



Cisco ONS 15327 User Documentation

Release 3.3
June 2002

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-7813197=
Text Part Number: 78-13197-01

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

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

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

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

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

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

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

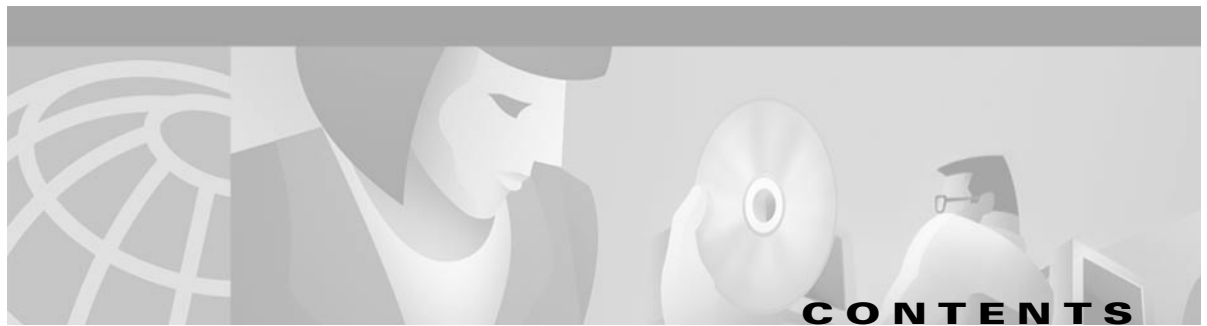
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)

Cisco ONS 15327 User Documentation

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.



About This Manual	xliv
Audience	xliv
Organization	xliv
Related Documentation	xlvi
Conventions	xlvii
Obtaining Documentation	xlvii
World Wide Web	xlvii
Optical Networking Product Documentation CD-ROM	xlviii
Ordering Documentation	xlviii
Documentation Feedback	xlviii
Obtaining Technical Assistance	xlviii
Cisco.com	xliv
Technical Assistance Center	xliv
Contacting TAC by Using the Cisco TAC Website	xliv
Contacting TAC by Telephone	xliv

CHAPTER 1

Hardware Installation	1-1
1.1 Installation Overview	1-2
1.2 Installation Equipment	1-2
1.2.1 Included Materials	1-2
1.2.2 User-Supplied Materials	1-3
1.2.2.1 Tools Needed	1-3
1.2.2.2 Test Equipment	1-3
1.3 Rack Installation	1-4
1.3.1 Reversible Mounting Bracket	1-4
1.3.1.1 Reverse the Mounting Bracket to Fit a 19-Inch Rack	1-5
1.3.2 Mounting a Single Node	1-6
Procedure: Mount the ONS 15327 in a Rack	1-6
1.3.3 Mounting Multiple Nodes	1-7
Procedure: Mount Multiple ONS 15327s in a Rack	1-7
1.4 Fan-Tray Assembly Installation	1-7
Procedure: Install the Fan-Tray Assembly	1-8
Procedure: Remove the Fan-Tray Assembly	1-8
1.5 Power and Ground Installation	1-9

CHAPTER 2**Software Installation 2-1**

- 2.1 Installation Overview **2-1**
- 2.2 Computer Requirements **2-2**
- 2.3 Running the CTC Installation Wizard **2-4**
 - Run the CTC Installation Wizard for Windows **2-4**
 - Run the CTC Installation Wizard for UNIX **2-6**
 - Set Up the Java Runtime Environment for UNIX **2-8**
- Setting Up the CTC Computer **2-9**
 - Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses **2-11**
 - Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP **2-13**
 - Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection **2-14**
 - Set up a Solaris Workstation for a Craft Connection to an ONS 15327 **2-16**
 - Set Up a Computer for a Corporate LAN Connection **2-17**
 - Disable Proxy Service Using Internet Explorer (Windows) **2-18**
 - Disable Proxy Service Using Netscape (Windows and UNIX) **2-18**
 - Provision Remote Access to the ONS 15327 **2-18**
- 2.4 Connecting PCs to the ONS 15327 **2-19**
 - 2.4.1 Direct Connections to the ONS 15327 **2-19**
 - Creating a Direct Connection to an ONS 15327 **2-19**
 - 2.4.2 Network Connections **2-21**
 - Access the ONS 15327 from a LAN **2-21**
 - Disable Proxy Service Using Internet Explorer (Windows) **2-21**
 - Disable Proxy Service Using Netscape (Windows and Solaris) **2-22**
 - 2.4.3 Remote Access to the ONS 15327 **2-22**
 - 2.4.4 TL1 Terminal Access to the ONS 15327 **2-22**
- 2.5 Logging into the ONS 15327 **2-23**
 - Log into the ONS 15327 **2-23**
 - 2.5.1 Creating Login Node Groups **2-24**
 - Create a Login Node Group **2-25**
 - 2.5.2 Accessing ONS 15327s Behind Firewalls **2-26**
 - Set the IIOP Listener Port on the ONS 15327 **2-27**
 - Set the IIOP Listener Port on CTC **2-27**
- 2.6 Working with the CTC Window **2-27**
 - 2.6.1 Node View **2-28**
 - 2.6.1.1 CTC Card Colors **2-28**
 - 2.6.1.2 Node View Card Shortcuts **2-29**
 - 2.6.1.3 Node View Tabs **2-29**

- 2.6.2 Network View **2-29**
 - 2.6.2.1 CTC Node Colors **2-30**
 - 2.6.2.2 Network View Tasks **2-31**
 - 2.6.2.3 Creating Domains **2-32**
 - 2.6.2.4 Changing the Network View Background Color **2-33**
 - Modify the Network View or Domain Background Color **2-33**
 - 2.6.2.5 Changing the Network View Background Image **2-34**
 - Change the Network View Background Image **2-34**
 - Add a Node to the Current Session **2-35**
- 2.6.3 Card View **2-35**
- 2.7 CTC Navigation **2-36**
- 2.8 Viewing CTC Table Data **2-38**
- 2.9 Printing and Exporting CTC Data **2-40**
 - Print CTC Window and Table Data **2-41**
 - Export CTC Data **2-42**
- 2.10 Displaying CTC Data in Other Applications **2-43**

CHAPTER 3

Node Setup 3-1

- 3.1 Before You Begin **3-1**
- 3.2 Setting Up Basic Node Information **3-2**
 - Add the Node Name, Contact, Location, Date, and Time **3-2**
- 3.3 Setting Up Network Information **3-3**
 - Set Up Network Information **3-3**
- 3.4 Creating Users and Setting Security **3-5**
 - Create New Users **3-6**
 - Edit a User **3-7**
 - Delete a User **3-7**
- 3.5 Creating Protection Groups **3-8**
 - Create Protection Groups for Optical Cards **3-8**
 - Enable Ports **3-9**
 - Edit Protection Groups **3-9**
 - Delete Protection Groups **3-10**
- 3.6 Setting Up ONS 15327 Timing **3-11**
 - 3.6.1 Network Timing Example **3-11**
 - 3.6.2 Synchronization Status Messaging **3-12**
 - Set Up ONS 15327 Timing **3-13**
 - Set Up Internal Timing **3-15**
- 3.7 Viewing ONS 15327 Inventory **3-16**

3.8 Viewing CTC Software Versions 3-17

CHAPTER 4

IP Networking 4-19

- 4.1 IP Networking Overview 4-19
- 4.2 ONS 15327 IP Addressing Scenarios 4-20
 - 4.2.1 Scenario 1: CTC and ONS 15327s on Same Subnet 4-21
 - 4.2.2 Scenario 2: CTC and ONS 15327s Connected to Router 4-22
 - 4.2.3 Scenario 3: Using Proxy ARP to Enable an ONS 15327 Gateway 4-23
 - 4.2.4 Scenario 4: Default Gateway on CTC Computer 4-24
 - 4.2.5 Scenario 5: Using Static Routes to Connect to LANs 4-25
 - 4.2.6 Scenario 6: Using OSPF 4-27
 - Procedure: Set Up OSPF 4-30
 - 4.2.7 Scenario 7: Provisioning the ONS 15327 Proxy Server 4-32
- 4.3 ONS 15327 Routing Table 4-38

CHAPTER 5

SONET Topologies 5-1

- 5.1 Before You Begin 5-1
- 5.2 Bidirectional Line Switched Rings 5-1
 - 5.2.1 Two-Fiber BLSRs 5-2
 - 5.2.2 BLSR Bandwidth 5-4
 - 5.2.3 Sample BLSR Application 5-5
 - 5.2.4 Setting Up BLSRs 5-7
 - Install the BLSR Trunk Cards 5-7
 - Create the BLSR DCC Terminations 5-8
 - Enable the BLSR Ports 5-8
 - Provision the BLSR 5-9
 - 5.2.5 Adding and Removing BLSR Nodes 5-11
 - Add a BLSR Node 5-12
 - Remove a BLSR Node 5-15
 - 5.2.6 Moving BLSR Trunk Cards 5-16
 - Move a BLSR Trunk Card 5-18
- 5.3 Unidirectional Path Switched Rings 5-20
 - 5.3.1 Example UPSR Application 5-22
 - 5.3.2 Setting Up a UPSR 5-23
 - Install the UPSR Trunk Cards 5-23
 - Configure the UPSR DCC Terminations 5-24
 - Enable the UPSR Ports 5-25
 - 5.3.3 Adding and Removing UPSR Nodes 5-25
 - Switch UPSR Traffic 5-25

- Add a UPSR Node **5-27**
- Remove a UPSR Node **5-28**
- 5.4 Subtending Rings **5-29**
 - Subtend a UPSR from a BLSR **5-30**
 - Subtend a BLSR from a UPSR **5-31**
 - Subtend a BLSR from a BLSR **5-32**
- 5.4.1 Connecting ONS 15327 Nodes and ONS 15454 Nodes **5-33**
- 5.5 Linear ADM Configurations **5-34**
 - Create a Linear ADM **5-35**
 - Convert a Linear ADM to UPSR **5-35**
 - Convert a Linear ADM to a BLSR **5-39**
- 5.6 Path-Protected Mesh Networks **5-42**

CHAPTER 6

Circuits and Tunnels 6-1

- 6.1 Circuits Overview **6-1**
- 6.2 Creating Circuits and VT Tunnels **6-2**
 - Create an Automatically Routed Circuit **6-2**
 - Create a Manually Routed Circuit **6-6**
- 6.3 Creating Multiple Drops for Unidirectional Circuits **6-8**
 - Create a Unidirectional Circuit with Multiple Drops **6-8**
- 6.4 Creating Monitor Circuits **6-9**
 - Create a Monitor Circuit **6-9**
- 6.5 Searching for Circuits **6-10**
 - Search for ONS 15327 Circuits **6-10**
- 6.6 Editing UPSR Circuits **6-10**
 - Edit a UPSR Circuit **6-11**
- 6.7 Creating a Path Trace **6-12**
 - Create a J1 Path Trace **6-13**
- 6.8 Cross-Connect Card Capacities **6-15**
 - 6.8.1 VT1.5 Cross-Connects **6-15**
 - 6.8.2 VT Tunnels **6-18**
- 6.9 Creating DCC Tunnels **6-20**
 - Provision a DCC Tunnel **6-21**

CHAPTER 7

Card Provisioning 7-1

- 7.1 Performance Monitoring Thresholds **7-1**
- 7.2 Provisioning Electrical Cards **7-2**
 - 7.2.1 Mapping Card Provisioning and Performance Monitoring **7-3**

- 7.2.2 DS-1 Card Parameters **7-4**
 - Modify Line and Threshold Settings for the DS-1 Card **7-4**
- 7.2.3 DS-3 Card Parameters **7-8**
 - Modify Line and Threshold Settings for the DS-3 Card **7-8**
- 7.3 Provisioning Optical Cards **7-10**
 - 7.3.1 Modifying Transmission Quality **7-11**
 - Provision Line Transmission Settings for OC-N Cards **7-11**
 - Provision Threshold Settings for OC-N Cards **7-12**
- 7.4 Provisioning IPPM **7-15**
 - Enable Intermediate-Path Performance Monitoring **7-16**
- 7.5 Using Virtual Wires **7-17**
 - 7.5.1 External Input Alarms **7-17**
 - Provision External Alarms **7-18**
 - 7.5.2 External Output Controls **7-19**
 - Provision External Controls **7-19**
 - 7.5.3 Provisioning Orderwire Pass-Through **7-20**
 - Provision Orderwire Pass-Through **7-21**

CHAPTER 8**Performance Monitoring 8-1**

- 8.1 Using the Performance Monitoring Screen **8-2**
 - 8.1.1 Viewing PMs **8-2**
 - View PMs **8-2**
 - 8.1.2 Changing the Screen Intervals **8-3**
 - Select Fifteen-Minute PM Intervals on the Performance Monitoring Screen **8-4**
 - Select Twenty-Four Hour PM Intervals on the Performance Monitoring Screen **8-5**
 - Clearing PM Data on the Performance Monitoring Screen **8-5**
 - 8.1.3 Viewing Near End and Far End PMs **8-6**
 - Select Near End PMs on the Performance Monitoring Screen **8-6**
 - Select Far End PMs on the Performance Monitoring Screen **8-7**
 - 8.1.4 Using the Signal-Type Menu **8-7**
 - Select Signal-Type Menus on the Performance Monitoring Screen **8-8**
 - 8.1.5 Using the Baseline Button **8-8**
 - Use the Baseline Button on the Performance Monitoring Screen **8-9**
 - 8.1.6 Using the Clear Button **8-9**
 - Use the Clear Button on the Performance Monitoring Screen **8-10**
- Threshold Reference **8-10**
- 8.2 Intermediate-Path Performance Monitoring Reference **8-12**
- 8.3 Pointer Justification Count Reference **8-13**
- 8.4 Performance Monitoring for Electrical Cards **8-16**

- 8.4.1 XTC DS1 Performance Monitoring Parameters **8-16**
- 8.4.2 XTC DS3 Card Performance Monitoring Parameters **8-21**
- 8.5 Performance Monitoring for Optical Cards **8-24**
 - 8.5.1 OC-3 Card Performance Monitoring Parameters **8-24**
 - 8.5.2 OC-12 Card Performance Monitoring Parameters **8-29**
 - 8.5.3 OC-48 Card Performance Monitoring Parameters **8-34**

CHAPTER 9

Ethernet Operation 9-1

- 9.1 Ethernet over SONET Application **9-1**
- 9.2 ONS 15327 Ethernet Card **9-2**
 - 9.2.1 E10/100-4 Card Port Provisioning **9-3**
 - Provision E10/100-4 Ethernet Ports **9-3**
- 9.3 Multicard and Single-Card EtherSwitch **9-4**
 - 9.3.1 Multicard EtherSwitch **9-4**
 - 9.3.2 Single-Card EtherSwitch **9-4**
 - 9.3.3 ONS 15454 E Series and ONS 15327 EtherSwitch Circuit Combinations **9-5**
- 9.4 Ethernet Circuit Configurations **9-6**
 - 9.4.1 Point-to-Point Ethernet Circuits **9-6**
 - Provision an EtherSwitch Point-to-Point Circuit (Multicard or Single-Card) **9-7**
 - 9.4.2 Shared Packet Ring Ethernet Circuits **9-9**
 - Provision a Shared Packet Ring **9-10**
 - 9.4.3 Hub and Spoke Ethernet Circuit Provisioning **9-13**
 - Provision a Hub and Spoke Ethernet Circuit **9-14**
 - 9.4.4 Ethernet Manual Cross-Connects **9-16**
 - Provision a Single-card EtherSwitch Manual Cross-Connect **9-17**
 - Provision a Multicard EtherSwitch Manual Cross-Connect **9-19**
- 9.5 VLAN Support **9-21**
 - 9.5.1 Q-Tagging (IEEE 802.1Q) **9-22**
 - 9.5.2 Priority Queuing (IEEE 802.1Q) **9-23**
 - 9.5.3 VLAN Membership **9-25**
 - Provision Ethernet Ports for VLAN Membership **9-25**
- 9.6 Spanning Tree (IEEE 802.1D) **9-26**
 - 9.6.1 Multi-Instance Spanning Tree and VLANs **9-27**
 - Enable Spanning Tree on Ethernet Ports **9-27**
 - 9.6.2 Spanning-Tree Parameters **9-27**
 - 9.6.3 Spanning-Tree Configuration **9-28**
 - 9.6.4 Spanning-Tree Map **9-28**
 - View the Spanning Tree Map **9-28**
 - 9.6.5 Ethernet Performance Screen **9-29**

9.6.5.1	Statistics Window	9-29
9.6.5.2	Line Utilization Window	9-30
9.6.5.3	Utilization Formula	9-30
9.6.5.4	History Window	9-30
9.6.6	Ethernet Maintenance Screen	9-30
9.6.6.1	MAC Table	9-30
	Retrieve the MAC Table Information	9-31
9.6.6.2	Trunk Utilization Window	9-31
9.7	Remote Monitoring Specification Alarm Thresholds	9-31
	Creating Ethernet RMON Alarm Thresholds	9-33

CHAPTER 10**Alarm Monitoring and Management 10-1**

10.1	Overview	10-1
10.2	Viewing ONS 15327 Alarms	10-1
10.2.1	Controlling Alarm Display	10-3
10.2.2	Viewing Alarm-Affected Circuits	10-3
10.2.3	Conditions Tab	10-4
10.2.3.1	Retrieve and Display Conditions	10-5
10.2.3.2	Conditions Column Descriptions	10-5
10.2.4	Viewing History	10-6
10.3	Alarm Profiles	10-7
10.3.1	Creating and Modifying Alarm Profiles	10-7
10.3.2	Alarm Profile Menus	10-8
10.3.3	Alarm Profile Editing	10-9
10.3.4	Alarm Severity Option	10-9
10.3.5	Row Display Options	10-9
10.3.6	Applying Alarm Profiles	10-10
10.4	Suppressing Alarms	10-11

CHAPTER 11**SNMP 11-1**

11.1	SNMP Overview	11-1
11.2	SNMP Basic Components	11-2
11.3	SNMP Support	11-3
11.4	SNMP MIBs	11-3
11.5	SNMP Traps	11-5
11.6	SNMP Community Names	11-7
11.7	SNMP Remote Monitoring	11-7
11.7.1	Ethernet Statistics Group	11-7

- 11.7.2 History Control Group **11-7**
- 11.7.3 Ethernet History Group **11-7**
- 11.7.4 Alarm Group **11-7**
- 11.7.5 Event Group **11-8**

CHAPTER 12

Maintenance 12-1

- 12.1 Air Filter Inspection and Replacement **12-2**
 - Inspect and Clean the Reusable Air Filter **12-2**
- 12.2 Fan-Tray Assembly Replacement **12-3**
 - Replace the Fan-Tray Assembly **12-3**
- 12.3 System Reset **12-5**
 - Perform a Software Reset **12-5**
 - Perform a Card Pull **12-5**
- 12.4 Database Backup and Restore **12-6**
 - Backup the Database **12-7**
 - Restore the Database **12-7**
- 12.5 Reverting to an Earlier Software Load **12-8**
 - Revert to an Earlier Software Load **12-9**
- 12.6 XTC-14 Card to XTC-28 Card Upgrade **12-10**
- 12.7 Span Upgrades **12-12**
 - Perform a Span Upgrade Using the Span Upgrade Wizard **12-13**
 - Perform a Manual Span Upgrade on a Two-Fiber BLSR **12-15**
 - Perform a Manual Span Upgrade on a UPSR **12-16**
 - Perform a Manual Span Upgrade on a 1+1 Protection Group **12-17**
- 12.8 Inhibit Protection Switching **12-18**
 - Apply a Lock On **12-18**
 - Apply a Lock Out **12-18**
 - Clear a Lock On or Lock Out **12-19**
- 12.9 Network Tests **12-19**
 - 12.9.1 Network Test Types **12-19**
- 12.10 Network Test Procedures **12-21**
 - 12.10.1 Perform a Facility Loopback on a Source XTC Card **12-21**
 - Create the Facility Loopback on the Source XTC Card **12-22**
 - Test the Facility Loopback **12-22**
 - Test the DS-N Cabling **12-23**
 - Test the XTC Card **12-23**
 - Test the MIC Card **12-23**
 - 12.10.2 Perform a Hairpin Circuit on a Source Node XTC Card **12-24**

- Create the Hairpin Loopback Circuit on the Source Node **12-24**
 - Test the Hairpin Loopback Circuit **12-25**
 - Test the Alternate Source XTC Card **12-25**
 - Retest the Original Source XTC Card **12-25**
 - 12.10.3 Perform a Hairpin on a Destination Node XTC Card **12-26**
 - Create the Hairpin Loopback Circuit on the Destination Node XTC Card **12-26**
 - Test the Hairpin Loopback Circuit on the Destination Node XTC Card **12-27**
 - Test the Alternate Destination XTC Card **12-27**
 - Retest the Original Destination XTC Card **12-28**
 - 12.10.4 Perform a Terminal Loopback on a Destination XTC Card **12-28**
 - Create the Terminal Loopback on a Destination XTC Card **12-29**
 - Test the Terminal Loopback Circuit on the Destination XTC Card **12-29**
 - Test the Destination XTC Card **12-30**
 - 12.10.5 Perform a Facility Loopback on a Destination XTC Card **12-30**
 - Create the Facility Loopback on a Destination XTC Card **12-31**
 - Test the Destination Facility Loopback **12-31**
 - Test the DS-N Cabling **12-31**
 - Test the XTC Card **12-32**
 - Test the MIC Card **12-32**
- 12.11 Creating Diagnostic Files **12-33**
 - Create a Diagnostic File **12-33**
- 12.12 Optic Fiber Cleaning **12-33**
 - Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes **12-33**
 - Clean Fiber Connectors with Cletop **12-34**
 - Clean the Fiber Adapters **12-34**
- 12.13 Power Down the ONS 15327 **12-35**
 - Power Down the ONS 15327 **12-35**

CHAPTER 13**Card Reference 13-1**

- 13.1 Overview **13-1**
 - 13.1.1 Common Control Cards **13-2**
 - 13.1.2 Mechanical Interface Cards **13-2**
 - 13.1.3 Optical Cards **13-2**
 - 13.1.4 Ethernet Card **13-2**
- 13.2 Card Protection **13-2**
 - 13.2.1 Unprotected **13-2**
 - 13.2.2 Electrical Protection **13-2**
 - 13.2.3 Optical Card Protection **13-3**
 - 13.2.4 Protection Switching **13-3**

- 13.3 XTC Cards (XTC-28-3/XTC-14) **13-3**
 - 13.3.1 XTC Card Description **13-3**
 - 13.3.1.1 XTC Front Panel **13-4**
 - 13.3.1.2 Support for DS-1 and DS-3 **13-4**
 - 13.3.1.3 XTC Timing and Control Functionality **13-5**
 - 13.3.1.4 XTC Cross-Connect Functionality **13-5**
 - 13.3.2 VT Mapping **13-6**
 - 13.3.3 XTC Cards (XTC 28-3/XTC-14) Specifications **13-8**
- 13.4 Mechanical Interface Cards **13-9**
 - 13.4.1 MIC Description **13-9**
 - 13.4.1.1 DS-1 Physical Interface **13-9**
 - 13.4.1.2 DS-3 Physical Interface **13-9**
 - 13.4.1.3 Power Connection **13-10**
 - 13.4.1.4 Alarm Interface **13-10**
 - 13.4.1.5 Provisioning I/O Alarm Contacts **13-10**
 - 13.4.1.6 BITS Interface **13-10**
 - 13.4.2 MIC Specifications **13-10**
- 13.5 OC3 IR 4 1310 Card **13-11**
 - 13.5.1 OC3 IR 4 1310 Card Description **13-11**
 - 13.5.2 OC3 IR 4 1310 Card-Level Indicators **13-11**
 - 13.5.3 OC3 IR 4 1310 Card Specifications **13-12**
- 13.6 OC12 IR 1310 Card **13-13**
 - 13.6.1 OC12 IR 1310 Card Description **13-13**
 - 13.6.2 OC12 IR 1310 Card-Level Indicators **13-14**
 - 13.6.3 OC12 IR 1310 Card Specifications **13-15**
- 13.7 OC12 LR 1550 Card **13-16**
 - 13.7.1 OC12 LR 1550 Card Description **13-16**
 - 13.7.2 OC12 LR 1550 Card-Level Indicators **13-16**
 - 13.7.3 OC12 LR 1550 Card Specifications **13-17**
- 13.8 OC48 IR 1310 Card **13-18**
 - 13.8.1 OC48 IR 1310 Card Description **13-18**
 - 13.8.2 OC48 IR 1310 Card-Level Indicators **13-19**
 - 13.8.3 OC48 IR 1310 Card Specifications **13-20**
- 13.9 OC48 LR 1550 Card **13-20**
 - 13.9.1 OC48 LR 1550 Card Description **13-21**
 - 13.9.2 OC48 LR 1550 Card-Level Indicators **13-21**
 - 13.9.3 OC48 LR 1550 Card Specifications **13-22**
- 13.10 E10/100-4 Card **13-23**
 - 13.10.1 E10/100-4 Card Description **13-23**

- 13.10.2 E10/100-4 Card-Level Indicators **13-24**
- 13.10.3 E10/100-4 Port-Level Indicators **13-24**
- 13.10.4 E10/100-4 Card Specifications **13-25**

CHAPTER 14**Alarm Troubleshooting 14-1**

- 14.1 Alarm Index **14-2**
- 14.2 Alarm Index by Alarm Type **14-3**
 - 14.2.1 Alarm Type/Object Definition **14-7**
- 14.3 Trouble Notifications **14-8**
 - 14.3.1 Conditions **14-8**
 - 14.3.2 Severities **14-9**
- 14.4 Alarm Procedures **14-9**
 - 14.4.1 AIS **14-9**
 - Clear the AIS Condition **14-9**
 - 14.4.2 AIS-L **14-9**
 - Clear the AIS-L Condition **14-10**
 - 14.4.3 AIS-P **14-10**
 - Clear the AIS-P Condition **14-10**
 - 14.4.4 AIS-V **14-10**
 - Clear the AIS-V Condition on the XTC-14 Card or XTC-28-3 Card **14-11**
 - 14.4.5 APSB **14-11**
 - Clear the APSB Alarm on an OC-N Card **14-11**
 - 14.4.6 APSCDFLTK **14-11**
 - Clear the APSCDFLTK Alarm **14-12**
 - 14.4.7 APSC-IMP **14-12**
 - Clear the APSC-IMP Alarm **14-13**
 - 14.4.8 APSCINCON **14-13**
 - Clear the APSCINCON Alarm on an OC-N Card in a BLSR **14-13**
 - 14.4.9 APSCM **14-14**
 - Clear the APSCM Alarm on an OC-N Card in 1+1 Mode **14-14**
 - 14.4.10 APSCNMIS **14-14**
 - Clear the APSCNMIS Alarm **14-14**
 - 14.4.11 APSMM **14-15**
 - Clear the APSMM Alarm in 1+1 Mode **14-15**
 - 14.4.12 AUTORESET **14-16**
 - Clear the AUTORESET Alarm **14-16**
 - 14.4.13 AUTOSW-AIS **14-16**
 - 14.4.14 AUTOSW-LOP (STSMON) **14-16**
 - 14.4.15 AUTOSW-LOP (VT-MON) **14-17**

- 14.4.16 AUTOSW-PDI **14-17**
- 14.4.17 AUTOSW-SDBER **14-17**
- 14.4.18 AUTOSW-SFBER **14-17**
- 14.4.19 AUTOSW-UNEQ (STSMON) **14-17**
- 14.4.20 AUTOSW-UNEQ (VT-MON) **14-17**
- 14.4.21 BKUPMEMP **14-18**
 - Clear the BKUPMEMP Alarm **14-18**
- 14.4.22 BLSROSYNC **14-19**
 - Clear the BLSROSYNC Alarm **14-19**
- 14.4.23 CARLOSS (E-Series) **14-20**
 - Clear the CARLOSS Alarm **14-20**
- 14.4.24 CARLOSS (EQPT) **14-21**
 - Clear the CARLOSS Alarm **14-22**
- 14.4.25 CLDRESTART **14-22**
 - Clear the CLDRESTART Condition **14-22**
- 14.4.26 CONCAT **14-23**
 - Clear the CONCAT Alarm **14-23**
- 14.4.27 CONTBUS-A **14-23**
 - Clear the CONTBUS-A Alarm **14-24**
- 14.4.28 CONTBUS-A-18 **14-24**
 - Clear the CONTBUS-A-18 Alarm **14-25**
- 14.4.29 CONTBUS-B **14-25**
 - Clear the CONTBUS-B **14-25**
- 14.4.30 CONTBUS-B-18 **14-26**
 - Clear the CONTBUS-B-18 Alarm on the XTC Card **14-26**
- 14.4.31 CTNEQPT-PBPROT **14-27**
 - Clear the CTNEQPT-PBPROT Alarm **14-27**
- 14.4.32 CTNEQPT-PBWORK **14-28**
 - Clear the CTNEQPT-PBWORK Alarm **14-28**
- 14.4.33 DATAFLT **14-30**
- 14.4.34 DS3-MISM **14-30**
 - Clear the DS3-MISM Alarm on the XTC-28-3 Card **14-30**
- 14.4.35 EOC **14-31**
 - Clear the EOC Alarm on an OC-N Card **14-31**
- 14.4.36 EQPT **14-32**
 - Clear the EQPT Alarm **14-33**
- 14.4.37 EQPT-MISS **14-33**
 - Clear the EQPT-MISS Alarm **14-33**
- 14.4.38 E-W-MISMATCH **14-33**
 - Clear the E-W-MISMATCH Alarm with a Physical Switch **14-34**

- Clear the E-W-MISMATCH Alarm with the CTC **14-34**
- 14.4.39 EXCCOL **14-35**
 - Clear the EXCCOL Alarm **14-35**
- 14.4.40 EXERCISE-RING-FAIL **14-35**
 - Clear the EXERCISE-RING-FAIL Condition **14-35**
- 14.4.41 EXERCISE-SPAN-FAIL **14-36**
 - Clear the EXERCISE-SPAN-FAIL Condition **14-36**
- 14.4.42 EXT **14-36**
 - Clear the EXT Alarm **14-36**
- 14.4.43 FAILTOSW-PATH **14-36**
 - Clear the FAILTOSW-PATH on a UPSR Configuration **14-37**
- 14.4.44 FAILTOSWR **14-38**
 - Clear the FAILTOSWR on a Four-Fiber BLSR Configuration **14-38**
- 14.4.45 FAILTOSWS **14-39**
- 14.4.46 FAN **14-39**
 - Clear the FAN Alarm **14-39**
- 14.4.47 FANDEGRADE **14-40**
 - Clear the FANDEGRADE Alarm **14-40**
- 14.4.48 FE-AIS **14-40**
 - Clear the FE-AIS Condition on the XTC-28-3 Cards in C-bit Format **14-41**
- 14.4.49 FE-DS1-MULTLOS **14-41**
 - Clear the FE-DS1-MULTLOS Condition on the XTC-14 Card or XTC-28-3 Card **14-41**
- 14.4.50 FE-DS1-SNGLLOS **14-41**
 - Clear the FE-DS1-SNGLLOS Condition on the XTC-14 **14-41**
- 14.4.51 FE-DS3-SA **14-42**
 - Clear the FE-DS3-SA Condition on the XTC28-3 Card in C-bit Format **14-42**
- 14.4.52 FE-EQPT-NSA **14-42**
 - Clear the FE-EQPT-NSA Condition on the XTC28-3 Card in C-bit Format **14-42**
- 14.4.53 FE-IDLE **14-42**
 - Clear the FE-IDLE Condition on the XTC28-3 Card in C-bit Format **14-43**
- 14.4.54 FE-LOCKOUT **14-43**
 - Clear the FE-LOCKOUT Condition on a BLSR **14-43**
- 14.4.55 FE-LOF **14-43**
 - Clear the FE-LOF Condition on the XTC28-3 Card in C-bit Format **14-43**
- 14.4.56 FE-LOS **14-44**
 - Clear the FE-LOS Condition on the XTC28-3 Card in C-bit Format **14-44**
- 14.4.57 FEPRLF **14-44**
 - Clear the FEPRLF Alarm on a Four-Fiber BLSR **14-44**
- 14.4.58 FORCED-REQ **14-44**
 - Clear the FORCED-REQ on an OC-N Card **14-45**

14.4.59	FRNGSYNC	14-45	
	Clear the FRNGSYNC Alarm	14-45	
14.4.60	FSTSYNC	14-45	
14.4.61	HITEMP	14-46	
	Clear the HITEMP Alarm	14-46	
14.4.62	HLDOVERSYNC	14-46	
	Clear the HLDOVERSYNC Alarm	14-46	
14.4.63	IMPROPRMVL	14-47	
	Clear the IMPROPRMVL Alarm	14-47	
14.4.64	INCOMPATIBLE-SW	14-48	
	Clear the INCOMPATIBLE-SW Alarm	14-48	
14.4.65	INVMACADDR	14-49	
	Clear the INVMACADDR Alarm	14-49	
14.4.66	LOCKOUT-REQ	14-49	
	Clear the Lockout Switch Request and the LOCKOUT-REQ Condition on an OC-N Card	14-49	
14.4.67	LOF (BITS)	14-49	
	Clear the LOF Alarm	14-50	
14.4.68	LOF (DS1)	14-50	
	Clear the LOF Alarm on the XTC-14 Card	14-50	
14.4.69	LOF (DS3)	14-51	
	Clear the LOF Alarm on the XTC-28-3 Card	14-51	
14.4.70	LOF (OC-N)	14-51	
	Clear the LOF Alarm on an OC-N Card	14-52	
14.4.71	LOGBUFR90	14-52	
	Clear the LOGBUFR90 Alarm	14-52	
14.4.72	LOGBUFROVFL	14-53	
	Clear the LOGBUFROVFL Alarm	14-53	
14.4.73	LOP-P	14-53	
	Clear the LOP-P Alarm	14-54	
14.4.74	LOP-V	14-55	
	Clear the LOP-V Alarm on the XTC Card	14-55	
14.4.75	LOS (BITS)	14-56	
	Clear the LOS Alarm	14-56	
14.4.76	LOS (DS-N)	14-56	
	Clear the LOS Alarm on the XTC Card	14-56	
14.4.77	LOS (OC-N)	14-57	
	Clear the LOS Alarm on an OC-N Card	14-57	
14.4.78	LPBKDS1FEAC	14-58	
14.4.79	LPBKDS3FEAC	14-58	
14.4.80	LPBKFACILITY (DS-N)	14-58	

- Clear the LBFACILITY Condition on the XTC-28-3 Card **14-59**
- 14.4.81 LPBFACILITY (OC-N) **14-59**
 - Clear the LBFACILITY Condition on the OC-N Card **14-60**
- 14.4.82 LPBKTERMINAL (DS-N) **14-60**
 - Clear the LPBKTERMINAL Condition on an XTC Card **14-60**
- 14.4.83 MANRESET **14-61**
- 14.4.84 MAN-REQ **14-61**
 - Clear the Manual Switch and the MAN-REQ Condition on an OC-N Card **14-61**
- 14.4.85 MEA (AIP) **14-61**
 - Clear the MEA Alarm on the AIP **14-61**
- 14.4.86 MEA (EQPT) **14-62**
 - Clear the MEA Alarm **14-62**
- 14.4.87 MEA (FAN) **14-63**
 - Clear the MEA Alarm on the Fan-Tray Assembly **14-63**
- 14.4.88 MEM-GONE **14-63**
- 14.4.89 MEM-LOW **14-63**
- 14.4.90 MFGMEM **14-64**
 - Clear the MFGMEM Alarm on the AIP, Fan Tray, or Backplane **14-64**
- 14.4.91 NOT-AUTHENTICATED **14-65**
 - Clear the NOT-AUTHENTICATED Alarm on the XTC Card **14-65**
- 14.4.92 PDI-P **14-65**
 - Clear the PDI-P Condition **14-66**
- 14.4.93 PEER-NORESPONSE **14-67**
 - Clear the PEER-NORESPONSE Alarm Reported on XTC or OC-N Card **14-67**
- 14.4.94 PLM-P **14-67**
 - Clear the PLM-P Alarm Reported on the XTC Card **14-67**
- 14.4.95 PLM-V **14-68**
 - Clear the PLM-V Alarm on the XTC-14 or XTC-28-3 Card **14-68**
- 14.4.96 PRC-DUPID **14-68**
 - Clear the PRC-DUPID Alarm on an OC-N Card in a BLSR **14-69**
- 14.4.97 RAI **14-69**
 - Clear the RAI Condition on XTC-28-3 Cards in C-bit Format **14-69**
- 14.4.98 RCVR-MISS **14-69**
 - Clear the RCVR-MISS Alarm on the XTC-14 Port **14-70**
- 14.4.99 RDI-P **14-70**
- 14.4.100 RFI-L **14-70**
 - Clear the RFI-L Condition on the OC-N Card **14-70**
- 14.4.101 RFI-P **14-70**
 - Clear the RFI-P Condition on the XTC or E10/100-4 Card **14-71**
- 14.4.102 RFI-V **14-71**

Clear the RFI-V Condition on the XTC Card	14-71
14.4.103 RING-MISMATCH	14-72
Clear the RING-MISMATCH Alarm	14-72
14.4.104 SD-L	14-72
Clear the SD-L Condition on an OC-N Card	14-73
14.4.105 SD-P	14-73
Clear the SD-P Condition on an OC-N Card	14-74
14.4.106 SF-L	14-74
Clear the SF-L Condition on an OC-N Card	14-75
14.4.107 SF-P	14-75
Clear the SF-P Condition on an OC-N Card	14-76
14.4.108 SFTWDOWN	14-76
14.4.109 SFTWDOWN-FAIL	14-76
Clear the SFTWDOWN-FAIL Alarm on the XTC Card	14-77
14.4.110 SNTP-HOST	14-77
Clear the SNTP-HOST Alarm	14-78
14.4.111 SQUELCH	14-78
Clear the SQUELCH Condition	14-78
14.4.112 SSM-FAIL	14-79
Clear the SSM-FAIL Alarm	14-79
14.4.113 STU	14-79
Clear the STU Condition	14-79
14.4.114 SWTOPRI	14-80
14.4.115 SWTOSEC	14-80
Clear the SWTOSEC Condition	14-80
14.4.116 SWTOTHIRD	14-80
Clear the SWTOTHIRD Condition	14-80
14.4.117 SYNCPRI	14-80
Clear the SYNCPRI Condition on the XTC Card	14-81
14.4.118 SYNCSEC	14-81
Clear the SYNCSEC Alarm on the XTC Card	14-81
14.4.119 SYNCTHIRD	14-81
Clear the SYNCTHIRD Alarm on the XTC Card	14-82
14.4.120 SYSBOOT	14-82
14.4.121 TIM-P	14-82
Clear the TIM-P Alarm	14-83
14.4.122 TRMT	14-83
Clear the TRMT Alarm on the XTC-14 Card	14-83
14.4.123 TRMT-MISS	14-83
Clear the TRMT-MISS Alarm	14-84

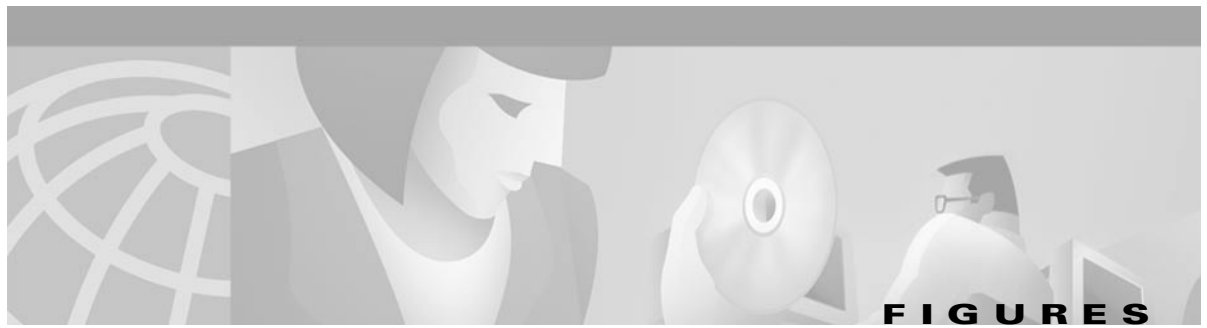
- 14.4.124 UNEQ-P **14-84**
 - Clear the UNEQ-P Alarm on the Line Card **14-84**
- 14.4.125 UNEQ-V **14-85**
 - Clear the UNEQ-V Alarm on the XTC-14 and XTC-28-3 Card **14-86**

Acronyms **A-1**

Regulatory Compliance and Safety Requirements for the *Cisco ONS 15327* **B-1**

- Contents **B-1**
- Japan and Korea Approvals **B-1**
 - Japan **B-1**
 - Label Requirements **B-1**
 - Korea **B-4**
 - Label Requirements **B-4**
- Regulatory Compliance **B-4**
- Class A Notice **B-5**
- Installation Warnings **B-6**
 - DC Power Disconnection Warning **B-7**
 - DC Power Connection Warning **B-8**
 - Power Supply Disconnection Warning **B-9**
 - Circuit Breaker (30A) Warning **B-10**
 - Class 1 Laser Product Warning **B-11**
 - Restricted Area Warning **B-12**
 - Ground Connection Warning **B-13**
 - Qualified Personnel Warning **B-14**
 - Invisible Laser Radiation Warning (other versions available) **B-14**
 - More Than One Power Supply **B-15**
- Related Documentation **B-16**
 - Release-Specific Documents **B-16**
- Obtaining Documentation **B-16**
 - World Wide Web **B-16**
 - Optical Networking Group CD-ROM **B-16**
 - Ordering Documentation **B-17**
 - Documentation Feedback **B-17**
- Obtaining Technical Assistance **B-17**
 - Cisco.com **B-17**
 - Technical Assistance Center **B-18**
 - Contacting TAC by Using the Cisco TAC Website **B-18**
 - Contacting TAC by Telephone **B-18**

INDEX



<i>Figure 1-1</i>	The ONS 15327 shelf assembly dimensions	1-4
<i>Figure 1-2</i>	Reversing the mounting brackets (23-inch position to 19-inch position)	1-5
<i>Figure 1-3</i>	Mounting an ONS 15327 in a rack	1-6
<i>Figure 1-4</i>	Removing or replacing the fan-tray air filter	1-7
<i>Figure 1-5</i>	Installing the fan-tray assembly	1-8
<i>Figure 1-6</i>	Removing a fan-tray assembly with installed cables	1-9
<i>Figure 1-7</i>	Removing the MIC power connector	1-11
<i>Figure 1-8</i>	Inserting a power cable into the MIC power connector	1-12
<i>Figure 1-9</i>	Installing the MIC power connector	1-13
<i>Figure 1-10</i>	Redundant power connected to an ONS 15327	1-13
<i>Figure 1-11</i>	Installing an XTC card (XTC 28-3)	1-17
<i>Figure 1-12</i>	Installing a high-speed card (E10/100-T)	1-17
<i>Figure 1-13</i>	ONS 15327 slot numbering	1-18
<i>Figure 1-14</i>	Managing front panel cables with locking cable guides	1-21
<i>Figure 1-15</i>	The cable installation sequence	1-22
<i>Figure 1-16</i>	Installing a fiber-optic cable	1-23
<i>Figure 1-17</i>	Installing a coaxial cable with BNC connectors	1-24
<i>Figure 1-18</i>	Installing a DS-1 cable	1-26
<i>Figure 1-19</i>	Pins 1 and 8 on the RJ-45 connector	1-27
<i>Figure 1-20</i>	BITS In pins on the RJ-45 connector	1-27
<i>Figure 1-21</i>	BITS Out pins on the RJ-45 connector	1-28
<i>Figure 2-1</i>	Starting the Cisco Transport Controller Installation Wizard	2-5
<i>Figure 2-2</i>	Logging into the ONS 15327	2-24
<i>Figure 2-3</i>	A login node group	2-26
<i>Figure 2-4</i>	ONS 15327s residing behind a firewall	2-27
<i>Figure 2-5</i>	A CTC computer and ONS 15327s residing behind firewalls	2-27
<i>Figure 2-6</i>	CTC window elements in the node view (default login view)	2-29
<i>Figure 2-7</i>	A three-node network displayed in CTC network view	2-31
<i>Figure 2-8</i>	Adding nodes to a domain	2-33
<i>Figure 2-9</i>	Outside nodes displayed within the domain	2-33
<i>Figure 2-10</i>	Nodes inside a domain	2-33

<i>Figure 2-11</i>	Changing the CTC background image	2-35
<i>Figure 2-12</i>	CTC card view showing an OC3 IR 1310 card	2-37
<i>Figure 2-13</i>	CTC node view showing popup information	2-38
<i>Figure 2-14</i>	Table shortcut menu that customizes table appearance	2-40
<i>Figure 2-15</i>	Selecting CTC data for print	2-43
<i>Figure 2-16</i>	Selecting CTC data for export	2-43
<i>Figure 3-1</i>	Setting up general network information	3-4
<i>Figure 3-2</i>	Specifying protection attributes in the Create Protection Group dialog box	3-9
<i>Figure 3-3</i>	Editing protection groups	3-10
<i>Figure 3-4</i>	An ONS 15327 timing example with external, BITS, and internal timing	3-12
<i>Figure 3-5</i>	Setting Up ONS 15327 timing	3-15
<i>Figure 3-6</i>	Displaying ONS 15327 hardware information	3-17
<i>Figure 4-1</i>	Scenario 1: CTC and ONS 15327s on same subnet	4-21
<i>Figure 4-2</i>	Scenario 2: CTC and ONS 15327s connected to router	4-22
<i>Figure 4-3</i>	Scenario 3: Using Proxy ARP	4-23
<i>Figure 4-4</i>	Scenario 4: Default gateway on a CTC computer	4-24
<i>Figure 4-5</i>	Scenario 5: Static route with one CTC computer used as a destination	4-25
<i>Figure 4-6</i>	Scenario 5: Static route with multiple LAN destinations	4-26
<i>Figure 4-7</i>	Scenario 6: OSPF enabled	4-28
<i>Figure 4-8</i>	Scenario 6: OSPF not enabled	4-29
<i>Figure 4-9</i>	Enabling OSPF on the ONS 15327	4-30
<i>Figure 4-10</i>	Scenario 7: Proxy Server Gateway Settings	4-33
<i>Figure 4-11</i>	Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on the same subnet	4-34
<i>Figure 4-12</i>	Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on different subnets	4-35
<i>Figure 4-13</i>	Scenario 7: ONS 15327 Proxy Server with ENEs on multiple rings	4-36
<i>Figure 4-14</i>	Viewing the ONS 15327 routing table	4-38
<i>Figure 5-1</i>	A four-node, two-fiber BLSR	5-2
<i>Figure 5-2</i>	Four-node, two-fiber BLSR sample traffic pattern	5-3
<i>Figure 5-3</i>	Four-node, two-fiber BLSR traffic pattern following line break	5-4
<i>Figure 5-4</i>	BLSR bandwidth reuse	5-5
<i>Figure 5-5</i>	A five-node BLSR	5-6
<i>Figure 5-6</i>	Shelf assembly layout for Node 0 in Figure 5-5	5-6
<i>Figure 5-7</i>	Shelf assembly layout for Nodes 1 – 4 in Figure 5-5	5-7
<i>Figure 5-8</i>	Connecting fiber to a four-node, two-fiber BLSR	5-8
<i>Figure 5-9</i>	Enabling an optical port	5-9

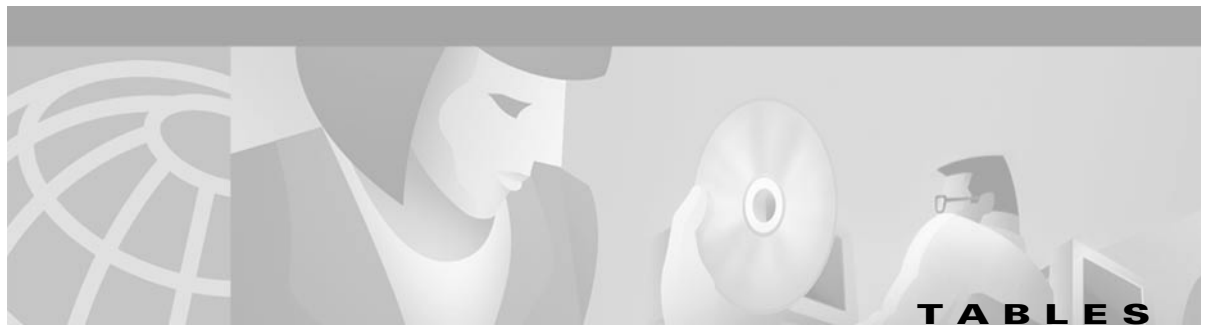
<i>Figure 5-10</i>	Setting BLSR properties	5-10
<i>Figure 5-11</i>	A three-node BLSR before adding a new node	5-12
<i>Figure 5-12</i>	A BLSR with a newly-added fourth node	5-14
<i>Figure 5-13</i>	A four-node BLSR before a trunk card switch	5-17
<i>Figure 5-14</i>	A four-node BLSR after the trunk cards are switched at one node	5-18
<i>Figure 5-15</i>	Deleting circuits from a BLSR trunk card	5-19
<i>Figure 5-16</i>	A basic four-node UPSR	5-21
<i>Figure 5-17</i>	A UPSR with a fiber break	5-21
<i>Figure 5-18</i>	An OC-3 UPSR	5-22
<i>Figure 5-19</i>	Layout of Node ID 0 in the OC-3 UPSR example (Figure 5-15)	5-23
<i>Figure 5-20</i>	Layout of Node IDs 1 – 3 in the OC-3 UPSR example (Figure 5-15)	5-23
<i>Figure 5-21</i>	Connecting fiber to a four-node UPSR	5-24
<i>Figure 5-22</i>	Using the span shortcut menu to display circuits	5-26
<i>Figure 5-23</i>	Switching UPSR circuits	5-27
<i>Figure 5-24</i>	An ONS 15327 with subtending rings	5-29
<i>Figure 5-25</i>	A UPSR subtending from a BLSR	5-30
<i>Figure 5-26</i>	A BLSR subtending from a BLSR	5-32
<i>Figure 5-27</i>	Configuring two BLSRs on the same node	5-33
<i>Figure 5-28</i>	A linear or UPSR connection between ONS 15454 and ONS 15327 nodes	5-34
<i>Figure 5-29</i>	ONS 15327 ring subtended from an ONS 15454 ring	5-34
<i>Figure 5-30</i>	A linear (point-to-point) ADM configuration	5-35
<i>Figure 5-31</i>	Verifying working slots in a protection group	5-36
<i>Figure 5-32</i>	Deleting a protection group	5-37
<i>Figure 5-33</i>	Converting a linear ADM to a UPSR	5-38
<i>Figure 5-34</i>	Converting a linear ADM to a BLSR	5-40
<i>Figure 5-35</i>	A path-protected mesh network	5-43
<i>Figure 5-36</i>	A PPMN virtual ring	5-44
<i>Figure 6-1</i>	Creating an automatically-routed circuit	6-3
<i>Figure 6-2</i>	Setting circuit routing preferences	6-4
<i>Figure 6-3</i>	Specifying circuit constraints	6-5
<i>Figure 6-4</i>	Creating a manually-routed circuit	6-6
<i>Figure 6-5</i>	A VT1.5 monitor circuit received at aDS-1 port	6-9
<i>Figure 6-6</i>	Editing UPSR selectors	6-11
<i>Figure 6-7</i>	Selecting the Edit Path Trace option	6-13
<i>Figure 6-8</i>	Setting up a path trace	6-14

<i>Figure 6-9</i>	Example #1: A VT1.5 circuit in a BLSR	6-16
<i>Figure 6-10</i>	Example #2: Two VT1.5 circuits in a BLSR	6-16
<i>Figure 6-11</i>	Example #3: VT1.5 circuit in a UPSR or 1+1 protection scheme	6-17
<i>Figure 6-12</i>	Example #4: Two VT1.5 circuits in UPSR or 1+1 protection scheme	6-17
<i>Figure 6-13</i>	A VT1.5 tunnel	6-18
<i>Figure 6-14</i>	A six-node ring with two VT1.5 tunnels	6-19
<i>Figure 6-15</i>	A DCC tunnel	6-21
<i>Figure 6-16</i>	Selecting DCC tunnel end points	6-22
<i>Figure 7-1</i>	Provisioning line parameters on the DS1-14 card	7-5
<i>Figure 7-2</i>	Provisioning thresholds for the OC48 IR 1310 card	7-12
<i>Figure 7-3</i>	IPPM provisioned for STS 1 on an OC-12 card	7-16
<i>Figure 7-4</i>	Example of external alarms and controls in a virtual wire configuration	7-17
<i>Figure 7-5</i>	The External Alarms subtab showing the XTC-28-3 card	7-18
<i>Figure 7-6</i>	The External Controls subtab showing the XTC-14 card	7-19
<i>Figure 7-7</i>	Example of the external alarm input and output process	7-20
<i>Figure 8-1</i>	Viewing performance-monitoring information	8-2
<i>Figure 8-2</i>	Time interval buttons on the card view Performance tab	8-4
<i>Figure 8-3</i>	Near End and Far End buttons on the card view Performance tab	8-6
<i>Figure 8-4</i>	Signal-type menus for an OC48 card	8-7
<i>Figure 8-5</i>	Baseline button for clearing displayed PM counts	8-8
<i>Figure 8-6</i>	Clear button for clearing PM counts	8-9
<i>Figure 8-7</i>	Threshold tab for setting threshold values	8-11
<i>Figure 8-8</i>	STS tab for enabling IPPM	8-12
<i>Figure 8-9</i>	Viewing pointer justification count parameters	8-14
<i>Figure 8-10</i>	Line tab for enabling pointer justification count parameters	8-15
<i>Figure 8-11</i>	Monitored signal types for the XTC DS1 cards	8-16
<i>Figure 8-12</i>	PM read points on the XTC DS1 cards	8-17
<i>Figure 8-13</i>	Monitored signal types for the XTC DS3 cards	8-22
<i>Figure 8-14</i>	PM read points on the XTC DS3 cards	8-22
<i>Figure 8-15</i>	PM read points on the OC-3 card	8-24
<i>Figure 8-16</i>	Monitored signal types for the OC-12 card	8-29
<i>Figure 8-17</i>	PM read points on the OC-12 card	8-29
<i>Figure 8-18</i>	Monitored signal types for the OC-48 cards	8-34
<i>Figure 8-19</i>	PM read points on the OC-48 cards	8-34
<i>Figure 9-1</i>	Ethernet transporting aggregate traffic from multiple sources	9-2

<i>Figure 9-2</i>	E10/100-4 Ethernet card faceplate	9-2
<i>Figure 9-3</i>	Provisioning E10/100-4 Ethernet ports	9-3
<i>Figure 9-4</i>	A Multicard EtherSwitch configuration	9-4
<i>Figure 9-5</i>	A Single-card EtherSwitch configuration	9-5
<i>Figure 9-6</i>	Multicard EtherSwitch point-to-point circuit	9-6
<i>Figure 9-7</i>	Single-card EtherSwitch point-to-point circuit	9-7
<i>Figure 9-8</i>	Choosing a circuit source	9-8
<i>Figure 9-9</i>	Choosing a VLAN name and ID	9-8
<i>Figure 9-10</i>	Selecting VLANs	9-9
<i>Figure 9-11</i>	Shared packet ring Ethernet circuit	9-10
<i>Figure 9-12</i>	Adding a span	9-12
<i>Figure 9-13</i>	Viewing a span	9-13
<i>Figure 9-14</i>	A Hub and spoke Ethernet circuit	9-14
<i>Figure 9-15</i>	Ethernet manual cross-connects	9-16
<i>Figure 9-16</i>	Creating an Ethernet circuit	9-17
<i>Figure 9-17</i>	Selecting VLANs	9-18
<i>Figure 9-18</i>	Creating an Ethernet circuit	9-19
<i>Figure 9-19</i>	Selecting VLANs	9-20
<i>Figure 9-20</i>	A Q-tag moving through a VLAN	9-23
<i>Figure 9-21</i>	Priority queuing process	9-24
<i>Figure 9-22</i>	Configuring VLAN membership for individual Ethernet ports	9-25
<i>Figure 9-23</i>	STP-blocked path	9-26
<i>Figure 9-24</i>	The Spanning-tree map on the circuit window	9-28
<i>Figure 9-25</i>	MAC addresses recorded in the MAC table	9-31
<i>Figure 9-26</i>	Creating RMON thresholds	9-33
<i>Figure 10-1</i>	Viewing alarms in CTC node view	10-2
<i>Figure 10-2</i>	Selecting the Affected Circuits Option	10-4
<i>Figure 10-3</i>	Highlighted circuit appears	10-4
<i>Figure 10-4</i>	Viewing fault conditions under the Conditions Tab	10-5
<i>Figure 10-5</i>	Viewing all alarms reported for the current session	10-7
<i>Figure 10-6</i>	Network View Alarm Profiles subtab showing the default profiles of listed alarms	10-8
<i>Figure 10-7</i>	Node view Alarm Behavior subtab of an OC-12 alarm profile	10-10
<i>Figure 10-8</i>	Card view Alarm Behavior subtab of an OC-12 alarm profile	10-11
<i>Figure 10-9</i>	The suppress alarms check box	10-12
<i>Figure 11-1</i>	A basic network managed by SNMP	11-2

<i>Figure 11-2</i>	SNMP agent gathering data from an MIB and sending traps to the manager	11-2
<i>Figure 11-3</i>	Example of the primary SNMP components	11-3
<i>Figure 12-1</i>	Removing and replacing the reusable fan-tray air filter	12-3
<i>Figure 12-2</i>	Removing a fan-tray assembly with installed cables	12-4
<i>Figure 12-3</i>	Replacing the fan-tray assembly	12-4
<i>Figure 12-4</i>	Backing up the ONS 15327 database	12-7
<i>Figure 12-5</i>	Restoring the database—traffic loss warning	12-8
<i>Figure 12-6</i>	Restoring the XTC database—in-progress notification	12-8
<i>Figure 12-7</i>	Resetting the XTC card	12-11
<i>Figure 12-8</i>	Span pull-down menu	12-14
<i>Figure 12-9</i>	Beginning the Span Upgrade Wizard	12-14
<i>Figure 12-10</i>	The facility loopback process on an XTC card	12-20
<i>Figure 12-11</i>	The hairpin circuit process on an OC-N card	12-20
<i>Figure 12-12</i>	The terminal loopback process on an OC-N card	12-21
<i>Figure 12-13</i>	Facility loopback on a source XTC card	12-22
<i>Figure 12-14</i>	Hairpin circuit on a source node XTC card	12-24
<i>Figure 12-15</i>	Hairpin on a destination node XTC card	12-26
<i>Figure 12-16</i>	Terminal loopback on a destination XTC card	12-28
<i>Figure 12-17</i>	Facility loopback on a destination XTC card	12-30
<i>Figure 13-1</i>	ONS 15327 slot assignments	13-1
<i>Figure 13-2</i>	XTC-28-3 card faceplate	13-4
<i>Figure 13-3</i>	XTC-14 card faceplate	13-4
<i>Figure 13-4</i>	Cross-connect matrix	13-6
<i>Figure 13-5</i>	XTC block diagram	13-8
<i>Figure 13-6</i>	MIC A card faceplate	13-9
<i>Figure 13-7</i>	MIC B card faceplate	13-9
<i>Figure 13-8</i>	OC3 IR 4 1310 card faceplate	13-11
<i>Figure 13-9</i>	OC3 IR 4 1310 card block diagram	13-12
<i>Figure 13-10</i>	OC12 IR 1310 card faceplate	13-14
<i>Figure 13-11</i>	OC12 IR 1310 card block diagram	13-15
<i>Figure 13-12</i>	OC12 LR 1550 card faceplate	13-16
<i>Figure 13-13</i>	OC12 LR 1550 card block diagram	13-17
<i>Figure 13-14</i>	OC48 IR 1310 faceplate	13-18
<i>Figure 13-15</i>	OC48 IR 1310 block diagram	13-19
<i>Figure 13-16</i>	OC48 LR 1550 faceplate	13-21

- Figure 13-17* OC48 LR 1550 block diagram **13-22**
- Figure 13-18* E10/100-4 faceplate **13-23**
- Figure 13-19* E10/100-4 block diagram **13-25**



<i>Table 1-1</i>	Installation Tasks	1-2
<i>Table 1-2</i>	External Timing Pin Assignments for BITS	1-14
<i>Table 1-3</i>	Card Ports, Line Rates, and Connectors	1-16
<i>Table 1-4</i>	Pin Assignments for CHAMP Connector (the shaded area corresponds to the white/orange binder group)	1-24
<i>Table 1-5</i>	Alarm Input Pin Assignments	1-26
<i>Table 1-6</i>	Alarm (External Control) Output Pin Assignments	1-26
<i>Table 1-7</i>	BITS Cable Pin Assignments	1-27
<i>Table 2-1</i>	JRE Compatibility	2-2
<i>Table 2-2</i>	Computer Requirements for CTC	2-3
<i>Table 2-3</i>	ONS 15327 Connection Methods	2-10
<i>Table 2-4</i>	ONS 15327 Craft Connection Options	2-11
<i>Table 2-5</i>	Set Up Windows PC for Craft ONS 15327 Connections on the Same Subnet Using Static IP Addresses	2-13
<i>Table 2-6</i>	Set Up Windows PC for Craft ONS 15327 Connections Using DHCP	2-14
<i>Table 2-7</i>	Set Up Windows PC for Craft ONS 15327 Connections Using Automatic Host Detection	2-16
<i>Table 2-8</i>	Setting Up Windows 95/98, Windows NT, and Windows 2000 PCs for Direct ONS 15327 Connections	2-21
<i>Table 2-9</i>	Node View Card Colors	2-29
<i>Table 2-10</i>	Node View Tabs and Subtabs	2-30
<i>Table 2-11</i>	Node Status	2-31
<i>Table 2-12</i>	Performing Network Management Tasks in Network View	2-32
<i>Table 2-13</i>	Managing Domains	2-34
<i>Table 2-14</i>	CTC Window Navigation	2-38
<i>Table 2-15</i>	Table Display Options	2-40
<i>Table 2-16</i>	Table Data with Export Capability	2-41
<i>Table 3-1</i>	ONS 15327 Security Levels—Node View	3-5
<i>Table 3-2</i>	ONS 15327 User Idle Times	3-6
<i>Table 3-3</i>	Protection Types	3-8
<i>Table 3-4</i>	SSM Generation 1 Message Set	3-12
<i>Table 3-5</i>	SSM Generation 2 Message Set	3-13
<i>Table 4-1</i>	General ONS 15327 IP Networking Checklist	4-20
<i>Table 4-2</i>	ONS 15327 Gateway and Element NE Settings	4-35
<i>Table 4-3</i>	Proxy Server Firewall Filtering Rules	4-36

<i>Table 4-4</i>	Proxy Server Firewall Filtering Rules When Packet Addressed to ONS 15327	4-37
<i>Table 4-5</i>	Sample Routing Table Entries	4-38
<i>Table 5-1</i>	ONS 15327 Rings	5-1
<i>Table 5-2</i>	Two-Fiber BLSR Capacity	5-4
<i>Table 6-1</i>	ONS 15327 Cards Supporting J1 Path Trace	6-12
<i>Table 6-2</i>	Path Trace Source and Drop Provisioning	6-12
<i>Table 6-3</i>	VT1.5-Mapped STS Use in Figure 6-6	6-19
<i>Table 6-4</i>	DCC Tunnels	6-20
<i>Table 7-1</i>	DS-N Card Provisioning Overview	7-2
<i>Table 7-2</i>	Mapping Card Provisioning and Performance Monitoring	7-3
<i>Table 7-3</i>	DS-1 Card Parameters	7-6
<i>Table 7-4</i>	DS-3 Card Parameters	7-9
<i>Table 7-5</i>	OC-N Card Line Settings on the Provisioning > Line Tab	7-11
<i>Table 7-6</i>	OC-N Card Threshold Settings on the Provisioning > Thresholds Tab	7-13
<i>Table 8-1</i>	Reference Topics for Performance Monitoring	8-1
<i>Table 8-2</i>	Traffic Cards That Terminate the Line, Called LTEs	8-12
<i>Table 8-3</i>	DS1 Line PMs for the XTC DS1 Cards	8-17
<i>Table 8-4</i>	DS1 Receive Path PMs for the XTC DS1 Cards	8-18
<i>Table 8-5</i>	DS1 Transmit Path PMs for the XTC DS1 Cards	8-19
<i>Table 8-6</i>	VT Path PMs for the XTC DS1 Cards	8-20
<i>Table 8-7</i>	Far-End VT Path PMs for the XTC DS1 Card	8-20
<i>Table 8-8</i>	SONET Path PMs for the XTC DS1 Cards	8-21
<i>Table 8-9</i>	Near-End DS3 Line PMs for the XTC DS3 Cards	8-23
<i>Table 8-10</i>	Near-End SONET Path PMs for the XTC DS3 Cards	8-23
<i>Table 8-11</i>	Near-End Section PMs for the OC-3 Card	8-24
<i>Table 8-12</i>	Near-End Line Layer PMs for the OC-3 Cards Card	8-25
<i>Table 8-13</i>	Near-End Protection-Switching PMs for the OC-3 Cards	8-26
<i>Table 8-14</i>	Near-End SONET Path H-byte PMs for the OC-3 Card	8-26
<i>Table 8-15</i>	Near-End SONET Path PMs for the OC-3 Card	8-27
<i>Table 8-16</i>	Far-End Line Layer PMs for the OC-3 Card	8-27
<i>Table 8-17</i>	Near-End Section PMs for the OC-12 Card	8-30
<i>Table 8-18</i>	Near-End Line Layer PMs for the OC-12 Card	8-30
<i>Table 8-19</i>	Near-End SONET Path H-byte PMs for the OC-12 Card	8-31
<i>Table 8-20</i>	Near-End Protection-Switching PMs for the OC-12 Card	8-31
<i>Table 8-21</i>	Near-End Protection-Switching Path PMs for the OC-12 Card	8-32

<i>Table 8-22</i>	Far-End Line Layer PMs for the OC-12 Card	8-33
<i>Table 8-23</i>	Near-End Section PMs for the OC-48 Cards	8-35
<i>Table 8-24</i>	Near-End Line Layer PMs for the OC-48 Cards	8-35
<i>Table 8-25</i>	Near-End SONET Path H-byte PMs for the OC-48 Cards	8-36
<i>Table 8-26</i>	Near-End Protection-Switching PMs for the OC-48 Cards	8-36
<i>Table 8-27</i>	Near-End SONET Path PMs for the OC-48 Cards	8-37
<i>Table 8-28</i>	Far-End Line Layer PMs for the OC-48 Cards	8-38
<i>Table 9-1</i>	E10/1004 faceplate LEDs	9-2
<i>Table 9-2</i>	ONS 15454 and ONS 15327 Ethernet Circuit Combinations	9-5
<i>Table 9-3</i>	Priority Queuing	9-24
<i>Table 9-4</i>	Port Settings	9-26
<i>Table 9-5</i>	Spanning-Tree Parameters	9-27
<i>Table 9-6</i>	Spanning-Tree Configuration	9-28
<i>Table 9-7</i>	Ethernet Parameters	9-29
<i>Table 9-8</i>	maxRate for STS Circuits	9-30
<i>Table 9-9</i>	Ethernet Threshold Variables (MIBs)	9-32
<i>Table 10-1</i>	Alarms Column Descriptions	10-2
<i>Table 10-2</i>	Color Codes for Alarms, Conditions, and Events	10-3
<i>Table 10-3</i>	Alarm Display	10-3
<i>Table 10-4</i>	Conditions Columns Description	10-5
<i>Table 10-5</i>	Alarm Profile Buttons	10-8
<i>Table 10-6</i>	Alarm Profile Editing Options	10-9
<i>Table 11-1</i>	SNMP Message Types	11-4
<i>Table 11-2</i>	IETF Standard MIBs Implemented in the ONS 15327 SNMP Agent	11-4
<i>Table 11-3</i>	SNMP Trap Variable Bindings Used in ONS 15327	11-5
<i>Table 11-4</i>	Traps Supported in the ONS 15327	11-6
<i>Table 13-1</i>	ONS 15327 VT mapping	13-6
<i>Table 13-2</i>	OC3 IR 4 1310 Card-Level Indicators	13-12
<i>Table 13-3</i>	OC12 IR 1310 Card-Level Indicators	13-14
<i>Table 13-4</i>	OC12 LR 1550 Card-Level Indicators	13-17
<i>Table 13-5</i>	OC48 IR 1310 Card-Level Indicators	13-19
<i>Table 13-6</i>	OC48 LR 1550 Card-Level Indicators	13-21
<i>Table 13-7</i>	E10/100-4 Card-Level Indicators	13-24
<i>Table 13-8</i>	E10/100-4 Port-Level Indicators	13-24
<i>Table 14-1</i>	Alarm Index	14-2

<i>Table 14-2</i>	Alarm Index by Alarm Type	14-3
<i>Table 14-3</i>	Alarm Type/Object Definition	14-7
<i>Table B-1</i>	Card Approvals	B-1
<i>Table B-2</i>	Certification of Information and Communication Equipment	B-4
<i>Table B-3</i>	Standards	B-4



Contacting TAC by Using the Cisco TAC Website **xlvii**

Contacting TAC by Telephone **xlvii**

Hardware Installation

Procedure: Mount the ONS 15327 in a Rack **1-6**

Procedure: Mount Multiple ONS 15327s in a Rack **1-7**

Procedure: Install the Fan-Tray Assembly **1-8**

Procedure: Remove the Fan-Tray Assembly **1-8**

Procedure: Install Redundant Power Feeds **1-10**

Attach Ferrites to Power Cabling **1-14**

Install ONS 15327 Cards **1-16**

Procedure: Verify Successful Turn-Up of MICs **1-18**

Procedure: Verify Successful Turn-Up of XTC Cards **1-19**

Procedure: Verify Successful Turn-Up of High-Speed Cards **1-19**

Procedure: Install and Route Fiber-Optic Cables in the ONS 15327 **1-22**

Procedure: Install Coaxial Cable With BNC Connectors **1-23**

Procedure: Install DS-1 CHAMP Cables on a MIC **1-25**

Software Installation

Run the CTC Installation Wizard for Windows **2-4**

Run the CTC Installation Wizard for UNIX **2-6**

Set Up the Java Runtime Environment for UNIX **2-8**

Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses **2-11**

Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP **2-13**

Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection **2-15**

Set up a Solaris Workstation for a Craft Connection to an ONS 15327 **2-17**

Set Up a Computer for a Corporate LAN Connection **2-18**

Disable Proxy Service Using Internet Explorer (Windows) **2-19**

Disable Proxy Service Using Netscape (Windows and UNIX) **2-19**

Provision Remote Access to the ONS 15327 **2-19**

Creating a Direct Connection to an ONS 15327 **2-20**

- Access the ONS 15327 from a LAN 2-22
- Disable Proxy Service Using Internet Explorer (Windows) 2-22
- Disable Proxy Service Using Netscape (Windows and Solaris) 2-23
- Log into the ONS 15327 2-24
- Create a Login Node Group 2-26
- Set the IIOF Listener Port on the ONS 15327 2-28
- Set the IIOF Listener Port on CTC 2-28
- Modify the Network View or Domain Background Color 2-34
- Change the Network View Background Image 2-35
- Add a Node to the Current Session 2-36
- Print CTC Window and Table Data 2-42
- Export CTC Data 2-43

Node Setup

- Add the Node Name, Contact, Location, Date, and Time 3-2
- Set Up Network Information 3-3
- Create New Users 3-6
- Edit a User 3-7
- Delete a User 3-7
- Create Protection Groups for Optical Cards 3-8
- Enable Ports 3-9
- Edit Protection Groups 3-9
- Delete Protection Groups 3-10
- Set Up ONS 15327 Timing 3-13
- Set Up Internal Timing 3-15

IP Networking

- Procedure: Set Up OSPF 4-30

SONET Topologies

- Install the BLSR Trunk Cards 5-7
- Create the BLSR DCC Terminations 5-8
- Enable the BLSR Ports 5-8
- Provision the BLSR 5-9
- Add a BLSR Node 5-12
- Remove a BLSR Node 5-15

- Move a BLSR Trunk Card **5-18**
- Install the UPSR Trunk Cards **5-23**
- Configure the UPSR DCC Terminations **5-24**
- Enable the UPSR Ports **5-25**
- Switch UPSR Traffic **5-25**
- Add a UPSR Node **5-27**
- Remove a UPSR Node **5-28**
- Subtend a UPSR from a BLSR **5-30**
- Subtend a BLSR from a UPSR **5-31**
- Subtend a BLSR from a BLSR **5-32**
- Create a Linear ADM **5-35**
- Convert a Linear ADM to UPSR **5-35**
- Convert a Linear ADM to a BLSR **5-39**

Circuits and Tunnels

- Create an Automatically Routed Circuit **6-2**
- Create a Manually Routed Circuit **6-6**
- Create a Unidirectional Circuit with Multiple Drops **6-8**
- Create a Monitor Circuit **6-9**
- Search for ONS 15327 Circuits **6-10**
- Edit a UPSR Circuit **6-11**
- Create a J1 Path Trace **6-13**
- Provision a DCC Tunnel **6-21**

Card Provisioning

- Modify Line and Threshold Settings for the DS-1 Card **7-4**
- Modify Line and Threshold Settings for the DS-3 Card **7-8**
- Provision Line Transmission Settings for OC-N Cards **7-11**
- Provision Threshold Settings for OC-N Cards **7-12**
- Enable Intermediate-Path Performance Monitoring **7-16**
- Provision External Alarms **7-18**
- Provision External Controls **7-19**
- Provision Orderwire Pass-Through **7-21**

Performance Monitoring

- View PMs **8-2**

- Select Fifteen-Minute PM Intervals on the Performance Monitoring Screen 8-4
- Select Twenty-Four Hour PM Intervals on the Performance Monitoring Screen 8-5
- Clearing PM Data on the Performance Monitoring Screen 8-5
- Select Near End PMs on the Performance Monitoring Screen 8-6
- Select Far End PMs on the Performance Monitoring Screen 8-7
- Select Signal-Type Menus on the Performance Monitoring Screen 8-8
- Use the Baseline Button on the Performance Monitoring Screen 8-9
- Use the Clear Button on the Performance Monitoring Screen 8-10

Ethernet Operation

- Provision E10/100-4 Ethernet Ports 9-3
- Provision an EtherSwitch Point-to-Point Circuit (Multicard or Single-Card) 9-7
- Provision a Shared Packet Ring 9-10
- Provision a Hub and Spoke Ethernet Circuit 9-14
- Provision a Single-card EtherSwitch Manual Cross-Connect 9-17
- Provision a Multicard EtherSwitch Manual Cross-Connect 9-19
- Provision Ethernet Ports for VLAN Membership 9-25
- Enable Spanning Tree on Ethernet Ports 9-27
- View the Spanning Tree Map 9-28
- Retrieve the MAC Table Information 9-31
- Creating Ethernet RMON Alarm Thresholds 9-33

Alarm Monitoring and Management

SNMP

Maintenance

- Inspect and Clean the Reusable Air Filter 12-2
- Replace the Fan-Tray Assembly 12-3
- Perform a Software Reset 12-5
- Perform a Card Pull 12-5
- Backup the Database 12-7
- Restore the Database 12-7
- Revert to an Earlier Software Load 12-9
- Perform a Span Upgrade Using the Span Upgrade Wizard 12-13
- Perform a Manual Span Upgrade on a Two-Fiber BLSR 12-15
- Perform a Manual Span Upgrade on a UPSR 12-16

- Perform a Manual Span Upgrade on a 1+1 Protection Group **12-17**
- Apply a Lock On **12-18**
- Apply a Lock Out **12-18**
- Clear a Lock On or Lock Out **12-19**
- Create the Facility Loopback on the Source XTC Card **12-22**
- Test the Facility Loopback **12-22**
- Test the DS-N Cabling **12-23**
- Test the XTC Card **12-23**
- Test the MIC Card **12-23**
- Create the Hairpin Loopback Circuit on the Source Node **12-24**
- Test the Hairpin Loopback Circuit **12-25**
- Test the Alternate Source XTC Card **12-25**
- Retest the Original Source XTC Card **12-25**
- Create the Hairpin Loopback Circuit on the Destination Node XTC Card **12-26**
- Test the Hairpin Loopback Circuit on the Destination Node XTC Card **12-27**
- Test the Alternate Destination XTC Card **12-27**
- Retest the Original Destination XTC Card **12-28**
- Create the Terminal Loopback on a Destination XTC Card **12-29**
- Test the Terminal Loopback Circuit on the Destination XTC Card **12-29**
- Test the Destination XTC Card **12-30**
- Create the Facility Loopback on a Destination XTC Card **12-31**
- Test the Destination Facility Loopback **12-31**
- Test the DS-N Cabling **12-31**
- Test the XTC Card **12-32**
- Test the MIC Card **12-32**
- Create a Diagnostic File **12-33**
- Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes **12-33**
- Clean Fiber Connectors with Cletop **12-34**
- Clean the Fiber Adapters **12-34**
- Power Down the ONS 15327 **12-35**

Card Reference

Alarm Troubleshooting

- Clear the AIS Condition **14-9**
- Clear the AIS-L Condition **14-10**

- Clear the AIS-P Condition **14-10**
- Clear the AIS-V Condition on the XTC-14 Card or XTC-28-3 Card **14-11**
- Clear the APSB Alarm on an OC-N Card **14-11**
- Clear the APSCDFLTk Alarm **14-12**
- Clear the APSC-IMP Alarm **14-13**
- Clear the APSCINCON Alarm on an OC-N Card in a BLSR **14-13**
- Clear the APSCM Alarm on an OC-N Card in 1+1 Mode **14-14**
- Clear the APSCNMIS Alarm **14-14**
- Clear the APSMM Alarm in 1+1 Mode **14-15**
- Clear the AUTORESET Alarm **14-16**
- Clear the BKUPMEMP Alarm **14-18**
- Clear the BLSROSYNC Alarm **14-19**
- Clear the CARLOSS Alarm **14-20**
- Clear the CARLOSS Alarm **14-22**
- Clear the CLDRESTART Condition **14-22**
- Clear the CONCAT Alarm **14-23**
- Clear the CONTBUS-A Alarm **14-24**
- Clear the CONTBUS-A-18 Alarm **14-25**
- Clear the CONTBUS-B **14-25**
- Clear the CONTBUS-B-18 Alarm on the XTC Card **14-26**
- Clear the CTNEQPT-PBPROT Alarm **14-27**
- Clear the CTNEQPT-PBWORK Alarm **14-28**
- Clear the DS3-MISM Alarm on the XTC-28-3 Card **14-30**
- Clear the EOC Alarm on an OC-N Card **14-31**
- Clear the EQPT Alarm **14-33**
- Clear the EQPT-MISS Alarm **14-33**
- Clear the E-W-MISMATCH Alarm with a Physical Switch **14-34**
- Clear the E-W-MISMATCH Alarm with the CTC **14-34**
- Clear the EXCCOL Alarm **14-35**
- Clear the EXERCISE-RING-FAIL Condition **14-35**
- Clear the EXERCISE-SPAN-FAIL Condition **14-36**
- Clear the EXT Alarm **14-36**
- Clear the FAILTOSW-PATH on a UPSR Configuration **14-37**
- Clear the FAILTOSWR on a Four-Fiber BLSR Configuration **14-38**
- Clear the FAN Alarm **14-39**

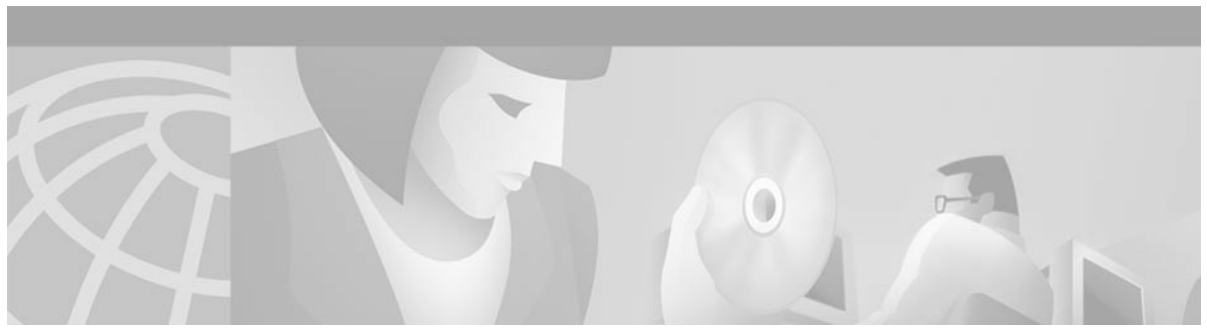
- Clear the FANDEGRADE Alarm **14-40**
- Clear the FE-AIS Condition on the XTC-28-3 Cards in C-bit Format **14-41**
- Clear the FE-DS1-MULTLOS Condition on the XTC-14 Card or XTC-28-3 Card **14-41**
- Clear the FE-DS1-SNGLLOS Condition on the XTC-14 **14-41**
- Clear the FE-DS3-SA Condition on the XTC28-3 Card in C-bit Format **14-42**
- Clear the FE-EQPT-NSA Condition on the XTC28-3 Card in C-bit Format **14-42**
- Clear the FE-IDLE Condition on the XTC28-3 Card in C-bit Format **14-43**
- Clear the FE-LOCKOUT Condition on a BLSR **14-43**
- Clear the FE-LOF Condition on the XTC28-3 Card in C-bit Format **14-43**
- Clear the FE-LOS Condition on the XTC28-3 Card in C-bit Format **14-44**
- Clear the FEPRLF Alarm on a Four-Fiber BLSR **14-44**
- Clear the FORCED-REQ on an OC-N Card **14-45**
- Clear the FRNGSYNC Alarm **14-45**
- Clear the HITEMP Alarm **14-46**
- Clear the HLDOVERSYNC Alarm **14-46**
- Clear the IMPROPRMVL Alarm **14-47**
- Clear the INCOMPATIBLE-SW Alarm **14-48**
- Clear the INVMACADDR Alarm **14-49**
- Clear the Lockout Switch Request and the LOCKOUT-REQ Condition on an OC-N Card **14-49**
- Clear the LOF Alarm **14-50**
- Clear the LOF Alarm on the XTC-14 Card **14-50**
- Clear the LOF Alarm on the XTC-28-3 Card **14-51**
- Clear the LOF Alarm on an OC-N Card **14-52**
- Clear the LOGBUFR90 Alarm **14-52**
- Clear the LOGBUFROVFL Alarm **14-53**
- Clear the LOP-P Alarm **14-54**
- Clear the LOP-V Alarm on the XTC Card **14-55**
- Clear the LOS Alarm **14-56**
- Clear the LOS Alarm on the XTC Card **14-56**
- Clear the LOS Alarm on an OC-N Card **14-57**
- Clear the LBKFACILITY Condition on the XTC-28-3 Card **14-59**
- Clear the LBKFACILITY Condition on the OC-N Card **14-60**
- Clear the LPBKTERMINAL Condition on an XTC Card **14-60**
- Clear the Manual Switch and the MAN-REQ Condition on an OC-N Card **14-61**
- Clear the MEA Alarm on the AIP **14-61**

- Clear the MEA Alarm **14-62**
- Clear the MEA Alarm on the Fan-Tray Assembly **14-63**
- Clear the MFGMEM Alarm on the AIP, Fan Tray, or Backplane **14-64**
- Clear the NOT-AUTHENTICATED Alarm on the XTC Card **14-65**
- Clear the PDI-P Condition **14-66**
- Clear the PEER-NORESPONSE Alarm Reported on XTC or OC-N Card **14-67**
- Clear the PLM-P Alarm Reported on the XTC Card **14-67**
- Clear the PLM-V Alarm on the XTC-14 or XTC-28-3 Card **14-68**
- Clear the PRC-DUPID Alarm on an OC-N Card in a BLSR **14-69**
- Clear the RAI Condition on XTC-28-3 Cards in C-bit Format **14-69**
- Clear the RCVR-MISS Alarm on the XTC-14 Port **14-70**
- Clear the RFI-L Condition on the OC-N Card **14-70**
- Clear the RFI-P Condition on the XTC or E10/100-4 Card **14-71**
- Clear the RFI-V Condition on the XTC Card **14-71**
- Clear the RING-MISMATCH Alarm **14-72**
- Clear the SD-L Condition on an OC-N Card **14-73**
- Clear the SD-P Condition on an OC-N Card **14-74**
- Clear the SF-L Condition on an OC-N Card **14-75**
- Clear the SF-P Condition on an OC-N Card **14-76**
- Clear the SFTWDOWN-FAIL Alarm on the XTC Card **14-77**
- Clear the SNTP-HOST Alarm **14-78**
- Clear the SQUELCH Condition **14-78**
- Clear the SSM-FAIL Alarm **14-79**
- Clear the STU Condition **14-79**
- Clear the SWTOSEC Condition **14-80**
- Clear the SWTOTHIRD Condition **14-80**
- Clear the SYNCPRI Condition on the XTC Card **14-81**
- Clear the SYNCSEC Alarm on the XTC Card **14-81**
- Clear the SYNCTHIRD Alarm on the XTC Card **14-82**
- Clear the TIM-P Alarm **14-83**
- Clear the TRMT Alarm on the XTC-14 Card **14-83**
- Clear the TRMT-MISS Alarm **14-84**
- Clear the UNEQ-P Alarm on the Line Card **14-84**
- Clear the UNEQ-V Alarm on the XTC-14 and XTC-28-3 Card **14-86**
- Label Requirements **B-1**

Label Requirements **B-4**

Contacting TAC by Using the Cisco TAC Website **B-18**

Contacting TAC by Telephone **B-18**



About This Manual

This section explains who should read the *Cisco ONS 15327 User Documentation Release 3.3*, how the document is organized, related documentation, document conventions, how to order print and CD-ROM documentation, and how to obtain technical assistance.

Audience

This guide is for Cisco ONS 15327 technicians and administrators who are responsible for installing, configuring, maintaining, and enhancing ONS 15327 networks.

Organization

Chapter	Description
Chapter 1, “Hardware Installation”	Provides rack installation and power instructions for the ONS 15327, including component installation such as cards and cables.
Chapter 2, “Software Installation”	Explains how to install the ONS 15327 software application and use its graphical user interface (GUI).
Chapter 3, “Node Setup”	Explains how to provision a node, including setting up timing, protection, and security and storing general node and network information.
Chapter 4, “IP Networking”	Explains how to set up ONS 15327’s in internet protocol (IP) networks and provides scenarios showing nodes in common IP configurations. It explains how to create static routes and use the Open Shortest Path First (OSPF) protocol.
Chapter 5, “SONET Topologies”	Provides instructions for configuring UPSRs, BLSRs, subtending rings, linear 1+1 ADM protection, PPMNs, and DCC tunnels.
Chapter 6, “Circuits and Tunnels”	Describes how to create standard STS and VT1.5 circuits as well as VT tunnels, multiple drop circuits, and monitor circuits. The chapter also explains how to edit UPSR circuits and create path traces to monitor traffic.

Chapter	Description
Chapter 7, “Card Provisioning”	Provides procedures for changing the default transmission parameters for ONS 15327 electrical and optical cards.
Chapter 8, “Performance Monitoring”	Provides performance monitoring thresholds for ONS 15327 electrical and optical cards.
Chapter 9, “Ethernet Operation”	Explains how to use the Ethernet features of the ONS 15327, including transporting Ethernet traffic over SONET, creating and provisioning VLANs, protecting Ethernet traffic, provisioning Multicard and Single-card EtherSwitch, provisioning several types of Ethernet circuits, viewing Ethernet performance data, and creating Ethernet remote monitoring (RMON) alarm thresholds.
Chapter 10, “Alarm Monitoring and Management”	Explains how to view and manage alarms with CTC, which includes viewing current and historical alarm data, creating alarm profiles, and suppressing alarms. To find procedures for clearing CTC alarms, refer to the “Alarm Troubleshooting” chapter.
Chapter 11, “SNMP”	Explains how Simple Network Management Protocol (SNMP) is used with the ONS 15327.
Chapter 12, “Maintenance”	Explains how to perform several routine hardware and software maintenance procedures.
Chapter 13, “Card Reference”	Provides a functional description, illustration, block diagram, and the specifications for every ONS 15327 card.
Chapter 14, “Alarm Troubleshooting”	Alphabetically lists the alarms generated by the ONS 15327 and provides troubleshooting procedures for each alarm.
Appendix A, “Acronyms”	Defines commonly-used abbreviations
Appendix B, “Regulatory Compliance and Safety Requirements for the Cisco ONS 15327”	Lists customer, industry, and government requirements met by the Cisco ONS 15327
Glossary	Defines commonly-used terms

Related Documentation

Release Notes for Cisco ONS 15327 Release 3.3

Cisco ONS 15327 Product Overview

Cisco ONS 15327 Common TL1 Command Quick Reference Card

Cisco ONS 15327 Quick Reference Guide

Related products:

Cisco ONS 15454 User Documentation

Installing the Cisco ONS 15216 DWDM Filters

Cisco ONS 15454 Product Overview

Cisco Warranty Services for ONG Products

Cisco ONS 15454 Quick Configuration Guide

Cisco ONS 15454 Quick Installation Guide

Conventions

The following conventions are used throughout this publication:



Note

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



Caution

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



Warning

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



Tip

Means the information might help you solve a problem.

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

Obtaining Documentation

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

World Wide Web

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

- <http://www.cisco.com>

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

Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including the *Cisco ONS 15327 User Documentation*, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM, a member of the Cisco Connection Family, is updated as required. Therefore, it might be more current than printed documentation. To order additional copies of the Optical Networking Product Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation, including the Optical Networking Product CD-ROM, from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



Hardware Installation

This chapter provides procedures for installing the Cisco ONS 15327. Chapter topics include:

- Installation Equipment
- Rack Installation
- Fan-Tray Assembly Installation
- Power and Ground Installation
- Card Installation and Turn-Up
- Cable Description and Installation
- Hardware Specifications



Note

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



Warning

The ONS 15327 is intended for installation in restricted access areas. In a restricted access area, service personnel can gain access only using a special tool, lock, key, or other means of security. A restricted access area is controlled by the authority responsible for the location.



Warning

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



Warning

Only trained and qualified personnel should install or replace this equipment.



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, 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 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 quickly determine if any alarms are present on the assembly.

The ONS 15327 is powered using -48V DC 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.

Table 1-1 lists the tasks required to install an ONS 15327.

Table 1-1 Installation Tasks

Task	Reference
Mount the ONS 15327 in the rack.	See the “Rack Installation” section on page 1-4.
Install the fan-tray assembly.	See the “Fan-Tray Assembly Installation” section on page 1-8.
Ground the equipment.	See the “Power and Ground Installation” section on page 1-10.
Install the MICs	See the “Card Installation and Turn-Up” section on page 1-16.
Run the power cables and fuse the power connections.	See the “Power and Ground Installation” section on page 1-10.
Install the XTC cards	See the “Card Installation and Turn-Up” section on page 1-16.
Install the optical and electrical cards	See the “Card Installation and Turn-Up” section on page 1-16.
Install cables	See the “Cable Description and Installation” section on page 1-21.

1.2 Installation Equipment

You will need the following tools and equipment to install and test the ONS 15327.

1.2.1 Included Materials

These materials are shipped with the ONS 15327. The number in parentheses provides the quantity of the item included in the package.

- #12-24 x 1/2 pan head phillips mounting screws (4)

- #10-32 x 3/8 pan head phillips power lug screws (2)
- #12 AWG dual hole 5/8 in. spaced grounding lug
- Electrostatic discharge (ESD) wrist strap with 1.8 m (6 ft.) coil cable (1)

1.2.2 User-Supplied Materials

These materials and tools are required but are not supplied with the ONS 15327.

- Equipment rack (22 inches total width for a 19-inch rack; 26 inches total width for a 23-inch rack)
- Fuse panel
- Copper power cable (from fuse and alarm panel to assembly), #12-16 AWG
The National Electrical Code recommends #12-14 AWG power cable.
- Ground cable, #12 AWG stranded (minimum)
- Alarm cable, category 5 terminated with RJ-45 for all alarm connections
- Building Integrated Timing Supply (BITS) clock cable, category 5 terminated with RJ-45
- Single-mode SC fiber jumpers with UPC polish (55 dB or better) for OC12 and OC-48 cards and fiber jumpers with LC connectors for the OC-3 card.
- Shielded coaxial cable terminated with BNC connectors for DS-3 cards
- Shielded ABAM cable terminated with CHAMP connectors for DS-1 cards with #22 or #24 AWG ground wire (typically about two feet in length)
- Tie wraps and/or lacing cord
- Labels

1.2.2.1 Tools Needed

- #2 phillips screw driver
- Medium slot head screw driver
- Small slot head screw driver
- Wire cutters
- Wire strippers
- Crimp tool
- Needle nose pliers (for bail locks on CHAMP connectors)

1.2.2.2 Test Equipment

- Volt meter
- Power meter (for use with fiber optics only)
- Bit Error Rate (BER) tester, DS-1 and DS-3

**Note**

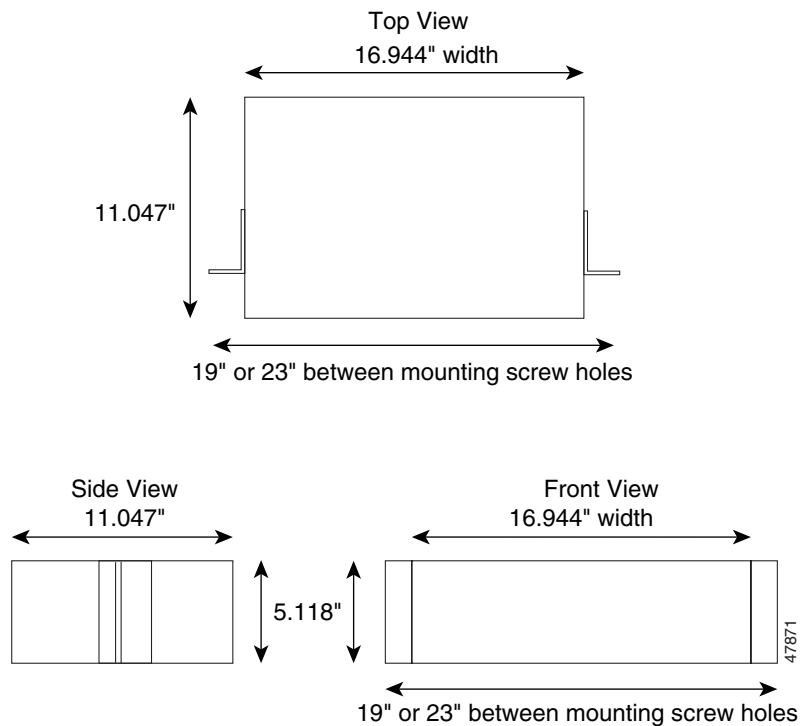
In this chapter, the terms “ONS 15327” and “shelf assembly” are used interchangeably. In the installation context, these terms have the same meaning. Otherwise, shelf assembly refers to the physical steel enclosure that holds cards and connects power, and ONS 15327 refers to the entire system, both hardware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

1.3 Rack Installation

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 The ONS 15327 shelf assembly dimensions



1.3.1 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**

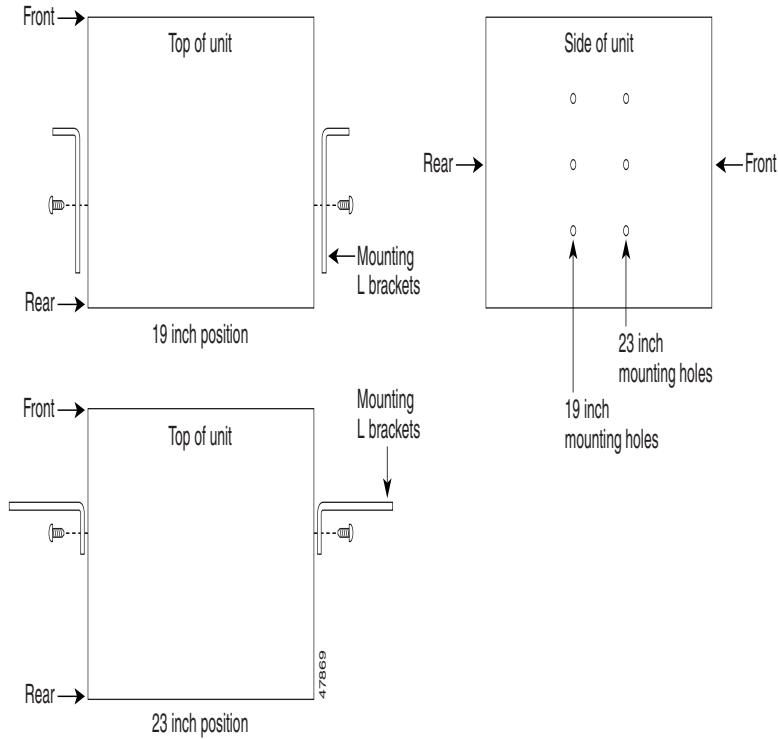
When mounting the ONS 15327 in a frame with a non-conductive coating (such as paint, lacquer, or enamel) use either the thread-forming screws provided with the ONS 15327 shipping kit or remove the coating from the threads to ensure electrical continuity.

