported in the ONS 15327 (continued)

Trap	From RFC# MIB	Description
dsx3LineStatusChange	RFC2496/ DS3-MIB	A dsx3LineStatusLastChange trap is sent when the value of an instance of dsx3LineStatus changes. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (such as, DS-1), no traps for the lower level are sent.
risingAlarm	RFC1757/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC1757/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

11.6 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination dialog box in CTC. In effect, SNMP considers any request valid that uses a community name matching a community name on the list of provisioned SNMP trap destinations. Otherwise, SNMP considers the request invalid and drops it.

If an SNMP request contains an invalid community name, the request silently drops and the MIB variable (snmpInBadCommunityNames) increments. All MIB variables managed by the agent grant access to all SNMP requests containing a validated community name.

11.7 SNMP Remote Network Monitoring

The ONS 15327 incorporates RMON to allow network operators to monitor the ONS 15327 Ethernet cards. This feature is not apparent to the typical CTC user, because RMON interoperates with an NMS. However, with CTC you can provision the RMON alarm thresholds. For the procedure, see the *Cisco ONS 15327 Procedure Guide*. CTC also monitors the five RMON groups implemented by the ONS 15327.

ONS 15327 RMON implementation is based on the IETF-standard MIB Request for Comment (RFC)1757. The ONS 15327 implements five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

11.7.1 Ethernet Statistics Group

The Ethernet Statistics group contains the basic statistics for each monitored subnetwork in a single table named etherstats.

11.7.2 History Control Group

The History Control group defines sampling functions for one or more monitor interfaces. RFC 1757 defines the historyControlTable.

11.7.3 Ethernet History Group

The ONS 15327 implements the etherHistoryTable as defined in RFC 1757, within the bounds of the historyControlTable.

11.7.4 Alarm Group

The Alarm group consists of a single alarm table. This table provides the network performance alarm thresholds for the network management application. With CTC, you can provision the thresholds in the table.

11.7.5 Event Group

The Event group consists of two tables, eventTable and logTable. The eventTable is read-only. The ONS 15327 implements the logTable as specified in RFC 1757.

Regulatory and Compliance Requirements

This appendix lists customer, industry, and government requirements met by the Cisco ONS 15327. Installation warnings are also included.

A.1 Regulatory Compliance

Table A-1 Standards

Discipline	Country	Specification
EMC Emissions (Class A)	Canada	ICES-003 Issue 3, 1997 Telcordia GR-1089-CORE
	USA	Telcordia GR-1089-CORE 47CFR15
	Japan	VCCI V3/2000.04
	Korea	CISPR22
	Mexico	EN55022
	Europe	EN 300-386-TC
EMC Immunity	Canada	Telcordia GR-1089-CORE
	USA	Telcordia GR-1089-CORE
	Japan	Not Applicable
	Korea	CISPR24
	Europe	EN50082-2, EN 300-386-TC
	Mexico	EN55024

Table A-1 Standards (continued)

Discipline	Country	Specification
Safety	Canada	CAN/CSA-C22.2 No. 950-95, 3rd Ed. Telcordia GR-1089-CORE Telcordia GR-63-CORE
	USA	UL 1950, 3rd Ed. Telcordia GR-1089-CORE Telcordia GR-63-CORE
	Europe	IEC60950/EN60950, 3rd Ed.
	Japan	EN60950 (to A4)
	Korea	EN60950 (to A4)
	Mexico	Certified
Telecommunications	Japan	Blue Book 1996, Green Book 1997
	Canada	Not Applicable
	USA	Not Applicable
	Europe	No requirement
	Korea	OC12, OC48
	Mexico	Certified
Environmental	Canada	Telcordia GR-63-CORE NEBS
	USA	Cisco Mechanical Environmental Design and Qualification Guideline ENG-3396
Structural Dynamics (Mechanical)	Canada	Telcordia GR-63-CORE NEBS
	USA	Cisco Mechanical Environmental Design and Qualification Guideline ENG-3396
		AT&T Network Equipment Development Standards (NEDS)
Power & Grounding	Global	SBC Local Exchange Carriers, Network Equipment Power, Grounding, Environmental, and Physical Design Requirements, TP76200MP

A.2 Japanese Approvals

Table A-2 Card Approvals

Card	Certificate Number
MIC-28-3-A/B	L01-0055
OC12 IR 1310	L01-0052
OC48 IR 1310	L01-0053

A.2.1 Label Information

The following labels are applicable for use in Japan.