The shelf assembly comes with mounting brackets that can be reversed for use with a 19- or 23-inch rack. The following steps describe how to reverse the shelf assembly mounting bracket to fit a 19- inch rack.

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

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

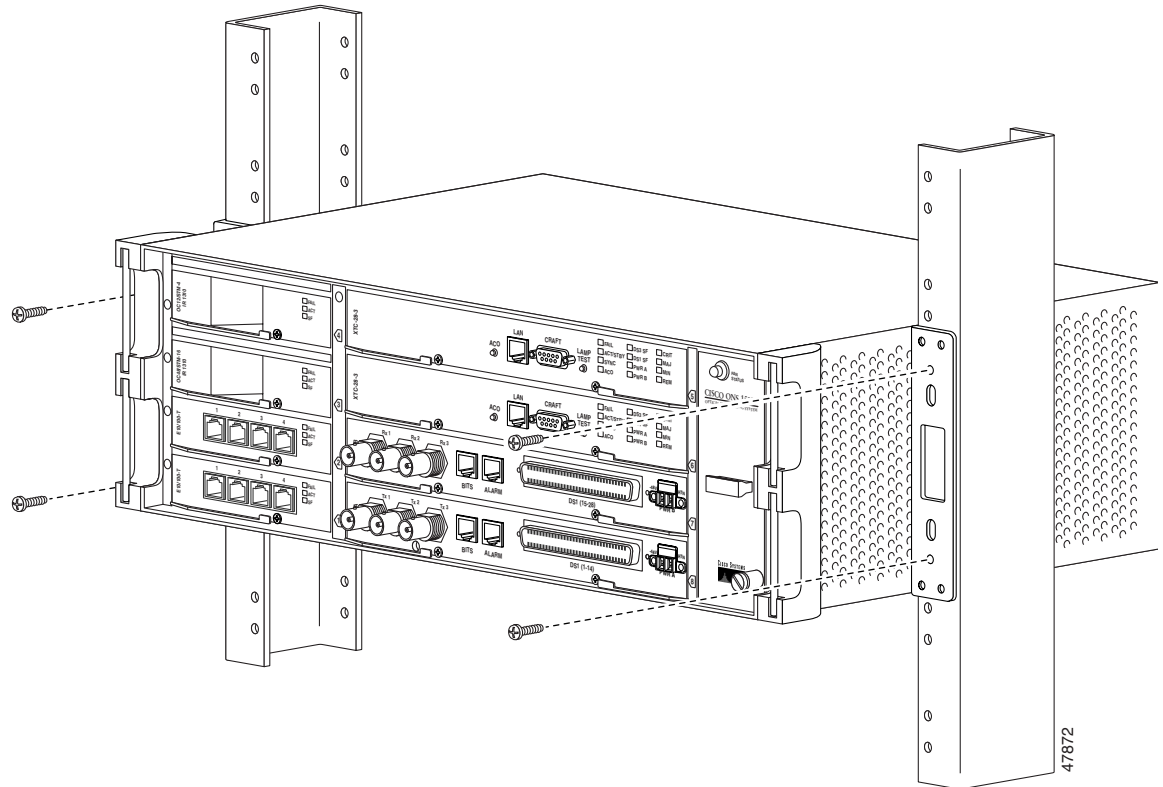
Figure 1-2 Reversing the mounting brackets (23-inch position to 19-inch position)



1.3.2 Mounting a Single Node

Mounting the ONS 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



One person can install the shelf assembly using the mounting screws provided. For easier lifting, the shelf should be empty of cards and the fan tray.

Procedure: Mount the ONS 15327 in a Rack

-
- Step 1** Ensure that the shelf assembly is set for the desired rack size (either 19 or 23 inches).
 - Step 2** Lift the shelf assembly to the desired rack position.
 - Step 3** Align the screw holes on the mounting ears with the mounting holes in the rack.
 - Step 4** Install one mounting screw in each side of the assembly.
You should use at least one set of the horizontal screw slots on the mounting brackets to prevent future slippage.
 - Step 5** When the shelf assembly is secured to the rack, install the remaining mounting screws.
-

1.3.3 Mounting Multiple Nodes

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

Procedure: Mount Multiple ONS 15327s in a Rack

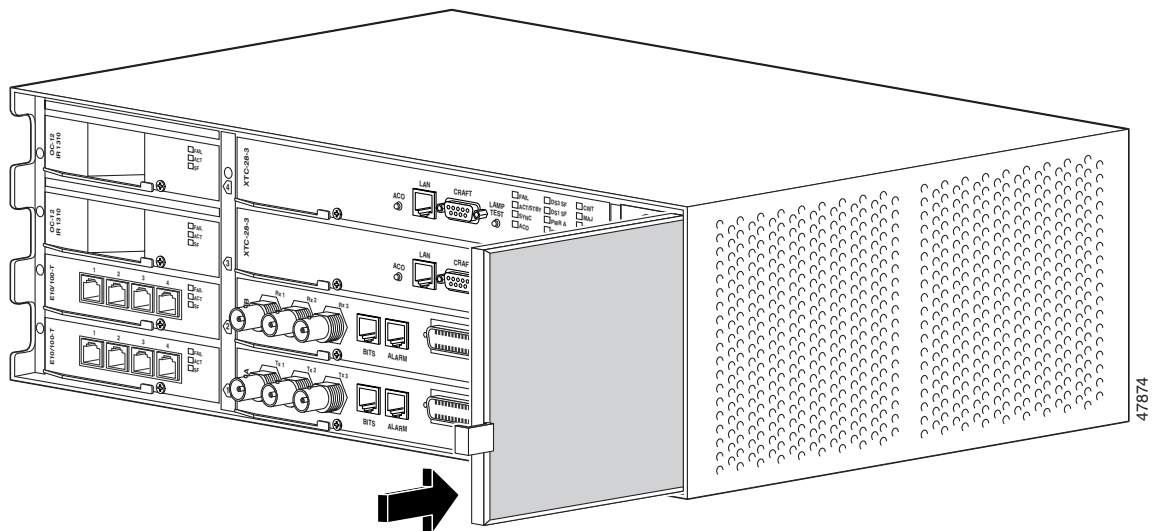
-
- Step 1** Install the fuse and alarm panel at the top.
 - Step 2** Mount the first ONS 15327 directly below the fuse and alarm panel.
 - Step 3** Repeat the procedure with the remainder of the ONS 15327s.
-

1.4 Fan-Tray Assembly Installation

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

The fan-tray assembly has an air filter on the right side of the fan tray that you can install and remove by hand. Remove and visually inspect this filter every 30 days. For inspection procedures, refer to the “Air Filter Inspection and Replacement” section on page 12-2. 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.

Figure 1-4 Removing or replacing the fan-tray air filter



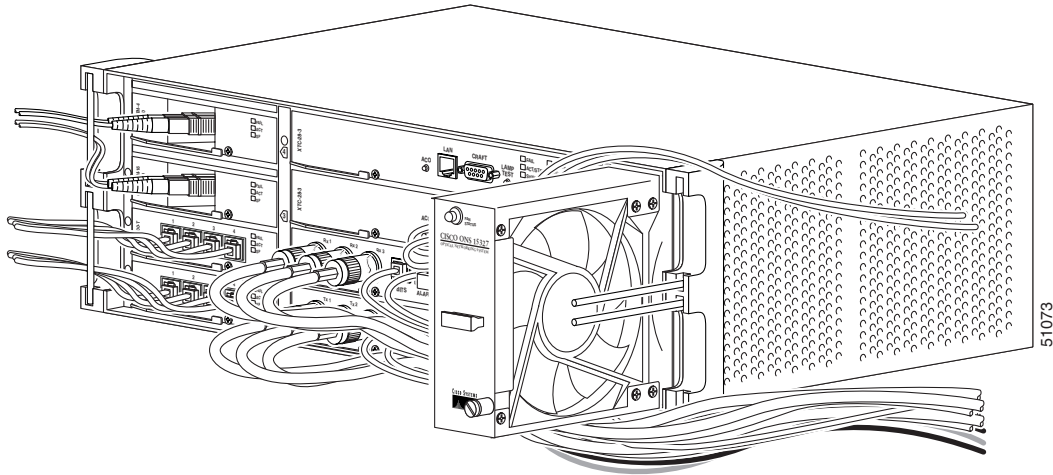
Caution

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.

Procedure: Install the Fan-Tray Assembly

-
- Step 1** If cables are installed, move them away from the fan tray slot.

Figure 1-6 Removing a fan-tray assembly with installed cables



If the fan fails on the fan-tray assembly, replace the entire assembly. You cannot replace an individual fan. The FAN STATUS LED turns red when one or more fans fail. For a procedure that replaces the fan tray, see the “Install the Fan-Tray Assembly” section on page 1-8.

1.5 Power and Ground Installation

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.

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

**Note**

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

The ONS 15327 has redundant -48V DC power terminals on the MICs. 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.

Procedure: Install Redundant Power Feeds

Step 1 Terminate the chassis ground to either the office ground or rack ground.

The ground connection point is located on the left-hand side panel as you face the ONS 15327.

**Note**

To ensure that the equipment is properly grounded, use the provided 12 AWG dual-hole grounding lug and the #10-32 x 3/8 pan head phillips power lug screws to connect the ground cable to the chassis. Apply 30-36 in.-lbs of torque when tightening the screws.

Step 2 Measure and cut the cables as needed to reach the ONS 15327 from the fuse panel. Use the correct size fuse for each power lead.

Step 3 Dress the power and ground cables according to local site practice.

**Warning**

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

Step 4 Strip .22 inches of insulation from all power cables that you connect to the ONS 15327 power connectors.

Step 5 Install MICs in Slots 7 and 8.

See the “Card Installation and Turn-Up” section on page 1-16 for installation in instructions.

**Warning**

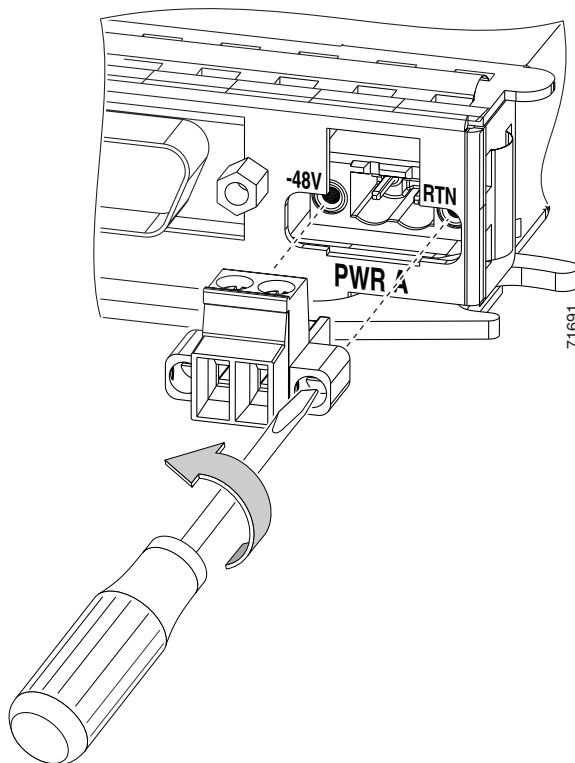
Do not expose more than .22 inches of bare wire on power cables.

**Caution**

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

Step 6 Remove the connector from the slot by grasping it with your fingers and gently pulling it. If you cannot remove it easily, you can use a pair of needle nose pliers and grab it by the center of the channel. Figure 1-7 shows the MIC power connector being removed.

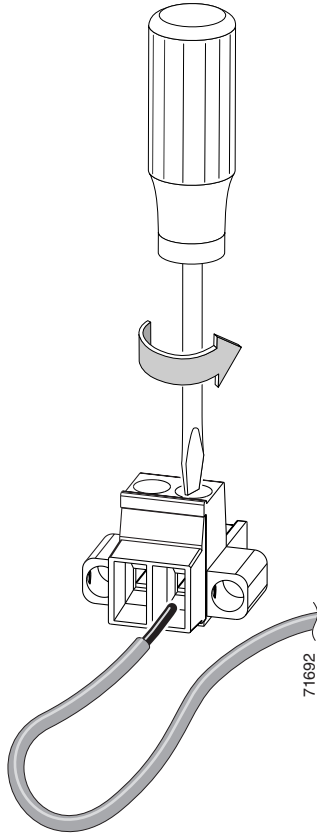
Figure 1-7 Removing the MIC power connector



Step 7 Remove the cable fastening screws (the screws on the top of the connector that become visible when the connector is removed).

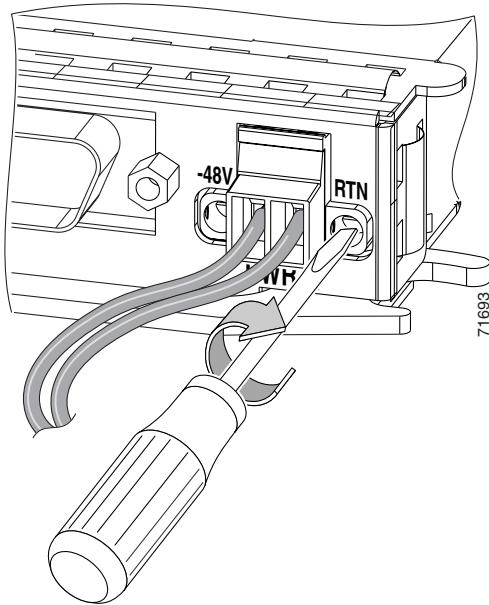
- Step 8** Insert the return (black) wire into the right hand (RTN) slot of the connector. Figure 1-8 shows a power cable being inserted into the MIC power connector.

Figure 1-8 Inserting a power cable into the MIC power connector



- Step 9** Replace the cable fastening screw for the return (RTN) wire and tighten with a small slot head screwdriver.
- Step 10** Insert the battery (red) wire into the left hand (-48V) slot of the connector.
- Step 11** Replace the cable fastening screw for the battery (-48V) wire and tighten with the screwdriver.
- Step 12** Insert the connector back into the slot on the MIC and tighten the screws with the screwdriver. Figure 1-9 shows the MIC power connector being installed.

Figure 1-9 Installing the MIC power connector

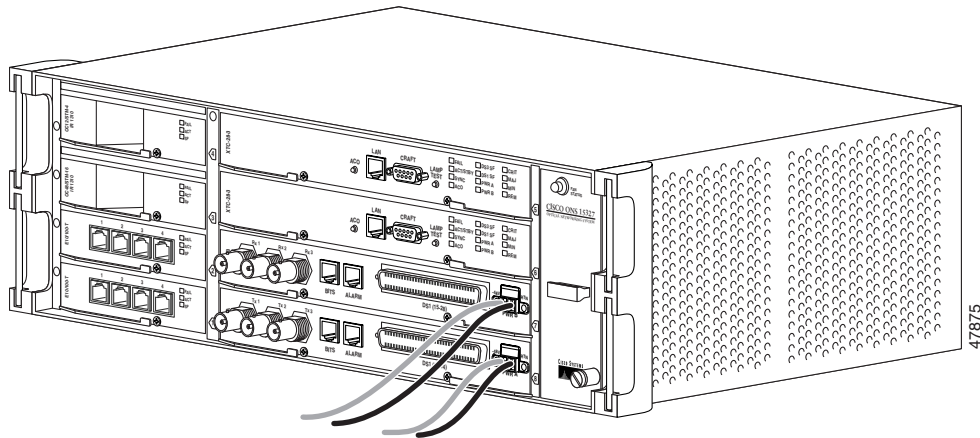


Step 13 Use a small flat-head screwdriver to open the return (RTN) terminal and insert the return lead.

Step 14 If you use redundant power leads, repeat Steps 6– 13 on the other MIC.

Figure 1-10 shows redundant power connected to an ONS 15327.

Figure 1-10 Redundant power connected to an ONS 15327



1.5.1 Ferrite Installation

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.

Procedure: Attach Ferrites to Power Cabling

Use a single block ferrite Fair Rite 0443164151 for each pair of cables.

-
- Step 1** Wrap the cables once around and through the block ferrites.
- Step 2** Place the block ferrite within 5 to 6 inches of the power terminals.
-

1.6 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, See the “Alarm Cable Installation” section on page 1-27. For procedures that resolve alarms, refer to Chapter 14, “Alarm Troubleshooting.”

1.7 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 1-2 lists the pin assignments for the BITS timing pin fields. For more information about connecting BITS timing to the ONS 15327, See the “BITS Cable Installation” section on page 1-28.

Table 1-2 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

Table 1-2 External Timing Pin Assignments for BITS (continued)

External Device	Contact	RJ-45 Pin	Tip & Ring	Function
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

1.8 Card Installation and Turn-Up

**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 1-11 shows XTC card installation (which is the same as MIC installation) and Figure 1-12 shows high-speed card installation.

**Warning**

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

**Warning**

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

**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.

1.8.1 Slot Requirements

The ONS 15327 shelf assembly has eight card slots; four high speed slots, two Cross-Connect, Timing and Control (XTC) slots, and two Mechanical Interface Card (MIC) slots. The wider slots host the XTC cards and MICs. The narrower, high-speed 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 13, “Card Reference,” for more information about ONS 15327 cards.

Table 1-3 lists the number of ports, line rates, connector options, and connector locations for ONS 15327 optical and electrical cards.

Table 1-3 Card Ports, Line Rates, and Connectors

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
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

Procedure: Install ONS 15327 Cards

-
- Step 1** Open the card ejectors.
 - Step 2** Slide the cards along the guide rails into the desired card slot.
 - Step 3** Close the ejectors.
 - Step 4** Lock the cards into place by tightening the ejector locking screws.
-

Figure 1-11 Installing an XTC card (XTC 28-3)

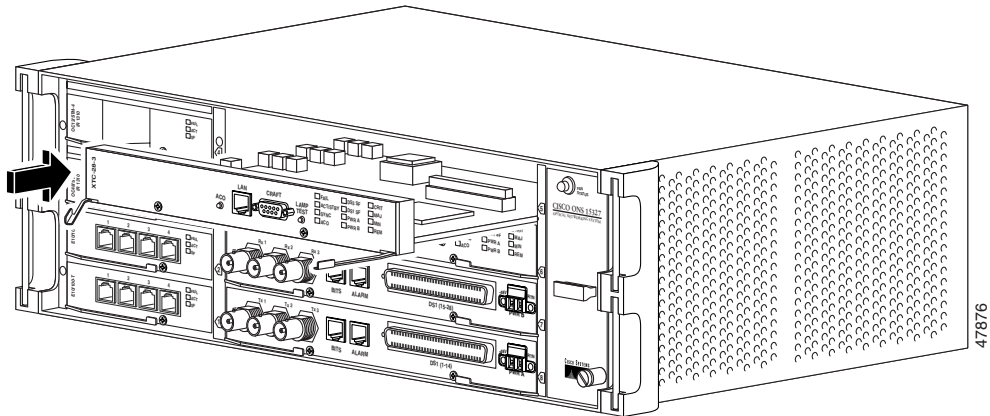
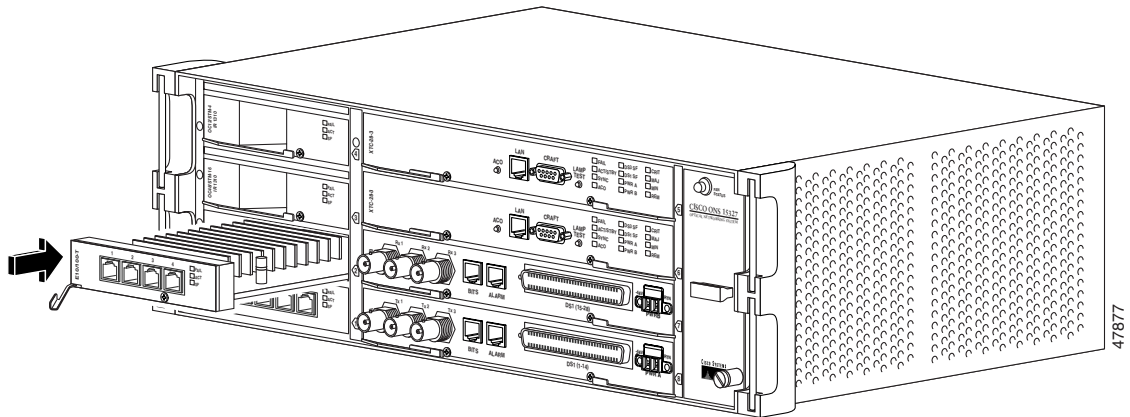


Figure 1-12 Installing a high-speed card (E10/100-T)

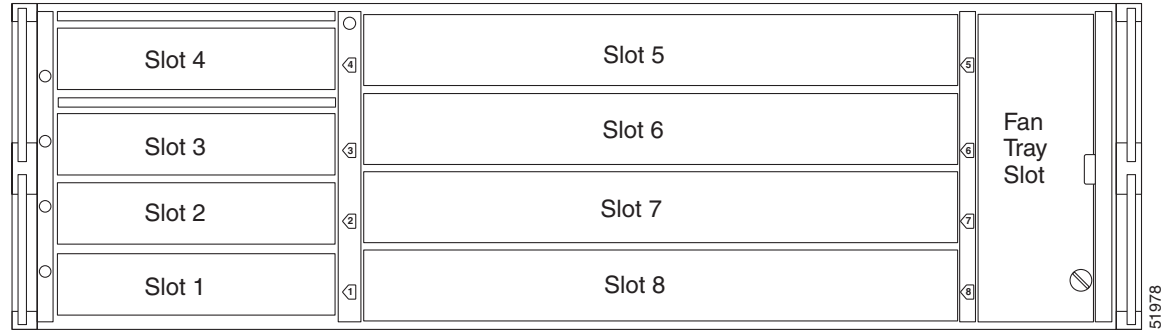


1.8.2 Card Turn-Up

The procedure for turning up ONS 15327 cards is slightly different for each card. Before installing any XTC or high-speed 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 high-speed cards after you have successfully installed and turned up the XTC cards and MICs. Follow the steps in this section to verify card turn-up.

The card turn-up procedures reference the slot numbers for the ONS 15327. Figure 1-13 shows the location and corresponding number of each slot.

Figure 1-13 ONS 15327 slot numbering

**Note**

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

Procedure: Verify Successful Turn-Up of MICs

- Step 1** Install MIC A in Slot 8.
- The slots are keyed to ensure that cards are installed in the correct slot.
- Step 2** Verify that the power and ground cables are installed correctly.
- Step 3** With power applied to MIC A, insert the fan-tray assembly and verify that the fans activate.
- The fans will only activate if at least one XTC card is installed.
- Step 4** If you require redundant power, more than 14 DS-1s, or you are using DS-3s, install MIC B in Slot 7. If MIC B is not required, proceed to Step 7.
- Step 5** With power applied to MIC B, unplug MIC A from the backplane (do not remove it completely) and verify that the fans are still running.

**Warning**

Disconnect power before removing MICs from the ONS 15327.

- Step 6** Plug MIC A back into the backplane and reconnect power.
- Step 7** Verify that the card appears in the correct slot on the CTC node view (default login) screen.
- Step 8** Verify that the card is white on the CTC node view screen.
- Step 9** If MIC A was unplugged in Step 5, plug it back into the backplane and verify that it appears in the correct slot and is white on the CTC node view screen.

Refer to Chapter 2, “Software Installation,” for more information about using CTC.

Procedure: Verify Successful Turn-Up of XTC Cards

-
- Step 1** Install an XTC in Slot 6.
Slot 6 is the working XTC slot.
 - Step 2** Verify that the red FAIL LED blinks for approximately 30 seconds.
 - Step 3** Verify that all LEDs blink once and turn off.
 - Step 4** Verify the ACT/STBY LED is green (active).
 - Step 5** Install the second XTC in Slot 5.
Slot 5 is the protect XTC slot.
 - Step 6** After the LED boot sequence (Steps 3 and 4), verify that the ACT/STBY LED is yellow. The yellow LED indicates that the second XTC is the standby XTC.
 - Step 7** Press the LAMP TEST button on the faceplate of each XTC and verify that all LEDs illuminate while you press the button.
 - Step 8** Verify that the card appears in the correct slot on the CTC node view screen.
 - Step 9** Verify that the card is white on the CTC node view screen.
Refer to Chapter 2, “Software Installation” for more information about using CTC.
-

Procedure: Verify Successful Turn-Up of High-Speed Cards

-
- Step 1** Install a high speed card in Slots 1–4.
 - Step 2** Verify that the red FAIL LED turns on and remains lit for 20 to 30 seconds.
 - Step 3** Verify that the red FAIL LED blinks for 30 to 45 seconds.
 - Step 4** Verify that all LEDs blink once and turn off for 5 to 10 seconds.
 - Step 5** Verify the ACT LED turns on.
 - Step 6** Verify that the card appears in the correct slot on the CTC node view screen.
-



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.

1.8.3 Card Software Installation

After you install an ONS 15327 card in a valid card slot, the card’s software automatically updates to the version that operates correctly with the software installed on the XTC. To verify the current version of software installed on the XTC, click **Help** and then click **About CTC**. Refer to Chapter 2, “Software Installation” for more information about using CTC.

**Note**

Always point your browser to the node running the most recent release (version) of CTC. CTC is backward compatible but not forward compatible.

1.9 Cable Description and Installation

This section explains how to install fiber-optic, DS-3 (coaxial), DS-1 (CHAMP), and twisted-pair cables.

1.9.1 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 1-23). 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.
- **CHAMP Cables:** CHAMP cables connect to MICs on the ONS 15327 using CHAMP cable connectors. Each CHAMP connector on the MIC supports one 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 1-25 for more information about the CHAMP cables and connectors.
- **Twisted-pair Cables:** Twisted-pair cables connect to the ports on the Ethernet card, the Alarm and BITS ports on the MICs, and the LAN port on the XTCs. The twisted-pair cables use RJ-45 connectors. The Ethernet card ports and the LAN ports use a standard straight-through cable. Connecting to either the BITS or Alarm ports requires special cables described in the “Alarm Cable Installation” section on page 1-27 and the “BITS Cable Installation” section on page 1-28.

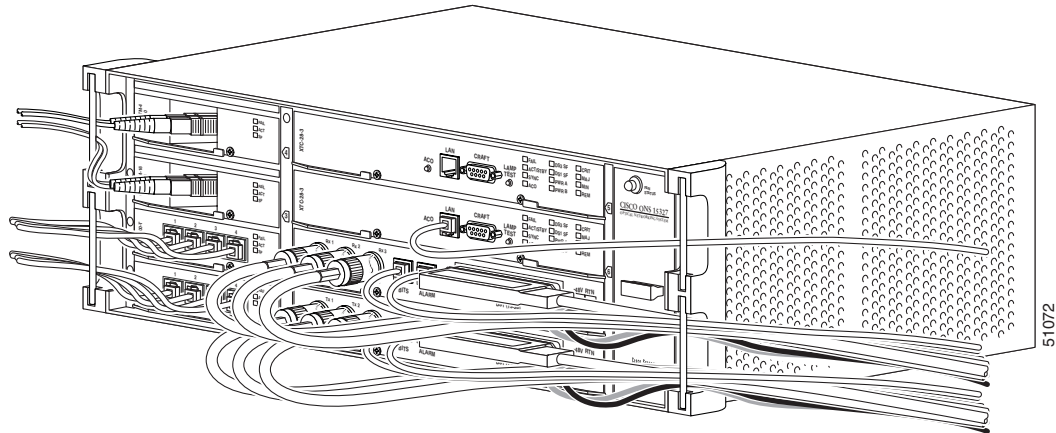
1.9.2 Cable Installation Overview

Because the ONS 15327 supports a large number of interfaces on the front panel, proper cable management and the correct cabling sequence during installation are required.

1.9.2.1 Cable Guides

The ONS 15327 has cable guides located on each side of the front of the shelf assembly. 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 1-14 Managing front panel cables with locking cable guides



1.9.2.2 Cabling Sequence and Location

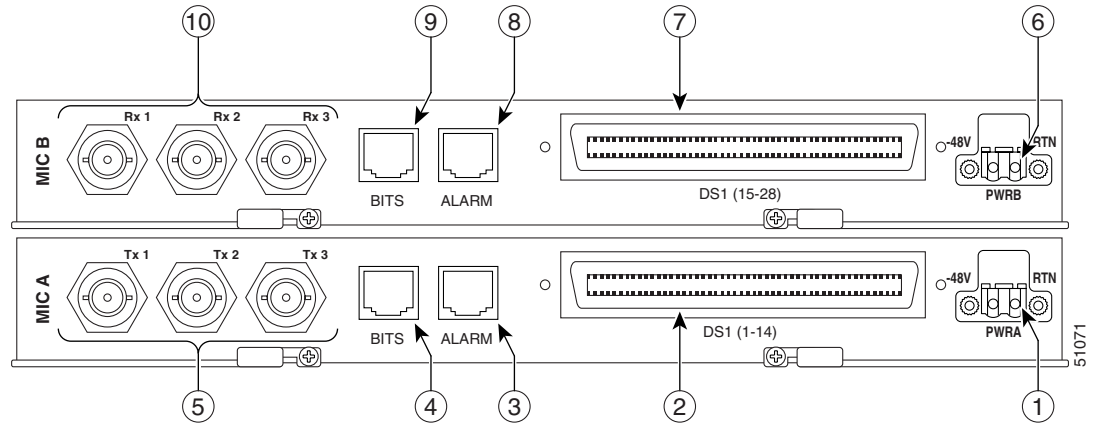
The two cable management considerations are the sequence of cable installation and the location of cable routing. To maintain access to all of the connectors during cable installation, cables must be attached to the MICs in the following order starting with MIC A (the bottom MIC) and repeating for MIC 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 XTCs and high-speed cards in any particular order. Route XTC cables through the top right cable guide. Route high-speed cables out through the corresponding cable guides on the left-hand side of the shelf assembly. Figure 1-15 shows the order in which you should install cables on the ONS 15327.

Figure 1-15 The cable installation sequence



1.9.3 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 high-speed and XTC slots.

ONS 15327 OC-12 and OC-48 cards have SC connectors and the OC-3 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. On ONS 15327 OC-12 and OC-48 card ports, the left-hand connector is the transmit port and the right-hand 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.

Procedure: Install and Route Fiber-Optic Cables in the ONS 15327

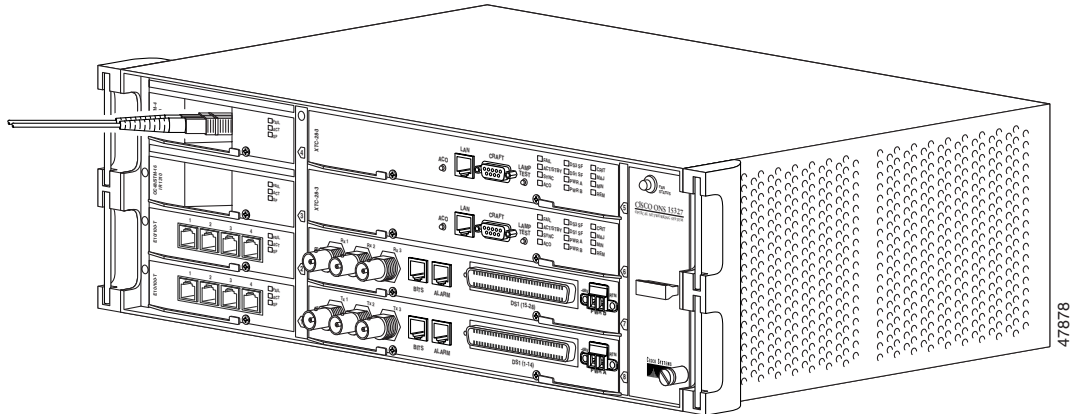
- Step 1** Place the SC connector in front of the connection point on the card faceplate. Each card supports at least one transmit and one receive connector to create an optical carrier port. Figure 1-16 shows the cable location.



Note

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

Figure 1-16 Installing a fiber-optic cable



- Step 2** Align the keyed ridge of the cable connector with the receiving slot on the faceplate connection point.
- Step 3** Gently push the cable connector into the faceplate connection point until the connector snaps into place.
- Step 4** Route fiber cables out through the cable guides on the side of the shelf assembly.
- See the “Cable Guides” section on page 1-21 for more information about cable management.

1.9.4 Coaxial Cable Installation

DS-3s connect to the ONS 15327 using 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.



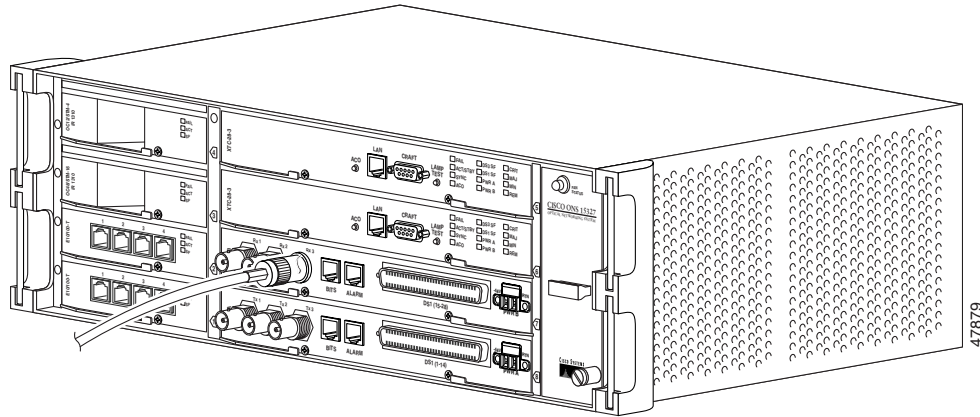
Caution

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.

Procedure: Install Coaxial Cable With BNC Connectors

- Step 1** Place a BNC cable connector over the desired connector on the MIC.
- Figure 1-17 shows how to connect a coaxial cable to the ONS 15327 MIC.

Figure 1-17 Installing a coaxial cable with BNC connectors



- Step 2** Position the cable connector so that the slot in the connector is above the corresponding notch on the MIC connection point.
- Step 3** Gently push the connector down until the notch on the MIC connector slides into the slot on the cable connector.
- Step 4** Turn the cable connector until the notch clicks into place.
- Step 5** Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice.

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

1.9.5 DS-1 Cable Installation

DS-1s support CHAMP connector cabling. This section provides information about the DS-1 cables and connectors.

Installing CHAMP connector DS-1 cables requires 64-pin bundled cable connectors with a 64-pin female CHAMP connector. You need CHAMP connector #552276-1 for the receptacle side and #1-552496-1 for the right-angle shell housing, or their functional equivalents. The corresponding 64-pin male CHAMP connector on the MIC supports one receive (in) and one transmit (out) for each DS-1 port for the corresponding XTC.

Because each DS1-14 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 1-4 shows the pin assignments for the CHAMP connectors on the ONS 15327 MICs.

Table 1-4 Pin Assignments for CHAMP Connector (the shaded area corresponds to the white/orange binder group)

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 yellow/orange	17	49	Rx Ring 1 orange/yellow
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 yellow/green	18	50	Rx Ring 2 green/yellow

Table 1-4 Pin Assignments for CHAMP Connector (the shaded area corresponds to the white/orange binder group) (continued)

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 yellow/brown	19	51	Rx Ring 3 brown/yellow
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 yellow/slate	20	52	Rx Ring 4 slate/yellow
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare 0+ N/A	15	47	Tx Spare 0- N/A	Rx Spare 0+ N/A	31	63	Rx Spare 0- N/A
Tx Spare 1+ N/A	16	48	Tx Spare 1- N/A	Rx Spare 1+ N/A	32	64	Rx Spare 1- N/A

**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.

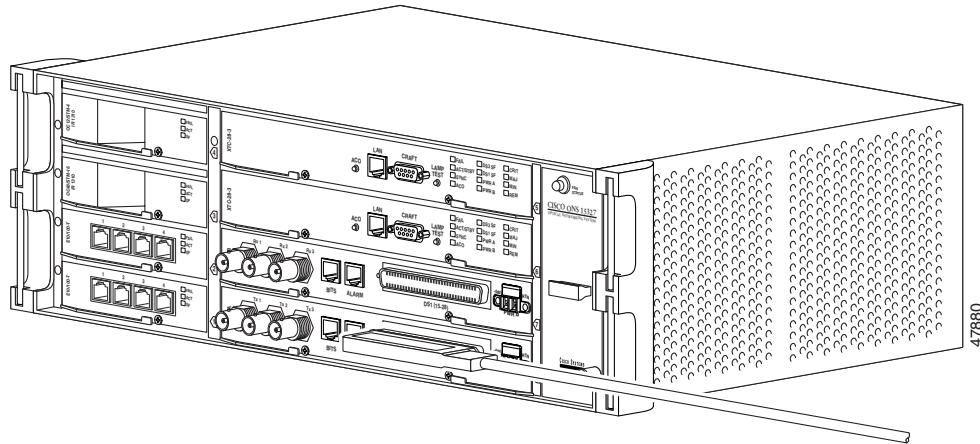
Procedure: Install DS-1 CHAMP Cables on a MIC

- Step 1** Prepare a 56-wire cable for each DS-1 connection you will make. See Table 1-4 for the ONS 15327 CHAMP connector pin assignments.
- Step 2** Connect the male CHAMP connector on the cable to the female CHAMP connector on the ONS 15327 MIC.

Figure 1-18 shows DS-1 cable installation.

Step 3 Use the screws on the male CHAMP connector to secure the connection.

Figure 1-18 Installing a DS-1 cable



1.9.6 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.

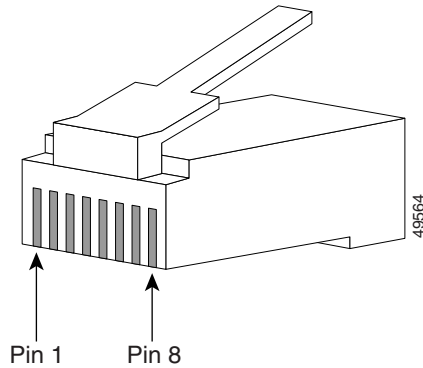
The pins on the ALARM port correspond to the six external alarm inputs and the two external alarm outputs (controls) that can you can define using CTC (for procedures, refer to the “Using Virtual Wires” section on page 7-17). Alarms 2, 4, and 6 correspond to MIC A and alarms 1, 3, and 5 correspond to MIC B. Alarm output 1 corresponds to MIC B and alarm output 2 corresponds to MIC A. Table 1-5 shows the input alarm pinouts and the corresponding alarm numbers assigned to each MIC/port. Table 1-6 shows the output alarm pinouts. Refer to these tables when connecting alarm cables to the ONS 15327. See Figure 1-19 for RJ-45 pin numbering.

Table 1-5 Alarm Input Pin Assignments

Alarm Number (MIC A)	Alarm 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 1-6 Alarm (External Control) Output Pin Assignments

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

Figure 1-19 Pins 1 and 8 on the RJ-45 connector

1.9.7 BITS Cable Installation

The BITS cables attach to the MICs using twisted-pair cables 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. See Table 1-7, Figure 1-20, and Figure 1-21 when connecting BITS cables to the ONS 15327.

Table 1-7 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 1-20 BITS In pins on the RJ-45 connector

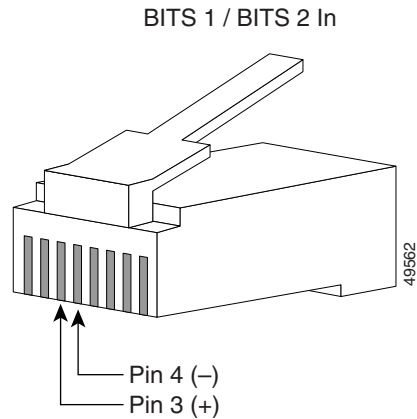
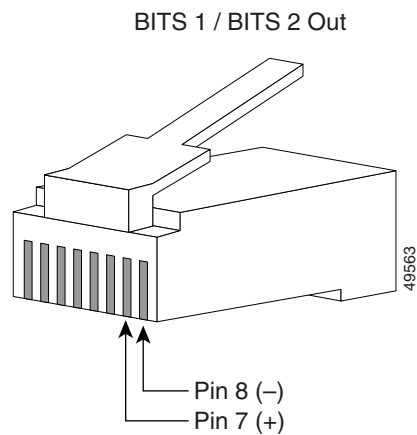


Figure 1-21 BITS Out pins on the RJ-45 connector



1.10 Hardware Specifications

1.10.1 Slot Assignments

- Total card slots: 8
- High-speed slots (Ethernet, 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
- OC-3 IR 1310
- OC-12 IR 1310
- OC-12 LR 1550
- OC-48 IR 1310
- OC-48 LR 1550

1.10.3 Configurations

- Terminal mode
- Add-drop multiplexer
- Regenerator mode
- 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: 96MB, 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: 3.7×10^{-7} /day, including temperature (< 255 slips in first 24 hours)
- Reference: External BITS, line, internal

1.10.12 Power Specifications

- Input power: -48V DC
- 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

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); 27 lbs, maximum



Software Installation

Cisco Transport Controller (CTC), the Cisco ONS 15327's software interface, is stored on the XTC card and downloads to your workstation each time you log into the ONS 15327. This chapter:

- Describes how Cisco Transport Controller (CTC) software is installed on PCs and Solaris workstations
- Tells you how to connect PCs and Solaris workstations to the Cisco ONS 15327, including direct connections, LAN connections, remote connections, and firewall-compliant connections
- Describes the CTC graphic user interface, including the three main CTC views, network, node, and card
- Explains how to create domains to manage multiple nodes, change the network view background color and image (map), and add a node to the network map
- Describes the different ways you can invoke commands within CTC
- Explains how to print and export CTC data

2.1 Installation Overview

ONS 15327 provisioning and administration is performed using the Cisco Transport Controller software. CTC is a Java application that is installed in two locations:

- ONS 15327 Cross Connect Timing and Control card (XTC)
- PCs and Solaris workstations that connect to the ONS 15327

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

For PCs and Solaris workstations, CTC is downloaded from the XTC card and installed on your computer automatically after you connect to the ONS 15327. To connect to an ONS 15327, 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 installation occurs automatically:

1. A CTC launcher applet is downloaded from the XTC card to your computer's Temp directory. (If these files are deleted, they are reinstalled the next time you connect to the ONS 15327.)
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. 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 are logged into. Therefore, always log into nodes having the latest software release.

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.

2.2 Computer Requirements

To use CTC in ONS 15327 Release 3.3, your computer must have a web browser with the correct Java Runtime Environment (JRE) installed. The correct JRE for each CTC software release is included on the Cisco ONS 15327 software CD. If you are running multiple CTC software releases on a network, the JRE installed on your computer must be compatible with the different software releases. Table 2-1 shows JRE compatibility with ONS software releases.

Table 2-1 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible
ONS 15327 Release 1.0	Yes	No
ONS 15327 Release 1.0.1	Yes	Yes
ONS 15454 Release 2.2.1 and earlier	Yes	No
ONS 15454 Release 2.2.2	Yes	Yes
ONS 15454 Release 3.0	Yes	Yes
ONS 15454 Release 3.1	Yes	Yes
ONS 15454 Release 3.2	Yes	Yes
ONS 15327/ONS 15454 Release 3.3	Yes	Yes

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

Table 2-2 Computer Requirements for CTC

Area	Requirements	Notes
Processor	Pentium II 300 MHz, UltraSPARC, or equivalent	300 Mhz is the minimum recommended processor speed. You can use computers with less processor speed; however, you may experience longer response times and slower performance.
RAM	128 MB	
Hard drive	2 GB	CTC application files are downloaded from the XTC card to your computer's Temp directory. These files occupy 3-5 MB of hard drive space.
Operating System	<ul style="list-style-type: none"> PC: Windows 95, Windows 98, Windows NT 4.0, or Windows 2000 Workstation: Solaris 2.6 or 2.7 	
Web browser	<ul style="list-style-type: none"> PC: Netscape Navigator 4.51 or higher, or Netscape Communicator 4.61 or higher, or Internet Explorer 4.0 (service pack 2) or higher Workstation: Netscape Navigator 4.73 or higher 	Either Netscape Communicator 4.73 (Windows) or 4.76 (Solaris) are installed by the CTC Setup Wizard included on the Cisco ONS 15327 software and documentation CDs.
Java Runtime Environment	<p>JRE 1.2.2_05 with Java Plugin 1.2.2 minimum</p> <p>JRE 1.3.1_02 (PC) recommended</p> <p>JRE 1.3.0_01 (Solaris) recommended</p>	<p>Use JRE 1.2.2_05 if you connect to ONS 15454s running CTC Release 2.2.1 or earlier (the earliest available ONS 15327 software is CTC Release 2.3).</p> <p>Use JRE 1.3.1_02 if all ONS 15454s that you connect to are running Release 2.2.2 or later. JRE 1.3.1_02 is installed by the CTC Setup Wizard included on the Cisco ONS 15327 software and documentation CDs.</p>
Java.policy file	A java.policy file modified for CTC must be installed.	A modified java.policy file is installed by the CTC Setup Wizard included on the Cisco ONS 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 through a LAN.	

2.3 Running the CTC Installation Wizard

The ONS 15327 provides a setup wizard that installs the files needed to run CTC on PCs and Solaris workstations. You can run the setup wizard from the Cisco ONS 15327 software CD or from the Cisco ONS 15327 documentation CD. The wizard will install:

- Netscape Communicator 4.73 (Windows) or 4.76 (Solaris)
- JRE 1.3.1_02 (Windows and Solaris)
- Cisco ONS 15327 CTC online help
- Modified java.policy file

For Solaris workstations, the JRE may require patches to run properly. You can find the patch tar file in the Jre/Solaris directory on the CD. For information about installing the patches, see the Jre/Solaris/Solaris.txt file on the CD. After installing the patches, if necessary, perform the “Set Up the Java Runtime Environment for UNIX” procedure on page 2-8 to set up JRE on the workstation.

Procedure: Run the CTC Installation Wizard for Windows

Step 1 Verify that your computer has the following:

- Processor—Pentium II, 300 Mhz or faster
- RAM—128 MB
- Hard drive—2 GB is recommended. 50 MB of space must be available.
- Operating System—Windows 95, Windows 98, Windows NT 4.0, or Windows 2000

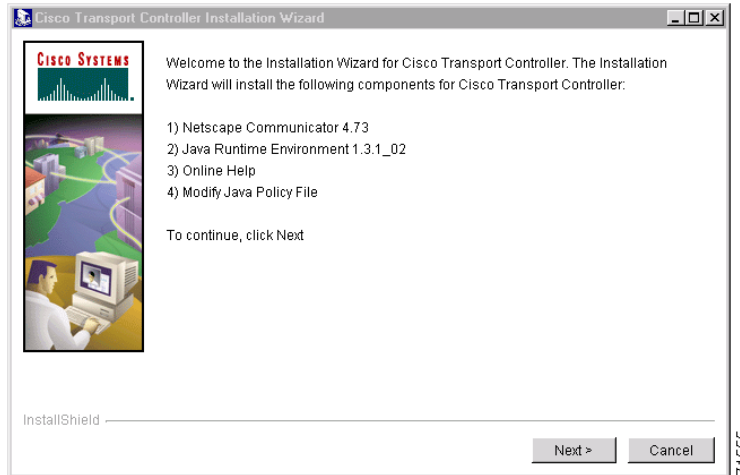


Note These requirements are guidelines. CTC performance will be faster if your computer has a faster processor and more RAM.

Step 2 Insert the Cisco ONS 15327 Release 3.3 software or documentation CD into your computer CD drive. The installation program begins running automatically. If it does not start, navigate to your computer's CD directory and double-click **setup.exe**.

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

Figure 2-1 Starting the Cisco Transport Controller Installation Wizard



- Step 3** Click **Next**.
- Step 4** For installation type, choose **Typical** to install all the components shown in Figure 2-1, or choose **Custom** if you only want to install some the components.
- Step 5** Click **Next**.
- Step 6** If you selected **Custom** in Step 4, select the CTC components you want to install by checking or unchecking the boxes, then click **Next**. If you selected **Typical**, skip this step.
- Step 7** The directory where the installation wizard will install CTC online help is displayed. The default is C:\Program Files\Cisco\CTC\Documentation.
- Step 8** If you wish to change the CTC online help directory, type the new directory path in the *Directory Name* field, or click **Browse** to navigate to the directory. If you do not wish to change the directory, skip this step.
- Step 9** Click **Next**.
- Step 10** Review the components that will be installed. If you wish to change them, click **Back**. If you have an active CTC session (for example, you are running the setup program to install additional components), close CTC before going to the next step.
- Step 11** Click **Next**. The InstallShield program begins the Netscape Communicator 4.73 Setup program.
- Step 12** Complete the Netscape installation:
- a. On the Netscape Communicator 4.73 Setup dialog box, click **Next**.
 - b. On the Software License Agreement dialog box, click **Yes**.
 - c. On the Setup Type dialog box, click **Typical**.



Note If the Netscape installation hangs when installing RealPlayer G2, restart the CTC installation. When the Netscape installation begins, select **Custom** at Step c, then deselect RealPlayer, then continue.

- d. On the Netscape Desktop Preferences dialog box, check the boxes that apply, then click **Next**.
- e. On the Program Folder dialog box, click **Next**.
- f. On the Start Copying Files dialog box, click **Install**. The program begins the Netscape installation.

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

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

Step 14 Complete the JRE installation:

- a. On the Software License Agreement dialog box, click **Yes**.
- b. On the Choose Destination Location dialog box, click **Next**.
- c. On the Select Browser dialog box, click the Microsoft Internet Explorer and Netscape 6 checkboxes, then click **Next**.

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

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

Step 16 Choose the JRE policy file to modify:

- Choose **User Policy File** (default) to modify the policy file that applies only to your user profile. This file will not be overwritten if you upgrade or reinstall the JRE. If you are the only user who will access an ONS 15327 from the PC you are setting up, choose this option.
- Select **System Policy File** to modify the system JRE policy file. This policy file applies to all computer users. If more than one individual will use this computer to access the ONS 15327, choose this option. However, if you reinstall or upgrade the JRE, the system policy file is overwritten and you will need to run the CTC Installation Setup program again to modify it.

Step 17 Click **Next**.

Step 18 If you selected System Policy File in Step 16, complete the following steps. If you selected User Policy File, go to the next step.

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

Step 19 Click **Finish**.

Procedure: Run the CTC Installation Wizard for UNIX

Step 1 Verify that your computer has the following:

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



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

Step 2 Change the directory, type:

```
cd /cdrom/cdrom0/
```


Step 3 From the techdoc327 CD directory, type:

```
./setup.bat
```

The Cisco Transport Controller Installation Wizard displays the components that will be installed on your computer (Figure 2-1 on page 2-5):

- Netscape Communicator 4.76
- Java Runtime Environment 1.3.1_02
- CTC Online Help
- Modify Policy File—the JRE java.policy file is modified to enable CTC to download files needed to run the Cisco Transport Controller when you connect to an ONS 15327.

Step 4 Click **Next**.

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

Step 6 Click **Next**.

Step 7 If you selected **Custom** in Step 5, select the CTC components you want to install by checking or unchecking the boxes, then click **Next**. If you selected **Typical**, skip this step.

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

Step 9 Click **Next**.

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

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

Step 12 Complete the Netscape installation:

- a. On the Netscape Communicator 4.73 Setup dialog box, click **Next**.
- b. On the Software License Agreement dialog box, click **Yes**.
- c. On the Setup Type dialog box, click **Typical**.
- d. On the Netscape Desktop Preferences dialog box, check the boxes that apply, then click **Next**.
- e. On the Program Folder, click **Next**.
- f. On the Start Copying Files dialog box, click **Install**. The program begins the Netscape installation.
- g. On the Question dialog box, click **No**.
- h. On the Restart Windows dialog box, click **No, I will restart later**, then click **OK**.

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

Step 14 Complete the JRE installation:

- a. On the Software License Agreement dialog box, click **Yes**.
- b. On the Choose Destination Location dialog box, click **Next**.
- c. On the Select Browser dialog box, click the Microsoft Internet Explorer and Netscape 6 checkboxes, then click **Next**.

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

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

Step 16 Choose the JRE policy file to modify:

- Choose **User Policy File** (default) to create a policy file that applies only to your user profile. This file will not be overwritten if you upgrade or reinstall the JRE. If you are the only computer user who will access an ONS 15327, choose this option.
- Select **System Policy File** to modify the system JRE policy file. This policy file applies to all computer users. If more than one individual will use this computer to access the ONS 15327, choose this option. However, if you reinstall or upgrade the JRE, the system policy file is overwritten and you will need to run the CTC Installation Setup program again to modify it.

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



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

Step 18 If your installation included the JRE (that is, you chose the Typical installation or selected JRE from the custom installation), go to the “Set Up the Java Runtime Environment for UNIX” procedure on page 2-81.



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

Procedure: Set Up the Java Runtime Environment for UNIX



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



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

Step 1 Set up the environment variable:

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

```
setenv JRE [JRE path]
setenv NETSCAPE [Netscape path]
setenv NPX_PLUGIN_PATH $JRE/j2re1_3_1_02/plugin/sparc/ns4
```

```
set path = ( /usr/openwin/bin $NETSCAPE $path)
```

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

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

Step 2 Set the JRE reference:

- a. Run the Control Panel by typing:
[JRE path]/j2re1_3_1_02/bin/ControlPanel
- b. Click the **Advanced** tab.
- c. From the combo box, select **[JRE path]/j2rel1_3_1_02**. If the JRE is not found, select **other** and enter the following in the Path text box:
[JRE path]/j2re 1_3_1_02
- d. Click **Apply**. Go to the “Connecting PCs to the ONS 15327” procedure on page 2-20.



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

Setting Up the CTC Computer

Before you run CTC on your Windows PC or Solaris workstation, you need to set up the computer for the specific method you will use to connect to the ONS 15327. Table 2-3 lists the methods for connecting to the ONS 15327. Use the table to find the connection method you will use and check the Requirements column before performing the set up procedures.



Note For initial shelf turn up, you must use a local connection to the ONS 15327.

Table 2-3 ONS 15327 Connection Methods

Method	Description	Requirements
Local craft	Refers to onsite network connections between the CTC computer and the ONS 15327 using: <ul style="list-style-type: none"> • The RJ-45 jack on the XTC, or • A hub or switch to which the ONS 15327 is connected. 	<ul style="list-style-type: none"> • If you do not use DHCP, you will need to change the computer IP address, subnet mask, and default router.
Corporate LAN	Refers to a connection to the ONS 15327 through a corporate or NOC LAN.	<ul style="list-style-type: none"> • The ONS 15327 must be provisioned for LAN connectivity, including IP address, subnet mask, and default gateway. • The ONS 15327 must be physically connected to the corporate LAN. • The CTC computer must be connected to the corporate LAN that has connectivity to the ONS 15327.
TL1	Refers to a connection to the ONS 15327 using TL1 rather than CTC. TL1 sessions can be started from CTC, or you can use a TL1 terminal. The physical connection can be a craft connection, corporate LAN, or a TL1 terminal. Refer to the <i>Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide</i> .	
Remote	Refers to a connection made to the ONS 15327 using a modem.	<ul style="list-style-type: none"> • A modem must be connected to the ONS 15327. • The modem must be provisioned for ONS 15327. To run CTC, the modem must be provisioned for Ethernet access.

After you have determined which method you will use to connect to the ONS 15327, find the necessary procedures in Table 2-4.

Table 2-4 ONS 15327 Craft Connection Options

Direct Connection Procedure	Description
<ul style="list-style-type: none"> Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses, page 2-11, or Set up a Solaris Workstation for Craft Connection to an ONS 15327, page 2-17 	Complete this procedure if: <ul style="list-style-type: none"> You will access nodes running CTC software releases before Release 3.3 You will connect to one ONS 15327; if you will connect to multiple ONS 15454s, you may need to reconfigure your computer's IP settings each time you connect to an ONS 15454 You need to access non-ONS 15327 applications such as ping and trace route
<ul style="list-style-type: none"> Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP, page 2-14 	Complete this procedure if: <ul style="list-style-type: none"> The CTC computer is provisioned for DHCP The ONS 15327 has DHCP forwarding enabled and is connected to a DHCP server
<ul style="list-style-type: none"> Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection, page 2-15, or Set up a Solaris Workstation for Craft Connection to an ONS 15327, page 2-17 	Complete this procedure if: <ul style="list-style-type: none"> You are connecting to a node that resides in a secure network employing the ONS 15327 proxy server All nodes that you will access are running software Release 3.3 You will connect to ONS 15327s at different locations and times You do not need to access a LAN or use non-ONS 15327 applications such as ping and gateway TL1

- To set up the computer for LAN access, complete the “Set Up a Computer for a Corporate LAN Connection” procedure on page 2-18.
- To set up the computer for TL1 access, see the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide* for setup procedures.
- To set up the computer for remote access, complete the “Provision Remote Access to the ONS 15327” procedure on page 2-19.

Step 3 After your computer is set up to connect to the ONS 15327, go to the “Logging into the ONS 15327” procedure on page 2-24.

Procedure: Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses

Use this procedure to set up your computer for a local craft connection to the ONS 15327 when:

- You will access nodes running software releases before Release 3.3
- You will connect to one ONS 15327; if you will connect to multiple ONS 15327s, you may need to reconfigure your computer's IP settings each time you connect to an ONS 15327

- You need to use non-ONS 15327 applications such as ping and trace route
 - You need to access the corporate LAN
-

- Step 1** Verify the operating system that is installed on your computer:
- a. From the Windows Start menu, choose **Settings > Control Panel**.
 - b. On the Control Panel window, double-click the **System** icon.
 - c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 95, Windows 98, Windows 2000, or Windows NT 4.0.
- Step 2** Complete the steps in Table 2-5 for the operating system installed on your PC.

Table 2-5 Set Up Windows PC for Craft ONS 15327 Connections on the Same Subnet Using Static IP Addresses

For Windows 95/98:	For Windows NT:	For Windows 2000:
<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Control Panel. 2. On the Control Panel dialog box, click the Network icon. 3. In the Network dialog box select TCP/IP for your PC Ethernet card, then click Properties. 4. On the TCP/IP Properties dialog box, click the DNS Configuration tab and choose Disable DNS. 5. Click the WINS Configuration tab and choose Disable WINS Resolution. 6. Click the IP Address tab. 7. In the IP Address window, click Specify an IP address. 8. In the IP Address field, enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. 9. In the Subnet Mask field, type 255.255.255.0. 10. Click OK. 11. On the TCP/IP dialog box, click the Gateway tab. 12. In the New Gateway field, type the ONS 15327 IP address. Click Add. 13. Verify that the IP address displays in the Installed Gateways field, then click OK. 14. When the prompt to restart your PC displays, click Yes. 	<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Control Panel. 2. On the Control Panel dialog box, click the Network icon. 3. In the Network dialog box click the Protocols tab, choose TCP/IP Protocol, then click Properties. 4. Click the IP Address tab. 5. In the IP Address window, click Specify an IP address. 6. In the IP Address field, enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. 7. In the Subnet Mask field, type 255.255.255.0. 8. Click the Advanced button. 9. Under the Gateways List, click Add. The TCP/IP Gateway Address dialog box is displayed. 10. Type the ONS 15327 IP address in the Gateway Address field. 11. Click Add. 12. Click OK. 13. Click Apply. 14. In some cases, Windows NT will prompt you to reboot your PC. If you receive this prompt, click Yes. 	<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Network and Dial-up Connections > Local Area Connection. 2. On the Local Area Connection Status dialog box, click Properties. 3. On the General tab, choose Internet Protocol (TCP/IP), then click Properties. 4. Click Use the following IP address. 5. In the IP Address field, enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. 6. In the Subnet Mask field, type 255.255.255.0. 7. In the Default Gateway field, type the ONS 15327 IP address. 8. Click OK. 9. On the Local Area Connection Status dialog box, click Close. 10. On the Local Area Connection Properties dialog box, click OK.

Step 3 After you set up your PC, go to the “Logging into the ONS 15327” procedure on page 2-24 to log into the ONS 15327.

Procedure: Set Up a Windows PC for Craft Connection to an ONS 15327 Using DHCP

Use this procedure to set up your computer for craft connection to the ONS 15327 using DHCP (dynamic host configuration protocol).



Caution

You will not be able to connect to the ONS 15327 if DHCP forwarding is not enabled on the ONS 15327 or the ONS 15327 is not connected to a DHCP server. By default, DHCP forwarding is not enabled. If you are connecting to an ONS 15327 to perform initial shelf turnup, complete the “Set Up a Windows PC for Craft Connection to an ONS 15327 on the Same Subnet Using Static IP Addresses” procedure on page 2-11 or the “Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection” procedure on page 2-15.

- Step 1** Verify the operating system that is installed on your computer:
- a. From the Windows Start menu, choose **Settings > Control Panel**.
 - b. On the Control Panel window, double-click the **System** icon.
 - c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 95, Windows 98, Windows 2000, or Windows NT 4.0
- Step 2** Complete the steps in Table 2-6 for the operating system installed on your PC.

Table 2-6 Set Up Windows PC for Craft ONS 15327 Connections Using DHCP

For Windows 95/98:	For Windows NT:	For Windows 2000:
<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Control Panel. 2. On the Control Panel dialog box, click the Network icon. 3. In the Network dialog box select TCP/IP for your PC Ethernet card, then click Properties. 4. On the TCP/IP Properties dialog box, click the DNS Configuration tab and choose Disable DNS. 5. Click the WINS Configuration tab and choose Disable WINS Resolution. 6. Click the IP Address tab. 7. In the IP Address window, click Obtain an IP address from a DHCP Server. 8. Click OK. 9. When the prompt to restart your PC displays, click Yes. 	<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Control Panel. 2. On the Control Panel dialog box, click the Network icon. 3. In the Network dialog box click the Protocols tab, choose TCP/IP Protocol, then click Properties. 4. Click the IP Address tab. 5. In the IP Address window, click Obtain an IP address from a DHCP Server. 6. Click OK. 7. Click Apply. 8. If Windows prompts you to restart your PC, click Yes. 	<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Network and Dial-up Connections > Local Area Connection. 2. On the Local Area Connection Status dialog box, click Properties. 3. On the General tab, choose Internet Protocol (TCP/IP), then click Properties. 4. Click Obtain an IP address from a DHCP Server. 5. Click OK. 6. On the Local Area Connection Status dialog box, click Close. 7. On the Local Area Connection Properties dialog box, click OK.

- Step 3** After you set up your PC, go to the “Logging into the ONS 15327” procedure on page 2-24 to log into the ONS 15327.
-

Procedure: Set Up a Windows PC for Craft Connection to an ONS 15327 Using Automatic Host Detection

Use this procedure to set up your computer for local craft connection to the ONS 15327 when:

- You are connecting to a node that resides in a secure network employing the ONS 15327 proxy server.
- All nodes that you will access are running software release Release 3.3.
- You will connect to multiple ONS 15327s.

You do not need to access a corporate LAN or use non-ONS 15327 applications such as ping and trace route.



Note

This procedure employs the ONS 15327 automatic host detection to allow you to directly connect to multiple ONS 15327s successively without reconfiguring your computer’s IP address. However, if proxy server is not enabled on the ONS 15327, DCC-connected nodes on different subnets will not be visible.

- Step 1** Verify the operating system that is installed on your computer:
- a. From the Windows Start menu, choose **Settings > Control Panel**.
 - b. On the Control Panel window, double-click the **System** icon.
 - c. On the General tab of the System Settings window, verify that the Windows operating system is one of the following: Windows 95, Windows 98, Windows 2000, or Windows NT 4.0
- Step 2** Complete the steps in Table 2-7 for the operating system installed on your PC.

Table 2-7 Set Up Windows PC for Craft ONS 15327 Connections Using Automatic Host Detection

For Windows 95/98:	For Windows NT:	For Windows 2000:
<ol style="list-style-type: none"> From the Windows Start menu, choose Settings > Control Panel. On the Control Panel dialog box, click the Network icon. In the Network dialog box select TCP/IP for your PC Ethernet card, then click Properties. On the TCP/IP Properties dialog box, click the DNS Configuration tab and choose Disable DNS. Click the WINS Configuration tab and choose Disable WINS Resolution. Click the IP Address tab. In the IP Address window, click Specify an IP address. In the IP Address field, enter a legitimate IP address. In the Subnet Mask field, type 255.255.255.0. Click OK. On the TCP/IP dialog box, click the Gateway tab. In the New Gateway field, type PC IP address (the address entered in Step 8). Click Add. Verify that the IP address displays in the Installed Gateways field, then click OK. When the prompt to restart your PC displays, click Yes. 	<ol style="list-style-type: none"> From the Windows Start menu, choose Settings > Control Panel. On the Control Panel dialog box, click the Network icon. In the Network dialog box click the Protocols tab, choose TCP/IP Protocol, then click Properties. Click the IP Address tab. In the IP Address window, click Specify an IP address. In the IP Address field, enter a legitimate IP address. In the Subnet Mask field, type 255.255.255.0. Click the Advanced button. Under the Gateways List, click Add. The TCP/IP Gateway Address dialog box is displayed. Type the IP address entered in Step 6 in the Gateway Address field. Click Add. Click OK. Click Apply. In some cases, Windows NT will prompt you to reboot your PC. If you receive this prompt, click Yes. 	<ol style="list-style-type: none"> From the Windows Start menu, choose Settings > Network and Dial-up Connections > Local Area Connection. On the Local Area Connection Status dialog box, click Properties. On the General tab, choose Internet Protocol (TCP/IP), then click Properties. Click Use the following IP address. In the IP Address field, enter a legitimate IP address. In the Subnet Mask field, type 255.255.255.0. Type the IP address entered in Step 5 in the Gateway Address field. Click OK. On the Local Area Connection Status dialog box, click Close. On the Local Area Connection Properties dialog box, click OK.

Step 3 After you set up your PC, you can go to the “Logging into the ONS 15327” procedure on page 2-24 to log into the ONS 15327.

Procedure: Set up a Solaris Workstation for Craft Connection to an ONS 15327

Use this procedure to connect your workstation directly to the ONS 15327.



Note

This procedure employs the ONS 15327 automatic host detection to allow you to directly connect to multiple ONS 15327s successively without reconfiguring your workstation's IP address. However, if proxy server is not enabled on the ONS 15327, DCC-connected nodes on different subnets will not be visible.

Step 1

Choose a cable connection method:

- **RJ-45 jack on the ONS 15327 XTC:** Attach a CAT-5 cable from the workstation's NIC card to the RJ-45 jack on the ONS 15327 XTC.
- **Hub or switch:** Attach a CAT-5 cable from the workstation's NIC card to the RJ-45 jack on a hub or switch to which the ONS 15327 is physically connected.

Step 2

Log into the workstation as the root user.

Step 3

Check to see if the interface is plumbed by typing:

```
# ifconfig <device>
```

For example: **# ifconfig hme1**

- a. If the interface is plumbed, a message similar to the following appears:
hme1:flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4>mtu 1500 index 2 inet 0.0.0.0 netmask 0. Go to Step 4.
- b. If the interface is not plumbed, a message similar to the following appears: ifconfig: status: SIOCGLIFFLAGS: hme1: no such interface. Plumb the interface by typing:

```
# if config <device> plumb
```

For example: **ifconfig hme1 plumb**

Step 4

Configure the IP address on the interface by typing:

```
#ifconfig <interface> <ip address> netmask <netmask> up
```

For example: **#ifconfig hme0 10.20.30.40 netmask 255.255.255.0 up**



Note

Enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. In the Subnet Mask field, type 255.255.255.0.

Step 5

Test the connection:

- a. Start Netscape Navigator or Internet Explorer.
- b. Enter the Cisco ONS 15327 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box display. If this occurs, go to Step 2 of the "Log into the ONS 15327" procedure on page 2-24 to complete the login. If the Login dialog box does not appear, complete Steps c and d.

- c. At the prompt, type:

```
ping [ONS 15327 IP address]
```

For example, you would type “ping 192.168.1.1” to connect to an ONS 15327 with default IP address 192.168.1.1. If your workstation is connected to the ONS 15327, an “[IP address] is alive” message displays.



Note Skip this step if “Craft Access Only” from **Provisioning > Network > General > Gateway Settings** is checked.

- d. If CTC is not responding, a “Request timed out” message displays. Verify IP and submask information. Check that the cables connecting the workstation to the ONS 15327 are securely attached. Check the Link Status by typing:

```
#nnd -set /dev/<device> instance 0
```

```
#nnd -get /dev/<device> link_status
```

For example:

```
#nnd -set /dev/hme instance 0
```

```
#nnd -get /dev/hme link_status
```

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



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

- Step 6** After you set up your workstation, you can go to the “Log into the ONS 15327” procedure on page 2-24 to log into the ONS 15327.
-

Procedure: Set Up a Computer for a Corporate LAN Connection

Use this task to set up your computer to access the ONS 15327 through a corporate LAN.

- Step 1** If your computer is connected to the corporate LAN, go to Step 2. If you changed your computer’s network settings for direct access to the ONS 15327, change the settings back to the corporate LAN access settings. This generally means:
- Set the IP Address on the TCP/IP dialog box back to “Obtain an IP address automatically” (Windows 95/98) or “Obtain an IP address from a DHCP server” (Windows NT/2000).
 - If your LAN requires that DNS or WINS be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.
- Step 2** If your computer is connected to a proxy server, disable proxy service or add the ONS 15327 nodes as exceptions. To disable proxy service, complete the task for the web browser you use:
- Disable Proxy Service Using Internet Explorer (Windows), page 2-19, or

- Disable Proxy Service Using Netscape (Windows and Solaris), page 2-23
-

Procedure: Disable Proxy Service Using Internet Explorer (Windows)

Disables proxy service for PCs running Internet Explorer.

- Step 1** From the Start menu, select **Settings > Control Panel**.
 - Step 2** In the Control Panel window, choose **Internet Options**.
 - Step 3** From the Internet Properties dialog box, click **Connections > LAN Settings**.
 - Step 4** On the LAN Settings dialog box, either:
 - Deselect **Use a proxy server** to disable the service, or
 - Leave **Use a proxy server** selected and click **Advanced**. On the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15327 nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS 15327s on your network. Click **OK** to close each open dialog box.
-

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

Disables proxy service for PCs and UNIX workstations running Netscape.

- Step 1** Open Netscape.
 - Step 2** From the Edit menu, choose **Preferences**.
 - Step 3** In the Preferences dialog box under Category, choose **Advanced > Proxies**.
 - Step 4** On the right side of the Preferences dialog box under Proxies, either:
 - Choose **Direct connection to the Internet** to bypass the proxy serveror
 - Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. On the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15327 nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.
-

Procedure: Provision Remote Access to the ONS 15327

Use this task to connect an ONS 15327 using a LAN modem.

- Step 1** Connect the modem to the RJ-45 port on the XTC.
- Step 2** Refer to the modem documentation to provision the modem for the ONS 15327:
 - For CTC access, set the modem for Ethernet access.
 - Assign an IP address to the modem that is on the same subnet as the ONS 15327.

- The IP address the modem assigns to the CTC computer must be on the same subnet as the modem and the ONS 15327.



Note For assistance on provisioning specific modems, contact the Cisco Technical Assistance Center, at 1-877-323-7368.

2.4 Connecting PCs to the ONS 15327

You can connect a PC to the ONS 15327 using the RJ-45 LAN port on the XTC card. Each ONS 15327 must have a unique IP address that you use to access the ONS 15327. The initial IP address, 192.1.0.2, is the default address for ONS 15327 access and configuration. Each computer used to communicate with the ONS 15327 should have only one IP address.



Note Do not use dual network interface cards (NIC) or an enabled NIC card and dial-up adapter at the same time; this hampers communication between CTC and ONS 15327s.

2.4.1 Direct Connections to the ONS 15327

A direct PC to ONS 15327 connection means your computer is physically connected to the ONS 15327. This is done by connecting a CAT-5 straight-through cable from your PC NIC card to the RJ-45 (LAN) port on the XTC card. (Direct connections include connections to switches or hubs to which the ONS 15327 is physically connected.) To connect to the ONS 15327 with a direct connection, you must:

- Set up Windows on your PC for direct connections
- Attach cables from the PC to the ONS 15327
- Test your connection

Procedure: Create a Direct Connection to an ONS 15327

-
- Step 1** Attach a CAT-5 cable from the PC NIC card to one of the following:
- RJ-45 jack on the ONS 15327 XTC card
You can connect to either the active or standby XTC LAN port, but not both simultaneously.
 - RJ-45 jack on a hub or switch to which the ONS 15327 is physically connected
- Step 2** Use the steps in Table 2-8 to set up Windows for direct connections to an ONS 15327 when:
- DHCP (Dynamic Host Configuration Protocol) is not enabled on the ONS 15327 or the ONS 15327 is not connected to a DHCP server. For information about DHCP, see the “Setting Up Network Information” section on page 3-3.
 - The ONS 15327 is not connected to a LAN.

Table 2-8 *Setting Up Windows 95/98, Windows NT, and Windows 2000 PCs for Direct ONS 15327 Connections*

Windows 95/98	Windows NT	Windows 2000
<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Control Panel. 2. On the Control Panel dialog box, click the Network icon. 3. In the Network dialog box select TCP/IP for your PC Ethernet card, then click Properties. 4. On the TCP/IP Properties dialog box, click the DNS Configuration tab and choose Disable DNS. 5. Click the WINS Configuration tab and choose Disable WINS Resolution. 6. Click the IP Address tab. 7. In the IP Address window, click Specify an IP address. 8. In the IP Address field, enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. 9. In the Subnet Mask field, type 255.255.255.0. 10. Click OK. 11. On the TCP/IP dialog box, click the Gateway tab. 12. In the New Gateway field, type the ONS 15327 IP address. Click Add. 13. Verify that the IP address displays in the Installed Gateways field, then click OK. 14. When the prompt to restart your PC displays, click Yes. 	<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Control Panel. 2. On the Control Panel dialog box, click the Network icon. 3. In the Network dialog box click the Protocols tab, choose TCP/IP Protocol, then click Properties. 4. Click the IP Address tab. 5. In the IP Address window, click Specify an IP address. 6. In the IP Address field, enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. 7. In the Subnet Mask field, type 255.255.255.0. 8. Click OK. 9. On the TCP/IP Properties dialog box, type the ONS 15327 IP address in the Default Gateway field. 10. Click Apply. 11. In some cases, Windows NT will prompt you to reboot your PC. If you receive this prompt, click Yes. 	<ol style="list-style-type: none"> 1. From the Windows Start menu, choose Settings > Network and Dial-up Connections > Local Area Connection. 2. On the Local Area Connection Status dialog box, click Properties. 3. On the General tab, choose Internet Protocol (TCP/IP), then click Properties. 4. Click Use the following IP address. 5. In the IP Address field, enter an IP address that is identical to the ONS 15327 IP address except for the last three digits. The last three digits must be between 1 and 254. 6. In the Subnet Mask field, type 255.255.255.0. 7. In the Default Gateway field, type the ONS 15327 IP address. 8. Click OK.

Step 3 Test the connection:

- a. Start Netscape Navigator or Internet Explorer.
- b. Enter the Cisco ONS 15327 IP address in the web address (URL) field. If the connection is established, a Java Console window, CTC caching messages, and the Cisco Transport Controller Login dialog box display. If this occurs, go to Step 2 of the “Log into the ONS 15327” procedure on page 2-24 to complete the login. If the Login dialog box does not appear, complete Steps c and d.
- c. From the Windows Start menu, choose the MS-DOS or command prompt.

- d. At the prompt, type:

```
ping [ONS 15327 IP address]
```

For example, you would type “ping 192.1.0.2” to connect to an ONS 15327 with default IP address 192.1.0.2. If your computer is connected to the ONS 15327, a “reply from [IP address]” message displays.

If your PC is not connected, a Request timed out message displays. If this occurs, check that the cables connecting the PC to the ONS 15327 are securely attached. Check the Link Status LED on the PC NIC card. Repeat the procedures provided in Table 2-8 while verifying IP and subnet mask information.

2.4.2 Network Connections

When connecting the PC to the ONS 15327 through a LAN, the PC’s IP address must be configured to be on the same subnet as the ONS 15327’s LAN interface. If needed, change the IP address configuration on the PC.

Procedure: Access the ONS 15327 from a LAN

Step 1 Change the ONS 15327 IP address to an IP address that exists on the LAN. (See the “Setting Up Network Information” procedure on page 3-3 for instructions.)

Step 2 Ensure that the ONS 15327 is physically connected to the LAN (typically using a cross-over cable to a hub or switch).



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

Step 3 If you changed the PC network settings for direct access to the ONS 15327, change the settings back to the LAN access settings. Usually this means setting the IP Address on the TCP/IP dialog box back to “Obtain an IP address automatically” (Windows 95/98) or “Obtain an IP address from a DHCP server” (Windows NT/2000). If your LAN requires that DNS or WINS be enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog box.

Step 4 If your computer is connected to a proxy server, disable proxy service or add the ONS 15327 nodes as exceptions.

Step 5 Start your web browser and type the ONS 15327 IP address in the URL field.

Procedure: Disable Proxy Service Using Internet Explorer (Windows)

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

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

- Step 2** In the Control Panel window, choose **Internet Options**.
- Step 3** From the Internet Properties dialog box, click **Connections > LAN Settings**.
- Step 4** On the LAN Settings dialog box, either:
- Deselect **Use a proxy server** to disable the service
- or
- Leave **Use a proxy server** selected and click **Advanced**. On the Proxy Setting dialog box under Exceptions, enter the IP addresses of ONS 15327 nodes that you will access. Separate each address with a semicolon. You can insert an asterisk for the host number to include all the ONS 15327s on your network. Click **OK** to close each open dialog box.
-

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

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

-
- Step 1** Open Netscape.
- Step 2** From the Edit menu, choose **Preferences**.
- Step 3** In the Preferences dialog box under Category, choose **Advanced > Proxies**.
- Step 4** On the right side of the Preferences dialog box under Proxies, either:
- Choose **Direct connection to the Internet** to bypass the proxy server
- or
- Choose **Manual proxy configuration** to add exceptions to the proxy server, then click **View**. On the Manual Proxy Configuration dialog box under Exceptions, enter the IP addresses of the ONS 15327 nodes that you will access. Separate each address with a comma. Click **OK** to close each open dialog box.
-

2.4.3 Remote Access to the ONS 15327

You can use LAN modems to access ONS 15327s from remote sites. The LAN modem must be connected to the RJ-45 port on an XTC card. The LAN modem must be properly configured for use with the ONS 15327. When the modem is installed, dial-up access to the ONS 15327 is available using a PC or Solaris workstation modem.

2.4.4 TL1 Terminal Access to the ONS 15327

You can communicate with the ONS 15327 using TL1. To connect a TL1 terminal (or a PC running terminal emulation software) to the ONS 15327, you can:

- Use the DB-9 plug on the front panel of the XTC card.

You can connect to either the active or standby XTC DB-9 plug to gain terminal access, but not both simultaneously.

- Telnet to port 3083 with a LAN connection.
- Start a TL1 session from CTC by selecting Open TL1 Session from the CTC Tools menu and selecting the node where you want to hold the TL1 session in the Select Node dialog box.

For information about using TL1 commands with the ONS 15327, see the *Cisco ONS 15xxx TL1 Command Guide*.

2.5 Logging into the ONS 15327

After you set up the physical connections between the PC and ONS 15327 and change your PC network settings, you can log into CTC.

Procedure: Log into the ONS 15327

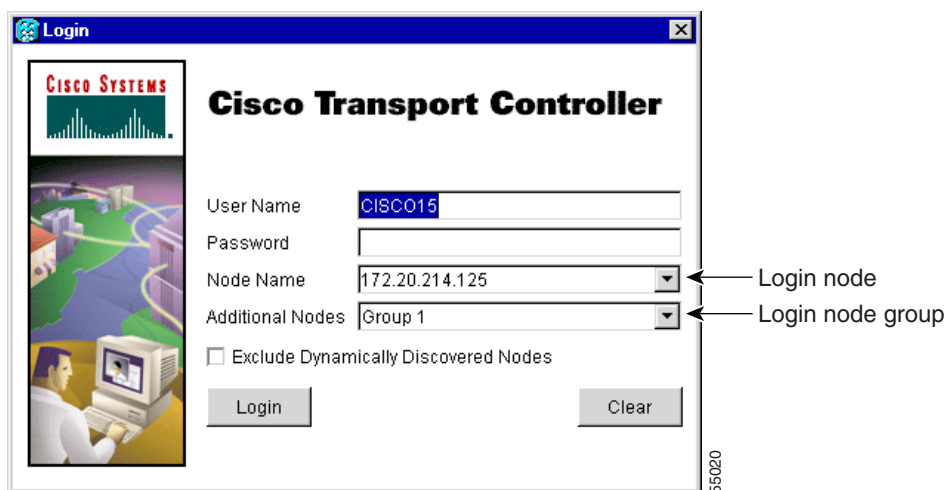
- Step 1** From the PC connected to the ONS 15327, start Netscape or Internet Explorer.
- Step 2** In the Netscape or Internet Explorer Web address (URL) field, enter the ONS 15327 IP address. For initial setup, this is the default address, 192.1.0.2. Press **Enter**.



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

A Java Console window displays the CTC file download status. The web browser displays information about your Java and system environments. If this is the first login, CTC caching messages display while CTC files are downloaded to your computer; then the CTC Login dialog box displays (Figure 2-2).

Figure 2-2 Logging into the ONS 15327



- Step 3** Type a user name and password (both are case sensitive). For initial setup, type the user name “CISCO15” and click **Login** (no password is required).

**Note**

The CISCO15 user is provided with every ONS 15327. CISCO15 has superuser privileges, so you can create other users. CISCO15 is delivered without a password. To create one, click the **Provisioning > Security** tabs after you log in and change the CISCO15 password. (You cannot delete the CISCO15 user.) For more information about ONS 15327 security, see the “Creating Users and Setting Security” section on page 3-4.

Step 4 Set the following login options, as needed:

- *Node Name*—Displays the IP address entered in the web browser and a pull-down menu of previously-entered ONS 15327 IP addresses. You can select any ONS 15327 (or ONS 15454) on the list for the login, or you can enter the IP address (or node name) of any new node where you want to log in.
- *Additional Nodes*—Displays a list of login node groups that were created. Login node groups allow you to display ONS 15327s and/or ONS 15454s that are not connected by the SONET Data Communications Channel (DCC) to the ONS 15327 in the Node Name field. (For instructions, see the “Creating Login Node Groups” section on page 2-25.)

**Note**

Topology hosts that were created in previous ONS 15327 releases by modifying the cms.ini file are displayed as a “Topology Host” group under Additional Nodes.

- *Exclude Dynamically Discovered Nodes*—Check this box to view only the ONS 15327 (and login node group members, if any) entered in the Node Name field. Nodes linked to the Node Name ONS 15327 through the DCC are not displayed.

Step 5 Click **Login**.

If login is successful, the CTC window displays. From here, you can navigate to other CTC views to provision and manage the ONS 15327.

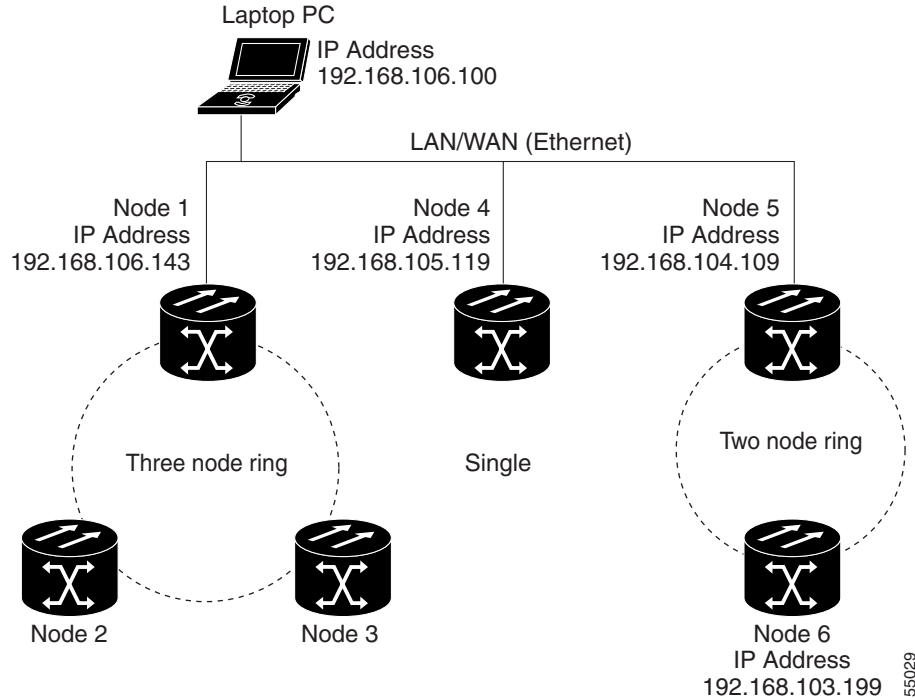
2.5.1 Creating Login Node Groups

When you log into an ONS 15327 node, only ONS 15327s optically connected (i.e., with DCC connections) to the node will display in network view. However, you can create a login node group to view and manage ONS 15327s that only have an IP connection. For example, logging into Node 1 in Figure 2-3 displays Node 2 and Node 3 because they are optically connected to Node 1. Nodes 4, 5, and 6 do not display because DCC connections do not exist. To view all six nodes at once, you create a login node group with the IP addresses of Nodes 1, 4, and 5. Those nodes, and all nodes optically connected to them, display when you log into any node in the group.

**Caution**

ONS 15327s propagate VLANs whenever a node appears on the same network view of another node regardless of whether the nodes connect through DCC or not. For example, if two ONS 15327s without DCC connectivity belong to the same Login Node Group, then whenever CTC gets launched from within this login node group, VLANs propagate from one to another. This happens even though the ONS 15327s do not belong to the same SONET ring.

Figure 2-3 A login node group



Procedure: Create a Login Node Group

-
- Step 1** From the CTC Edit menu, choose **Preferences**.
 - Step 2** Click the **Login Node Group** tab and click **Create Group**.
 - Step 3** Enter a name for the group in the Create Login Group Name dialog box. Click **OK**.
 - Step 4** Under Members, type the IP address (or node name) of a node you want to add to the group. Click **Add**. Repeat this step for each node you want to add to the group.
 - Step 5** Click **OK**.

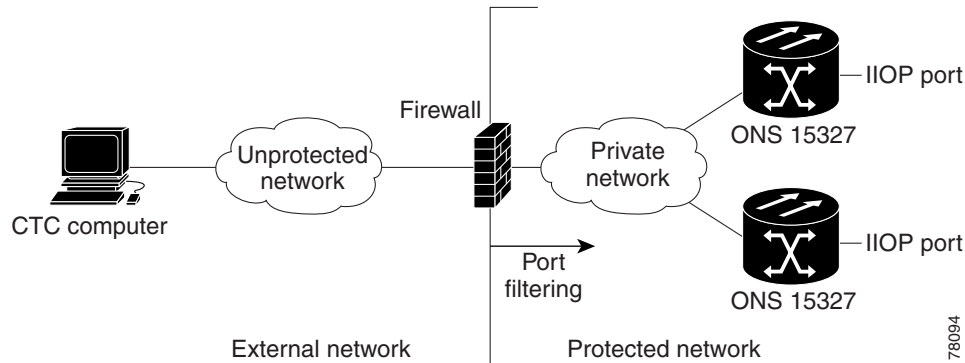
The next time you log into an ONS 15327, the login node group will be available in the Additional Nodes list of the Login dialog box. You can create as many login groups as you need. The groups are stored in the CTC preferences file and are not visible to other users.

2.5.2 Accessing ONS 15327s Behind Firewalls

If an ONS 15327 or CTC computer resides behind a firewall that uses port filtering, you must receive an Internet Inter-ORB Protocol (IIOP) port from your network administrator and enable the IIOP port on the ONS 15327 and/or CTC computer, depending on whether one or both devices reside behind firewalls.

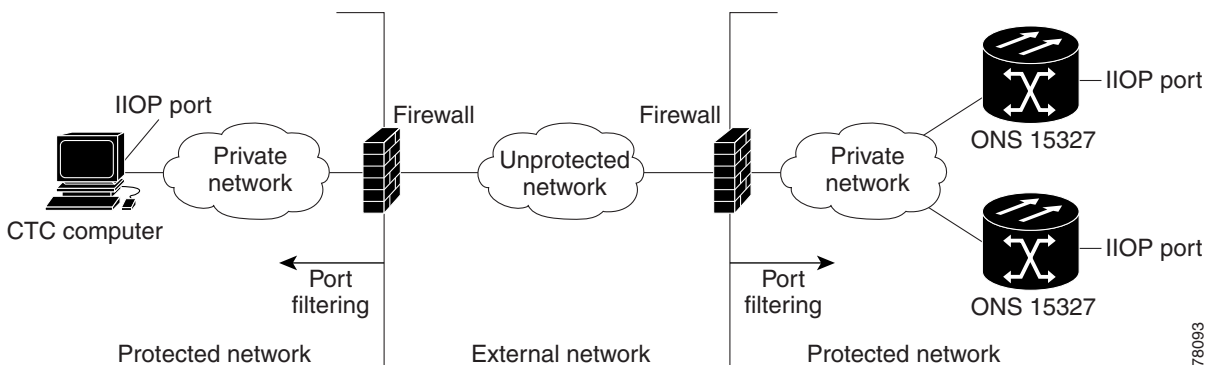
If the ONS 15327 is in a protected network and the CTC computer is in an external network, as shown in Figure 2-4, enable the IIOP listener port specified by the firewall administrator on the ONS 15327. The ONS 15327 sends the port number to the CTC computer during the initial contact between the devices using Hyper-Text Transfer Protocol (HTTP). After the CTC computer obtains the ONS 15327 IIOP port, the computer opens a direct session with the node using the specified IIOP port.

Figure 2-4 ONS 15327s residing behind a firewall



If the CTC computer and the ONS 15327 both reside behind firewalls (Figure 2-5), set the IIOP port on the CTC computer and on the ONS 15327. Each firewall can use a different IIOP port. For example, if the CTC computer firewall uses IIOP port 4000, and the ONS 15327 firewall uses IIOP port 5000, 4000 is the IIOP port set on the CTC computer and 5000 is the IIOP port set on the ONS 15327.

Figure 2-5 A CTC computer and ONS 15327s residing behind firewalls



Procedure: Set the IIOP Listener Port on the ONS 15327

-
- Step 1** Log into the ONS 15327 node from a CTC computer that is behind the firewall.
- Step 2** In node view, select the **Provisioning > Network** tabs.
- Step 3** On the **General** subtab under XTC card CORBA (IIOP) Listener Port, select a listener port option:
- *Default - XTC Fixed*—Used to connect to ONS 15327s on the same side of the firewall or if no firewall is used
 - *Standard Constant*—Uses port 683, the CORBA default port number
 - *Other Constant*—Allows you to set an IIOP port specified by your firewall administrator
- Step 4** Click **Apply** to apply the change.
- Step 5** When the Change Network Configuration? message displays, click **Yes**.
Both ONS 15327 XTC cards will reboot, one at a time.
-

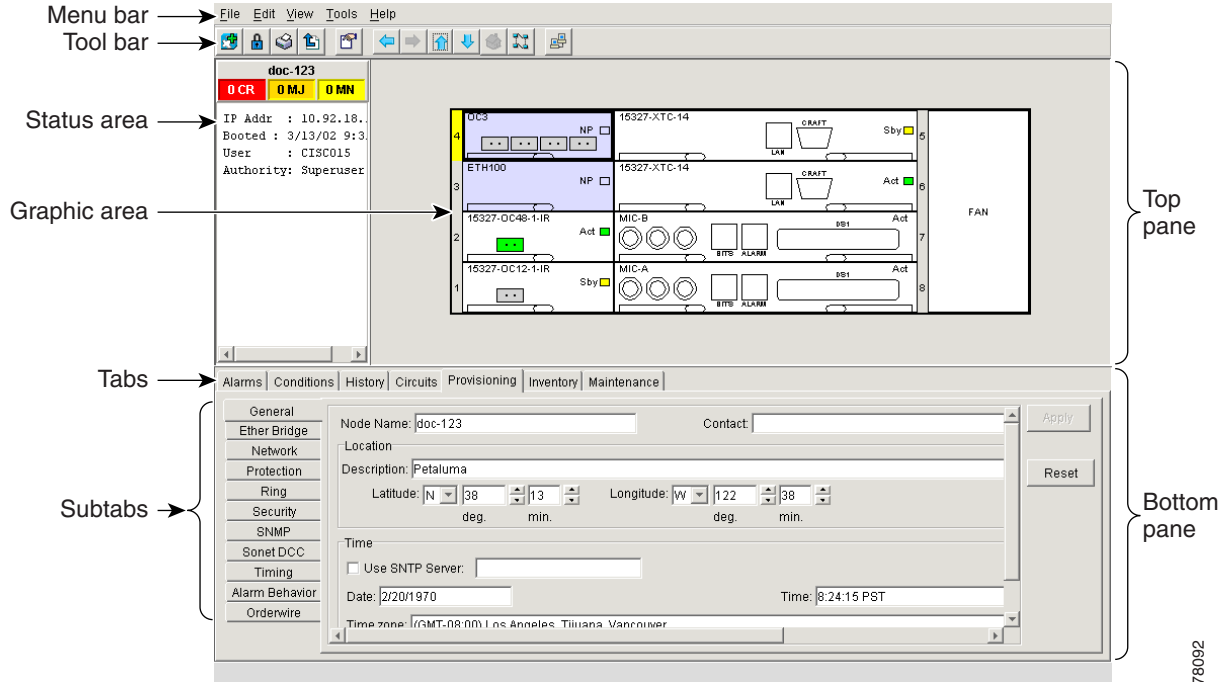
Procedure: Set the IIOP Listener Port on CTC

-
- Step 1** From the CTC Edit menu, select **Preferences**.
- Step 2** On the Preferences dialog box, select the **Firewall** tab.
- Step 3** Under CTC CORBA (IIOP) Listener Port, set the listener port option:
- *Default - Variable*—Used to connect to ONS 15327s from within a firewall or if no firewall is used
 - *Standard Constant*—Uses port 683, the CORBA default port number
 - *Other Constant*—Allows you to specify an IIOP port defined by your administrator
- Step 4** Click **OK** to apply the change and close the dialog box.
-

2.6 Working with the CTC Window

The CTC window (screen) displays after you log into an ONS 15327 (Figure 2-6). 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 2-6 CTC window elements in the node view (default login view)



78092

2.6.1 Node View

The CTC node view, shown in Figure 2-6, 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.

2.6.1.1 CTC Card Colors

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 2-9).

Table 2-9 Node View Card Colors

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

2.6.1.2 Node View Card Shortcuts

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

2.6.1.3 Node View Tabs

Use the node view tabs and subtabs, shown in Table 2-10, to provision and manage the ONS 15327.

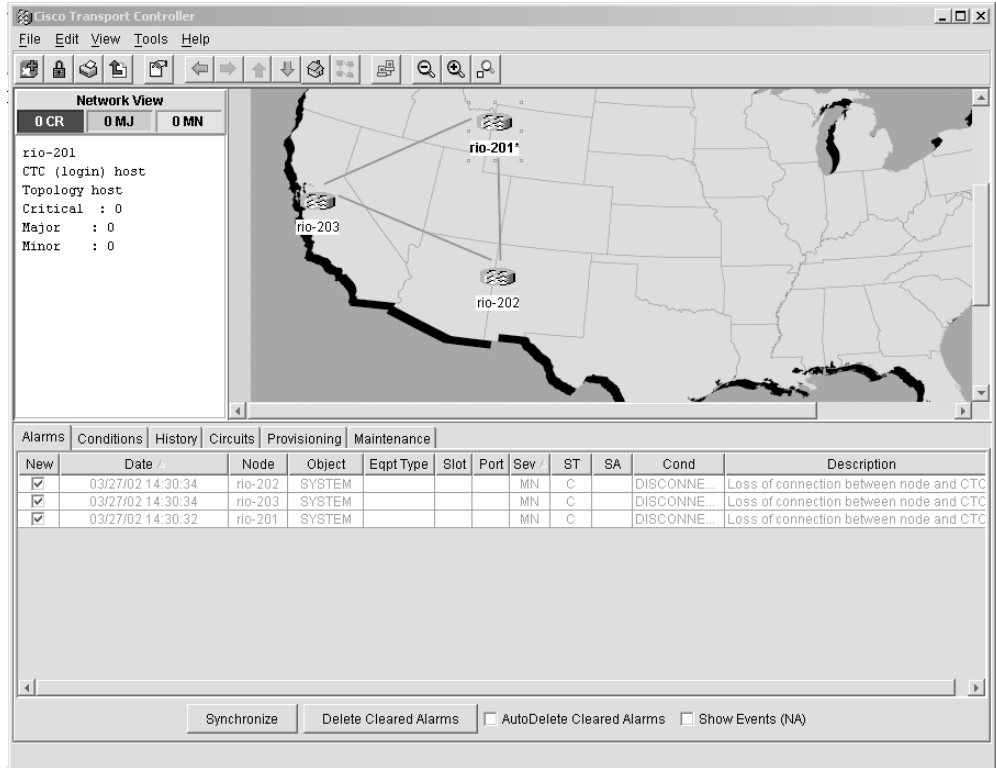
Table 2-10 Node View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms (CR, MJ, MN) for the node and updates them in real-time	none
Conditions	Displays a list of standing conditions on the node	none
History	Provides a history of node alarms including date, type, and severity of each alarm. The Session subtab displays alarms and events for the current session. The Node subtab displays alarms and events retrieved from a fixed-size log on the node.	Session, Node
Circuits	Create, delete, edit, and search circuits	none
Provisioning	Provision the ONS 15327 node	General, Ether Bridge, Network, Protection, Ring, Security, SNMP, Sonet DCC, Timing, Alarm Behavior, Orderwire
Inventory	Provides inventory information (part number, serial number, CLEI codes) for cards installed in the node. Allows you to delete and reset cards.	none
Maintenance	Perform maintenance tasks for the node	Database, Ether Bridge, Protection, Ring, Software, Diagnostic, Timing, Audit, Routing Table, Test Access

2.6.2 Network View

Network view (Figure 2-7) allows you to view and manage ONS 15327s and ONS 15454s that have DCC connections to the node that you logged into and any login node groups you may have selected. (Nodes with DCC connections to the login node will not display if you selected Exclude Dynamically Discovered Nodes on the Login dialog box.) The graphic area displays a background image with colored ONS 15327 icons. The icon colors indicate the node status (Table 2-11). Green lines show DCC connections between the nodes. Selecting a node or span in the graphic area displays information about the node and span in the status area.

Figure 2-7 A three-node network displayed in CTC network view



71740

2.6.2.1 CTC Node Colors

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

Table 2-11 Node Status

Color	Alarm Status
Green	No alarms
Yellow	Minor alarms
Orange	Major alarms
Red	Critical alarms
Grey with node name	Node is initializing
Grey with IP address	<ul style="list-style-type: none"> Node is initializing A problem exists with the IP routing from the node to CTC The node is incompatible with the node you logged into because it contains newer software The log in password exists only on the node you logged into and not on all of the nodes in the network

2.6.2.2 Network View Tasks

Right-click the network view graphic area or a node, span, or domain (domains are described in the “Creating Domains” section on page 2-33) to display shortcut menus. Table 2-12 lists the actions that are available from the network view.

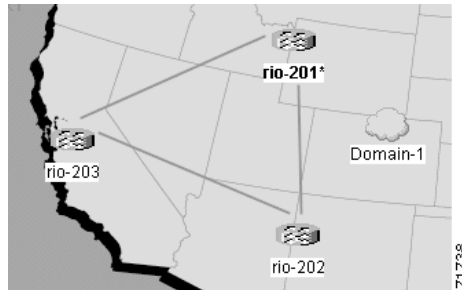
Table 2-12 Performing Network Management Tasks in Network View

Action	Procedure
Open a node	Any of the following: <ul style="list-style-type: none"> • Double-click a node icon • Right-click a node icon and choose Open Node from the shortcut menu • Click a node and choose Go to Selected Object View from the CTC View menu • From the View menu choose Go to Other Node. Select a node from the Select Node dialog box • Double-click a node alarm or event in the Alarms or History tabs
Move a node icon	Press the Ctrl key and the left mouse button simultaneously and drag the node icon to a new location.
Reset node icon position	Right-click a node and choose Reset Node Position from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the Provisioning > General tabs in node view.
Provision a circuit	Right-click a node. From the shortcut menu, choose Provision Circuit To and select the node where you want to provision the circuit. For circuit creation procedures, see the “Create an Automatically Routed Circuit” procedure on page 6-2.
Update circuits with new node	Right-click a node and choose Update Circuits With New Node from the shortcut menu. Use this command when you add a new node and want to pass circuits through it.
Display a link end point	Right-click a span. On the shortcut menu, select Go To [node/slot/port] for the drop port you want to view. CTC displays the card in card view.
Display span properties	Any of the following: <ul style="list-style-type: none"> • Move the mouse over a span; properties display near the span • Click a span; properties display in the upper left corner of the window • Right-click a span; properties display at the top of the shortcut menu
Perform a UPSR protection switch for an entire span	Right-click a network span and click Circuits . See the “Switch UPSR Traffic” procedure on page 5-25 for UPSR protection switch procedures.
Upgrade a span	Right-click a span and choose Upgrade Span from the shortcut menu.

2.6.2.3 Creating Domains

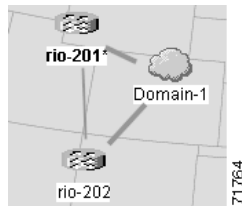
Domains are icons where you can add a group of ONS 15327s or ONS 15454s. Adding domains to the network view map makes networks with many nodes easier to manage. After you create a domain, you can drag and drop ONS 15327 icons into it (Figure 2-8). The ONS 15327s are hidden until you open the domain. Figure 2-10 shows an example of an opened domain.

Figure 2-8 Adding nodes to a domain



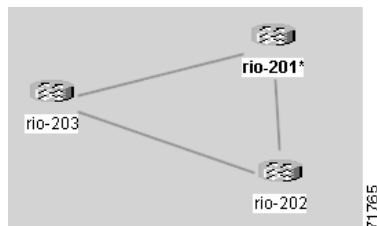
After you add a node to a domain, the span lines leading to nodes within the domain become thicker (Figure 2-9). The thick lines may represent multiple spans. For example, if the “rio-104” node in Figure 2-9 is connected to two nodes within domain-0, the thick line represents two spans. The thick line is green if all spans it represents are active and grey if any one span it represents is down. The domain icon color reflects the highest alarm severity of any node within it.

Figure 2-9 Outside nodes displayed within the domain



Within the domain, external nodes and domains that are directly connected to nodes inside the domain are displayed in a dimmed color (Figure 2-10). DCC links with one or two ends inside the domain are also displayed.

Figure 2-10 Nodes inside a domain



You manage ONS 15327s that reside within a domain the same way you manage ONS 15327s on the network map. Table 2-13 shows the domain actions.

**Note**

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

Table 2-13 Managing Domains

Action	Procedure
Create a domain	Right-click the network map and choose Create New Domain from the shortcut menu. When the domain icon appears on the map, type the domain name.
Move a domain	Press Ctrl and click and drag the domain icon to the new location.
Rename a domain	Right-click the domain icon and choose Rename Domain from the shortcut menu. Type the new name in the domain name field. Press Enter .
Add a node to a domain	Drag a node icon to the domain icon. Release the mouse button when the node icon is over the domain icon.
Move a node from a domain to the network map	Right-click a node and choose Move Node Back To Parent View .
Open a domain	<ul style="list-style-type: none"> • Double-click the domain icon. • Right-click the domain and choose Open Domain.
Return to network view	Right-click the domain view area and choose Go to Parent View from the shortcut menu.
Preview domain contents	Right-click the domain icon and choose Show Domain Overview . The domain icon shows a small preview of the nodes in the domain. To turn off the domain overview, right-click the preview and select Show Domain Overview .
Remove domain	Right-click the domain icon and choose Remove Domain . Any nodes residing in the domain are returned to the network map.

2.6.2.4 Changing the Network View Background Color

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

Procedure: Modify the Network View or Domain Background Color

-
- Step 1** Right-click the network view or domain map area and choose **Set Background Color** from the shortcut menu.
- Step 2** On the Choose Color dialog box, select a background color.
- Step 3** Click **OK**.
-

2.6.2.5 Changing the Network View Background Image

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



Note

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

Procedure: Change the Network View Background Image

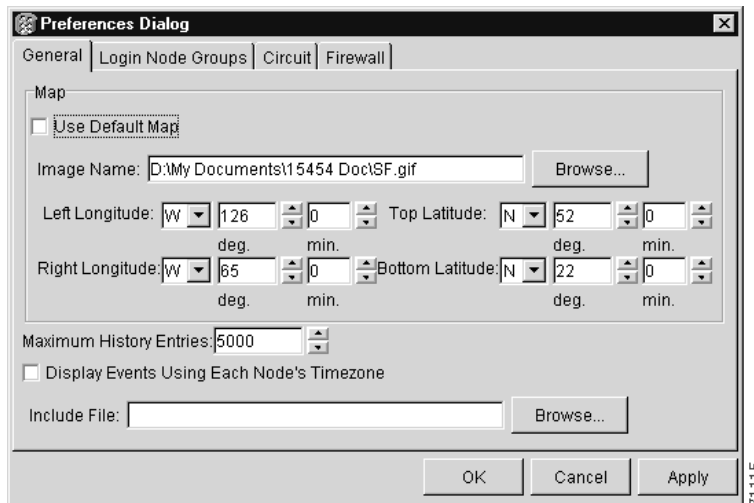


Caution

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

- Step 1** In network view, choose **Edit > Preferences**. (You also right-click the network or domain map and select **Set Background Image**.)
- Step 2** On the **General** tab of the Preferences dialog box (Figure 2-11), deselect **Use Default Map**.

Figure 2-11 Changing the CTC background image



- Step 3** Click **Browse**. Navigate to the graphic file you want to use as a background.
- Step 4** Select the file. Click **Open**.
- Step 5** (Optional) Enter the coordinates for the map image edges in the longitude and latitude fields on the Preferences dialog box. CTC uses the map's longitude and latitude to position the node icons based on the node coordinates entered for each node on the Provisioning > General tabs. Coordinates only need to be precise enough to place ONS node icons in approximate positions on the image. You can also drag and drop nodes to position them on the network view map.

- Step 6** Click **Apply** and then click **OK**.
- Step 7** At the network view, use the CTC toolbar Zoom buttons (or right-click the graphic area and select a Zoom command from the shortcut menu) to set the area of the image you can view.
-

Procedure: Add a Node to the Current Session

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

- Step 1** From the CTC File menu, click **Add Node** (or click the Add Node button on the toolbar).
- Step 2** On the Add Node dialog box, enter the node name (or IP address).
- Step 3** If you want to add the node to the current login group, click **Add Node to Current Login Group**. Otherwise, leave it unchecked.
- Step 4** Click **OK**.

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

2.6.3 Card View

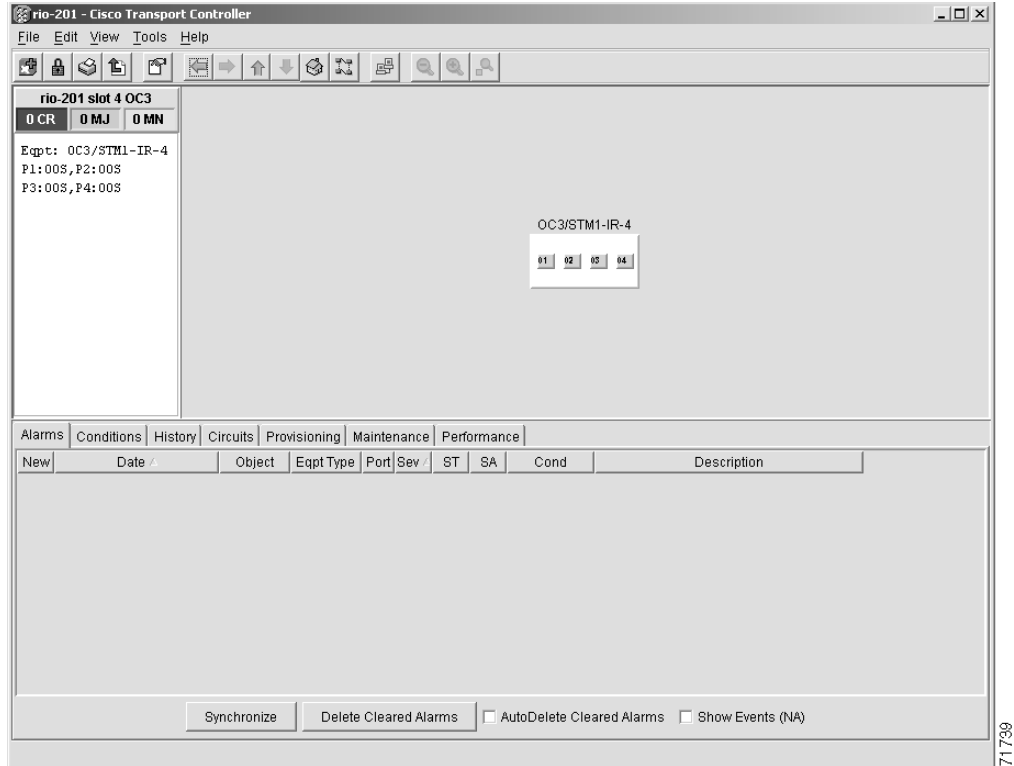
Card view displays information about individual ONS 15327 cards and is the window where you perform card-specific maintenance and provisioning (Figure 2-12). A graphic of the selected card is shown in the graphic area. The status area displays the node name, slot, number of alarms, card type, equipment type, and either the card status (active or standby) or port status (IS [in service] or OOS [out of service]). The information that is displayed and the actions you can perform depend on the card.



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

Card view provides access to the following tabs: Alarms, History, Circuits, Provisioning, Maintenance, Performance, and Conditions. The subtabs, fields, and information displayed under each tab depend on the card type selected.

Figure 2-12 CTC card view showing an OC3 IR 1310 card



2.7 CTC Navigation

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

Figure 2-13 CTC node view showing popup information

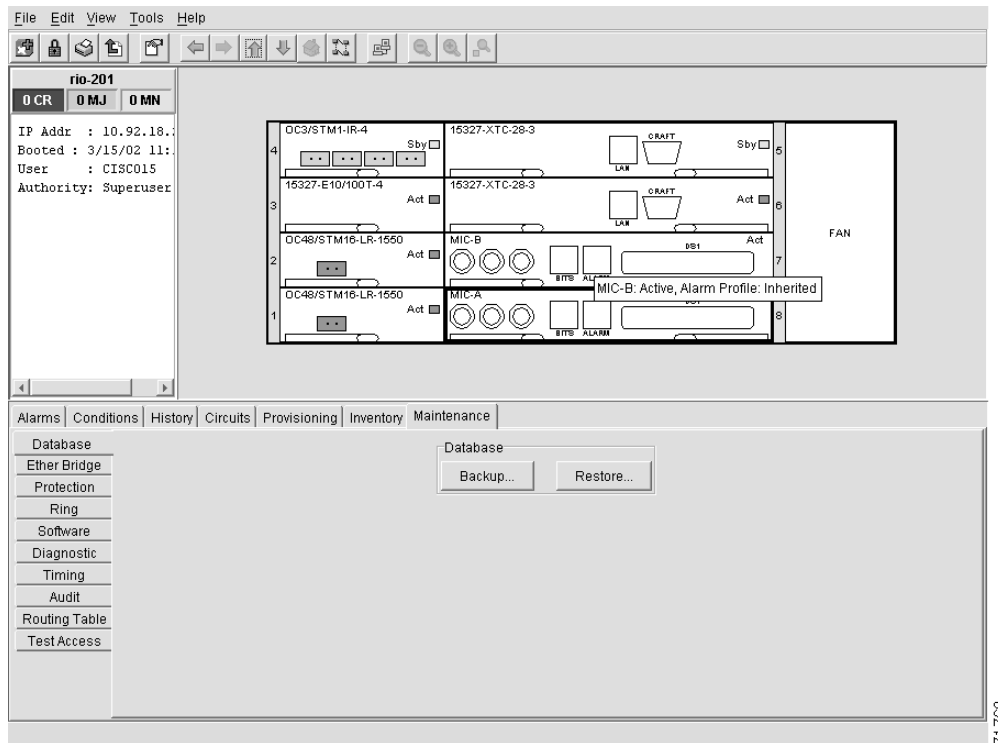


Table 2-14 describes different methods for navigating within the CTC window.

Table 2-14 CTC Window Navigation

Technique	Description
View menu and Toolbar	<p>You can choose from:</p> <ul style="list-style-type: none"> Go to Previous View (available after you navigate to two or more views) Go to Next View (available after you navigate to previous views) Go to Parent View (parent of the currently-selected view. Network is the parent of node view; node view is the parent of card view.) Go to Currently Selected Object (For example, selecting a card on the node view graphic displays the card in card view; selecting a node on the network view map displays the node in node view.) Go to Home View (the node you initially logged into) Go to Network View The Other Node (View menu only) Different zoom levels (toolbar only, network view only)
Double-Click	<ul style="list-style-type: none"> A node in network view to display the node view A card in node view to display the card view

Table 2-14 CTC Window Navigation (continued)

Technique	Description
Right-Click	<ul style="list-style-type: none"> • Network view graphic area—Displays a menu where you can create a new domain, change the position and zoom level of the graphic image, and change the background image and color. • Node in network view—Displays a menu where you can open the node, provision circuits, update circuits with a new node, and reset the node icon position to the longitude and latitude set on the Provisioning > General tabs. • Span in network view—Displays a menu where you can view information about the source and destination ports, the span’s protection scheme, and the span’s optical or electrical level. You can also display the Circuits on Span dialog box, which displays additional span information and allows you to perform UPSR protection switching. • Card in node view—Displays a menu where you can open, delete, reset, and change cards. The card that is selected determines the commands that are displayed.
Move Mouse Cursor	<ul style="list-style-type: none"> • Over node in network view—Displays a summary of node alarms and provides a warning if the node icon has been moved out of the map range • Over span in network view—Displays circuit (node, slot, port) and protection information • Over card in node view—Displays card type and card status • Over card port in node view—Displays port number and port status

2.8 Viewing CTC Table Data

Much of the ONS 15327 data that CTC displays, such as alarms, alarm history, circuits, and inventory, is displayed in tables. You can change the way the CTC tables are displayed. For example, you can:

- Rearrange or hide table columns
- Sort tables by primary and secondary keys in descending or ascending order. (Sorting and hiding is available for all read-only tables.)
- Export CTC table data to spreadsheets and database management programs to perform additional data manipulation. To export table data, see the “Printing and Exporting CTC Data” section on page 2-41.

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

Figure 2-14 Table shortcut menu that customizes table appearance

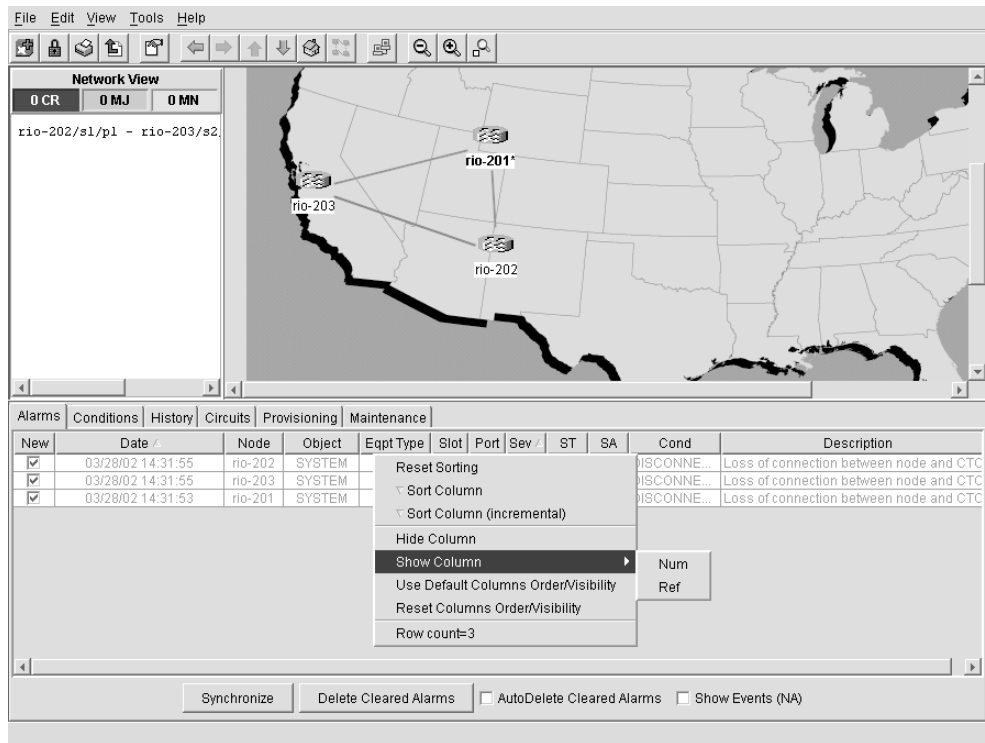


Table 2-15 lists the options that you can use to customize information that is displayed in CTC tables.

Table 2-15 Table Display Options

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

Table 2-15 Table Display Options (continued)

Task	Click	Right-Click Shortcut Menu
Reset sorting	N/A	Choose Reset Sorting
View table row count	N/A	Choose Row count ; it is the last item on the shortcut menu

2.9 Printing and Exporting CTC Data

You can print CTC windows and table data such as alarms and inventory using the File menu. You can also export CTC table data for use by other applications such as spreadsheets, word processors, and database management applications. Table 2-16 shows CTC data that can be exported.

Table 2-16 Table Data with Export Capability

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

Table 2-16 Table Data with Export Capability (continued)

View or Card	Tab	Subtab(s)
	Circuits	
	Provisioning	Line/Threshold/STS/Alarm Behavior
	Maintenance	Loopback/Info
	Performance	
XTC (DS-N) Cards	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	DS1 (Line/Line Threshold/Electric Path Threshold/Sonet Path Threshold/Alarming)
		DS3 (Line/Line Threshold/STS 1 Path Threshold/Alarming)
		External Alarms
		External Controls
E10/100T-4	Alarms	
	Conditions	
	History	Session/Card
	Circuits	
	Provisioning	Port/VLAN/Alarm Behavior
	Performance	Statistics/Utilization/History

Procedure: Print CTC Window and Table Data

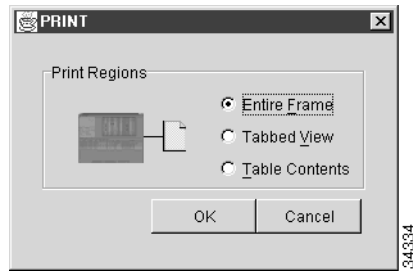
Use the following procedure to print CTC windows and table data. Before you start, make sure your PC is connected to a printer.

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

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

- *Entire Frame*—Prints the entire CTC window
- *Tabbed View*—Prints the lower half of the CTC window
- *Table Contents*—Prints CTC data in table format; this option is only available for CTC table data (see the “Viewing CTC Table Data” section on page 2-39).

Figure 2-15 Selecting CTC data for print



Step 3 Click **OK**.

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

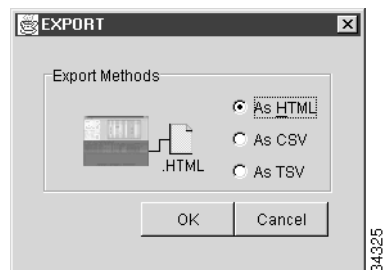
Procedure: Export CTC Data

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

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

- *As HTML*—Saves the data as an HTML file. The file can be viewed with a web browser without running CTC.
- *As CSV*—Saves the CTC table values as text, separated by commas. You can import CSV data into spreadsheets and database management programs.
- *As TSV*—Saves the CTC table values as text, separated by tabs. You can import TSV data into spreadsheets and database management programs.

Figure 2-16 Selecting CTC data for export



Step 3 Click **OK**.

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

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

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

Step 6 Click **OK**.

2.10 Displaying CTC Data in Other Applications

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

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

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



Node Setup

This chapter explains how to set up a Cisco ONS 15327 node using the Cisco Transport Controller (CTC). Topics include:

- Setting up general node information
- Setting up network information
- Creating, editing, and deleting ONS 15327 users and assigning user security levels
- Setting the node timing references
- Creating card protection groups
- Viewing node inventory
- Viewing CTC software versions

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

3.1 Before You Begin

Before you begin node setup, review the following checklist to ensure you have the prerequisite information. Basic node information that you will need includes node name, contact, location, date, and time. If the ONS 15327 will be connected to a network, you will need:

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

If you are responsible for setting up IP networking for the ONS 15327 network, see Chapter 4, “IP Networking” for more information.

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

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



Note

You must be able to log into the node to complete node provisioning. If you cannot log into the node, see “Connecting PCs to the ONS 15327” section on page 2-20.

3.2 Setting Up Basic Node Information

Setting basic information for each Cisco ONS 15327 node is one of the first provisioning tasks you perform. This information includes node name, location, contact, and timing. Completing the information for each node facilitates ONS 15327 management, particularly when the node is connected to a large ONS 15327 or ONS 15454 network.

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

Step 1 Log into the ONS 15327 node. The CTC node view is displayed.

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

Step 3 Enter the following:

- *Node Name*—Type a name for the node. For TL1 compliance, names must begin with an alpha character and have no more than 20 alphanumeric characters.
- *Contact*—Type the name of the node contact person and the phone number (optional).
- *Location (Description)*—Type the node location, for example, a city name or specific office location (optional).
- *Latitude*—Enter the node latitude: N (North) or S (South), degrees, and minutes (optional).
- *Longitude*—Enter the node longitude: E (East) or W (West), degrees, and minutes (optional).

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

- *Use NTP/SNTP Server*—When checked, CTC uses a Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) server to set the date and time of the node.

If you do not use an SNTP or NTP server, complete the *Date* and *Time* fields. The ONS 15327 will use these fields for alarm dates and times. (CTC displays all alarms in the login node's time zone for cross network consistency.)



Note Using an NTP or SNTP server ensures that all ONS 15327 network nodes use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

If you check *Use NTP/SNTP Server*, type the IP address of either (a) an NTP/SNTP server, or (b) the IP address of an ONS 15327 with NTP/SNTP Server enabled. If you enable *Enable Firewall* for the ONS 15327 proxy server, external ONS 15327 NEs must reference the gateway ONS 15327 NE for NTP/SNTP timing.



Caution

If you reference another ONS 15327 for the NTP/SNTP server, make sure the second ONS 15327 references an NTP/SNTP server, and not the first ONS 15327. That is, do not create an NTP/SNTP timing loop by having two ONS 15327s reference each other.

- *Date*—If *Use NTP/SNTP Server* is not selected, type the current date in the format mm/dd/yyyy, for example, September 24, 2002 is 09/24/2002.

- *Time*—If *Use NTP/SNTP Server* is not selected, type the current time in the format hh:mm:ss, for example, 11:24:58. The ONS 15327 uses a 24-hour clock, so 10:00 PM is entered as 22:00:00.
- *Time Zone*—Click the field and choose the time zone from the pop-up menu.

Step 4 Click **Apply**.

Step 5 On the confirmation dialog box, click **Yes**.

Step 6 Review the node information. If you need to make corrections, repeat Steps 3 – 5 to enter the corrections.

3.3 Setting Up Network Information

ONS 15327s almost always operate in network environments. Before you connect an ONS 15327 to other ONS 15327s or to a LAN, you must change the default IP address that is shipped with each ONS 15327 (192.1.0.2). IP addresses are unique identifiers for devices—called hosts—that connect to TCP/IP networks. Every IP address includes a network number, which is assigned to an organization, and a host (device) number, which the organization’s LAN administrator assigns to an individual network device. Subnetting enables LAN administrators to create subnetworks that are transparent to the Internet. Within networks, ONS 15327s often exist as subnetworks, which are created by adding a subnet mask to the ONS 15327 IP address.

The following procedure tells you how to set up the essential ONS 15327 networking information. Additional ONS 15327 networking information and procedures, including IP addressing examples, static route scenarios and Open Shortest Path First (OSPF) protocol options are provided in Chapter 4, “IP Networking.”

Procedure: Set Up Network Information

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

Step 2 Complete the following:

- *IP Address*—Type the IP address assigned to the ONS 15327 node.
- *Default Router*—If the ONS 15327 must communicate with a device on a network to which the ONS 15327 is not connected, the ONS 15327 forwards the packets to the default router. Type the IP address of the router in this field. If the ONS 15327 is not connected to a LAN, leave the field blank.
- *Subnet Mask Length*—If the ONS 15327 is part of a subnet, type the subnet mask length (decimal number representing the subnet mask length in bits) or click the arrows to adjust the subnet mask length. The subnet mask length is the same for all ONS 15327s in the same subnet.

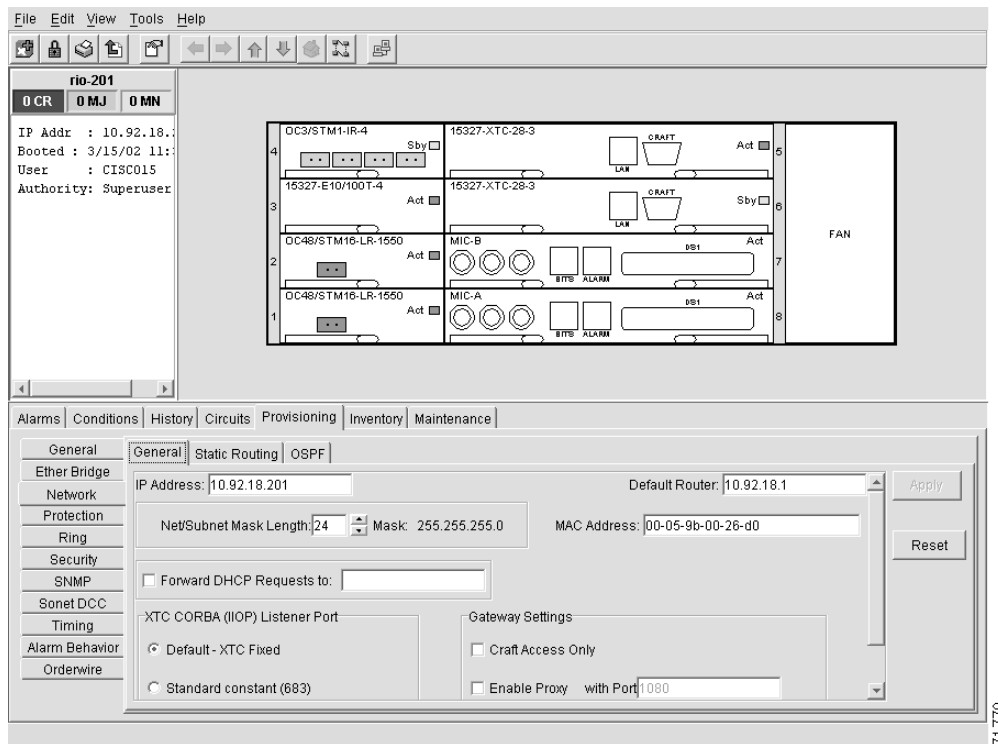


Note The MAC Address is read only. It displays the ONS 15327 address as it is identified on the IEEE 802 Media Access Control (MAC) layer.

- *Forward DHCP Request To*—When checked, forwards Dynamic Host Configuration Protocol requests to the IP address entered in the Request To field. DHCP is a TCP/IP protocol that enables CTC computers to get temporary IP addresses from a server. If you enable DHCP, CTC computers that are directly connected to an ONS 15327 node can obtain temporary IP addresses from the DHCP server.

- *XTC CORBA (IIOP) Listener Port*—Sets a listener port to allow communication with the ONS 15327 through firewalls. See the “Accessing ONS 15327s Behind Firewalls” section on page 2-27 for more information.

Figure 3-1 Setting up general network information



Step 3 Click **Apply**.

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

Both ONS 15327 XTC cards will reboot, one at a time.

3.4 Creating Users and Setting Security

The CISCO15 user provided with each ONS 15327 can be used to set up other ONS 15327 users. You can add up to 500 users to one ONS 15327. Each ONS 15327 user can be assigned one of the following security levels:

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

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

Table 3-1 ONS 15327 Security Levels—Node View

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser	
Alarms	n/a	Synchronize alarms	X	X	X	X	
Conditions	n/a	Retrieve	X	X	X	X	
History	Session	Read only					
	Node	Retrieve Alarms/Events	X	X	X	X	
Circuits	n/a	Create/Delete/Edit/ Upgrade			X	X	
		Path Selector Switching		X	X	X	
		Search	X	X	X	X	
		Switch retrieval	X	X	X	X	
Provisioning	General	Edit			X	X	
	EtherBridge	Spanning Trees: Edit			X	X	
		Thresholds: Create/Delete			X	X	
	Network	All				X	
	Protection	Create/Delete/Edit			X	X	
		Browse groups	X	X	X	X	
	Ring	All (BLSR)			X	X	
	Security	Create/Delete				X	
		Change password	same user	same user	same user	all users	
		SNMP	Create/Delete/Edit				X
		Browse trap destinations	X	X	X	X	
		Sonet DCC	Create/Delete				X
		Timing	Edit			X	X
		Alarm Behavior	Edit			X	X
	Orderwire	Create/Delete				X	
Inventory	n/a	Delete			X	X	
		Reset		X	X	X	
Maintenance	Database	Backup/Restore				X	
	EtherBridge	Spanning Tree Retrieve	X	X	X	X	
		Spanning Tree Clear/Clear all		X	X	X	
		MAC Table Retrieve	X	X	X	X	
		MAC Table Clear/Clear all		X	X	X	
		Trunk Utilization Refresh	X	X	X	X	
	Protection	Switch/lock out operations		X	X	X	
	Ring	BLSR maintenance		X	X	X	
	Software	Download/Upgrade/ Activate/Revert				X	

Table 3-1 ONS 15327 Security Levels—Node View (continued)

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
	Diagnostic	Retrieve/Lamp test		X	X	X
	Timing	Edit		X	X	X
	Audit	Retrieve	X	X	X	X
	Routing Table	Read only				
	Test Access	Read only				

Each ONS 15327 user has a specified amount of time that he or she can leave the system idle before the CTC window is locked. The lockouts prevent unauthorized users from making changes. Higher-level users have shorter idle times, as shown in Table 3-2.

Table 3-2 ONS 15327 User Idle Times

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

You can perform ONS 15327 user management tasks from network or node view. In network view, you can add, edit, or delete users from multiple nodes at one time. If you perform user management tasks in node view, you can only add, edit, or delete users from that node.

**Note**

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

Procedure: Create New Users

-
- Step 1** In network view, select the **Provisioning > Security** tabs.
- Step 2** On the Security pane, click **Create**.
- Step 3** In the Create User dialog box, enter the following:
- *Name*—Type the user name.
 - *Password*—Type the user password. The password must be a minimum of six and a maximum of ten alphabetic (a-z, A-Z), numeric, (0-9) and special characters (+, #, %), where at least one character is alphabetic, one is numeric, and one is a special character.
 - *Confirm Password*—Type the password again to confirm it.
 - *Security Level*—Select the user's security level.
- Step 4** Under "Select applicable nodes," deselect any nodes where you do not want to add the user (all network nodes are selected by default).
- Step 5** Click **OK**.
-

Procedure: Edit a User

-
- Step 1** In network view, select the **Provisioning > Security** tabs.
- Step 2** Click **Change**.
- Step 3** On the Change User dialog box, edit the user information: name, password, password confirmation, and/or security level. (A Superuser does not need to enter an old password. Other users must enter their old password when changing their own passwords.)



Note You cannot change the CISCO15 user name. The CISCO15 password can and should be changed if you need to restrict the number of superusers accessing the ONS 15327.

- Step 4** If you do not want the user changes to apply to all network nodes, deselect the unchanged nodes in the Change Users dialog box.
- Step 5** Click **OK**.
- Changed user permissions and access levels do not take effect until the user logs out of CTC and logs back in.
-

Procedure: Delete a User

-
- Step 1** In network view, select the **Provisioning > Security** tabs.
- Step 2** Click **Delete**.
- Step 3** On the Delete User dialog box, enter the name of the user you want to delete.
- Step 4** If you do not want to delete the user from all network nodes, deselect the nodes.
- Step 5** Click **OK** and click **Apply**.
-

3.5 Creating Protection Groups

The ONS 15327 provides several card protection methods. When you set up 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 3-3 shows the protection types that can be set up for ONS 15327 cards. For a description of protection groups, see the “Card Protection” section on page 13-2.

For the ONS 15327, a 1:1 (electrical) XTC protection group is pre-provisioned. 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.

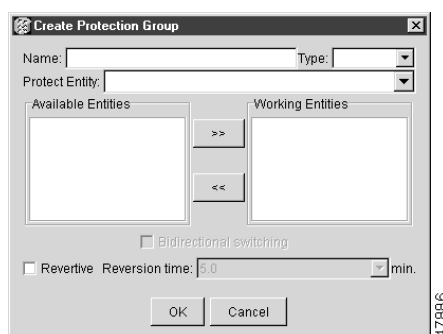
Table 3-3 Protection Types

Type	Cards	Description
1:1	XTC	Default and only available protection for electrical circuits (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.

Procedure: Create Protection Groups for Optical Cards

- Step 1** From the CTC node view, click the **Provisioning** tab.
- Step 2** Click the **Protection** subtab.
- Step 3** Under Protection Groups, click **Create**.
- Step 4** In the Create Protection Group dialog box (Figure 3-2), enter the following:
- *Name*—Type a name for the protection group, up to 32 alphanumeric characters.
 - *Type*—Choose 1+1 as the protection type. The protection selected determines the ports that are available to serve as protect and working ports.
 - *Protect Entity*—Choose protect port from the list. Because 1:1 protection is pre-provisioned, no XTC cards or MICs appear under available cards.

Based on these selections, a list of available working ports displays under Available Entities.

Figure 3-2 Specifying protection attributes in the Create Protection Group dialog box

- Step 5** From the Available Entities list, choose the port that you want to provision as the working port. This port will be protected by the port you selected in Protect Entity. Select the top arrow button to move it to the Working Entities list. You cannot move more than one port.
- Step 6** Complete the remaining fields:
- *Bidirectional switching*—(optical cards only) if checked, both transmit and receive channels switch if a failure occurs to one.

- *Revertive*—if checked, the ONS 15327 reverts back to the working port after failure conditions are corrected.
- *Reversion time*—if *Revertive* is checked, enter the amount of time following a corrected failure condition that the ONS 15327 should switch back to the working port.

Step 7 Click **OK**.



Note

The default XTCPROTGRP provides XTC-level protection for DS-1 and DS-3 ports. It is non-revertive and cannot be modified or deleted.

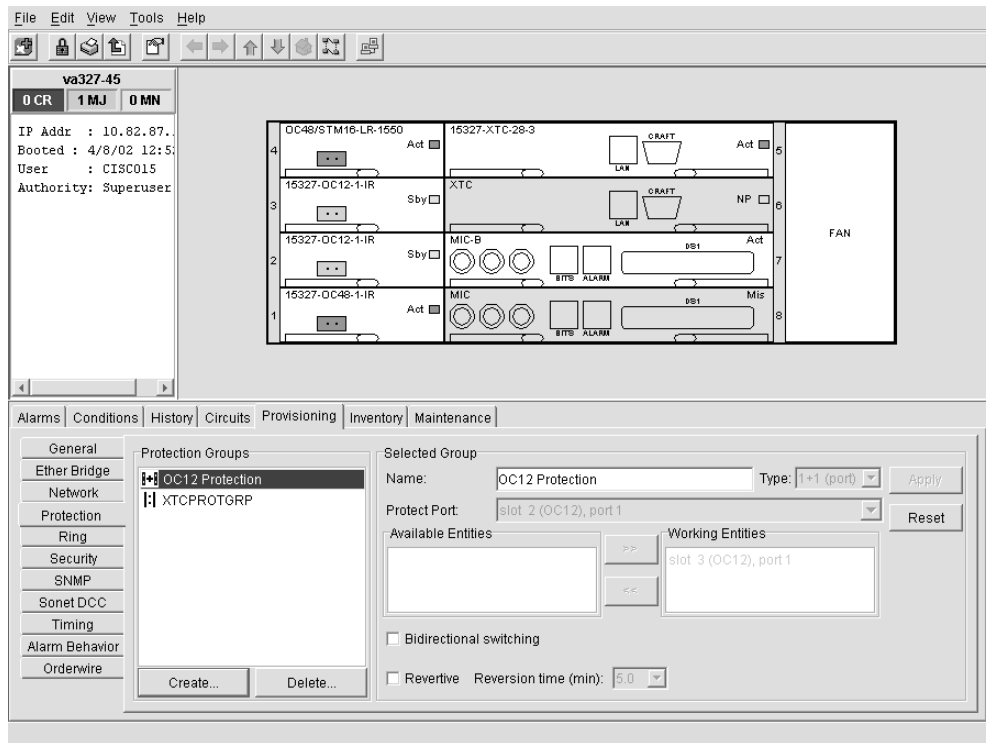
Procedure: Enable Ports

- Step 1** Log into the node in CTC and display the card you want to enable in card view.
- Step 2** Click the **Provisioning > Line** tabs.
- Step 3** Under the Status column, select **In Service**.
- Step 4** Click **Apply**.

Procedure: Edit Protection Groups

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

Figure 3-3 Editing protection groups



- Step 2** In the Protection Groups section, choose a protection group.
- Step 3** In the Selected Group section, edit the fields as appropriate. (For field descriptions, see the “Create Protection Groups for Optical Cards” procedure on page 3-8.)
- Step 4** Click **Apply**.

Procedure: Delete Protection Groups

- Step 1** From the CTC node view, click the **Maintenance > Protection** tabs.
- Step 2** Verify that working traffic is not running on the protect card:
- In the Protection Groups section, choose the group you want to delete.
 - In the Selected Group section, verify that the protect card is in standby mode. If it is in standby mode, continue with Step 3. If it is active, complete Step c.
 - If the working card is in standby mode, manually switch traffic back to the working card. In the Selected Group pane, click the protect card, then click **Manual**. Verify that the protect card switches to standby mode and the working card is active. If it does, continue with Step 3. If the protect card is still active, do not continue. Begin troubleshooting procedures or call technical support.
- Step 3** From the node view, click the **Provisioning > Protection** tabs.
- Step 4** In the Protection Groups section, click a protection group.
- Step 5** Click **Delete**.

3.6 Setting Up ONS 15327 Timing

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

- 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
- A BITS source connected to the BITS port on the MIC

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. In typical ONS 15327 networks:

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

You can set three timing references for each ONS 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.

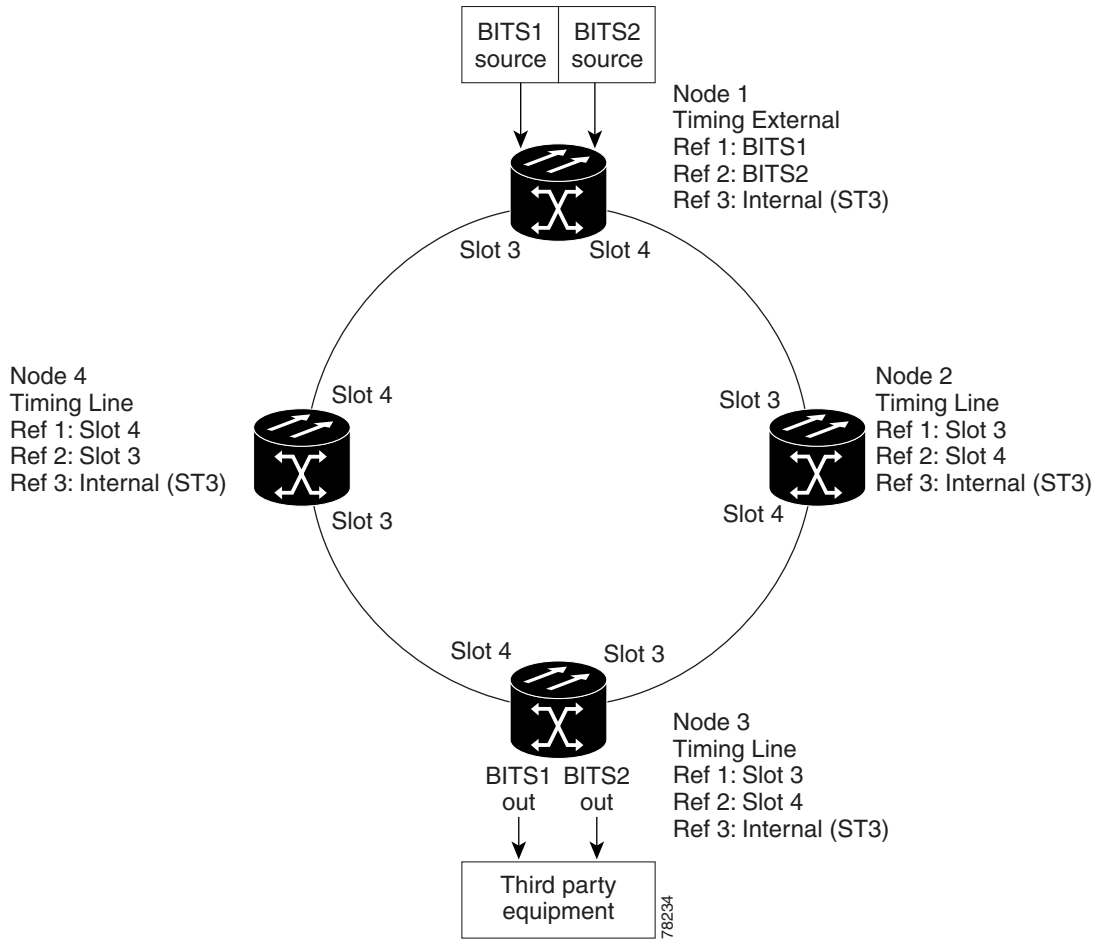
**Caution**

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 this mode with caution.

3.6.1 Network Timing Example

Figure 3-4 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 3-4 An ONS 15327 timing example with external, BITS, and internal timing



3.6.2 Synchronization Status Messaging

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

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

Table 3-4 SSM Generation 1 Message Set

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

Table 3-4 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 3-5 SSM Generation 2 Message Set

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

Procedure: Set Up ONS 15327 Timing

Step 1 From the CTC node view, click the **Provisioning > Timing** tabs (Figure 3-5).

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

- *Timing Mode*—Set to External if the ONS 15327 derives its timing from a BITS source wired to the BITS port on the MIC; set to Line if timing is derived from an OC-N card that is optically connected to the timing node. A third option, Mixed, allows you to set external and line timing references. (Because Mixed timing may cause timing loops, Cisco does not recommend its use. Use this mode with care.)
- *SSM Message Set*—Choose the message set level supported by your network. If a Generation 1 node receives a Generation 2 message, the message will be mapped down to the next available Generation 1. For example, an ST3E message becomes an ST3.
- *Quality of RES*—If your timing source supports the reserved S1 byte, you set the timing quality here. (Most timing sources do not use RES.) Qualities are displayed in descending quality order as ranges. For example, ST3<RES<ST2 means the timing reference is higher than a Stratum 3 and lower than a Stratum 2. See Table 3-4 and Table 3-5 for more information.
- *Revertive*—If checked, the ONS 15327 reverts to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- *Revertive Time*—If Revertive is checked, indicate the amount of time the ONS 15327 will wait before reverting back to its primary timing source.

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



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

- *State*—Set the BITS reference to IS (In Service) or OOS (Out of Service). For nodes set to Line timing with no equipment timed through BITS Out, set State to OOS. For nodes using External timing or Line timing with equipment timed through BITS Out, set State to IS.
- *Coding*—Set to the coding used by your BITS reference, either B8ZS or AMI.
- *Framing*—Set to the framing used by your BITS reference, either ESF (Extended Super Frame, or SF (D4) (Super Frame). SSM is not available with Super Frame.
- *Sync Messaging*—Check to enable SSM.
- *AIS Threshold*—Sets the quality level where a node sends an Alarm Indication Signal (AIS) from the BITS 1 Out and BITS 2 Out MIC connections. When a node times at or below the AIS Threshold quality, AIS is sent (used when SSM is disabled or frame is SF).
- *LBO*—Line build out (LBO) relates to the length of the bits cable. Select the appropriate distance depending on the length of cable required to connect the ONS 15327 BITS port to the BITS timing source.

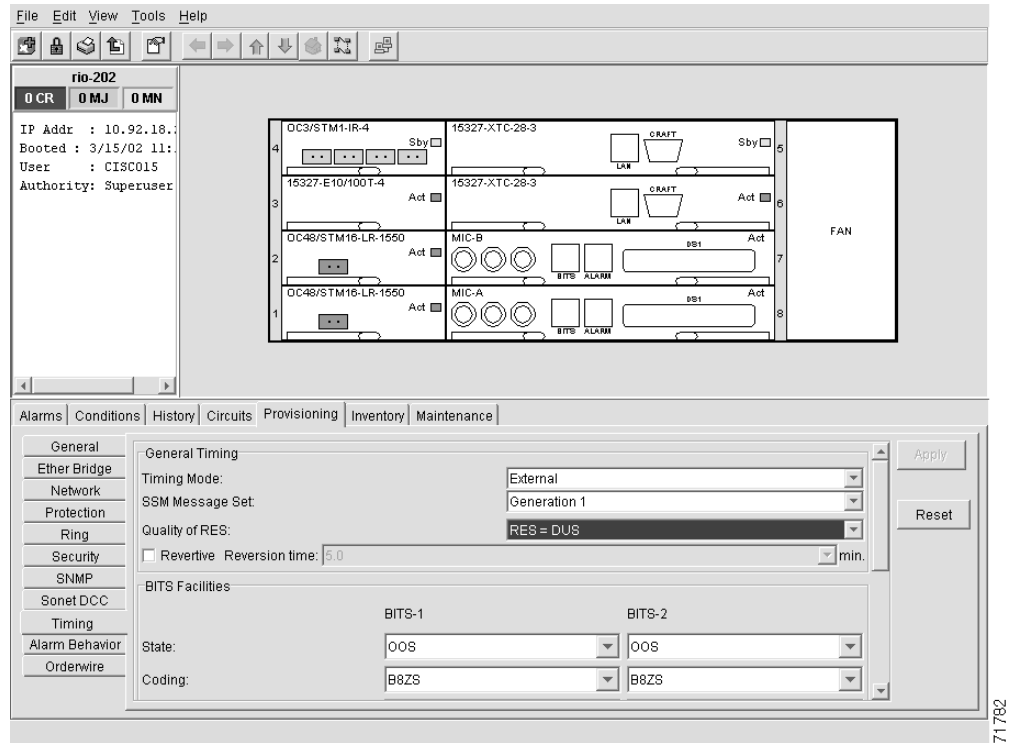
Step 4 Under Reference Lists, complete the following information:



Note Reference lists define up to three timing references for the node and up to six BITS Out references. BITS Out references define the timing references used by equipment that can be attached to the node's BITS Out connections on the MIC. If you attach equipment to BITS Out connections, you normally attach it to a node with Line mode because equipment near the External timing reference can be directly wired to the reference.

- *NE Reference*—Allows you to define three timing references (Ref 1, Ref 2, Ref3). The node uses Reference 1 unless a failure occurs to that reference, in which case, the node uses Reference 2. If that fails, the node uses Reference 3, which is typically set to Internal Clock. This is the Stratum 3 clock provided on the XTC. The options displayed depend on the Timing Mode setting.
 - Timing Mode set to External—options are BITS1, BITS2, and Internal Clock.
 - Timing Mode set to Line—options are the node's working optical cards and Internal Clock. Select the cards/ports that are directly or indirectly connected to the node wired to the BITS source, that is, the node's trunk cards. Set Reference 1 to the trunk card that is closest to the BITS source. For example, if Slot 5 is connected to the node wired to the BITS source, select Slot 5 as Reference 1.
 - Timing Mode set to Mixed—both BITS and optical cards are available, allowing you to set a mixture of external BITS and optical trunk cards as timing references.
- *BITS 1 Out/BITS 2 Out*—Define the timing references for equipment wired to the BITS Out connections on the MIC. Normally, BITS Out is used with Line nodes, so the options displayed are the working optical cards. BITS 1 and BITS 2 Out are enabled as soon as BITS-1 and BITS-2 facilities are placed in service.

Figure 3-5 Setting Up ONS 15327 timing



Step 5 Click **Apply**.



Note Refer to Chapter 10, “Alarm Monitoring and Management,” for timing-related alarms.

Procedure: Set Up Internal Timing

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



Caution

Internal timing is Stratum 3 and not intended for permanent use. All ONS 15327s should be timed to a Stratum 2 or better primary reference source.

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

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

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

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

- *Revertive Time*—The default setting (5 minutes) is sufficient.
- Step 4** In the BITS Facilities section, enter the following information:
- *State*—Set BITS 1 and BITS 2 to OOS (Out of Service).
 - *Coding*—Is not relevant for internal timing. The default (B8ZS) is sufficient.
 - *Framing*—Is not relevant for internal timing. The default (ESF) is sufficient.
 - *Sync Messaging*—Checked
 - *AIS Threshold*—Is not available.
 - *LBO*—Is not relevant for internal timing.
- Step 5** In the Reference Lists section, enter the following information:
- *NE Reference*:
 - Ref1—Set to Internal Clock.
 - Ref2—Set to Internal Clock.
 - Ref3—Set to Internal Clock.
 - *BITS 1 Out/BITS 2 Out*—Set to None
- Step 6** Click **Apply**.
- Step 7** Log into a node that will be timed from the node set up in Steps 1–4.
- Step 8** In the CTC node view, click the **Provisioning > Timing** tabs.
- Step 9** In the General Timing section, enter the same information as entered in Step 3, except for the following:
- *Timing Mode*—Set to Line.
- Reference Lists:
- *NE Reference*:
 - Ref1—Set to the OC-N trunk card with the closest connection to the node in Step 3.
 - Ref2—Set to the OC-N trunk card with the next closest connection to the node in Step 3.
 - Ref3—Set to Internal Clock.
- Step 10** Click **Apply**.
- Step 11** Repeat Steps 7–10 at each node that will be timed by the node in Step 3.
-

3.7 Viewing ONS 15327 Inventory

The Inventory tab (Figure 3-6) displays information about cards installed in the ONS 15327 node including part numbers, serial numbers, hardware revisions, and equipment types. The tab provides a central location to obtain information and to determine applicability of ONS 15327 Product Change Notices (PCNs) and Field Service Bulletins (FSBs). Using the ONS 15327 export feature, you can export inventory data from ONS 15327 nodes into spreadsheet and database programs to consolidate ONS 15327 information for network inventory management and reporting.

Figure 3-6 Displaying ONS 15327 hardware information

Location	Eqpt Type	Actual Eqpt Type	HW Part #	HW Rev	Serial #	CLEI Code	Firmware Rev
Chassis	BACKPLANE_15327						
1	OC48	OC48/STM16-LR-1...	800-17152-01	20	SAG053559V3	NOCLEI	001a
2	OC48	OC48/STM16-LR-1...	800-17152-01	20	SAG053559Q6	NOCLEI	001a
3	ETH100	15327-E10/100T-4	800-07019-01	B0	SAG051440RR	SOIFSARGAA	001a
4	OC3	OC3/STM1-IR-4	800-09189-01	27	SAG054575M3	NOCLEI	57-4982-01
5	XTC	15327-XTC-28-3	800-07661-01	D0	SAG05164CCA	SOIFX20GAA	76-99-00000-X01A
6	XTC	15327-XTC-28-3	800-07661-01	D0	SAG05164CN1	SOIFX20GAA	76-99-00000-X01A
7	MIC	MIC-B	800-07666-03	A0	SAG05154BYL	SOIFY38GAA	unknown
8	MIC	MIC-A	800-07399-03	A0	SAG05154B8N	SOIFY37GAA	unknown
Chassis	FAN_TRAY		800-07246-03	B0	CMC0522005U	SOMYAAKCAA	

The Inventory tab displays the following information about the cards installed in the ONS 15327:

- *Location*—The slot where the card is installed
- *Eqpt Type*—Equipment type the slot is provisioned for, for example, OC-12 or XTC
- *Actual Eqpt Type*—The actual card that is installed in the slot, for example, OC12 IR or XTC-28-3



Tip

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

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

3.8 Viewing CTC Software Versions

CTC software is pre-loaded on the ONS 15327 XTC cards; therefore, you do not need to install software on the XTC. When a new CTC software version is released, you must follow procedures provided by the Cisco Technical Assistance Center (TAC) to upgrade the ONS 15327 software.

When you upgrade CTC software, the XTC stores the older CTC version as the protect CTC version, and the newer CTC release becomes the working version. You can view the software versions that are installed on an ONS 15327 by selecting the Maintenance tab followed by the Software subtab. Select these tabs in node view to display the software installed on one node. Select the tabs in network view to display the software versions installed on all the network nodes.



IP Networking

This chapter explains how to set up Cisco ONS 15327s in internet protocol (IP) networks and includes:

- Scenarios showing Cisco ONS 15327s in common IP network configurations
- Procedures for creating static routes
- Procedures for using the Open Shortest Path First (OSPF) protocol

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



Note

To set up ONS 15327s within an IP network, you must work with a LAN administrator or other individual at your site who has IP networking training and experience. To learn more about IP networking, many outside resources are available. *IP Routing Fundamentals*, by Mark Sportack (Cisco Press, 1999), provides a comprehensive introduction to routing concepts and protocols in IP networks.

4.1 IP Networking Overview

ONS 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 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 can be used to control the visibility and accessibility between CTC computers and ONS 15327 element nodes.

4.2 ONS 15327 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 4-1 provides a general list of items to check when setting up ONS 15327s in IP networks. Additional procedures for troubleshooting Ethernet connections and IP networks are provided in Chapter 9, “Ethernet Operation.”

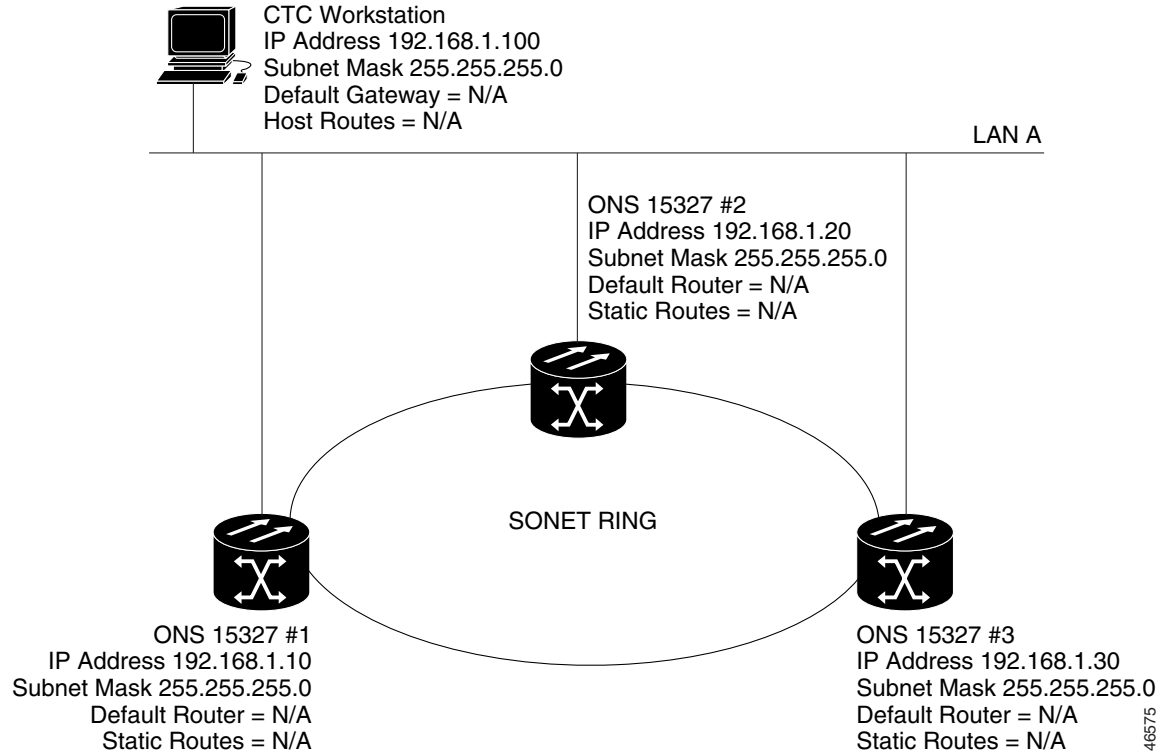
Table 4-1 General ONS 15327 IP Networking Checklist

Item	What to check
Link integrity	Verify link integrity exists between: <ul style="list-style-type: none"> • CTC computer and network hub/switch • ONS 15327s (RJ-45 port) and network hub/switch • Router ports and hub/switch ports
ONS 15327 hub/switch ports	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 ONS 15327 IP addresses and subnet masks are set up correctly.
Optical connectivity	Verify ONS 15327 optical trunk ports are in service; DCC is enabled on each trunk port.

4.2.1 Scenario 1: CTC and ONS 15327s on Same Subnet

Scenario 1 shows a basic ONS 15327 LAN configuration (Figure 4-1). 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 4-1 Scenario 1: CTC and ONS 15327s on same subnet

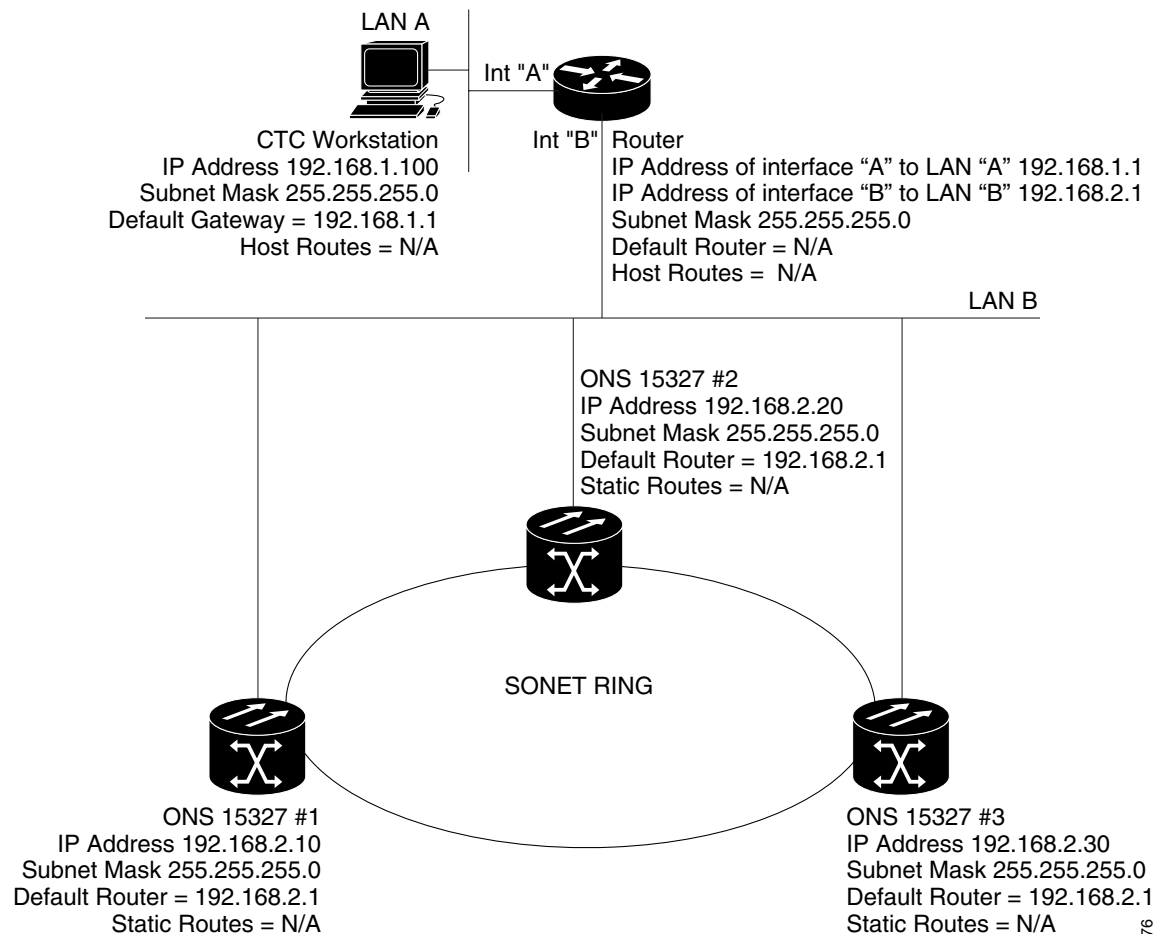


4.2.2 Scenario 2: CTC and ONS 15327s Connected to Router

In Scenario 2 the CTC computer resides on a subnet (192.168.1.0) and attaches to LAN A (Figure 4-2). The ONS 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 DHCP (Dynamic Host Configuration Protocol), the default gateway and IP address are assigned automatically. In the Figure 4-2 example, a DHCP server is not available.

Figure 4-2 Scenario 2: CTC and ONS 15327s connected to router

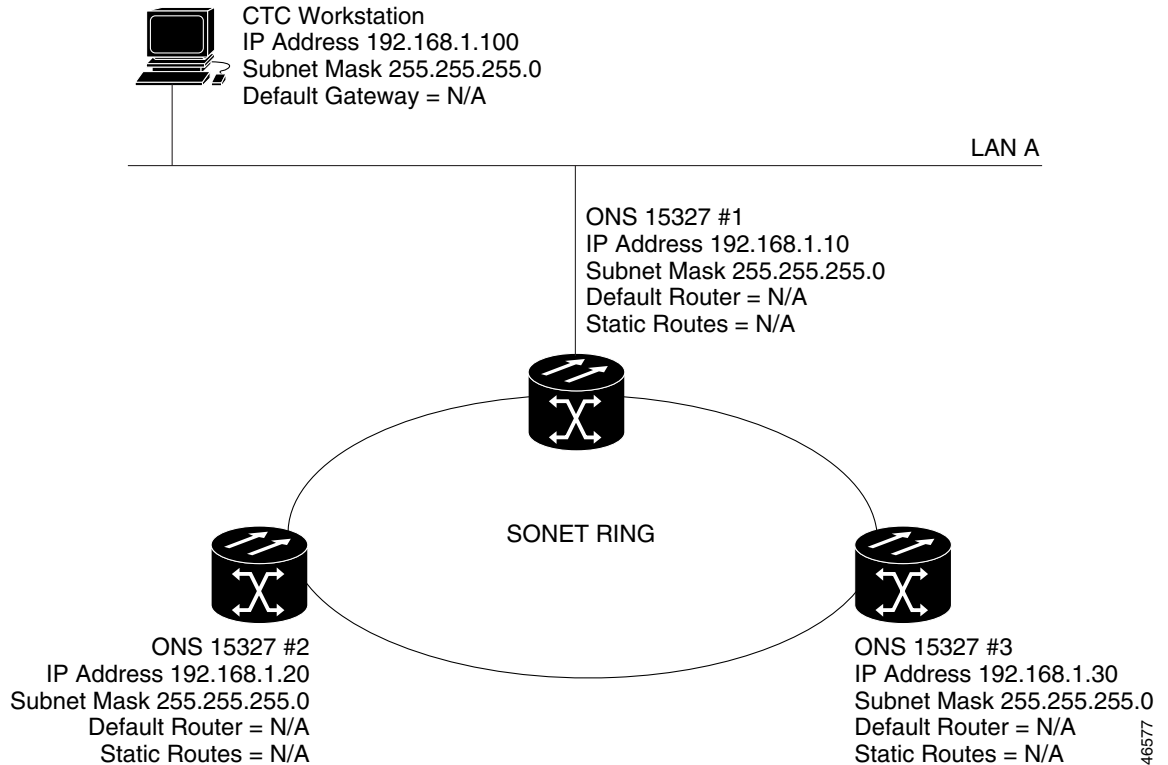


46576

4.2.3 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 4-3). Two ONS 15327s (#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 ONS 15327 #1 to serve as a gateway for ONS 15327s #2 and #3.

Figure 4-3 Scenario 3: Using Proxy ARP



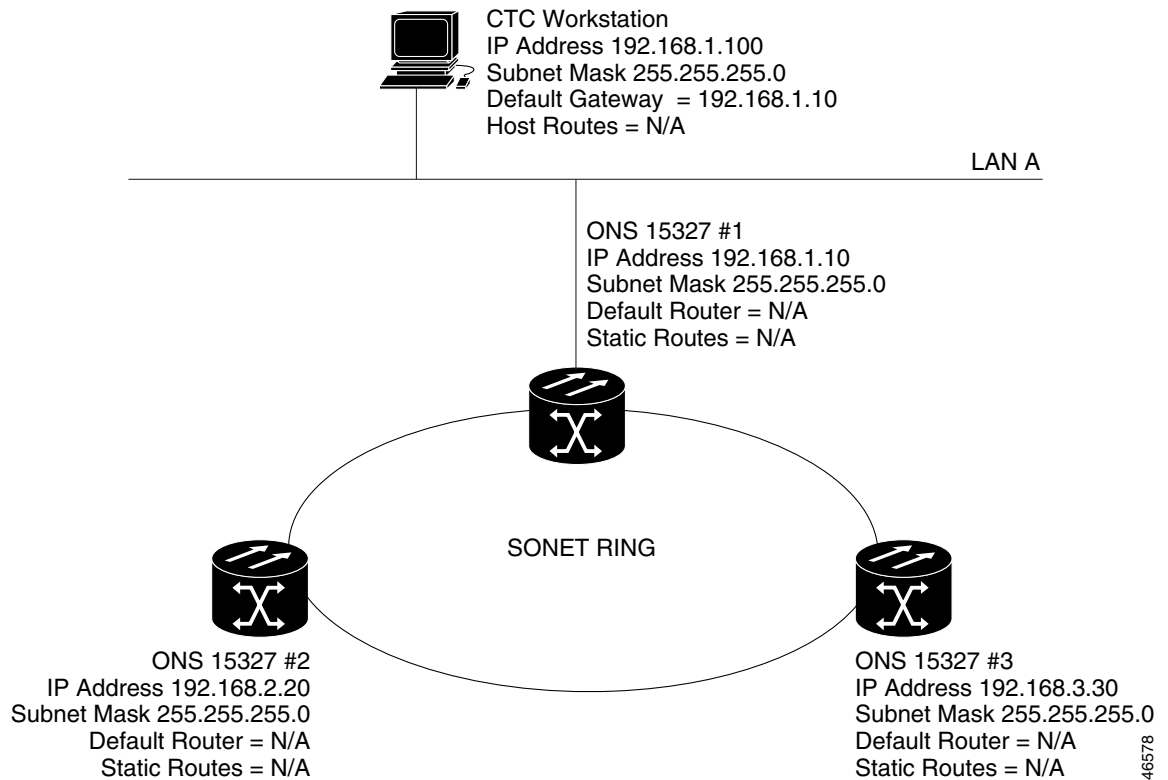
ARP matches higher-level IP addresses to the physical addresses of the destination host. It uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of the machines on the network recognizes its own IP address in the request, it sends an ARP reply back to the requesting host. The reply contains the physical hardware address of the receiving host. The requesting host stores this address in its ARP cache so that all subsequent datagrams (packets) to this destination IP address can be translated to a physical address.

Proxy ARP enables one LAN-connected ONS 15327 to respond to the ARP request for ONS 15327s not connected to the LAN. (ONS 15327 Proxy ARP requires no user configuration.) For this to occur, 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.

4.2.4 Scenario 4: Default Gateway on CTC Computer

Scenario 4 is similar to Scenario 3, but nodes #2 and #3 reside on different subnets, 192.168.2.0 and 192.168.3.0, respectively (Figure 4-4). Node #1 and the CTC computer are on subnet 192.168.1.0. Proxy ARP is not used because the network includes different subnets. In order for the CTC computer to communicate with ONS 15327s #2 and #3, ONS 15327 #1 is entered as the default gateway on the CTC computer.

Figure 4-4 Scenario 4: Default gateway on a CTC computer



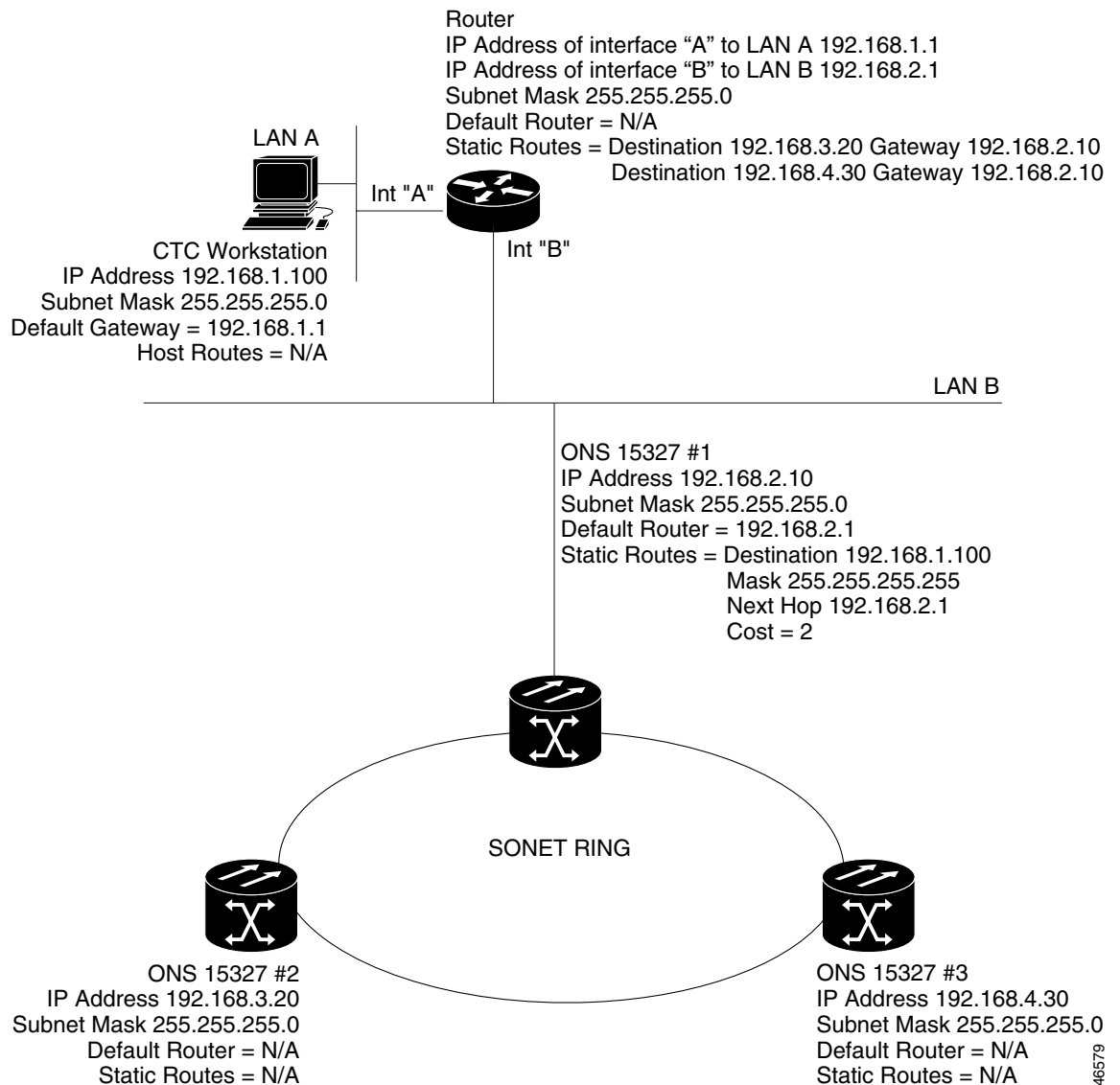
4.2.5 Scenario 5: Using Static Routes to Connect to LANs

Static routes are used for two purposes:

- To connect ONS 15327s to CTC sessions on one subnet connected by a router to ONS 15327s residing on another subnet. (These static routes are not needed if OSPF is enabled. Scenario 7 shows an OSPF example.)
- To enable multiple CTC sessions among ONS 15327s residing on the same subnet.

In Figure 4-5, one CTC residing on subnet 192.168.1.0 connects to a router through interface A. (The router is not set up with OSPF.) ONS 15327s residing on subnet 192.168.2.0 are connected through ONS 15327 #1 to the router through interface B. Proxy ARP enables ONS 15327 #1 as a gateway for ONS 15327s #2 and #3. To connect to CTC computers on LAN A, a static route is created on ONS 15327 #1.

Figure 4-5 Scenario 5: Static route with one CTC computer used as a destination



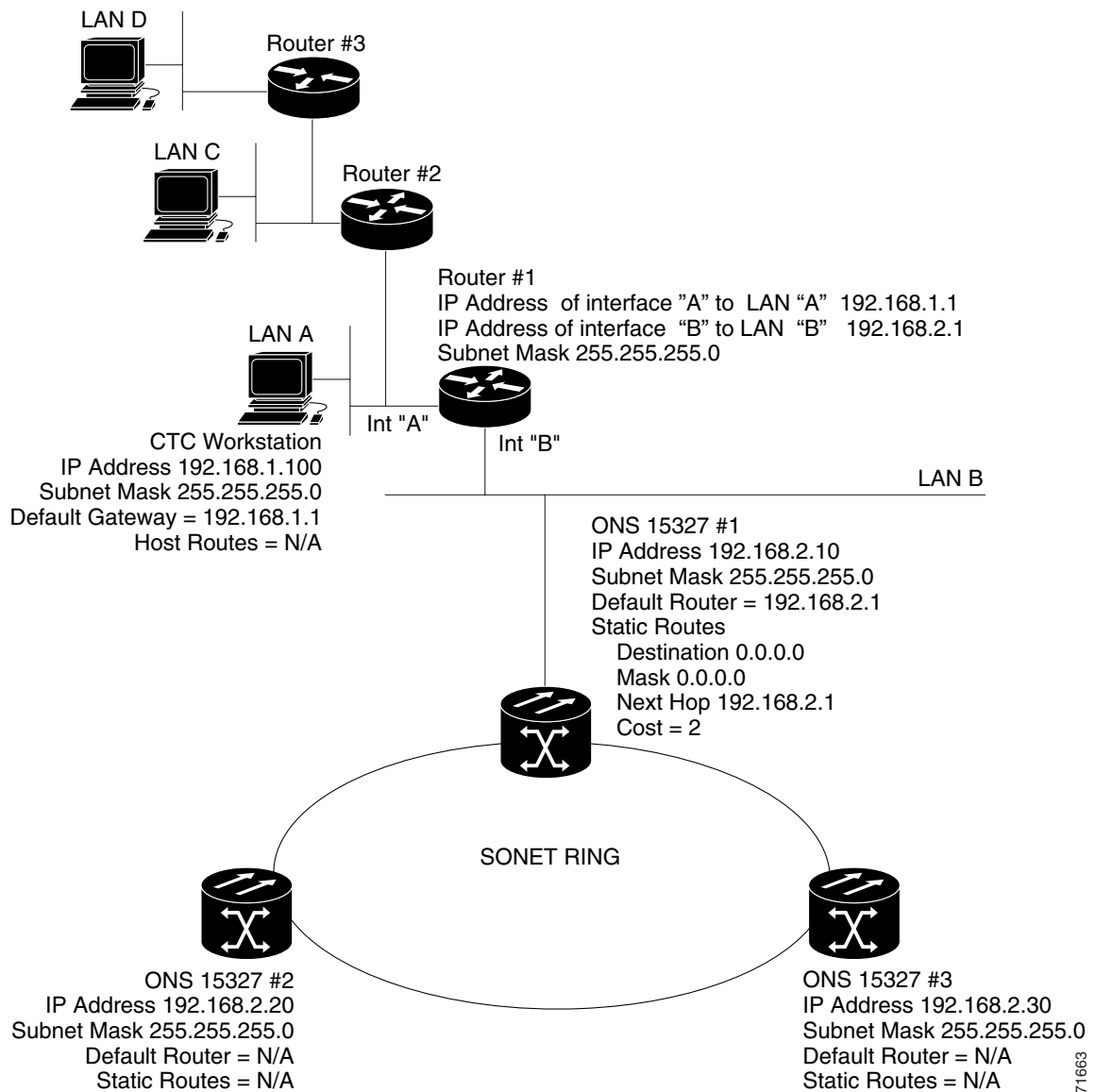
46579

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

- If a single CTC computer is connected to router, enter the complete CTC “host route” IP address as the destination with a subnet mask of 255.255.255.255.
- If CTC computers on a subnet are connected to router, enter the destination subnet (in this example, 192.168.1.0) and a subnet mask of 255.255.255.0.
- If all CTC computers are connected to router, enter a destination of 0.0.0.0 and a subnet mask of 0.0.0.0. Figure 4-6 shows an example.

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

Figure 4-6 Scenario 5: Static route with multiple LAN destinations



71663

4.2.6 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 continuously recalculated to capture ongoing topology changes.

ONS 15327s use the OSPF protocol in internal ONS 15327 networks for node discovery, circuit routing, and node management. You can enable OSPF on the ONS 15327s 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 manually enter static routes for ONS 15327 subnetworks. Figure 4-7 shows the same network enabled for OSPF. Figure 4-8 shows the same network without OSPF. Static routes must be manually added to the router in order for CTC computers on LAN A to communicate with ONS 15327 #2 and #3 because these nodes reside on different subnets.

OSPF divides networks into smaller regions, called areas. An area is a collection of networked end systems, routers, and transmission facilities organized by traffic patterns. Each OSPF area has a unique ID number, known as the area ID, that can range from 0 to 4,294,967,295. Every OSPF network has one backbone area called “area 0.” All other OSPF areas must connect to area 0.

When you enable ONS 15327 OSPF topology for advertising to an OSPF network, you must assign an OSPF area ID to the ONS 15327 network. Coordinate the area ID number assignment with your LAN administrator. In general, all DCC-connected ONS 15327s are assigned the same OSPF area ID.

Figure 4-7 Scenario 6: OSPF enabled

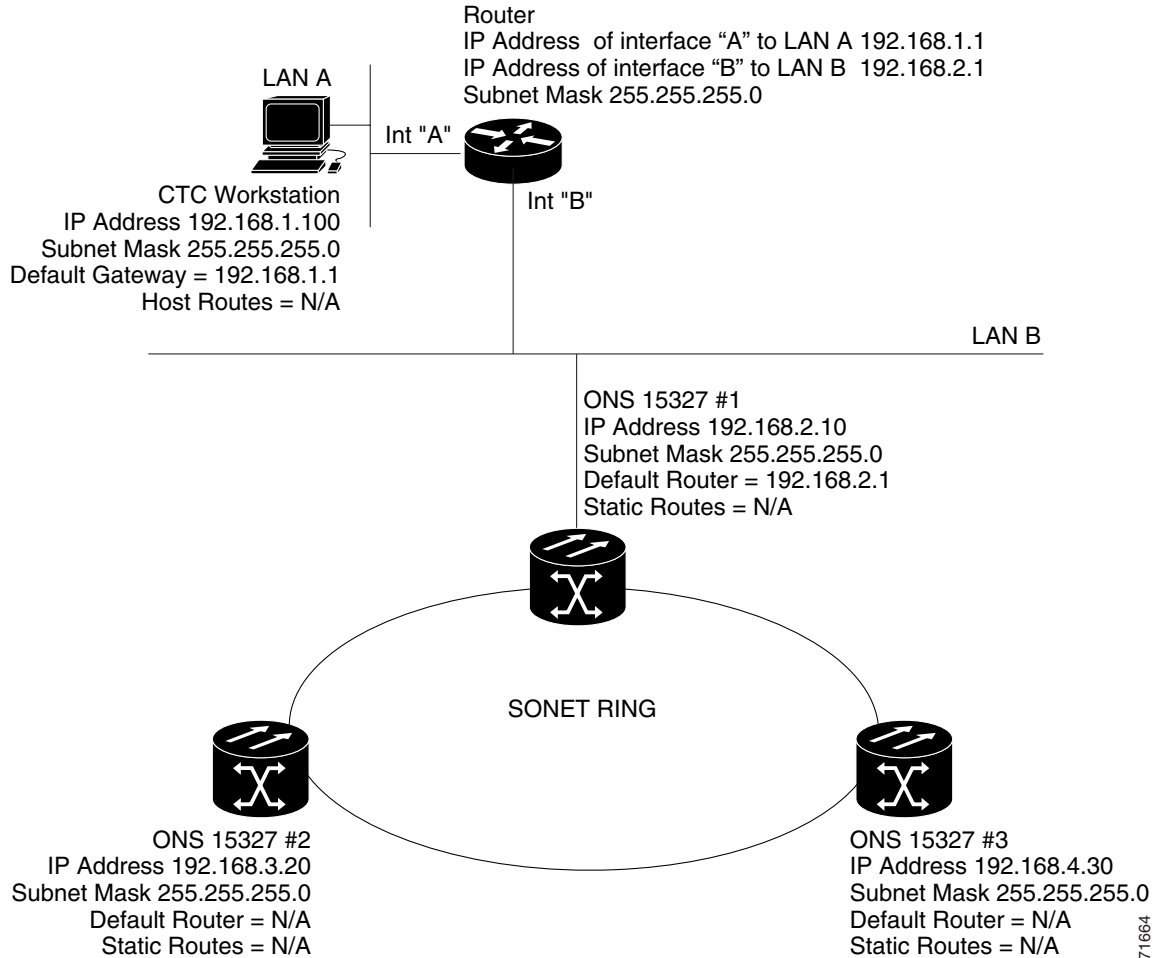
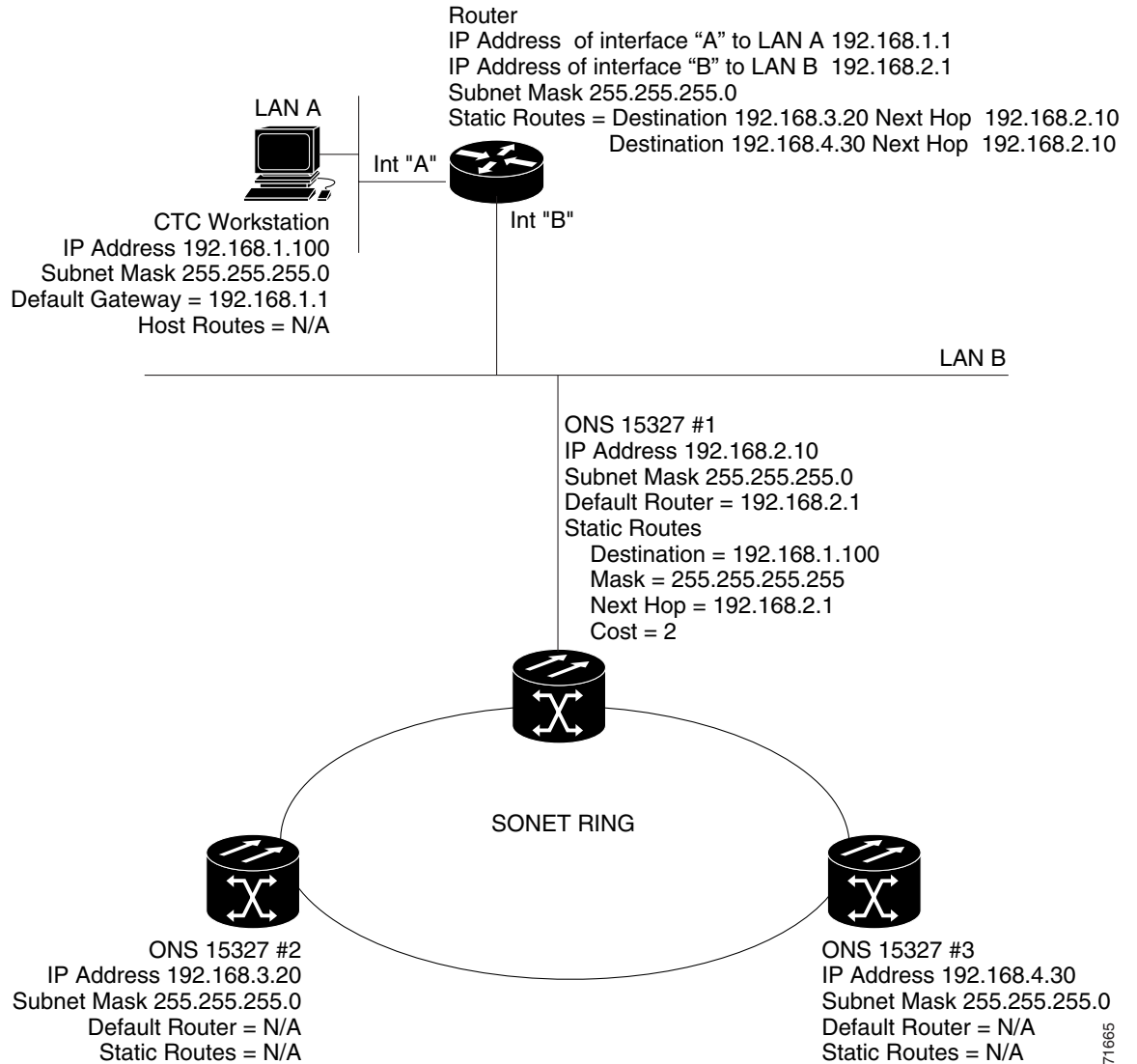


Figure 4-8 Scenario 6: OSPF not enabled



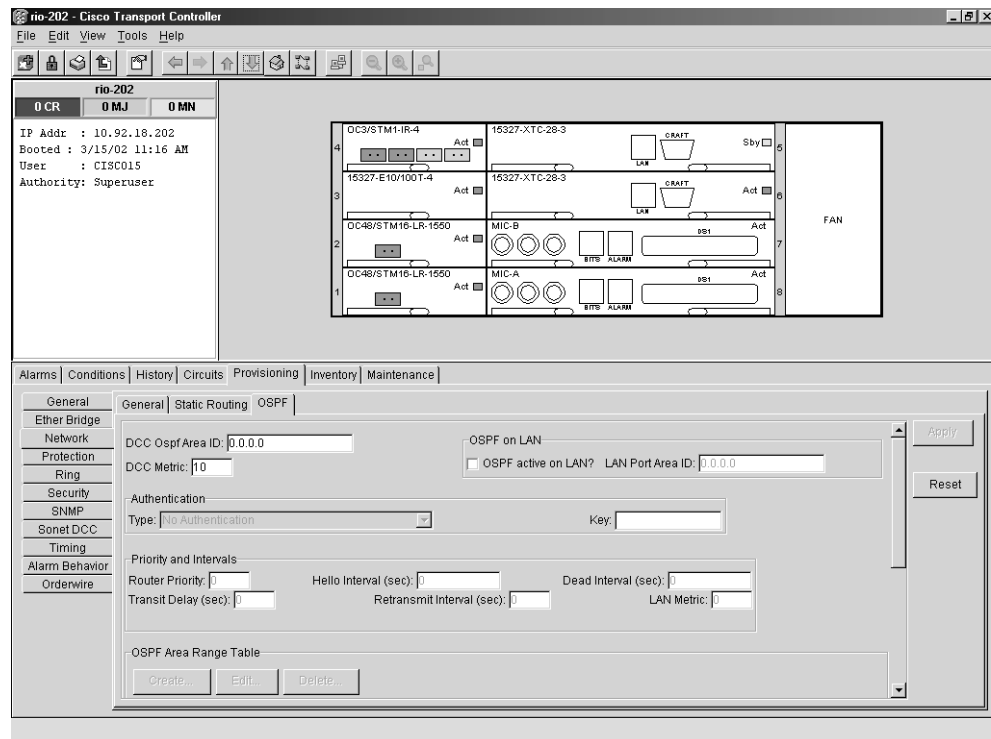
71665

Use the following procedure to enable OSPF on each ONS 15327 node that you want included in the OSPF network topology. ONS 15327 OSPF settings must match router OSPF settings, so you will need to get the OSPF Area ID, Hello and Dead intervals, and authentication key (if OSPF authentication is enabled) from the router to which the ONS 15327 network is connected before enabling OSPF.