Figure A-1 Optical Card OC3 IR 4 1310

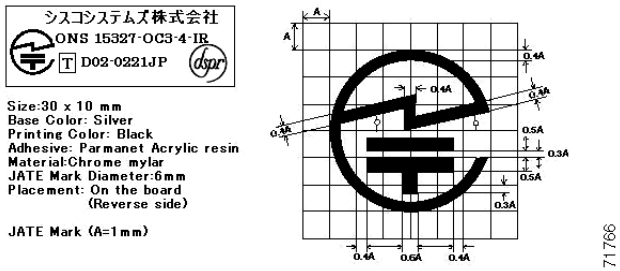


Figure A-2 Optical Card OC12 IR 1310

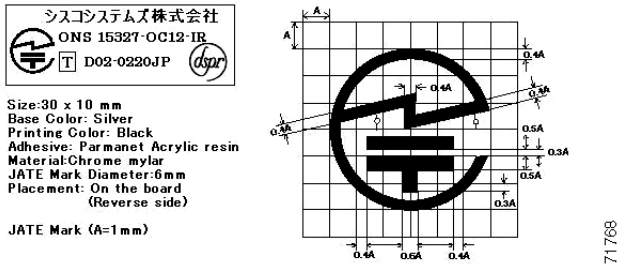


Figure A-3 Optical Card OC12 LR 1550

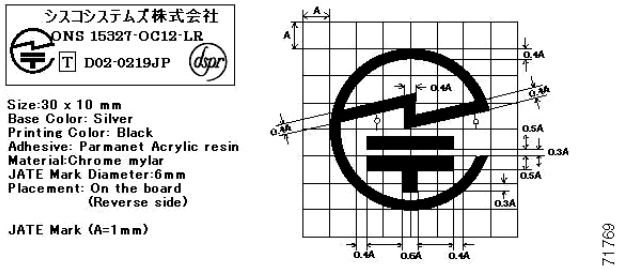


Figure A-4 Optical Card OC48 IR 1310

Figure A-5 Optical Card OC48 LR 1550

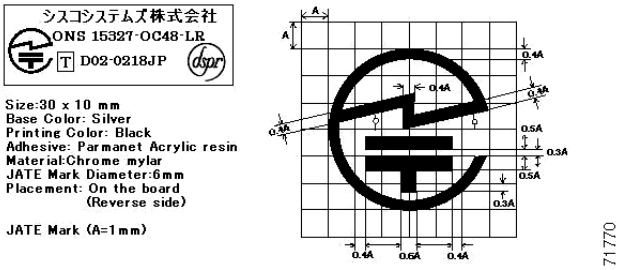


Figure A-6 Gigabit Ethernet Card G1000-2

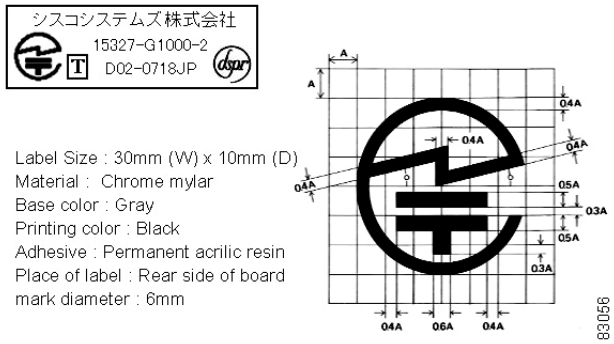
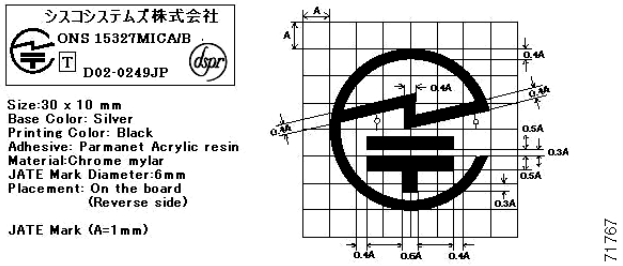


Figure A-7 Mechanical Interface Card (MIC) (DS-1, DS-3) MIC-28-3-A/B



A.3 Korean Approvals and Labels

Table A-3 Certification of Information and Communication Equipment

Model	Certificate Number
ONS 15327	T-C99-01-0266
Cards	
OC12-IR-1310	
OC48-IR-1310	
XTC-14	
MIC-28-3	
E10/100-4	

Figure A-8 Korean Label

A.3.1 Class A Notice

Warning **This is a Class A Information Product. When used in residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.**

주의 這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，
在這種情況下，使用者會被要求採取某些適當的對策。

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

A.4 Installation Warnings

Install the ONS 15327 in compliance with your local and national electrical codes:

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

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

Waarschuwing **Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.**

Varoitus **Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.**

Attention **Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.**

Warnung **Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.**

Avvertenza **Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.**

Advarsel **Les installasjonsinstruksjonene før systemet kobles til strømkilden.**

Aviso **Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.**

¡Advertencia! **Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.**

Varning! **Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.**

警告 システムを電源に接続する前に、インストレーションについての説明書を必ずお読みください。

A.4.1 DC Power Disconnection Warning

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

Waarschuwing **Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.**

Varoitus **Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.**

Attention **Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.**

Warnung **Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.**

Avvertenza **Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata (OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.**

Advarsel **Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.**

Aviso **Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.**

¡Advertencia! **Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).**

Varning! **Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.**

A.4.2 DC Power Connection Warning

Warning **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.**

Waarschuwing **Nadat de bedrading van de gelijkstroom voeding aangebracht is, verwijdert u het plakband van de schakelaarhendel van de stroomverbreker en schakelt de stroom weer in door de hendel van de stroomverbreker naar de AAN positie te draaien.**

Varoitus **Yhdistettyäsi tasavirtalähteen johdon avulla poista teippi suojakytkimen varresta ja kytke virta uudestaan kääntämällä suojakytkimen varsi KYTKETTY-asentoon.**

Attention **Une fois l'alimentation connectée, retirer le ruban adhésif servant à bloquer la poignée du disjoncteur et rétablir l'alimentation en plaçant cette poignée en position de marche (ON).**

Warnung **Nach Verdrahtung des Gleichstrom-Netzgeräts entfernen Sie das Klebeband vom Schaltergriff des Unterbrechers und schalten den Strom erneut ein, indem Sie den Griff des Unterbrechers auf EIN stellen.**

Avvertenza **Dopo aver eseguito il cablaggio dell'alimentatore CC, togliere il nastro adesivo dall'interruttore automatico e ristabilire l'alimentazione spostando all'interruttore automatico in posizione ON.**

Advarsel **Etter at likestrømsenheten er tilkoblet, fjernes teipen fra håndtaket på strømbryteren, og deretter aktiveres strømmen ved å dreie håndtaket på strømbryteren til PÅ-stilling.**

Aviso **Depois de ligar o sistema de fornecimento de corrente contínua, retire a fita isoladora da manivela do disjuntor, e volte a ligar a corrente ao deslocar a manivela para a posição ON (Ligado).**

¡Advertencia! **Después de cablear la fuente de alimentación de corriente continua, retirar la cinta de la palanca del interruptor automático, y restablecer la alimentación cambiando la palanca a la posición de Encendido (ON).**

Varning! **När du har kopplat ledningarna till strömförsörjningsenheten för inmatad likström tar du bort tejpen från överspänningsskyddets omkopplare och slår på strömmen igen genom att ställa överspänningsskyddets omkopplare i TILL-läget.**

A.4.3 Power Supply Disconnection Warning

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.**

Waarschuwing **Voordat u aan een frame of in de nabijheid van voedingen werkt, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen; voor gelijkstroom toestellen dient u de stroom uit te schakelen bij de stroomverbreker.**