Procedure: Set Up OSPF

- Step 1** Display the node view.
- Step 2** Click the **Provisioning** > **Network** > **OSPF** tabs (Figure 4-9).

Figure 4-9 Enabling OSPF on the ONS 15327



- Step 3** On the top left side of the OSPF pane, complete the following:
- *DCC OSPF Area ID*—Enter the number that identifies the ONS 15327s as a unique OSPF area ID entered in dotted decimal format. It can be any number between 000.000.000.000 and 255.255.255.255. The number must be unique to the LAN OSPF area.
 - *DCC Metric*—This value is normally unchanged. It sets a “cost” for sending packets across the DCC, which is used by OSPF routers to calculate the shortest path. This value should always be higher than the LAN metric. The default DCC metric is 10. The metric changes to 100 if you check the *OSPF Active on LAN* check box in Step 4.
- Step 4** Under OSPF on LAN, complete the following:
- *OSPF active on LAN*—When checked, enables ONS 15327 OSPF topology to be advertised to OSPF routers on the LAN. Enable this field on ONS 15327s that directly connect to OSPF routers.

- *Area ID for LAN Port*—Enter the OSPF area ID (dotted decimal format) for the router port where the ONS 15327 is connected. (This number is different from the DCC OSPF Area ID.)

Step 5 Under Authentication, complete the following:

- *Type*—If the router where the ONS 15327 is connected requires authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
- *Key*—If Simple Password is selected as the Authentication type, enter the password (OSPF key).

Step 6 Under Priority and Intervals, complete the following:

The OSPF priority and intervals default to values most commonly used by OSPF routers. In the Priority and Intervals area, verify that these values match those used by the OSPF router where the ONS 15327 is connected.

- *Router Priority*—Used to select the designated router for a subnet.
- *Hello Interval (sec)*—Sets the number of seconds between OSPF “hello” packet advertisements sent by OSPF routers. Ten seconds is the default.
- *Dead Interval*—Sets the number of seconds that will pass while an OSPF router’s packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- *Transit Delay (sec)*—Indicates the service speed. One second is the default.
- *Retransmit Interval (sec)*—Sets the time that will elapse before a packet is resent. Five seconds is the default.
- *LAN Metric*—Sets a “cost” for sending packets across the LAN. This value should always be lower than the DCC metric. Ten is the default.

Step 7 Under OSPF Area Range Table, create an area range table if one is needed:



Note Area range tables consolidate the information that is propagated outside an OSPF Area border. One ONS 15327 in the ONS 15327 OSPF area is connected to the OSPF router. An area range table on this node points the router to the other nodes that reside within the ONS 15327 OSPF area.

- a. Under OSPF Area Range Table, click **Create**.
- b. In the Create Area Range dialog box, enter the following:
 - *Range Address*—Enter the area IP address for the ONS 15327s that reside within the OSPF area. For example, if the ONS 15327 OSPF area includes nodes with IP addresses 10.10.20.100, 10.10.30.150, 10.10.40.200, and 10.10.50.250, the range address would be 10.10.0.0.
 - *Range Area ID*—Enter the OSPF area ID for the ONS 15327s. This is either the ID in the *DCC OSPF Area ID* field or the ID in the *Area ID for LAN Port* field.
 - *Mask Length*—Enter the subnet mask length. In the Range Address example, this is 16.
 - *Advertise*—Check if you want to advertise the OSPF range table.
- c. Click **OK**.

Step 8 All OSPF areas must be connected to Area 0. If the ONS 15327 OSPF area is not physically connected to Area 0, use the following steps to create a virtual link table that will provide the disconnected area with a logical path to Area 0:

- a. Under OSPF Virtual Link Table, click **Create**.

- b. In the Create Virtual Link dialog box, complete the following fields (OSPF settings must match OSPF settings for the ONS 15327 OSPF area):
- *Neighbor*—The router ID of the Area 0 router.
 - *Transit Delay (sec)*—The service speed. One second is the default.
 - *Hello Int (sec)*—The number of seconds between OSPF “hello” packet advertisements sent by OSPF routers. Ten seconds is the default.
 - *Auth Type*—If the router where the ONS 15327 is connected uses authentication, choose **Simple Password**. Otherwise, choose **No Authentication**.
 - *Retransmit Int (sec)*—Sets the time that will elapse before a packet is resent. Five seconds is the default.
 - *Dead Int (sec)*—Sets the number of seconds that will pass while an OSPF router’s packets are not visible before its neighbors declare the router down. Forty seconds is the default.
- c. Click **OK**.

Step 9 After entering ONS 15327 OSPF area data, click **Apply**.

If you changed the Area ID, the XTC cards will reset, one at a time. The reset will take approximately 10-15 minutes.

4.2.7 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 both access the same ONS 15327s while preventing direct access between the field and the NOC LAN. To do this, one ONS 15327 is provisioned as a gateway NE (GNE) and the other ONS 15327s are provisioned as element NEs (ENEs). The GNE ONS 15327 tunnels connections between a CTC computers and ENE ONS 15327s, providing management capability while preventing access for non-ONS 15327 management purposes.

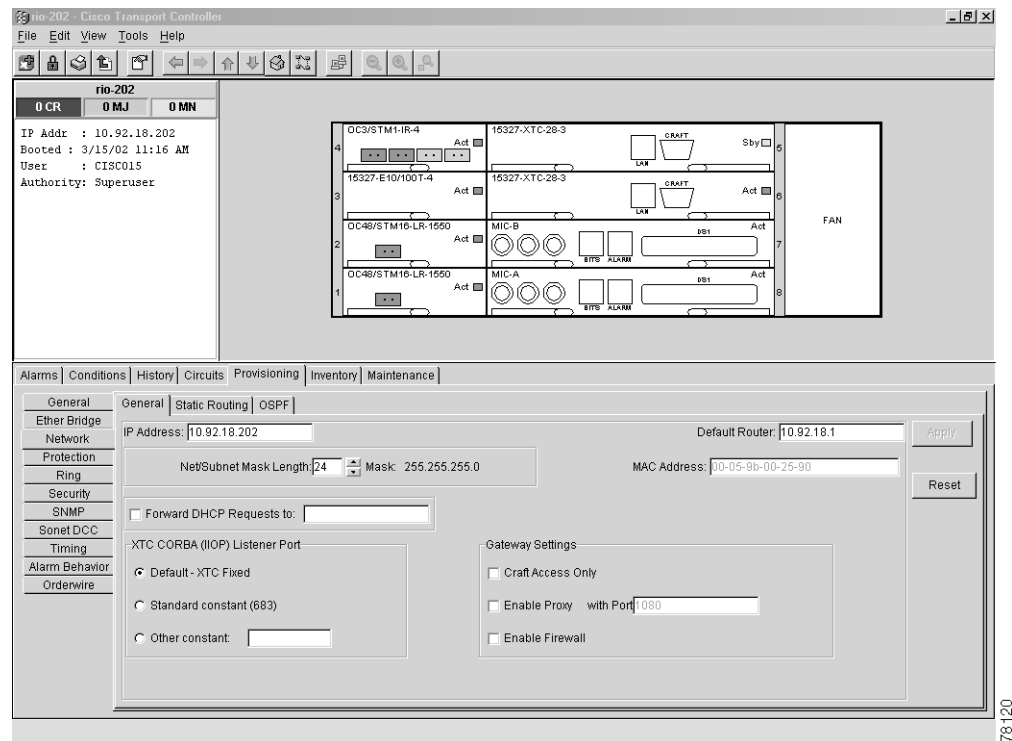
The ONS 15327 proxy server performs the following tasks:

- Isolates DCC IP traffic from Ethernet (craft port) traffic and accepts packets based on filtering rules. The filtering rules 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 timing from an SNTP/NTP LAN server through the GNE ONS 15327.
- Process SNMPv1 traps. The GNE ONS 15327 receives SNMPv1 traps from the ENE ONS 15327s and forwards them to all provisioned SNMPv1 trap destinations.

The ONS 15327 proxy server is provisioned using three checkboxes on the Provisioning > Network > General tab (see Figure 4-10 on page 4-15):

- *Craft Access Only*—When enabled, the ONS 15327 neither installs nor advertises default or static routes. CTC computers can communicate with the ONS 15327, but they cannot communicate directly with any other DCC-connected ONS 15327.
- *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 reach from the host on which it runs. If *Enable Proxy* is off, the node does not proxy for any CTC clients, although any established proxy connections will continue until the CTC client exits.
- *Enable Firewall*—If selected, the node prevents IP traffic from being routed between the DCC and the Ethernet port. The ONS 15327 can communicate with hosts connected to the Ethernet port or connected through the DCC. However, the DCC-connected hosts cannot communicate with the Ethernet-connected hosts, and the Ethernet-connected hosts cannot communicate with the DCC-connected hosts. A CTC client using the Ethernet to connect to the firewall-enabled node can use the proxy capability to manage the DCC-connected nodes that would otherwise be unreachable. A CTC client connected to a DCC-connected node can only manage other DCC-connected nodes and the firewall itself.

Figure 4-10 Scenario 7: Proxy Server Gateway Settings



78-120

Figure 4-11 shows an ONS 15327 proxy server implementation. A GNE ONS 15327 is connected to a central office LAN and to ENE ONS 15327s. The central office LAN is connected to a NOC LAN, which has CTC computers. The NOC CTC computer and craft technicians must both be able to access the ONS 15327 ENEs. However, the craft technicians must be prevented from accessing or seeing the NOC or central office LANs.

In the example, the ONS 15327 GNE is assigned an IP address within the central office LAN and is physically connected to the LAN through its LAN port. ONS 15327 ENEs are assigned IP addresses that are outside the central office LAN and given private network IP addresses. If the ONS 15327 ENEs are co-located, the craft LAN ports could be connected to a hub. However, the hub should have no other network connections.

Figure 4-11 Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on the same subnet

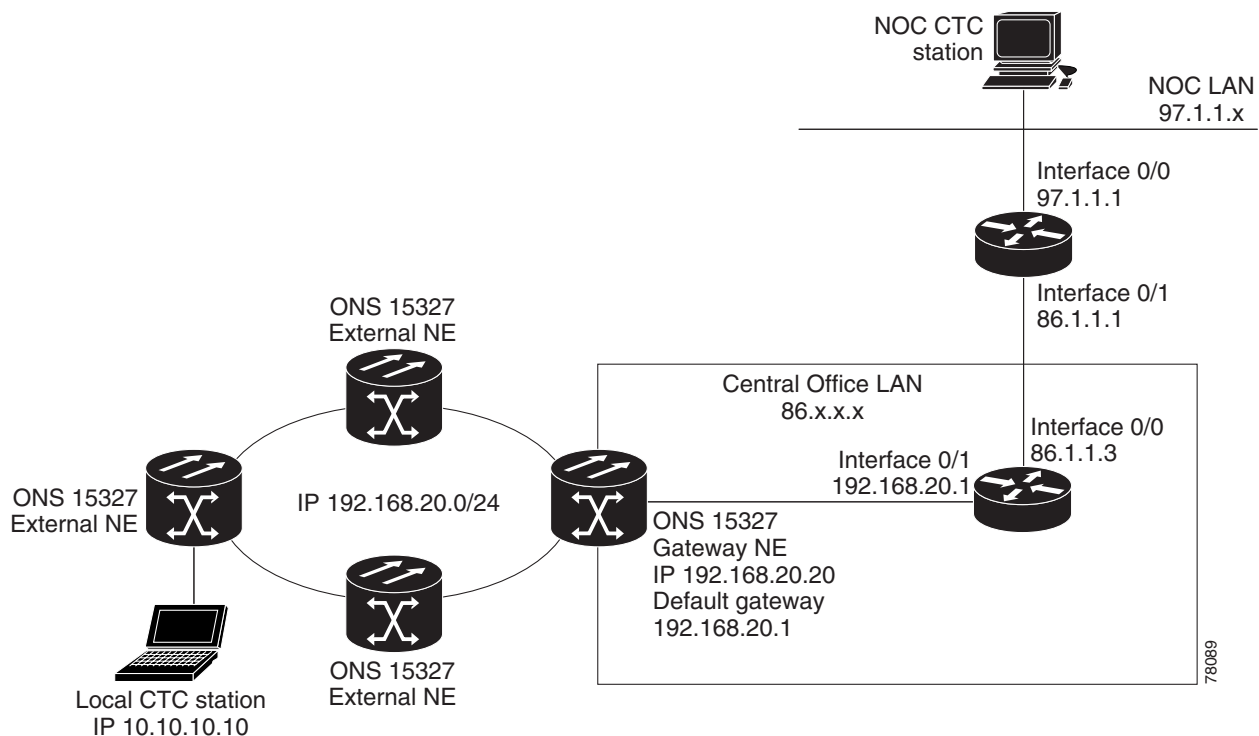


Table 4-2 shows recommended settings for ONS 15327 GNEs and ENEs in the configuration shown in Figure 4-11.

Table 4-2 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 (the ENE SNMPv1 trap destination must use port 391, if the destination is a GNE)

Figure 4-12 shows the same proxy server implementation with ONS 15327 ENEs on different subnets. Figure 4-13 shows the implementation with ONS 15327 ENEs in multiple rings. In each example, ONS 15327 GNEs and ENEs are provisioned with the settings shown in Table 4-2.

Figure 4-12 Scenario 7: ONS 15327 Proxy Server with GNE and ENEs on different subnets

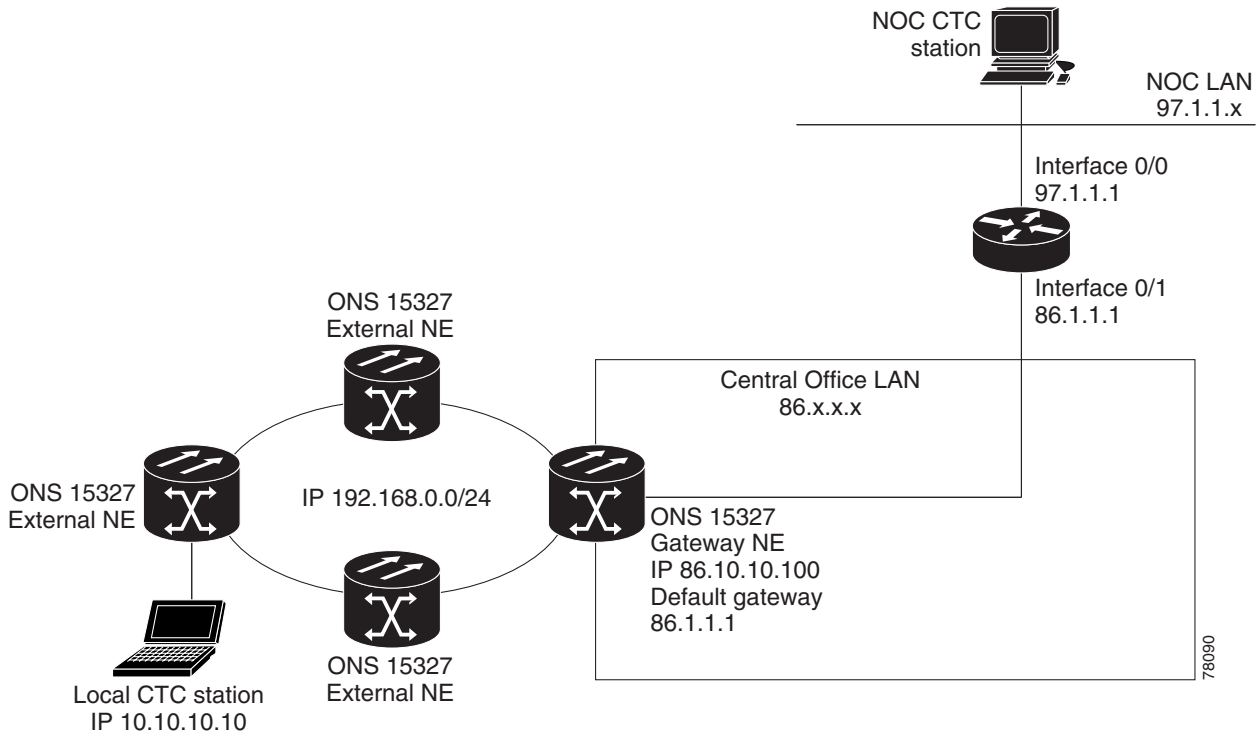


Figure 4-13 Scenario 7: ONS 15327 Proxy Server with ENEs on multiple rings

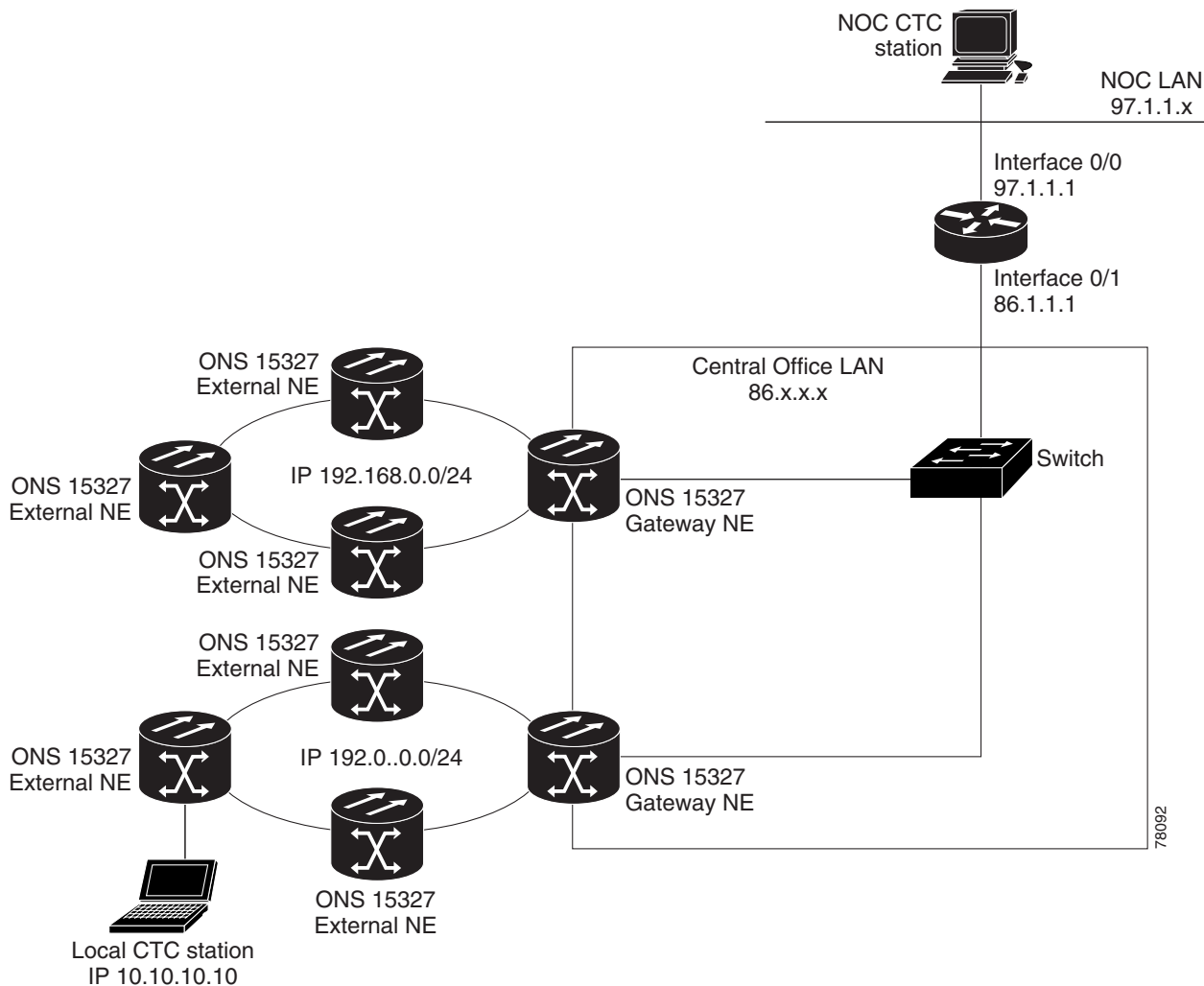


Table 4-3 shows the rules the ONS 15327 follows to filter packets when *Enable Firewall* is enabled. If the packet is addressed to the ONS 15327, additional rules, shown in Table 4-4, are applied. Rejected packets are silently discarded.

Table 4-3 Proxy Server Firewall Filtering Rules

Packets Arrive At	Accepted
XTC Ethernet Interface	<ul style="list-style-type: none"> The ONS 15327 itself The ONS 15327's subnet broadcast address Within the 224.0.0.0/8 network (reserved network used for standard multicast messages) 255.255.255.255
DCC Interface	<ul style="list-style-type: none"> The ONS 15327 itself An OSPF peer (another DCC-connected ONS 15327) Within the 224.0.0.0/8 network

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

Packets Arrive At	Accepted	Rejected
XTC Ethernet Interface	<ul style="list-style-type: none"> All UDP packets except those in the Rejected column All TCP, OSPF and ICMP packets 	<ul style="list-style-type: none"> UDP packets addressed to the SNMP trap relay port (391) are rejected
DCC Interface	<ul style="list-style-type: none"> All UDP packets All TCP packets except those in the Rejected column OSPF packets ICMP packets 	<ul style="list-style-type: none"> TCP packets addressed to the telnet port are rejected. TCP packets addressed to the IO card telnet ports are rejected. TCP packets addressed to the proxy server port are rejected.

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

- 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.
- 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.
- All DCC-connected ONS 15327s in the same SDCC area must have the same *Enable Firewall* setting. Mixed values will produce unpredictable results. Some nodes may become unreachable.
- If you enable *Enable Firewall*, always enable *Enable Proxy*. If *Enable Proxy* is not enabled, CTC will not be able to see nodes on the DCC side of the ONS 15327.
- If *Craft Access Only* is enabled, enable *Enable Proxy*. If *Enable Proxy* is not enabled, 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:

- 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.

4.3 ONS 15327 Routing Table

ONS 15327 routing information is displayed on the Maintenance > Routing Table tabs (Figure 4-14). The routing table provides the following information:

- *Destination*—Displays the IP address of the destination network or host.
- *Mask*—Displays the subnet mask used to reach the destination host or network.
- *Gateway*—Displays the IP address of the gateway used to reach the destination network or host.
- *Usage*—Shows the number of times this route has been used.
- *Interface*—Shows the ONS 15327 interface used to access the destination. Values are:
 - cpm0—the ONS 15327 Ethernet interface, that is, the RJ-45 jack on the XTC.
 - pdcc0—an SDCC interface, that is, an OC-N trunk card identified as the SDCC termination.
 - lo0—a loopback interface

Figure 4-14 Viewing the ONS 15327 routing table

Database	Destination	Mask	Gateway	Usage	Interface
Ether Bridge	0.0.0.0	0.0.0.0	10.92.18.1	6348	cpm0
Protection	10.92.18.0	255.255.255.0	10.92.18.201	0	cpm0
Ring	10.92.18.201	255.255.255.255	127.0.0.1	0	lo0
Software	10.92.18.202	255.255.255.255	0.0.0.0	20907	pdcc0
Software	10.92.18.203	255.255.255.255	0.0.0.0	20907	pdcc1
Diagnostic	192.1.0.0	255.255.255.0	10.92.18.1	0	cpm0

Table 4-5 shows sample routing entries for an ONS 15327.

Table 4-5 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

Table 4-5 Sample Routing Table Entries (continued)

Entry	Destination	Mask	Gateway	Interface
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.



SONET Topologies

This chapter explains how to set up the Cisco ONS 15327 in different SONET topologies, including:

- Two-fiber bidirectional line switched rings (BLSRs)
- Unidirectional path switched rings (UPSRs)
- Subtending rings
- Linear add/drop multiplexers (ADMs)
- Path-protected mesh networks (PPMNs)

5.1 Before You Begin

To avoid errors during network configuration, Cisco recommends that you draw the complete ONS 15327 SONET topology on paper (or electronically) before you begin the physical implementation. A sketch ensures that you have adequate slots, cards, and fibers to complete the topology.

Table 5-1 shows the SONET rings that can be created on each ONS 15327 node.

Table 5-1 ONS 15327 Rings

Ring Type	Maximum per node
All rings	5
2-Fiber BLSR	2
UPSR	5

5.2 Bidirectional Line Switched Rings

The ONS 15327 can support two concurrent BLSRs in one of the following configurations:

- Two, two-fiber BLSRs, or
- One two-fiber BLSR.

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.

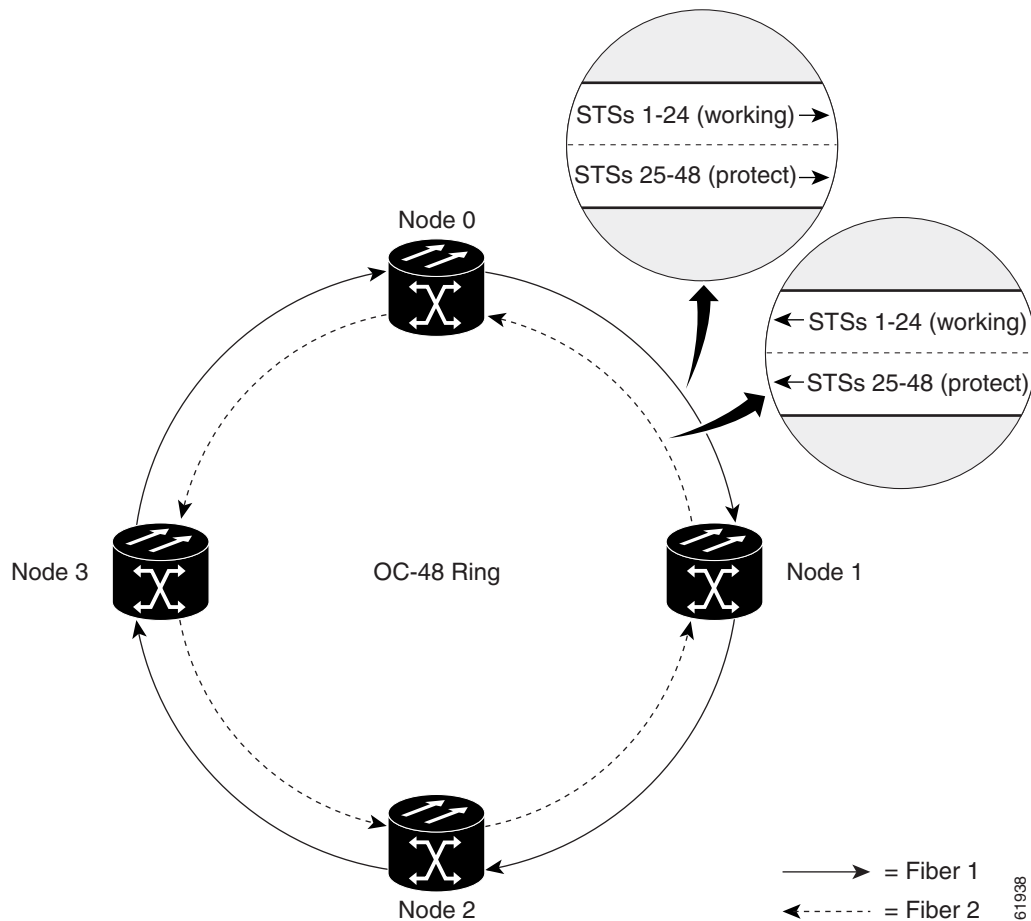
**Note**

Two-fiber BLSRs can support up to 32 ONS 15327s, but switch times are slightly longer for rings containing more than 16 nodes. BLSRs with 16 or fewer nodes will meet the GR-1230 switch time requirement.

5.2.1 Two-Fiber BLSRs

In two-fiber BLSRs, each fiber is divided into working and protect bandwidths. For example, in an OC-48 BLSR (Figure 5-1), STSs 1 – 24 carry the working traffic, and STSs 25 – 48 are reserved for protection. Working traffic (STSs 1 – 24) travels in one direction on one fiber and in the opposite direction on the second fiber. The Cisco Transport Controller (CTC) circuit routing routines calculate the “shortest path” for circuits based on many factors, including requirements set by the circuit provisioner, traffic patterns, and distance. For example, in Figure 5-1, circuits going from Node 0 to Node 1 typically will travel on Fiber 1, unless that fiber is full, in which case circuits will be routed on Fiber 2 through Node 3 and Node 2. Traffic from Node 0 to Node 2 (or Node 1 to Node 3), may be routed on either fiber, depending on circuit provisioning requirements and traffic loads.

Figure 5-1 A four-node, two-fiber BLSR sample traffic pattern



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

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

Figure 5-2 shows a sample traffic pattern on a four-node, two-fiber BLSR.

Figure 5-2 Four-node, two-fiber BLSR sample traffic pattern

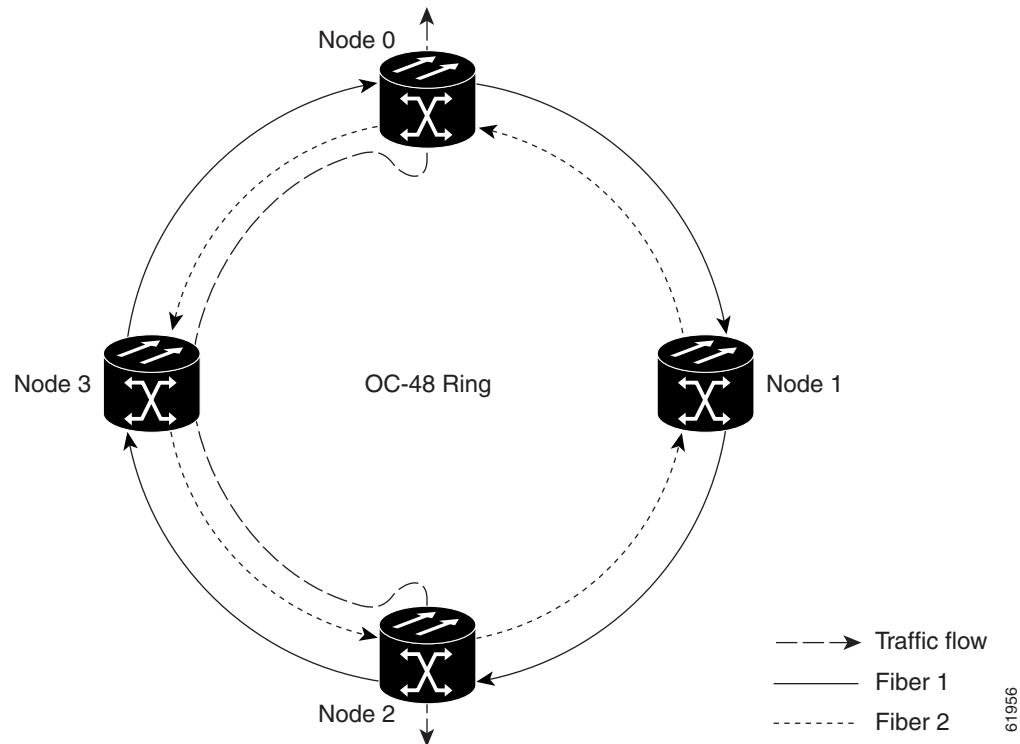
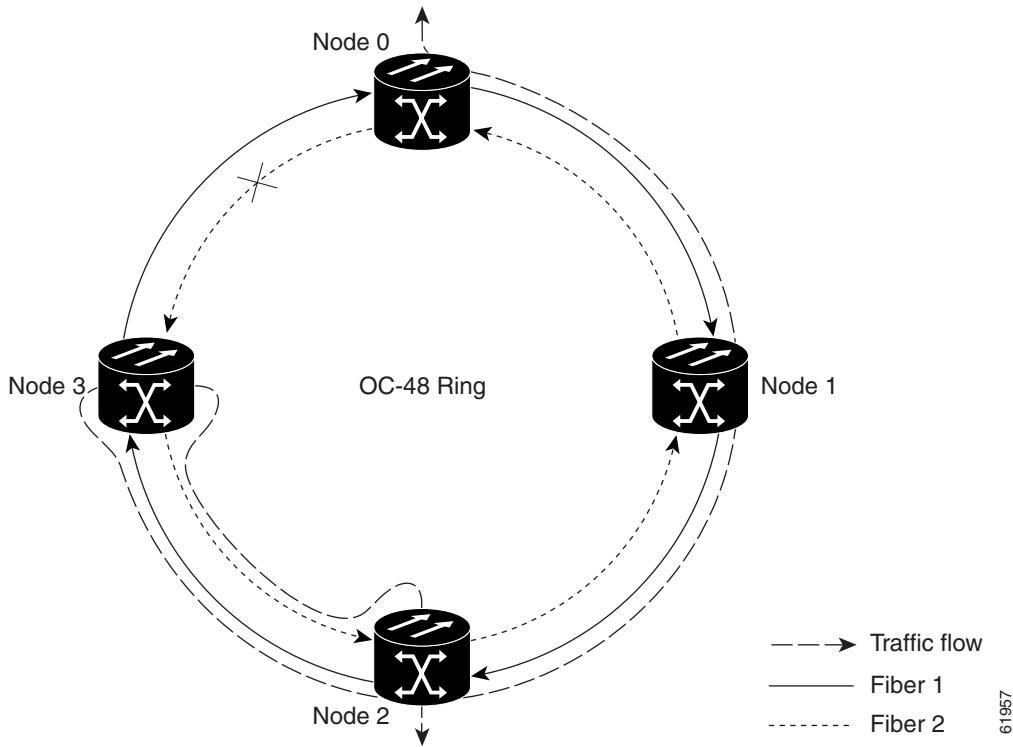


Figure 5-3 shows how traffic is rerouted following a line break between Node 0 and Node 3.

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

Figure 5-3 Four-node, two-fiber BLSR traffic pattern following line break



5.2.2 BLSR Bandwidth

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

BLSRs allow bandwidth to be reused around the ring and can carry more traffic than a network with traffic flowing through one central hub. BLSRs can also carry more traffic than a UPSR operating at the same OC-N rate. Table 5-2 shows the bidirectional bandwidth capacities of two-fiber BLSRs. The capacity is the OC-N rate divided by two, multiplied by the number of nodes in the ring minus the number of pass-through STS-1 circuits.

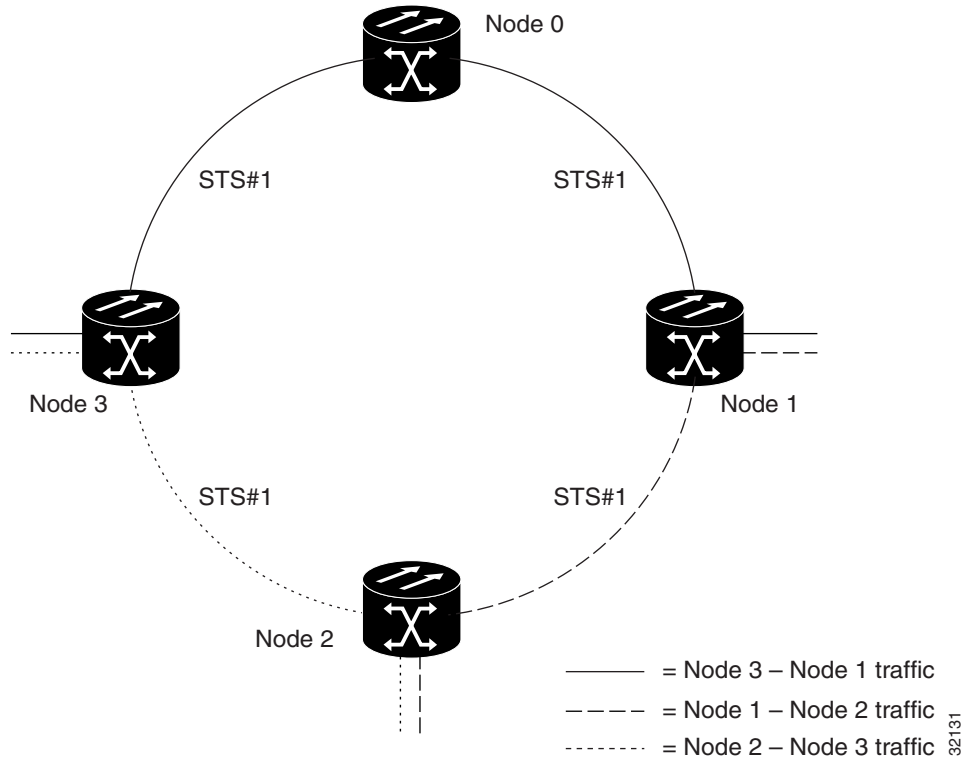
Table 5-2 Two-Fiber BLSR Capacity

OC Rate	Working Bandwidth	Protection Bandwidth	Ring Capacity
OC-12	STS1-6	STS 7-12	$6 \times N^1 - PT^2$
OC-48	STS 1-24	STS 25-48	$24 \times N - PT$

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 5-4 shows an example of BLSR bandwidth reuse. The same STS carries three different traffic sets simultaneously on different spans on the ring: one set from Node 3 to Node 1, one from Node 1 to Node 2, and another from Node 2 to Node 3.

Figure 5-4 BLSR bandwidth reuse



5.2.3 Sample BLSR Application

Figure 5-5 shows a sample two-fiber BLSR implementation. A regional long-distance network connects to other carriers at Node 0. Traffic is delivered to the service provider's major hubs.

- Carrier 1 delivers two DS-3s over one OC-3 span 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 5-5 A five-node BLSR

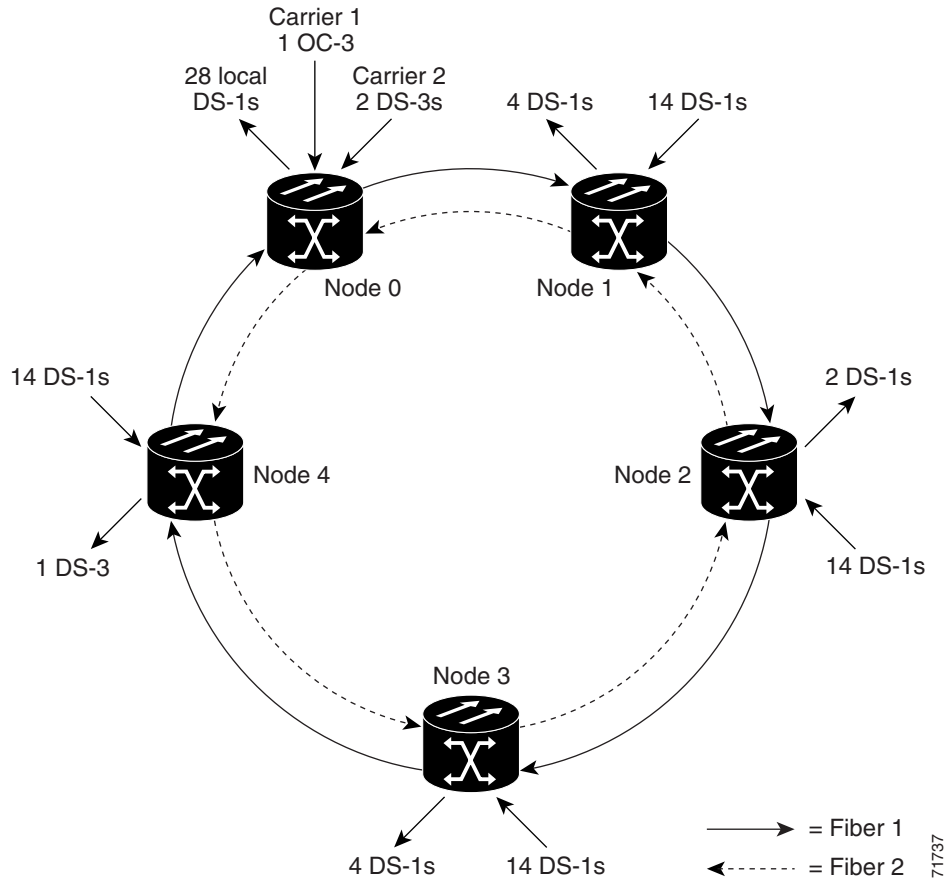


Figure 5-6 shows the shelf assembly layout for Node 0, which has no free slots. Figure 5-7 shows the shelf assembly layout for the remaining sites in the ring. In this BLSR configuration, an additional three DS-3s at Node IDs 1, 2, 3 and 4 can be activated. Each remote site has a free slot for future traffic needs.

Figure 5-6 Shelf assembly layout for Node 0 in Figure 5-5

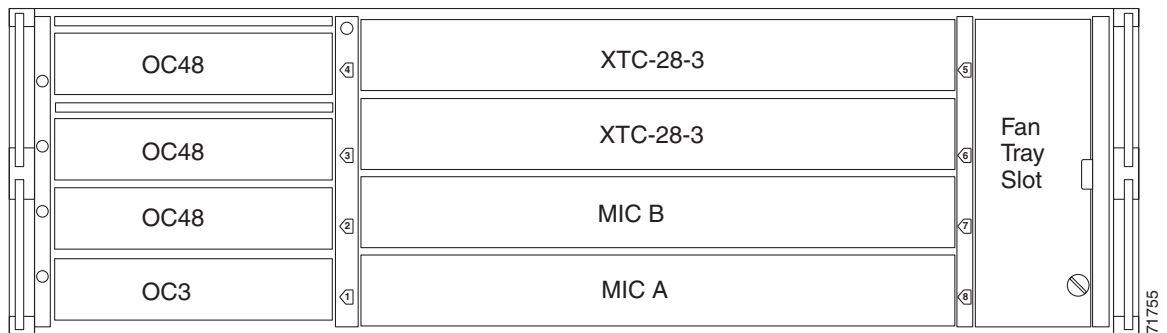
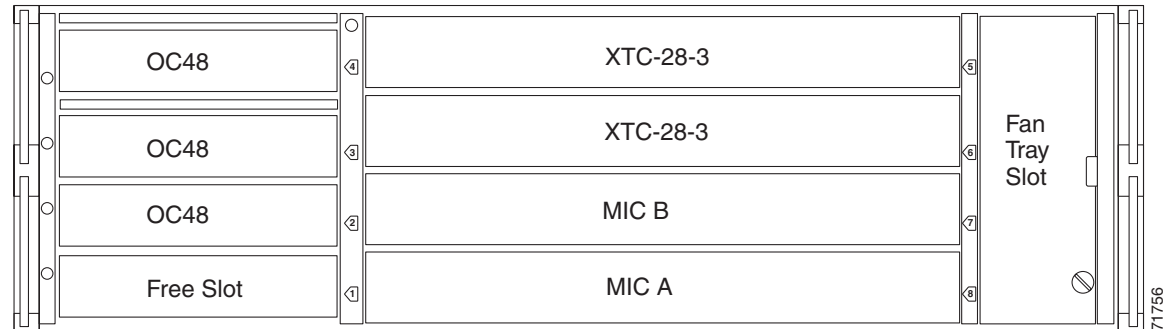


Figure 5-7 Shelf assembly layout for Nodes 1 – 4 in Figure 5-5



5.2.4 Setting Up BLSRs

To set up a BLSR on the ONS 15327, you perform five basic procedures:

- Install the BLSR trunk cards. See the “Install the BLSR Trunk Cards” procedure on page 5-7.
- Create the BLSR DCC terminations. See the “Create the BLSR DCC Terminations” procedure on page 5-8.
- Enable the BLSR ports. See the “Enable the BLSR Ports” procedure on page 5-8.
- Set up BLSR timing. See the “Setting Up ONS 15327 Timing” section on page 3-11.
- Provision the BLSR. See the “Provision the BLSR” procedure on page 5-9.

Procedure: Install the BLSR Trunk Cards

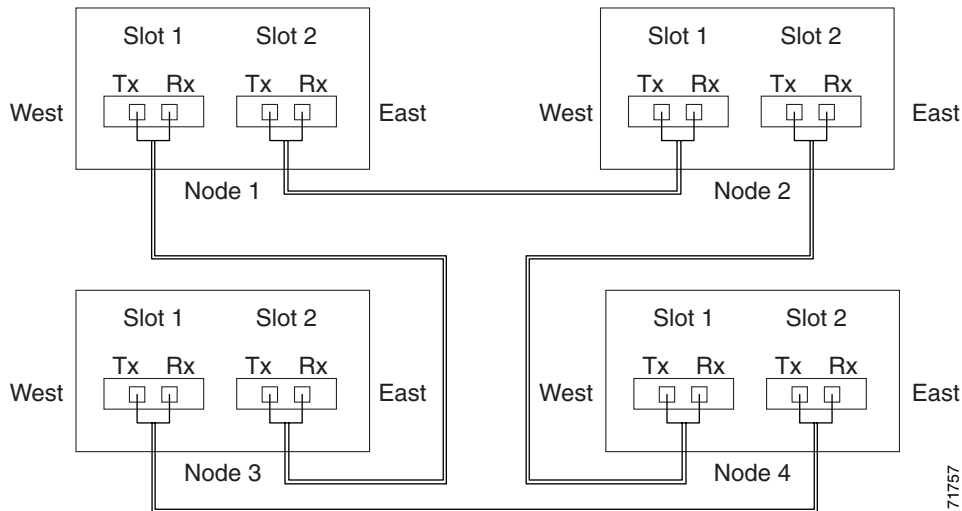
- Step 1** Install the OC-12 or OC-48 cards that will serve as the BLSR trunk cards. You can install the OC-12 and OC-48 cards in any high-speed slot (Slots 1–4).
- Step 2** Allow the cards to boot.
- Step 3** Attach the fiber to the east and west BLSR ports at each node.

Plan your fiber connections and use the same plan for all BLSR nodes. For example, make the east port Slot 2 and the west port Slot 1 at every node. Plug fiber connected to an east port at one node into the west port on an adjacent node. Figure 5-8 shows fiber connections for a two-fiber BLSR with trunk cards in Slot 1 (west) and Slot 2 (east).



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

Figure 5-8 Connecting fiber to a four-node, two-fiber BLSR



Procedure: Create the BLSR DCC Terminations

-
- Step 1** Log into the first node that will be in the BLSR.
 - Step 2** Click the **Provisioning > Sonet DCC** tabs.
 - Step 3** In the SDCC Terminations section, click **Create**.
 - Step 4** On the Create SDCC Terminations dialog box, press **Ctrl** and click the two slots/ports that will serve as the BLSR ports at the node. For example, Slot 1 (OC-48)/Port 1 and Slot 2 (OC-48)/Port 1.
 - Step 5** If you want the ports to be put in service (enabled) automatically, leave the Set Port in Service checkbox checked. Otherwise, uncheck the box and follow the steps to enable the ports.
 - Step 6** Click **OK**.
 - Step 7** The slots/ports appear in the SDCC Terminations list.
 - Step 8** Complete Steps 2 – 5 at each node that will be in the BLSR.



Note

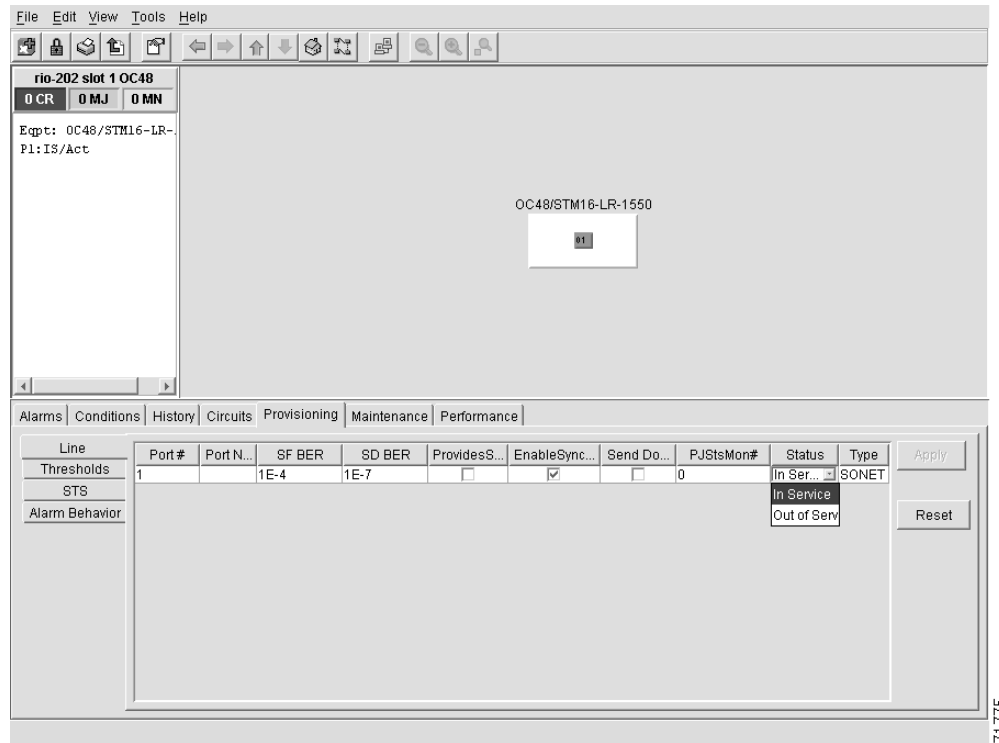
The ONS 15327 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs; therefore, the Line DCCs are available to tunnel DCCs from third-party equipment across ONS 15327 networks. For more detail, see the “Creating DCC Tunnels” section on page 6-20.

Procedure: Enable the BLSR Ports

-
- Step 1** Log into one of the nodes that will be in the BLSR.
 - Step 2** Double-click one of the OC-N cards that you configured as a DCC termination.

- Step 3** Click the **Provisioning > Line** tabs.
- Step 4** Click **Status** (Figure 5-9) and choose **In Service**.
- Step 5** Click **Apply**.

Figure 5-9 Enabling an optical port



- Step 6** Repeat Steps 2 – 4 for the other optical card configured as a DCC termination.
- Step 7** Repeat Steps 2 – 5 at each node that will be in the BLSR.

After configuring the SONET DCC, set the timing for the node. For procedures, see the “Setting Up ONS 15327 Timing” section on page 3-11. After you configure the timing you can provision the BLSR.

Procedure: Provision the BLSR

- Step 1** Log into one BLSR node.
- Step 2** Select the **Provisioning > Ring** tabs.
- Step 3** Click **Create**.
- Step 4** On the Create BLSR dialog box (Figure 5-10), set the BLSR properties:
- *Ring ID*—Assign a ring ID (a number between 0 and 9999). Nodes in the same BLSR must have the same Ring ID.
 - *Node ID*—Assign a Node ID. The Node ID identifies the node to the BLSR. Nodes in the same BLSR must have unique Node IDs (0–31).

- *Ring Reversion*—Set the amount of time that will pass before the traffic reverts to the original working path. The default is 5 minutes. All nodes in a BLSR ring should have the same ring reversion setting, particularly if “never” (i.e., non-revertive) is selected.
- *West Line*—Assign the west BLSR port for the node from the pull-down menu. (In Figure 5-8, this is Slot 1.)
- *East Line*—Assign the east BLSR port for the node from the pull-down menu. (In Figure 5-8, this is Slot 2.)

The east and west ports must match the fiber connections and DCC terminations set up in the “Install the BLSR Trunk Cards” procedure on page 5-7 and the “Create the BLSR DCC Terminations” procedure on page 5-8.

Figure 5-10 Setting BLSR properties

Step 5 Click **OK**.



Note Some or all of the following alarms display during BLSR setup: E-W MISMATCH, RING MISMATCH, APSCIMP, APSDFLTK, BLSROSYNC. The alarms will clear after you configure all the nodes in the BLSR.

Step 6 Complete Steps 2 – 5 at each node that you are adding to the BLSR.

Step 7 After you configure the last BLSR node, wait for the BLSR Ring Map Change dialog box to display (this can take 10 – 30 seconds).



Note The dialog box will not display if SDCC Termination alarms (e.g., EOC) or BLSR alarms (such as E-W MISMATCH and RING MISMATCH) are present. If an SDCC alarm is present, review the DCC provisioning at each node; use the “Create the BLSR DCC Terminations” procedure on page 5-8. If BLSR alarms have not cleared, repeat Steps 1 – 6 at each node, making sure each node is provisioned correctly. You can also follow alarm troubleshooting procedures provided in Chapter 14, “Alarm Troubleshooting”.

Step 8 On the BLSR Ring Map Change dialog, click **Yes**.

Step 9 On the BLSR Ring Map dialog box, verify that the ring map contains all the nodes you provisioned in the expected order. If so, click **Accept**. If the nodes do not appear, or are not in the expected order, repeat Steps 1 – 8, making sure no errors are made.

Step 10 Switch to network view and verify the following:

- A green span line appears between all BLSR nodes

- All E-W MISMATCH, RING MISMATCH, APSCIMP, DFLTK, and BLSROSYNC alarms are cleared.

Step 11 Test the BLSR using testing procedures normal for your site. Here are a few steps you can use:

- a. Run test traffic through the ring.
 - b. Log into a node, click the **Maintenance > Ring** tabs, and choose **MANUAL RING** from the East Switch list. Click **Apply**.
 - c. In network view, click the **Conditions** tab and click **Retrieve**. You should see a Ring Switch West event, and the far-end node that responded to this request will report a Ring Switch East event.
 - d. Verify that traffic switches normally.
 - e. Choose **Clear** from the East Switch list and click **Apply**.
 - f. Repeat Steps a – d for the West Switch.
 - g. Disconnect the fibers at one node and verify that traffic switches normally.
-

5.2.5 Adding and Removing BLSR Nodes

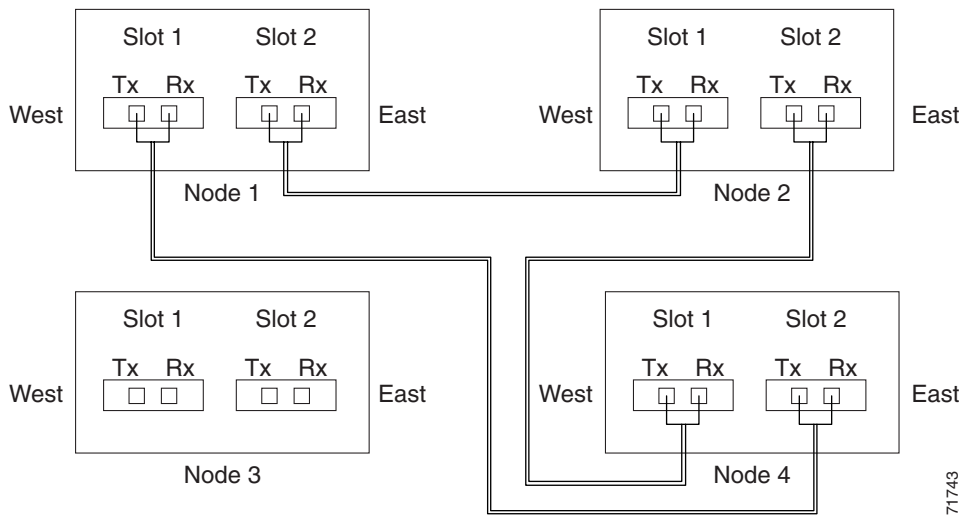
This section explains how to add and remove BLSR nodes. To add or remove a node, you force a protection switch to route traffic away from the span where you will add or remove the node. Figure 5-11 shows a three-node BLSR before the new node is added. To add Node 3, you would:

- Force a protection switch on the Node 1 (Slot 1, West) and Node 4 (Slot 2, East) span. The protection switch forces traffic away from the fibers that you will remove and reconnect to the added node.
- Provision the node for the BLSR (SDCC, timing, enable the ports)
- Remove fibers from Node 1/Slot 1 and Node 4/Slot 2, then, using additional fibers, connect Node 1 and Node 4 to Node 3.
- Remove the protection switch to route traffic through the added node.

**Note**

You can only add one node at a time to an ONS 15327 BLSR.

Figure 5-11 A three-node BLSR before adding a new node



71743

Procedure: Add a BLSR Node

Perform these steps on-site and not from a remote location.

- Step 1** Draw a diagram, similar to Figure 5-11, for the BLSR installation where you will add the node. In the diagram, identify the nodes, cards (slots) and spans (east or west) that will connect to the new node. This information is essential to complete this procedure without error. For example, in Figure 5-11, you would circle Slot 1 (west) on Node 1, and Slot 2 (east) on Node 4.
- Step 2** Log into CTC and display the BLSR nodes in network view. Verify the following:
- All BLSR spans on the network map are green.
 - On the **Alarms** tab, no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. In a BLSR, these facility conditions may be reported as minor alarms.
 - On the **Conditions** tab, no ring switches are active.
- If trouble is indicated, for example, a major alarm exists, resolve the problem before proceeding.
- Step 3** Install the OC-N cards in the ONS 15327 that you will add to the BLSR; use the “Install the BLSR Trunk Cards” procedure on page 5-7. Ensure fiber cables are available to connect to the cards. Run test traffic through the node to ensure the cards are functioning properly.
- Step 4** Log into the new node and complete the BLSR setup.
- Provision the SONET DCC using the “Create the BLSR DCC Terminations” procedure on page 5-8.
 - Configure the BLSR timing using the “Set Up ONS 15327 Timing” procedure on page 3-13.
 - Enable the BLSR ports using the “Enable the BLSR Ports” procedure on page 5-8.
 - If the BLSR will connect to third party equipment that cannot transport the K3 byte, the third party equipment must connect to a Cisco ONS 15454 node. (The BLSR must be a mixed ring of ONS 15327s and ONS 15454s to remap the K3 byte. If connecting rings to third party equipment, refer the *Cisco ONS 15454 Procedure Guide*.)
 - Provision the BLSR using the “Provision the BLSR” procedure on page 5-9

Step 5 Log into the node that will connect to the new node through its east port (Node 4 in the Figure 5-11 example).

Step 6 Switch protection on the east port:

- a. Click the **Maintenance > Ring** tabs.
- b. From the East Switch list, choose **FORCE RING**. Click **Apply**.

Performing a FORCE switch generates a force switch request on an equipment (FORCE-REQ) alarm. This is normal.



Caution Traffic is unprotected during a protection switch.

Step 7 Log into the node that will connect to the new node through its west port (Node 1 in the Figure 5-11 example).

Step 8 Switch protection on the west port:

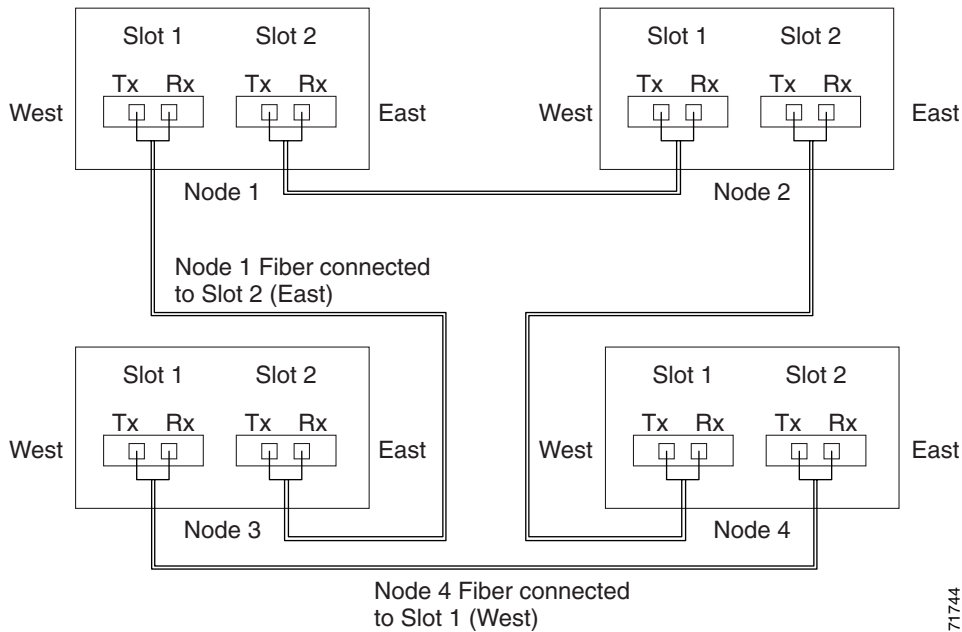
- a. Click the **Maintenance > Ring** tabs.
- b. From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 9 Following the diagram that you created in Step 1, remove the fiber connections from the two nodes that will connect directly to the new node.

- a. Remove the east fiber from the node that will connect to the west port of the new node. In the Figure 5-11 example, this is Node 4/Slot 2.
- b. Remove the west fiber from the node that will connect to the east port of the new node. In the Figure 5-11 example, this is Node 1/Slot 1.

Step 10 Replace the removed fibers with fibers that are connected to the new node. Connect the west port to the east port and the east port to the west port. Figure 5-12 shows the BLSR in the Figure 5-11 example after the node is connected.

Figure 5-12 A BLSR with a newly-added fourth node



- Step 11** Log out of CTC and then log back into any node in the BLSR.
- Step 12** In node view, select the **Provisioning > Ring** tabs and click **Ring Map**.
- Step 13** On the BLSR Map Ring Change dialog box, click **Yes**.
- Step 14** On the BLSR Ring Map dialog box, verify that the new node is added. If it is, click **Accept**. If it does not appear, log into the new node. Verify that the BLSR is provisioned correctly according to the “Provision the BLSR” procedure on page 5-9, then repeat Steps 12 – 13. If the node still does not appear, repeat the steps in the procedure making sure that no errors were made.
- Step 15** From the Go To menu, select **Network View**. Click the **Circuits** tab. Wait until all the circuits are discovered. The circuits that pass through the new node will be shown as incomplete.
- Step 16** In network view, right-click the new node and select **Update Circuits With The New Node** from the shortcut menu. Verify that the number of updated circuits displayed in the dialog box is correct.
- Step 17** Select the **Circuits** tab and verify that no incomplete circuits are present.
- Step 18** Clear the protection switch for the node that is using its east port to connect to the new node, and for the node that is using its west port to connect to the new node:
- To clear the protection switch from the east port, display the **Maintenance > Ring** tabs. From the East Switch list choose **CLEAR**. Click **Apply**.
 - To clear the protection switch from the west port, choose **CLEAR** from the West Switch list. Click **Apply**.

Procedure: Remove a BLSR Node

**Caution**

The following procedure minimizes traffic outages during node deletions. You may need to delete and create circuits that pass through the node to be deleted if the circuit enters and exits the node on different STSs. This occurrence is rare, and only applies to circuits created with R2.x software. Traffic will be lost when you delete and recreate circuits that passed through the deleted node.

-
- Step 1** Before you start this procedure, make sure you know the following:
- Which node is connected through its east port to the node that will be deleted. For example if you are deleting Node 1 in Figure 5-12, Node 3 is the node connected through its east port to Node 1.
 - Which node is connected through its west port to the node that will be deleted. In Figure 5-12, Node 2 is connected to Node 1 through its west port.
- Step 2** Log into a node on the same BLSR as the node you will remove. (Do not log into the node that you will remove.)
- Step 3** Display the BLSR nodes in network view and verify the following:
- All BLSR spans on the network map are green.
 - No critical or major alarms (LOF, LOS, ASP, ASL) are displayed on the **Alarms** tab.
 - On the **Conditions** tab, no ring switches are active.
- If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding.
- Step 4** Display the node that you will remove in node view.
- Step 5** Delete all the circuits that originate or terminate in that node. (If a circuit has multiple drops, delete only the drops that terminate on the node you want to delete.)
- a. Click the **Circuits** tab. The circuits that use this node are displayed.
 - b. Select circuits that originate or terminate on the node. Click **Delete**.
 - c. Click **Yes** when prompted.
 - d. If a multidrop circuit has drops at the node that will be removed, select the circuit, click **Edit**, and remove the drops.
- Step 6** Complete this step if circuits that were created using Cisco Transport Controller Release 2.x pass through the node that will be deleted:
- a. On the Circuits tab of the node that will be deleted, select a circuit and click **Edit**.
 - b. On the Edit Circuits window, check **Show Detailed Map**.
 - c. Verify that the circuits enter and exit the node on the same STS. For example, if a circuit enters on s1/p1/S1 (Slot 1, Port 1, STS1), verify that it exits on STS1. If a circuit enters/exits on different STSs, write down the name of the circuit. You will delete and recreate these circuits in Step e.
 - d. From the View menu, select **Go to Network View** and then select the **Circuits** tab.
 - e. Delete, then recreate each circuit recorded in Step c that entered/exited the node to be deleted on different STSs. To delete the circuit, select the circuit on the Circuits window, then click the **Delete** button. To create the circuit, go to the “Create an Automatically Routed Circuit” procedure on page 6-2.
 - f. Repeat Steps a – e for each circuit displayed on the Circuits tab.

g. Repeat Steps a – c for each circuit displayed on the Circuits tab.

Step 7 Use information recorded in Step 1 to switch traffic away from the ports of neighboring nodes that will be disconnected when the node is removed:



Caution Traffic is unprotected during the protection switch.

a. Open the neighboring node that is connected through its east port to the removed node.

b. Click the **Maintenance > Ring** tabs.

c. From the East Switch list, choose **FORCE RING**. Click **Apply**.

d. Open the node that is connected through its west port to the removed node.

e. Click the **Maintenance > Ring** tabs.

f. From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 8 Remove all fiber connections between the node being removed and the two neighboring nodes.

Step 9 Reconnect the two neighboring nodes directly, west port to east port.

Step 10 Close CTC, then log into a node on the reduced ring.

Step 11 Wait for the BLSR Map Ring Change dialog box to display. (If the dialog box does not display after 10 – 15 seconds, select the **Provisioning > Ring** tabs and click **Ring Map**.) When the dialog box displays, click **Yes**.

Step 12 On the BLSR Ring Map dialog box, click **Accept**.

Step 13 Clear the protection switches on the neighboring nodes:

a. Open the node with the protection switch on its east port.

b. Click the **Maintenance > Ring** tabs and choose **CLEAR** from the East Switch list. Click **Apply**.

c. Open the node with the protection switch on its west port.

d. Click the **Maintenance > Ring** tabs and choose **CLEAR** from the West Switch list. Click **Apply**.

Step 14 If a BITS clock is not used at each node, check that the synchronization is set to one of the eastbound or westbound BLSR spans on the adjacent nodes. If the removed node was the BITS timing source, use a new node as the BITS source or select internal synchronization at one node where all other nodes will derive their timing. (For information about ONS 15327 timing, see the “Setting Up ONS 15327 Timing” section on page 3-11.)

5.2.6 Moving BLSR Trunk Cards



Caution

Call the Technical Assistance Center (1-877-323-7368) before performing this procedure to ensure that circuit and provisioning data is preserved.



Caution

To change BLSR trunk cards, you will drop one node at a time from the current BLSR. This procedure is service-affecting during the time needed to complete the steps below. This applies to all BLSR nodes where cards will change slots. Review all the steps before you proceed.

Figure 5-13 shows a four node OC-48 BLSR using trunk cards in Slots 1 and 2 at all four nodes. Trunk cards will be moved at Node 4 from slot 1 and 2 to Slots 3 and 4. To do this Node 4 is temporarily removed from the active BLSR while the trunk cards are switched.

Figure 5-13 A four-node BLSR before a trunk card switch

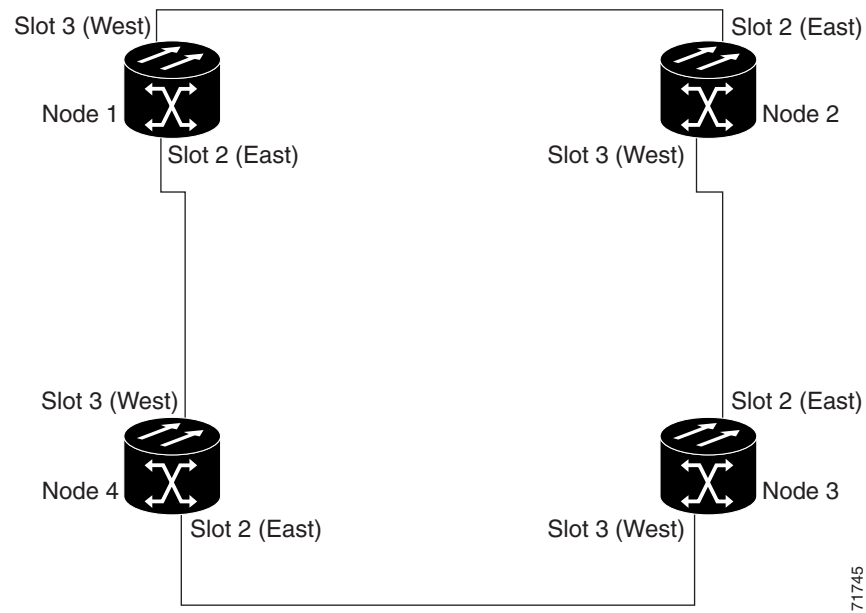
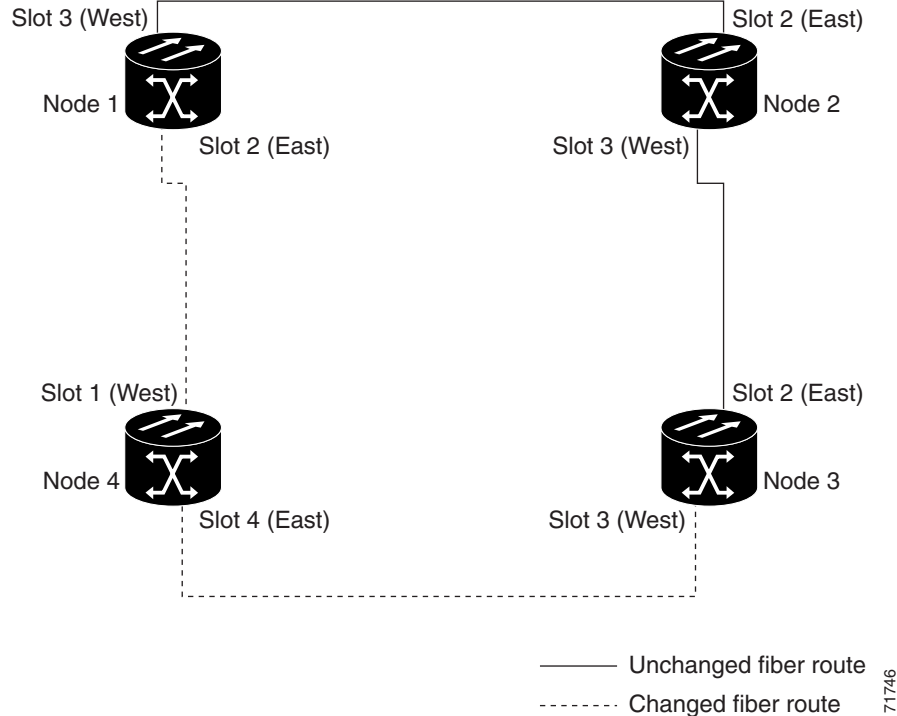


Figure 5-14 shows the BLSR after the cards are switched.

Figure 5-14 A four-node BLSR after the trunk cards are switched at one node



Procedure: Move a BLSR Trunk Card

Use the following steps to move one BLSR trunk card to a different slot. Use this procedure for each card you want to move. Although the procedure is for OC-48 BLSR trunk cards, you can use the same procedure for OC-12 cards.



Note

The ONS 15327 nodes must have CTC Release 3.3 or later and cannot have active alarms for the OC-48 or OC-12 cards or the BLSR configuration.

Step 1 Log into CTC and display the BLSR nodes in network view. Verify the following:

- All BLSR spans on the network map are green.
- On the **Alarms** tab, no critical or major alarms are present, nor any facility alarms, such as LOS, LOF, AIS-L, SF, and SD. In a BLSR, these facility conditions may be reported as minor alarms.
- On the **Conditions** tab, no ring switches are active.

If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding. See Chapter 14, “Alarm Troubleshooting,” for alarm troubleshooting procedures.

Step 2 Switch traffic away from the node where the trunk card will be switched:

- a. Log into the node that is connected through its east port to the node where the trunk card will be moved. (In the Figure 5-13 example, this is Node 1.) Click the **Maintenance > Ring** tabs.
- b. From the East Switch list, choose **FORCE RING**. Click **Apply**.

When you perform a manual switch, a manual switch request equipment alarm (MANUAL-REQ) is generated. This is normal.



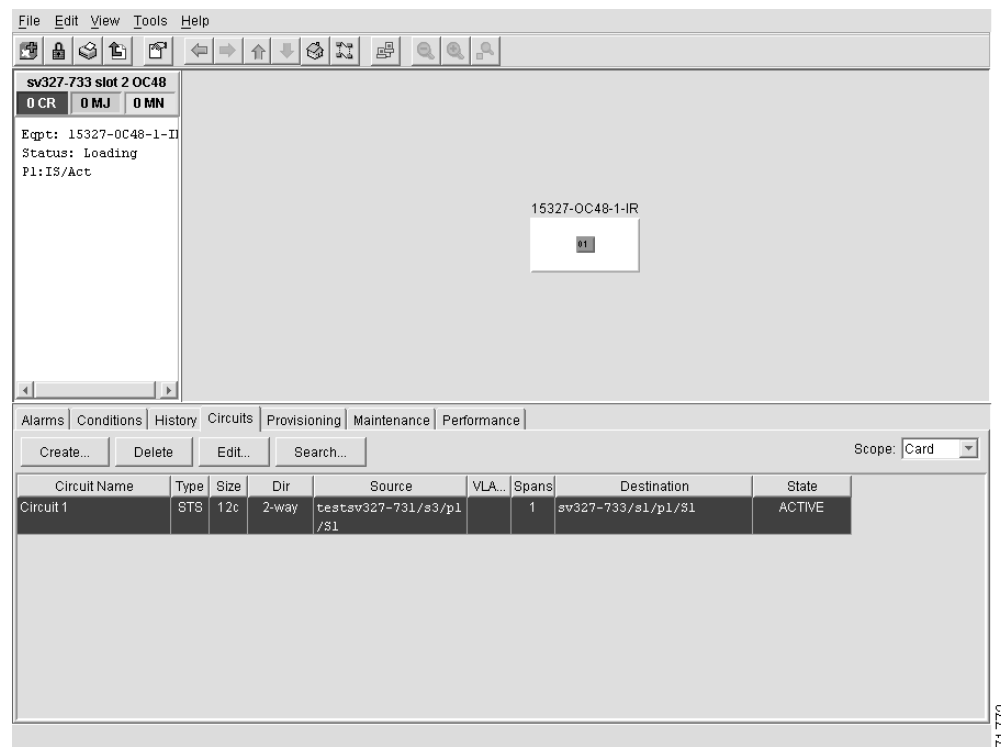
Caution Traffic is unprotected during a protection switch.

- c. Log into the node that is connected through its west port to the node where the trunk card will be moved. (In the Figure 5-13 example, this is Node 3.) Click the **Maintenance > Ring** tabs.
- d. From the West Switch list, choose **FORCE RING**. Click **Apply**.

Step 3 Log into the node where the trunk card you will move is installed.

Step 4 Click the **Circuits** tab (Figure 5-15). Write down the circuit information or, from the File menu, select **Print** or **Export** to print or export the information; you will need it to restore the circuits later. See the “Printing and Exporting CTC Data” section on page 2-41 for more information.

Figure 5-15 Deleting circuits from a BLSR trunk card



Step 5 Delete the circuits on the card you are removing:

- a. Highlight the circuit(s). To select multiple circuits, press the Shift or Ctrl key.
- b. Click **Delete**.
- c. On the Delete Circuit dialog box, click **Yes**.

Step 6 Delete the SONET DCC termination on the card you are removing:

- a. Click the **Provisioning > Sonet DCC** tabs.
- b. From the SDCC Terminations list, click the SONET DCC you need to delete and click **Delete**.

- Step 7** Disable the ring on the current node:
- Click the **Provisioning > Ring** tabs.
 - Highlight the ring and click **Delete**.
 - On the confirmation message, confirm that this is the ring you want to delete. If so, click **Yes**.
- Step 8** If an OC-N card is a timing source, select the **Provisioning > Timing** tabs and set timing to Internal.
- Step 9** Place the ports on the card out of service:
- Double-click the card.
 - On the **Provisioning > Line** tabs in the Status section, choose **Out of Service** for each port.
- Step 10** Physically remove the card.
- Step 11** Insert the card into its new slot and wait for the card to boot.
- Step 12** To delete the card from its former slot, right-click the card in node view and select **Delete** from the list of options.
- Step 13** Place the port(s) back in service:
- To open the card, double-click or right-click the card and select **Open**.
 - Click the **Provisioning** tab.
 - From Status choose **In Service**.
 - Click **Apply**.
- Step 14** Follow the steps described in the “Setting Up BLSRs” section on page 5-7 to reenable the ring using the same cards (in their new slots) and ports for east and west. Use the same BLSR Ring ID and Node ID that was used before the trunk card was moved.
- Step 15** Recreate the circuits that were deleted. See the “Create an Automatically Routed Circuit” procedure on page 6-2 for instructions.
- Step 16** If you use line timing and the card you are moving is a timing reference, reenable the timing parameters on the card. See the “Set Up ONS 15327 Timing” procedure on page 3-13 for instructions.
-

5.3 Unidirectional Path Switched Rings

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

CTC automates ring configuration. UPSR traffic is defined within the ONS 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.

Figure 5-16 shows a basic UPSR configuration. If Node ID 0 sends a signal to Node ID 2, the working signal travels on the working traffic path through Node ID 1. The same signal is also sent on the protect traffic path through Node ID 3. If a fiber break occurs (Figure 5-17), Node ID 2 switches its active receiver to the protect signal coming through Node ID 3.

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

Figure 5-16 A basic four-node UPSR

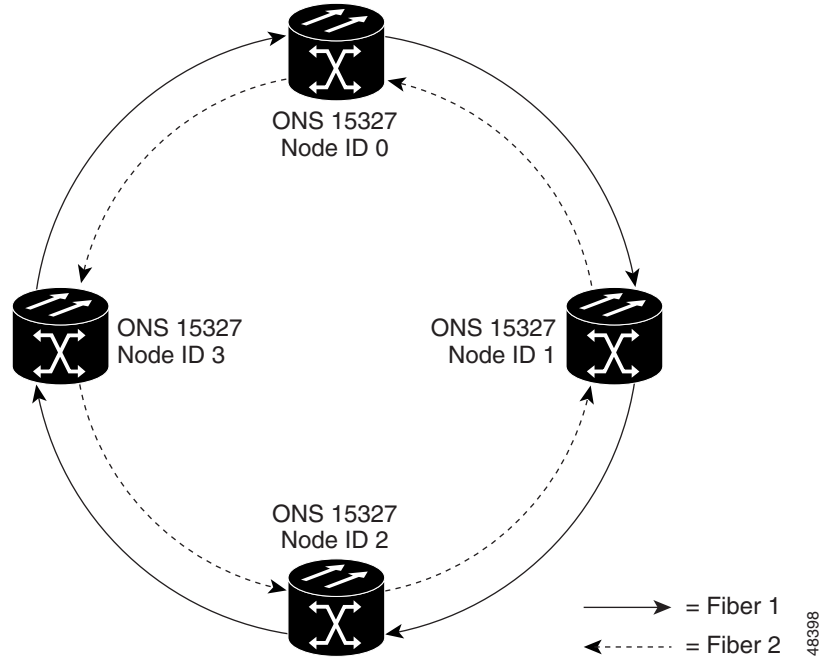
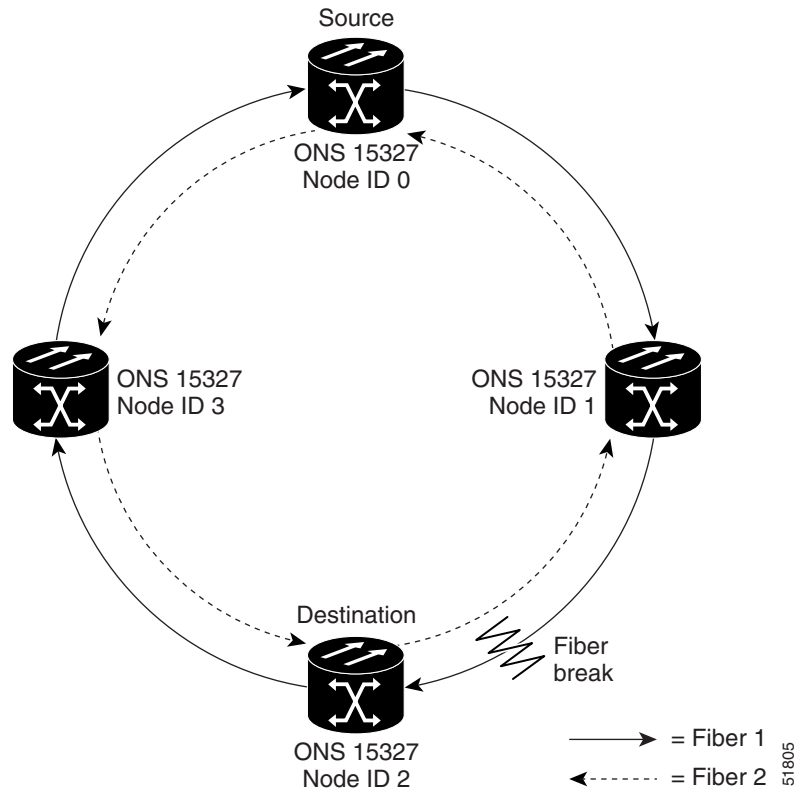


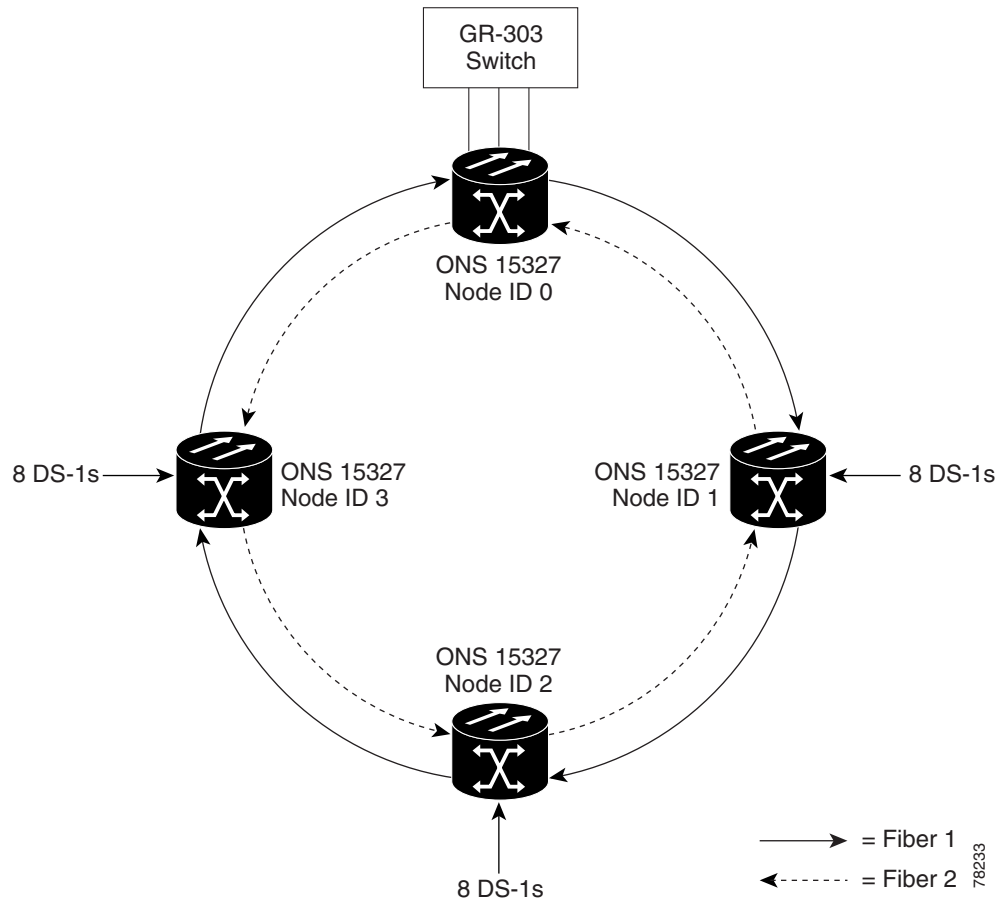
Figure 5-17 A UPSR with a fiber break



5.3.1 Example UPSR Application

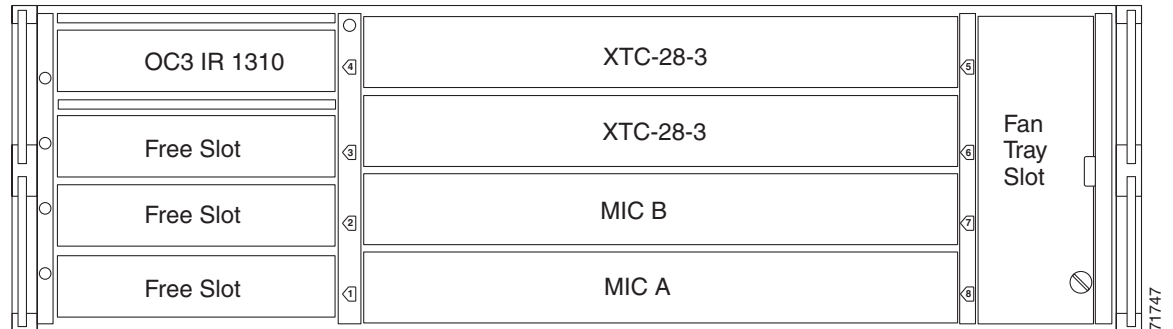
Figure 5-18 shows a common UPSR application. OC-3 optics provide remote switch connectivity to a host GR-303 switch. In the example, each remote switch requires eight DS-1s to return to the host switch. Figure 5-19 and Figure 5-20 show the shelf layout for each site.

Figure 5-18 An OC-3 UPSR

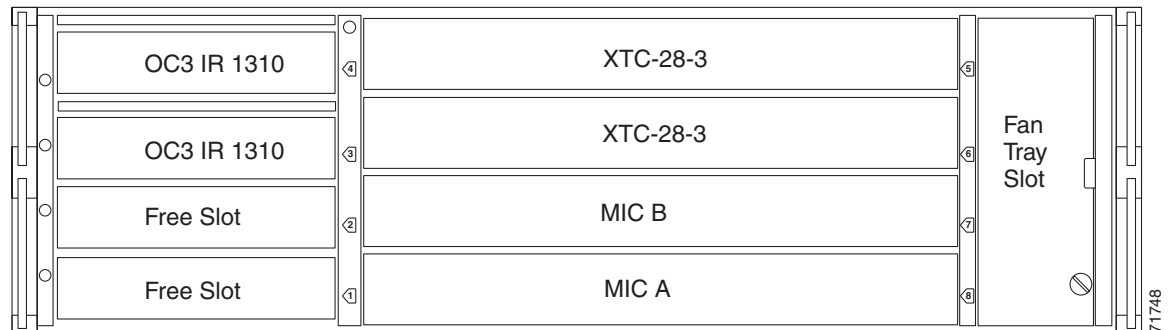


Node ID 0 has two XTC-28-3 cards to provide 28 active DS-1 ports. The other sites only require XTC-14 cards to handle the eight DS-1s to and from the remote switch. You can use the other half of each ONS 15327 shelf assembly to provide support for a second or third ring to other existing or planned remote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

In this sample OC-3 UPSR, Node ID 0 contains four DS1-14 cards and two OC3 IR 4 1310 cards. Six free slots also exist in this setup and can be provisioned with cards or left empty. Figure 5-19 shows the shelf setup for these cards.

Figure 5-19 Layout of Node ID 0 in the OC-3 UPSR example (Figure 5-15)

In the Figure 5-18 on page 5-22 example, Nodes IDs 1 - 3 each contain two DS1-14 cards and two OC3 4 IR 1310 cards. Eight free slots exist. They can be provisioned with other cards or left empty. Figure 5-20 shows the shelf assembly setup for this configuration sample.

Figure 5-20 Layout of Node IDs 1 – 3 in the OC-3 UPSR example (Figure 5-15)

5.3.2 Setting Up a UPSR

To set up a UPSR, you perform four basic procedures:

- Install the UPSR trunk cards. Use the “Install the UPSR Trunk Cards” procedure on page 5-24.
- Create the DCC terminations. Use the “Configure the UPSR DCC Terminations” procedure on page 5-24.
- Configure the timing. Use the “Set Up ONS 15327 Timing” procedure on page 3-13.
- Enable the ports. Use the “Enable the UPSR Ports” procedure on page 5-25.

After you enable the ports, you set up the UPSR circuits. UPSR signal thresholds—the levels that determine when the UPSR path is switched—are set at the circuit level. To create UPSR circuits, see the “Circuits Overview” section on page 6-1.

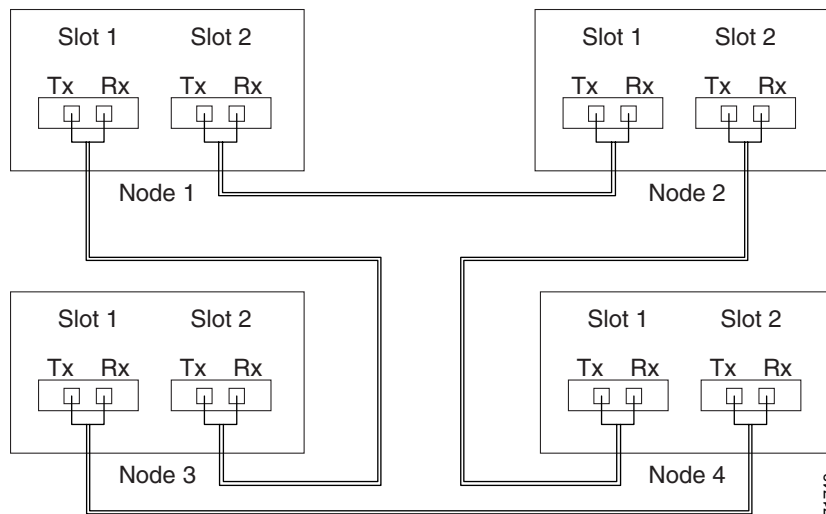
Procedure: Install the UPSR Trunk Cards

- Step 1** Install the OC-N cards that will serve as the UPSR trunk cards. You can install the OC-3, OC-12, and OC-48 cards in any high-speed slot (Slots 1–4).
- Step 2** Allow the cards to boot.
- Step 3** Attach the fiber to the east and west UPSR ports at each node.

To avoid errors, make the east and west ports the same slot in each node. Fiber connected to an east port at one node must plug into the west port on an adjacent node. Figure 5-21 shows fiber connections for a four-node UPSR with trunk cards in Slot 1 (west) and Slot 2 (east).

Always plug the fiber plugged into the transmit (Tx) connector of an OC-N card at one node into the receive (Rx) connector of an OC-N card at the adjacent node. The card will display an SF LED if Tx and Rx fibers are mismatched.

Figure 5-21 Connecting fiber to a four-node UPSR



Procedure: Configure the UPSR DCC Terminations

- Step 1** Log into the first node that will be in the UPSR.
- Step 2** Click the **Provisioning > Sonet DCC** tabs.
- Step 3** In the SDCC Terminations section, click **Create**.
- Step 4** On the Create SDCC Terminations dialog box, press Control and click the two slots/ports that will serve as the UPSR ports at the node. For example, Slot 3 (OC-48)/Port 1 and Slot 2 (OC-48)/Port 1.



Note The ONS 15327 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs. Line DCCs can be used to tunnel DCCs from third party equipment across ONS 15327 networks. For procedures, see the “Creating DCC Tunnels” section on page 6-20.

- Step 5** Click **OK**.
The slots/ports display in the SDCC Terminations section.
- Step 6** Complete Steps 2 – 5 at each node that will be in the UPSR.
-

After configuring the SONET DCC, set the timing for the node. For procedures, see the “Set Up ONS 15327 Timing” procedure on page 3-13. After configuring the timing, enable the UPSR ports as described in the following procedure.

Procedure: Enable the UPSR Ports

- Step 1** Log into the first UPSR node.
- Step 2** Double-click one of the cards that you configured as an SDCC termination.
- Step 3** Click the **Provisioning > Line** tabs.
- Step 4** Under Status, select **In Service** for each port that you want enabled.
- Step 5** Repeat Steps 2 - 4 for the second card.
- Step 6** Click **Apply**.
-

You configured a UPSR for one node. Use the same procedures to configure the additional nodes. To create path-protected mesh networks, see the “Path-Protected Mesh Networks” section on page 5-42. To create circuits, see the “Creating Circuits and VT Tunnels” section on page 6-2.

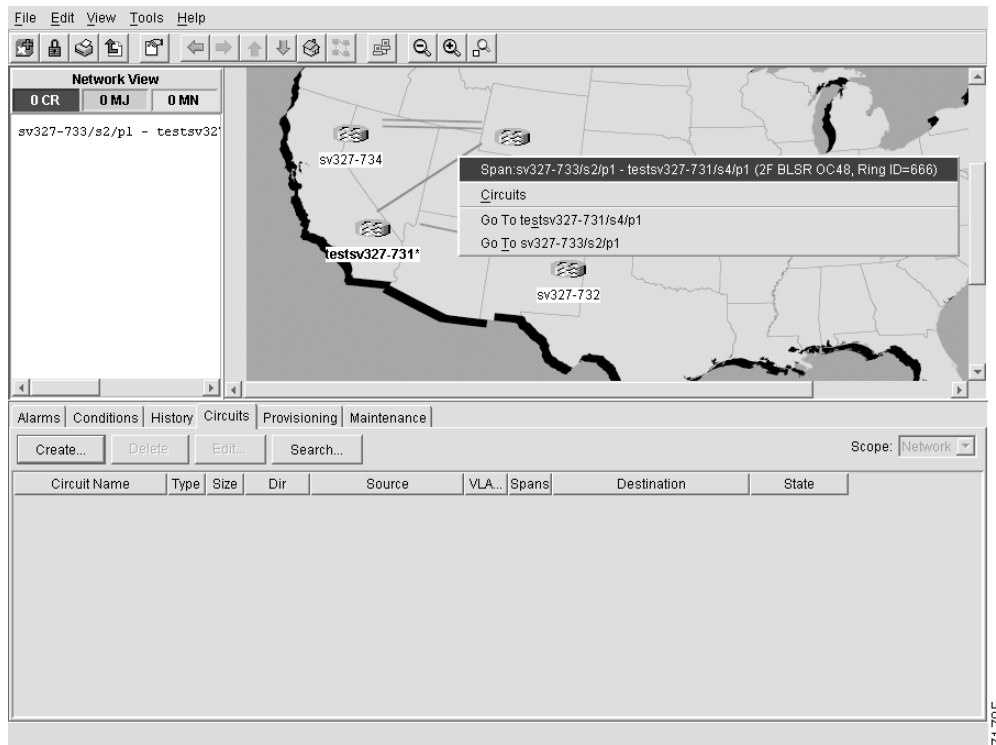
5.3.3 Adding and Removing UPSR Nodes

This section explains how to add and remove nodes in an ONS 15327 UPSR configuration. To add or remove a node, you switch traffic on the affected spans to route traffic away from the area of the ring where service will be performed. Use the span selector switch option to switch traffic from a UPSR span at different protection levels. The span selector switch option is useful when you need to reroute traffic from a UPSR span temporarily to add or drop nodes, perform maintenance, or perform other operations.