Varoitus **Kytke irti vaihtovirtalaitteiden virtajohto ja katkaise tasavirtalaitteiden virta suojakytkimellä, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.**

Attention **Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif ; couper l'alimentation des unités en courant continu au niveau du disjoncteur.**

Warnung **Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw. schalten Sie bei Gleichstromeinheiten den Strom am Unterbrecher ab.**

Avvertenza **Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all'interruttore automatico sulle unità CC.**

Advarsel **Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut på vekselstrømsenheter og strømmen kobles fra ved strømbryteren på likestrømsenheter.**

Aviso **Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada; desligue a corrente no disjuntor nas unidades de corrente contínua.**

¡Advertencia! **Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA); cortar la alimentación desde el interruptor automático en los equipos de corriente continua (CC).**

Varning! **Innan du arbetar med ett chassi eller nära strömförsörjningsenheter skall du för växelströmsenheter dra ur nätsladden och för likströmsenheter bryta strömmen vid överspänningsskyddet.**

警告 シャーシの取り扱いや電源まわりの作業を行う前に、AC装置の電源コードを抜いてください。DC装置では遮断器の電源を切り離してください。

A.4.4 Outside Line Connection Warning

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

Waarschuwing **Metaalhoudende interfaces bestemd voor aansluiting op fabrieksleidingen buiten (zoals T1/E1/T3/E3 etc.) dienen aangesloten te worden m.b.v. een geregistreerd of goedgekeurd apparaat zoals CSU/DSU of NT1.**

Varoitus **Laitoksen ulkopuolisten linjojen (T1/E1/T3/E3 jne.) kytkentään tarkoitetut metalliset rajapinnat on kytkettävä rekisteröidyn tai hyväksytyn laitteen, kuten CSU/DSU tai NT1, kautta.**

Attention **Les interfaces métalliques destinées à une connexion à des lignes extérieures au site (par exemple : T1/E1/T3/E3, etc.) doivent être raccordées sur un appareil homologué ou approuvé tel que CSU/DSU ou NT1.**

Warnung **Metallische Schnittstellen für die Verbindung mit Leitungen außerhalb der Anlagen (wie z.B. T1/E1/T3/E3 usw.) müssen durch ein registriertes oder zugelassenes Gerät wie CSU/DSU oder NT1 angeschlossen werden.**

Avvertenza **Le interfacce metalliche per la connessione a linee di impianti esterni (come T1/E1/T3/E3 ecc.) devono essere connesse mediante un dispositivo registrato o approvato, come per esempio CSU/DSU (Channel Service Unit/Data Service Unit) o NT1 (Network Terminator).**

Advarsel **Metallgrensesnitt for kopling til eksterne anleggslinjer (for eksempel T1/E1/T3/E3 osv.) skal koples gjennom en registrert eller godkjent enhet, for eksempel CSU/DSU eller NT1.**

Aviso **As interfaces metálicas para conexão com as linhas externas (como T1/E1/T3/E3 etc) devem ser conectadas através de um dispositivo aprovado ou certificado como CSU/DSU ou NT1.**

¡Advertencia! **Las interfaces metálicas destinadas a las conexiones de líneas exteriores (por ejemplo, T1/E1/T3/E3, etc.) deben conectarse mediante un dispositivo registrado o aprobado como, por ejemplo, CSU/DSU o NT1.**

Varning! **Metallkontakter för anslutning till utomhusledningar (t.ex. T1/E1/T3/E3 m.fl.) måste anslutas via en registrerad eller godkänd enhet, t.ex. CSU/DSU eller NT1.**

A.4.5 Class 1 Laser Product Warning

Warning **Class 1 laser product.**

Waarschuwing **Klasse-1 laser produkt.**

Varoitus **Luokan 1 lasertuote.**

Attention **Produit laser de classe 1.**

Warnung **Laserprodukt der Klasse 1.**

Avvertenza **Prodotto laser di Classe 1.**

Advarsel **Laserprodukt av klasse 1.**

Aviso **Produto laser de classe 1.**

¡Advertencia! **Producto láser Clase I.**

Varning! **Laserprodukt av klass 1.**

警告 第１種レーザー製品

경고 1급 레이저 제품.

A.4.6 Class I and Class 1M Laser Warning

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

Waarschuwing **Laserproducten van Klasse I (21 CFR 1040.10 en 1040.11) en Klasse 1M (IEC 60825-1 2001-01).**

Varoitus **Luokan I (21 CFR 1040.10 ja 1040.11) ja luokan 1M (IEC 60825-1 2001-01) lasertuotteita.**

Attention **Produits laser catégorie I (21 CFR 1040.10 et 1040.11) et catégorie 1M (IEC 60825-1 2001-01).**

Warnung **Laserprodukte der Klasse I (21 CFR 1040.10 und 1040.11) und Klasse 1M (IEC 60825-1 2001-01).**

Avvertenza **Prodotti laser di Classe I (21 CFR 1040.10 e 1040.11) e Classe 1M (IEC 60825-1 2001-01).**

Advarsel **Klasse I (21 CFR 1040.10 og 1040.11) og klasse 1M (IEC 60825-1 2001-01) laserprodukter.**

Aviso **Produtos laser Classe I (21 CFR 1040.10 e 1040.11) e Classe 1M (IEC 60825-1 2001-01).**

¡Advertencia! **Productos láser de Clase I (21 CFR 1040.10 y 1040.11) y Clase 1M (IEC 60825-1 2001-01).**

Varning! **Laserprodukter av Klass I (21 CFR 1040.10 och 1040.11) och Klass 1M (IEC 60825-1 2001-01).**

A.4.7 Restricted Area Warning

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

Waarschuwing **Dit toestel is bedoeld voor installatie op plaatsen met beperkte toegang. Een plaats met beperkte toegang is een plaats waar toegang slechts door servicepersoneel verkregen kan worden door middel van een speciaal instrument, een slot en sleutel, of een ander veiligheidsmiddel, en welke beheerd wordt door de overheidsinstantie die verantwoordelijk is voor de locatie.**

Varoitus **Tämä laite on tarkoitettu asennettavaksi paikkaan, johon pääsy on rajoitettua. Paikka, johon pääsy on rajoitettua, tarkoittaa paikkaa, johon vain huoltohenkilöstö pääsee jonkin erikoistyökalun, lukkoon sopivan avaimen tai jonkin muun turvalaitteen avulla ja joka on paikasta vastuussa olevien toimivaltaisten henkilöiden valvoma.**

Attention **Cet appareil est à installer dans des zones d'accès réservé. Ces dernières sont des zones auxquelles seul le personnel de service peut accéder en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité. L'accès aux zones de sécurité est sous le contrôle de l'autorité responsable de l'emplacement.**

Warnung **Diese Einheit ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Ein Bereich mit beschränktem Zutritt ist ein Bereich, zu dem nur Wartungspersonal mit einem Spezialwerkzeugs, Schloß und Schlüssel oder anderer Sicherheitsvorkehrungen Zugang hat, und der von dem für die Anlage zuständigen Gremium kontrolliert wird.**

Avvertenza **Questa unità deve essere installata in un'area ad accesso limitato. Un'area ad accesso limitato è un'area accessibile solo a personale di assistenza tramite un'attrezzo speciale, lucchetto, o altri dispositivi di sicurezza, ed è controllata dall'autorità responsabile della zona.**

Advarsel **Denne enheten er laget for installasjon i områder med begrenset adgang. Et område med begrenset adgang gir kun adgang til servicepersonale som bruker et spesielt verktøy, lås og nøkkel, eller en annen sikkerhetsanordning, og det kontrolleres av den autoriteten som er ansvarlig for området.**

Aviso **Esta unidade foi concebida para instalação em áreas de acesso restrito. Uma área de acesso restrito é uma área à qual apenas tem acesso o pessoal de serviço autorizado, que possua uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.**

¡Advertencia! **Esta unidad ha sido diseñada para instalarse en áreas de acceso restringido. Área de acceso restringido significa un área a la que solamente tiene acceso el personal de servicio mediante la utilización de una herramienta especial, cerradura con llave, o algún otro medio de seguridad, y que está bajo el control de la autoridad responsable del local.**