Procedure: Switch UPSR Traffic

- Step 1** Display the network view.
- Step 2** Right-click the span that will be cut to add or delete a node and select **Circuits** from the shortcut menu (Figure 5-22).

Figure 5-22 Using the span shortcut menu to display circuits



Step 3 On the Circuits on Span dialog box (Figure 5-23), select the protection from the **Switch all UPSR circuits away** menu:

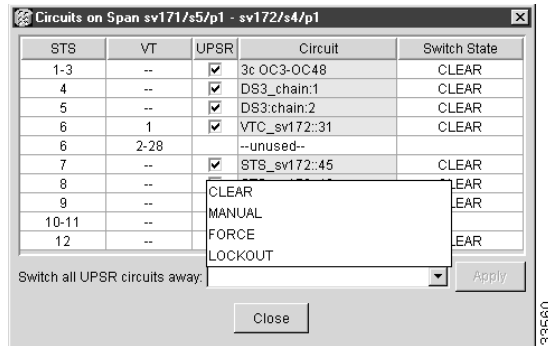
- CLEAR removes a previously-set switch command.
- MANUAL switches the span if the new span is error free.
- FORCE forces the span to switch, regardless of whether the new span is error free.
- LOCKOUT locks out or prevents switching to a highlighted span. (LOCKOUT is only available when Revertive traffic is enabled.)



Caution

FORCE and LOCKOUT commands override normal protective switching mechanisms. Applying these commands incorrectly can cause traffic outages.

Figure 5-23 Switching UPSR circuits



- Step 4** Click Apply.
- Step 5** When the confirmation dialog box appears, click **OK** to confirm the protection switching. The column under **Switch State** changes to your chosen level of protection.
- Step 6** Click **Close** after **Switch State** changes.

Procedure: Add a UPSR Node



Note You can add only one node at a time. Perform these steps onsite and not from a remote location.

- Step 1** Log into CTC and display the UPSR nodes in network view. Verify the following:
- All UPSR spans on the network map are green.
 - No critical or major alarms (LOF, LOS, ASP, ASL) are displayed on the **Alarms** tab.
 - On the **Conditions** tab, no UPSR switches are active.
 - At each physical UPSR node, all fibers are securely connected to the appropriate ports.


If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding.

- Step 2** At the node that will be added to the UPSR:
- Verify that the OC-N cards are installed and fiber is available to connect to the other nodes.
 - Run test traffic through the cards that will connect to the UPSR.
 - Use the “Setting Up a UPSR” section on page 5-23 to provision the new node.
- Step 3** Log into a node that will directly connect to the new node.
- Step 4** Use the “Switch UPSR Traffic” procedure on page 5-25 to initiate a FORCE switch to switch traffic away from the span that will connect to the new node.



Caution Traffic is not protected during a protection switch.

- Step 5** Two nodes will connect directly to the new node; remove their fiber connections:
- a. Remove the east fiber connection from the node that will connect to the west port of the new node.

- b.** Remove the west fiber connection from the node that will connect to the east port of the new node.
- Step 6** Replace the removed fiber connections with connections from the new node.
-  **Note** Perform this step on site at the new node.
-
- Step 7** Log out of CTC and then log back in.
- Step 8** Display the network view. The new node should appear in the network map. Wait for a few minutes to allow all the nodes to appear.
- Step 9** Click the **Circuits** tab and wait for all the circuits to appear, including spans. The affected circuit will display as “incomplete.”
- Step 10** In the network view, right-click the new node and select **Update Circuits With New Node** from the list of options. Wait for the confirmation dialog box to appear. Verify that the number of updated circuits displayed in the dialog box is correct.
- Step 11** Select the **Circuits** tab and verify that no incomplete circuits are displayed. If incomplete circuits are displayed, repeat Step 9.
- Step 12** Use the “Switch UPSR Traffic” procedure on page 5-25 to clear the protection switch.
-

Procedure: Remove a UPSR Node



Caution

The following procedure is designed to minimize traffic outages while nodes are removed, but traffic will be lost when you delete and recreate circuits that passed through the removed node.

- Step 1** Log into a node on the same network as the node you will remove. (Do not log into the node that you will remove.)
- Step 2** From the View menu choose **Go to Network View** to display the UPSR. Verify the following:
- All UPSR spans on the network map are green.
 - No critical or major alarms (LOF, LOS, ASP, ASL) are displayed on the **Alarms** tab.
 - On the **Conditions** tab, no UPSR switches are active.
 - At each UPSR node, all fibers are securely connected to the appropriate ports.
- If trouble is indicated, for example, a critical or major alarm exists, resolve the problem before proceeding.
- Step 3** Delete and recreate the following types of circuits:
- a.** Identify unprotected circuits that pass through the node you are removing and delete and recreate each circuit one at a time so that they no longer pass through that node.
 - b.** Identify the UPSR circuits that pass through the node you are removing but do not ingress and egress on the same STSs and delete and recreate each circuit one at a time so that they ingress and egress on the same STS.
 - c.** If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.
If UPSR circuits ingress and egress on the same STS, the circuit will repair itself when the protection switch clears.

- Step 4** Use the “Switch UPSR Traffic” procedure on page 5-25 to initiate a FORCE switch to switch traffic away from the node you are removing. Initiate a FORCE switch on all spans connected to the node you are removing.
- Step 5** If the removed node was the BITS timing source, select a new node as the BITS source or select another node as the master timing node.



Caution Traffic is not protected during a forced protection switch.

- Step 6** Remove all fiber connections between the node being removed and the two neighboring nodes.
- Step 7** Reconnect the fiber of the two neighboring nodes directly, west port to east port.
- Step 8** Restart CTC so that the removed node is no longer visible.
- Step 9** Open the Alarms tab of each newly-connected node and verify that the span cards are free of alarms. Resolve any alarms before proceeding.
- Step 10** Use the “Switch UPSR Traffic” procedure on page 5-25 to clear the protection switch.

5.4 Subtending Rings

The ONS 15327 supports up to ten SONET DCCs. Therefore, one ONS 15327 node can terminate and groom any one of the following ring combinations:

- 5 UPSRs, or
- 4 UPSRs and 1 BLSR, or
- 2 BLSRs

Subtending rings from an ONS 15327 reduces the number of nodes and cards required and reduces external shelf-to-shelf cabling. Figure 5-24 shows an ONS 15327 with multiple subtending rings.

Figure 5-24 An ONS 15327 with subtending rings

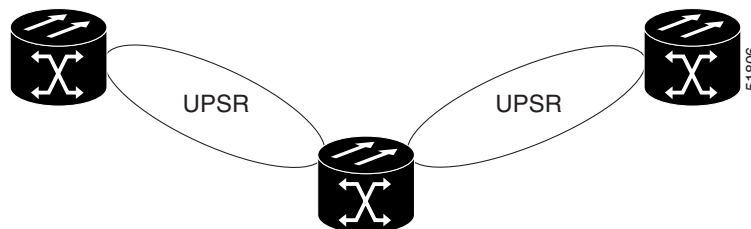
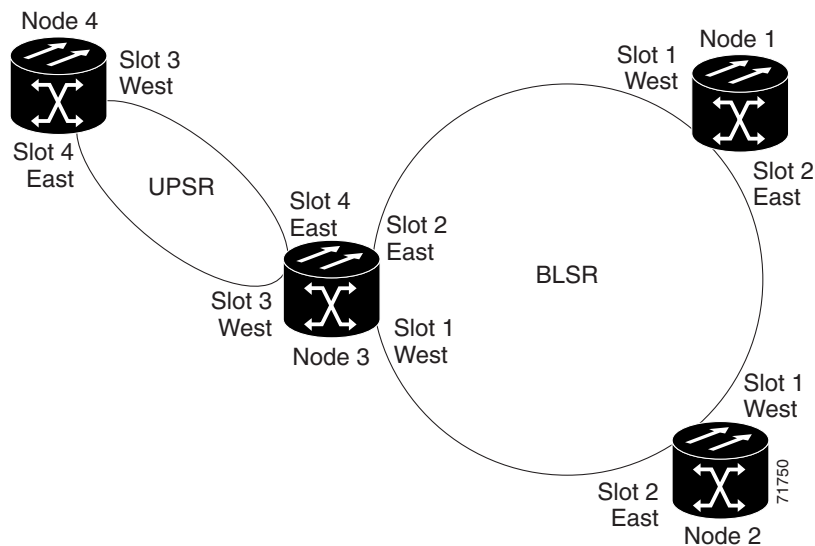


Figure 5-25 shows a UPSR subtending from a BLSR. In this example, Node 3 is the only node serving both the BLSR and UPSR. OC-N cards in Slots 1 and 2 serve the BLSR, and OC-N cards in Slots 3 and 4 serve the UPSR.

Figure 5-25 A UPSR subtending from a BLSR



Procedure: Subtend a UPSR from a BLSR

This procedure requires an established BLSR and one BLSR node with OC-N cards and fibers to carry the UPSR. The procedure also assumes you can set up a UPSR. (For UPSR setup procedures, see the “Setting Up a UPSR” section on page 5-23.)

-
- Step 1** In the node that will subtend the UPSR (Node 3 in Figure 5-25), install the OC-N cards that will serve as the UPSR trunk cards (Node 3, Slots 3 and 4).
 - Step 2** Attach fibers from these cards to the UPSR trunk cards on the UPSR nodes. In Figure 5-25, Slot 3 Node 3 connects to Slot 4/Node 5, and Slot 4 connects to Slot 3/Node 6.
 - Step 3** From the node view, click the **Provisioning > Sonet DCC** tabs.
 - Step 4** Click **Create**.
 - Step 5** In the Create SDCC Terminations dialog box, click the slot and port that will carry the UPSR.
 - Step 6** Click **OK**.
The selected slots/ports are displayed in the SDCC Terminations section.
 - Step 7** Put the ports that you will use for the UPSR in service:
 - a. In the node view, double-click UPSR trunk card.
 - b. Select the **Provisioning > Line** tabs. Under Status, choose **In Service**.
 - c. Click **Apply**.
 - d. Repeat steps a - c for the second UPSR trunk card.
 - Step 8** Follow Steps 1 – 7 for the other nodes you will use for the UPSR.

Step 9 Go to the network view to view the subtending ring.

Procedure: Subtend a BLSR from a UPSR

This procedure requires an established UPSR and one UPSR node with OC-N cards and fibers to connect to the BLSR. The procedure also assumes you can set up a BLSR. (For BLSR setup procedures, see the “Setting Up BLSRs” section on page 5-7.)

-
- Step 1** In the node that will subtend the BLSR (Node 3 in the Figure 5-25 example), install the OC-N cards that will serve as the BLSR trunk cards (in Figure 5-25, Node 3, Slots 3 and 4).
- Step 2** Attach fibers from these cards to the BLSR trunk cards on the BLSR nodes. In Figure 5-25, Slot 3/Node 3 connects to Slot 4/Node 5, and Slot 4 connects to Slot 3/Node 6.
- Step 3** From the node view, click the **Provisioning > Sonet DCC** tabs.
- Step 4** Click **Create**.
- Step 5** In the Create SDCC Terminations dialog box, click the slot and port that will carry the BLSR.
- Step 6** Click **OK**.
- Step 7** The selected slots/ports are displayed under SDCC Terminations.
- Step 8** Put the ports that you will use for the BLSR in service:
- In the node view, double-click the BLSR trunk card.
 - Select the **Provisioning > Line** tabs. Under Status, choose **In Service**.
 - Click **Apply**.
 - Repeat steps a – c for the second BLSR trunk card.
- Step 9** Use the “Provision the BLSR” procedure on page 5-9 to configure the BLSR.
- Step 10** Follow Steps 1– 8 for the other nodes that will be in the BLSR.
- Step 11** Go to the network view to see the subtending ring.
-

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

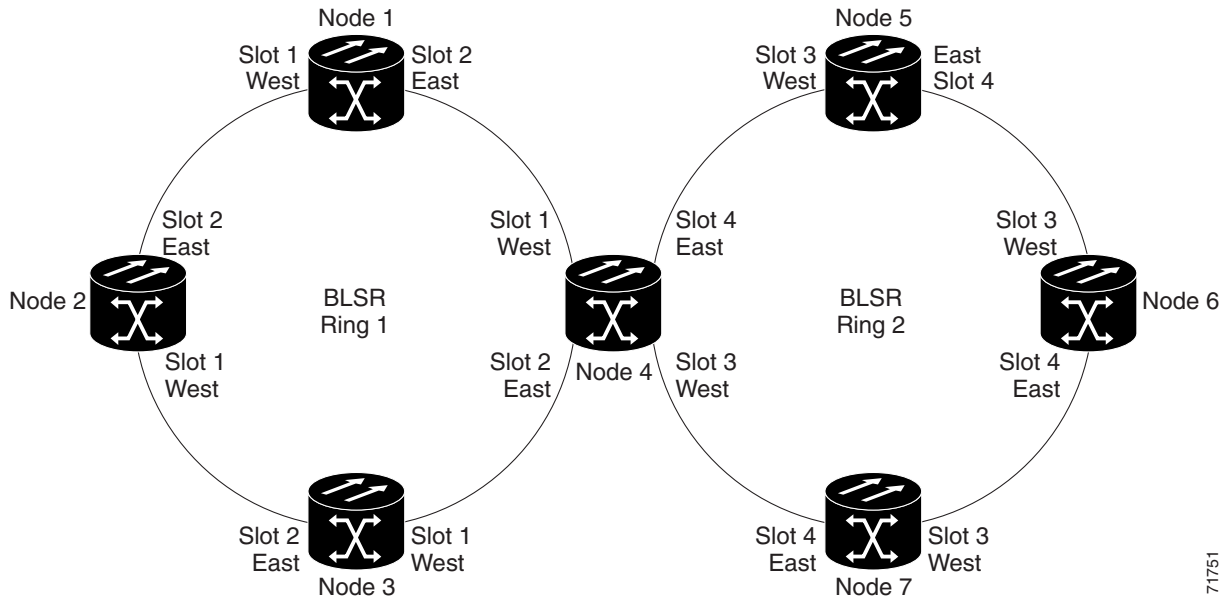
Figure 5-26 shows two BLSRs shared by one ONS 15327. Ring 1 runs on Nodes 1, 2, 3, and 4. Ring 2 runs on Nodes 4, 5, 6, and 7. Two BLSR rings, Ring 1 and Ring 2, are provisioned on Node 4. Ring 1 uses cards in Slots 1 and 2, and Ring 2 uses cards in Slots 3 and 4.



Note

Although different node IDs are used for the two BLSRs shown in Figure 5-26, nodes in different BLSRs can use the same node ID.

Figure 5-26 A BLSR subtending from a BLSR



After subtending two BLSRs, you can route circuits from nodes in one ring to nodes in the second ring. For example in Figure 5-26, you can route a circuit from Node 1 to Node 7. The circuit would normally travel from Node 1 to Node 4 to Node 7. If fiber breaks occur, for example between Nodes 1 and 4 and Nodes 4 and 7, traffic is rerouted around each ring: in this example, Nodes 2 and 3 in Ring 1 and Nodes 5 and 6 in Ring 2.

Procedure: Subtend a BLSR from a BLSR

This procedure requires an established BLSR and one BLSR node with OC-N cards and fibers to carry the BLSR. The procedure also assumes you know how to set up a BLSR. For BLSR setup procedures, see the “Setting Up BLSRs” section on page 5-7.

- Step 1** In the node that will subtend the BLSR (Node 4 in Figure 5-26), install the OC-N cards that will serve as the BLSR trunk cards (Node 4, Slots 3 and 4).
- Step 2** Attach fibers from these cards to the BLSR trunk cards on the BLSR nodes. In Figure 5-26, Node 4/Slot 3 connects to Node 7/Slot 4, and Slot 4 connects to Node 5/Slot 3.
- Step 3** From the node view, click the **Provisioning > Sonet DCC** tabs.
- Step 4** Click **Create**.
- Step 5** In the Create SDCC Terminations dialog box, click the slot and port that will carry the BLSR.
- Step 6** Click **OK**.
- Step 7** The selected slots/ports are displayed in the SDCC Terminations section.
- Step 8** Put the ports that you will use for the BLSR in service:
 - a. In the node view, double-click the BLSR trunk card.
 - b. Select the **Provisioning > Line** tabs. Under Status, choose **In Service**.
 - c. Click **Apply**.

- d. Repeat steps a – c for the second BLSR trunk card.
- Step 9** To configure the BLSR, use the “Provision the BLSR” procedure on page 5-9. The subtending BLSR must have a ring ID that differs from the ring ID of the first BLSR.
- Step 10** Follow Steps 1 – 8 for the other nodes that will be in the subtending BLSR.
- Step 11** Display the network view to see the subtending ring.

Figure 5-27 shows the Ring subtab for Node 5, which is the node that carries the two rings.

Figure 5-27 Configuring two BLSRs on the same node

The screenshot displays the configuration for two BLSRs on a node. The hardware view shows slots 1-4 with OC48-1-IR cards and slots 5-6 with XTC-28-3 cards. The configuration table below is as follows:

Type	Rate	Ring ID	Node ID	Ring Reversion	Span Reversion	West Line	East Line	Apply
2-Fiber	OC12	333	0	5.0 min.		s3/p1 (Work/Act) s3/p1 (Prot/Stby)	s4/p1 (Work/Act) s4/p1 (Prot/Stby)	Apply
2-Fiber	OC48	666	7	0.5 min.		s2/p1 (Work/Act) s2/p1 (Prot/Stby)	s1/p1 (Work/Act) s1/p1 (Prot/Stby)	Reset

5.4.1 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 this chapter whenever you make connections between ONS 15454 and ONS 15327 nodes. Figure 5-28 shows a basic linear or UPSR connection between ONS 15327 and ONS 15454 nodes.

Figure 5-28 A linear or UPSR connection between ONS 15454 and ONS 15327 nodes

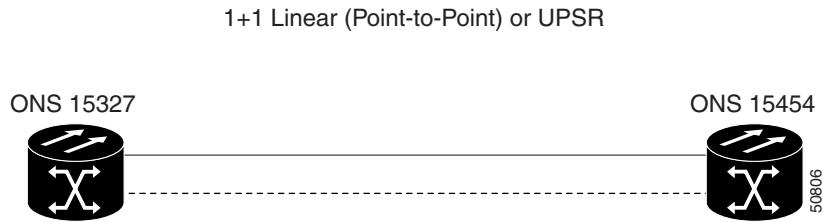
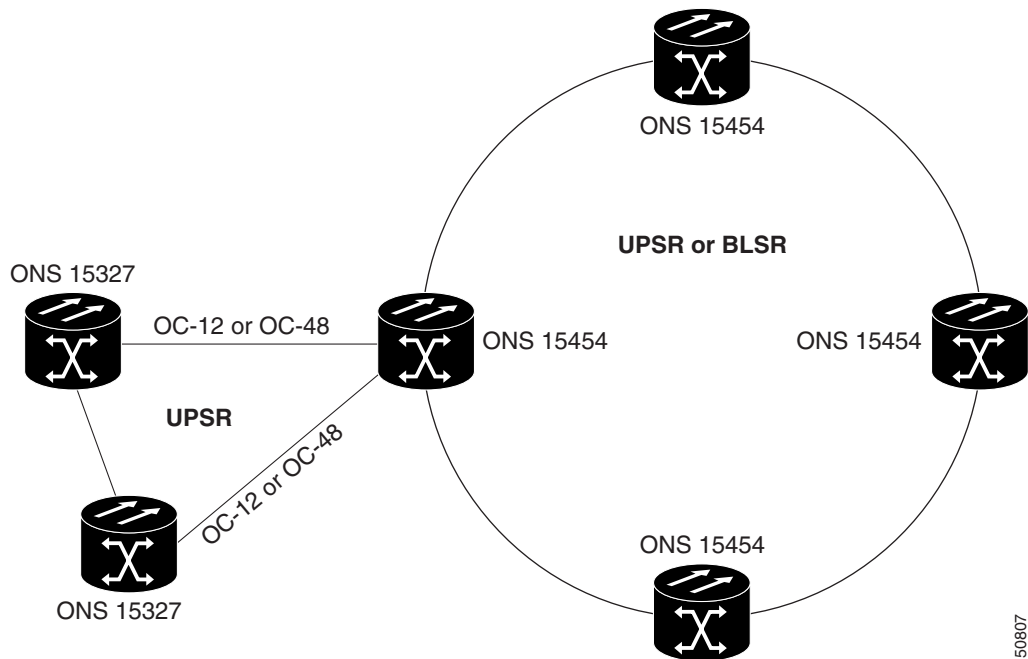


Figure 5-29 shows a ring of ONS 15327s subtended from a ring of ONS 15454s.

Figure 5-29 ONS 15327 ring subtended from an ONS 15454 ring

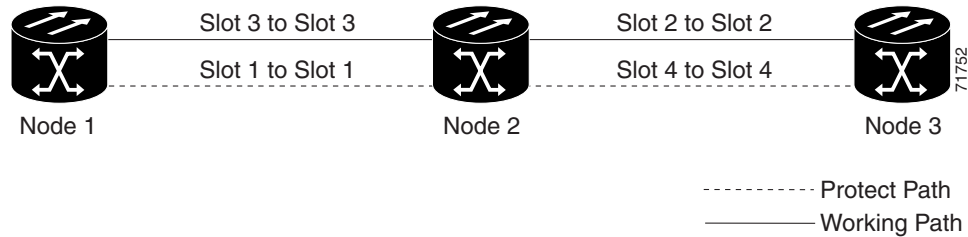


5.5 Linear ADM Configurations

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

Figure 5-30 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 5-30 A linear (point-to-point) ADM configuration



Procedure: Create a Linear ADM

Complete the following steps for each node that will be included in the linear ADM.

-
- Step 1** Complete the general setup information for the node. For procedures, see the “Setting Up Basic Node Information” section on page 3-2.
- Step 2** Set up the network information for the node. For procedures, see the “Setting Up Network Information” section on page 3-3.
- Step 3** Set up 1+1 protection for the OC-N cards in the ADM. In Figure 5-30, Slots 2 and 3 are the working ports and Slots 1 and 4 are the protect ports. In this example, you would set up one protection group for Node 1 (Slots 1 and 3), two for Node 2 (Slots 1 and 3, and 2 and 4) and one for Node 3 (Slots 2 and 4). To create protection groups, see the “Creating Protection Groups” section on page 3-7.
- Step 4** For OC-N ports connecting ONS 15327s, set the SONET DCC terminations:
- Log into a linear ADM node and select the **Provisioning > Sonet DCC** tabs.
 - In the SDCC Terminations section, click **Create**.
 - On the Create SDCC Terminations dialog box, select the working port. Click **OK**.



Note Terminating nodes (Nodes 1 and 3 in Figure 5-30) will have one SDCC, and intermediate nodes (Node 2 in Figure 5-30) will have two SDCCs.

- Step 5** Use the “Set Up ONS 15327 Timing” procedure on page 3-13 to set up the node timing. If a node is using line timing, set the working OC-N card as the timing source.
- Step 6** Place the OC-N ports in service:
- Open an OC-N card that is connected to the linear ADM.
 - On the **Provisioning > Line** tabs under Status, select **In Service**.
 - Click **Apply**.

Repeat Step 6 for each OC-N card connected to the linear ADM.

Procedure: Convert a Linear ADM to UPSR

The following procedures describe how to convert a three-node linear ADM to a UPSR. You will need a SONET test set to monitor traffic while you perform these procedures.

**Caution**

This procedure is service affecting.

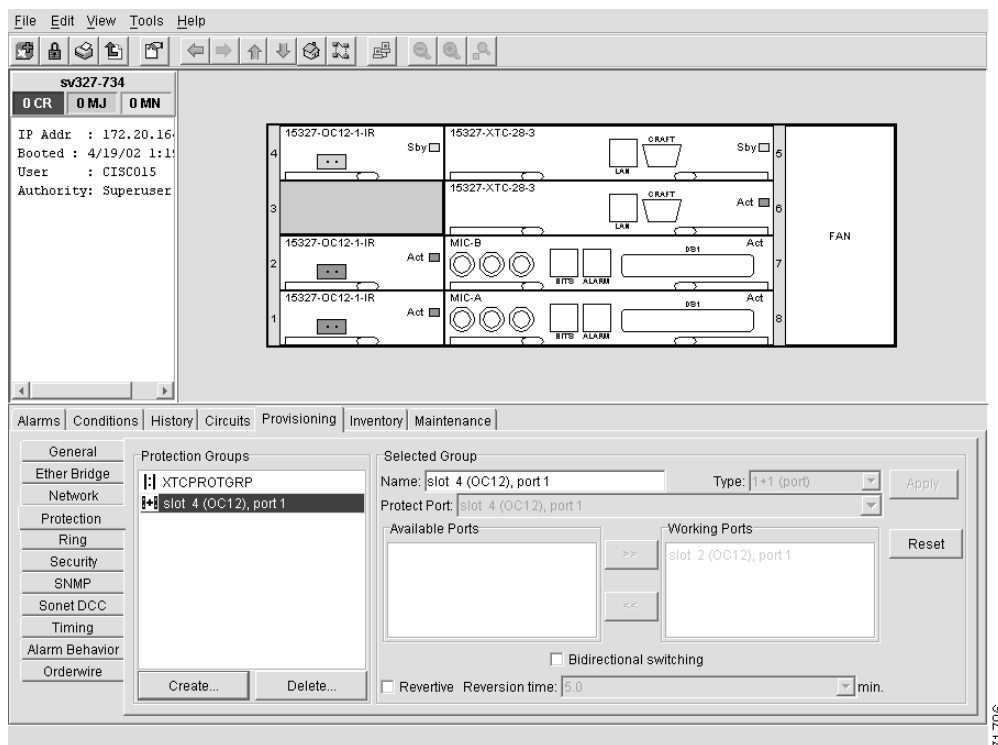
**Caution**

Always wear an authorized electrostatic discharge wrist band when removing or installing ONS 15327 cards.

Step 1 Start CTC and log into one of the nodes that you want to convert from linear to ring.

Step 2 Click the **Maintenance > Protection** tabs (Figure 5-31).

Figure 5-31 Verifying working slots in a protection group



Step 3 Under Protection Groups, select the 1+1 protection group (that is, the group supporting the 1+1 span cards).

Step 4 Under Selected Group, verify that the working slot/port is shown as “Working/Active.” If yes, go to Step 5. If the working slot says “Working/Standby” and the protect slot says “Protect/Active,” switch traffic to the working slot:

- a. Under Selected Group, select the protect slot, that is, the slot that says “Protect/Active.”
- a. From the Switch Commands, select **Manual**.
- b. Click **Yes** on the confirmation dialog box.
- c. Under Selected Group, verify that the working slot/port says “Working/Active.” If so, continue to Step (d). If not, clear the conditions that prevent the card from carrying working traffic before proceeding.
- d. From the Switch Commands, select **Clear**. A Confirm Clear Operation dialog is displayed.

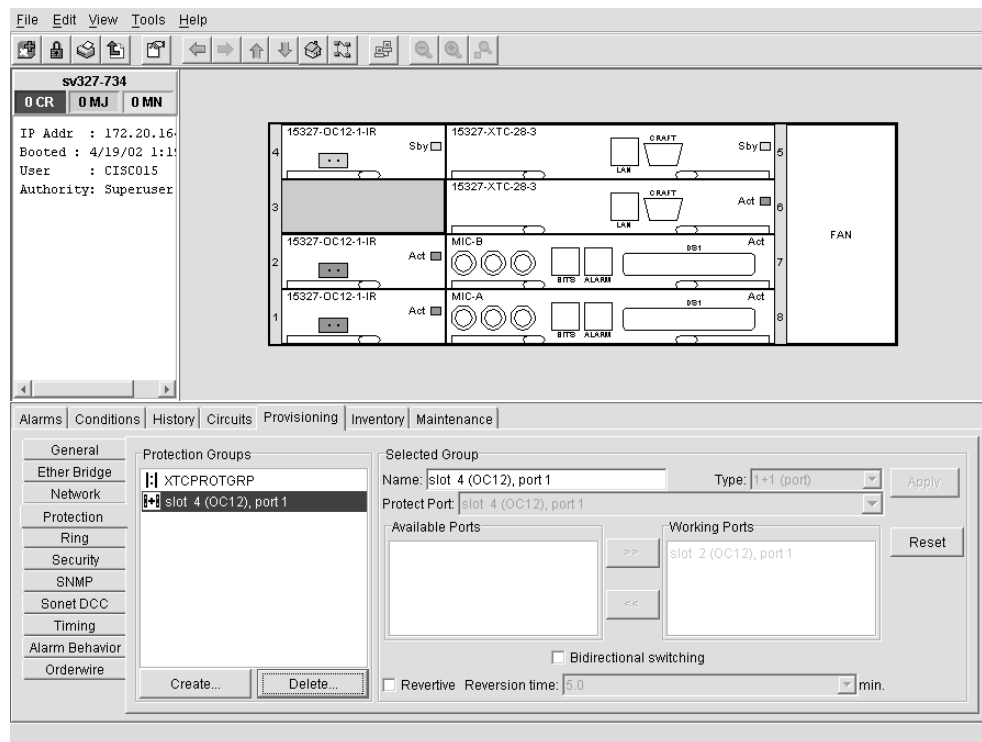
- e. Click **Yes** on the confirmation dialog box.
- Step 5** Repeat Step 4 for each group in the 1+1 Protection Groups list at all nodes that will be converted.
- Step 6** For each node, delete the 1+1 OC-N protection group that supports the linear ADM span:



Note Deleting a 1+1 protection group may cause unequipped path (UNEQ-P) alarms to occur.

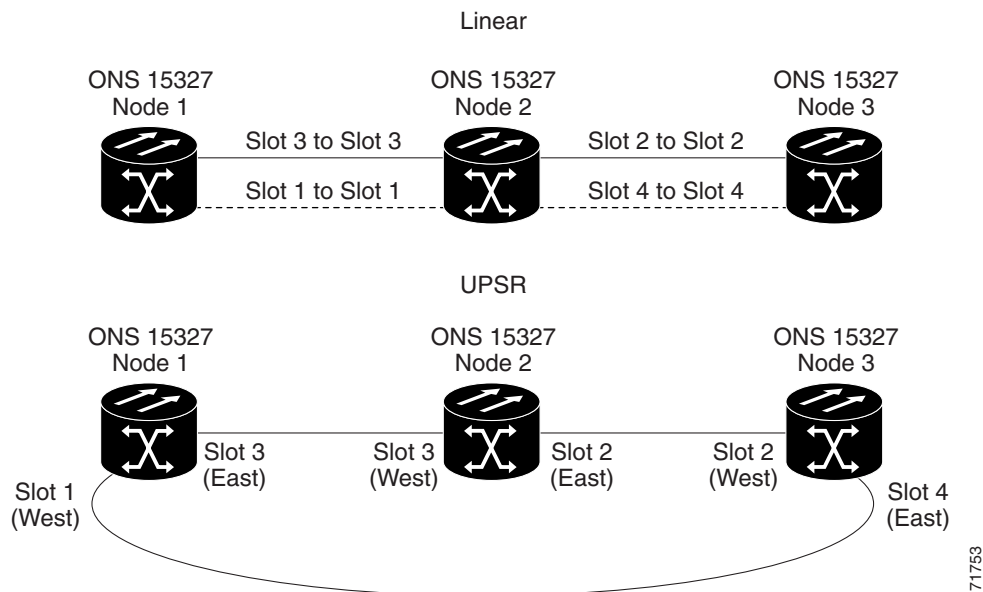
- a. Click the **Provisioning > Protection** tabs (Figure 5-32).
- b. From the Protection Groups list, choose the 1+1 group you want to delete. Click **Delete**.
- c. Click **Yes** on the confirmation dialog box.
- d. Verify that no traffic disruptions are indicated on the test set. If disruptions occur, do not proceed. Recreate the protection group and isolate the cause of the disruption.
- e. Continue deleting 1+1 protection groups while monitoring the existing traffic with the test set.

Figure 5-32 Deleting a protection group



- Step 7** Physically remove one of the protect fibers running between the middle and end nodes. For example, in the Figure 5-33, the fiber from Node 2/Slot 4 to Node 3/Slot 4 is removed. The corresponding OC-48 card will go into an LOS condition for that fiber and port.

Figure 5-33 Converting a linear ADM to a UPSR



- Step 8** Physically reroute the other protect fiber to connect the two end nodes. In the Figure 5-33 example, the fiber between Node 1/Slot 1 and Node 2/Slot 1 is rerouted to connect Node 1/Slot 1 to Node 3/Slot 4. If you are leaving the OC-N cards in place, go to Step 13. If you are removing the cards, complete Steps 9 – 12. (In this example, cards in Node 2/Slots 1 and 4 are removed.)
- Step 9** In the middle node, place the cards in Slots 1 and 4 out of service:
- Display the first card in card view and select the **Provisioning > Line** tabs.
 - Under Status, select **Out of Service**. Click **Apply**.
 - Repeat Steps a and b for the second card.
- Step 10** Delete the equipment records for the cards:
- Display the node view. (In card view, click the Up arrow on the toolbar.)
 - Right-click the card you just took out of service (e.g. Slot 1) and select **Delete Card**. (You can also go to the **Inventory** tab, select the card, and click **Delete**.)
 - Click **Yes** on the confirmation dialog box.
 - Repeat (a) through (c) for the second card (e.g. Slot 4).
- Step 11** Save all circuit information.
- In node view, select the **Provisioning > Circuits** tab.
 - Record the circuit information using one of the following procedures:
 - From the File menu, select **Print** to print the circuits table, or
 - From the File menu, select **Export** to export the circuit data in HTML, CSV (comma separated values), or TSV (tab separated values). Click **Ok** and save the file in a temporary directory.

See the “Printing and Exporting CTC Data” section on page 2-41 for more information.

- Step 12** Remove the OC-N cards that are no longer connected to the end nodes (Slots 1 and 4, in the example).
- Step 13** Display one of the end nodes (Node 1 or Node 3 in the example).
- Step 14** Click the **Provisioning > Sonet DCC** tabs.
- Step 15** In the SDCC Terminations section, click **Create**.
- Step 16** In the Create SDCC Terminations dialog box, select the slot/port that had been the protect slot in the linear ADM, for example, for Node 1, this would be Slot 1/Port 1 (OC-48).
- Step 17** Click **OK**.
An EOC SDCC alarm will occur until an SDCC termination is created on the adjacent node.
- Step 18** Go to the node on the opposite end (Node 3 in the Figure 5-33 example) and repeat Steps 14 – 17.
- Step 19** Delete and reenter the circuits one at a time. (See the “Creating Circuits and VT Tunnels” section on page 6-2.)



Note Deleting circuits is traffic affecting.

You can create the circuits automatically or manually. However, circuits must be protected. When they were built in the linear ADM, they were protected by the protect path on Node 1/Slot 1 to Node 2/Slot 1 to Node 3/Slot 4. With the new UPSR, circuits should also be created with protection.

Deleting the first circuit and recreating it to the same card/port should restore the circuit immediately.

- Step 20** Monitor your SONET test set to verify that the circuit was deleted and restored.
 - Step 21** You should also verify that the new circuit path for the clockwise (CW) fiber from Node 1 to Node 3 is working. To do this, switch to network view and move your cursor to the green span between Node 1 and 3.
Although the cursor only shows the first circuit created, do not become alarmed that the other circuits are not present. Verify with the SONET test set that the original circuits and the new circuits are operational. The original circuits were created on the counter clockwise linear path.
 - Step 22** Go to the network map to view the newly-created ring.
-

Procedure: Convert a Linear ADM to a BLSR

The following procedures describe how to convert a three-node linear ADM to a BLSR. You will need a SONET test set to monitor traffic while you perform these procedures.



This procedure is service-affecting.



Always wear an authorized electrostatic discharge wrist band when removing or installing ONS 15327 cards.

- Step 1** Start CTC and log into one of the nodes that you want to convert from linear to ring.
- Step 2** Click the **Maintenance > Protection** tabs.

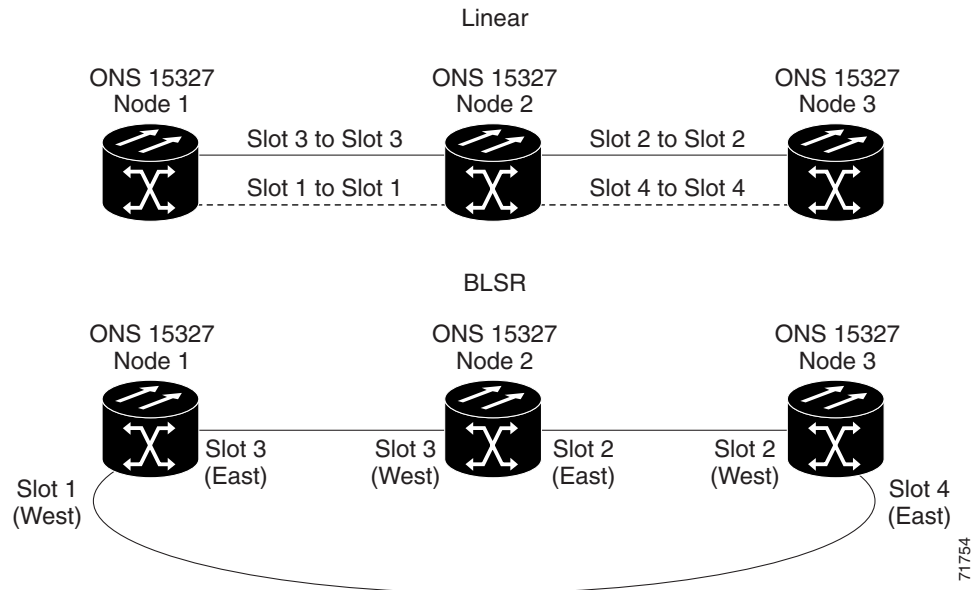
- Step 3** Under Protection Groups, select the 1+1 protection group (that is, the group supporting the 1+1 span cards).
- Step 4** Under Selected Group, verify that the working slot/port is shown as “Working/Active.” If yes, go to Step 5. If the working slot says “Working/Standby” and the protect slot says “Protect/Active,” switch traffic to the working slot:
- Under Selected Group, select the protect slot, that is, the slot that says “Protect/Active.”
 - From the Switch Commands, select **Manual**.
 - Click **Yes** on the confirmation dialog box.
 - Verify that the working slot is carrying traffic. If it is, continue to Step (d). If not, clear the conditions that prevent the card from carrying working traffic before proceeding.
 - From the Switch Commands, select **Clear**. A Confirm Clear Operation dialog is displayed.
 - Click **Yes** on the confirmation dialog box.
- Step 5** Repeat Step 4 for each group in the 1+1 Protection Groups list at all nodes that will be converted.
- Step 6** For each node, delete the 1+1 OC-N protection group that supports the linear ADM span:
- Click the **Provisioning > Protection** tabs.
 - From the Protection Groups list, choose the group you want to delete. Click **Delete**.
 - Click **Yes** on the confirmation dialog box.
 - Verify that no traffic disruptions are indicated on the SONET test set. If disruptions occur, do not proceed. Add the protection group and begin troubleshooting procedures to find out the cause of the disruption.



Note Deleting a 1+1 protection group may cause unequipped path (UNEQ-P) alarms to occur.

- Step 7** Physically remove one of the protect fibers running between the middle and end nodes. In the Figure 5-34 example, the fiber running from Slot 4/Node 2 to Slot 4/Node 3 is removed. The corresponding end-node trunk card will display an LOS alarm.

Figure 5-34 Converting a linear ADM to a BLSR



- Step 8** Physically reroute the other protect fiber so it connects the two end nodes. In the Figure 5-34 example, the fiber between Node 1/Slot 1 and Node 2/Slot 1 is rerouted to connect Node 1/Slot 1 to Node 3/Slot/ 13.
- If you are leaving the OC-N cards in place, go to Step 13. If you are removing the cards, complete Steps 9 – 12. (In this example, cards in Node 2/Slots 1 and 4 are removed.)
- Step 9** In the middle node, place the cards in Slots 1 and 4 out of service:
- Display the first card in card view, then select the **Provisioning > Line** tabs.
 - Under Status, select **Out of Service**. Click **Apply**.
 - Repeat Steps a and b for the second card.
- Step 10** Delete the equipment records for the cards:
- From the View menu, choose **Node View**.
 - Right-click the card you just took out of service (e.g. Slot 1) and select **Delete Card**. (You can also go to the **Inventory** tab, select the card, and click **Delete**.)
 - Click **Yes** on the confirmation dialog box.
 - Repeat (a) through (c) for the second card (e.g. Slot 4).
- Step 11** Save all circuit information:
- In node view, select the **Provisioning > Circuits** tab.
 - Record the circuit information using one of the following procedures:
 - From the File menu, select **Print** to print the circuits table, or,
 - From the File menu, select **Export** to export the circuit data in HTML, CSV (comma separated values), or TSV (tab separated values). Click **Ok** and save the file in a temporary directory.
 See the “Printing and Exporting CTC Data” section on page 2-41 for more information.
- Step 12** Remove the OC-N cards that are no longer connected to the end nodes (Slots 1 and 4, in the example).
- Step 13** Log into an end node. In node view, click the **Provisioning > Sonet DCC** tabs.

- Step 14** In the SDCC Terminations section, click **Create**.
- Step 15** Highlight the slot that is not already in the SDCC Terminations list (in this example, Port 1 of Slot 1 (OC-48) on Node 1).
- Step 16** Click **OK**. (An EOC SDCC alarm will occur until the DCC is created on the other node; in the example, Node 3/Slot 4).
- Step 17** Display the node on the opposite end (Node 3 in Figure 5-34) and repeat Steps 13 – 16.
- Step 18** For circuits running on a BLSR protect STS (STSs 7 – 12 for an OC-12 BLSR, STSs 25 – 48 for an OC-48 BLSR), delete and recreate the circuit:
- Delete the first circuit.
 - Recreate the circuit on STSs 1 – 6 (for an OC-12 BLSR) or 1 – 24 (for an OC-48 BLSR) on the fiber that served as the protect fiber in the linear ADM. During circuit creation, deselect “Route Automatically” and “Fully Protected Path” on the Circuit Creation dialog box so you can manually route the circuit on the appropriate STSs. See the “Create a Unidirectional Circuit with Multiple Drops” procedure on page 6-8 for more information.
 - Repeat Steps (a) and (b) for each circuit residing on a BLSR protect STS.



Note Deleting circuits is traffic affecting.

- Step 19** Follow all procedures in the “Setting Up BLSRs” section on page 5-7 to configure the BLSR. The ring should have an East/West logical connection. While it may not physically be possible to connect the OC-N cards in an East/West pattern, it is strongly recommended. If the network ring that is already passing traffic does not provide the opportunity to connect fiber in this manner, logical provisioning can be performed to satisfy this requirement.

Be sure to assign the same Ring ID and different node IDs to all nodes in the BLSR. Do not accept the BLSR ring map until all nodes are provisioned.



Note E-W Mismatch alarms will occur until all nodes are provisioned.

- Step 20** Display the network map to view the newly-created ring.
-

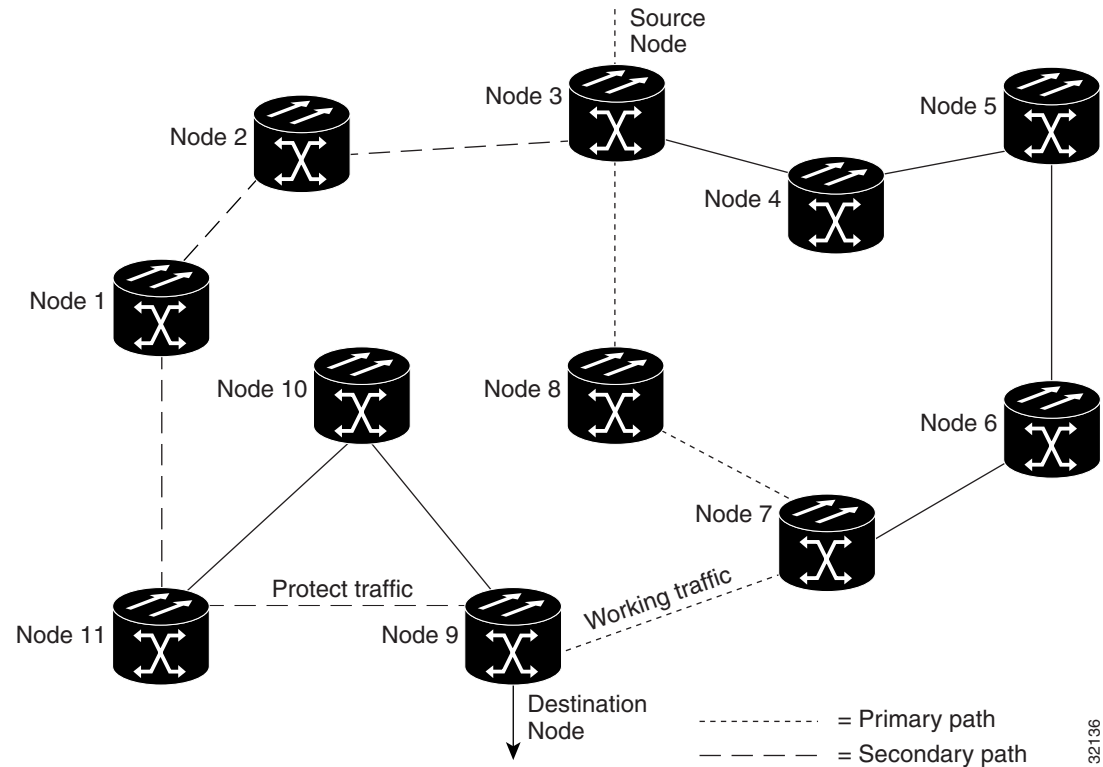
5.6 Path-Protected Mesh Networks

In addition to single BLSRs, UPSRs and ADMs, you can extend ONS 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 5-35, a circuit is created from Node 3 to Node 9. CTC determines that the shortest route between the two nodes passes through Node 8 and Node 7, shown by the dotted line, and automatically creates cross-connections at Nodes, 3, 8, 7, and 9 to provide the primary circuit path.

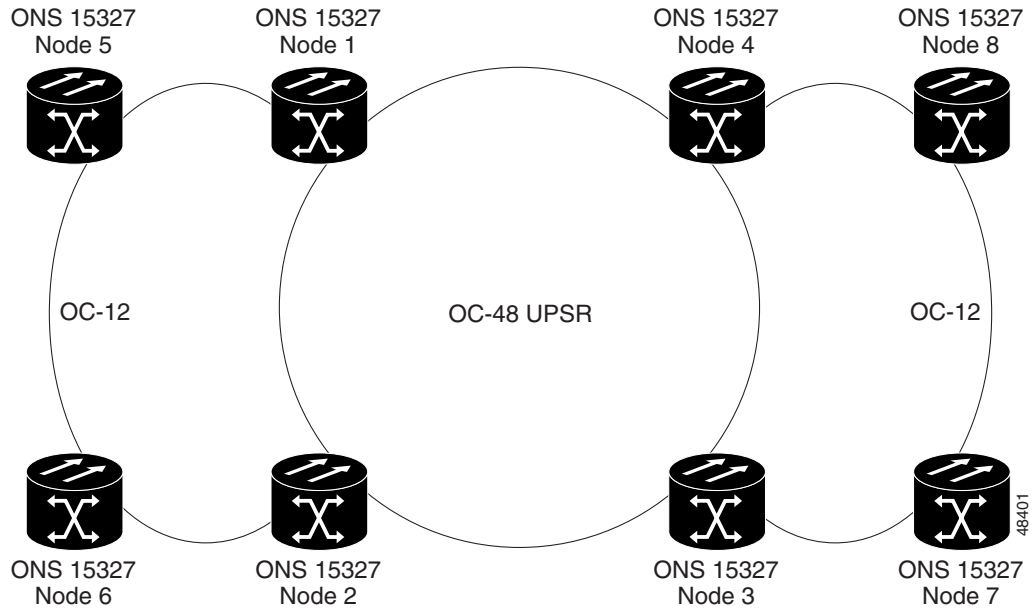
If full protection is selected, CTC creates a second unique route between Nodes 3 and 9 which, in this example, passes through Nodes 2, 1, and 11. Cross-connections are automatically created at Nodes 3, 2, 1, 11, and 9, shown by the dashed line. If a failure occurs on the primary path, traffic switches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

Figure 5-35 A path-protected mesh network



PPMN also allows spans of different SONET line rates to be mixed together in “virtual rings.” Figure 5-36 shows Nodes 1, 2, 3, and 4 in a standard OC-48 ring. Nodes 5, 6, 7, and 8 link to the backbone ring through OC-12 fiber. The “virtual ring” formed by Nodes 5, 6, 7, and 8 uses both OC-48 and OC-12.

Figure 5-36 A PPMN virtual ring





Circuits and Tunnels

This chapter explains how to create and administer Cisco ONS 15327 circuits and tunnels, which includes:

- Creating standard STS and VT1.5 circuits
- Creating VT tunnels
- Creating multiple drop circuits
- Creating monitor circuits
- Editing UPSR circuits
- Creating path traces to monitor traffic
- Reviewing ONS 15327 cross-connect card capacities
- Creating DCC tunnels to tunnel third-party equipment through ONS 15327 networks

6.1 Circuits Overview

You can create STS and VT1.5 circuits across and within ONS 15327 nodes and assign different attributes to circuits, for example:

- Create one-way, two-way, or broadcast circuits.
- Assign user-defined names to circuits.
- Assign different circuit sizes. STS circuits can be STS-1, STS-3c, STS-12c, or STS-48c. Ethernet circuits can be STS-1, STS-3c, STS-6c, or STS-12c. (To create Ethernet circuits see the “Ethernet Circuit Configurations” section on page 9-6.)
- Route circuits automatically or manually.
- Automatically create multiple circuits.
- Require the circuit path to be fully protected.
- Require protected source and destination cards and ports.
- Define a secondary circuit source or destination that allows you to interoperate an ONS 15327 unidirectional path switched ring (UPSR) with third-party equipment UPSRs.

**Note**

In this chapter, “cross-connect” and “circuit” have the following meanings: Cross-connect refers to the connections that occur within a single ONS 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).

6.2 Creating Circuits and VT Tunnels

This section explains how to create STS and VT1.5 circuits and VT tunnels. For an explanation and examples of circuits and VT tunnels, see the “Cross-Connect Card Capacities” section on page 6-15. You can create unidirectional or bidirectional, revertive or non-revertive circuits. You can have circuits routed automatically or you can manually route them. The auto range feature eliminates the need to individually build circuits of the same type; CTC can create additional sequential circuits if you specify the number of circuits you need and build the first circuit.

You can provision circuits at any of the following points:

- Before cards are installed. The ONS 15327 allows you to provision slots and circuits before installing the traffic cards. (To provision an empty slot, right-click it and select a card from the shortcut menu.) However, circuits will not carry traffic until you install the cards and place their ports in service. For procedures, see the “Card Installation and Turn-Up” procedure on page 1-16 and the “Enable Ports” procedure on page 3-9.
- Cards are installed; ports are out of service. You must place the ports in service before circuits will carry traffic.
- Cards are installed, and their ports are in service. Circuits will carry traffic as soon as the signal is received.

Procedure: Create an Automatically Routed Circuit

**Note**

If you want to route circuits on protected drops, create the card protection groups before creating circuits. See the “Create Protection Groups for Optical Cards” procedure on page 3-8 if you are using optical cards. Electrical cards are automatically protected.

Step 1 Log into an ONS 15327 and click the **Circuits** tab.

**Tip**

You can also right-click a source node in network view, select **Provision Circuit To**, and choose the circuit destination node from the menu.

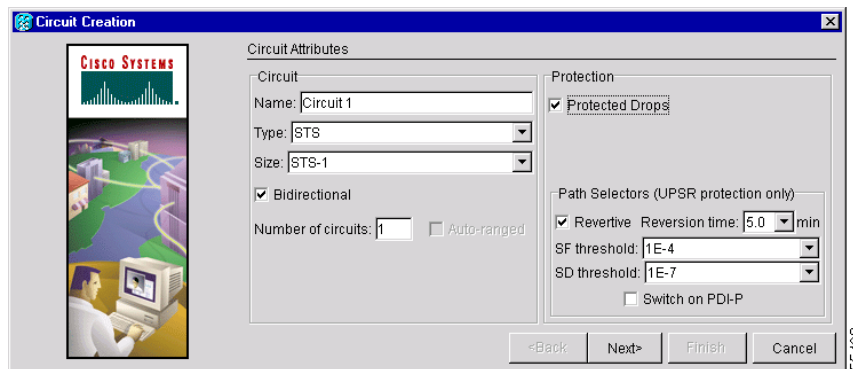
Step 2 Click **Create**.

Step 3 In the Circuit Creation dialog box (Figure 6-1), complete the following fields:

- *Name*—(optional) Assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.
- *Type*—Select the type of circuit you want to create: STS, VT (VT1.5), or VT tunnel. The circuit type determines the circuit-provisioning options that are displayed. See the “VT1.5 Cross-Connects” section on page 6-15 and the “VT Tunnels” section on page 6-18 for more information.

- *Size*—Select the circuit size (STS circuits only). The “c” indicates concatenated STSs.
- *Bidirectional*—Check this box to create a two-way circuit; uncheck it to create a one-way circuit (STS and VT circuits only; VT tunnels are bidirectional).
- *Number of circuits*—Type the number of circuits you want to create. If you enter more than 1, you can use auto-ranging to create the additional circuits automatically. Otherwise, CTC returns to the Circuit Source page after you create each circuit until you finish creating the number of circuits specified here.
- *Auto Ranged*—This checkbox is automatically selected when you enter more than one in the *Number of circuits* field. If selected, and you select the source and destination of one circuit, CTC automatically determines the source and destination for the remaining *Number of circuits* and creates the circuits. To determine the source and destination, CTC increments the most specific part of the end points. An end point can be a port, an STS, or a VT/DS-1. If CTC runs out of choices, or selects an end point that is already in use, CTC stops and allows you to either select a valid end point or cancel. If you select a valid end point and continue, auto-ranging begins after you click **Finish** for the current circuit. Deselect the box if you do not want CTC to create the circuits automatically.
- *Protected Drops*—If this box is checked, CTC only displays protected cards and ports (1:1 or 1+1 or BLSR protection) as choices for the circuit source and destination.

Figure 6-1 Creating an automatically-routed circuit



Step 4 (UPSR circuits only) Set the UPSR Selector Defaults:

- *Revertive*—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If Revertive is not chosen, traffic remains on the protect path after the switch.
- *Reversion time*—If *Revertive* is checked, set the reversion time. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared (the default reversion time is 5.0 minutes and the range is .5 to 12.0 minutes).
- *SF threshold*—Set the UPSR path-level signal failure bit error rate (BER) thresholds (STS circuits only).
- *SD threshold*—Set the UPSR path-level signal degrade BER thresholds (STS circuits only).
- *Switch on PDI-P*—Check this box if you want traffic to switch when an STS payload defect indicator is received (STS circuits only).

Step 5 Click **Next**.

Step 6 In the Circuit Source dialog box, set the circuit source.

Options include node, slot, port, STS, and VT/DS-1. The options that display depend on the circuit type and circuit properties you selected in Step 3 and the cards installed in the node. For Ethergroups, see the “Ethernet Circuit Configurations” section on page 9-6.

Click **Use Secondary Source** if you need to create a UPSR bridge/selector circuit entry point in a multivendor UPSR.

Step 7 Click **Next**.

Step 8 In the Circuit Destination dialog box, enter the appropriate information for the circuit destination. If the circuit is bidirectional, you can click **Use Secondary Destination** if you need to create a UPSR bridge/selector circuit destination point in a multivendor UPSR. (To add secondary destinations to unidirectional circuits, see “Create a Unidirectional Circuit with Multiple Drops” procedure on page 6-8.)

Step 9 Click **Next**.

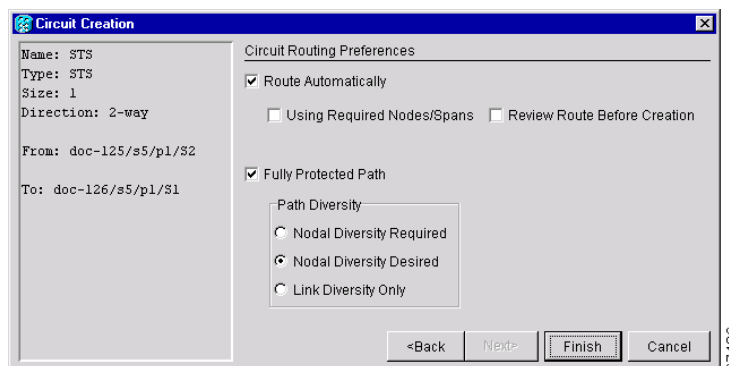
Step 10 Under Circuit Routing Preferences (Figure 6-2), select **Route Automatically**. The following options (described in detail in the next step) are available:

- *Using Required Nodes/Spans*—If selected, you can specify nodes and spans to include or exclude in the CTC-generated circuit route.
- *Review Route Before Creation*—If selected, you can review and edit the circuit route before the circuit is created.

Step 11 If you want the circuit routed on a protected path, select **Fully Protected Path**. Otherwise, go to Step 12. CTC creates a primary and alternate circuit route (virtual UPSR) based on the path diversity option you select:

- *Nodal Diversity Required*—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse. (For information about PPMN, see the “Path-Protected Mesh Networks” section on page 5-42.)
- *Nodal Diversity Desired*—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.
- *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.

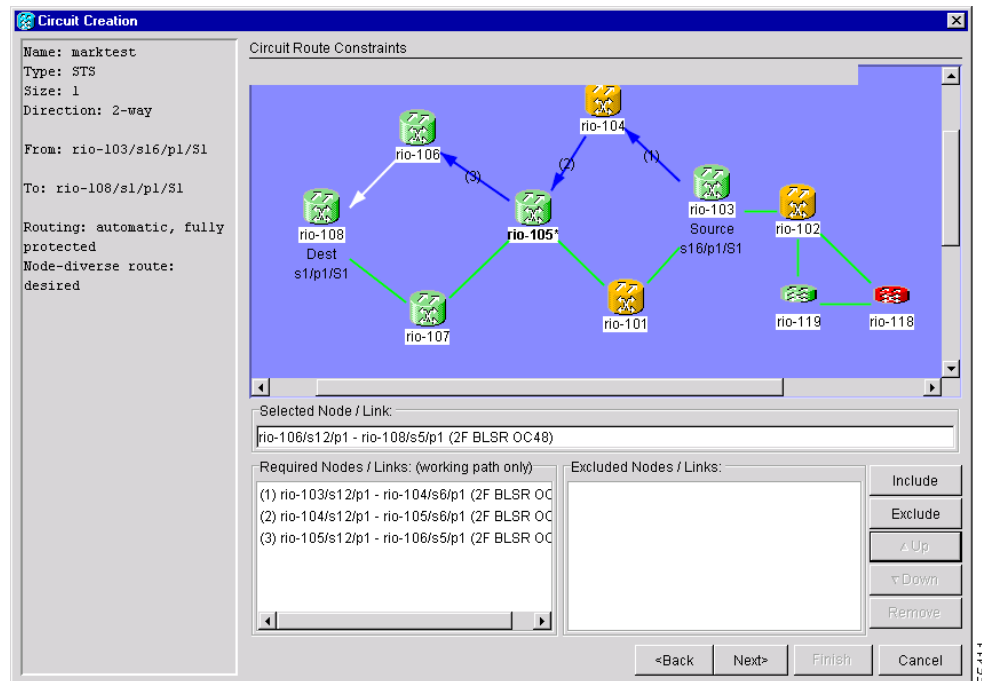
Figure 6-2 Setting circuit routing preferences



Step 12 Click **Finish** or **Next** depending on whether you selected **Using Required Nodes/Spans** and/or **Review Route Before Creation**:

- *Using Required Nodes/Spans*—If selected, click **Next** to display the Circuit Route Constraints panel (Figure 6-3). On the circuit map, click a node or span and click **Include** (to include the node or span in the circuit) or **Exclude** (to exclude the node/span from the circuit). The order in which you select included nodes and spans sets the circuit sequence. Click spans twice to change the circuit direction. After you add the spans and nodes, you can use the Up and Down buttons to change their order, or click **Remove** to remove a node or span. When you are finished, click **Finish** or **Next**, depending on whether you selected **Review Route Before Creation**.

Figure 6-3 Specifying circuit constraints



- *Review Route Before Creation*—If selected, click **Next** to display the route for you to review. To add or delete a circuit span, select a node on the circuit route. Blue arrows show the circuit route. Green arrows indicate spans that you can add. Click a span arrowhead, then click **Include** to include the span or **Remove** to remove the span.

When you click **Finish**, CTC creates the circuit and returns to the Circuits window. If you entered more than 1 in *Number of Circuits* in the Circuit Attributes dialog box in Step 3, the Circuit Source dialog box is displayed so you can create the remaining circuits. If Auto Ranged is checked, CTC automatically creates the number of sequential circuits that you entered in *Number of Circuits*.

Step 13 If you are provisioning circuits before installing the traffic cards and enabling their ports, you must install the cards and enable the ports before circuits will carry traffic. For procedures, see the “Install ONS 15327 Cards” procedure on page 1-17 and the “Enable Ports” procedure on page 3-9.

Procedure: Create a Manually Routed Circuit



Note

If you want to route circuits on protected drops, create the card protection groups before creating circuits. See the “Create Protection Groups for Optical Cards” procedure on page 3-8 if you are using optical cards. Electrical cards are automatically protected.

Step 1

Log into an ONS 15327 and click the **Circuits** tab.



Tip

You can also right-click a source node in network view, select **Provision Circuit To**, and choose the circuit destination node from the menu.

Step 2

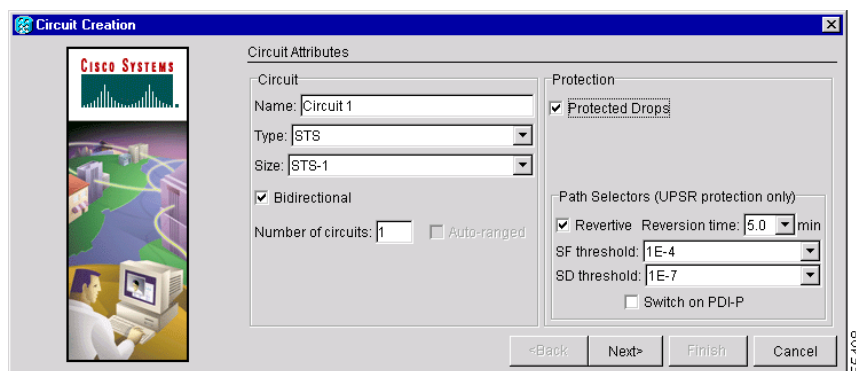
Click **Create**.

Step 3

In the Circuit Creation dialog box (Figure 6-1), complete the following fields:

- *Name*—(optional) Assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces). If you leave the Name field blank, CTC assigns a default name to the circuit.
- *Type*—Select the type of circuit you want to create: STS, VT (VT1.5), or VT tunnel. The circuit type determines the circuit-provisioning options that are displayed. “VT1.5 Cross-Connects” section on page 6-15 and the “VT Tunnels” section on page 6-18 for more information.
- *Size*—Select the circuit size (STS circuits only). The “c” indicates concatenated STSs.
- *Bidirectional*—Check this box to create a two-way circuit; uncheck it to create a one-way circuit (STS and VT circuits only; VT tunnels are bidirectional).
- *Number of circuits*—Type the number of circuits you want to create. CTC returns to the Circuit Source page after you create each circuit until you finish creating the number of circuits specified here.
- *Auto Ranged*—This option is not available with manual circuit routing.
- *Protected Drops*—If this box is checked, CTC only displays protected cards and ports (1:1, 1:N, 1+1 or BLSR protection) as choices for the circuit source and destination.

Figure 6-4 Creating a manually-routed circuit



- Step 4** (UPSR circuits only) Set the UPSR Selector Defaults:
- *Revertive*—Check this box if you want traffic to revert to the working path when the conditions that diverted it to the protect path are repaired. If Revertive is not chosen, traffic remains on the protect path after the switch.
 - *Reversion time*—If Revertive is checked, set the reversion time. This is the amount of time that will elapse before the traffic reverts to the working path. Traffic can revert when conditions causing the switch are cleared (the default reversion time is 5 minutes).
 - *SF threshold*—Set the UPSR path-level signal failure bit error rate (BER) thresholds (STS circuits only).
 - *SD threshold*—Set the UPSR path-level signal degrade BER thresholds (STS circuits only).
 - *Switch on PDI-P*—Check this box if you want traffic to switch when an STS payload defect indicator is received (STS circuits only).
- Step 5** Click **Next**.
- Step 6** In the Circuit Source dialog box, set the circuit source.
- Options include node, slot, port, STS, and VT/DS-1. The options that display depend on the circuit type and circuit properties you selected in Step 3 and the cards installed in the node. For Ethergroups, see the “Ethernet Circuit Configurations” section on page 9-6.
- Click **Use Secondary Source** if you need to create a UPSR bridge/selector circuit entry point in a multivendor UPSR.
- Step 7** Click **Next**.
- Step 8** In the Circuit Destination dialog box, enter the appropriate information for the circuit destination. If the circuit is bidirectional, you can click **Use Secondary Destination** if you need to create a UPSR bridge/selector circuit destination point in a multivendor UPSR. (To add secondary destinations to unidirectional circuits, see “Create a Unidirectional Circuit with Multiple Drops” procedure on page 6-8.)
- Step 9** Click **Next**.
- Step 10** Under Circuit Routing Preferences (Figure 6-2 on page 6-4), de-select **Route Automatically**.
- Step 11** If you want the circuit routed on a protected path, select **Fully Protected Path**. Otherwise, go to Step 12. CTC creates a primary and alternate circuit route (virtual UPSR) based on the nodal diversity option you select:
- *Nodal Diversity Required*—Ensures that the primary and alternate paths within path-protected mesh network (PPMN) portions of the complete circuit path are nodally diverse. (For information about PPMN, see the “Path-Protected Mesh Networks” section on page 5-42.)
 - *Nodal Diversity Desired*—Specifies that node diversity should be attempted, but if node diversity is not possible, CTC creates link diverse paths for the PPMN portion of the complete circuit path.
 - *Link Diversity Only*—Specifies that only link-diverse primary and alternate paths for PPMN portions of the complete circuit path are needed. The paths may be node-diverse, but CTC does not check for node diversity.
- Step 12** Click **Next**. The Route Review and Edit panel is displayed for you to manually route the circuit. The green arrows pointing from the source node to other network nodes indicate spans that are available for routing the circuit.
- Step 13** Set the circuit route:
- a. Click the arrowhead of the span you want the circuit to travel.
 - b. If you want to change the source STS or VT, change it in the Source STS or Source VT fields.

c. Click **Add Span**.

The span is added to the Included Spans list and the span arrow turns blue. To remove a span, select it in the Included Spans list and click **Remove**.

- Step 14** Repeat Step 13 until the circuit is provisioned from the source to the destination node.
- When provisioning a protected circuit, you only need to select one path of BLSR or 1+1 spans from the source to the drop. If you select unprotected spans as part of the path, select two different paths for the unprotected segment of the path.
- Step 15** When the circuit is provisioned, click **Finish**.
- If you entered more than 1 in *Number of Circuits* in the Circuit Attributes dialog box in Step 3, the Circuit Source dialog box is displayed so you can create the remaining circuits.
- Step 16** If you are provisioning circuits before installing the traffic cards and enabling their ports, you must install the cards and enable the ports before circuits will carry traffic. For procedures, see the “Install ONS 15327 Cards” procedure on page 1-17 and the “Enable Ports” procedure on page 3-9.

6.3 Creating Multiple Drops for Unidirectional Circuits

Unidirectional circuits can have multiple drops for use in broadcast circuit schemes. In broadcast scenarios, one source transmits traffic to multiple destinations, but traffic is not returned back to the source.

When you create a unidirectional circuit, the port that does not have its Rx input terminated with a valid input signal (a destination drop port for example) generates a loss of service (LOS) alarm. To mask the alarm, create an alarm profile suppressing the LOS alarm and apply it to the port that does not have its Rx input terminated. See the “Creating and Modifying Alarm Profiles” section on page 10-7 for information.

Procedure: Create a Unidirectional Circuit with Multiple Drops

- Step 1** Use the “Create an Automatically Routed Circuit” procedure on page 6-2 to create a circuit. To make it unidirectional, uncheck the Bidirectional check box on the Circuit Creation dialog box.
- Step 2** After the unidirectional circuit is created, in node or network view select the **Circuits** tab.
- Step 3** Select the unidirectional circuit and click **Edit** (or double-click the circuit).
- Step 4** On the **Drops** tab of the Edit Circuits dialog box, click **Create** or, if Show Detailed Map is selected, right-click a node on the circuit map and select **Add Drop**.
- Step 5** On the Define New Drop dialog box, complete the appropriate fields to define the new circuit drop: *Node, Slot, Port, STS, VT* (if applicable).
- Step 6** Click **OK**.
- Step 7** If you need to create additional drops, repeat Steps 4 – 6. If not, click **Close**.
- Step 8** Verify the new drops on the Edit Circuit map:
- If Show Detailed Map is selected: a “D” enclosed by circles appears on each side of the node graphic.

- If Show Detailed Map is not selected: “Drop #1, Drop #2” appear under the node graphic.

6.4 Creating Monitor Circuits

You can set up secondary circuits to monitor traffic on primary bidirectional circuits. Figure 6-5 shows an example of a monitor circuit. At Node 1, a VT1.5 is dropped from Port 1 of a DS-1 card. To monitor the VT1.5 traffic, test equipment is plugged into Port 2 of the DS-1 card and a monitor circuit to Port 2 is provisioned in CTC. Circuit monitors are one-way. The monitor circuit in Figure 6-5 is used to monitor VT1.5 traffic received by Port 1 of the DS-1 card.



Note

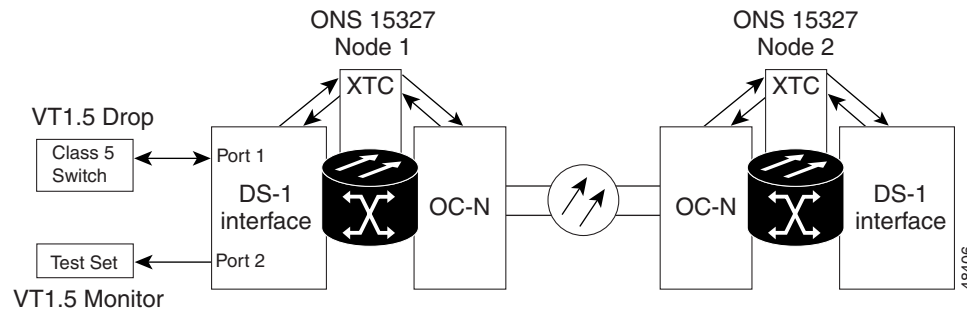
Monitor circuits cannot be used with EtherSwitch circuits.



Note

For unidirectional circuits, create a drop to the port where the test equipment is attached.

Figure 6-5 A VT1.5 monitor circuit received at a DS-1 port



Procedure: Create a Monitor Circuit

- Step 1** Log into CTC.
- Step 2** In node view, select the **Circuits** tab.
- Step 3** Select the bidirectional circuit that you want to monitor. Click **Edit**.
- Step 4** On the Edit Circuit dialog box, click the **Monitors** tab.
- Step 5** The Monitors tab displays ports that you can use to monitor the circuit selected in Step 3.
- Step 6** On the Monitors tab, select a port. The monitor circuit displays traffic coming into the node at the card/port you select. In Figure 6-5, you would select either the DS1 card (to test circuit traffic entering Node 2 on the DS1) or the OC-N card at Node 1 (to test circuit traffic entering Node 1 on the OC-N card).
- Step 7** Click **Create Monitor Circuit**.
- Step 8** On the Circuit Creation dialog box, select the destination node, slot, port, and STS for the monitored circuit. In the Figure 6-5 example, this is Port 2 on the DS-1 card. Click **Next**.
- Step 9** On the Circuit Creation dialog box confirmation, review the monitor circuit information. Click **Finish**.

Step 10 On the Edit Circuit dialog box, click **Close**. The new monitor circuit displays on the Circuits tab.

6.5 Searching for Circuits

CTC provides the ability to search for ONS 15327 circuits based on circuit name. Searches can be conducted at the network, node, and card level. You can search for whole words and include capitalization as a search parameter.

Procedure: Search for ONS 15327 Circuits

- Step 1** Log into CTC.
- Step 2** Switch to the appropriate CTC view:
- Network view to conduct searches at the network level
 - Node view to conduct searches at the network or node level
 - Card view to conduct searches at the card, node, or network level
- Step 3** Click the **Circuits** tab.
- Step 4** If you are in Node or Card view, select the scope for the search in the Scope field.
- Step 5** Click **Search**.
- Step 6** In the Circuit Name Search dialog box, complete the following:
- *Find What*—Enter the text of the circuit name you want to find.
 - *Match Whole Word Only*—If checked, CTC selects circuits only if the entire word matches the text in the Find What field.
 - *Match Case*—If checked, CTC selects circuits only when the capitalization matches the capitalization entered in the Find What field.
 - *Direction*—Select the direction for the search. Searches are conducted up or down from the currently selected circuit.
- Step 7** Click **Find Next**.
- Step 8** Repeat Steps 6 and 7 until you are finished, then click **Cancel**.
-

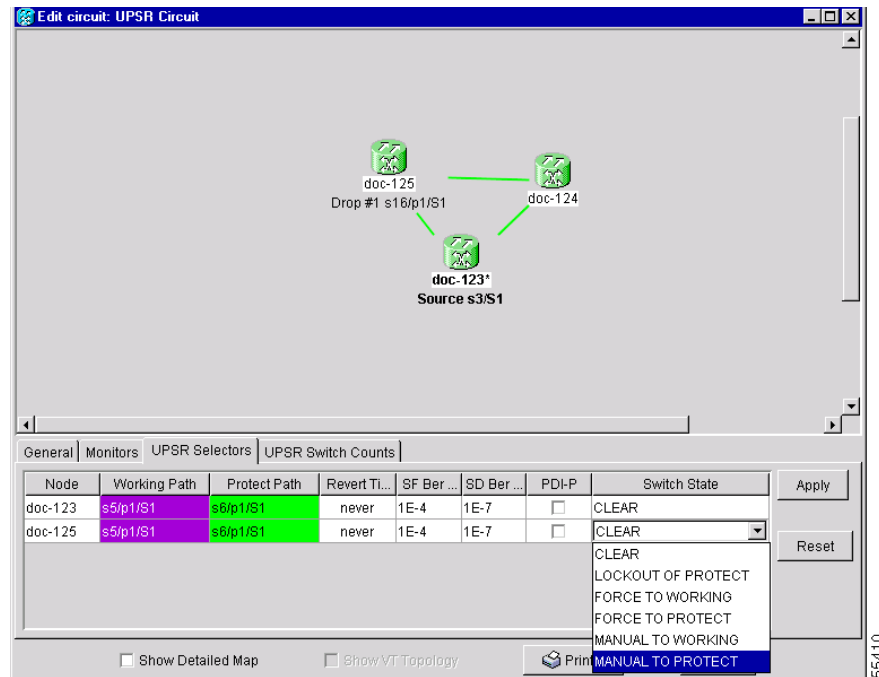
6.6 Editing UPSR Circuits

Use the Edit Circuits window to change UPSR selectors and switch protection paths (Figure 6-6). In this window, you can:

- View the UPSR circuits working and protection paths
- Edit the reversion time
- Edit the Signal Fail/Signal Degrade thresholds

- Change PDI-P settings, perform maintenance switches on the circuit selector, and view switch counts for the selectors
- Display a map of the UPSR circuits to better see circuit flow between nodes

Figure 6-6 Editing UPSR selectors



55410

Procedure: Edit a UPSR Circuit

- Step 1** Log into the source or drop node of the UPSR circuit.
- Step 2** Click the **Circuits** tab.
- Step 3** Click the circuit you want to edit, then click **Edit**.
- Step 4** On the Edit Circuit window, click the **UPSR** tab.
- Step 5** Edit the UPSR selectors:
 - *Reversion Time*—Controls whether traffic reverts to the working path when conditions that diverted it to the protect path are repaired. If you select Never, traffic does not revert. Selecting a time sets the amount of time that will elapse before traffic reverts to the working path.
 - *SF Ber Level*—Sets the UPSR signal failure BER threshold (STS circuits only).
 - *SD Ber Level*—Sets the UPSR signal degrade BER threshold (STS circuits only).
 - *PDI-P*—When checked, traffic switches if an STS payload defect indication is received (STS circuits only).
 - *Switch State*—Switches circuit traffic between the working and protect paths. The color of the Working Path and Protect Path fields indicates the active path. Normally, the Working Path is green and the Protect Path is purple. If the Protect Path is green, working traffic has switched to the Protect Path.

- *CLEAR*—Removes a previously-set switch command.
- *LOCKOUT OF PROTECT*—Prevents traffic from switching to the protect circuit path.
- *FORCE TO WORKING*—Forces traffic to switch to the working circuit path, regardless of whether the path is error free.
- *FORCE TO PROTECT*—Forces traffic to switch to the protect circuit path, regardless of whether the path is error free.
- *MANUAL TO WORKING*—Switches traffic to the working circuit path when the working path is error free.
- *MANUAL TO PROTECT*—Switches traffic to the protect circuit path when the protect path is error free.

**Caution**

The *FORCE* and *LOCKOUT* commands override normal protection switching mechanisms. Applying these commands incorrectly can cause traffic outages.

- Step 6** Click **Apply**, then check that the selector switches as you expect.

6.7 Creating a Path Trace

The SONET J1 Path Trace is a repeated, fixed-length string comprised of 64 consecutive J1 bytes. You can use the string to monitor interruptions or changes to circuit traffic. Table 6-1 shows the ONS 15327 cards that support path trace. DS-1 ports can transmit and receive the J1 field, while the OC-3, and OC-48 can only receive it. Cards not listed in the table do not support the J1 byte.

Table 6-1 ONS 15327 Cards Supporting J1 Path Trace

Card	Receive	Transmit
XTC (DS1)	X	X
OC3 IR 4 1310	X	
OC48 IR/STM16 IR 1310	X	
OC48 LR/STM16 1550	X	

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

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

Table 6-2 shows the general flow for setting up the J1 path trace. To set up a path trace on an ONS 15327 circuit, follow the steps in the “Create a J1 Path Trace” procedure on page 6-13.

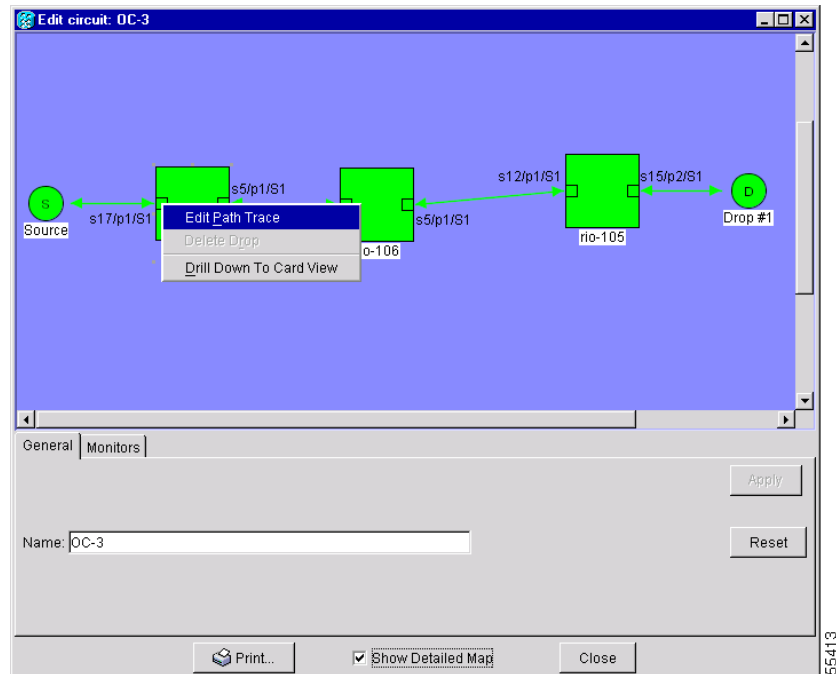
Table 6-2 Path Trace Source and Drop Provisioning

Step	Port	Action	Notes
1	Source	Edit the path-trace transmit string.	If not edited, an empty string is transmitted.
2	Drop	Edit the path-trace transmit string.	If not edited, an empty string is transmitted.
3	Source	Edit the path-trace expected string.	Only if Path Trace mode is set to Manual, and only on DS-1 ports.
4	Drop	Edit the path-trace expected string	Only Path Trace mode is set to Manual, and only on DS-1 ports.
5	Drop	Change Path Trace Mode	Automatic or Manual.
6	Source	Change Path Trace Mode	Automatic or Manual.

Procedure: Create a J1 Path Trace

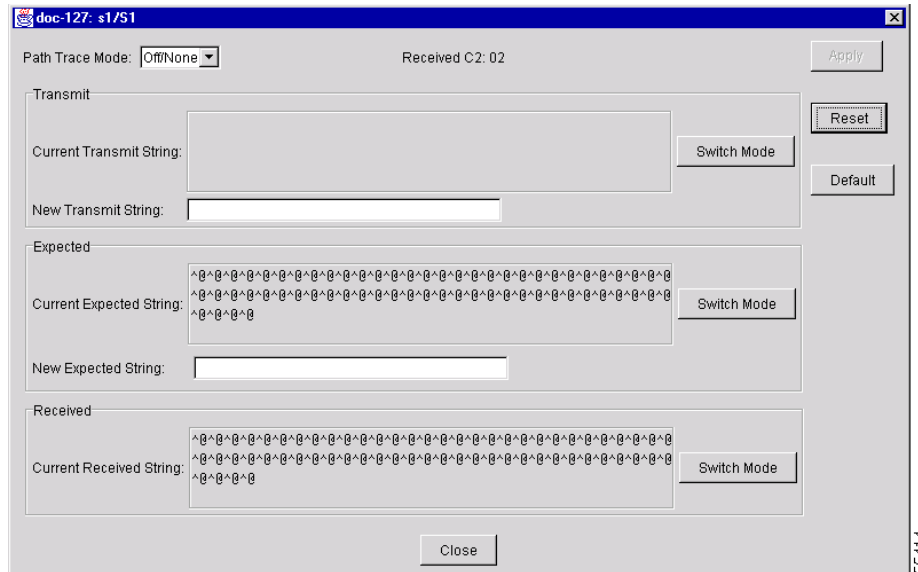
To perform this procedure, you must have an STS circuit using the DS-1 ports on the XTC card at the circuit source and drop ports, or an STS circuit passing through an OC-3 or OC-48 card.

- Step 1** Log into the circuit source node and select the **Circuits** tab.
- Step 2** Select the circuit you want to trace, then click **Edit**.
- Step 3** On the Edit Circuit window, click **Show Detailed Map** at the bottom of the window.
- Step 4** On the detailed circuit map, right-click the source port for the circuit and select **Edit Path Trace** from the shortcut menu. Figure 6-7 shows an example.

Figure 6-7 Selecting the Edit Path Trace option

- Step 5** On the Circuit Path Trace window (Figure 6-8) in the New Transmit String field (this field is not available for optical cards), enter the string that you want the source port to transmit. For example, you could enter the node IP address, node name, circuit name, or another string. If the New Transmit String field is left blank, the J1 transmits an empty string.

Figure 6-8 Setting up a path trace



- Step 6** Click **Apply** but do not close the window.
- Step 7** Return to the Edit Circuit window (Figure 6-7).
- Step 8** On the circuit map, right-click the drop port for the circuit and select **Edit Path Trace** from the shortcut menu.
- Step 9** On the Circuit Path Trace window (Figure 6-8) in the New Transmit String field, enter the string that you want the drop port to transmit. If the field is left blank, the J1 transmits an empty string.
- Step 10** If you will set Path Trace Mode to Manual in Step 11, enter the string that the drop port should expect to receive in the New Expected String field. This string must match the New Transmit String entered for the source port in Step 5. (When you click **Apply** in Step 12, this string becomes the Current Expected String.)
- Step 11** In the Path Trace Mode field, select one of the following options:
- *Auto*—Assumes the first string received from the source port is the baseline string. An alarm is raised when a string that differs from the baseline is received.
 - *Manual*—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.
- Step 12** Click **Apply** and then click **Close**.
- Step 13** Display the Circuit Path Trace window for the source port from Step 5.
- Step 14** If you will set the Path Trace Mode to Manual in Step 15, enter the string the source port should expect to receive in the New Expected String field. This string must match the New Transmit String entered for the source port in Step 9.
- Step 15** In the Path Trace Mode field, select one of the following options:

- *Auto*—Assumes that the first string received from the drop port is the baseline string. An alarm is raised when a string that differs from the baseline is received.
- *Manual*—Uses the Current Expected String field as the baseline string. An alarm is raised when a string that differs from the Current Expected String is received.

Step 16 Click **Apply** and click **Close**.

After you set up the path trace, the received string is displayed in the Received box on the path trace setup window (Figure 6-8). Click **Switch Mode** to toggle between ASCII and hexadecimal display. Click the **Reset** button to reread values from the port. Click **Default** to return to the path trace default settings (Path Trace Mode is set to Off and the New Transmit and New Expected Strings are null).

6.8 Cross-Connect Card Capacities

The ONS 15327 XTC cards perform port-to-port time-division multiplexing (TDM) at the STS-1 and VT 1.5 levels.

XTC cards have the capacity to terminate 288 STSs, or 144 STS cross-connections (each STS cross-connection uses two STS ports on the cross-connect card STS matrix).

6.8.1 VT1.5 Cross-Connects

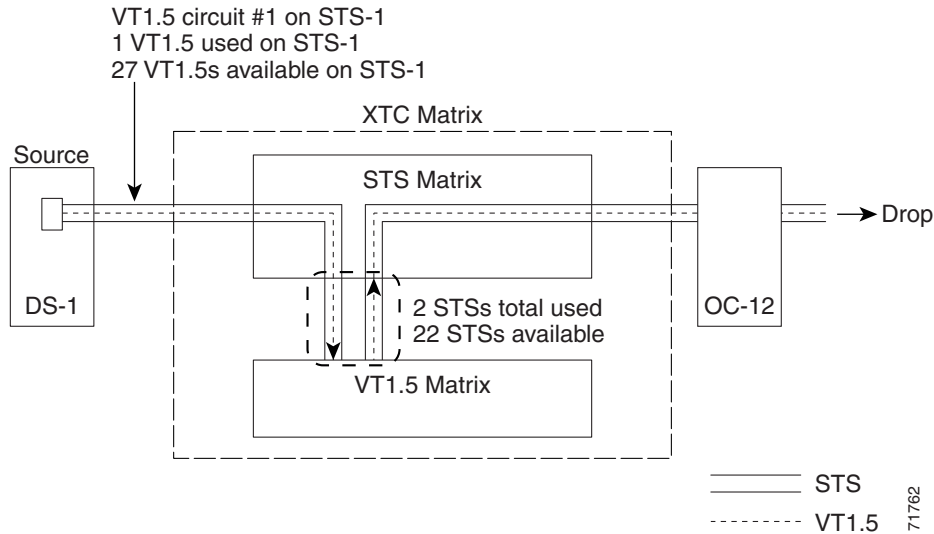
The XTC card can map up to 24 STSs for VT1.5 traffic. Because one STS can carry 28 VT1.5s, the XTC card can terminate up to 672 VT1.5s, or 336 VT1.5 cross-connects. However, to terminate 336 VT1.5 cross-connects:

- 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 VT1.5 cross-connect capacity will be reached after you create 12 VT1.5 circuits.
- ONS 15327s must be in a bidirectional line switched ring (BLSR). Source and drop nodes in UPSR or 1+1 (linear) protection have capacity for only 224 VT1.5 cross-connects because an additional STS is used for the protect path.

Figure 6-9 shows the logical flow of a VT1.5 circuit through the XTC card STS and VT matrices at a BLSR node. The circuit source is a DS-1 port using STS-1. After the circuit is created:

- Two of the 24 XTC STSs available for VT1.5 traffic are used (one STS for VT1.5 input into the VT matrix; one STS for VT1.5 output).
- 22 STSs are available for VT1.5 circuits.
- The STS-1 from the DS-1 port has capacity for 27 more VT1.5 circuits.

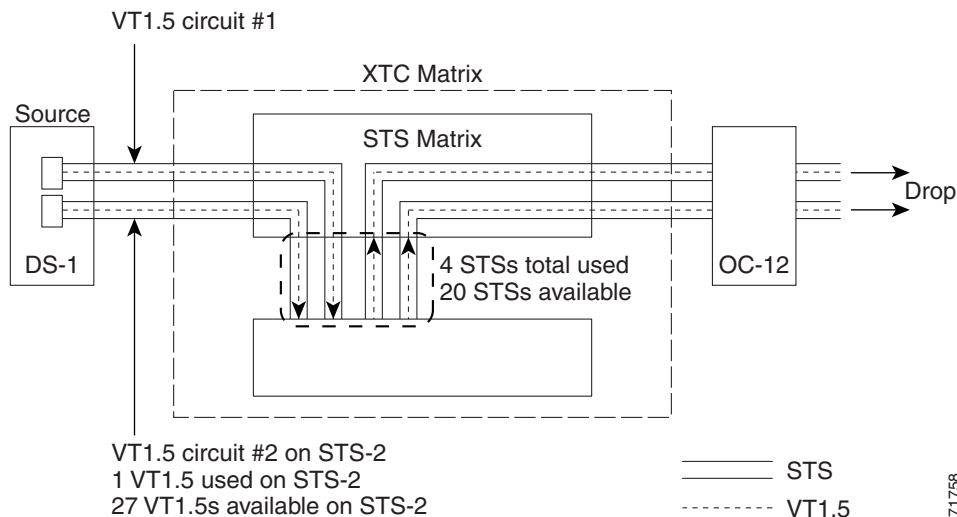
Figure 6-9 Example #1: A VT1.5 circuit in a BLSR



In Figure 6-10, a second VT1.5 circuit is created from the DS-1 port. In this example, the circuit is assigned to STS-2:

- Two more of the 24 STSs available for VT1.5 traffic are used.
- 20 STSs are available for VT1.5 circuits.
- STS-2 can carry 27 additional VT1.5 circuits.

Figure 6-10 Example #2: Two VT1.5 circuits in a BLSR



If you create VT1.5 circuits on nodes in UPSR or 1+1 protection, an additional STS is used for the protect path at the source and drop nodes. Figure 6-11 shows a VT1.5 circuit at a UPSR source node. When the circuit is completed:

- Three of the 24 STSs available for VT1.5 mapping on the XTC card are used (one input and two outputs, one output for the working path and one output for the protect path).
- 21 STSs are available for VT1.5 circuits.

Figure 6-11 Example #3: VT1.5 circuit in a UPSR or 1+1 protection scheme

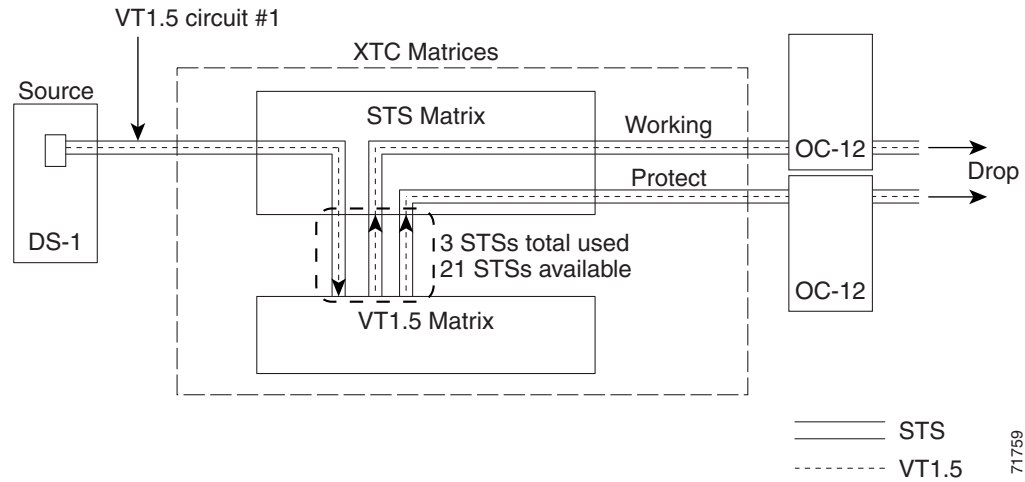
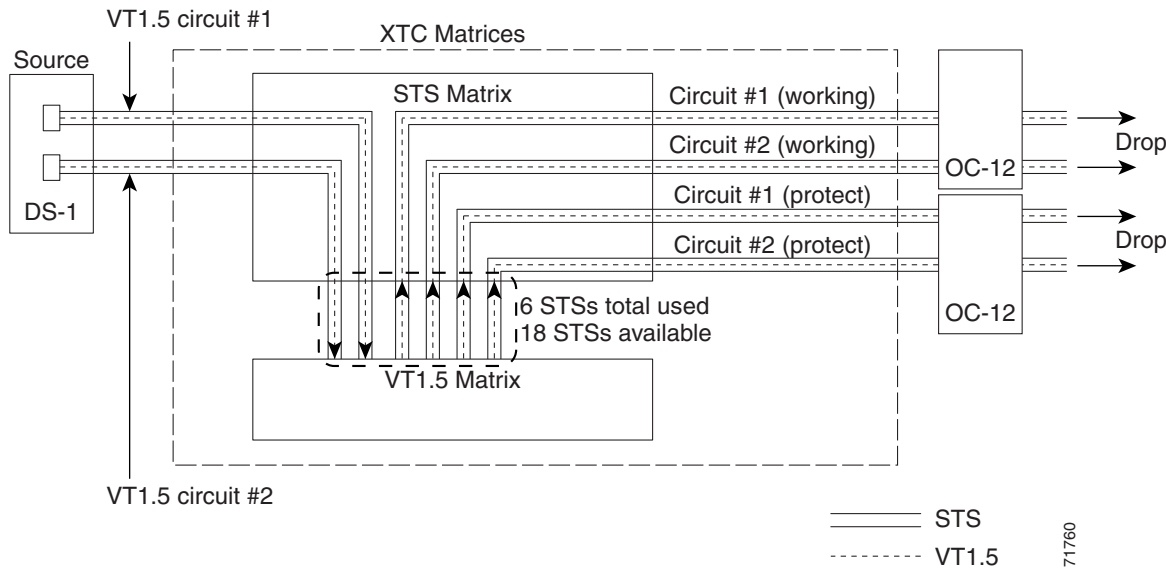


Figure 6-12 shows a second VT1.5 circuit that was created using STS-2. When the second VT1.5 circuit is created:

- Three more VT1.5-mapped STSs are used.
- 18 STSs are available for VT1.5 circuits.