Varning! **Denna enhet är avsedd för installation i områden med begränsat tillträde. Ett område med begränsat tillträde får endast tillträdas av servicepersonal med ett speciellt verktyg, lås och nyckel, eller annan säkerhetsanordning, och kontrolleras av den auktoritet som ansvarar för området.**

A.4.8 Ground Connection Warning

Warning **When installing the unit, always make the ground connection first and disconnect it last.**

Waarschuwing **Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.**

Varoitus **Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.**

Attention **Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.**

Warnung **Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.**

Avvertenza **In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.**

Advarsel **Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.**

Aviso **Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.**

¡Advertencia! **Al instalar el equipo, conectar la tierra la primera y desconectarla la última.**

Varning! **Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.**

A.4.9 Qualified Personnel Warning

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

Waarschuwing Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.

Varoitus Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.

Avertissement Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.

Achtung Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.

Avvertenza Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.

Advarsel Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.

Aviso Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.

¡Atención! Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.

Varning! Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.

A.4.10 Invisible Laser Radiation Warning (other versions available)

Warning Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

Waarschuwing Omdat er onzichtbare laserstraling uit de opening van de poort geëmitteerd kan worden wanneer er geen kabel aangesloten is, dient men om blootstelling aan laserstraling te vermijden niet in de open openingen te kijken.

Varoitus Kun porttiin ei ole kytketty kaapelia, portin aukosta voi vuotaa näkymätöntä lasersäteilyä. Älä katso avoimiin aukkoihin, jotta et altistu säteilylle.

Attention Etant donné qu'un rayonnement laser invisible peut être émis par l'ouverture du port quand aucun câble n'est connecté, ne pas regarder dans les ouvertures béantes afin d'éviter tout risque d'exposition au rayonnement laser.

Warnung **Aus der Öffnung des Ports kann unsichtbare Laserstrahlung austreten, wenn kein Kabel angeschlossen ist. Kontakt mit Laserstrahlung vermeiden und nicht in offene Öffnungen blicken.**

Avvertenza **Poiché quando nessun cavo è collegato alla porta, da quest'ultima potrebbe essere emessa radiazione laser invisibile, evitare l'esposizione a tale radiazione e non fissare con gli occhi porte a cui non siano collegati cavi.**

Advarsel **Usynlige laserstråler kan sendes ut fra åpningen på utgangen når ingen kabel er tilkoblet. Unngå utsettelse for laserstråling og se ikke inn i åpninger som ikke er tildekket.**

Aviso **Evite uma exposição à radiação laser e não olhe através de aberturas expostas, porque poderá ocorrer emissão de radiação laser invisível a partir da abertura da porta, quando não estiver qualquer cabo conectado.**

¡Advertencia! **Cuando no esté conectado ningún cable, pueden emitirse radiaciones láser invisibles por el orificio del puerto. Evitar la exposición a radiaciones láser y no mirar fijamente los orificios abiertos.**

Varning! **Osynliga laserstrålar kan sändas ut från öppningen i porten när ingen kabel är ansluten. Undvik exponering för laserstrålning och titta inte in i ej täckta öppningar.**

A.4.11 More Than One Power Supply

Warning **This unit has more than one power supply connection; all connections must be removed completely to completely remove power from the unit.**

Waarschuwing **Deze eenheid heeft meer dan één stroomtoevoerverbinding; alle verbindingen moeten volledig worden verwijderd om de stroom van deze eenheid volledig te verwijderen.**

Varoitus **Tässä laitteessa on useampia virtalähdekytkentöjä. Kaikki kytkennät on irrotettava kokonaan, jotta virta poistettaisiin täysin laitteesta.**

Attention **Cette unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.**

Warnung **Diese Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.**

Avvertenza **Questa unità ha più di una connessione per alimentatore elettrico; tutte le connessioni devono essere completamente rimosse per togliere l'elettricità dall'unità.**