Figure 6-12 Example #4: Two VT1.5 circuits in UPSR or 1+1 protection scheme



Unless you create VT tunnels (see the “VT Tunnels” section on page 6-18), VT1.5 circuits use STSs on the XTC VT matrix at each node through which the circuit passes.

- Two STSs are used at each node in the Figure 6-9 example, and three STSs are used at each node in the Figure 6-11 example.
- In the Figure 6-10 example, three STSs are used at the source and drop nodes and four STSs are used at pass-through nodes. In Figure 6-12, six STSs are used at the source and drop nodes and four STSs at the pass-through nodes.

6.8.2 VT Tunnels

To maximize VT matrix resources, you can tunnel VT1.5 circuits through ONS 15327 pass-through nodes (nodes that are not a circuit source or drop). VT1.5 tunnels provide two benefits:

- They allow you to route VT1.5 circuits through ONS 15454s that have XC cards. (VT1.5 circuits require XCVT or XC10G cards at circuit source and drop nodes.)
- When tunneled through nodes, VT1.5 tunnels do not use VT matrix capacity, thereby freeing the VT matrix resources for other VT1.5 circuits.

Figure 6-13 shows a VT tunnel through the XTC matrices. No VT1.5-mapped STSs are used by the tunnel, which can carry 28 VT1.5s. However, the tunnel does use two STS matrix ports on each node through which it passes.

Figure 6-13 A VT1.5 tunnel

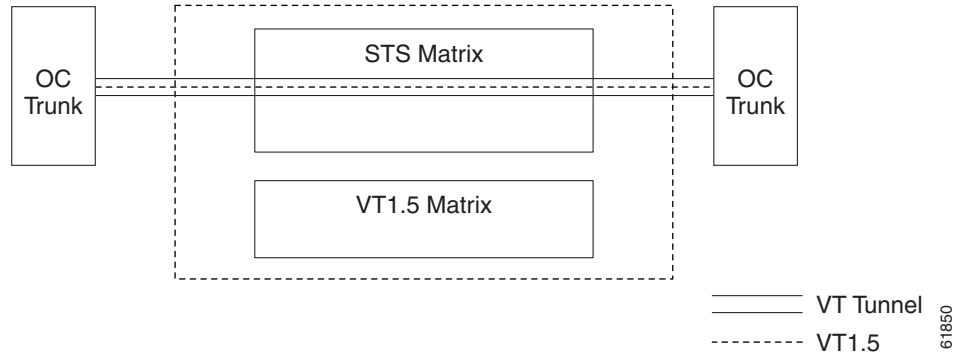


Figure 6-14 shows a six-node ONS 15327 ring with two VT tunnels. One tunnel carries VT1.5 circuits from Node 1 to Node 3. The second tunnel carries VT1.5 circuits from Node 1 to Node 4. Table 6-3 shows the VT1.5-mapped STS usage at each node in a ring based on protection scheme and use of VT tunnels. In the Figure 6-14 example, the circuit travels west through Nodes 2, 3, and 4. Subsequently, VT-mapped STS usage at these nodes is greater than at Nodes 5 and 6.

Figure 6-14 A six-node ring with two VT1.5 tunnels

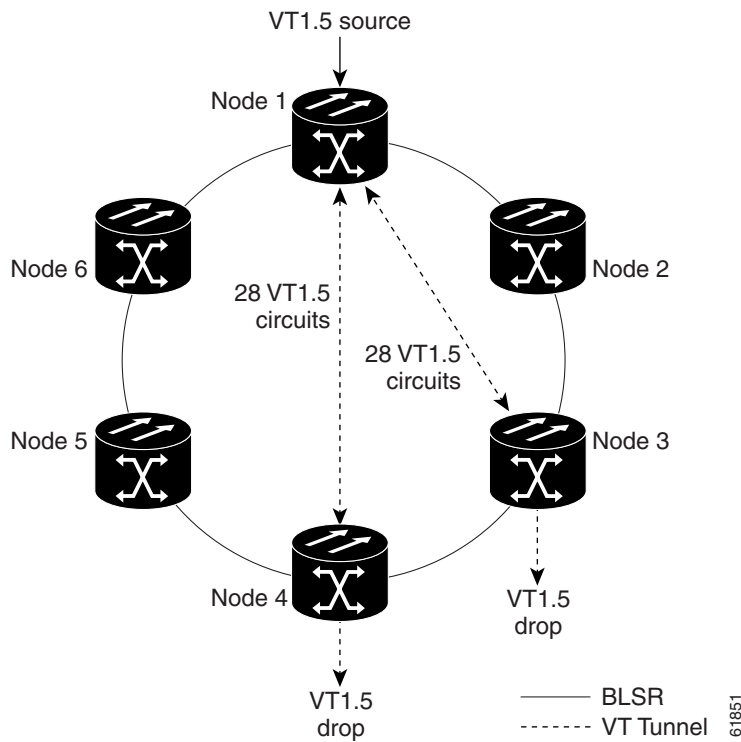


Table 6-3 VT1.5-Mapped STS Use in Figure 6-6

Node	VT Tunnel (BLSR)	VT Tunnel (UPSR, 1+1)	No VT Tunnel (BLSR)	No VT Tunnel (UPSR)	No VT Tunnel (1+1)
1	4	6	4	6	6
2	0	0	4	4	8
3	2	3	4	5	7
4	2	3	2	5	3
5	0	0	0	4	0
6	0	0	0	4	0

When planning VT1.5 circuits, weigh the benefits of using tunnels with the need to maximize STS capacity. For example, a VT1.5 tunnel between Node 1 and Node 4 passing (transparently) through Nodes 2 and Node 3 is advantageous if a full STS is used for Node 1 – Node 4 VT1.5 traffic (that is, the number of VT1.5 circuits between these nodes is close to 28). A VT tunnel is required if:

- Node 2 or Node 3 are ONS 15454s with XC cards, or
- All VT1.5-mappable STSs at Node 2 and Node 3 are in use.

However, if the Node 1 – Node 4 tunnel will carry few VT1.5 circuits, creating a regular VT1.5 circuit between Nodes 1, 2, 3, and 4 might maximize STS capacity.

When you create a VT1.5 circuit, CTC determines whether a tunnel already exists between source and drop nodes. If a tunnel exists, CTC checks the tunnel capacity. If the capacity is sufficient, CTC routes the circuit on the existing tunnel. If a tunnel does not exist, or if an existing tunnel does not have sufficient capacity, CTC displays a dialog box asking whether you want to create a tunnel. Before you create the tunnel, review the existing tunnel availability, keeping in mind future bandwidth needs. In some cases, you may want to manually route a circuit rather than create a new tunnel.

6.9 Creating DCC Tunnels

SONET provides four data communications channels (DCCs) for network element operations, administration, maintenance, and provisioning: one on the SONET Section layer and three on the SONET Line layer. The ONS 15327 uses the Section DCC (SDCC) for ONS 15327 management and provisioning. You can use the Line DCCs (LDCCs) and the SDCC (when the SDCC is not used for ONS 15327 DCC terminations) to tunnel third-party SONET equipment across ONS 15327 networks. To create a DCC tunnel, you connect the tunnel end points from one ONS 15327 optical port to another. DCC traffic is forwarded transparently across the ONS 15327 network.

A DCC tunnel is a series of connection points that map third-party equipment SDCCs to ONS 15327 LDCCs. DCC tunnel end-points are defined by Slot, Port, and DCC type, where DCC can be either the SDCC, Tunnel 1, Tunnel 2, or Tunnel 3 (LDCCs). You can link an SDCC to an LDCC (Tunnel 1, Tunnel 2, or Tunnel 3), and an LDCC to an SDCC. You can also link LDCCs to LDCCs and link SDCCs to SDCCs.

The ONS 15327 OC-3 card supports tunnels on all four ports. Each ONS 15327 and 15454 can support up to 32 DCC tunnels. The maximum number of optical ports available on an ONS 15327 is 16 (four-port OC3 cards installed in all high-speed slots). Each port can support four different DCC tunnels (one section and three line). This allows 64 (4 x 16) tunnel terminations. Because each tunnel must have two terminations, the ONS 15327 can support a maximum of 32 DCC tunnel connections.

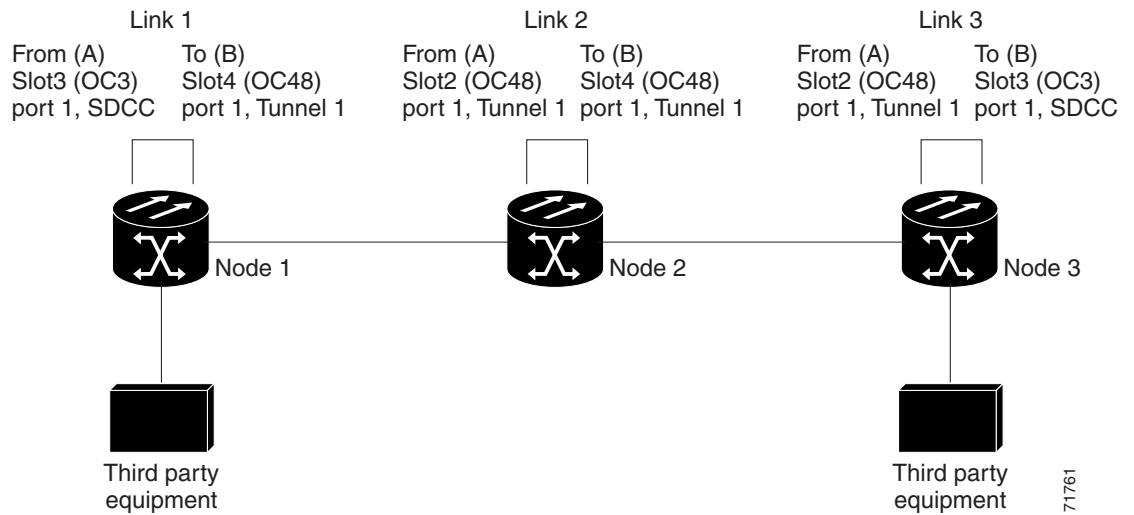
Table 6-4 shows the DCC tunnels that you can create.

Table 6-4 DCC Tunnels

DCC	SONET Layer	SONET Bytes	OC-3 (all ports)	OC-12, OC-48
SDCC	Section	D1 - D3	Yes	Yes
Tunnel 1	Line	D4 - D6	Yes	Yes
Tunnel 2	Line	D7 - D9	Yes	Yes
Tunnel 3	Line	D10 - D12	Yes	Yes

Figure 6-15 shows a DCC tunnel example. Third-party equipment is connected to OC-3 cards at Node 1/Slot 3/Port 1 and Node 3/Slot 3/Port 1. Each ONS 15327 node is connected by OC-48 trunk cards. In the example, three tunnel connections are created, one at Node 1 (OC-3 to OC-48), one at Node 2 (OC-48 to OC-48), and one at Node 3 (OC-48 to OC-3).

Figure 6-15 A DCC tunnel



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 SDCC terminations.
- An SDCC that is terminated cannot be used as a DCC tunnel end-point.
- An SDCC that is used as a DCC tunnel end-point cannot be terminated.
- All DCC tunnel connections are bidirectional.

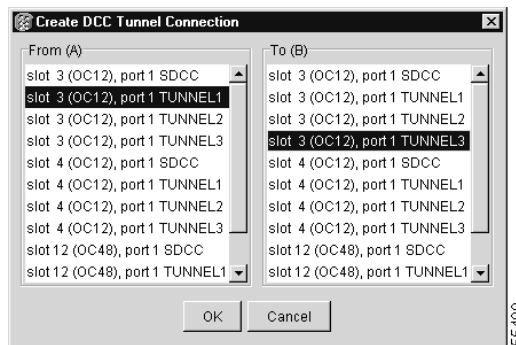
Procedure: Provision a DCC Tunnel

- Step 1** Log into an ONS 15327 that is connected to the non-ONS 15327 network.
- Step 2** Click the **Provisioning > Sonet DCC** tabs.
- Step 3** Beneath the DCC Tunnel Connections area (bottom right of the screen), click **Create**.
- Step 4** In the Create DCC Tunnel Connection dialog box (Figure 6-16), select the tunnel end points from the *From (A)* and *To (B)* lists.



Note You cannot use the SDCC listed under SDCC Terminations (left side of the window) for tunnel connections. These are used for ONS 15327 optical connections.

Figure 6-16 Selecting DCC tunnel end points



- Step 5** Click **OK**.
- Step 6** Put the ports hosting the DCC tunnel in service:
- Double-click the card hosting the DCC in the shelf graphic or right-click the card on the shelf graphic and select **Open**.
 - Click the **Provisioning > Line** tabs.
 - Under Status, select **In Service**.
 - Click **Apply**.

DCC provisioning is now complete for one node. Repeat these steps for all slots/ports that are part of the DCC tunnel, including any intermediate nodes that will pass traffic from third-party equipment. The procedure is confirmed when the third-party network elements successfully communicate over the newly-established DCC tunnel.



Card Provisioning

This chapter provides Cisco ONS 15327 procedures for:

- Changing the default transmission parameters for electrical (DS-N) and optical (OC-N) cards
- Setting performance monitoring (PM) thresholds, including intermediate path performance monitoring
- Provisioning the Alarm Interface Controller card



Note

Ethernet card provisioning is described in Chapter 9, “Ethernet Operation.”

Because much of the electrical and optical card provisioning involves PM thresholds, see Chapter 8, “Performance Monitoring,” for definitions and general information about ONS 15327 performance monitoring parameters. In addition, refer to the Telcordia GR-1230-CORE, GR-820-CORE, and GR-253-CORE documents. The default thresholds delivered with ONS 15327 cards are based on specifications contained in those documents.



Note

For information about creating protection groups, see the “Creating Protection Groups” section on page 3-7. For circuit creation procedures, see Chapter 6, “Circuits and Tunnels.”

7.1 Performance Monitoring Thresholds

ONS 15327 card default thresholds are based on GR-253-CORE and GR-820-CORE. If you change their settings, the following rules apply:

- The minimum threshold that you can set is 1.
- If you set a threshold to 0, no threshold crossing alert (TCA) is issued.
- You can set thresholds to any DS-N or OC-N maximum. However, CTC does not perform range checking. Setting a threshold to a value greater than what is logically possible is the same as setting the threshold to zero. No TCA will be issued.

7.2 Provisioning Electrical Cards

The ONS 15327 electrical cards (DS-1 ports on the XTC-14 and XTC-28-3 and DS-3 ports on the XTC-28-3) are pre-provisioned with settings that you can modify to manage transmission quality. When you open an XTC card in CTC and select the Provisioning tab, the following subtabs are commonly displayed:

- *Line*—Sets line setup parameters, such as line coding and line length. This is also where you put ports in and out of service.
- *Line Threshold*—Sets the line-level PM thresholds.
- *Electric Path Threshold*—Sets the path-level PM thresholds for DS-1 traffic.
- STS 1 Path Threshold—Sets the path-level PM thresholds for DS-3 traffic.
- *SONET Path Threshold*—Sets the path-level PM thresholds for (STS/VT1.5) traffic.
- *Alarming*—Sets alarm profiles for individual ports and suppresses alarms. See Chapter 10, “Alarm Monitoring and Management” for information about alarm profiles and alarm suppression.

Table 7-1 provides an overview of DS-1 and DS-3 parameters (an X means the item is available for the card).

Table 7-1 DS-N Card Provisioning Overview

Subtab	Provisioning Item	DS1	DS3
Line	Port #	X	X
	Port Name	X	X
	Line Type	X	
	Detected Line Type		
	Line Coding	X	
	Line Length	X	X
	Status	X	X
Line Threshold	Port	X	X
	CV	X	X
	ES	X	X
	SES	X	X
	LOSS	X	X
Electric Path Threshold	Port	X	
	CV	X	
	ES	X	
	SES	X	
	SAS	X	
	AIS	X	
	UAS	X	

Table 7-1 DS-N Card Provisioning Overview (continued)

Subtab	Provisioning Item	DS1	DS3
STS 1 Path Threshold	Port		X
	CV		X
	ES		X
	FC		X
	SES		X
	UAS		X
SONET Path Threshold (Sts Term)	Port	X	
	CV	X	
	ES	X	
	FC	X	
	SES	X	
	UAS	X	
SONET Path Threshold (Vt Term)	Port	X	
	ES	X	
	SES	X	
	CV	X	
	UAS	X	
Alarming	Port	X	X
	Profile	X	X
	Suppress Alarms	X	X

7.2.1 Mapping Card Provisioning and Performance Monitoring

The card provisioning items in Table 7-1 map to the performance monitoring (PM) parameters displayed when you click the **Performance** tab. Table 7-2 shows the relationship between the card provisioning items and the PM parameters.

Table 7-2 Mapping Card Provisioning and Performance Monitoring

Tab Name	Provisioning Item	PM Parameter
Line Threshold	CV	CV-L
Line Threshold	ES	ES-L
Line Threshold	SES	SES-L
Line Threshold	LOSS	LOSS-L
Electric Path Threshold	CV	DS1 Rx CV-P/DS1 Tx CV-P
Electric Path Threshold	ES	DS1 Rx ES-P/DS1 Tx ES-P
Electric Path Threshold	SES	DS1 Rx SES-P/DS1 Tx SES-P
Electric Path Threshold	SAS	DS1 Rx SAS-P/DS1 Tx SAS-P

Table 7-2 Mapping Card Provisioning and Performance Monitoring (continued)

Tab Name	Provisioning Item	PM Parameter
Electric Path Threshold	AIS	DS1 Rx AISS-P/DS1 Tx AISS-P
Electric Path Threshold	UAS	DS1 Rx UAS-P/DS1 Tx UAS-P
Sonet Path Threshold	CV (VT Term)	CV-V
Sonet Path Threshold	ES (VT Term)	ES-V
Sonet Path Threshold	SES (VT Term)	SES-V
Sonet Path Threshold	UAS (VT Term)	UAS-V
Sonet Path Threshold	CV (Sts Term)	CV-P
Sonet Path Threshold	ES (Sts Term)	ES-P
Sonet Path Threshold	FC (Sts Term)	FC-P
Sonet Path Threshold	SES (Sts Term)	SES-P
Sonet Path Threshold	UAS (Sts Term)	UAS-P

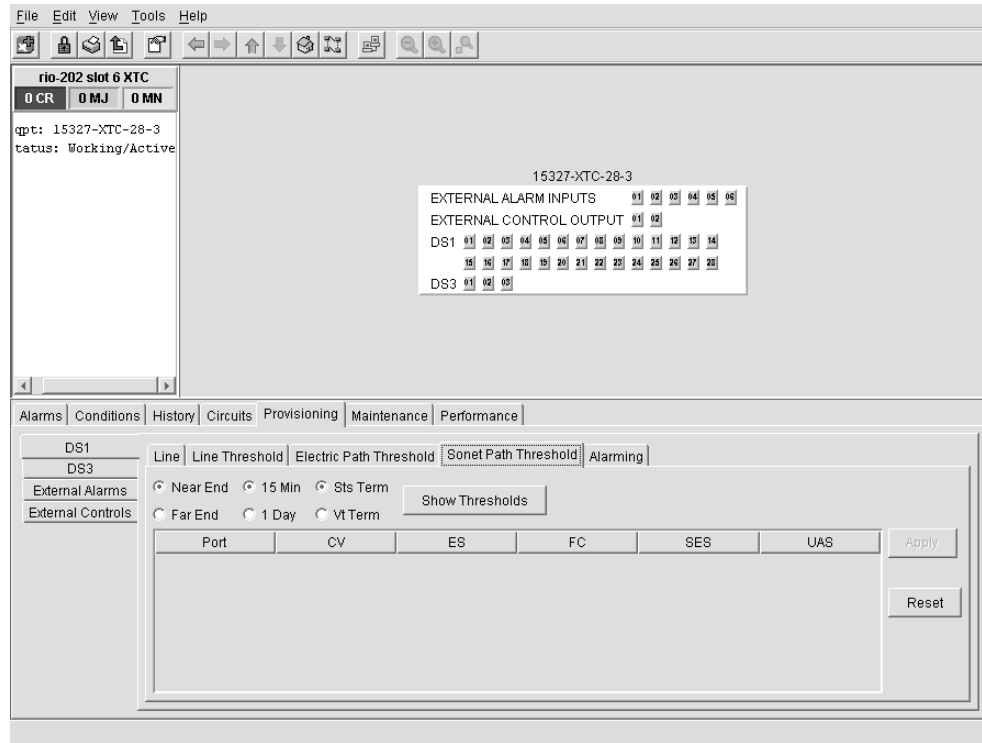
7.2.2 DS-1 Card Parameters

The ONS 15327XTC cards provide 14 (XTC-14) or 28 (XTC-28-3) DS-1 ports. Each port operates at 1.544 Mbps. Default thresholds are based on recommendations in GR-820-CORE, Section 4.0.

Procedure: Modify Line and Threshold Settings for the DS-1 Card

-
- Step 1** Display the XTC card in CTC card view.
 - Step 2** Click the **Provisioning** tab (Figure 7-1).

Figure 7-1 Provisioning line parameters on the DS1-14 card



71783

- Step 3** Depending on the setting you need to modify, click the **Line**, **Line Threshold**, **Electric Path Threshold**, **Sonet Path Threshold**, or **Alarming** subtab.



Note See Chapter 10, “Alarm Monitoring and Management” for information about the Alarm Behavior tab.

- Step 4** Modify the settings shown in Table 7-3 on page 7-6. For drop-down lists, select an item from the list. For numerics, double-click the field and type the new number.

Table 7-3 DS-1 Card Parameters

Subtab	Parameter	Description	Options
Line	Port #	Port number	<ul style="list-style-type: none"> 1-14 (XTC-14) 1 - 28 (XTC-28-3)
	Port	Port name	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	Line Type	Defines the line framing type	<ul style="list-style-type: none"> D4 (default) ESF - Extended Super Frame Unframed
	Line Coding	Defines the DS-1 transmission coding type	<ul style="list-style-type: none"> AMI - Alternate Mark Inversion (default) B8ZS - Bipolar 8 Zero Substitution
	Line Length	Defines the distance (in feet) from backplane connection to the next termination point	<ul style="list-style-type: none"> 0 - 131 (default) 132 - 262 263 - 393 394 - 524 525 - 655
	Status	Places port in or out of service	<ul style="list-style-type: none"> Out of Service (default) In Service
Line Threshold	CV	Coding violations	Numeric. Defaults: <ul style="list-style-type: none"> 13340 (15 min) 133400 (1 day)
	ES	Errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> 65 (15 min) 648 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> 10 (15 minutes) 100 (1 day)
	Loss	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Defaults: <ul style="list-style-type: none"> 10 (15 minutes) 10 (1 day)

Table 7-3 DS-1 Card Parameters (continued)

Subtab	Parameter	Description	Options
Electric Path Threshold	CV	Coding violations	Numeric. Defaults: <ul style="list-style-type: none"> • 13296 (15 minutes) • 132960 (1 day)
	ES	Errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 65 (15 minutes) • 648 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 10 (15 minutes) • 100 (1 day)
	SAS	Severely errored frame/alarm indication signal	Numeric. Defaults: <ul style="list-style-type: none"> • 2 (15 minutes) • 17 (1 day)
	AIS	Alarm indication signal	Numeric. Defaults: <ul style="list-style-type: none"> • 10 (15 minutes) • 10 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 10 (15 minutes) • 10 (1 day)
SONET Path Threshold (Sts Term)	Port	DS-1 port number	1 - 28
	CV	Coding violations	Numeric. Defaults: <ul style="list-style-type: none"> • 15 (15 minutes) • 125 (1 day)
	ES	Errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 12 (15 minutes) • 100 (1 day)
	FC	Failure count	Numeric. Defaults (VT termination): <ul style="list-style-type: none"> • 10 (15 minutes) • 10 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 3 (15 minutes) • 7 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 10 (15 minutes) • 10 (1 day)

Table 7-3 DS-1 Card Parameters (continued)

Subtab	Parameter	Description	Options
SONET Path Threshold (VT Term)	ES	Errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 12 (15 minutes) • 100 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 3 (15 minutes) • 7 (1 day)
	CV	Coding violations	Numeric. Defaults: <ul style="list-style-type: none"> • 15 (15 minutes) • 125 (1 day)
	UAS	Unavailable seconds	Numeric. Defaults: <ul style="list-style-type: none"> • 10 (15 minutes) • 10 (1 day)
Alarming	Port	DS-1 port number	1 - 28
	Profile	Sets the alarm profile for the port	<ul style="list-style-type: none"> • Default • Inherited • Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port	<ul style="list-style-type: none"> • Unselected (default) • Selected

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.2.3 DS-3 Card Parameters

The ONS 15327 XTC-28-3 card provides 3 DS-3 ports. Each port operates at 44.736 Mbps. Default thresholds are based on recommendations in GR-820-CORE, Section 5.0.

Procedure: Modify Line and Threshold Settings for the DS-3 Card

Step 1 Display the XTC card in CTC card view.

Step 2 Click the **Provisioning** tab.

Step 3 Depending on the setting you need to modify, click the **Line**, **Line Threshold**, **STS 1Path Threshold**, or **Alarming** subtab.



Note See Chapter 10, “Alarm Monitoring and Management” for information about the Alarm Behavior tab.

Step 4 Modify the settings shown in Table 7-4. For drop-down lists, select an item from the list. For numerics, double-click the field and type the new number.

Table 7-4 DS-3 Card Parameters

Subtab	Parameter	Description	Options
Line	Port #	Port number	1 - 3
	Port Name	Name of the port	To enter a name for the port, click the cell and type the name. To change a name, double-click the cell, then edit the text.
	Line Length	Defines the distance (in feet) from backplane connection to the next termination point	<ul style="list-style-type: none"> 0 - 225 (default) 226 - 450
	Status	Places port in or out of service	<ul style="list-style-type: none"> Out of Service (default) In Service
Line Threshold	Port	DS-3 port number	1 - 3
	CV	Coding violations	Numeric. Defaults: <ul style="list-style-type: none"> 387 (15 minutes) 3865 (1 day)
	ES	Errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> 25 (15 minutes) 250 (1 day)
	SES	Severely errored seconds	Numeric. Defaults: <ul style="list-style-type: none"> 4 (15 minutes) 40 (1 day)
	Loss	Loss of signal; number of one-second intervals containing one or more LOS defects	Numeric. Defaults: <ul style="list-style-type: none"> 10 (15 minutes) 10 (1 day)

Table 7-4 DS-3 Card Parameters (continued)

Subtab	Parameter	Description	Options
STS 1 Path Threshold	Port	DS-3 port and STS used by that port	<ul style="list-style-type: none"> DS-3 ports 1 - 3 Any available STS
	CV	Coding violations	Numeric. Defaults (Near End, STS termination): <ul style="list-style-type: none"> 15 (15 minutes) 125 (1 day)
	ES	Errored seconds	Numeric. Defaults (Near End, STS termination): <ul style="list-style-type: none"> 12 (15 minutes) 100 (1 day)
	FC	Failure count	Numeric. Defaults (Near End, STS termination): <ul style="list-style-type: none"> 10 (15 minutes) 10 (1 day)
	SES	Severely errored seconds	Numeric. Defaults (Near End, STS termination): <ul style="list-style-type: none"> 3 (15 minutes) 7 (1 day)
	UAS	Unavailable seconds	Numeric. Default (Near End, STS termination): <ul style="list-style-type: none"> 10 (15 minutes) 10 (1 day)
Alarming	Port	Port number	1 - 3
	Profile	Sets the alarm profile for the port.	<ul style="list-style-type: none"> Default Inherited Custom profiles (if any)
	Suppress Alarms	Suppresses alarm display for the port.	<ul style="list-style-type: none"> Unselected (default) Selected

Step 5 Click **Apply**.

Step 6 Repeat Steps 4 – 5 for each subtab that has parameters you want to provision.

7.3 Provisioning Optical Cards

This section explains how to modify transmission quality by provisioning line and threshold settings for OC-N cards.

7.3.1 Modifying Transmission Quality

The OC-3, OC-12 and OC-48 cards are pre-provisioned with settings that you can modify to manage transmission quality. Depending on the optical card, you can specify thresholds for near and far end nodes at the Line, Section, and Path levels for 15-minute and one day intervals.

Procedure: Provision Line Transmission Settings for OC-N Cards

- Step 1** Display the OC-N card in CTC card view.
- Step 2** Click the **Provisioning > Line** tabs.
- Step 3** Modify the settings shown in Table 7-5.

Table 7-5 OC-N Card Line Settings on the Provisioning > Line Tab

Heading	Description	Options
Port #	Port number	<ul style="list-style-type: none"> 1 (OC-12, OC-48) 1-4 (OC-3)
Port Name	Name of the OC-N port	32 alpha-numeric characters
SF BER Level	Sets the signal fail bit error rate	<ul style="list-style-type: none"> 1E-3 1E-4 (default) 1E-5
SD BER Level	Sets the signal degrade bit error rate	<ul style="list-style-type: none"> 1E-5 1E-6 1E-7 (default) 1E-8 1E-9
Provides Synch	If checked, the card is provisioned as a network element timing reference on the Provisioning > Timing tabs	Read-only <ul style="list-style-type: none"> Yes (checked) No (unchecked)
Enable Synch Messages	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source	<ul style="list-style-type: none"> Yes (checked, default) No (unchecked)
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte	<ul style="list-style-type: none"> Yes (checked) No (unchecked; default)

Table 7-5 OC-N Card Line Settings on the Provisioning > Line Tab (continued)

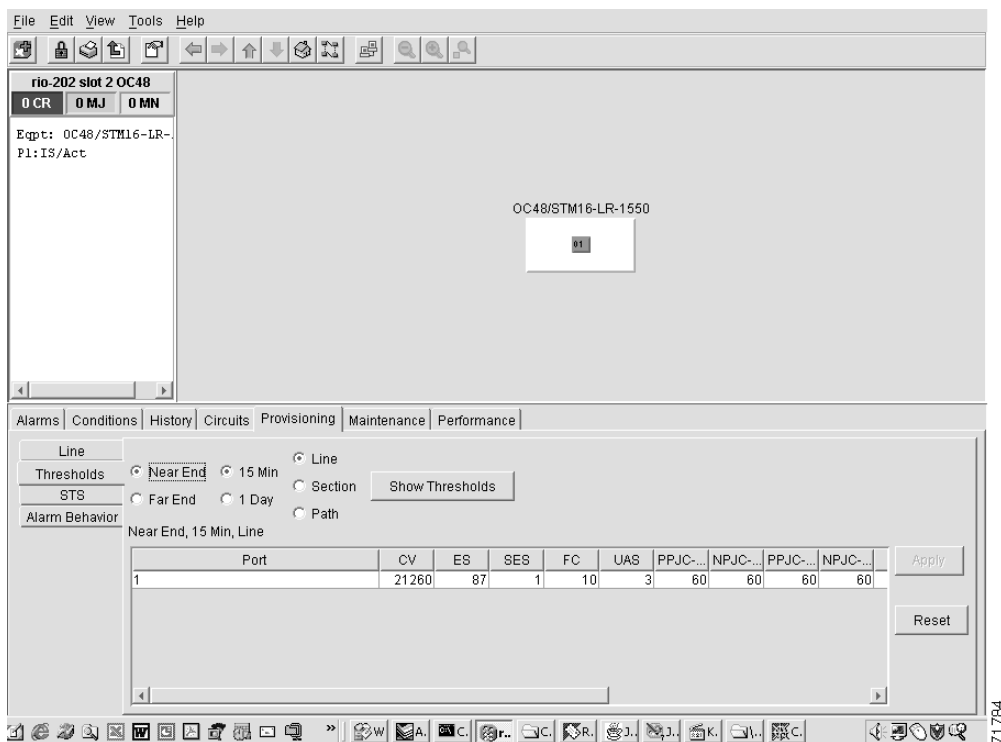
Heading	Description	Options
PJ Sts Mon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. Only one STS can be monitored on each OC-N port. See the “Pointer Justification Count Reference” section on page 8-13 for more information.	<ul style="list-style-type: none"> 0 (default) - 3 (OC-3, per port) 0 (default) - 12 (OC-12) 0 (default) - 48 (OC-48)
Status	Places port in or out of service	<ul style="list-style-type: none"> Out of Service (default) In Service
Type	Defines the port as SONET or SDH.	Sonet only

Step 4 Click **Apply**.

Procedure: Provision Threshold Settings for OC-N Cards

Step 1 Display the OC-N card in CTC card view (Figure 7-2 on page 7-12).

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

Figure 7-2 Provisioning thresholds for the OC48 IR 1310 card

Step 3 Modify the settings shown in Table 7-6 on page 7-13.

Default thresholds apply to all optical cards unless otherwise specified.

Table 7-6 OC-N Card Threshold Settings on the Provisioning > Thresholds Tab

Heading	Description	Options
Port	Port number	<ul style="list-style-type: none"> • 1, 2, 3, or 4 (OC-3) • 1 (OC-12, OC-48)
CV	Coding violations	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> • 1312/13120 (OC-3 Near and Far End) • 5315/53150 (OC-12 Near and Far End) • 21260/212600 (OC-48 Near and Far End) Section <ul style="list-style-type: none"> • 10000/100000 (Near End); N/A (Far End) Path <ul style="list-style-type: none"> • 15/125 (Near End); N/A (Far End)
ES	Errored seconds	Numeric. Default (15 min/1 day): Line <ul style="list-style-type: none"> • 87/864 (Near and Far End) Section <ul style="list-style-type: none"> • 500/5000 (Near End); (NA Far End) Path <ul style="list-style-type: none"> • 12/100 (Near End); N/A (Far End)
SES	Severely errored seconds	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> • 1/4 (Near and Far End) Section <ul style="list-style-type: none"> • 500/5000 (Near End); N/A (Far End) Path <ul style="list-style-type: none"> • 3/7 (Near End); N/A (Far End)
FC	Failure count	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> • 10/40 (Near and Far End) Path <ul style="list-style-type: none"> • 10/10 (Near End); N/A (Far End)
UAS	Unavailable seconds	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> • 3/10 (Near and Far End) Path <ul style="list-style-type: none"> • 10/10 (Near End); N/A (Far End)

Table 7-6 OC-N Card Threshold Settings on the Provisioning > Thresholds Tab (continued)

Heading	Description	Options
SEFS	Severely errored framing seconds	Numeric. Defaults (15 min/1 day): Section <ul style="list-style-type: none"> 500/5000 (Near End); N/A (Far End)
PPJC-Pdet	Positive Pointer Justification Count, STS Path detected. See the “Performance Monitoring for Optical Cards” section on page 8-24 for more information.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 60/5760 Near End
NPJC-Pdet	Negative Pointer Justification Count, STS Path detected. See the “Performance Monitoring for Optical Cards” section on page 8-24 for more information.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 60/5760 (OC-3 Near End); N/A (OC-3 Far End) 0/0 (OC-12 and OC-48 Near End); N/A (OC-12 and OC-48 Far End)
PPJC-Pgen	Positive Pointer Justification Count, STS Path generated. See the “Performance Monitoring for Optical Cards” section on page 8-24 for more information.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 60/5760 (OC-3 Near End); N/A (OC-3 Far End) 0/0 (OC-12 and OC-48 Near End); N/A (OC-12 and OC-48 Far End)
NPJC-Pgen	Negative Pointer Justification Count, STS Path generated. See the “Performance Monitoring for Optical Cards” section on page 8-24 for more information.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 60/5760 (OC-3 Near End); N/A (OC-3 Far End) 0/0 (OC-12 and OC-48 Near End); N/A (OC-12 and OC-48 Far End)
PSC	Protection Switching Count (Line)	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 1/5 (Near End); N/A (Far End)
PSD	Protection Switch Duration (Line)	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 300/600 (Near End); N/A (Far End)
PSC-W	Protection Switching Count - Working line BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 1/5 (Near End); N/A (Far End)

Table 7-6 OC-N Card Threshold Settings on the Provisioning > Thresholds Tab (continued)

Heading	Description	Options
PSD-W	Protection Switching Duration - Working line BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 300/600 (Near End); N/A (Far End)
PSC-S	Protection Switching Duration - Span BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 1/5 (Near End); N/A (Far End)
PSD-S	Protection Switching Duration - Span BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 300/600 (Near End); N/A (Far End)
PSC-R	Protection Switching Duration - Ring BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S, and PSC-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 1/5 (Near End); N/A (Far End)
PSD-R	Protection Switching Duration - Ring BLSR is not supported on the OC-3 card; therefore, the PSD-W, PSD-S, and PSD-R PMs do not increment.	Numeric. Defaults (15 min/1 day): Line <ul style="list-style-type: none"> 300/600 (Near End); N/A (Far End)

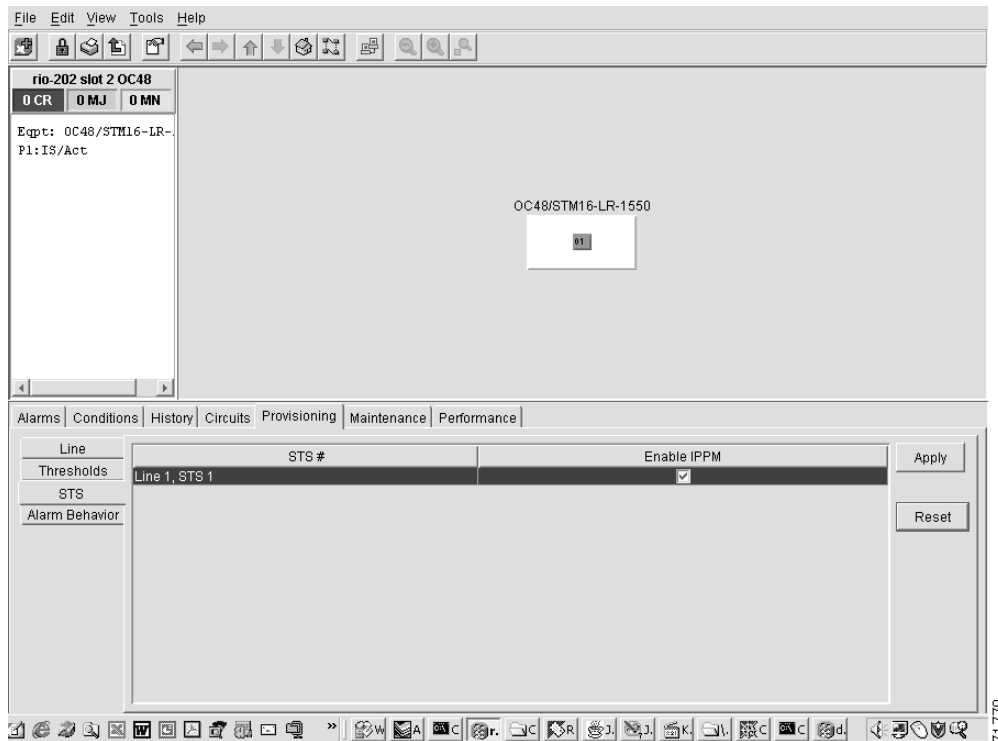
Click **Apply**.

7.4 Provisioning IPPM

Intermediate-Path Performance Monitoring (IPPM) allows you to transparently monitor traffic originating on DS-1 or DS-3 ports on XTC cards (Path Terminating Equipment) as it passes through OC-3, OC-12, and OC-48 cards (Line Terminating Equipment). To use IPPM, you create the STS circuit on the DS-N cards, then enable IPPM on the OC-N cards that carry the circuit.

For example, suppose you have an STS circuit that originates and terminates on DS-N ports at Nodes 1 and 4. You want to monitor the circuit as it passes through OC-N cards at Nodes 2 and 3. To do this, you enable IPPM on the OC-N card by selecting the appropriate STS, in this example, STS 1 (Figure 7-3).

Figure 7-3 IPPM provisioned for STS 1 on an OC-12 card



After enabling IPPM, performance is displayed on the Performance tab for the OC-48 card. IPPM enables per-path statistics for STS CV-P (coding violations), STS ES-P (errored seconds), STS FC-P (failure count), STS SES-P (severely errored seconds), and STS UAS-P (unavailable seconds). Additional rows will appear in the table on the STS IPPM subtab as circuits are created. After the circuits are created, you can enable for IPPM collection. See Chapter 8, “Performance Monitoring” for a definition of every parameter.

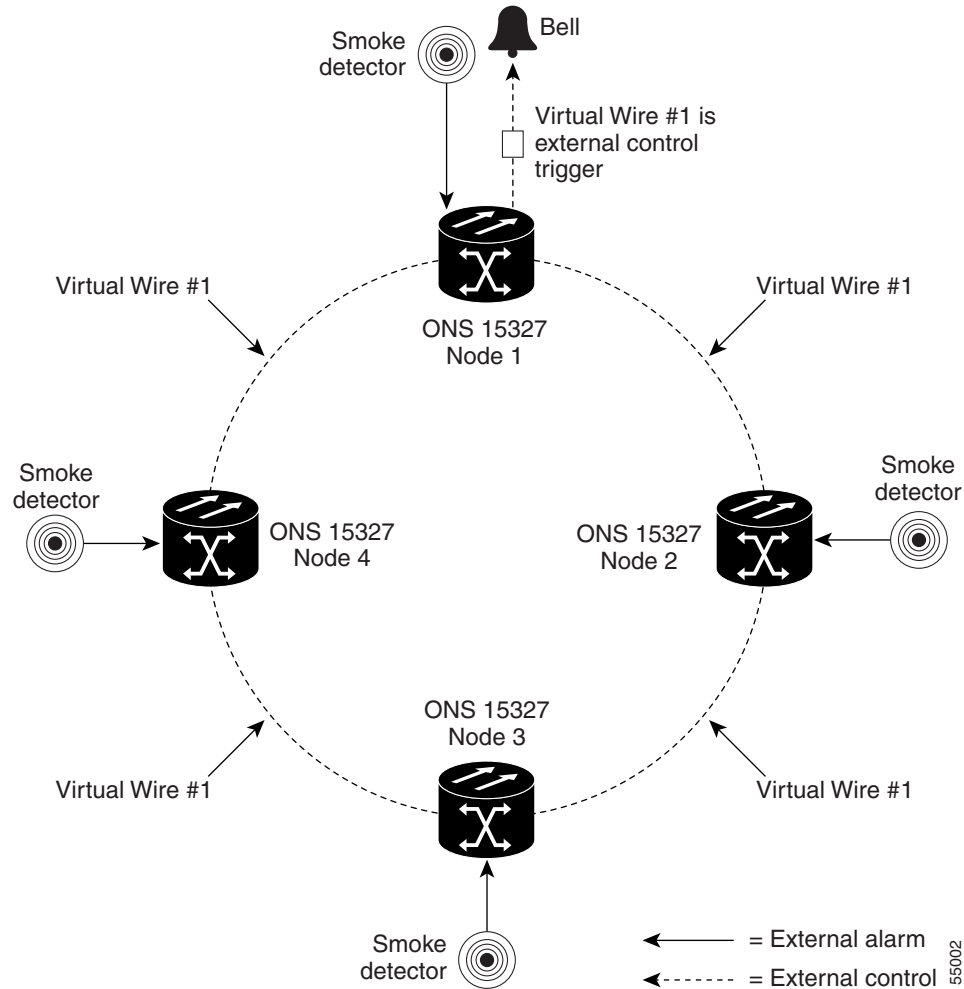
Procedure: Enable Intermediate-Path Performance Monitoring

-
- Step 1** If the STS circuit does not exist, create the circuit. (The circuit must pass through the OC-N card before you can enable IPPM on the circuit.)
 - Step 2** In CTC, open the card view of an OC-N card that carries the circuit.
 - Step 3** Select the **Provisioning > STS** tabs.
 - Step 4** Click **Enable IPPM** for the STS you want to monitor.
 - Step 5** Click **Apply**.
-

7.5 Using Virtual Wires

Provisioning the external alarms provides a “virtual wires” option that you can use to route external alarms and controls from different nodes to one or more alarm collection centers. For example, in Figure 7-4, smoke detectors provisioned as external alarms at Nodes 1, 2, 3, and 4 are assigned to Virtual Wire #1, and Virtual Wire #1 is provisioned as the trigger (external output control) for an external bell at Node 1.

Figure 7-4 Example of external alarms and controls in a virtual wire configuration



7.5.1 External Input Alarms

Use external alarms for sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

Provision External Alarms

- Step 1** Wire the external-device relays to the Alarm RJ-45 connector on the MIC.
- Step 2** Log into CTC and display the working XTC card in card view.
- Step 3** Click the **Provisioning > External Alarms** tabs (Figure 7-5).
- Step 4** Complete the following fields for each external device wired to the RJ-45 connector on the MIC card:
- *Enabled*—Click the box to activate the fields for the corresponding alarm input number.
 - *Alarm Type*—Select an alarm type from the list provided.
 - *Severity*—Select a severity. The severity determines how the alarm displays in the CTC Alarms and History tabs and whether the LEDs activate. Critical, Major, and Minor activate the appropriate LEDs. Not Alarmed and Not Reported do not activate LEDs, but do report the information in CTC.
 - *Virtual Wire*—Select the virtual wire that will carry the alarm signal (none or Virtual Wire 1– 4).
 - *Raised When*—Select the contact condition (open or closed) that will trigger the alarm in CTC.
 - *Description*—Default descriptions are provided for each alarm type; change the description as necessary. The description appears in Alarms tab view when the alarm is raised.
- Step 5** To provision additional devices, complete Step 4 for each additional device.
- Step 6** Click **Apply**.
- Step 7** Figure 7-5 shows the External Alarms subtab.

Figure 7-5 The External Alarms subtab showing the XTC-28-3 card

The screenshot shows the Cisco CTC interface for the XTC-28-3 card. The main display area shows the card details and a table of external alarm inputs. The table has columns for Input#, Enabled, Alarm Type, Severity, Virtual Wire, Raised When, and Description. The first row is for Input# 1, which is enabled and has an alarm type of Smoke, severity of Major, and a description of Smoke Detector.

Input#	Enabled	Alarm Type	Severity	Virtual Wire	Raised When	Description
1	<input checked="" type="checkbox"/>	Smoke	Major	Wire 1	Closed	Smoke Detector
2	<input type="checkbox"/>					
3	<input type="checkbox"/>					
4	<input type="checkbox"/>					
5	<input type="checkbox"/>					
6	<input type="checkbox"/>					

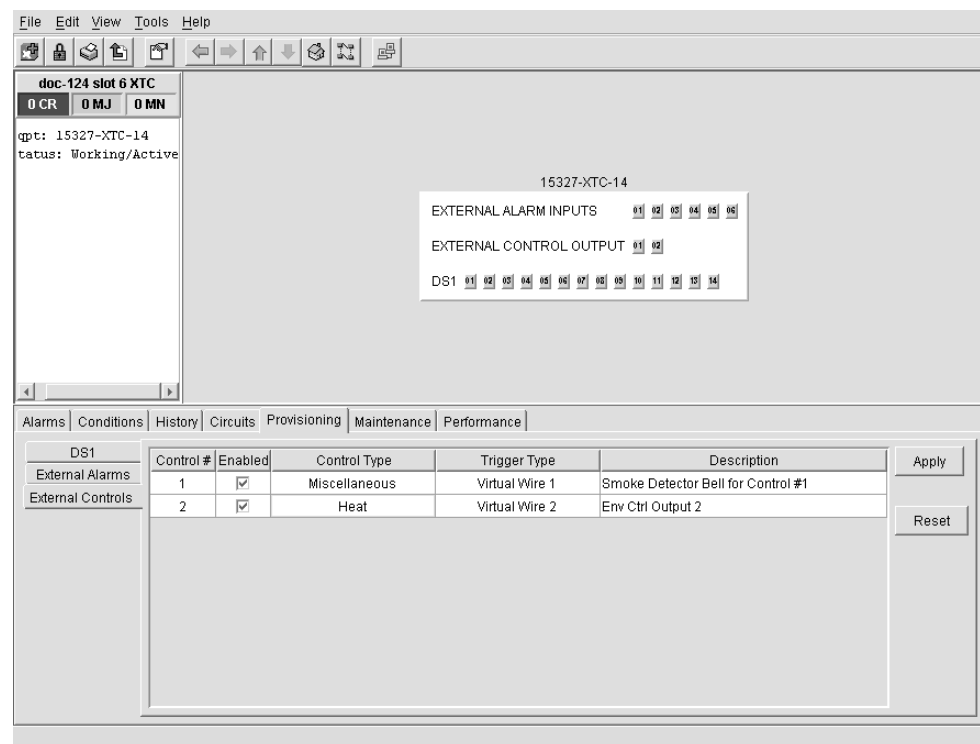
7.5.2 External Output Controls

Use external controls, or office alarms, to drive visual or audible devices such as bells and lights. The alarm-triggering conditions for the external controls can be the user-defined external input alarms (virtual wire), local severity-based alarms (e.g. trigger when any Major alarm happens), or remote severity-based alarms.

Provision External Controls

- Step 1** Wire the external control relays to the ALARM RJ-45 connector on the MIC.
- Step 2** In CTC, log into the node and display the XTC card view.
- Step 3** Click the **Provisioning > External Controls** tabs as shown in Figure 7-6.

Figure 7-6 The External Controls subtab showing the XTC-14 card

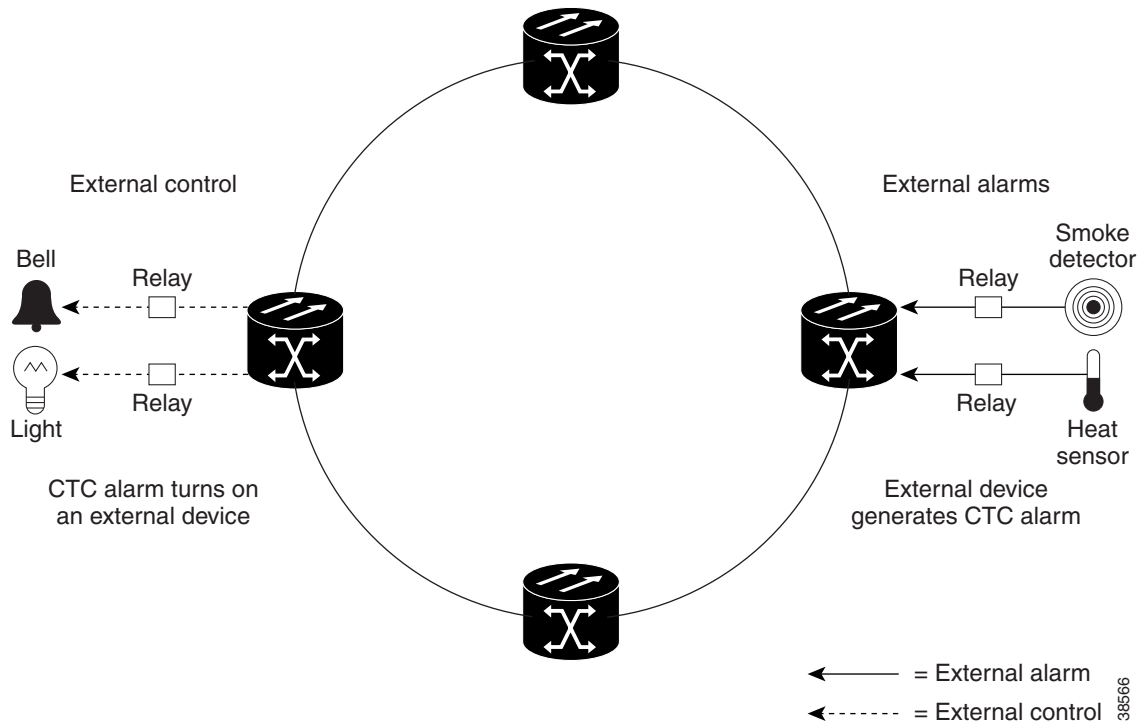


- Step 4** Complete the following fields for each external control wired to the Alarm connector on the MIC:
- *Enabled*—Click the box to activate the fields for alarm input number 1 or 2.
 - *Control Type*—Select a control type: Air Conditioning, Engine, Fan, Generator, Heat, Light, Miscellaneous, or Sprinkler.
 - *Trigger Type*—Select a trigger type: a local Minor, Major, or Critical alarm; a remote Minor, Major, or Critical alarm; or a virtual wire activation.
 - *Description*—Enter a description.
- Step 5** To provision additional controls, complete Step 4 for each additional device.

Step 6 Click **Apply**.

Figure 7-7 shows a functional diagram of alarm input and output.

Figure 7-7 Example of the external alarm input and output process



7.5.3 Provisioning Orderwire Pass-Through

Orderwire allows onsite personnel to communicate with one another using standard phone sets. Although the ONS 15327 does not terminate orderwire (there is no RJ-11 jack), it can pass through Local and Express orderwire traffic using the SONET Orderwire overhead:

- Local orderwire is carried on the SONET Section layer E1 byte. Regenerators on either side of ONS 15327 nodes terminate the channel.
- Express orderwire is carried on the E2 byte of the SONET Line layer. Regenerators on either side of ONS 15327 nodes terminate the channel.

Use the E1 byte (Local) when making orderwire connections to section terminating equipment and the E2 byte (Express) when making orderwire connections to line terminating equipment. The ONS 15327 and ONS 15454 are both section and line terminating equipment. When provisioning orderwire pass-through across networks that are exclusively ONS 15327s and/or ONS 15454s, you can use either Local or Express orderwire. If other equipment will be used to pass or terminate orderwire traffic, consult the documentation for that equipment to determine if it is section or line terminating equipment.

Procedure: Provision Orderwire Pass-Through

- Step 1** In CTC, open the node view.
 - Step 2** Select the Orderwire subtab.
 - Step 3** Click **Create**.
 - Step 4** Select a slot/port in the From (A) column and the To (B) column.
 - Step 5** Click **OK**.
-



Performance Monitoring

Performance-monitoring parameters (PMs) 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.

For information about Ethernet PMs, see Chapter 9, “Ethernet Operation.” Additional PM information can also be found under Digital transmission surveillance, in Telcordia’s GR-1230-CORE, GR-820-CORE, and GR-253-CORE documents and the ANSI document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

Table 8-1 lists PM reference topics.

Table 8-1 Reference Topics for Performance Monitoring

Reference Topics
Using the Performance Monitoring Screen, page 8-2
Intermediate-Path Performance Monitoring Reference, page 8-12
Pointer Justification Count Reference, page 8-13
XTC DS1 Performance Monitoring Parameters, page 8-16
XTC DS3 Card Performance Monitoring Parameters, page 8-21
OC-3 Card Performance Monitoring Parameters, page 8-24
OC-12 Card Performance Monitoring Parameters, page 8-28
OC-48 Card Performance Monitoring Parameters, page 8-33

8.1 Using the Performance Monitoring Screen

The following sections describe how to use basic screen elements such as tabs, menus, and informational columns. Figure 8-1 shows the Performance tab of Cisco Transport Controller (CTC) card-level view.

Figure 8-1 Viewing performance-monitoring information

Performance tab

Card view

rio-202 - Cisco Transport Controller

rio-202 slot 2 OC48

OC48/STM16-LR-1550

Alarms | Conditions | History | Circuits | Provisioning | Maintenance | Performance

15 min | Near End | 1 day | Far End | Port: 1 | STS: 1 | Refresh | Auto-refresh: None | Baseline | Clear...

15-minute, near-end registers for Port #1, STS #1, at 4/29/2002 8:06:37

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PRC-R										

8.1.1 Viewing PMs

Before you view PMs, be sure you have created the appropriate circuits and provisioned the card according to your specifications. For information about circuit creation and card provisioning, see Chapter 6, “Circuits and Tunnels” and Chapter 7, “Card Provisioning.”



Note

Rows relating directly to a card port are always present. Rows relating to an STS or virtual tunnel (VT) carried on the port appear at the time of circuit creation.

Procedure: View PMs

- Step 1** Open the desired electrical or optical card. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once only highlights the card.)

- Step 2** From the card view, click the **Performance** tab.
- Step 3** View the PM parameter names that appear on the left portion of the screen in the Param column. The parameter numbers appear on the right portion of the screen in the Curr (current) and Prev (previous) columns.
-

8.1.2 Changing the Screen Intervals

Changing the screen view allows you to view PMs in 15-minute intervals or 24-hour periods. Figure 8-2 shows the time interval buttons on the Performance Monitoring screen. Thirty-three 15-minute periods and two one-day periods of performance monitoring can be displayed. Each period is displayed in one column. The 15-minute periods are anchored to the system clock quarter-hour marks. The one-day periods are anchored to the system clock one-day periods.

**Note**

White fields with data indicate the number is applicable to the card. White fields without data indicate the field is inapplicable to the card. Yellow fields with data indicate that the field is applicable, but the data contained there is invalid.

Performance-monitoring data for OC-n cards is refreshed on entry to the performance-monitoring pane, or when the signal type is changed. It is not refreshed for Ethernet cards. Data can also be refreshed by clicking the Refresh button (Figure 8-2), or by choosing an auto-refresh time interval.

**Note**

Choosing an auto-refresh period does not immediately refresh the data. The user must click the Refresh button, or select an auto-refresh period when changing the period, end, or monitored interface.

**Note**

In a 1:1 or 1:n protection scheme, protection data is only available for the working or protect active card. The data is displayed in the working card performance-monitoring pane. In a 1+1 protection scheme, data is available for the working and protect active and standby cards. The data is displayed on each card pane.

Figure 8-2 Time interval buttons on the Performance tab (card view)

Fifteen-minute and twenty-four hour intervals

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PSC-R										

Procedure: Select Fifteen-Minute PM Intervals on the Performance Monitoring Screen

- Step 1** Open the electrical or optical card of choice. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
- Step 2** From the card view, click the **Performance** tab.
- Step 3** Click the **15 min** button.
- Step 4** Click the **Refresh** button. Performance-monitoring parameters display in 15-minute intervals synchronized with the time of day.
- Step 5** View the Current column to find PM counts for the current 15-minute interval.

Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 15-minute interval, a threshold crossing alert (TCA) will be raised. The value represents the counter for each specific performance-monitoring parameter.



Note A TCA is a transient event. It is documented in the History pane if the Show Events check box is selected.

- Step 6** View the Prev-N columns to find PM counts for the preceding 15-minute intervals.

**Note**

If a complete 15-minute interval count is not possible, the value displays with a yellow background. An incomplete or incorrect count can be caused by changing node timing settings, changing the time zone settings on CTC, replacing a card, resetting a card, or by changing port states. When a complete count occurs, the subsequent 15-minute interval appears with a white background.

Procedure: Select Twenty-Four Hour PM Intervals on the Performance Monitoring Screen

- Step 1** Open the electrical or optical card of choice. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
- Step 2** From the card view, click the **Performance** tab.
- Step 3** Click the **1 day** button.
- Step 4** Click the **Refresh** button. Performance monitoring displays in 24-hour periods synchronized with the time of day.
- Step 5** View the Current column to find PM counts for the current 24-hour period.
- Each monitored performance parameter has corresponding threshold values for the current time period. If the value of the counter exceeds the threshold value for a particular 24-hour period, a TCA will be raised. The value represents the counter for each specific performance-monitoring parameter.
- Step 6** View the Prev columns to find PM counts for the preceding 24-hour period.

**Note**

If a complete count over a 24-hour period is not possible, the value displays with a yellow background. An incomplete or incorrect count can be caused by changing node timing settings, changing the time zone settings on CTC, replacing a card, resetting a card, or by changing port states. When a complete count occurs, the subsequent 24-hour period appears with a white background.

Procedure: Clearing PM Data on the Performance Monitoring Screen

- Step 1** In the card view, click the **Performance** tab.
- Step 2** Click the **Clear** button. The Clear Statistics dialog box appears. Click one of three options:
- Selected interfaces. This refers to the port-level data, STS-level data, and VT-level data. Choosing this option will clear the entire set of displayed data at the NE level, rather than the selected row.
 - All interfaces on port [1]. Choosing this option will clear data for all interfaces at the NE level, including those not currently displayed, such as the ends, periods, and VTs.
 - All interfaces on card. Choosing this option will only clear the interfaces that apply to the selected card at the NE.
- Step 3** Click **OK**. Clearing the data will invalidate all data for the current 15-minute period because the data does not reflect the full period.

Step 4 To cancel changes, click **Cancel**. bsequent 24-hour period appears with a white background.

8.1.3 Viewing Near-End and Far-End PMs

Select the Near End or Far End button depending on the PMs you wish to view. Only cards that allow both near-end and far-end monitoring have these buttons as an option. Figure 8-3 shows the Near End and Far End buttons on the Performance Monitoring screen.

Figure 8-3 Near End and Far End buttons on the card view Performance tab

Near end and far end buttons

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PSC-R										

Procedure: Select Near-End PMs on the Performance Monitoring Screen

- Step 1** Open the electrical or optical card of choice. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
- Step 2** From the card view, click the **Performance** tab.
- Step 3** Click the **Near End** button.
- Step 4** Click the **Refresh** button. All PMs occurring for the selected card on the incoming signal are displayed.

Procedure: Select Far-End PMs on the Performance Monitoring Screen

- Step 1** Open the electrical or optical card of choice. To do so, double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
- Step 2** From the card view, click the **Performance** tab.
- Step 3** Click the **Far End** button.
- Step 4** Click the **Refresh** button. All PMs recorded by the far-end node for the selected card on the outgoing signal are displayed.

8.1.4 Using the Signal-Type Menu

Use the signal-type menus to monitor PMs for near-end or far-end signals on a selected port. Different signal-type menus appear depending on the card type and the circuit type. The appropriate types (DS1, DS3, VT path, STS path, OCn section, line) appear based on the card. For example, the XTC-28-3 has DS3, DS1, VT path, and STS path PMs. Figure 8-4 shows the signal-type menus on the Performance Monitoring screen for an OC48 card.

Figure 8-4 Signal-type menus for an OC48 card

Signal-type menu

15-minute, near-end registers for Port #1, STS #1, at 4/29/2002 8:06:37

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PSC-R										

Procedure: Select Signal-Type Menus on the Performance Monitoring Screen

-
- Step 1** Open the electrical or optical card of choice. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
 - Step 2** From the card view, click the **Performance** tab.
 - Step 3** Click the signal-type menu. (For example, the OC48 card has a menu labeled STS.)
 - Step 4** Select a port using the signal-type menu.
-

8.1.5 Using the Baseline Button

In Software R3.0 and higher, the Baseline button located on the far right of the screen clears the PM count displayed in the Current column, but does not clear the PM count on the card. The value is changed in the CTC software, but is not changed for the NE. When the current 15-minute or 24-hour time interval expires or the screen view changes, the total number of PM counts on the card and on the screen appear in the appropriate column, decrementing from the values at the time the command is performed.

The baseline values are discarded if you select a new port, interval, near-end, far-end, STS, or if you change views to a different screen and then return to the Performance Monitoring screen. The Baseline button enables you to easily see how quickly PM counts are rising without having to perform calculations. Figure 8-5 shows the Baseline button on the Performance Monitoring screen.

Figure 8-5 Baseline button for clearing displayed PM counts

The screenshot shows the Performance Monitoring screen for 'rio-202 slot 2 OC48'. The 'Performance' tab is selected. The interface includes a menu for '15 min', 'Near End', 'Port: 1', and 'STS: 1'. A 'Baseline' button is located on the right side of the screen, with an arrow pointing to it from the label 'Baseline button'. Below the menu is a table of performance registers.

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PRC-R										

Procedure: Use the Baseline Button on the Performance Monitoring Screen

- Step 1** Open the electrical or optical card of choice. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
- Step 2** From the card view, click the **Performance** tab.
- Step 3** Click the **Baseline** button.

8.1.6 Using the Clear Button

The Clear button located on the far right of the Performance Monitoring screen clears certain PM counts depending on the option selected. Figure 8-6 shows the Clear button on the Performance Monitoring screen.



Caution

Use caution when pressing the Clear button; improper use can potentially mask problems. This button is commonly used for testing purposes such as clearing a count that results in the UAS count incrementing. The UAS state suppresses counting CVs.

Figure 8-6 Clear button for clearing PM counts

The screenshot shows the Performance Monitoring screen for 'rio-202 slot 2 OC48'. The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar, and a main display area showing 'OC48/STM16-LR-1550' with a green status indicator. Below the main display are tabs for Alarms, Conditions, History, Circuits, Provisioning, Maintenance, and Performance. The Performance tab is active, showing a table of 15-minute, near-end registers for Port #1, STS #1, at 4/29/2002 8:06:37. The table has columns for Param, Curr, Prev, and eight Previews (Prev-1 to Prev-8). The 'Clear...' button is located at the bottom right of the Performance tab, and an arrow points to it with the label 'Clear button'.

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
CV-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PSC-R										

Procedure: Use the Clear Button on the Performance Monitoring Screen

-
- Step 1** Open the electrical or optical card of choice. Double-click the card graphic in the main (node) view or right-click the card and select **Open Card**. (Clicking a card once highlights the card only.)
- Step 2** From the card view, click the **Performance** tab.
- Step 3** Click the **Clear** button. The Clear Statistics dialog box appears.
- Step 4** From the Clear Statistics menu, choose one of three options:
- *Selected Interfaces*: Clearing selected interfaces erases all PM counts associated with the selected radio buttons at the NE level. This refers to the port-level data, STS-level data, and VT-level data. Choosing this option will clear the entire set of displayed data at the NE level, rather than the selected row.
 - *All interfaces on port x*: Choosing this option will clear data for all interfaces at the NE level, including those not currently displayed, such as the ends, periods, and VTs.
 - *All interfaces on card*: Choosing this option will only clear the interfaces that apply to the selected card at the NE.
- Step 5** Click **OK**.
- Step 6** From the Zero Data menu, click **Yes** to clear the selected statistics.

**Note**

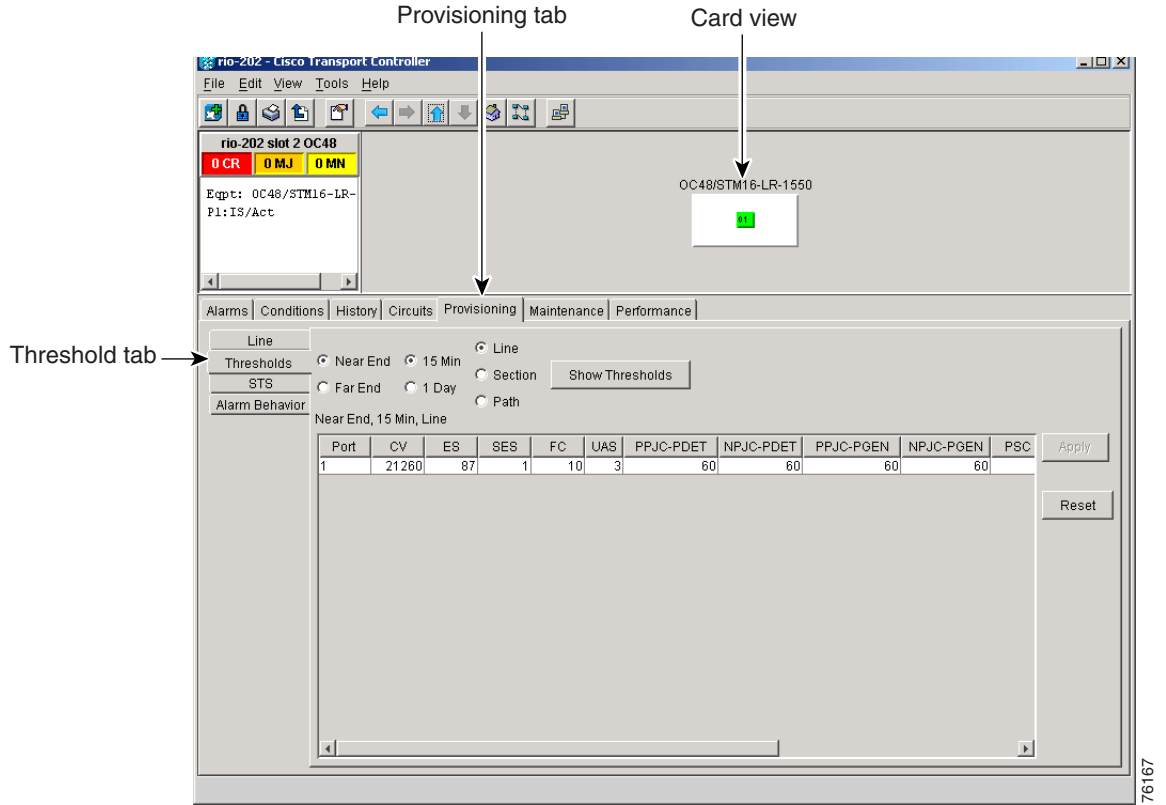
The Ethernet cards are the only cards without the Clear button option.

Threshold Reference

Thresholds are used to set error levels for each PM. You can program PM threshold ranges from the Provisioning > Threshold tabs on the card view. For procedures on provisioning card thresholds, such as line, path, and SONET thresholds, see the Card Provisioning chapter.

During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a TCA is generated by the node and sent to CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the performance monitoring parameter is disabled. Figure 8-7 shows the Provisioning > Threshold tabs for an OC-48 card.

Figure 8-7 Threshold tab for setting threshold values



Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical DS1 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

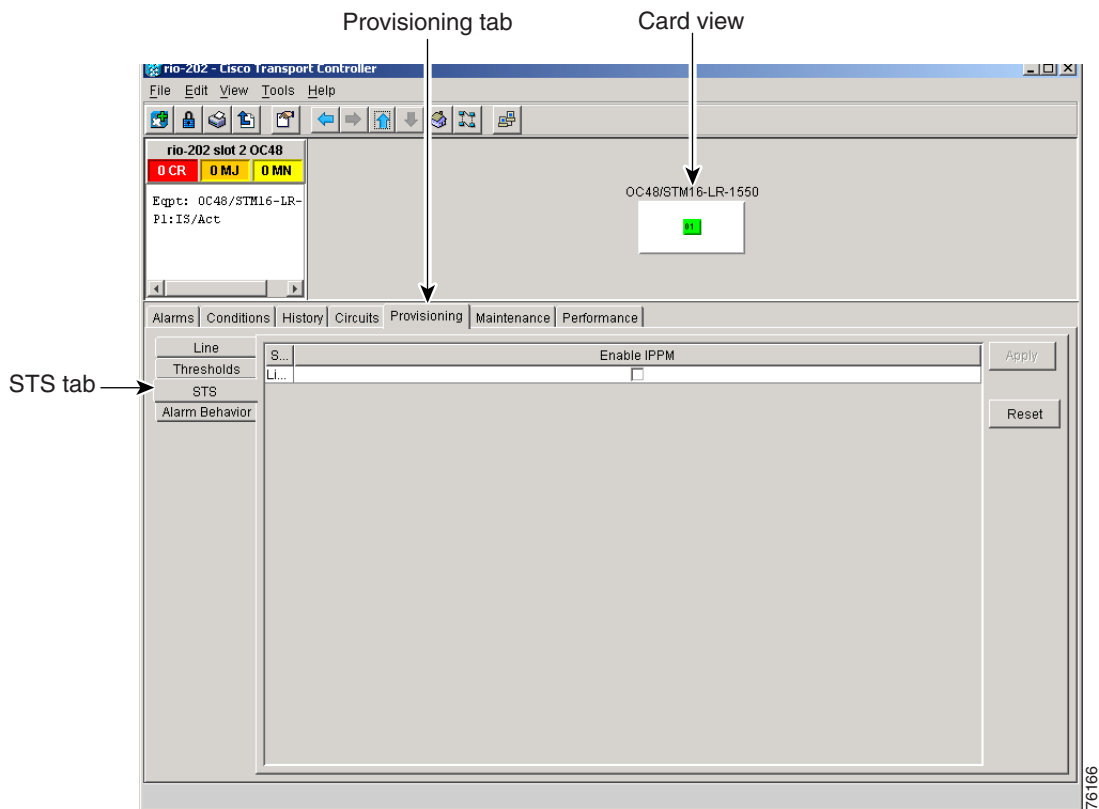
8.2 Intermediate-Path Performance Monitoring Reference

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. In addition to the path-terminating equipment (PTE) on the XTC, such as DS1s and DS3s, an ONS 15327 can terminate optical lines. Table 8-2 shows ONS 15327 cards that are considered LTEs. Figure 8-8 shows the Provisioning > STS tabs for an OC-3 card.

Table 8-2 Traffic Cards That Terminate the Line (LTEs)

Line Terminating Equipment	
OC3 IR 1310	OC48 IR 1310
OC12 IR 1310	OC48 LR 1550
OC12 LR 1550	

Figure 8-8 STS tab for enabling IPPM



Software R3.0 and higher allows LTE cards to monitor near-end PM data on individual STS payloads by enabling IPPM. After enabling IPPM provisioning on the line card, service providers can monitor large amounts of STS traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on STS paths that have IPPM enabled, and TCAs are raised only for PM parameters on the selected IPPM paths. The monitored IPPMs are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P. For more information about enabling IPPM, see Intermediate-Path Performance Monitoring Reference, page 8-12.

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

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

8.3 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 synchronization, signal jitter and signal wander occur on the transported signal. Excessive wander can cause terminating equipment to slip. It also causes slips at the SDH and 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 retransmitted.

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

Figure 8-9 shows pointer justification count parameters on the Performance Monitoring screen. You can enable PPJC and NPJC performance monitoring parameters for LTE cards. See Table 8-2 on page 8-12 for a list of Cisco ONS 15327 LTE cards.

Figure 8-9 Viewing pointer justification count parameters

Provisioning tab

Card view

rio-202 slot 2 OC48

0 CR 0 MJ 0 MN

Eqpt: OC48/STM16-LR-Pl:IS/Act

OC48/STM16-LR-1550

Alarms | Conditions | History | Circuits | Provisioning | Maintenance | Performance

15 min Near End Port: STS: Refresh Auto-refresh: None Baseline Clear...

1 day Far End

15-minute, near-end registers for Port #1, STS #1, at 4/18/2002 7:57:58

Param	Curr	Prev	Prev-1	Prev-2	Prev-3	Prev-4	Prev-5	Prev-6	Prev-7	Prev-8
CV-S	0	0	0	0	0	0	0	0	0	0
ES-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
SEFS-S	0	0	0	0	0	0	0	0	0	0
C-V-L	0	0	0	0	0	0	0	0	0	0
ES-L	0	0	0	0	0	0	0	0	0	0
SES-L	0	0	0	0	0	0	0	0	0	0
UAS-L	0	0	0	0	0	0	0	0	0	0
FC-L	0	0	0	0	0	0	0	0	0	0
PPJC-Pdet										
NPJC-Pdet										
PPJC-Pgen										
NPJC-Pgen										
PSC										
PSD										
PSC-W										
PSD-W										
PSC-S										
PSD-S										
PSD-S										
PSC-R										

Pointer justification counts

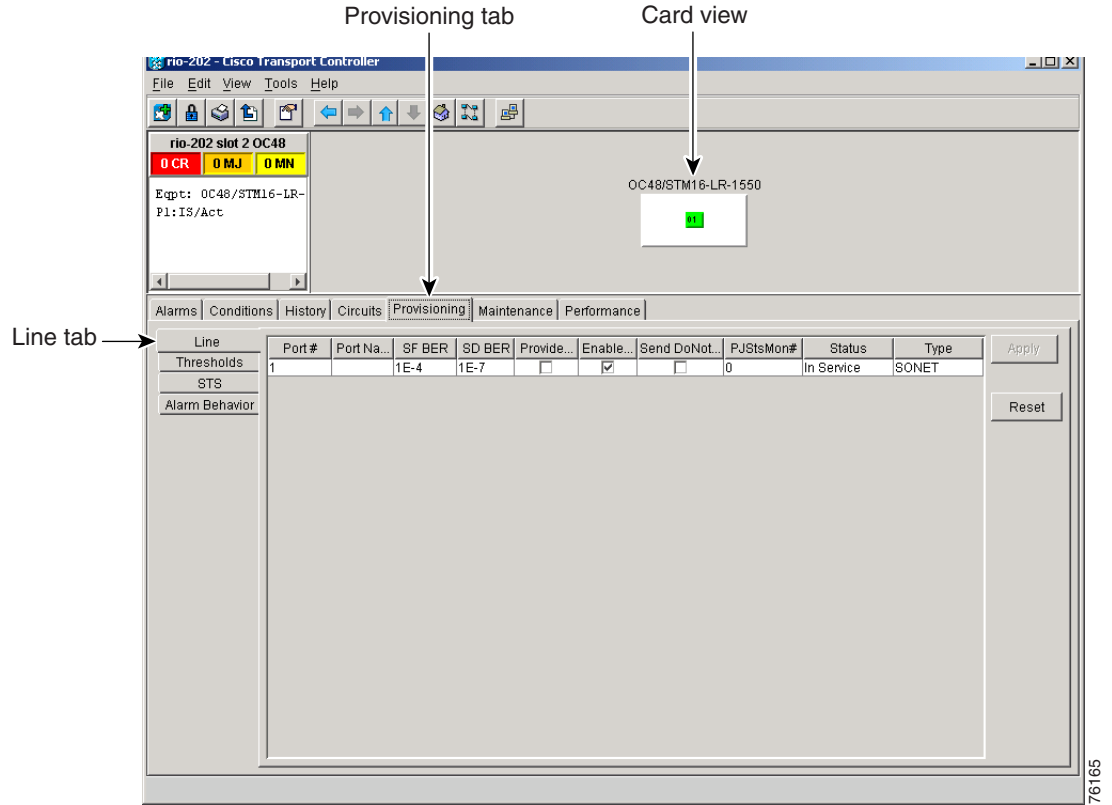
There are positive (PPJC) and negative (NPJC) pointer justification count parameters. PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications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

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 “OC-3 Card Performance Monitoring Parameters” section on page 8-24, “OC-12 Card Performance Monitoring Parameters” section on page 8-28, or the “OC-48 Card Performance Monitoring Parameters” section on page 8-33.

On CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. Figure 8-10 shows the PJStsMon# menu on the Provisioning screen. Pointer justification is only enabled for one STS at a time.

Figure 8-10 Line tab for enabling pointer justification count parameters



76165

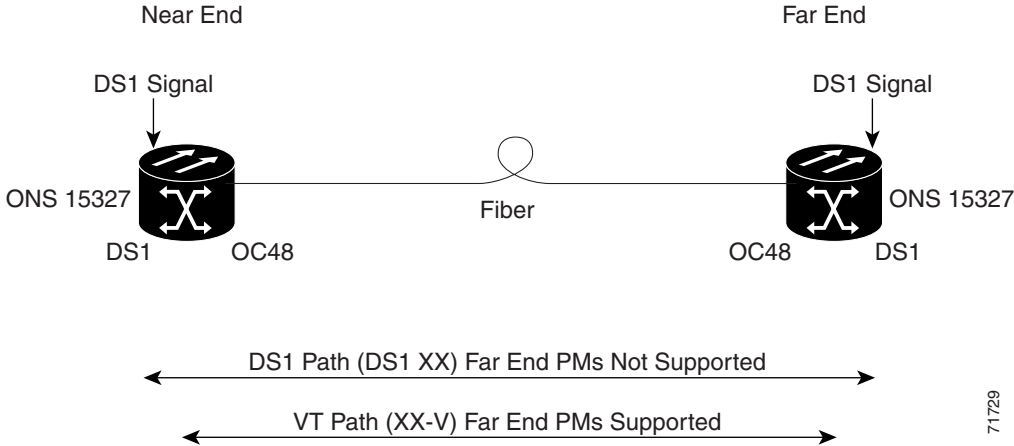
8.4 Performance Monitoring for Electrical Cards

The following sections define performance monitoring parameters for the XTC DS1 and XTC DS3 electrical cards.

8.4.1 XTC DS1 Performance Monitoring Parameters

Figure 8-11 shows the signal types that support far-end PMs. Far-end VT and STS path-performance monitoring is supported for the DS1 card. Far-end DS1 path-performance monitoring is not supported for the DS1 card. Figure 8-12 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS1 cards.

Figure 8-11 Monitored signal types for the XTC DS1 cards



Note

The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-12 PM read points on the XTC DS1 cards

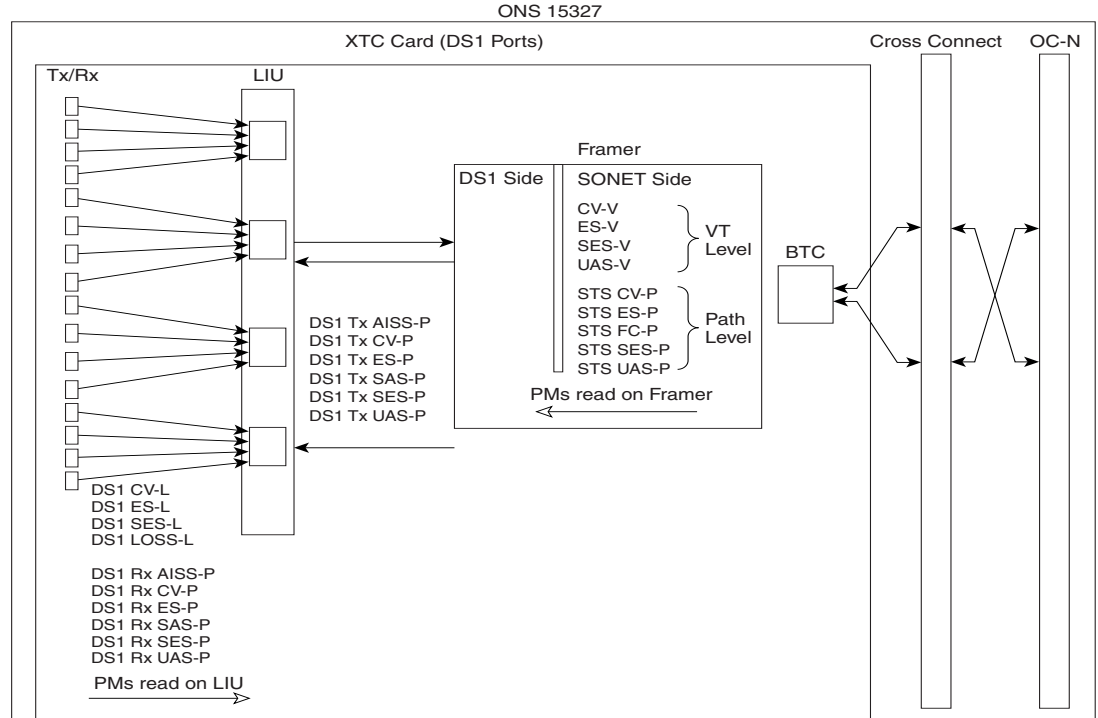


Table 8-3 DS1 Line PMs for the XTC DS1 Cards

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

Table 8-4 DS1 Receive Path PMs for the XTC DS1 Cards

Parameter	Definition
Note	Under the Provisioning > Threshold tab, the DS1 cards have user-defined thresholds for the DS1 receive (Rx) path PMs. In the Threshold tab they are displayed as Code Violation (CV), Errored Seconds (ES), Severely Errored Seconds (SES), Unavailable Seconds (UAS), Alarm Indication Signal (AISS), and Seconds Frame/Alarm Indication Signal (SAS) without the Rx prefix.
DS1 Rx AISS-P	Receive Path Alarm Indication Signal (Rx AISS-P) means an alarm indication signal occurred on the receive end of the path. This parameter is a count of seconds containing one or more Alarm Indication Signal (AIS) defects.
DS1 Rx CV-P	Receive Path Code Violation (Rx CV-P) means a coding violation occurred on the receive end of the path. For DS1-ESF paths, this parameter is a count of detected CRC-6 errors. For the DS1-SF paths, the Rx CV-P parameter is a count of detected frame-bit errors (FE).
DS1 Rx ES-P	Receive Path Errored Seconds (Rx ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths on the receive end of the signal. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more Severely Errored Frame (SEF) or Alarm Indication Signal (AIS) defects. For DS1-SF paths, the Rx ES-P parameter is a count of one-second intervals containing one or more frame-bit errors (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 Alarm Indication Signal (AIS) defects on the receive end of the signal.
DS1 Rx SES-P	Receive Path Severely Errored Seconds (Rx SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths on the receive end of the signal. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more Severely Errored Frame (SEF) or Alarm Indication Signal (AIS) defects occurred. For DS1-SF paths, a Severely Errored Second (SES) is a second containing either the occurrence of four frame-bit errors (FEs) or one or more SEF or AIS defects.
DS1 Rx UAS-P	Receive Path Unavailable Seconds (Rx UAS-P) is a count of one-second intervals when the DS1 path is unavailable on the receive end of the signal. The DS1 path is unavailable at the onset of 10 consecutive seconds that qualify as Severely Errored Seconds (SESS), and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as Severely Errored Seconds Path (SES-Ps). The ten seconds with no SES-Ps are excluded from unavailable time.

Table 8-5 DS1 Transmit Path PMs for the XTC DS1 Cards

Parameter	Definition
Note	Under the Performance tab, the displayed DS1 Tx path PM values are based on calculations performed by the card and therefore have no user-defined thresholds. The tab is labeled “Elect[rical] Path Threshold.”
DS1 Tx AIS-P	Transmit Path Alarm Indication Signal (Tx AIS-P) means an alarm indication signal occurred on the transmit end of the path. This parameter is a count of seconds containing one or more Alarm Indication Signal (AIS) defects.
DS1 Tx CV-P	Transmit Path Code Violation (Tx CV-P) means a coding violation occurred on the transmit end of the path. For DS1-ESF paths, this parameter is a count of detected CRC-6 errors. For the DS1-SF paths, the Tx CV-P parameter is a count of detected frame-bit errors (FEs).
DS1 Tx ES-P	Transmit Path Errored Seconds (Tx ES-P) is a count of the seconds containing one or more anomalies and/or defects for paths on the transmit end of the signal. For DS1-ESF paths, this parameter is a count of one-second intervals containing one or more CRC-6 errors, or one or more CS events, or one or more Severely Errored Frame (SEF) or Alarm Indication Signal (AIS) defects. For DS1-SF paths, the Tx ES-P parameter is a count of one-second intervals containing one or more frame bit error (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 Alarm Indication Signal (AIS) defects on the transmit end of the signal.
DS1 Tx SES-P	Transmit Path Severely Errored Seconds (Tx SES-P) is a count of the seconds containing more than a particular quantity of anomalies and/or defects for paths on the transmit end of the signal. For the DS1-ESF paths, this parameter is a count of seconds when 320 or more CRC-6 errors or one or more Severely Errored Frame (SEF) or Alarm Indication Signal (AIS) defects occurred. For DS1-SF paths, a Severely Errored Second (SES) is a second containing either the occurrence of four frame-bit errors (FEs) or one or more SEF or AIS defects.
DS1 Tx UAS-P	Transmit Path Unavailable Seconds (Tx UAS-P) is a count of one-second intervals when the DS1 path is unavailable on the transmit end of the signal. The DS1 path is unavailable at the onset of 10 consecutive seconds that qualify as Severely Errored Seconds (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 8-6 VT Path PMs for the XTC DS1 Cards

Parameter	Definition
CV-V	Code Violation VT Layer (CV-V) is a count of the B IP errors detected at the VT path layer. Up to two B IP 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 B IP error was detected. An Alarm Indication Signal VT Layer (AIS-V) defect (or 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 B IP errors were detected. SES-V can also be caused by an Alarm Indication Signal VT Layer (AIS-V) defect (or 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 Severely Errored Seconds VT Layer (SES-Vs), and continues to be unavailable until the onset of ten consecutive seconds occur that do not qualify as SES-Vs.

Table 8-7 Far-End VT Path PMs for the XTC DS1 Card

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

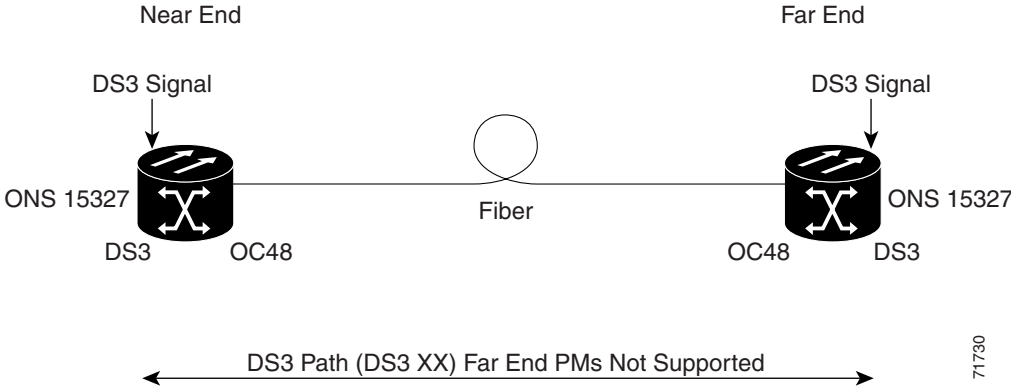
Table 8-8 SONET Path PMs for the XTC DS1 Cards

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (STS CV-P) is a count of B IP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight B IP 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 B IP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (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 ERDI-P for that path. The failure event ends when these failures are cleared.
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 B IP 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 Severely Errored Seconds Path (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 Severely Errored Seconds Path (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.

8.4.2 XTC DS3 Card Performance Monitoring Parameters

Figure 8-13 shows the signal types that support far-end PMs. Figure 8-14 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the XTC DS3 cards.

Figure 8-13 Monitored signal types for the XTC DS3 cards



Note

The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-14 PM read points on the XTC DS3 cards

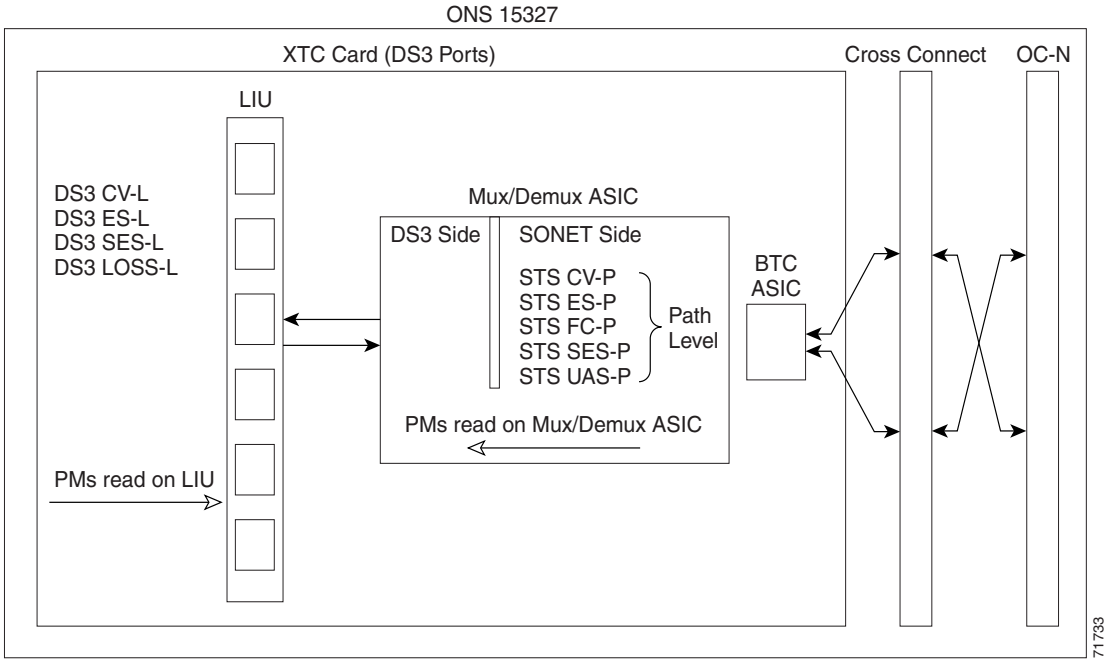


Table 8-9 Near-End DS3 Line PMs for the XTC DS3 Cards

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

Table 8-10 Near-End SONET Path PMs for the XTC DS3 Cards

Parameter	Definition
STS CV-P	Near-End STS Path Coding Violations (STS CV-P) is a count of B IP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight B IP errors can be detected per frame; each error increments 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 B IP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (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 ERDI-P for that path. The failure event ends when these failures are cleared.
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 B IP 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 Severely Errored Second Path (SES-P).
STS UAS-P	Near-End STS Path Unavailable Seconds (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 Severely Errored Seconds Path (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.

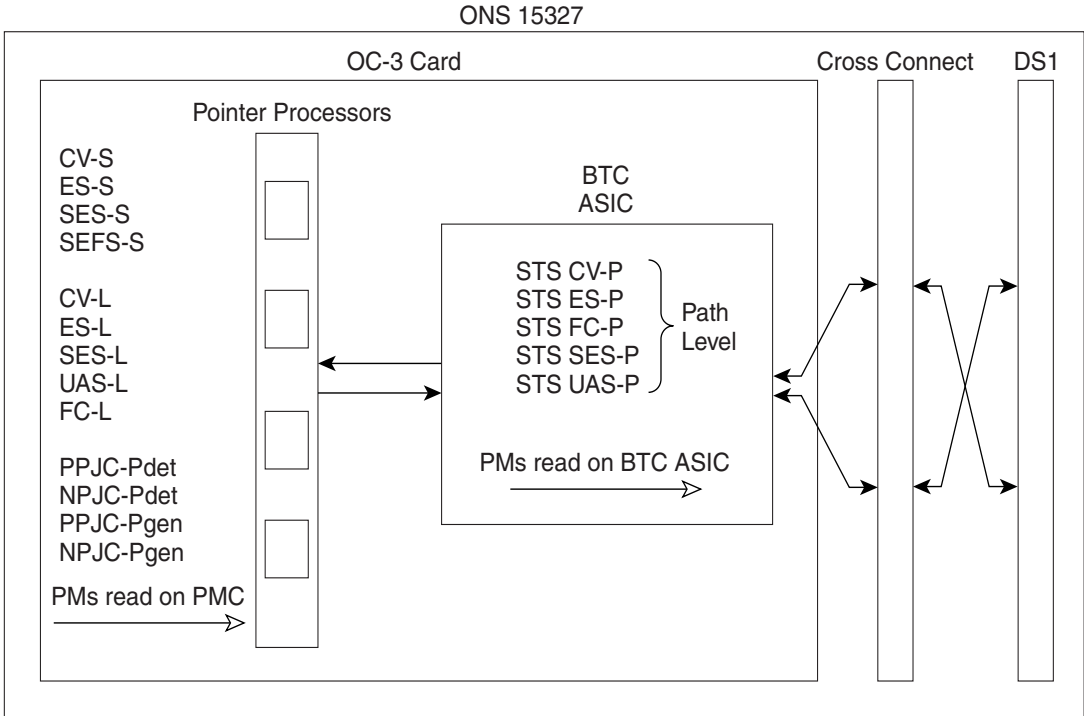
8.5 Performance Monitoring for Optical Cards

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

8.5.1 OC-3 Card Performance Monitoring Parameters

Figure 8-15 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-3 card.

Figure 8-15 PM read points on the OC-3 card



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

Table 8-11 Near-End Section PMs for the OC-3 Card

Parameter	Definition
CV-S	Section Coding Violation (CV-S) is a count of B IP errors detected at the section-layer (i.e. using the B1 byte in the incoming SONET signal). Up to eight section B IP errors can be detected per STS-N frame, with each error incrementing the current CV-S second register.
ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer B IP error was detected or a Severely Errored Frame (SEF) or Loss of Signal (LOS) defect was present.

Table 8-11 Near-End Section PMs for the OC-3 Card (continued)

Parameter	Definition
SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see GR-253 for value) or more section-layer B IP errors were detected or a (Severely Errored Frame) SEF or Loss of Signal (LOS) defect was present.
SEFS-S	Section Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when a Severely Errored Frame (SEF) defect was present. A (Severely Errored Frame) SEF defect is expected to be present during most seconds when a Loss of Signal (LOS) or Loss of Frame (LOF) defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect.

Table 8-12 Near-End Line Layer PMs for the OC-3 Cards Card

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

Table 8-13 Near-End Protection-Switching PMs for the OC-3 Cards

Parameter	Definition
	For information about Troubleshooting UPSR switch counts, see the alarm troubleshooting information in Chapter 14, "Alarm Troubleshooting". For information about creating circuits that perform a switch, see Chapter 6, "Circuits and Tunnels."
PSC (1+1 protection)	<p>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.</p> <p>For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM is only applicable if revertive line-level protection switching is used.</p> <p>Note BLSR is not supported on the OC-3 card; therefore, the PSC-W, PSC-S and PSC-R PMs do not increment.</p>
PSD	<p>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.</p> <p>For the protection line, PSD is a count of the seconds that the line was used to carry service. The PSD PM is only applicable if revertive line-level protection switching is used.</p> <p>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) PMs do not increment.</p>

Table 8-14 Near-End SONET Path H-Byte PMs for the OC-3 Card

Parameter	Definition
Note	On CTC, the count fields for Positive Pointer Justification Count (PPJC) and Negative Pointer Justification Count (NPJC) PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. See Pointer Justification Count Reference, page 8-13.
PPJC-Pdet	Positive Pointer Justification Count path-detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	Negative Pointer Justification Count path-detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	Positive Pointer Justification Count path-generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	Negative Pointer Justification Count path-generated (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 8-15 Near-End SONET Path PMs for the OC-3 Card

Parameter	Definition
Note	SONET path PMs will not count unless IPPM is enabled. For additional information, see the “Intermediate-Path Performance Monitoring Reference” section on page 8-12.
STS CV-P	Near-End STS Path Coding Violations (STS CV-P) is a count of B IP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight B IP errors can be detected per frame; each error increments 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 one or more STS path B IP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (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 ERDI-P for that path. The failure event ends when these failures are cleared.
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 B IP 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 Severely Errored Seconds Path (SES-P).
STS UAS-P	Near-End STS Path Unavailable Seconds (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 Severely Errored Seconds Path (SES-Ps), and continues to be unavailable until the onset of ten consecutive seconds that do not qualify as SES-Ps.

Table 8-16 Far-End Line Layer PMs for the OC-3 Card

Parameter	Definition
CV-L	Code Violation Line (CV-L) is a count of B IP 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 B IP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 B IP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each B IP error indicated by the incoming REI-L.
ES-L	Errored Seconds Line (ES-L) is a count of the seconds when at least one line-layer B IP error was reported by the far-end LTE or an RDI-L defect was present.
SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer B IP errors were reported by the far-end LTE or an RDI-L defect was present.

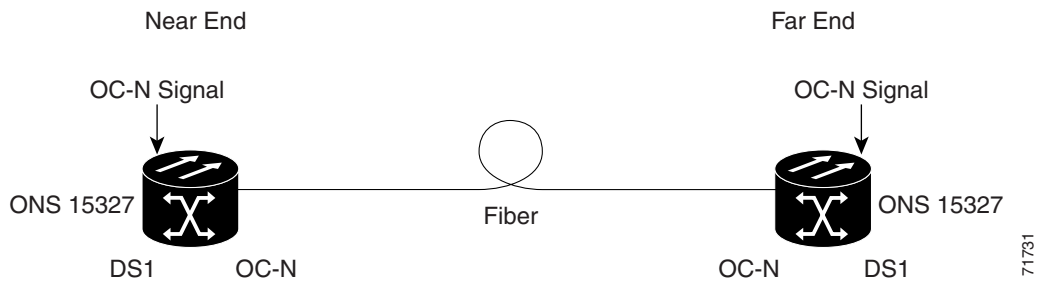
Table 8-16 Far-End Line Layer PMs for the OC-3 Card (continued)

Parameter	Definition
UAS-L	UAS-L 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-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 it ends when the RFI-L failure clears. A failure event that begins in one period and ends in another period is counted only in the period where it began.

8.5.2 OC-12 Card Performance Monitoring Parameters

Figure 8-16 shows the signal types that support far-end PMs. Figure 8-17 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-12 card.

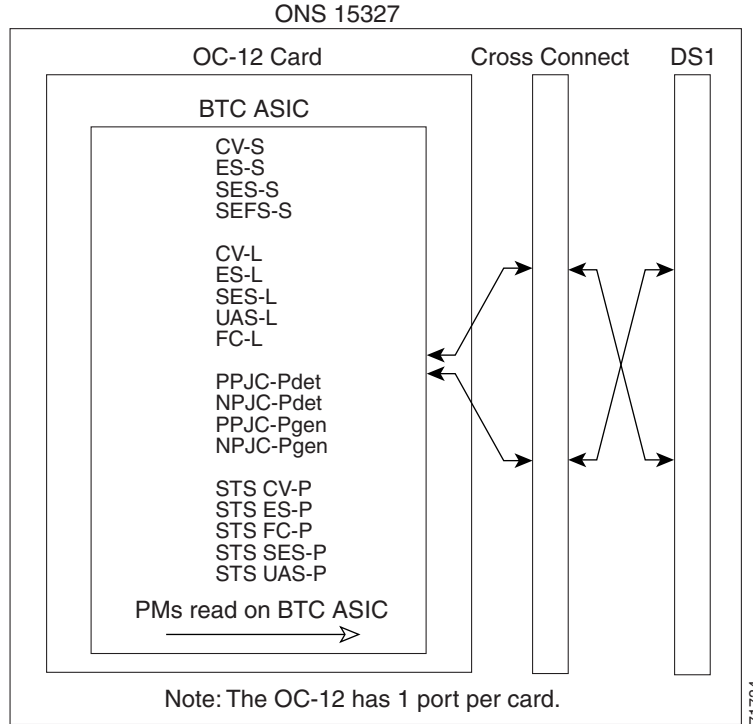
Figure 8-16 Monitored signal types for the OC-12 card



Note

PMs on the protect STS are not supported for BLSR. The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-17 PM read points on the OC-12 card



Note

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

Table 8-17 Near-End Section PMs for the OC-12 Card

Parameter	Definition
CV-S	CV-S is a count of B IP errors detected at the section-layer (i.e. using the B1 byte in the incoming SONET signal). Up to eight section B IP 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 B IP error was detected or a (Severely Errored Frame) SEF or Loss of Signal (LOS) defect was present.
SES-S	SES-S is a count of the seconds when K (see GR-253 for value) or more section-layer B IP errors were detected or a Severely Errored Frame (SEF) or Loss of Signal (LOS) defect was present.
SEFS-S	SEFS-S is a count of the seconds when a (Severely Errored Frame) SEF defect was present. An SEF defect is expected to be present during most seconds when a Loss of Signal (LOS) or Loss of Frame (LOF) defect is present. However, there may be situations when the SEFS-S parameter is only incremented based on the presence of an SEF defect.

Table 8-18 Near-End Line Layer PMs for the OC-12 Card

Parameter	Definition
CV-L	Code Violation Line (CV-L) is a count of B IP errors detected at the line-layer (i.e. using the B2 bytes in the incoming SONET signal). Up to 8 x N B IP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	Errored Seconds Line (ES-L) is a count of the seconds when at least one line-layer B IP error was detected or an AIS-L defect was present.
SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds when K (see GR-253 for values) or more line-layer B IP 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 Severely Errored Seconds Line (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.

Table 8-19 Near-End SONET Path H-byte PMs for the OC-12 Card

Parameter	Definition
Note	On CTC, the count fields for Positive Pointer Justification Count (PPJC) and Negative Pointer Justification Count (NPJC) PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. See Pointer Justification Count Reference, page 8-13.
PPJC-Pdet	Positive Pointer Justification Count path-detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	Negative Pointer Justification Count path-detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	Positive Pointer Justification Count path-generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	Negative Pointer Justification Count path-generated (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 8-20 Near-End Protection-Switching PMs for the OC-12 Card

Parameter	Definition
	<p>For information about Troubleshooting UPSR switch counts, see Chapter 14, “Alarm Troubleshooting.” For information about creating circuits that perform a switch, see Chapter 6, “Circuits and Tunnels.”</p>
PSC (BLSR)	<p>For a protect line in a 2-fiber ring, Protection Switching Count (PSC) refers to the number of times a protection switch has occurred either to a particular span’s line protection or away from a particular span’s line protection. Therefore, if a protection switch occurs on a 2-fiber BLSR, the PSC of the protection span to which the traffic is switched will increment, and when the switched traffic returns to its original working span from the protect span, the PSC of the protect span will increment again.</p> <p>Note 4-fiber BLSR is not supported on the OC-12 card; therefore, the PSC-S and PSC-R PMs do not increment.</p>
PSC (1+1 protection)	<p>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.</p> <p>For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM is only applicable if revertive line-level protection switching is used.</p>
PSD	<p>For an active protection line in a 2-fiber BLSR, Protection Switching Duration (PSD) is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. PSD increments on the active protect line and Protection Switching Duration-Working (PSD-W) increments on the failed working line.</p> <p>Note 4-fiber BLSR is not supported on the OC-12 card; therefore, the Protection Switching Duration-Span (PSD-S), and Protection Switching Duration-Ring (PSD-R) PMs do not increment.</p>
PSC-W	<p>For a working line in a 2-fiber BLSR, Protection Switching Count-Working (PSC-W) is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line and PSC increments on the active protect line.</p>
PSD-W	<p>For a working line in a 2-fiber BLSR, Protection Switching Duration-Working (PSD-W) is a count of the number of seconds that service was carried on the protection line. PSD-W increments on the failed working line and PSD increments on the active protect line.</p>

Table 8-21 Near-End Protection-Switching Path PMs for the OC-12 Card

Parameter	Definition
Note	SONET path PMs will not count unless IPPM is enabled. For additional information, see the “Intermediate-Path Performance Monitoring Reference” section on page 8-12.
STS CV-P	Near-End STS Path Coding Violations (STS CV-P) is a count of B IP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight B IP errors can be detected per frame; each error increments 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 B IP error was detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an STS ES-P.
STS FC-P	Near-End STS Path Failure Counts (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 ERDI-P for that path. The failure event ends when these failures are cleared.
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 B IP 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 Severely Errored Seconds Path (SES-P).
STS UAS-P	Near-End STS Path Unavailable Seconds (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 Severely Errored Seconds Path (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 8-22 Far-End Line Layer PMs for the OC-12 Card

Parameter	Definition
CV-L	Code Violation Line (CV-L) is a count of B IP 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 B IP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 B IP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each B IP error indicated by the incoming REI-L.
ES-L	Errored Seconds Line (ES-L) is a count of the seconds when at least one line-layer B IP error was reported by the far-end LTE or an RDI-L defect was present.
SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer B IP errors were reported by the far-end LTE or an RDI-L defect was present.

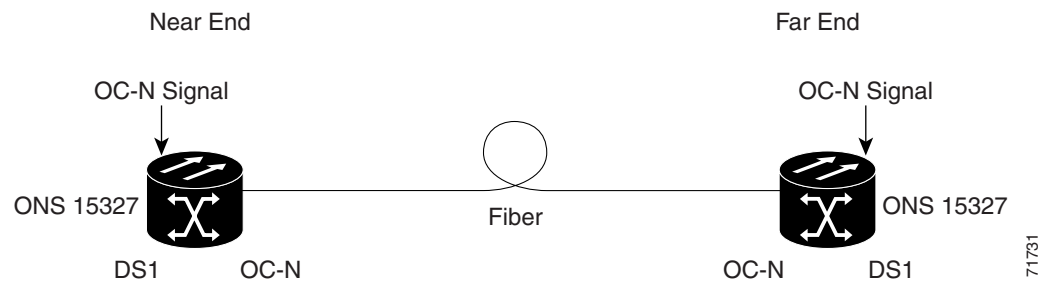
Table 8-22 Far-End Line Layer PMs for the OC-12 Card (continued)

Parameter	Definition
UAS-L	UAS-L 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-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.

8.5.3 OC-48 Card Performance Monitoring Parameters

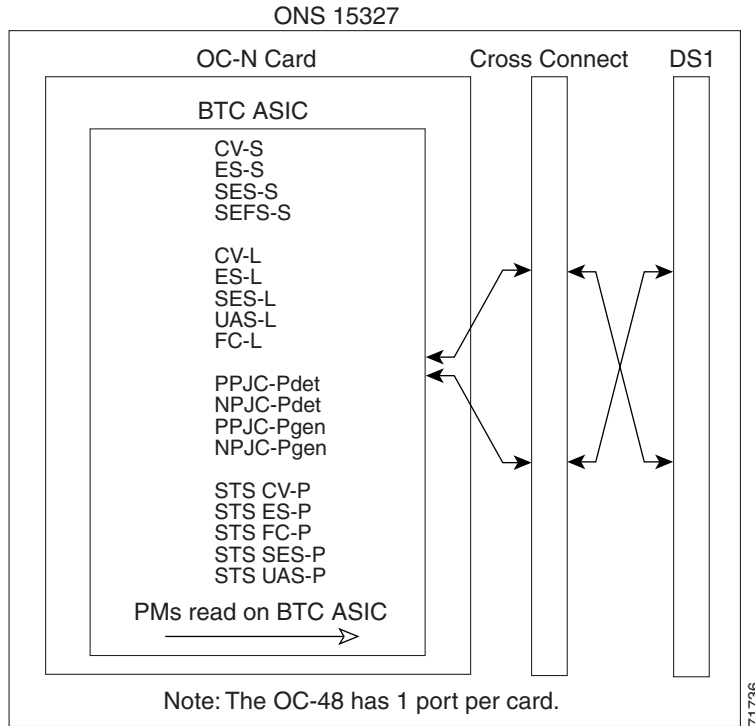
Figure 8-18 shows the signal types that support far-end PMs. Figure 8-19 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC-48 cards.

Figure 8-18 Monitored signal types for the OC-48 cards

**Note**

PMs on the protect STS are not supported for BLSR. The XX in the illustration above represents all PMs listed below with the given prefix and/or suffix.

Figure 8-19 PM read points on the OC-48 cards



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

Table 8-23 Near-End Section PMs for the OC-48 Cards

Parameter	Definition
CV-S	CV-S is a count of B IP errors detected at the section-layer (i.e. using the B1 byte in the incoming SONET signal). Up to eight section B IP 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 B IP error was detected or a Severely Errored Frame (SEF) or Loss of Signal (LOS) defect was present.
SES-S	SES-S is a count of the seconds when K (see GR-253 for value) or more section-layer B IP errors were detected or a Severely Errored Frame (SEF) or Loss of Signal (LOS) defect was present.
SEFS-S	SEFS-S is a count of the seconds when a Severely Errored Frame (SEF) defect was present. An SEF defect is expected to be present during most seconds when a Loss of Signal (LOS) or Loss of Frame (LOF) defect is present. However, there may be situations when the SEFS-S parameter is only incremented based on the presence of an SEF defect.

Table 8-24 Near-End Line Layer PMs for the OC-48 Cards

Parameter	Definition
CV-L	Code Violation Line (CV-L) is a count of B IP errors detected at the line-layer (i.e. using the B2 bytes in the incoming SONET signal). Up to 8 x N B IP errors can be detected per STS-N frame; each error increments the current CV-L second register.
ES-L	Errored Seconds Line (ES-L) is a count of the seconds when at least one line-layer B IP error was detected or an AIS-L defect was present.
SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds when K (see GR-253 for values) or more line-layer B IP 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 Severely Errored Seconds Line (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.

Table 8-25 Near-End SONET Path H-byte PMs for the OC-48 Cards

Parameter	Definition
Note	On CTC, the count fields for Positive Pointer Justification Count (PPJC) and Negative Pointer Justification Count (NPJC) PMs appear white and blank unless they are enabled on the Provisioning > Line tabs. See the "Pointer Justification Count Reference" section on page 8-13.
PPJC-Pdet	Positive Pointer Justification Count path-detected (PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SONET signal.
NPJC-Pdet	Negative Pointer Justification Count path-detected (NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SONET signal.
PPJC-Pgen	Positive Pointer Justification Count path-generated (PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
NPJC-Pgen	Negative Pointer Justification Count path-generated (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 8-26 Near-End Protection-Switching PMs for the OC-48 Cards

Parameter	Definition
	For information about Troubleshooting UPSR switch counts, see Chapter 14, “Alarm Troubleshooting.” For information about creating circuits that perform a switch, see Chapter 6, “Circuits and Tunnels.”
PSC (BLSR)	For a protect line in a 2-fiber ring, Protection Switching Count (PSC) refers to the number of times a protection switch has occurred either to a particular span’s line protection or away from a particular span’s line protection. Therefore, if a protection switch occurs on a 2-fiber BLSR, the PSC of the protection span to which the traffic is switched will increment, and when the switched traffic returns to its original working span from the protect span, the PSC of the protect span will increment again.
PSC (1+1 protection)	In a 1+1 protection scheme for a working card, PSC is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM is only applicable if revertive line-level protection switching is used.
PSD	For an active protection line in a 2-fiber BLSR, Protection Switching Duration (PSD) is a count of the number of seconds that the protect line is carrying working traffic following the failure of the working line. PSD increments on the active protect line and Protection Switching Duration-Working (PSD-W) increments on the failed working line.
PSC-W	For a working line in a 2-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 2-fiber BLSR, PSD-W is a count of the number of seconds that service was carried on the protection line. Protection Switching Duration-Working (PSD-W) increments on the failed working line and PSD increments on the active protect line.

Table 8-27 Near-End SONET Path PMs for the OC-48 Cards

Parameter	Definition
Note	SONET path PMs will not count unless IPPM is enabled. For additional information, see the “Intermediate-Path Performance Monitoring Reference” section on page 8-12.
STS CV-P	Near-End STS Path Coding Violations (STS CV-P) is a count of B IP errors detected at the STS path layer (i.e., using the B3 byte). Up to eight B IP errors can be detected per frame; each error increments 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 B IP 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.

Table 8-27 Near-End SONET Path PMs for the OC-48 Cards (continued)

Parameter	Definition
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 with an AIS-P failure, an LOP-P failure, a UNEQ-P failure or a TIM-P failure is declared, or if the STS PTE that is monitoring the path supports ERDI-P for that path. The failure event ends when these failures are cleared.
STS SES-P	Near-End STS Path Severely Errored Seconds (STS SES-P) is a count of the seconds when K (2400) or more STS path B IP 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 Severely Errored Seconds Path (SES-P).
STS UAS-P	Near-End STS Path Unavailable Seconds (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 Severely Errored Seconds Path (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 8-28 Far-End Line Layer PMs for the OC-48 Cards

Parameter	Definition
CV-L	Code Violation Line (CV-L) is a count of B IP 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 B IP errors per STS-N frame can be indicated using the REI-L. For OC-48 signals, up to 255 B IP errors per STS-N frame can be indicated. The current CV-L second register is incremented for each B IP error indicated by the incoming REI-L.
ES-L	Errored Seconds Line (ES-L) is a count of the seconds when at least one line-layer B IP error was reported by the far-end LTE or an RDI-L defect was present.
SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds when K (see GR-253-CORE for values) or more line-layer B IP 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.



Ethernet Operation

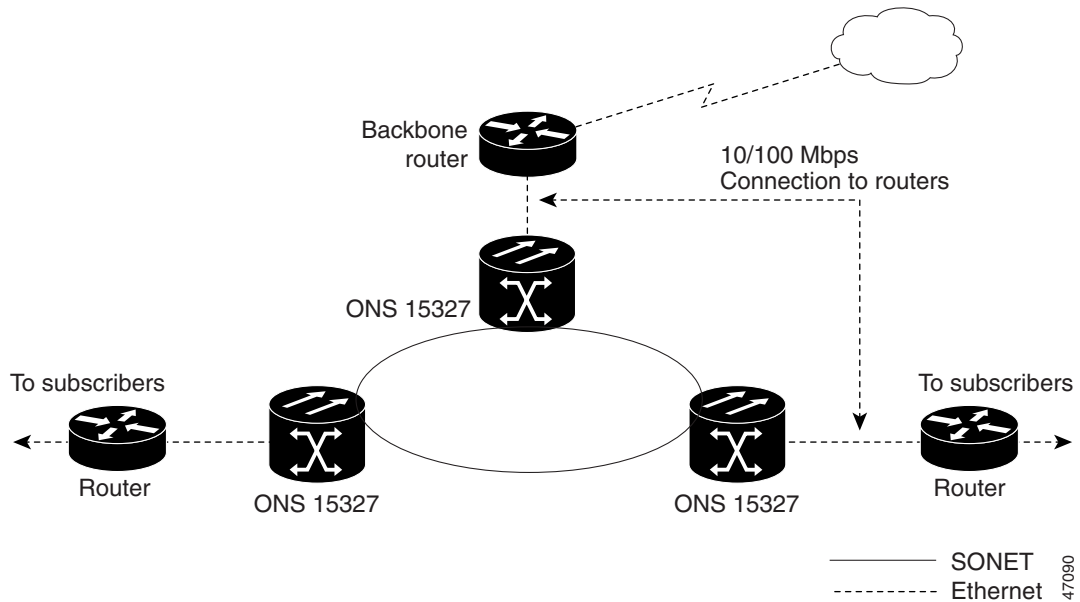
This chapter explains how to use the Ethernet features of the Cisco ONS 15327, including transporting ONS 15327 Ethernet data over SONET, creating and provisioning VLANs, protecting Ethernet traffic with Spanning Tree Protocol (STP), provisioning Multicard and Single-card EtherSwitch, provisioning several types of Ethernet circuits, viewing Ethernet performance data stored in CTC, creating Ethernet Remote Monitoring (RMON) alarm thresholds, and troubleshooting Ethernet connections.

9.1 Ethernet over SONET Application

The ONS 15327 integrates Ethernet access into the same SONET platform that transports voice traffic. Ethernet over SONET lets service providers augment time division multiplexing (TDM) services with Ethernet, and allows users to deliver data traffic over existing facilities. The ONS 15327 supports layer 2 switching and the ability to classify Ethernet traffic as defined in the IEEE 802.1Q standard. You can switch tagged traffic onto separate SONET STS channels to allocate bandwidth by traffic class. The ONS 15327 can also concentrate Ethernet ports into one or more STS-N circuits to use bandwidth more efficiently.

The ONS 15327 Ethernet solution uses existing SONET infrastructure to transport aggregate (combined) traffic from multiple, remote sources. Figure 9-1 illustrates aggregation and transport.

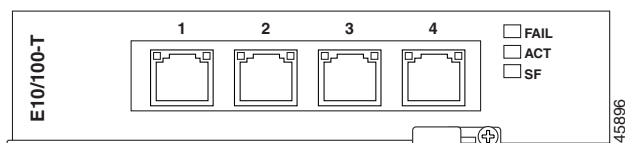
Figure 9-1 Ethernet transporting aggregate traffic from multiple sources



9.2 ONS 15327 Ethernet Card

The ONS 15327 uses the E10/100-4 Ethernet card to provide Ethernet interfaces. Figure 9-2 shows the E10/100-4 Ethernet card faceplate. For a detailed description of the E10/100-4 card, refer to Chapter 13, “Card Reference.”

Figure 9-2 E10/100-4 Ethernet card faceplate



The E10/E100-4 has a bi-color LED on both sides of each of the four RJ-45 connectors. Each pair of LEDs shows the port's state. LED states are listed in Table 9-1.

Table 9-1 E10/1004 faceplate LEDs

LED State – Left and Right	Description
Green and Amber	Transmitting/Receiving
Green and Off	Idle and Link Integrity

The ONS 15327 uses E10/100-4 cards for Ethernet (10 Mbps) and Fast Ethernet (100 Mbps). The E10/100-4 enables network operators to provide multiple 10/100-Mbps access drops for high-capacity customer LAN interconnections. The card provides efficient transport and coexistence of traditional TDM traffic with packet-switched data traffic. The E10/100-4 helps eliminate the need for external Ethernet aggregation equipment.

E10/100-4 specifications:

- Operating temperature: 32 to 131 degrees Fahrenheit (0 to +55 degrees Celsius)
- Operating humidity: 5 to 95% non-condensing
- Power consumption: 30 Watts

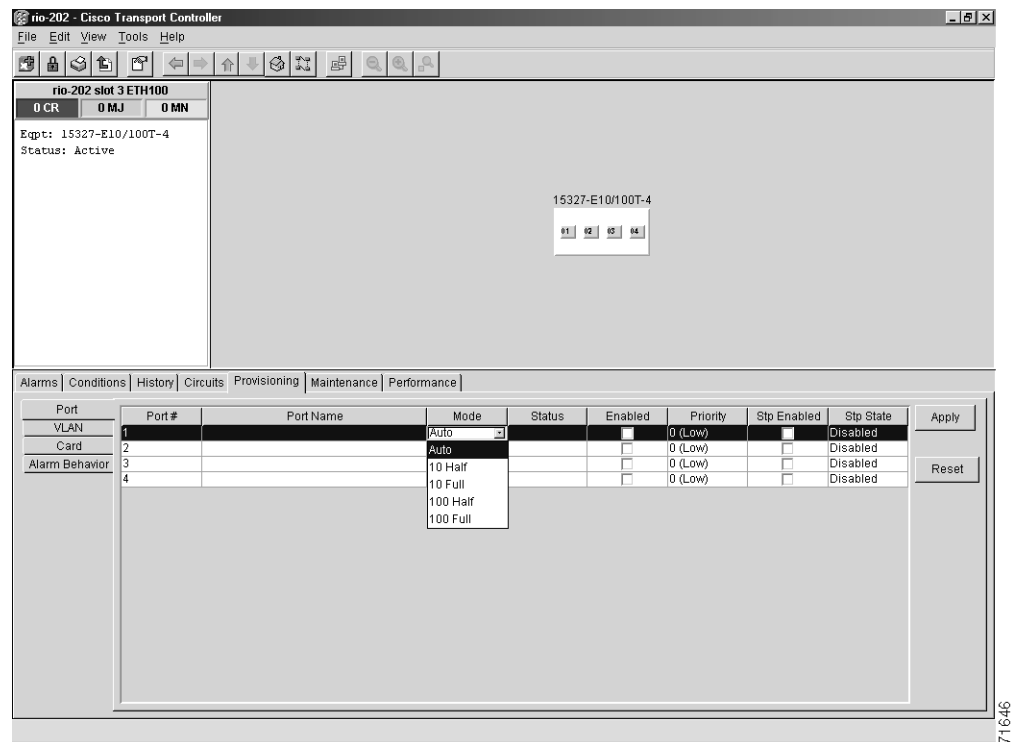
9.2.1 E10/100-4 Card Port Provisioning

This section explains how to provision Ethernet ports on an E10/100-4 Ethernet card. Most provisioning requires you to fill in two fields: Enabled and Mode. However, you can also map incoming traffic to a low priority or a high priority queue using the Priority column, and you can enable spanning tree with the Stp Enabled column. For more information about spanning tree, see the “Spanning Tree (IEEE 802.1D)” section on page 9-26. The Status column displays information about the port’s current operating mode, and the Stp State column provides the current spanning tree status.

Procedure: Provision E10/100-4 Ethernet Ports

- Step 1** In card view, click the **Provisioning > Port** tabs. Figure 9-3 shows the Provisioning tab with the Port function subtab selected.

Figure 9-3 Provisioning E10/100-4 Ethernet ports



- Step 2** From the Port tab, choose the appropriate mode for each Ethernet port. Valid choices for the E10/100-4 card are Auto, 10 Half, 10 Full, 100 Half, or 100 Full.
- Step 3** Click the **Enabled** check box(es) to activate the corresponding Ethernet port(s).

Step 4 Click **Apply**.

Your Ethernet ports are now provisioned and ready to be configured for VLAN membership.

Step 5 Repeat this procedure for all other cards that will be in the VLAN.

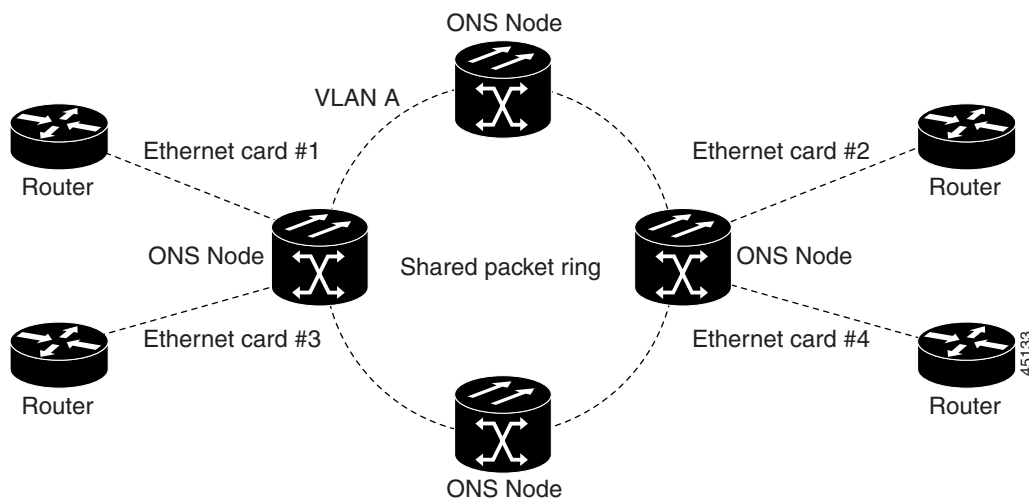
9.3 Multicard and Single-Card EtherSwitch

The ONS 15327 enables Multicard and Single-card EtherSwitch modes. At the Ethernet card view in CTC, click the **Provisioning > Card** tabs to reveal the Card Mode option.

9.3.1 Multicard EtherSwitch

Multicard EtherSwitch provisions two or more Ethernet cards to act as a single layer 2 switch. It supports one STS-3c circuit or three STS-1 shared packet rings. The bandwidth of the single switch formed by the Ethernet cards matches the bandwidth of the provisioned Ethernet circuit up to STS-3c worth of bandwidth. Figure 9-4 illustrates a Multicard EtherSwitch configuration.

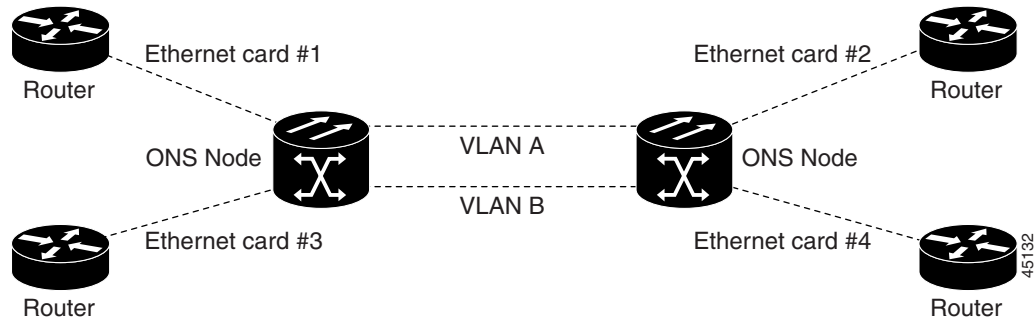
Figure 9-4 A Multicard EtherSwitch configuration



9.3.2 Single-Card EtherSwitch

Single-card EtherSwitch allows each Ethernet card to remain a single switching entity within the ONS 15327 shelf. This option allows a full STS-12c worth of bandwidth between two Ethernet circuit points. Figure 9-5 illustrates a Single-card EtherSwitch configuration.

Figure 9-5 A Single-card EtherSwitch configuration



Seven scenarios exist for provisioning Single-card EtherSwitch bandwidth:

1. STS 12c
2. STS 6c + STS 6c
3. STS 6c + STS 3c + STS 3c
4. STS 6c + 6 STS-1s
5. STS 3c + STS 3c + STS 3c + STS 3c
6. STS 3c + STS 3c + 6 STS-1s
7. 12 STS-1s

**Note**

You cannot provision a mixed Ethernet STS circuit on a single (unstiched) card.

9.3.3 ONS 15454 E Series and ONS 15327 EtherSwitch Circuit Combinations

Table 9-2 shows the Ethernet circuit combinations available in the ONS 15327 E10/100-4 cards and ONS 15454 E series cards.

Table 9-2 ONS 15454 and ONS 15327 Ethernet Circuit Combinations

15327 Single-Card	15327 Multicard	15454 E Series Single-Card	15454 E Series Multicard
six STS-1s	three STS-1s	one STS 12c	six STS-1s
two STS 3cs	one STS 3c	two STS 6cs	two STS 3cs
one STS 6c		one STS 6c and two STS 3cs	one STS 6c
one STS 12c		one STS 6c and six STS-1s	
		four STS 3cs	
		two STS 3cs and six STS-1s	
		twelve STS-1s	

9.4 Ethernet Circuit Configurations

Ethernet circuits can link ONS nodes through point-to-point, shared packet ring, or hub and spoke configurations. Two nodes usually connect with a point-to-point configuration. More than two nodes usually connect with a shared packet ring configuration or a hub and spoke configuration. This section includes procedures for creating these configurations and also explains how to create Ethernet manual cross-connects. Ethernet manual cross-connects allow you to cross connect individual Ethernet circuits to an STS channel on the ONS 15327 optical interface and also to bridge non-ONS SONET network segments.


Note

Before making Ethernet connections, choose a STS-1, STS-3c, STS-6c, or STS-12c circuit size.


Note

When making an STS-6c or STS-12c Ethernet circuit, Ethernet cards must be configured as Single-card EtherSwitch. Multicard mode does not support STS-6c or STS-12c Ethernet circuits.

9.4.1 Point-to-Point Ethernet Circuits

The ONS 15327 can set up a point-to-point (straight) Ethernet circuit as Single-card or Multicard. Multicard EtherSwitch limits bandwidth to STS-3c of bandwidth between two Ethernet circuit points, but allows you to add nodes and cards and make a shared packet ring. Single-card EtherSwitch allows a full STS-12c of bandwidth between two Ethernet circuit points. Figure 9-6 shows a Multicard EtherSwitch point-to-point circuit. Figure 9-7 shows a Single-card EtherSwitch point-to-point circuit.

Figure 9-6 Multicard EtherSwitch point-to-point circuit

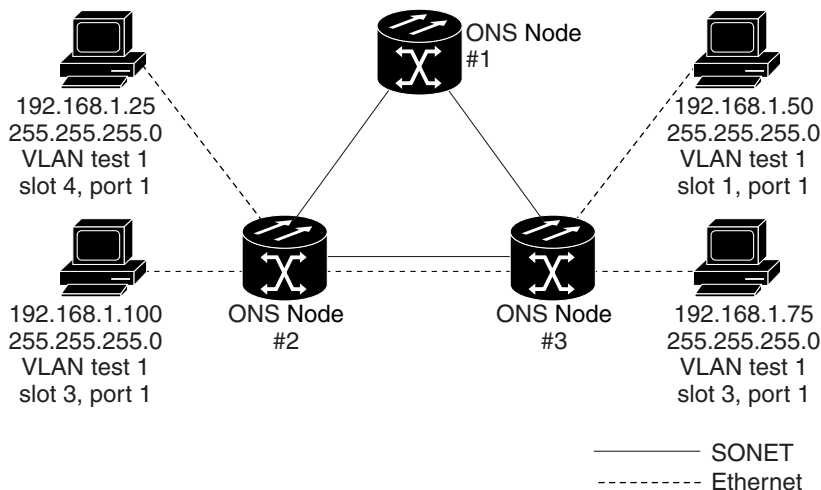
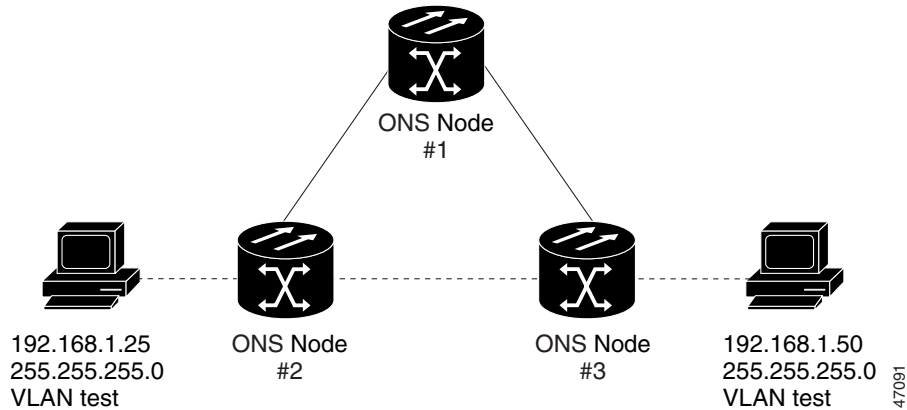


Figure 9-7 Single-card EtherSwitch point-to-point circuit



Procedure: Provision an EtherSwitch Point-to-Point Circuit (Multicard or Single-Card)

- Step 1** Display CTC for one of the ONS 15327 Ethernet circuit endpoint nodes.
- Step 2** Double-click one of the Ethernet cards that will carry the circuit.
- Step 3** Click the **Provisioning > Card** tabs.
- Step 4** If you are building a Multicard EtherSwitch point-to-point circuit:
- Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.
 - If **Multi-card EtherSwitch Group** is not checked, check it and click **Apply**.
 - Repeat Steps 2–4 for all other Ethernet cards in the ONS 15327 that will carry the circuit.

If you are building a Single-card EtherSwitch circuit:

- Under Card Mode, verify that **Single-card EtherSwitch** is checked.
 - If **Single-card EtherSwitch** is not checked, check it and click **Apply**.
- Step 5** Navigate to the other ONS 15327 Ethernet circuit endpoint.

Step 6 Repeat Steps 2–5.

Step 7 Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box appears.

Step 8 In the Name field, type a name for the circuit.

Step 9 From the Type pull-down menu, choose **STS**.



Note

The VT and VT Tunnel types do not apply to Ethernet circuits.

Step 10 Choose the size of the circuit from the Size pull-down menu.

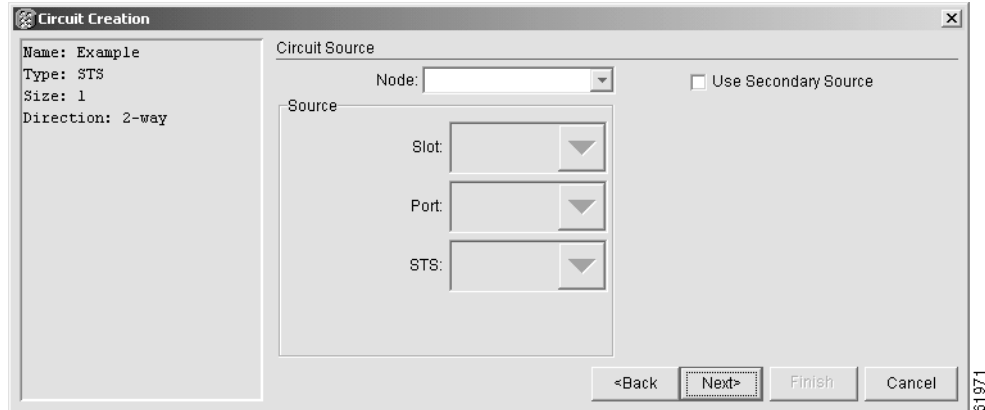
The valid circuit sizes for an Ethernet Multicard circuit are STS-1 and STS-3c.

The valid circuit sizes for an Ethernet Single-card circuit are STS-1, STS-3c, STS-6c and STS-12c.

Step 11 Verify that the **Bidirectional** check box is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box appears (Figure 9-8).

Figure 9-8 Choosing a circuit source



- Step 12** Choose the circuit source from the Node menu. Either end node can be the circuit source.
- Step 13** If you are building a Multicard EtherSwitch circuit, choose **Ethergroup** from the Slot menu and click **Next**.
- Step 14** If you are building a Single-card EtherSwitch circuit, from the Slot menu choose the Ethernet card where you enabled the Single-card EtherSwitch and click **Next**.

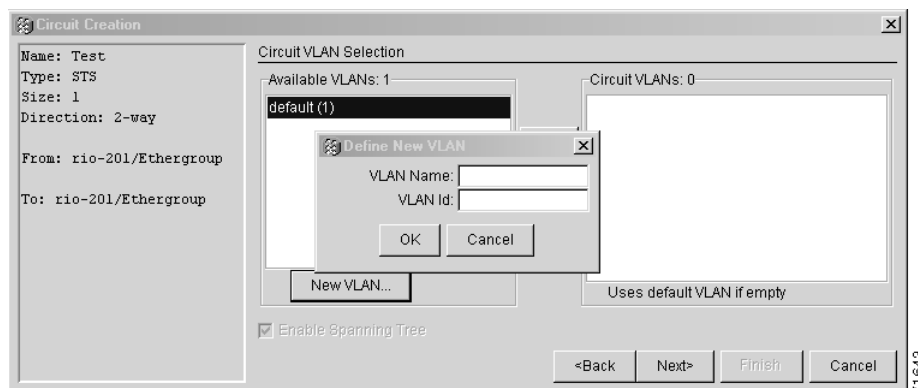
The Circuit Creation (Destination) dialog box opens.

- Step 15** Choose the circuit destination from the Node menu. Choose the node that is not the source.
- Step 16** If you are building a Multicard EtherSwitch circuit, choose **Ethergroup** from the Slot menu and click **Next**.
- Step 17** If you are building a **Single-card EtherSwitch** circuit, from the Slot menu choose the Ethernet card for which you enabled the Single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box appears.

- Step 18** Create the VLAN:
- Click the **New VLAN** tab.
 - Assign an easily identifiable name to your VLAN (Figure 9-9).

Figure 9-9 Choosing a VLAN name and ID



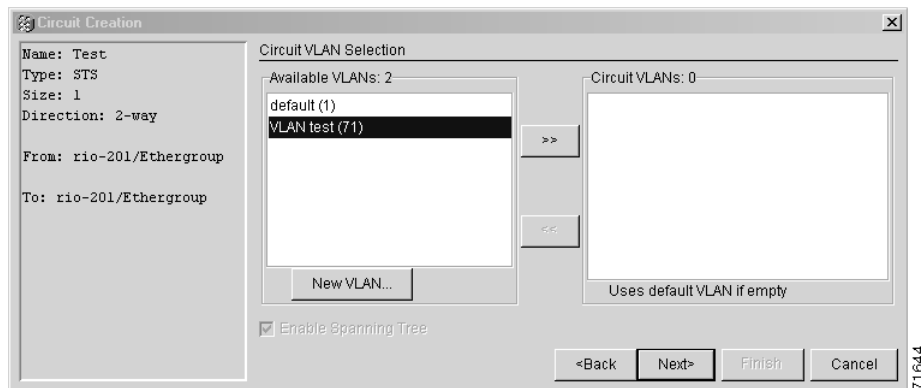
- Assign a VLAN ID.



Note The VLAN ID should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

- d. Click **OK**.
- e. Highlight the VLAN name and click the >> button to move the available VLAN to the Circuit VLANs column (Figure 9-10).

Figure 9-10 Selecting VLANs



Step 19 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box appears.

Step 20 Confirm that the following information about the point-to-point circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs on the circuit
- ONS 15327 nodes included in the circuit

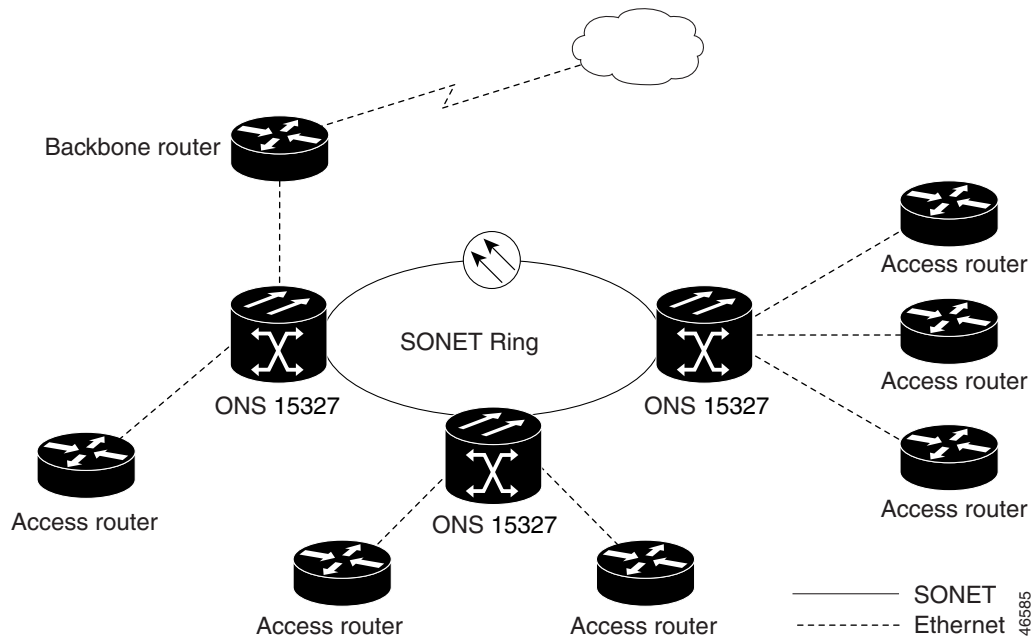
Step 21 Click **Finish**.

Step 22 You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the “Provision E10/100-4 Ethernet Ports” procedure on page 9-3. For instructions about assigning ports to VLANs, see the “Provision Ethernet Ports for VLAN Membership” procedure on page 9-25. For information about manually provisioning circuits, see the “Ethernet Manual Cross-Connects” section on page 9-16.


9.4.2 Shared Packet Ring Ethernet Circuits

This section provides steps for creating a shared packet ring (Figure 9-11). Your network architecture may differ from the example.

Figure 9-11 Shared packet ring Ethernet circuit



Procedure: Provision a Shared Packet Ring

- Step 1** Display CTC for one of the ONS 15327 Ethernet circuit endpoints.
 - Step 2** Double-click one of the Ethernet cards that will carry the circuit.
 - Step 3** Click the **Provisioning > Card** tabs.
 - Step 4** Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.
 - Step 5** If **Multi-card EtherSwitch Group** is not checked, check it and click **Apply**.
 - Step 6** Display the node view.
 - Step 7** Repeat Steps 2–6 for all other Ethernet cards in the ONS 15327 that will carry the shared packet ring.
 - Step 8** Navigate to the other ONS 15327 endpoint.
 - Step 9** Repeat Steps 2–7.
 - Step 10** Click the **Circuits** tab and click **Create**.
The Circuit Creation (Circuit Attributes) dialog box appears.
 - Step 11** In the Name field, type a name for the circuit.
 - Step 12** From the Type pull-down menu, choose **STS**.
-  **Note** The VT and VT Tunnel types do not apply to Ethernet circuits.
- Step 13** From the Size pull-down menu, choose the size of the circuit.
For shared packet ring Ethernet, valid circuit sizes are STS-1 and STS-3c.
 - Step 14** Verify that the **Bidirectional** check box is checked.



Note If you are building a shared packet ring configuration, you must manually provision the circuits.

Step 15 Click **Next**.

The Circuit Creation (Circuit Source) dialog box appears.

Step 16 From the Node menu, choose the circuit source.

Any shared packet ring node can serve as the circuit source.

Step 17 Choose **Ethergroup** from the Slot menu and click **Next**.

The Circuit Creation (Circuit Destination) dialog box appears.

Step 18 Choose the circuit destination from the Node menu.

Step 19 Except for the source node, any shared packet ring node can serve as the circuit destination.

Step 20 Choose **Ethergroup** from the Slot menu and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box appears.

Step 21 Create the VLAN:

- a. Click the **New VLAN** tab.

The Circuit Creation (Define New VLAN) dialog box appears (Figure 9-9).

- b. Assign an easily identifiable name to your VLAN.
- c. Assign a VLAN ID.

This VLAN ID number must be unique. It is usually the next available number not already assigned to an existing VLAN (between 2 and 4093). Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

- d. Click **OK**.
- e. Highlight the VLAN name and click the >> button to move the VLAN from the Available VLANs column to the Circuit VLANs column (Figure 9-10).

By moving the VLAN from the Available VLANs column to the Circuit VLANs column, all the VLAN traffic is forced to use the shared packet ring circuit you created.

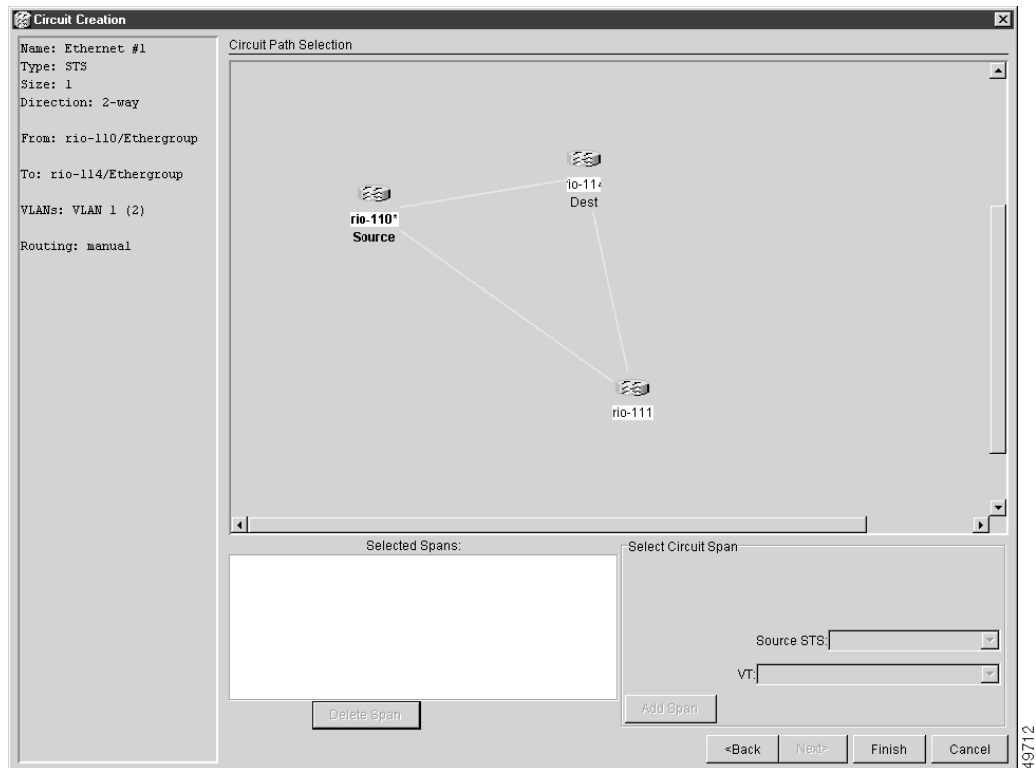
Step 22 Click **Next**.

Step 23 Uncheck the **Route Automatically** check box and click **Next**.

Step 24 Click either span (green arrow) leading from the source node (Figure 9-12).

The span turns white.

Figure 9-12 Adding a span

**Step 25** Click **Add Span**.

The span turns blue and the span is added to the Included Spans field.

Step 26 Click the node at the end of the blue span.**Step 27** Click the green span leading to the next node.

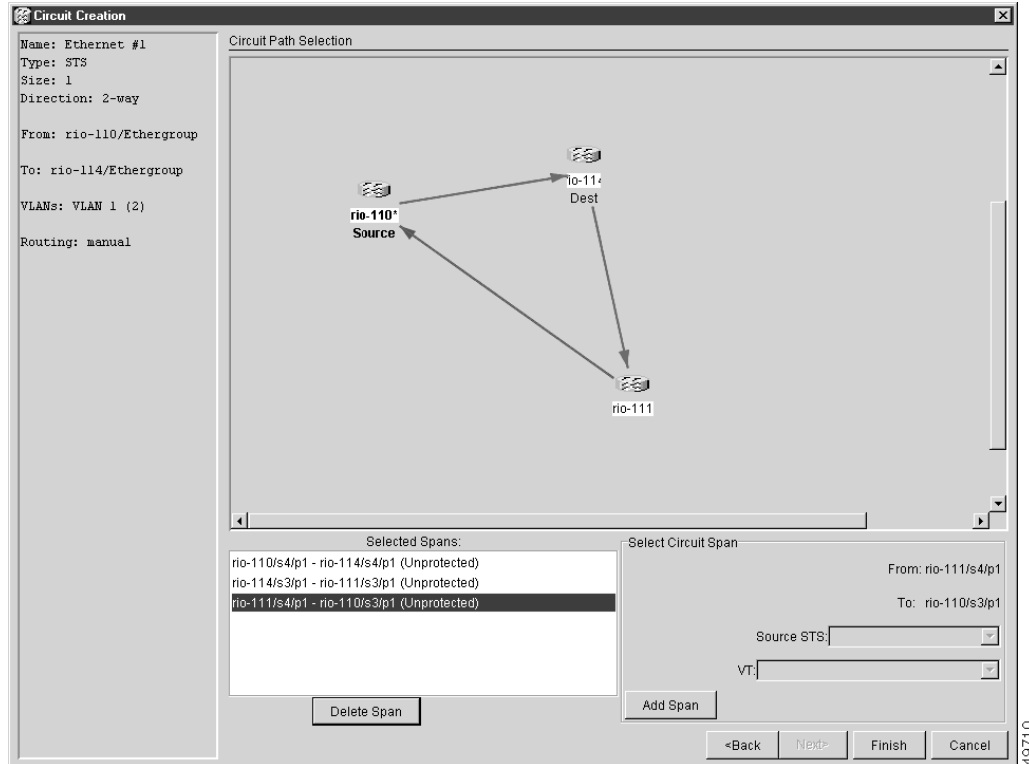
The span turns white.

Step 28 Click **Add Span**.

The span turns blue.

Step 29 Repeat Steps 24–28 for every node remaining in the ring. Figure 9-13 shows the Circuit Path Selection dialog box with all the spans selected.

Figure 9-13 Viewing a span



Step 30 Verify that the new circuit is correctly configured.



Note If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information. You can also click **Finish**, delete the completed circuit, and begin the procedure again.

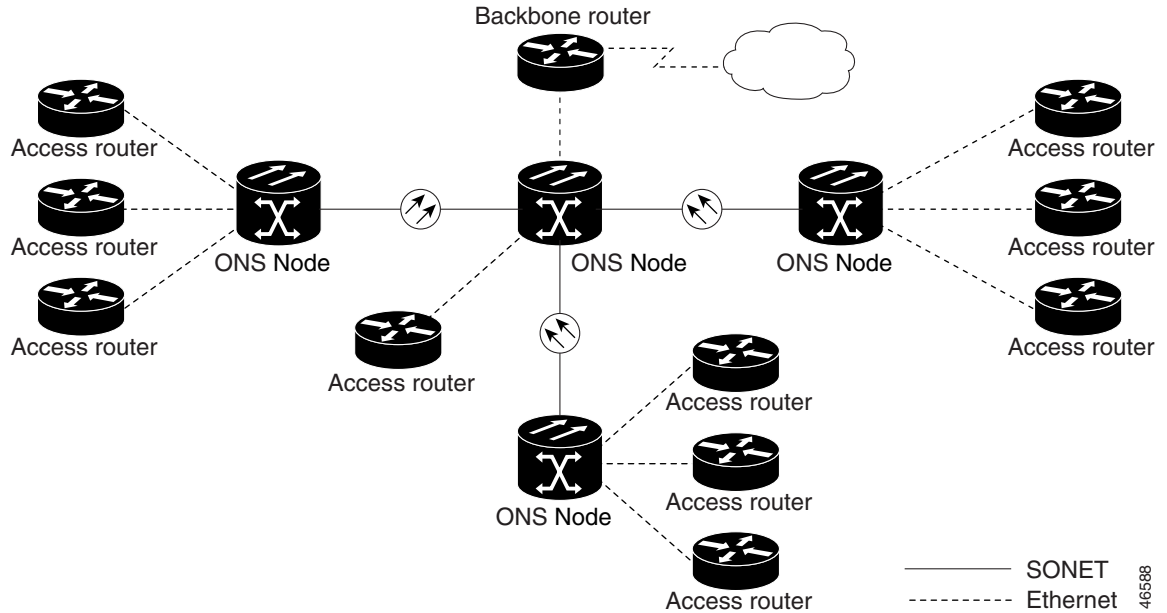
Step 31 Click **Finish**.

Step 32 You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the “Provision E10/100-4 Ethernet Ports” procedure on page 9-3. For instructions about assigning ports to VLANs, see the “Provision Ethernet Ports for VLAN Membership” procedure on page 9-25.

9.4.3 Hub and Spoke Ethernet Circuit Provisioning

This section provides steps for creating a hub and spoke Ethernet circuit configuration. The hub and spoke configuration connects point-to-point circuits (the spokes) to an aggregation point (the hub). In many cases, the hub links to a high-speed connection and the spokes are Ethernet cards. Figure 9-14 illustrates a sample hub and spoke ring. Your network architecture may differ from the example.

Figure 9-14 A Hub and spoke Ethernet circuit



Procedure: Provision a Hub and Spoke Ethernet Circuit

- Step 1** Display CTC for one of the ONS 15327 Ethernet circuit endpoints.
- Step 2** Double-click the Ethernet card that will create the circuit.
- Step 3** Click the **Provisioning > Card** tabs.
- Step 4** Under Card Mode, check the **Single-card EtherSwitch** check box.
If **Single-card EtherSwitch** is not checked, check it and click **Apply**.
- Step 5** Navigate to the other ONS 15327 endpoint and repeat Steps 2–4.
- Step 6** Display the node view or network view.
- Step 7** Click the **Circuits** tab and click **Create**.
The Circuit Creation (Circuit Attributes) dialog box appears.
- Step 8** In the Name field, type a name for the circuit.
- Step 9** From the Type pull-down menu, choose **STS**.



Note The types VT and VT Tunnel do not apply to Ethernet circuits.

- Step 10** Choose the size of the circuit from the Size pull-down menu.
- Step 11** Verify that the **Bidirectional** check box is checked and click **Next**.
The Circuit Creation (Circuit Source) dialog box appears.
- Step 12** From the Node menu, choose the circuit source.
Either end node can be the circuit source.

Step 13 From the Slot menu, choose the Ethernet card where you enabled the Single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit Destination) dialog box appears.

Step 14 Choose the circuit destination from the Node menu.

Choose the node that is not the source.

Step 15 From the Slot menu, choose the Ethernet card where you enabled the Single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box appears (Figure 9-8 on page 9-8).

Step 16 Create the VLAN:

- a. Click the **New VLAN** tab.

The Circuit Creation (Define New VLAN) dialog box appears (Figure 9-10 on page 9-9).

- b. Assign an easily identifiable name to your VLAN.
- c. Assign a VLAN ID.

This should be the next available number (between 2 and 4093) not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

- d. Click **OK**.
- e. Highlight the VLAN name and click the >> button to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-10 on page 9-9).

Step 17 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box appears.

Step 18 Confirm that the following information about the point-to-point circuit is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs that will be transported across this circuit
- ONS 15327 nodes included in this circuit



Note If the circuit information is not correct, click the **Back** button and repeat the procedure with the correct information. You can also click **Finish**, delete the completed circuit, and start the procedure from the beginning.

Step 19 Click **Finish**. You must now provision the second circuit and attach it to the already-created VLAN.

Step 20 Log into the ONS 15327 Ethernet circuit endpoint for the second circuit.

Step 21 Double-click the Ethernet card that will create the circuit. The CTC card view displays.

Step 22 Click the **Provisioning > Card** tabs.

Step 23 Under Card Mode, check **Single-card EtherSwitch**.

If the **Single-card EtherSwitch** check box is not checked, check it and click **Apply**.

Step 24 Log into the other ONS 15327 endpoint for the second circuit and repeat Steps 21–23.

Step 25 Display the CTC node view.

Step 26 Click the **Circuits** tab and click **Create**.

Step 27 Choose **STS** from the Type pull-down menu.



Note The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 28 From the Size pull-down menu, choose the size of the circuit.

Step 29 Verify that the **Bidirectional** check box is checked and click **Next**.

Step 30 Choose the circuit source from the Node menu and click **Next**.

Either end node can be the circuit source.

Step 31 Choose the circuit destination from the Node menu.

Choose the node that is not the source.

Step 32 From the Slot menu, choose the Ethernet card where you enabled the Single-card EtherSwitch and click **Next**.

The Circuit Creation (Circuit VLAN Selection) dialog box appears.

Step 33 Highlight the VLAN that you created for the first circuit and click the >> tab to move the VLAN(s) from the Available VLANs column to the Selected VLANs column.

Step 34 Click **Next** and click **Finish**.

Step 35 You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the “Provision E10/100-4 Ethernet Ports” procedure on page 9-3. For instructions about assigning ports to VLANs, see the “Provision Ethernet Ports for VLAN Membership” procedure on page 9-25.

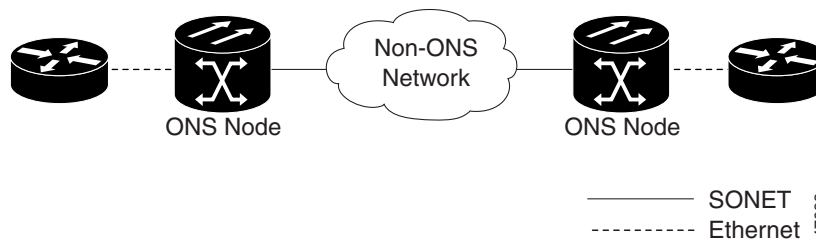
9.4.4 Ethernet Manual Cross-Connects

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 riding through the non-ONS network. This allows an Ethernet circuit to run from ONS node to ONS node utilizing the non-ONS network.



Note Provisioning manual cross-connects for Multicard EtherSwitch circuits is a separate procedure from provisioning manual cross-connects for Single-card EtherSwitch circuits. Both procedures follow.

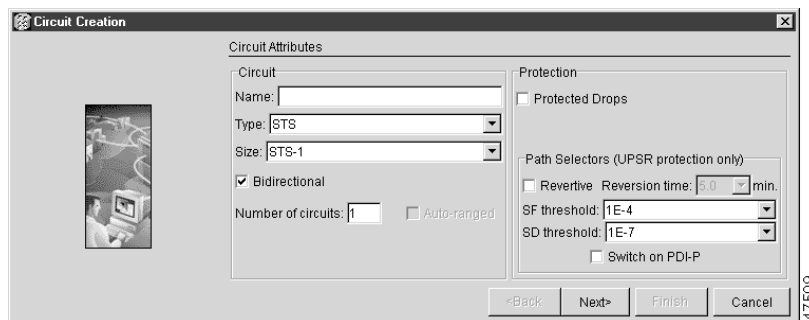
Figure 9-15 Ethernet manual cross-connects



Procedure: Provision a Single-card EtherSwitch Manual Cross-Connect

- Step 1** Display CTC for one of the ONS 15327 Ethernet circuit endpoints.
- Step 2** Double-click one of the Ethernet cards that will carry the circuit.
- Step 3** Click the **Provisioning > Card** tabs.
- Step 4** Under Card Mode, verify that **Single-card EtherSwitch** is checked.
If the **Single-card EtherSwitch** is not checked, check it and click **Apply**.
- Step 5** Display the node view.
- Step 6** Click the **Circuits** tab and click **Create**.
The Circuit Creation (Circuit Attributes) dialog box appears (Figure 9-16).

Figure 9-16 Creating an Ethernet circuit



- Step 7** In the Name field, type a name for the circuit.
- Step 8** From the Type pull-down menu, choose **STS**.



Note The types VT and VT Tunnel do not apply to Ethernet circuits.

- Step 9** Choose the size of the circuit from the Size pull-down menu.
The valid circuit sizes for an Ethernet Single-card circuit are STS-1, STS-3c, STS-6c and 12c.
- Step 10** Verify that the **Bidirectional** check box is checked and click **Next**.
The Circuit Creation (Circuit Source) dialog box appears.
- Step 11** From the Node menu, choose the current node as the circuit source.
- Step 12** From the Slot menu, choose the Ethernet card that will carry the circuit and click **Next**.
The Circuit Creation (Circuit Destination) dialog box appears.
- Step 13** From the Node menu, choose the current node as the circuit destination.
- Step 14** From the Slot menu, choose the optical card that will carry the circuit.
- Step 15** Choose the STS that will carry the circuit from the STS menu and click **Next**.



Note For Ethernet manual cross-connects, the same node serves as both source and destination.

The Circuit Creation (Circuit VLAN Selection) dialog box appears (Figure 9-10 on page 9-9).

Step 16 Create the VLAN:

- a. Click the **New VLAN** tab.

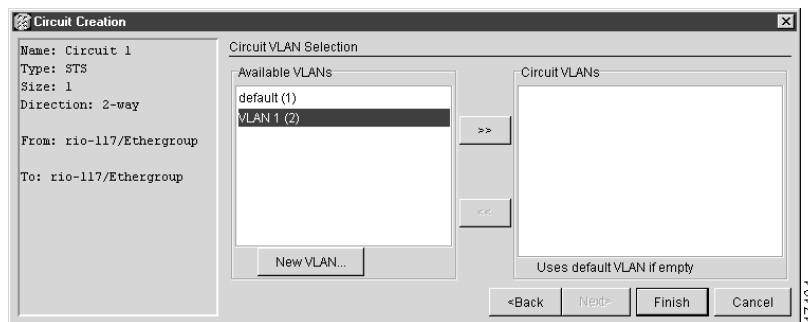
The Circuit Creation (Define New VLAN) dialog box appears (Figure 9-10 on page 9-9).

- b. Assign an easily identifiable name to your VLAN.
- c. Assign a VLAN ID.

The VLAN ID should be the next available number (between 2 and 4093) that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.

- d. Click **OK**.
- e. Highlight the VLAN name and click the arrow >> button to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-17).

Figure 9-17 Selecting VLANs

**Step 17** Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box appears.

Step 18 Confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs on this circuit
- ONS 15327 nodes included in this circuit



Note If the circuit information is not correct, click the Back button and repeat the procedure with the correct information. You can also click Finish, delete the completed circuit and start the procedure from the beginning.

Step 19 Click **Finish**.

Step 20 You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the “Provision E10/100-4 Ethernet Ports” procedure on page 9-3. For information about assigning ports to VLANs, see the “Provision Ethernet Ports for VLAN Membership” procedure on page 9-25.

Step 21 After assigning the ports to the VLANs, repeat Steps 1–19 at the second ONS 15327 Ethernet manual cross-connect endpoint.

**Note**

The appropriate STS circuit must exist in the non-ONS 15327 equipment to connect the two STSs from the ONS 15327 Ethernet manual cross-connect endpoints.

**Caution**

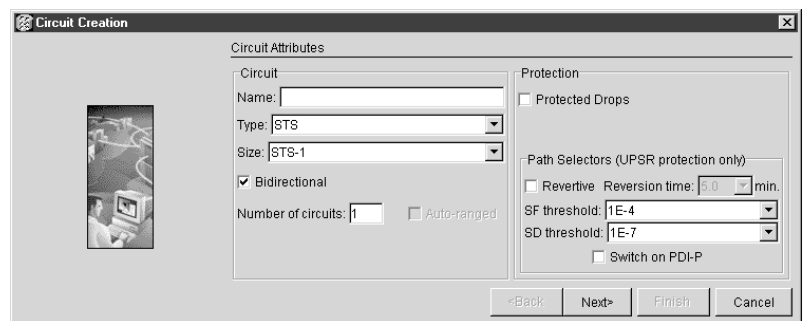
If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross-connect, the two Ethernet circuits may have a circuit-size mismatch. For example, a circuit size of STS-3c might have been configured on the first ONS 15327 and circuit size of STS-12c might have been configured on the second ONS 15327. To troubleshoot this occurrence of the CARLOSS alarm, refer to Chapter 14, “Alarm Troubleshooting”.

Procedure: Provision a Multicard EtherSwitch Manual Cross-Connect

- Step 1** Display CTC for one of the ONS 15327 Ethernet circuit endpoints.
- Step 2** Double-click one of the Ethernet cards that will carry the circuit.
- Step 3** Click the **Provisioning > Card** tabs.
- Step 4** Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.
If the **Multi-card EtherSwitch Group** is not checked, check it and click **Apply**.
- Step 5** Display the node view.
- Step 6** Repeat Steps 2–5 for any other Ethernet cards in the ONS 15327 that will carry the circuit.
- Step 7** Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box appears (Figure 9-18).

Figure 9-18 *Creating an Ethernet circuit*



- Step 8** In the Name field, type a name for the circuit.
- Step 9** From the Type pull-down menu, choose **STS**.

**Note**

The types VT and VT Tunnel do not apply to Ethernet circuits.

- Step 10** Choose the size of the circuit from the Size pull-down menu.
The valid circuit sizes for an Ethernet Multicard circuit are STS-1 and STS-3c.

- Step 11** Verify that the **Bidirectional** check box is checked and click **Next**.
The Circuit Creation (Circuit Source) dialog box appears.
- Step 12** From the Node menu, choose the current node as the circuit source.
- Step 13** Choose **Ethergroup** from the Slot menu and click **Next**.
The Circuit Creation (Circuit Destination) dialog box appears.
- Step 14** From the Node menu, choose the current node as the circuit destination.
- Step 15** Choose Ethergroup from the Slot menu and click **Next**.

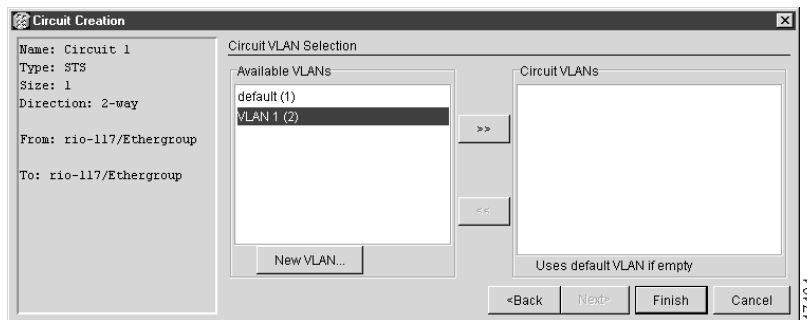


Note For the Ethernet manual cross-connect, the destination and source should be the same node.

The Circuit Creation (Circuit VLAN Selection) dialog box appears (Figure 9-10 on page 9-9).

- Step 16** Create the VLAN:
- Click the **New VLAN** tab.
The Circuit Creation (Define New VLAN) dialog box opens (Figure 9-9 on page 9-8).
 - Assign an easily identifiable name to your VLAN.
 - Assign a VLAN ID.
The VLAN ID should be the next available number (between 2 and 4093) that is not already assigned to an existing VLAN. Each ONS 15327 network supports a maximum of 509 user-provisionable VLANs.
 - Click **OK**.
 - Highlight the VLAN name and click the arrow **>>** button to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 9-19).

Figure 9-19 Selecting VLANs



- Step 17** Click **Next**.
The Circuit Creation (Circuit Routing Preferences) dialog box appears.
- Step 18** Confirm that the following information is correct:
- Circuit name
 - Circuit type
 - Circuit size
 - VLANs on this circuit

- ONS 15327 nodes included in this circuit



Note If the circuit information is not correct, click the Back button and repeat the procedure with the correct information. You can also click Finish, delete the completed circuit, and start the procedure from the beginning.

Step 19 Click **Finish**.

You now need to provision the Ethernet ports and assign ports to VLANs. For port provisioning instructions, see the “Provision E10/100-4 Ethernet Ports” procedure on page 9-3. For information about assigning ports to VLANs, see the “Provision Ethernet Ports for VLAN Membership” procedure on page 9-25. Return to Step 20 after assigning the ports to VLANs.

Step 20 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box appears.

Step 21 Click **Drops** and click **Create**.

The Define New Drop dialog box appears.

Step 22 From the Slot menu, choose the optical card that links the ONS 15327 to the non-ONS 15327 equipment.

Step 23 From the Port menu, choose the appropriate port.

Step 24 From the STS menu, choose the STS that matches the STS of the connecting non-ONS 15327 equipment.

Step 25 Click **OK**.

The Edit Circuit dialog box appears.

Step 26 Confirm the circuit information that appears in the Circuit Information dialog box and click **Close**.

Step 27 Repeat Steps 1–26 at the second ONS 15327 Ethernet manual cross-connect endpoint.



Note The appropriate STS circuit must exist in the non-ONS 15327 equipment to connect the two ONS 15327 Ethernet manual cross-connect endpoints.



Caution

If a CARLOSS alarm repeatedly appears and clears on an Ethernet manual cross -connect, the two Ethernet circuits may have a circuit-size mismatch. For example, a circuit size of STS-1 might have been configured on the first ONS 15327 and circuit size of STS-3c might have been configured on the second ONS 15327. To troubleshoot this occurrence of the CARLOSS alarm, refer to Chapter 14, “Alarm Troubleshooting”.

9.5 VLAN Support

Users can provision up to 509 VLANs 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 IEEE 802.1Q-based VLAN mechanism provides logical isolation of subscriber LAN traffic over a common SONET transport infrastructure. Each subscriber has an Ethernet port at each site, and each subscriber is assigned to a VLAN. Although the subscriber's VLAN data flows over shared circuits, the service appears to the subscriber as a private data transport.

9.5.1 Q-Tagging (IEEE 802.1Q)

IEEE 802.1Q allows the same physical port to host multiple IEEE 802.1Q VLANs. Each IEEE 802.1Q VLAN represents a different logical network.

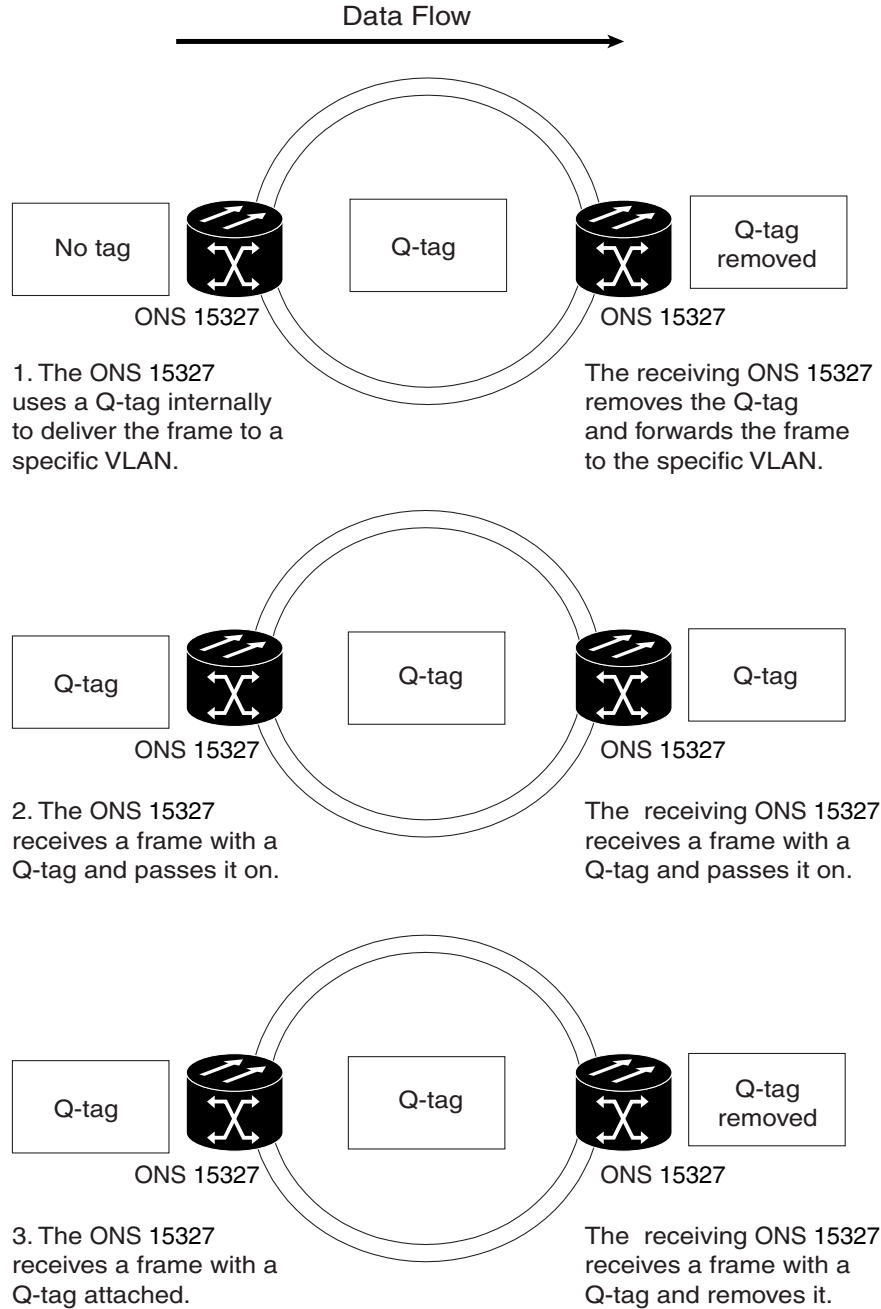
The ONS 15327 works with Ethernet devices that support IEEE 802.1Q and those that do not support IEEE 802.1Q. If a device attached to an ONS 15327 Ethernet port does not support IEEE 802.1Q, the ONS 15327 only uses Q-tags internally. The ONS 15327 associates these Q-tags with specific ports.

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 ingress port of the ONS network. The receiving ONS node removes the Q-tag when the frame leaves the ONS network (to prevent older Ethernet equipment from incorrectly identifying the IEEE 802.1Q packet as an illegal frame). The ingress and egress ports on the ONS network must be set to Untag for the process to occur. Untag is the default setting for ONS ports. Example 1 in Figure 9-20 illustrates Q-tag use only within an ONS network.

With Ethernet devices that support IEEE 802.1Q, the ONS 15327 uses the Q-tag attached by the external Ethernet devices. 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. Set both entry and egress ports on the ONS network to Tagged for this process to occur. Example 2 in Figure 9-20 illustrates the handling of packets that both enter and exit the ONS network with a Q-tag.

For more information about setting ports to Tagged and Untag, see the "Provision Ethernet Ports for VLAN Membership" procedure on page 9-25.

Figure 9-20 A Q-tag moving through a VLAN



9.5.2 Priority Queuing (IEEE 802.1Q)



Note IEEE 802.1Q was formerly IEEE 802.1P.

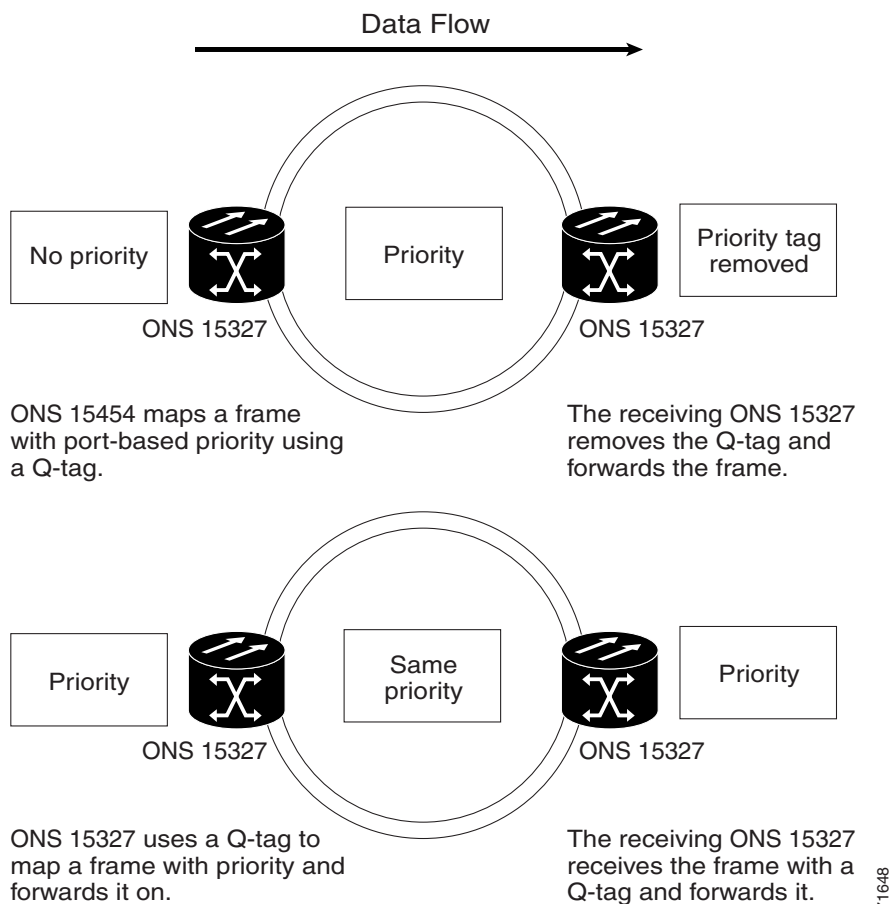
Networks without priority queuing handle all packets on a first-in, first-out (FIFO) basis. Priority queuing reduces the impact of network congestion by mapping Ethernet traffic to different priority levels. The ONS 15327 supports priority queuing. The ONS 15327 takes the eight priorities specified in IEEE 802.1Q and maps them to two queues (Table 9-3). 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 drops packets.

Table 9-3 Priority Queuing

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

Figure 9-21 Priority queuing process



9.5.3 VLAN Membership

This section explains how to provision Ethernet ports for VLAN membership. For initial port provisioning (before provisioning VLAN membership), see the “E10/100-4 Card Port Provisioning” section on page 9-3.



Caution

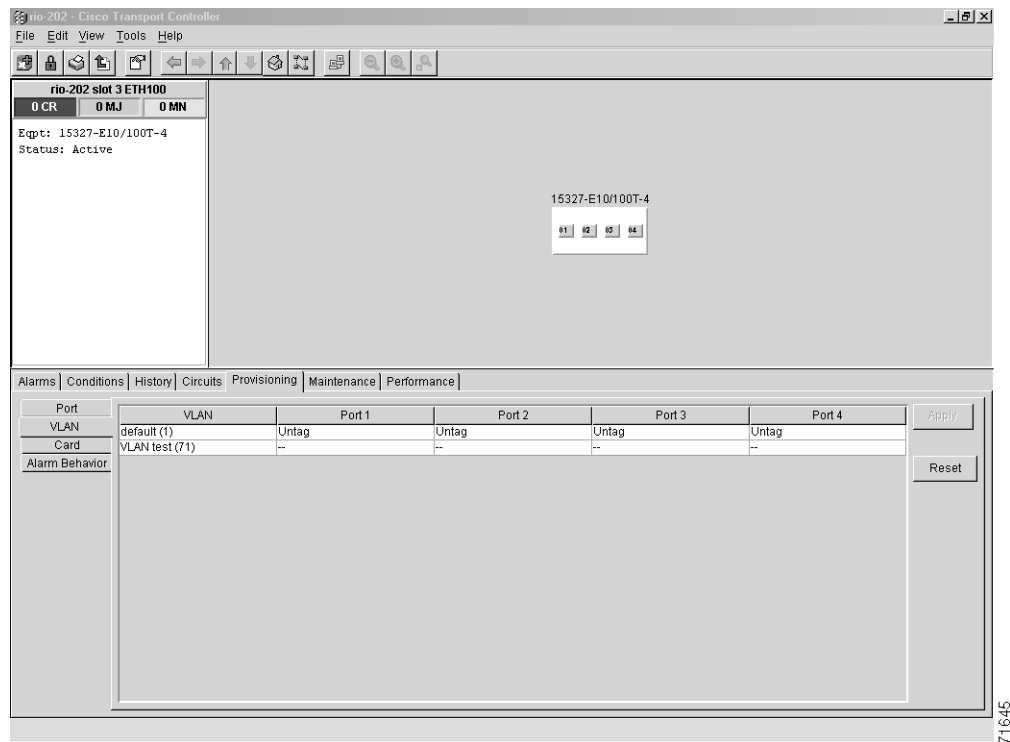
ONS 15327s propagate VLANs whenever a node appears on the same network view of another node regardless of whether the nodes connect through DCC. For example, if two ONS 15327s without DCC connectivity belong to the same Login Node Group, then whenever CTC gets launched from within this login node group, VLANs propagate from one to another. This happens even though the ONS 15327s do not belong to the same SONET ring.

The ONS 15327 allows you to configure the VLAN membership and Q-tag handling of individual Ethernet ports.

Procedure: Provision Ethernet Ports for VLAN Membership

- Step 1** Display the CTC card view for the Ethernet card.
- Step 2** Click the **Provisioning > VLAN** tabs (Figure 9-22).

Figure 9-22 Configuring VLAN membership for individual Ethernet ports



71645

Step 3 To put a port in a VLAN, click the port and choose either Tagged or Untag. Table 9-4 shows valid port settings.

Table 9-4 Port Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15327 tags ingress frames and strips tags from egress frames.
Tagged	The ONS 15327 handles ingress frames according to VLAN ID; egress frames do not have their tags removed.

If a port is a member of only one VLAN, go to the row of that VLAN and choose **Untag** from the Port column. Choose -- for all the other VLAN rows in that Port column. The VLAN with **Untag** selected can connect to the port, but other VLANs cannot access that port.

If a port is a trunk port, it connects multiple VLANs to an external device, such as a switch, that also supports trunking. A trunk port must have tagging (IEEE 802.1Q) enabled for all VLANs that connect to that external device. Choose **Tagged** for all VLAN rows that need to be trunked. Choose **Untag** for each of the VLAN rows in the trunk port column that do not need to be trunked, for example, the default VLAN. Each Ethernet port must be attached to at least one untagged VLAN.

Step 4 After each port is in the appropriate VLAN, click **Apply**.



Note

If Tagged is chosen, the attached external devices must recognize IEEE 802.1Q VLANs.

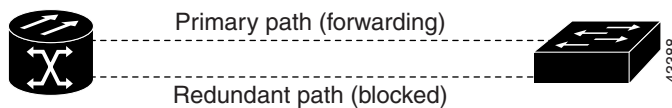
9.6 Spanning Tree (IEEE 802.1D)

The Cisco ONS 15327 operates Spanning Tree Protocol (STP) according to IEEE 802.1D when an Ethernet card is installed. STP operates over all packet-switched ports including Ethernet and SONET ports. On Ethernet ports, STP is disabled by default but may be enabled with a check box under the Provisioning > Port tabs at the card-level view. On SONET interface ports, STP activates by default and cannot be disabled.

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

STP detects and eliminates network loops. When STP detects multiple paths between any two network hosts, STP blocks ports until only one path exists between any two network hosts (Figure 9-23). The single path eliminates possible bridge loops. This is crucial for shared packet rings, which naturally include a loop.

Figure 9-23 STP-blocked path



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

9.6.1 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 (i.e., one for private TLS services and one for Internet access). Each circuit runs its own STP to maintain VLAN connectivity in a multi-ring environment.

Procedure: Enable Spanning Tree on Ethernet Ports

-
- Step 1** Display the CTC card view.
 - Step 2** Click the **Provisioning > Port** tabs.
 - Step 3** In the left column, find the applicable port number and check the **Stp Enabled** check box to enable STP for that port.
 - Step 4** Click **Apply**.
-

9.6.2 Spanning-Tree Parameters

Default spanning tree parameters are appropriate for most situations. Contact the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 before you change the default STP parameters.

At the node view, click the **Maintenance > Etherbridge > Spanning Trees** tabs to view spanning tree parameters.

Table 9-5 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 spanning-tree topology has been changed since the node booted up.
DesignatedRoot	Designated root of the spanning tree for a particular spanning-tree instance.
RootCost	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.

Table 9-5 Spanning-Tree Parameters (continued)

HelloTime	Time interval, in seconds, between the transmission of configuration BPDUs by a bridge that is the spanning-tree root or is attempting to become the spanning-tree root.
HoldTime	Minimum time period, in seconds, that elapses during the transmission of configuration information on a given port.
ForwardDelay	Time spent by a port in the listening state and the learning state.

9.6.3 Spanning-Tree Configuration

To view the spanning-tree configuration, at the node view click the **Provisioning** tab and **Etherbridge** subtab. Table 9-6 lists spanning-tree configuration information.

Table 9-6 Spanning-Tree Configuration

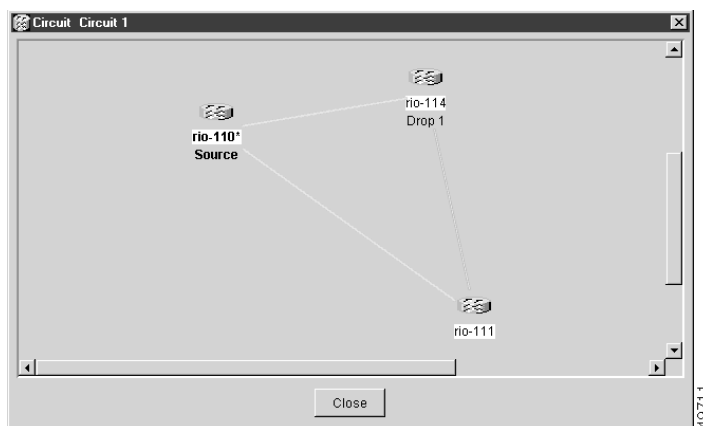
Column	Default Value	Value Range
Priority	32768	0–65535
Bridge maximum age	20 seconds	6–40 seconds
Bridge Hello Time	2 seconds	1–10 seconds
Bridge Forward Delay	15 seconds	4–30 seconds

9.6.4 Spanning-Tree Map

The Circuit window shows forwarding spans and blocked spans on the spanning tree map.

Procedure: View the Spanning Tree Map

On the circuit window (Figure 9-24), double-click an Ethernet circuit.

Figure 9-24 The Spanning-tree map on the Circuit window

**Note**

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

9.6.5 Ethernet Performance Screen

CTC provides Ethernet performance information that includes line-level parameters, the amount of port bandwidth used, and historical Ethernet statistics.

9.6.5.1 Statistics Window

The Ethernet statistics screen lists Ethernet parameters at the line level. Table 9-7 defines the parameters. Display the CTC card view for the Ethernet card and click the **Performance > Statistics** tabs to display the screen.

The Baseline button resets the values on the Statistics tab to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval for automatic refresh of statistics to occur.

Table 9-7 Ethernet Parameters

Parameter	Meaning
Link Status	Indicates whether or not link integrity is present; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with a frame check sequence (FCS) error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with alignment errors; alignment errors are received incomplete frames.
Rx Runts	Number of packets received that are less than 64 bytes in length.
Rx Giants	Number of packets received that are greater than 1518 bytes in length for untagged interfaces and 1522 bytes for tagged interfaces.
Tx Collisions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
Tx Excessive	Number of consecutive collisions.
Tx Deferred	Number of packets deferred.

9.6.5.2 Line Utilization Window

The Line Utilization window shows the percentage of line, or port, bandwidth used and the percentage used in the past. Display the CTC card view and click the Performance and Utilization tabs to display the window. From the Interval menu, choose a time segment interval. Valid intervals are 1 minute, 15 minutes, 1 hour, and 1 day. Press Refresh to update the data.

9.6.5.3 Utilization Formula

The utilization screen numbers may differ from the numbers encountered on an Ethernet test set. The line utilization numbers express the average of ingress and egress traffic as a percentage of the total capacity. Line utilization is calculated with the following formula: $(\text{InOctets} + \text{OutOctets}) * 8 \text{ bits/octets} / 100 / \text{intervals} * (\text{maxRate} * 2)$. Intervals are defined in seconds. maxRate is defined by raw bits/second in one direction for the circuit. maxRate is multiplied by 2 in the denominator to get the raw bit rate in both directions.

Table 9-8 maxRate for STS Circuits

Circuit	maxRate
STS-1	51840000 bps
STS-3c	155000000 bps
STS-6c	311000000 bps
STS-12c	622000000 bps

This formula does not take into account the HDLC headers, SONET header, and inter-frame gap. This means that the line utilization numbers do not reach 100 percent. It also means that smaller packet sizes result in lower utilization figures.



Note

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

9.6.5.4 History Window

The Ethernet History window lists past Ethernet statistics. At the CTC card view, click the Performance tab and History subtab to view the window. Choose the appropriate port from the Line menu and the appropriate interval from the Interval menu. Press Refresh to update the data.

9.6.6 Ethernet Maintenance Screen

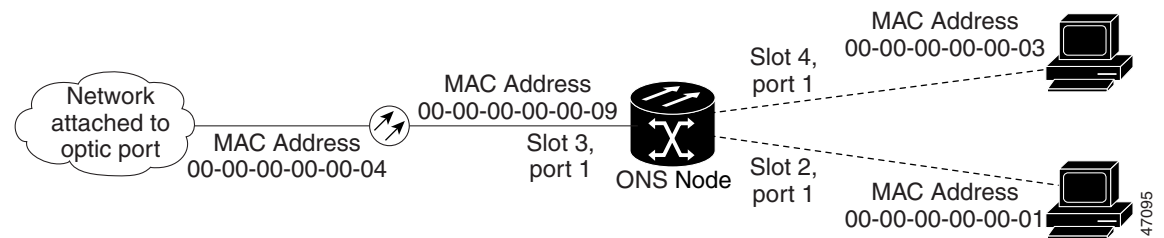
Display an Ethernet card in CTC card view and choose the Maintenance tab to display MAC address and bandwidth information.

9.6.6.1 MAC Table

A MAC address is a hardware address that physically identifies a network device. The ONS 15327 MAC table, also known as the MAC forwarding table, allows you to see all of the MAC addresses attached to the enabled ports of an Ethernet card or an Ethernet Group. This includes the MAC address of the

network device attached directly to the port and any MAC addresses on the network linked to the port. The MAC addresses table lists the MAC addresses stored by the ONS 15327 and the VLAN, Slot/Port/STS, and circuit that links the ONS 15327 to each MAC address (Figure 9-25).