Advarsel **Denne enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.**

Aviso **Este dispositivo possui mais do que uma conexão de fonte de alimentação de energia; para poder remover a fonte de alimentação de energia, deverão ser desconectadas todas as conexões existentes.**

¡Advertencia! **Esta unidad tiene más de una conexión de suministros de alimentación; para eliminar la alimentación por completo, deben desconectarse completamente todas las conexiones.**

Varning! **Denna enhet har mer än en strömförsörjningsanslutning; alla anslutningar måste vara helt avlägsnade innan strömtillförseln till enheten är fullständigt bruten.**

A.4.12 Unterminated Fiber Warning

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

Waarschuwing **Er kunnen onzichtbare laserstralen worden uitgezonden vanuit het uiteinde van de onafgebroken vezelkabel of connector. Niet in de straal kijken of deze rechtstreeks bekijken met optische instrumenten. Als u de laseruitvoer met bepaalde optische instrumenten bekijkt (zoals bijv. een oogloep, vergrootgras of microscoop) binnen een afstand van 100 mm kan dit gevaar voor uw ogen opleveren. Het gebruik van regelaars of bijstellingen of het uitvoeren van procedures anders dan opgegeven kan leiden tot blootstelling aan gevaarlijke straling.**

Varoitus **Päättämättömän kuitukaapelin tai -liittimen päästä voi tulla näkymätöntä lasersäteilyä. Älä tuijota sädettä tai katso sitä suoraan optisilla välineillä. Lasersäteen katsominen tietyillä optisilla välineillä (esim. suurennuslasilla tai mikroskoopilla) 10 cm:n päästä tai sitä lähempää voi olla vaarallista silmille. Säätimien tai säätöjen käyttö ja toimenpiteiden suorittaminen ohjeista poikkeavalla tavalla voi altistaa vaaralliselle säteilylle.**

Attention **Des émissions de radiations laser invisibles peuvent se produire à l'extrémité d'un câble en fibre ou d'un raccord sans terminaison. Ne pas fixer du regard le rayon ou l'observer directement avec des instruments optiques. L'observation du laser à l'aide certains instruments optiques (loupes et microscopes) à une distance inférieure à 100 mm peut poser des risques pour les yeux. L'utilisation de commandes, de réglages ou de procédures autres que ceux spécifiés peut entraîner une exposition dangereuse à des radiations.**

Warnung **Eine unsichtbare Laserstrahlung kann vom Ende des nicht angeschlossenen Glasfaserkabels oder Steckers ausgestrahlt werden. Nicht in den Laserstrahl schauen oder diesen mit einem optischen Instrument direkt ansehen. Ein Betrachten des Laserstrahls mit bestimmten optischen Instrumenten, wie z.B. Augenlupen, Vergrößerungsgläsern und Mikroskopen innerhalb eines Abstands von 100 mm kann für das Auge gefährlich sein. Die Verwendung von nicht spezifizierten Steuerelementen, Einstellungen oder Verfahrensweisen kann eine gefährliche Strahlenexposition zur Folge haben.**

Avvertenza **L'estremità del connettore o del cavo ottico senza terminazione può emettere radiazioni laser invisibili. Non fissare il raggio od osservarlo in modo diretto con strumenti ottici. L'osservazione del fascio laser con determinati strumenti ottici (come lupette, lenti di ingrandimento o microscopi) entro una distanza di 100 mm può provocare danni agli occhi. L'adozione di controlli, regolazioni o procedure diverse da quelle specificate può comportare il pericolo di esposizione a radiazioni.**

Advarsel **Usynlig laserstråling kan emittere fra enden av den ikke-terminerte fiberkabelen eller koblingen. Ikke se inn i strålen og se heller ikke direkte på strålen med optiske instrumenter. Observering av laserutgang med visse optiske instrumenter (for eksempel øyelupe, forstørrelsesglass eller mikroskoper) innenfor en avstand på 100 mm kan være farlig for øynene. Bruk av kontroller eller justeringer eller utførelse av prosedyrer som ikke er spesifiserte, kan resultere i farlig strålingseksponering.**

Aviso **Radiação laser invisível pode ser emitida pela ponta de um conector ou cabo de fibra não terminado. Não olhe fixa ou diretamente para o feixe ou com instrumentos ópticos. Visualizar a emissão do laser com certos instrumentos ópticos (por exemplo, lupas, lentes de aumento ou microscópios) a uma distância de 100 mm pode causar riscos à visão. O uso de controles, ajustes ou desempenho de procedimentos diferentes dos especificados pode resultar em exposição prejudicial de radiação.**

¡Advertencia! **El extremo de un cable o conector de fibra sin terminación puede emitir radiación láser invisible. No se acerque al radio de acción ni lo mire directamente con instrumentos ópticos. La exposición del ojo a una salida de láser con determinados instrumentos ópticos (por ejemplo, lupas y microscopios) a una distancia de 100 mm puede comportar lesiones oculares. La aplicación de controles, ajustes y procedimientos distintos a los especificados puede comportar una exposición peligrosa a la radiación.**

Varning! **Osynlig laserstrålning kan komma från änden på en oavslutad fiberkabel eller -anslutning. Titta inte rakt in i strålen eller direkt på den med optiska instrument. Att titta på laserstrålen med vissa optiska instrument (t.ex. lupper, förstoringsglas och mikroskop) från ett avstånd på 100 mm kan skada ögonen. Om andra kontroller eller justeringar än de angivna används, eller om andra processer än de angivna genomförs, kan skadlig strålning avges.**

A.4.13 Laser Activation Warning

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

Waarschuwing **De laser is aan zodra de kaart is opgestart en de veiligheidssleutel in de AAN-positie is (gelabeld 1). De poort hoeft niet in dienst te zijn om de laser aan te zetten. De laser is uit wanneer de veiligheidssleutel uit is (gelabeld 0).**

Varoitus **Laser on päällä, kun kortti käynnistetään ja turva-avain on päällä (1) -asennossa. Laser voi olla päällä, vaikka portti ei olekaan käytössä. Laser on pois päältä, kun turva-avain on pois (0) -asennossa.**

Attention **Le laser est allumé dès le démarrage de la carte et lorsque la clé de sûreté est en position allumée (ou 1). Il n'est pas nécessaire que le port soit en service pour que le laser soit allumé. Le laser est éteint lorsque la clé de sûreté est en position éteinte (ou 0).**

Warnung **Der Laser ist eingeschaltet, wenn die Karte geladen wurde und der Sicherheitsschlüssel eingeschaltet ist (mit 1 bezeichnete Stellung). Der Port muss nicht in Betrieb sein, wenn der Laser eingeschaltet ist. Der Laser ist ausgeschaltet, wenn sich der Sicherheitsschlüssel in der Aus-Stellung (mit 0 bezeichnet) befindet.**

Avvertenza **Il laser è attivato quando la scheda è inserita e la chiave di sicurezza è in posizione ON (indicata con I). Per l'attivazione del laser non è necessario che la porta sia in funzione. Il laser è disattivato quando la chiave di sicurezza è su OFF (indicata con 0).**

Advarsel **Laseren er aktivert når kortet er på plass og sikkerhetstasten er i på-stilling (merket 1). Porten trenger ikke å være aktiv selv om laseren er på. Laseren er av når sikkerhetstasten er i av-stilling (merket 0).**

Aviso **O laser está ativado quando a placa é reiniciada e a chave de segurança está na posição on (ou 1). A porta não precisa estar em atividade para o acionamento do laser. O laser está desativado quando a chave de segurança está na posição off (ou 0).**

¡Advertencia! **El láser está encendido cuando la tarjeta ha arrancado y la llave de seguridad se encuentra en la posición ON (etiquetada 1). No es necesario que el puerto esté en funcionamiento para que el láser pueda funcionar. El láser está apagado cuando la llave de seguridad se encuentra en la posición OFF (etiquetada 0).**

Varning! **Lasern är på när kortet är igångsatt och säkerhetsnyckeln är i läget På (markerat med 1). Porten behöver inte vara igång för att lasern ska vara på. Lasern är av när säkerhetsnyckeln är i läget Av (markerat med 0).**

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X