Figure 9-25 MAC addresses recorded in the MAC table



Procedure: Retrieve the MAC Table Information

-
- Step 1** Click the **Maintenance > EtherBridge > MAC Table** tabs.
 - Step 2** Select the appropriate Ethernet card or Ethergroup from the Layer 2 Domain pull-down menu.
 - Step 3** Click **Retrieve**. The ONS 15327 retrieves and displays the current MAC IDs.



Note Click **Clear** to clear the highlighted rows and click **Clear All** to clear all displayed rows.

9.6.6.2 Trunk Utilization Window

The Trunk Utilization window is similar to the Line Utilization window, but Trunk Utilization shows the percentage of circuit bandwidth used rather than the percentage of line bandwidth used. Click the Maintenance > Ether Bridge > Trunk Utilization tabs to view the window. Choose a time segment interval from the Interval menu.



Note The percentage shown is the average of ingress and egress traffic.

9.7 Remote Monitoring Specification Alarm Thresholds

The ONS 15327 features Remote Monitoring (RMON) that allows network operators to monitor the health of the network with a network management system (NMS). For a detailed description of the ONS SNMP implementation, see Chapter 11, “SNMP.”

One of the ONS 15327 RMON MIBs is the Alarm group. The alarm group consists of the alarmTable. An NMS uses the alarmTable to find the alarm-causing thresholds for network performance. The thresholds apply to the current 15-minute interval and the current 24-hour interval. RMON monitors several variables, such as Ethernet collisions, and triggers an event when the variable crosses a threshold

during that time interval. For example, if a threshold is set at 1000 collisions and 1001 collisions occur during the 15-minute interval, an event triggers. CTC allows you to provision these thresholds for Ethernet statistics.

**Note**

You can find performance monitoring specifications for all other cards in Chapter 8, “Performance Monitoring.”

**Note**

Table 9-9 defines the variables you can provision in CTC. For example, to set the collision threshold, choose etherStatsCollisions from the Variable menu.

Table 9-9 Ethernet Threshold Variables (MIBs)

Variable	Definition
ifInOctets	Total number of octets received on the interface, including framing octets
ifInUcastPkts	Total number of unicast packets delivered to an appropriate protocol
ifInErrors	Number of inbound packets discarded because they contain errors
ifOutOctets	Total number of transmitted octets, including framing packets
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address
dot3statsAlignmentErrors	Number of frames with an alignment error, i.e., the length is not an integral number of octets and the frame cannot pass the FCS test
dot3StatsFCSErrors	Number of frames with framecheck errors, i.e., there is an integral number of octets, but an incorrect FCS
dot3StatsSingleCollisionFrames	Number of successfully transmitted frames that had exactly one collision
dot3StatsMutlipleCollisionFrame	Number of successfully transmitted frames that had multiple collisions
dot3StatsDeferredTransmissions	Number of times that the first transmission was delayed because the medium was busy
dot3StatsLateCollision	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count)
dot3StatsExcessiveCollision	Number of frames where transmissions failed because of excessive collisions
etherStatsJabbers	Total number of octets of data (including bad packets) received on the network
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets
etherStatsFragments	Total number of packets that are not an integral number of octets or have a bad FCS, and that are less than 64 octets long
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length

Table 9-9 Ethernet Threshold Variables (MIBs) (continued)

Variable	Definition
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65–172 octets in length
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128–255 octets in length
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256–511 octets in length
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512–1023 octets in length
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024–1518 octets in length
etherStatsJabbers	Total number of packets longer than 1518 octets that were not an integral number of octets or had a bad FCS
etherStatsCollisions	Best estimate of the total number of collisions on this segment
etherStatsCollisionFrames	Best estimate of the total number of frame collisions on this segment
etherStatsCRCAlignErrors	Total number of packets with a length between 64 and 1518 octets, inclusive, that had a bad FCS or were not an integral number of octets in length

Procedure: Creating Ethernet RMON Alarm Thresholds

- Step 1** Display the CTC node view.
- Step 2** Click the **Provisioning > Etherbridge > Thresholds** tabs.
- Step 3** Click **Create**.

The Create Ether Threshold dialog box appears.

Figure 9-26 Creating RMON thresholds

- Step 4** From the Slot menu, choose the appropriate Ethernet card.

- Step 5** From the Port menu, choose the port on the Ethernet card.
- Step 6** From the Variable menu, choose the variable that you want to set. Table 9-9 lists and defines the Ethernet Threshold Variables available in this field.
- Step 7** From Alarm Type menu, indicate whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.
- Step 8** From the Sample Type pull-down menu, choose either **Relative** or **Absolute**. **Relative** restricts the threshold to use the number of occurrences in the user-set sample period. **Absolute** sets the threshold to use the total number of occurrences, regardless of any time period.
- Step 9** Type in an appropriate number of seconds for the Sample Period.
- Step 10** Type in the appropriate number of occurrences for the Rising Threshold.



Note To raise a rising type of alarm, the measured value must move from below the falling threshold to above the rising threshold. For example, if a network is running below a falling threshold of 400 collisions every 15 seconds and a problem causes 1001 collisions in 15 seconds, these occurrences raise an alarm.

- Step 11** Type in the appropriate number of occurrences for the Falling Threshold. In most cases a falling threshold is set lower than the rising threshold.

A falling threshold is the counterpart to a rising threshold. When the number of occurrences is above the rising threshold and then drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15 minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded. (Otherwise a single network problem might cause a rising threshold to be exceeded multiple times and cause a large number of events.)

- Step 12** Click **OK** to complete the procedure.
-



Alarm Monitoring and Management

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

- Viewing alarms
- Viewing history
- Viewing conditions
- Creating and managing alarm profiles
- Suppressing alarms

To troubleshoot specific alarms, see Chapter 14, “Alarm Troubleshooting”.

10.1 Overview

The CTC detects and reports SONET alarms generated by the Cisco ONS 15327 and larger SONET network. You can use CTC to monitor and manage alarms at the card, node, or network level. Default alarm severities conform to the Telcordia GR-253-CORE standard, but you can reset severities to customized alarm profiles or suppress CTC alarm reporting. For a detailed description of the standard Telcordia categories employed by ONS nodes, see Chapter 14, “Alarm Troubleshooting”.



Note

ONS 15327 alarms can also be monitored and managed through TL1 or a network management system (NMS).

10.2 Viewing ONS 15327 Alarms

At the card, node, or network-level CTC view, click the **Alarms** tab to display the alarms for that card, node or network. Table 10-1 lists the tab column headings and the information recorded in each column as shown from the CTC node view.

Table 10-1 Alarms Column Descriptions

Column	Information Recorded
New	Indicates a new alarm. To change this status, check either the Synchronize Alarms or Delete Cleared Alarms check box, or reset the active TCC+ card.
Date	Date and time of the alarm.
Node	Node where the alarm occurred (displayed in network view only).
Object	TL1 access identifier (AID) for the alarmed object.
Type	Card type in this slot.
Slot	Slot where the alarm occurred (displayed in network and node view only).
Port	Port where the alarm occurred.
Sev	Severity level: CR (critical), MJ (major), MN (minor), NA (not alarmed), NR (not reported).
ST	Status: R (raised), C (clear), T (transient).
SA	When checked, indicates a service-affecting alarm.
Cond	The error message/alarm name.
Description	Description of the alarm.
Num	A count of incrementing alarm messages (hidden by default).
Ref	The reference number assigned to a cleared alarm (hidden by default).

Figure 10-1 Viewing alarms in CTC node view

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
136	136	<input checked="" type="checkbox"/>	04/16/02 10:44:14 CDT	SLOT-1	OC12	1		MN	R		MEA	Mismatch Of Equipment And Attributes

Alarms are displayed in one of five background colors, listed in Table 10-2, to quickly communicate the alarm severity. Events, conditions, and cleared alarms are also color-coded. Conditions and events are displayed in the **History** or **Conditions** tab.

Table 10-2 Color Codes for Alarms, Conditions, and Events

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

10.2.1 Controlling Alarm Display

You can control the display of the alarms on the **Alarms** tab. Table 10-3 shows the actions you can perform from the **Alarms** tab.

Table 10-3 Alarm Display

Button	Action
Synchronize Alarms	Updates the alarm display; although CTC displays alarms in real time, the Synchronize Alarms button allows you to verify the alarm display. This is particularly useful during provisioning or troubleshooting.
Delete Cleared Alarms	Deletes alarms that have been cleared.
AutoDelete Cleared Alarms	If checked, CTC automatically deletes cleared alarms.
Show Events (NA)	If checked, CTC shows alarms and NA events or conditions. Not-alarmed events do not require action and normally are displayed only under the Conditions tab.

10.2.2 Viewing Alarm-Affected Circuits

User can view which ONS 15327 circuits are affected by a specific alarm. To do this, highlight an alarm and right-click it. The **Selected Affected Circuits** shortcut menu appears. Figure 10-2 illustrates the Select Affected Circuits option. When the option is clicked, the affected circuits are shown as in Figure 10-3.

Figure 10-2 Selecting the Affected Circuits option

The screenshot shows the Cisco Transport Controller interface for 'rio-201'. The 'Alarms' tab is selected, displaying a table of active alarms. The following table represents the data shown in the interface:

Num	Ref	New	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
136	136	<input checked="" type="checkbox"/>	04/16/02 10:44:14 CDT	SLOT-1	OC12	1		MN	R		MEA	Mismatch Of Equipment And Attributes

Below the table, the 'Select Affected Circuits' button is highlighted. Other buttons include 'Synchronize', 'Delete Cleared Alarms', 'AutoDelete Cleared Alarms', and 'Show Events (NA)'.

Figure 10-3 Highlighted circuit appears

The screenshot shows the Cisco Transport Controller interface for 'rio-201'. The 'Circuits' tab is selected, displaying a table of active circuits. The following table represents the data shown in the interface:

Circuit Name	Type	Size	Dir	State	Source	Destination	# of VLANs	# of Spar
Test	STS	1	2-way	ACTIVE	rio-201/s6/pd51/s1	rio-203/s6/pd51/s1		1

The 'Test' circuit is highlighted in the table. The interface also shows buttons for 'Create...', 'Delete', 'Edit...', and 'Search...'. The 'Scope' is set to 'Node'.

10.2.3 Conditions Tab

The Conditions tab displays retrieved fault conditions. A fault is a problem detected by ONS 15327 hardware or software. When a fault occurs and continues for a minimum time period, it raises a fault condition, which is a flag showing whether or not this particular fault currently exists on the ONS 15327. Fault conditions include all existing conditions, whether the severity is that of an alarm (Critical, Major

or Minor) or a condition (Not Reported or Non Alarmed.) See the trouble notifications information in Chapter 14, “Alarm Troubleshooting,” for more information on the classifications for alarms and conditions.

Displaying all existing fault conditions is helpful while troubleshooting the ONS 15327. The Conditions tab does not adhere to Telcordia guidelines for reporting alarms, events, and conditions. Alarm reporting under the Alarms tab is Telcordia-compliant.

10.2.3.1 Retrieve and Display Conditions

At the node view, click the **Conditions** tab and the **Retrieve Conditions** button to retrieve the current set of all existing fault conditions from the ONS 15327 as maintained by the alarm manager. Users can perform the same operation at the card view for the card level and at the network view for the network level. See Figure 10-4.

Figure 10-4 Viewing fault conditions under the Conditions Tab

The screenshot shows the Cisco Transport Controller interface. The top part displays a network diagram with various components and their status. Below the diagram, there is a table of conditions. The table has the following columns: Object, Eqpt Type, Slot, Port, Sev, SA, Cond, and Description. The table lists several conditions, including SYNC-NE, SLOT-1, and SYSTEM.

Object	Eqpt Type	Slot	Port	Sev	SA	Cond	Description
SYNC-NE				NA	SSM-ST3		Stratum 3 Traceable
SYNC-NE				NA	SWTOPRI		Switch To Primary Reference
SLOT-1	OC12	1		NR	CONTBUS-I...		TCC B To Shelf Slot Communication Failure
SLOT-1	OC12	1		MN	MEA		Mismatch Of Equipment And Attributes
SYSTEM				NR	PWR-B		NE Power Failure At Connector B

10.2.3.2 Conditions Column Descriptions

Table 10-4 lists the Conditions tab column headings and the information recorded in each column.

Table 10-4 Conditions Columns Description

Column	Information Recorded
Node	Node where the condition occurred (displayed in network view only)
Object	TL1 AID for the alarmed object
Type	Card type in this slot
Slot	Slot where the condition occurred (displayed in network and node view only)

Table 10-4 Conditions Columns Description (continued)

Column	Information Recorded
Port	Port where the condition occurred
Sev	Severity level: CR, MJ, MN, NA, NR
SA	When checked, indicates a service-affecting alarm
Cond	Condition name
Description	Description of the condition

10.2.4 Viewing History

The **History** tab displays historical alarm data. It also displays events, which are nonalarmed activities such as timing changes and threshold crossings. For example, protection switching events or performance monitoring threshold crossings appear here. The History tab presents two alarm history views:

- The Session subtab (Figure 10-5) presents alarms and events that have occurred during the current CTC session.
- The Node subtab shows the alarms and events that occurred at the node since the CTC software installation. The ONS 15327 can store up to 640 critical alarms, 640 major alarms, 640 minor alarms, and 256 events. When the limit is reached, the ONS 15327 discards the oldest alarms and events.



Tip

Double-click an alarm in the alarm table or an event in the history table to display the corresponding view. For example, double-clicking a card alarm takes you to card view. In network view, double-clicking a node alarm takes you to node view.

Figure 10-5 Viewing all alarms reported for the current session

The screenshot shows the CTC interface for node 'rio-201'. The top left panel displays system statistics: 0 CR, 0 MJ, 1 MN. Below this, system information is shown: IP Addr: 10.92.18.201, Booted: 3/15/02 1:35 PM, User: CISCO15, Authority: Superuser. The main area shows a network diagram with slots 1 through 8. Slot 1 contains an OC48/STM16-LR-1550 card with a 'Mis' alarm. Slot 2 contains an OC48/STM16-LR-1550 card with an 'Act' alarm. Slot 3 contains a 15327-E10/100T-4 card with an 'Act' alarm. Slot 4 contains a 15327-XTC-28-3 card with a 'CRAFT' alarm. Slot 5 contains a 15327-XTC-28-3 card with a 'CRAFT' alarm. Slot 6 contains a 15327-XTC-28-3 card with a 'Sby' alarm. Slot 7 contains a MIC-B card with a 'PS1' alarm. Slot 8 contains a MIC-A card with a 'PS1' alarm. A 'FAN' alarm is also visible on the right side of the diagram.

Session	Date	Object	Eqpt Type	Slot	Port	Sev	ST	SA	Cond	Description
Node	04/16/02 10:44:14 CDT	SLOT-1	OC12	1		MN	R		MEA	Mismatch Of Equipment And Attributes

76149

10.3 Alarm Profiles

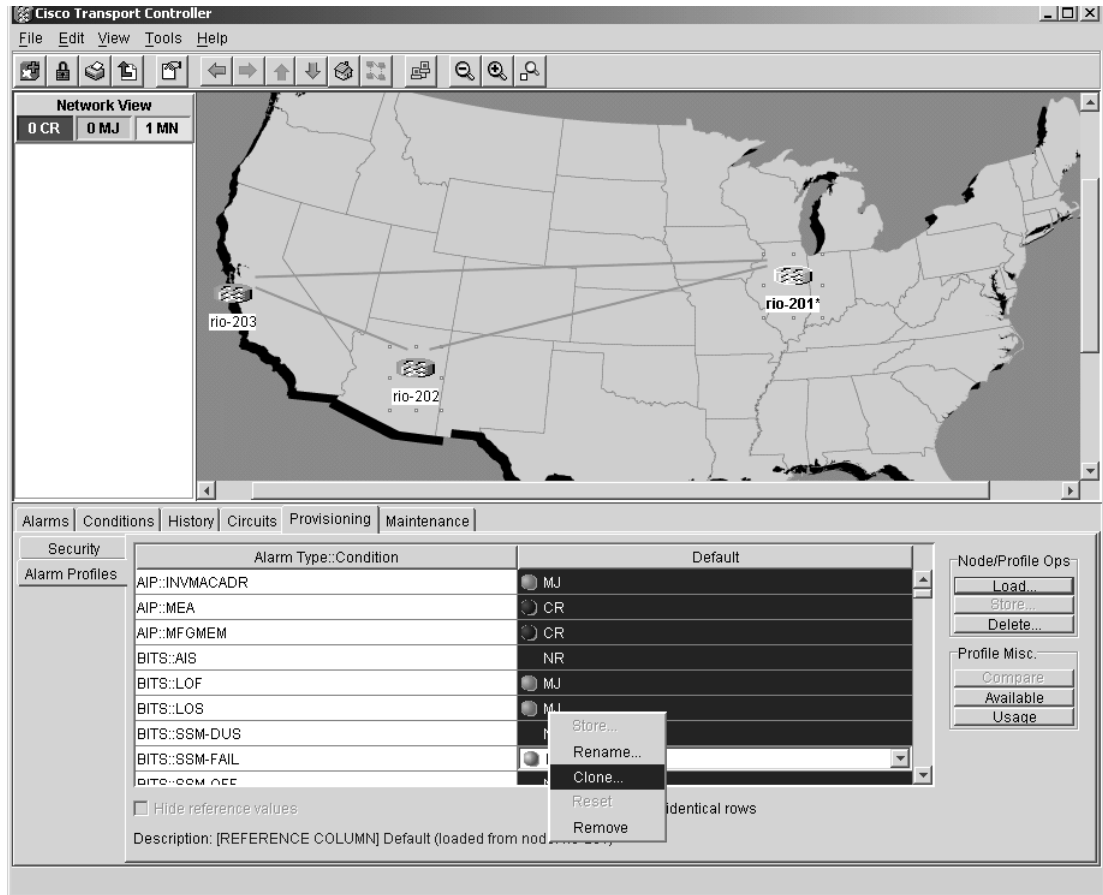
The alarm profiles feature allows you to change default alarm severities by creating unique alarm profiles for individual ONS 15327 nodes. A profile you create can be applied to any node on the network. Alarm profiles must be stored on a node before they can be applied to a node, card, or port. CTC can store up to ten alarm profiles; eight are available for custom use and two are reserved. CTC can load an unlimited number of alarm profiles that have been stored on a node, server, or CTC workstation.

The two reserved profiles include the default profile, which sets severities to standard Telcordia GR-253-CORE settings, and the Inherited profile, which sets all alarm severities to transparent (TR). If an alarm has an Inherited profile, it inherits (copies) its severity from the same alarm at the next level. For example, a card with an Inherited alarm profile copies the severities used by the node that contains the card. The Inherited profile is not available at the node level.

10.3.1 Creating and Modifying Alarm Profiles

Alarm profiles are created at the network view using the Provisioning > Alarm Profiles tabs (Figure 10-6.) A default alarm profile (in the Default column) is preprovisioned for every alarm. After loading the Default profile on the node, you can use the Clone feature to create new profiles based on the default alarm profile. After the new profile is created, the Alarm Profiles subtab shows the default profile and the new profile.

Figure 10-6 Network View Alarm Profiles subtab showing the default profiles of listed alarms



78143

10.3.2 Alarm Profile Menus

The Alarm Profiles subtab displays two menus on the right side, Node/Profile Ops and Profile Misc, which include six alarm profile buttons. Table 10-5 lists and describes each of the alarm profile buttons.

Table 10-5 Alarm Profile Buttons

Heading	Button	Description
Node Profile Ops	Load	Loads a profile to either a node or a file
	Store	Saves profiles on a node (or nodes) or in a file
	Delete	Deletes profiles from a node
Profile Misc.	Compare	Displays differences between alarm profiles (i.e., individual alarms that are not configured equivalently between profiles)
	Available	Displays all of the profiles available on each node
	Usage	Displays all of the entities present in the network and which profile(s) each is using

10.3.3 Alarm Profile Editing

Table 10-6 lists and describes the five profile editing options available when you right-click in an alarm profile column.

Table 10-6 Alarm Profile Editing Options

Button	Description
Store	Saves a profile in either a node or a file
Rename	Changes a profile name
Clone	Creates a new profile that contains the same alarm severity settings as the highlighted profile (the profile being cloned)
Reset	Restores a profile to the state of that profile before it was last applied or to the state when it was first loaded, if it has not yet been applied
Remove	Removes a profile from the table editor

10.3.4 Alarm Severity Option

You change or assign alarm severity using a menu. To view this menu, right-click the alarm you want to change in its alarm profile column. Seven severity levels appear for the alarm:

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



Note

Transparent and Unset only appear in alarm profiles; they do not appear when you view alarms, history, or conditions.

10.3.5 Row Display Options

The **Alarm Profiles** subtab also displays two check boxes at the bottom of the screen: Hide default values and Hide identical rows. The Hide default values check box highlights alarms with nondefault severities by clearing alarm cells with default severities. The Hide identical rows check box hides rows of alarms that contain the same severity for each profile.

10.3.6 Applying Alarm Profiles

In CTC card view, the Alarm Behavior subtab displays the alarm profiles of the selected card. In node view, the Alarm Behavior subtab displays alarm profiles for the node. Alarms form a hierarchy. A node-level alarm profile applies to all cards in the node, except those that have their own profiles. A card-level alarm profile applies to all ports on the card, except those that have their own profiles.

At the node level, you may apply profile changes on a card-by-card basis or set a profile for the entire node. Figure 10-7 shows the profile of an OC-12 card being changed to Inherited at the node view.

Figure 10-7 Node view Alarm Behavior subtab of an OC-12 alarm profile

The screenshot shows the CTC interface for node 'rio-201'. The 'Alarm Behavior' subtab is active, displaying a table for configuring alarm profiles. The table has columns for Location, Eqpt Type, Profile, Suppress Alarms, and Port-Level Profiles. The 'Node Profile' is set to 'NoMICB' and 'Suppress Alarms' is unchecked.

Location	Eqpt Type	Profile	Suppress Alarms	Port-Level Profiles
Backplane	all non-card objects	Inherited	<input type="checkbox"/>	
1	OC12	Inherited	<input type="checkbox"/>	
2	OC48	Inherited	<input type="checkbox"/>	
3	ETH100	Default	<input type="checkbox"/>	
5	XTC	NoMICB	<input type="checkbox"/>	
6	XTC	Inherited	<input type="checkbox"/>	
7	MIC	Inherited	<input type="checkbox"/>	
8	MIC	Inherited	<input type="checkbox"/>	

At the card level, you can apply profile changes on a port-by-port basis or set all ports on that card at once. Figure 10-8 shows the affected OC-12 card; notice that CTC shows Parent Card Profile: Inherited.

Figure 10-8 Card view Alarm Behavior subtab of an OC-12 alarm profile

The screenshot shows the Cisco Transport Controller interface for a card view. The main window title is "rio-201 - Cisco Transport Controller". The top menu bar includes "File", "Edit", "View", "Tools", and "Help". Below the menu bar is a toolbar with various icons. The main content area is divided into several sections:

- rio-201 slot 1 OC12**: A header section with sub-sections for "0 CR", "0 MJ", and "1 MN".
- Eqpt: OC48/STM16-LR-**: Equipment information.
- Status: Mismatch**: Current status.
- Pl: IS/Act**: Profile information.
- OC48/STM16-LR-1550**: Equipment identifier.
- 01**: A small box containing the number 01.
- Alarms | Conditions | History | Circuits | Provisioning | Maintenance | Performance**: A set of tabs for navigation.
- Parent Card Profile: Inherited, Suppressed: No**: Information about the parent profile.
- Table:** A table with columns for "Line", "Port", "Profile", and "Suppress Alarms". The "Line" column has a value of "1". The "Profile" column has a value of "Inherited". The "Suppress Alarms" column has a checkbox that is currently unchecked.
- Buttons:** "Apply" and "Reset" buttons are located to the right of the table.
- Force all ports to profile:** A dropdown menu set to "Inherited" and a button labeled "Force (still need to 'Apply')".

76144

10.4 Suppressing Alarms

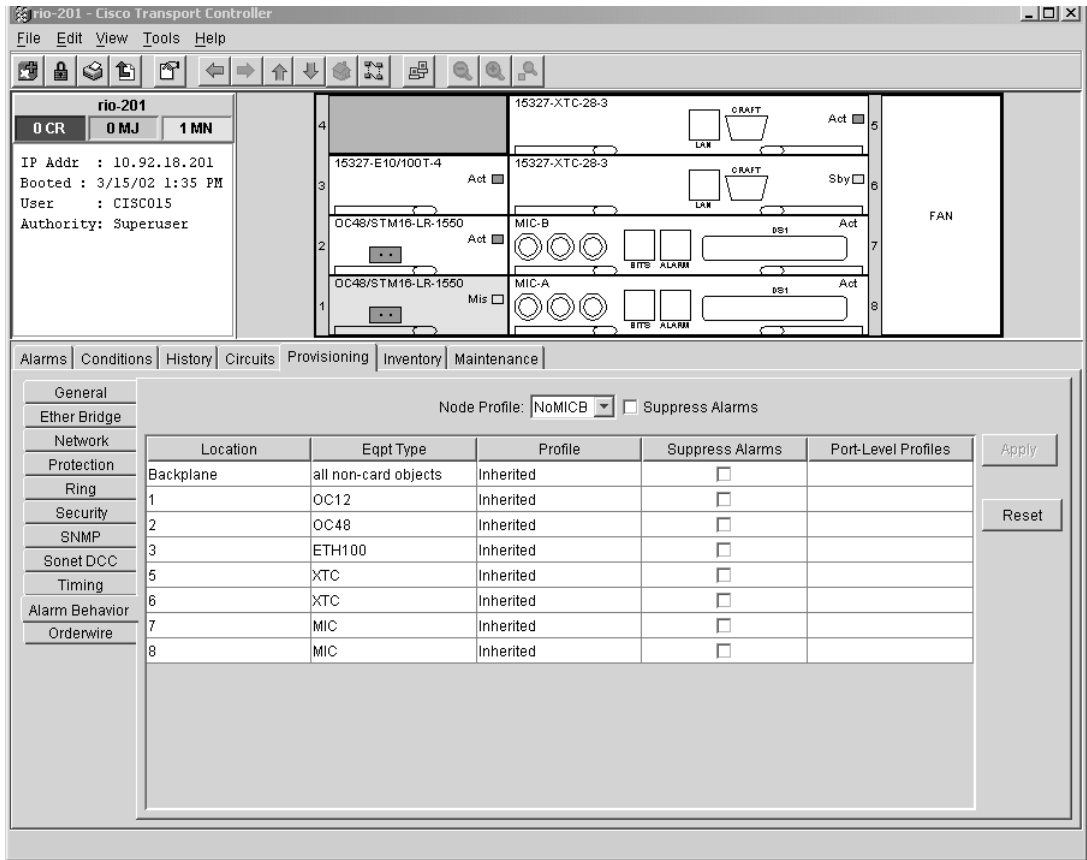
Suppressing alarms causes alarms to appear under the Conditions tab instead of the Alarms tab. It prevents alarms from appearing on CTC Alarm or History tabs or in any other clients. The suppressed alarms behave like conditions, which have their own nonreporting (NR) severities. Under the Conditions tab, the suppressed alarms appear with their alarm severity, color code, and service-affecting status (Figure 10-9).



Note

Use alarm suppression with caution. If multiple CTC/TL1 sessions are open, you will suppress the alarms in all other open sessions.

Figure 10-9 The Suppress Alarms check box



76147



SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15327.

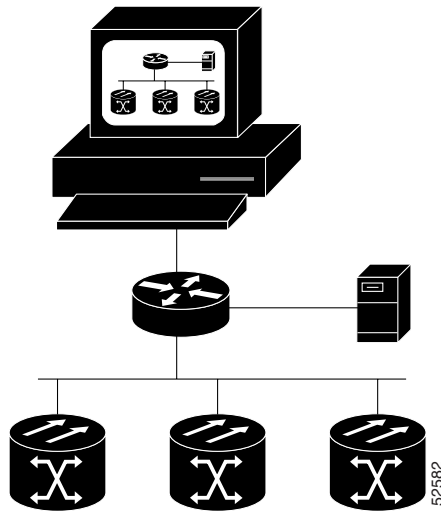
11.1 SNMP Overview

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) 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 System 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 illustrates a basic network managed by SNMP.

Figure 11-1 A basic network managed by SNMP

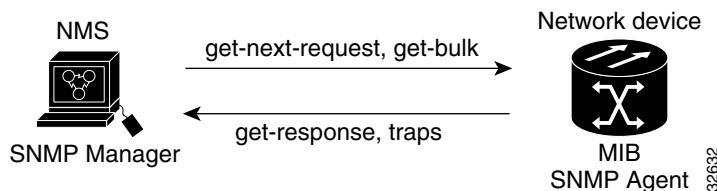


11.2 SNMP Basic Components

An SNMP-managed network consists of three primary components: managed devices, agents, and management systems. A managed device is a network node that contains an SNMP agent and resides on an SNMP-managed network. Managed devices collect and store management information and use SNMP to make this information available to management systems that use SNMP. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and network elements such as an ONS 15327.

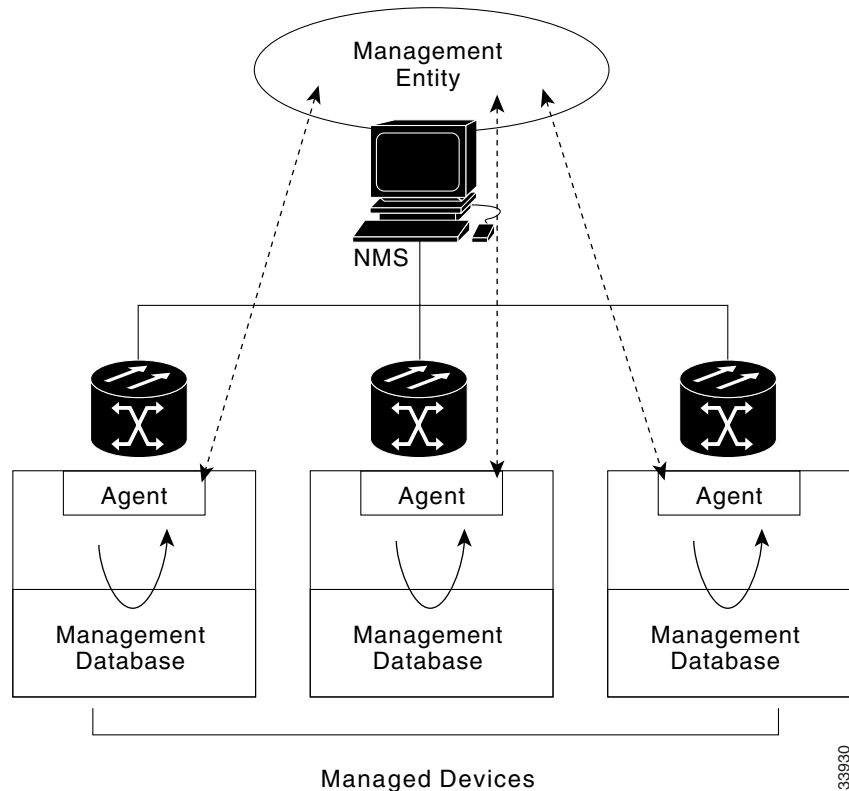
An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP manager gathers data from the SNMP agent using a Management Information Base (MIB), which is a textual (ASN.1) representation of management information such as device parameters and network data. The agent can also send traps, or notification of certain events, to the manager. Figure 11-2 illustrates these SNMP operations.

Figure 11-2 SNMP agent gathering data from an MIB and sending traps to the manager



A management system such as HP OpenView NNM executes applications that monitor and control managed devices. Management systems provide the bulk of the processing and memory resources required for network management. One or more management systems must exist on any managed network. Figure 11-3 illustrates the relationship between the three key SNMP components.

Figure 11-3 Example of the primary SNMP components



33930

11.3 SNMP Support

The ONS 15327 supports SNMPv1 and SNMPv2c 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. The ONS 15327 also supports set requests for the System Group in MIB-II and the Statistics, History and Alarm groups in the Remote Monitoring (RMON) MIB.

11.4 SNMP MIBs

A MIB is a hierarchically-organized collection of information. Network management applications gain access to MIBs and then the NMSs run SNMP queries on the MIB objects supported by the SNMP agent to gather management information. MIBs consist of managed objects and are identified by object identifiers.

The ONS 15327 SNMP agent communicates with an SNMP management application using SNMP messages. Table 11-1 describes these messages.

Table 11-1 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	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.
trap	Unsolicited message sent by an SNMP agent to an SNMP manager indicating that an event has occurred.

A managed object (sometimes called a MIB object) is one of any specific characteristics of a managed device. Managed objects consist of one or more object instances (variables). Table 11-2 lists the IETF standard MIBs implemented in the ONS 15327 SNMP Agent.

The ONS 15327 MIBs 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 sequence shown, one or more MIB files might not compile.

1. CERENT-GLOBAL-REGISTRY.mib
2. CERENT-TC.mib
3. CERENT-GENERIC.mib

If you cannot compile the ONS 15327 MIBs, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Table 11-2 IETF Standard MIBs Implemented in the ONS 15327 SNMP Agent

RFC#	Module Name	Title/Comments
1213 +1907	RFC1213-MIB, SNMPV2-MIB	MIB-II from RFC1213 with enhancement from RFC1907 for SNMPv2
1493	BRIDGE-MIB	Bridge/Spanning Tree (SNMPv1 MIB)
1757	RMON-MIB	RMON Ethernet
2737	ENTITY-MIB	Entity MIB using SMI v2 (version II)
2233	IF-MIB	Interface evolution (enhances MIB-II)
2358	Etherlike-MIB	Ethernet-like interface (SNMPv2 MIB)
2495	DS1-MIB	DS-1/E1
2496	DS3-MIB	DS-3/E3
2558	SONET-MIB	SONET
2674	P-BRIDGE-MIB, Q-BRIDGE-MIB	P-Bridge and Q-Bridge MIB

11.5 SNMP Traps

The ONS 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 11-3 for the ONS 15327.

Table 11-3 *SNMP Trap Variable Bindings Used in ONS 15327*

Number	Name	Description
1	cerentGenericAlarmTable	This table holds all the currently raised alarms. When an alarm is raised, it appears as a new entry in the table. When an alarm is cleared, it is removed from the table and all subsequent entries move up by one row.
2	cerentGenericAlarmIndex	This variable uniquely identifies each entry in an alarm table. When an alarm in the alarm table clears, the alarm indexes change for each alarm located subsequent to the cleared alarm.
3	cerentGenericAlarmObjectType	This variable provides the entity type that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
4	cerentGenericAlarmSlotNumber	This variable indicates the slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
5	cerentGenericAlarmPortNumber	This variable provides the port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
6	cerentGenericAlarmLineNumber	This variable provides the object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
7	cerentGenericAlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of the objects in each table; if the alarm is interface related, this is the index of the interfaces in the interface table.
8	cerentGenericAlarmType	This variable provides the exact alarm type.
9	cerentGenericAlarmState	This variable specifies alarm severity and service-affecting status. Severities are minor, major and critical. Service-affecting statuses are service-affecting and non-service affecting.

Table 11-3 SNMP Trap Variable Bindings Used in ONS 15327 (continued)

Number	Name	Description
10	cerentGenericAlarmTimeStamp	This variable gives the time when the alarm occurred. The value is the number of the ticks that have lapsed since 1/1/1970.
11	cerentGenericAlarmObjectName	This variable gives the TL1-style user-visible name that uniquely identifies an object in the system.

The ONS 15327 supports the generic and IETF traps listed in Table 11-4.

Table 11-4 Traps Supported in the ONS 15327

Trap	From RFC No.	Description
ColdStart	RFC1213-MIB	Agent up, cold start.
WarmStart	RFC1213-MIB	Agent up, warm start.
AuthenticationFailure	RFC1213-MIB	Community string does not match.
NewRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree.
TopologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or from Forwarding to Blocking.
EntConfigChange	RFC2037/ ENTITY-MIB	The entLastChangeTime value has changed.
ds1xLineStatusChange	RFC2495/ DS1-MIB	Sent when the value of an instance of 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 (for example, DS-3), no traps for the DS-1 are sent.
dsx3LineStatusChange	RFC2496/ DS3-MIB	Sent when the value of an instance of dsx3LineStatus changes. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (ex. DS-1), no traps for the lower-level are sent.
risingAlarm	RFC1757/ RMON-MIB	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	Generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

11.6 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination dialog box in CTC. (See the “SNMP Support” section on page 11-3.) In effect, SNMP considers any request valid that uses a community name matching a community name on the list of provisioned SNMP trap destinations. Otherwise, SNMP considers the request invalid and drops it.

If an SNMP request contains an invalid community name, the request silently drops and the MIB variable `snmpInBadCommunityNames` increments. All MIB variables managed by the agent grant access to all SNMP requests containing a validated community name.

11.7 SNMP Remote Monitoring

The ONS 15327 incorporates RMON to allow network operators to monitor the ONS 15327 E10/100-4 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. (See the “SNMP Remote Monitoring” section on page 11-7.) 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 Comments (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.



Maintenance

This chapter describes procedures that can be necessary to maintain the Cisco ONS 15327, including:

- Air filter inspection and replacement
- Fan-tray assembly replacement
- System reset
- Database backup and restore
- Reverting to an earlier software load
- XTC-14 card to XTC-28 card upgrade
- Span Upgrades
- Inhibit protection group switching
- Network Tests
- Creating diagnostic files
- Optic Fiber cleaning
- Powering down the ONS 15327

12.1 Air Filter Inspection and Replacement

The Cisco ONS 15327 contains an air filter that should be removed and visually inspected approximately every 30 days, depending on the cleanliness of the operating environment. The filter is reusable and made of a gray open-cell polyurethane foam, specially coated to provide fire and fungi resistance. Figure 12-1 illustrates the reusable fan-tray air filter. You do not need to remove the fan-tray assembly to remove the air filter.

Procedure: Inspect and Clean the Reusable Air Filter

- Step 1** Move any cables that are routed in front of the fan-tray assembly and air filter so you can easily slide the filter out, as shown in Figure 12-1.
- Step 2** Grasp the metal tab at the edge of the filter and slide the filter out of the bracket while being careful not to dislodge any dust that may have collected on the filter (Figure 12-1).
- Step 3** Visually inspect the filter material for dirt and dust.
- Step 4** If the reusable air filter contains a concentration of dirt and dust, either vacuum the filter and replace it or wash the filter under a faucet with a light detergent. Prior to washing the air filter, replace the dirty air filter with a clean air filter (spare filters should be kept in stock). Wash the dirty air filter under a faucet with a light detergent.



Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

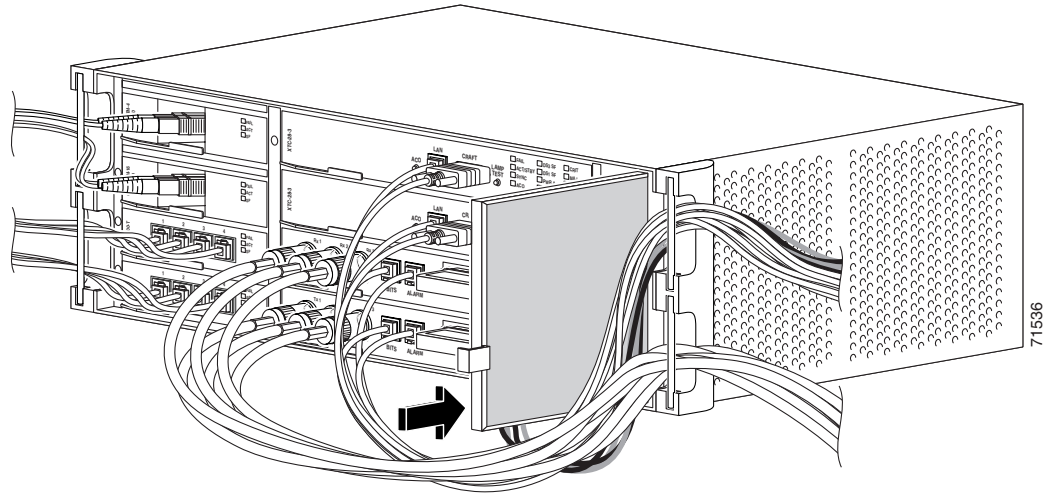
- Step 5** If you washed the filter, allow it to completely air dry for at least eight hours.



Warning **Do not put a damp filter back in the ONS 15327.**

- Step 6** Slide the filter back into the shelf (Figure 12-1).

Figure 12-1 Removing and replacing the reusable fan-tray air filter



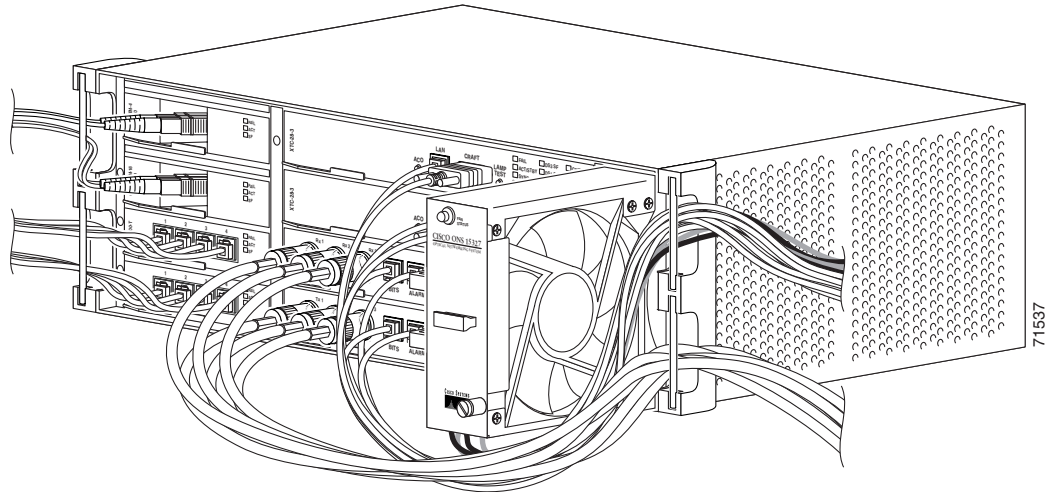
12.2 Fan-Tray Assembly Replacement

The fan tray is a removable drawer that holds fans and fan-control circuitry for the ONS 15327. You should not need to remove the fan-tray assembly unless a fan failure occurs and you must replace the fan-tray assembly. You cannot replace individual fans.

Procedure: Replace the Fan-Tray Assembly

- Step 1** Move any cables that are routed in front of the fan-tray assembly and air filter away so you can easily slide the filter out.
- Step 2** Loosen the fastening screw on the failed fan-tray assembly.
- Step 3** Grasp the fan tray handle and gently pull it one inch out of the slot and wait until the fans stop.
- Step 4** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly (Figure 12-2).

Figure 12-2 Removing a fan-tray assembly with installed cables

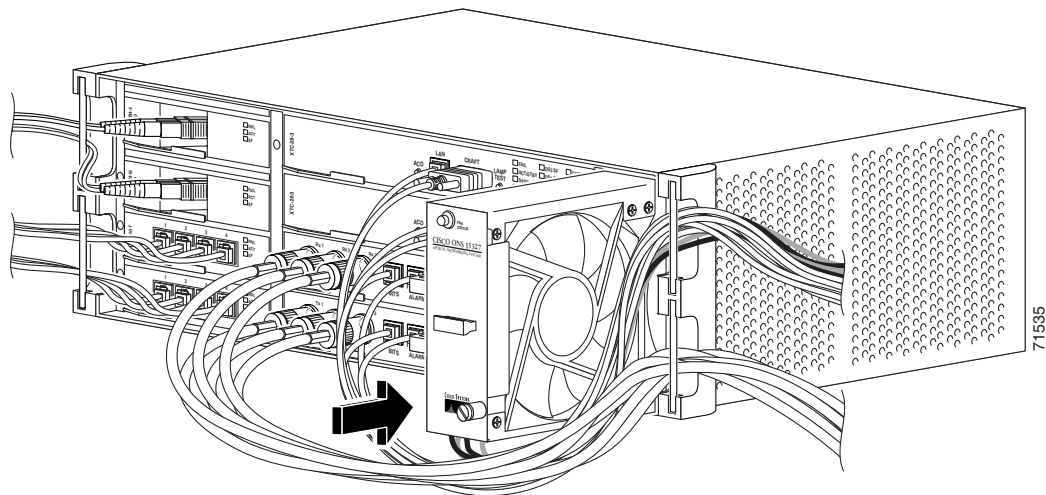


- Step 5** Slide the new fan-tray assembly into the shelf until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane (Figure 12-3).



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 12-3 Replacing the fan-tray assembly



- Step 6** Secure the fan tray into the slot using the attached fastening screw.
- Step 7** Confirm that the FAN STATUS LED on the front of the fan tray is illuminated. This indicates that the fan tray is operating.



Note The FAN STATUS LED only illuminates when an XTC card is installed.

12.3 System Reset

You can reset the ONS 15327 XTC card using the Cisco Transport Controller (CTC) software, or by physically reseating the XTC card (card pull). A software reset reboots the XTC and reloads the operating system and the application software. Additionally, a card pull reset temporarily removes power from the XTC and clears all buffer memory.

You can apply a software reset to either an active or standby XTC without affecting traffic, but you should only perform a card pull on a standby XTC. If you need to perform a card pull on an active XTC, put the XTC into standby mode first by performing a software reset on the card.



Warning

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



Note

A software or card pull reset of an active XTC card causes a standard Telcordia protection switch of less than 50 ms.

Procedure: Perform a Software Reset

-
- Step 1** Log into the node where you will perform the software reset.
 - Step 2** In node view, right click on the XTC card to reveal a pull-down menu.
 - Step 3** Click **Reset Card**.
 - Step 4** Click **Yes** when the “Are You Sure?” dialog box appears.
 - Step 5** Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.
 - Step 6** Confirm that the XTC is in standby mode after the reset.



Note

The XTC card takes several minutes to reboot. The Act/Stby LED glows amber during the reboot process. The AUTORESET alarm clears at the end of the boot process.

Procedure: Perform a Card Pull



Note

To determine whether you have an active or standby XTC, position the cursor over the XTC card graphic to display the status.

**Caution**

Always use the supplied electrostatic discharge band when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the front of the ONS 15327.

-
- Step 1** If you need to perform a hard reset on an active XTC card, first perform a soft reset on the active XTC as described in the “Perform a Software Reset” procedure on page 12-5.
- Step 2** When the XTC is in standby mode, unlatch both ejector levers on the XTC card.
- Step 3** Physically pull the card at least partly out of the slot until the lighted LEDs turn off.
- Step 4** Wait 30 seconds. Reinsert the card and close the ejector levers.
- Step 5** The XTC will take several minutes to reboot. The Act/Stby LED glows amber during the reboot process. The AUTORESET alarm clears at the end of the boot process.
-

12.4 Database Backup and Restore

Each XTC card installed in the ONS 15327 contains two copies of the database. A save to the flash memory is written to the standby database, and the standby database then becomes the active database. The previously active database then becomes available for writing the next time. With dual XTCS, the standby XTC keeps both copies of the database synchronized with the active XTC as changes are made so that it is ready to take over control as needed. You can also store a back-up version of the database on the workstation running CTC. Backing up the database should be part of a regular ONS 15327 maintenance program 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.

**Caution**

If you are restoring the database on multiple nodes, wait five minutes between each database restore.

**Caution**

E10/100-4 cards lose traffic for approximately 90 seconds when an ONS 15327 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm will appear and clear during this period.

**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 different node names, the circuits will map to the new node name. Cisco recommends keeping a record of the old and new node names.

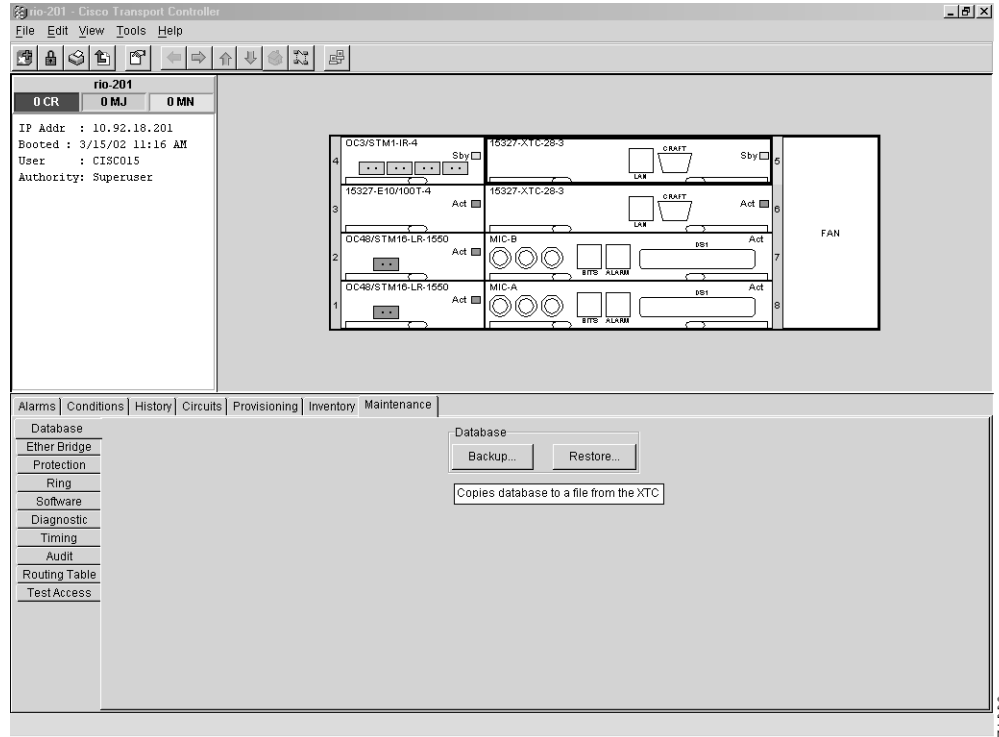
**Note**

You must back up and restore the database for each node on a circuit path in order to maintain a complete circuit

Procedure: Backup the Database

- Step 1** Log into the node where you want to backup the database.
- Step 2** In node view, click the **Maintenance > Database** tabs.

Figure 12-4 Backing up the ONS 15327 database



- Step 3** Click **Backup**.
- Step 4** Save the database on the workstation's hard drive or on network storage. Use an appropriate file name with the file extension .db, for example, database.db.
- Step 5** Click **Save** and click **OK** on the Backup Database Complete dialog box.

Procedure: Restore the Database



Caution

A restore from another node or an earlier backup may affect traffic.



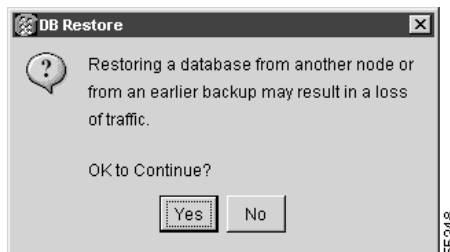
Note

The database must be restored to a compatible software version.

- Step 1** Log into the node where you want to restore the database.
- Step 2** In node view, click the **Maintenance > Database** tabs.

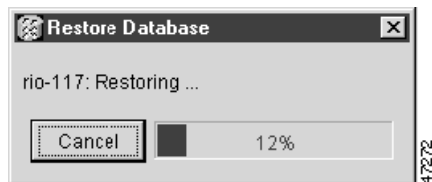
- Step 3** Click **Restore**.
- Step 4** Locate the database file stored on the workstation's hard drive or on network storage.
- Step 5** Click the database file to highlight it.
- Step 6** Click **Open**. The DB Restore dialog box appears. Opening a restore file from another node or from an earlier backup may affect traffic on the login node (Figure 12-5).

Figure 12-5 Restoring the database—traffic loss warning



- Step 7** Click **Yes**. The Restore Database dialog box monitors the file transfer (Figure 12-6).

Figure 12-6 Restoring the XTC database—in-progress notification



- Step 8** Wait for the file to complete the transfer to the XTC.
- Step 9** Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears. Wait for the node to reconnect.

12.5 Reverting to an Earlier Software Load

True Revert allows the system to revert to the protect system software image and its attendant database. The reversion does not affect DCC connectivity or traffic on circuits provisioned prior to the activation of the working software load. All versions of ONS 15327 software support this feature.

The ONS 15327 supports a working and protect software version on each XTC. The protect software version saves the provisioning that existed when the working load was activated. This means that the protect software load can only reinstate the circuits provisioned before the working load was activated. Circuits provisioned after the activation of the working load are lost during a revert.

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.

**Warning**

Working and protect XTCs must have the same version of the protect software load in order to revert to an earlier software load.

**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 to a maintenance release software load does not restore the database and no provisioning is lost. All other reverts do restore the database. (A maintenance release has a three-digit release number, e.g., 2.2.2).

**Note**

Circuits created and provisioning performed after a software load is activated will not reinstate with a revert. The database configuration at the time of activation is reinstated after a revert. This note does not apply to maintenance reverts (e.g., 2.2.2 to 2.2.1).

Procedure: Revert to an Earlier Software Load

- Step 1** Log into the node where you want to perform the revert.
- Step 2** Record the IP address of that node.
- Step 3** In node view, right-click the standby XTC card to reveal a pull-down menu.
- Step 4** Choose **Reset Card**.
- Step 5** Click **Yes** when the “Are You Sure?” dialog box appears.
- Step 6** Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.
- Step 7** Confirm that the XTC is in standby mode after the reset.
- Step 8** Click the **Maintenance > Software** tabs.
- Step 9** Click **Revert**.
The Revert button activates the protect software load. The ONS15327 node reboots and loses its connection to the CTC.
- Step 10** Wait until the software upgrade finishes. This may take as long as 30 minutes.
- Step 11** Completely close the browser.
- Step 12** Restart the browser and log back into the node using the IP address you recorded in Step 2.
The browser downloads the CTC applet for the standby software load.

12.6 XTC-14 Card to XTC-28 Card Upgrade

This section explains how to upgrade XTC-14 cards to XTC-28 cards on an ONS 15327 with live traffic. The procedure is non-service affecting; the upgrade will cause a switch less than 50 ms in duration.

**Note**

The UNEQ-P alarm might be raised during the upgrade if you have E10/E100-4 cards in the system. The alarm will appear and clear within a few seconds.

**Note**

The MEA (card mismatch) alarm appears because CTC recognizes a mismatch between XTC card types. Disregard this alarm; it clears by the end of the procedure.

Step 1

Physically replace the standby XTC-14 card on the ONS 15327 with an XTC-28 card:

- a. Unscrew and open the XTC-14 card ejector.
- b. Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete. Ensure that traffic is flowing over the 14 DS-1 ports.
- c. Open the ejector on the XTC-28 card.
- d. Slide the XTC-28 card into the slot along the guide rails.
- e. Close the ejector and secure the screw.
- f. Wait until the XTC-28 is fully booted and finishes synchronizing its software and database.

**Note**

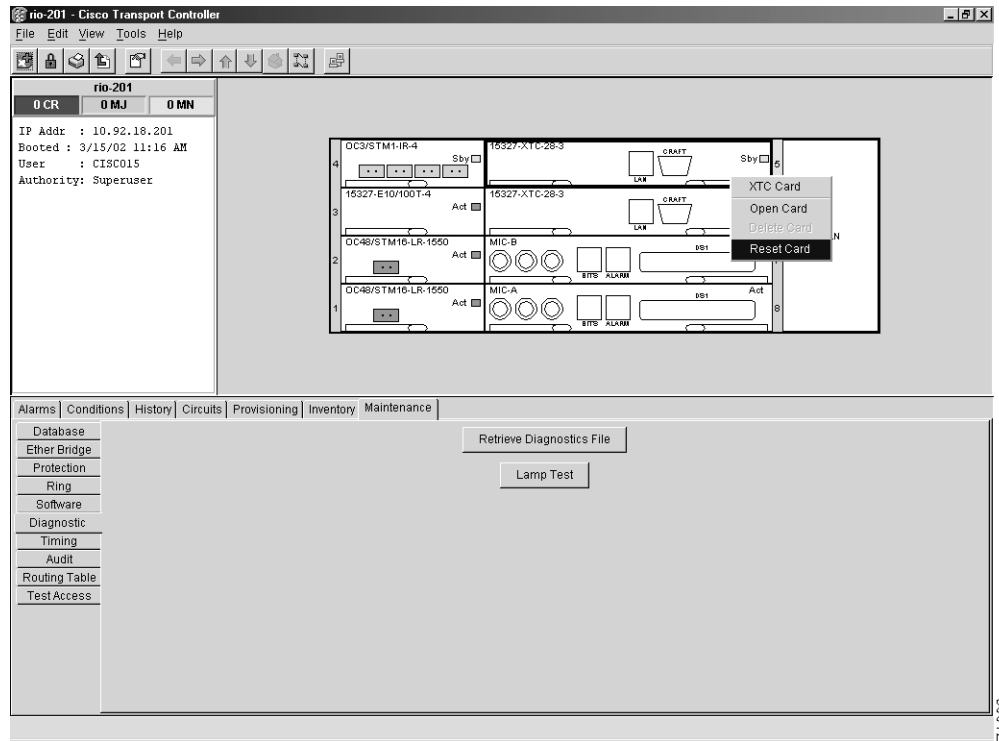
The LEDs will flash while the XTC-28 is loading.

Step 2

After the XTC-28 has finished synchronizing and is in standby mode, reset the active XTC-14:

- a. In node view, right-click on the active XTC-14 and choose **Reset** from the pull-down menu (Figure 12-7).
- b. Traffic switches to the XTC-28.

Figure 12-7 Resetting the XTC card



- Step 3** Physically replace the remaining XTC-14:
- Unscrew and open the XTC-14 card ejector.
 - Slide the card out of the slot. This raises the IMPROPRMVL alarm which will clear when the upgrade is complete.
 - Open the ejector on the XTC-28 card.
 - Slide the XTC-28 card into the slot along the guide rails.
 - Close the ejector and secure the screw.
- Step 4** Wait until the XTC-28 is fully booted and finishes synchronizing its software and database.

12.7 Span Upgrades

A span is the optical fiber connection between two ONS 15327 nodes. In a span 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 in which traffic carried at a lower OC-N rate is transferred to a higher OC-N. You can perform in-service span upgrades for the following ONS 15327 cards:

- OC-12 to OC-48
- OC-12 IR to OC-12 LR
- OC-48 IR to OC-48 LR

To perform a span upgrade, the higher-rate/long-reach optical card must replace the lower-rate/intermediate-reach card in the same slot. If the upgrade is conducted on spans residing in a BLSR, all spans in the ring must be upgraded. The protection configuration of the original lower-rate/intermediate-reach optical card (two-fiber BLSR, UPSR, and 1+1) is retained for the higher-rate/long-reach optical card.

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

The 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. The Span Upgrade procedures can also be used to perform span downgrades.

Cisco recommends using the Span Upgrade Wizard to perform span upgrades from OC-12 to OC-48. Manual Span Upgrade procedures are mainly provided for OC-12 IR to OC-12 LR or OC-48 IR to OC-48 LR span upgrades, or 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.



Warning

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



Caution

Do not perform any other maintenance operations or add any circuits during a span upgrade.



Note

Span upgrades do not upgrade SONET topologies, for example, a 1+1 group to a two-fiber BLSR.



Note

During the upgrade some minor alarms and conditions will be raised and will clear automatically. There should be no service-affecting (SA, Major, or Critical) alarms. If any service-affecting alarms occur, Cisco recommends backing out of the procedure. BLSR Out of Sync alarms will be raised during span upgrades and will clear when the upgrade of all nodes is complete; a four-node BLSR can take up to five minutes to clear all of the Out of Sync alarms. Allow extra time for a large BLSR to clear all of the Out of Sync alarms.

**Note**

If any of the cross connect cards reboot during the span upgrade, you must manually reset the card once the span upgrade procedure is completed on all the nodes in the ring.

Choose from four span upgrade options:

- “Perform a Span Upgrade Using the Span Upgrade Wizard” procedure on page 12-13
- “Perform a Manual Span Upgrade on a Two-Fiber BLSR” procedure on page 12-15
- “Perform a Manual Span Upgrade on a UPSR” procedure on page 12-16
- “Perform a Manual Span Upgrade on a 1+1 Protection Group” procedure on page 12-17

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/intermediate-reach card type. You cannot downgrade if circuits exist on the STSs that will be removed (the higher STSs).

**Note**

During the upgrade some minor alarms and conditions will be raised and will clear automatically. There should be no service-affecting (SA, Major, or Critical) alarms. If any service-affecting alarms occur, Cisco recommends backing out of the procedure.

BLSR Out of Sync alarms will be raised during span upgrades and will clear when the upgrade of all nodes is complete. Allow extra time for a large BLSR to clear all of the Out of Sync alarms.

Procedure: Perform a Span Upgrade Using the Span Upgrade Wizard

**Warning**

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

**Caution**

Do not perform any other maintenance operations or add any circuits during a span upgrade.

**Note**

The Span Upgrade Wizard only supports OC-N span upgrades. It does not support DS-3 upgrades.

**Note**

You must use the Manual Span Upgrades when performing OC-12 IR to OC-12 LR or OC-48 IR to OC-48 LR span upgrades.

Step 1

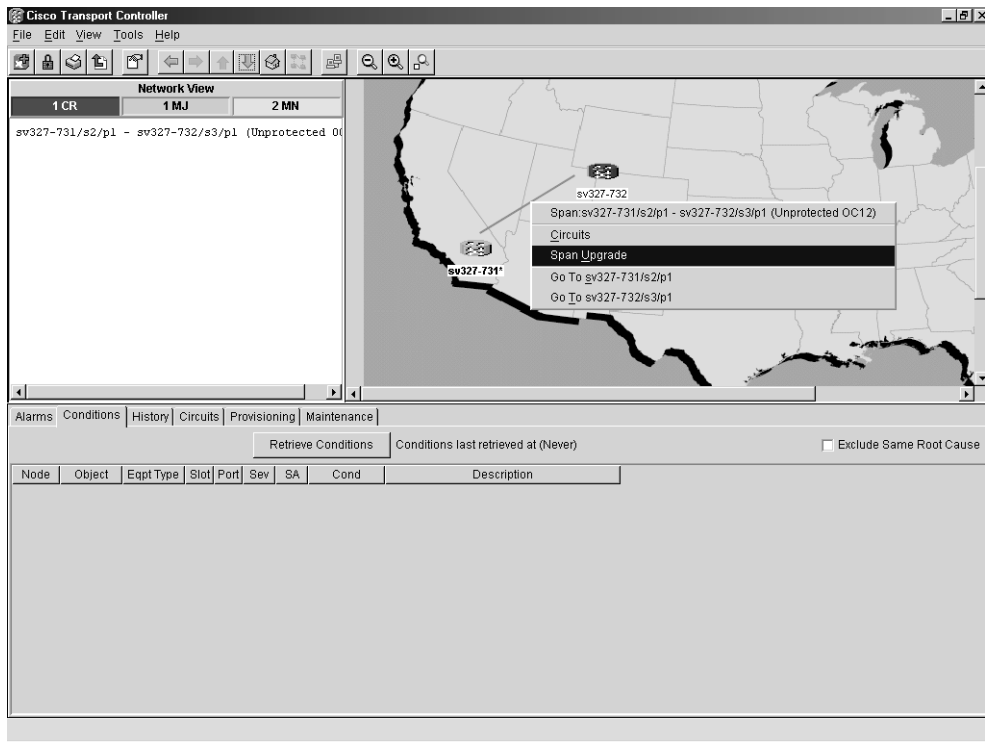
Log into an ONS 15327 and ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present:

- Navigate from the default (node) view to the network view.
- In network view, click on the **Alarms** tab to view a list of current alarms.
- In network view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.

An unresolved alarm or abnormal condition is the most probable reason for upgrade failure. If alarms are present, refer to Chapter 14, “Alarm Troubleshooting.”

- Step 2** In network view, right-click the span you want to upgrade.
- Step 3** Choose **Span Upgrade** from the pull-down menu (Figure 12-8).

Figure 12-8 Span pull-down menu

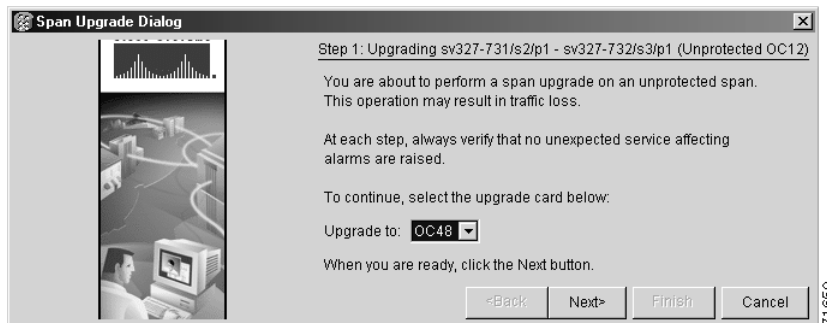


- Step 4** The first Span Upgrade dialog box appears (Figure 12-9). Follow the instructions on the dialog box and the wizard will lead you through the rest of the span upgrade.



Note The <Back button is only enabled on Step 2 of the wizard; because you cannot back out of an upgrade via the wizard, close the wizard and initiate the manual procedure if you need to back out of the upgrade at any point beyond Step 2.

Figure 12-9 Beginning the Span Upgrade Wizard





Note Remember to attach the fiber after installing the OC-N cards.

Procedure: Perform a Manual Span Upgrade on a Two-Fiber BLSR

All spans connecting the nodes in a BLSR must be upgraded before the added bandwidth is available.

-
- Step 1** Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the BLSR that you will upgrade:
- In network view, click the **Alarms** tab to view a list of current alarms.
 - In network view, click the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.
- An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.
- Step 2** Apply a force switch at both span endpoints (nodes) on the span that you will upgrade first:
- At the first endpoint, in node view, click the **Maintenance > Ring** tabs.
 - Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.
 - Click **Apply**.
 - At the second endpoint, in node view, click the **Maintenance > Ring** tabs.
 - Click either the West Switch or the East Switch field and choose **FORCE RING** from the menu.
 - Click **Apply**.
- Step 3** Remove the fiber from both endpoints and ensure that traffic is still running.
- Step 4** Remove the OC-N cards from both endpoints. If you are performing a span upgrade from OC-12 cards to OC-48 cards, proceed to Step 5. If you are performing a span upgrade from IR cards to LR cards of the same type; for example, OC-12 IR to OC-12 LR, proceed to Step 8.
- Step 5** From both endpoints, in node view, right-click on each OC-N slot and choose **Change Card**.
- Step 6** In the Change Card dialog box, choose the new OC-N type.
- Step 7** Click **OK**.
- Step 8** Install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
- Step 9** When cards at both endpoints have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch from both endpoints on the upgraded span:
- At the first endpoint, in node view, click the **Maintenance > Ring** tabs.
 - Click the West Switch or the East Switch field and choose **CLEAR** from the menu.
 - Click **Apply**.
 - At the second endpoint, in node view, click the **Maintenance > Ring** tabs.
 - Click the West Switch or the East Switch field and choose **CLEAR** from the menu.
 - Click **Apply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate/intermediate-reach card.



Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

- Step 10** Repeat these steps for each span in the BLSR.
When all spans in the BLSR have been upgraded, the span upgrade is complete.

Procedure: Perform a Manual Span Upgrade on a UPSR

- Step 1** Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade:
- In node view, click on the **Alarms** tab to view a list of current alarms.
 - In node view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.
- An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.
- Step 2** Apply a force switch on the span that you will upgrade:
- In network view, right-click the span and choose **Circuits**.
 - From the Circuits on Span dialog box in the Switch All UPSR Circuits Away field, choose **FORCE**.
 - Click **Apply**.
- Step 3** Remove the fiber from both endpoints (nodes) on the span and ensure that traffic is still running.
- Step 4** Remove the OC-N cards from both endpoints. If you are performing a span upgrade from OC-12 cards to OC-48 cards, proceed to Step 5. If you are performing a span upgrade from IR cards to LR cards of the same type; for example, OC-12 IR to OC-12 LR, proceed to Step 8.
- Step 5** For both endpoints, in node view, right-click on each OC-N slot and choose **Change Card**.
- Step 6** In the Change Card dialog box, choose the new OC-N type.
- Step 7** Click **OK**.
- Step 8** Install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become active.
- Step 9** When cards at both span endpoints have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch:
- In network view, right-click the span and choose **Circuits**.
 - From the Circuits on Span dialog box in the Switch All UPSR Circuits Away field choose **CLEAR**.
 - Click **Apply**.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate/intermediate-reach card.



Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

Procedure: Perform a Manual Span Upgrade on a 1+1 Protection Group

When upgrading a 1+1 group, upgrade the protect line first regardless of which line is active. Both lines in a 1+1 group must be upgraded before the added bandwidth will be available.



Note If the switching mode is bidirectional in the 1+1 protection group, apply the Force command to only one end of the span, not both. The Clear command will apply to the end the Force was applied to. If the Force command is applied to both ends when the switching mode is bidirectional, it will cause a switch of more than 50 ms in duration.

- Step 1** Ensure that no alarms or abnormal conditions (regardless of severity), including LOS, LOF, AIS-L, SF, SD, and FORCED-REQ-RING are present on the span that you will upgrade:
- In node view, click on the **Alarms** tab to view a list of current alarms.
 - In node view, click on the **Conditions** tab and click the **Retrieve Conditions** button to view a list of current conditions.
- An unresolved alarm or abnormal condition is the most probable reason for upgrade failure.
- Step 2** Apply a force switch on the ports that you will upgrade, beginning with the protect port:
- In node view, click the **Maintenance > Protection** tabs.
 - Under Protection Groups, choose the 1+1 protection group.
 - Under Selected Group, choose the protect port (regardless if it is active or standby).
 - From Switch Commands, click **Force**.
 - Click **Yes** on the confirmation dialog box.
- Step 3** Repeat Step 2 for each port.
- Step 4** Remove the fiber from both endpoints on the span and ensure that traffic is still running.
- Step 5** Remove the OC-N cards from both span endpoints. If you are performing a span upgrade from OC-12 cards to OC-48 cards, proceed to Step 6. If you are performing a span upgrade from IR cards to LR cards of the same type; for example, OC-12 IR to OC-12 LR, proceed to Step 9.
- Step 6** At both ends of the span, in node view, right-click the OC-N slot and choose **Change Card**.
- Step 7** In the Change Card dialog box, choose the new OC-N type.
- Step 8** Click **OK**.
- Step 9** Install the new OC-N cards in both endpoints and attach the fiber to the cards. Wait for the IMPROPRMVL alarm to clear and the cards to become standby.
- Step 10** When cards on each end of the line have been successfully upgraded and all the facility alarms (LOS, SD or SF) are cleared, remove the forced switch:
- In node view for either endpoint, click the **Maintenance > Protection** tabs.
 - Under Protection Groups, choose the 1+1 protection group.

- c. Under Selected Group, choose the port with the force on it.
- d. From Switch Commands, click **Clear**.
- e. Click **Yes** on the confirmation dialog box.

The forced switch clears and traffic is running. If you have lost traffic, perform a downgrade. The procedure for downgrading is the same as upgrading except that you choose a lower-rate/intermediate-reach card.



Note You cannot downgrade if circuits exist on the STSs that you will remove (the higher STSs).

- Step 11** Repeat these steps for the other line in the 1+1.
When the other line in the 1+1 has been upgraded, the span upgrade is complete.

12.8 Inhibit Protection Switching

This procedure describes how to apply a lock on or lock out and how to remove a lock on or lock out on OC-12 or OC-48 protection groups.

Procedure: Apply a Lock On

- Step 1** Use the following rules to determine if you can put the intended card in a Lock On state:
 - For a 1+1 optical protection group, only the working card can be placed in the Lock On state.
- Step 2** Log into the node where you will apply the Lock On.
- Step 3** Click the **Maintenance > Protection** tabs.
- Step 4** Under Protection Groups, click on the protection group where you want to apply a lock on.
- Step 5** If you determine that the protect card is inactive and you want to apply the lock on to the protect card, make the protect card active:
 - a. Under Selected Group, click the protect card.
 - b. Under switch Commands, click **Switch**.
- Step 6** Under Selected Group, click the active card you want to lock traffic onto.
- Step 7** From Inhibit Switching, click on **Lock On**.
- Step 8** Click **Yes** on the confirmation dialog box.

The Lock On has been applied and traffic cannot be switched to the opposite card. To clear the Lock On, see the “Clear a Lock On or Lock Out” procedure on page 12-19.

Procedure: Apply a Lock Out



Note Multiple Lock Outs in the same protection group is not allowed.

-
- Step 1** Use the following rules to determine if you can put the intended card in a Lock Out state:
- For a 1+1 optical protection group, only the protect card can be placed in the Lock Out state.
- Step 2** Log into the node where you will apply the Lock Out.
- Step 3** In Node view, click the **Maintenance > Protection** tabs.
- Step 4** Under Protection Groups, click on the protection group that contains the card you want to lock out.
- Step 5** Under Selected Group, click the card you want to lock traffic out of.
- Step 6** From Inhibit Switching, click on **Lock Out**.
- Step 7** Click **Yes** on the confirmation dialog box.

The lock out has been applied and traffic is switched to the opposite card. To clear the Lock Out, see the “Clear a Lock On or Lock Out” procedure on page 12-19.

Procedure: Clear a Lock On or Lock Out

-
- Step 1** Log into the node where you will clear the Lock Out or Lock On.
- Step 2** Click the **Maintenance > Protection** tabs.
- Step 3** Under Protection Groups, click the protection group that contains the card you want to clear.
- Step 4** Under Selected Group, click the card you want to clear.
- Step 5** From Inhibit Switching, click **Unlock**.
- Step 6** Click **Yes** on the confirmation dialog box.
- The Lock On or Lock Out is cleared.
-

12.9 Network Tests

Use loopbacks and hairpins to test newly-created circuits before adding live traffic or to logically isolate the source of a network failure. All ONS 15327 line (traffic) cards, except Ethernet cards, allow loopbacks and hairpins.



Caution

On OC-N cards, the entire card is put into loopback rather than an individual STS. Exercise caution when using loopbacks on an OC-N card carrying live traffic.

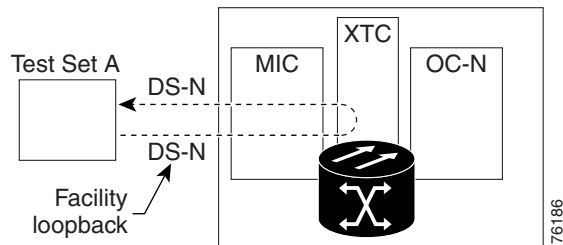
12.9.1 Network Test Types

A facility loopback tests the line interface of a card and related cabling. To test, put a facility loopback on a card and use a test set to run traffic over the loopback. A successful facility loopback eliminates the line interface of the card or cabling plant as the cause or potential cause of a network problem. In the ONS 15327 system, the Mechanical Interface (MIC-28-3-A or MIC-28-3-B) card contain ports for DS-1 or DS-3 traffic. Figure 12-10 shows a facility loopback on an XTC-14 or XTC-28-3 card.

**Caution**

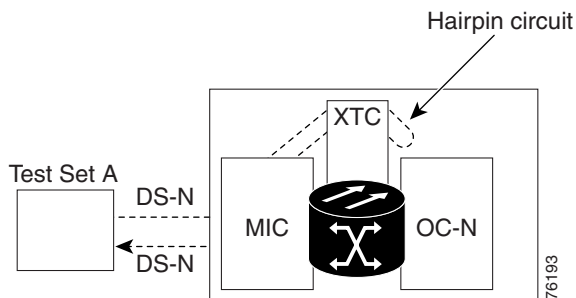
Before performing a facility loopback on an OC-N card, make sure there is another SDCC path to the ONS 15327 containing the OC-N card being put in loopback. A second SDCC path is necessary to provide a non-looped path to log into the ONS 15327 containing the OC-N card being put in loopback to enable removal of the facility loopback. This is not necessary if you are directly connected to the ONS 15327 containing the OC-N card being put in facility loopback.

Figure 12-10 The facility loopback process on an XTC card



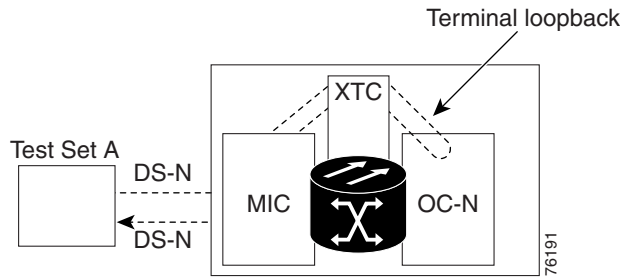
A hairpin circuit brings traffic in and out on a DS-N port instead of sending the traffic onto the OC-N. A hairpin loops back only the specific STS or VT circuit and does not cause an entire OC-N port to loop back, which would drop all traffic on the OC-N port. The hairpin allows you to test a circuit on nodes running live traffic.

Figure 12-11 The hairpin circuit process on an OC-N card



A terminal loopback tests a circuit path through the XTC card and as it loops back from the line card being tested. Figure 12-12 shows a terminal loopback set on an OC-N card. The test-set traffic comes in on the MIC card DS-N ports and goes through the XTC card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the line interface and sends it through the XTC card to the MIC card. This test verifies that the XTC cross-connect circuit paths are valid, but does not test the line interface on the OC-N card. To test the line interface on an OC-N card, connect an optical test set to the OC-N card ports and perform a facility loopback or use a loopback or hairpin on a card that is farther along the circuit path.

Figure 12-12 The terminal loopback process on an OC-N card



12.10 Network Test Procedures

Facility loopbacks, hairpin circuits and terminal loopbacks are often used together to test the circuit path through the network or to logically isolate a fault. Performing a network test at each point along the circuit path systematically eliminates possible points of failure. This example tests an XTC circuit on a two-node bidirectional line switched ring (BLSR). Using a series of facility loopbacks, hairpin circuits, and terminal loopbacks, the path of the circuit is traced and the possible points of failure eliminated.

A logical progression of five network test procedures apply to this scenario:

1. A facility loopback on the source-node XTC card,
2. A hairpin on the source-node XTC card,
3. A hairpin on the destination-node OC-N card,
4. A terminal loopback to the destination-node XTC card, and
5. A facility loopback to the destination XTC card.



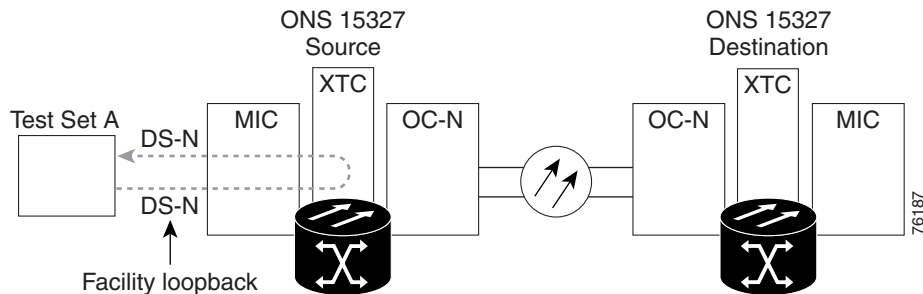
Note

These procedures are performed when power connections to the node(s) or site(s) are assumed to be within necessary specifications. If the network tests do not isolate the problems, troubleshoot outward for power failure.

12.10.1 Perform a Facility Loopback on a Source XTC Card

The first test is a facility loopback test performed on the first active card in the network circuit; in this example, the test is routed through the MIC card and performed on the XTC card in the source node. Completing a successful facility loopback on this card eliminates the cabling, MIC card, and XTC card as possible failure points.

Figure 12-13 Facility loopback on a source XTC card

**Caution**

Performing a loopback on an in-service circuit is service-affecting.

**Note**

Loopbacks operate only on in-service ports.

Procedure: Create the Facility Loopback on the Source XTC Card

- Step 1** Connect an electrical test set to the port you are testing. Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the MIC card, which will interface with the XTC card. Both transmit (Tx) and receive (Rx) connect to the same port. Adjust the test set accordingly.
- Step 2** Set the port into facility loopback mode.

**Note**

It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

- Step 3** Proceed to the “Test the Facility Loopback” procedure on page 12-22.

Procedure: Test the Facility Loopback

- Step 1** If the test set is not already sending traffic, send test-set traffic on the loopback.
- Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good loop, no further testing is necessary with the facility loopback. Clear the loopback circuit before testing the next segment of the network circuit path. Proceed to the “Perform a Hairpin Circuit on a Source Node XTC Card” procedure on page 12-24.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty MIC card, faulty XTC card, or faulty cabling from the DS-N port. Proceed to the “Test the DS-N Cabling” procedure on page 12-23.

Procedure: Test the DS-N Cabling

- Step 1** Replace the suspect cabling (the cables from the test set to the MIC ports) with a known-good cable.
- Step 2** If a known-good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the MIC and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or suspect.
- Step 3** Resend test-set traffic on the loopback circuit with a known-good cable installed.
- Step 4** If the test set indicates a good circuit, the problem was probably the defective cable.
- Make sure the faulty cable is replaced with known-good cable (such as the cable used for testing or another cable that has been tested before installation).
 - Clear the loopback circuit before testing the next segment of the network circuit path.
 - Proceed to the “Perform a Hairpin Circuit on a Source Node XTC Card” procedure on page 12-24.
- Step 5** If the test set indicates a faulty circuit, the problem may be a faulty card. Proceed to the “Test the XTC Card” procedure on page 12-23.
-

Procedure: Test the XTC Card

- Step 1** Replace the suspect card with a known-good card.
- Step 2** Resend test-set traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably a defective card. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- Make sure the faulty card is replaced with known-good card (such as the card used for testing or another card which has been tested before installation).
 - Clear the loopback circuit before testing the next segment of the network circuit path.
- Step 4** If the MIC card was at fault and has been replaced successfully, proceed to the “Perform a Hairpin Circuit on a Source Node XTC Card” procedure on page 12-24.
- Step 5** If the MIC card was not shown to be at fault but the loopback test was unsuccessful, proceed to the “Test the MIC Card” procedure on page 12-23.
-

Procedure: Test the MIC Card

- Step 1** Replace the suspect card with a known-good card.
- Step 2** Resend test-set traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably a defective card. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- Make sure the faulty card is replaced with known-good card (such as the card used for testing or another card which has been tested before installation).

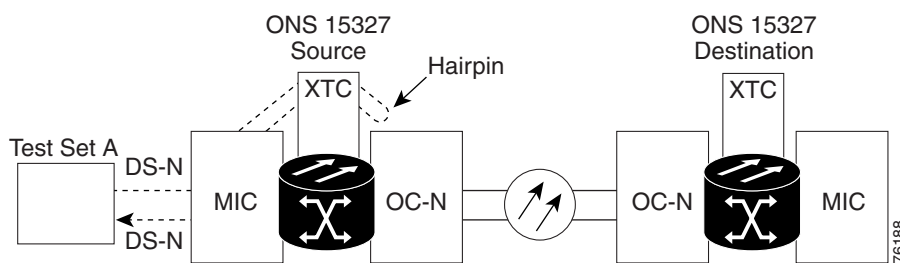
b. Clear the loopback circuit before testing the next segment of the network circuit path.

Step 4 If the MIC card was at fault and has been replaced successfully, proceed to the “Perform a Hairpin Circuit on a Source Node XTC Card” procedure on page 12-24.

12.10.2 Perform a Hairpin Circuit on a Source Node XTC Card

The second loopback test is a hairpin circuit performed on the first XTC card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through this card eliminates the possibility that the source XTC card is the cause of the faulty circuit.

Figure 12-14 Hairpin circuit on a source node XTC card



Note

An XTC card is required to operate the ONS 15327 and can be used in a redundant or non-redundant configuration.

Procedure: Create the Hairpin Loopback Circuit on the Source Node

- Step 1** Connect an electrical test set to the port you are testing.
- If you just completed the “Test the Facility Loopback” procedure on page 12-22, leave the electrical test set hooked up to the MIC card.
 - If you are starting the current procedure without the electrical test set hooked up to the MIC card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the MIC connectors for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.
 - Adjust the test set accordingly.
- Step 2** Use CTC to set up the hairpin loopback on the port being tested.
- Step 3** Confirm that the newly-created circuit appears with a direction column noting that this circuit is 1-way.
- Step 4** Proceed to the “Test the Hairpin Loopback Circuit” procedure on page 12-25.

Procedure: Test the Hairpin Loopback Circuit

-
- Step 1** If the test set is not already sending traffic, send test-set traffic on the loopback circuit.
- Step 2** Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the hairpin loopback circuit.
- Clear the hairpin loopback circuit before testing the next segment of the network circuit path.
 - Proceed to the “Perform a Hairpin on a Destination Node XTC Card” procedure on page 12-26.
- Step 4** If the test set indicates a faulty circuit, there may be a problem with the XTC card. Proceed to the “Test the Alternate Source XTC Card” procedure on page 12-25.
-

Procedure: Test the Alternate Source XTC Card

-
- Step 1** Perform a software reset on the active XTC card.



Caution XTC side switches are service-affecting. Any live traffic on any card in the node will endure a hit of up to 50 ms.



Note After the active XTC goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

- Step 2** Resend test-set traffic on the loopback circuit. The test-set traffic now travels through the alternate XTC card.
- Step 3** If the test set indicates a faulty circuit, assume the XTC card is not causing the problem.
- Clear the loopback circuit before testing the next segment of the network circuit path.
 - Proceed to the “Perform a Hairpin on a Destination Node XTC Card” procedure on page 12-26.
- Step 4** If the test set indicates a good circuit, the problem may be a defective card. To confirm a defective original XTC card, proceed to the “Retest the Original Source XTC Card” procedure on page 12-25.
-

Procedure: Retest the Original Source XTC Card

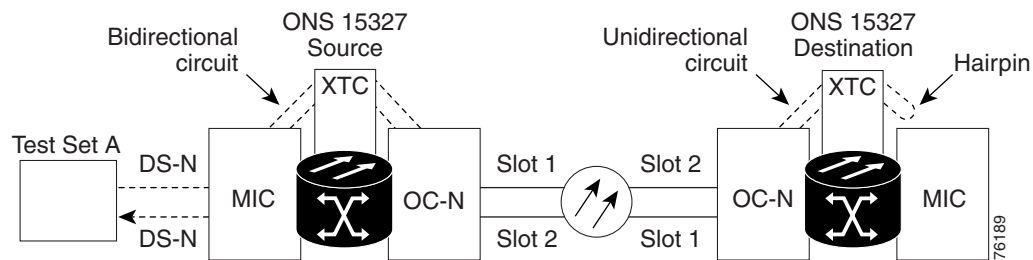
-
- Step 1** Perform a side switch of the XTC cards to make the original card the active card.
- Step 2** Resend test-set traffic on the loopback circuit.
- Step 3** If the test set indicates a faulty circuit on the original card, the problem is probably the defective card.
- Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
 - Make sure the defective cross-connect card is replaced (such as with the former standby card, or with another known-good card).

- c. Clear the loopback circuit before testing the next segment of the network circuit path.
 - d. Proceed to the “Perform a Hairpin on a Destination Node XTC Card” procedure on page 12-26.
- Step 4** If the test set indicates a good circuit, the original XTC card may have had a temporary problem that was cleared by the side switch.
- a. Clear the loopback circuit before testing the next segment of the network circuit path.
 - b. Proceed to the “Perform a Hairpin on a Destination Node XTC Card” procedure on page 12-26.

12.10.3 Perform a Hairpin on a Destination Node XTC Card

The third test is a hairpin circuit on the XTC card in the destination node. To perform this test, you must also create a bidirectional circuit from the source MIC card to the source OC-N node in the transmit direction. Creating the bidirectional circuit and completing a successful hairpin eliminates the possibility that the source and destination OC-N cards, the source and destination XTC cards, or the fiber span is responsible for the faulty circuit.

Figure 12-15 Hairpin on a destination node XTC card



Procedure: Create the Hairpin Loopback Circuit on the Destination Node XTC Card

- Step 1** Connect an electrical test set to the port you are testing.
- Step 2** Use CTC to set up the source loopback circuit on the port being tested.
- Step 3** Use CTC to set up the destination loopback circuit on the port being tested.



Note The destination loopback circuit on a port is a one-way test.

For example in a typical east-to-west slot configuration, a slot 1 (east) OC-N card on the source node is one end of the fiber span, and the slot 2 (west) OC-N card on the destination node is the other end.

- Step 4** Verify that the circuits connect to the correct slots. For example, source node/Slot 1 OC-N card (east slot) to destination node/Slot 2 (west slot). If two east slots or two west slots are connected, the circuit will not work. Except for the distinct slots, all other circuit information, such as ports, should be identical.

- Step 5** Proceed to the “Test the Hairpin Loopback Circuit on the Destination Node XTC Card” procedure on page 12-27.
-

Procedure: Test the Hairpin Loopback Circuit on the Destination Node XTC Card

- Step 1** If the test set is not already sending traffic, send test-set traffic on the loopback circuit.
- Step 2** Examine the test traffic received by the test set. Look for errors or any other signal information indicated by the test set.
- Step 3** If the test set indicates a good circuit, no further testing is necessary with the loopback circuit.
- Clear the loopback circuit before testing the next segment of the circuit path.
 - Proceed to the “Perform a Terminal Loopback on a Destination XTC Card” procedure on page 12-28.
- Step 4** If the test set indicates a faulty circuit, the problem may exist with the destination XTC card. Proceed to the “Test the Alternate Destination XTC Card” procedure on page 12-27.
-

Procedure: Test the Alternate Destination XTC Card

- Step 1** Perform a software reset on the active XTC card.



Caution XTC side switches are service-affecting. Any live traffic on any card in the node will endure a hit of up to 50 ms.



Note After the active XTC goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

- Step 2** Resend test-set traffic on the loopback circuit. The test-set traffic routes through the alternate XTC card.
- Step 3** If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem.
- Clear the loopback circuit before testing the next segment of the network circuit path.
 - Proceed to the “Perform a Terminal Loopback on a Destination XTC Card” procedure on page 12-28.
- Step 4** If the test set indicates a good circuit, the problem could be a defective card. To confirm a defective original XTC card, proceed to the “Retest the Original Destination XTC Card” procedure on page 12-28.
-

Procedure: Retest the Original Destination XTC Card

Step 1 Perform a side switch of the XTC cards to make the original card the active card.



Note After the active XTC goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 2 Resend test-set traffic on the loopback circuit. The test-set traffic routes through the original XTC card.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card.

- a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- b. Make sure the defective XTC card is replaced.
- c. Clear the loopback circuit before testing the next segment of the network circuit path.
- d. Proceed to the “Perform a Terminal Loopback on a Destination XTC Card” procedure on page 12-28.

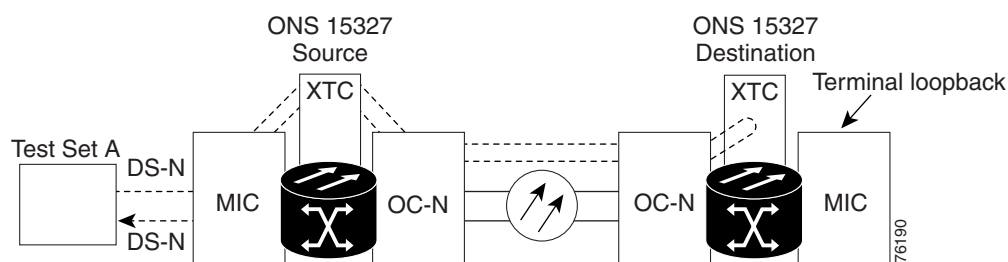
Step 4 If the test set indicates a good circuit, the XTC card may have had a temporary problem that was cleared by the side switch.

- a. Clear the loopback circuit before testing the next segment of the network circuit path.
- b. Proceed to the “Perform a Terminal Loopback on a Destination XTC Card” procedure on page 12-28.

12.10.4 Perform a Terminal Loopback on a Destination XTC Card

This test is a terminal loopback performed on the fourth line card in the circuit. In the following example, the XTC card in the destination node is tested. First, create a bidirectional circuit that starts on the source node DS-N port and terminates on the destination node DS-N port, then proceed with the terminal loopback test. Completing a successful terminal loopback to a destination node XTC card port verifies that the circuit is good up to the destination XTC.

Figure 12-16 Terminal loopback on a destination XTC card



Caution

Performing a loopback on an in-service circuit is service-affecting.

Procedure: Create the Terminal Loopback on a Destination XTC Card

-
- Step 1** Connect an electrical test set to the port you are testing:
- If you are starting the current procedure with the electrical test set hooked up to the MIC card in the source node, leave the test set hooked up.
 - If you are starting the current procedure without the electrical test set hooked up to the MIC card, use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the MIC connectors for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port.
- Step 2** Use CTC to set up the source loopback circuit on the port being tested.
- Step 3** Use CTC to set up the terminal loopback circuit on the port being tested.
- Step 4** Confirm that the newly created circuit appears on a Circuits screen row with a direction column that shows a 2-way circuit.



Note Loopbacks operate only on in-service ports.



Note It is normal for an alarm to appear during a loopback setup. The alarm clears when you remove the loopback.

- Step 5** Proceed to the “Test the Terminal Loopback Circuit on the Destination XTC Card” procedure on page 12-29.
-

Procedure: Test the Terminal Loopback Circuit on the Destination XTC Card

-
- Step 1** If the test set is not already sending traffic, send test-set traffic on the loopback circuit.
- Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.
- Step 3** If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Proceed to the “Perform a Facility Loopback on a Destination XTC Card” procedure on page 12-30.
- Step 4** If the test set indicates a faulty circuit, the problem may be a faulty card. Proceed to the “Test the Destination XTC Card” procedure on page 12-30.
-

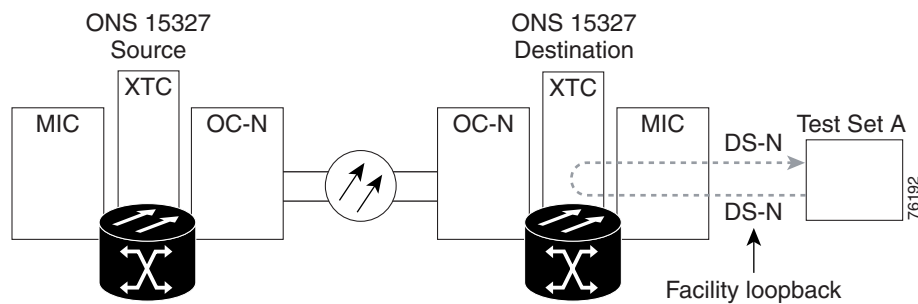
Procedure: Test the Destination XTC Card

-
- Step 1** Replace the suspect card with a known-good card.
- Step 2** Resend test-set traffic on the loopback circuit with a known-good card.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card.
- a. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
 - b. Replace the defective XTC card.
 - c. Proceed to the “Perform a Facility Loopback on a Destination XTC Card” procedure on page 12-30.
-

12.10.5 Perform a Facility Loopback on a Destination XTC Card

The final test is a facility loopback performed on the last port in the circuit, in this case the XTC card in the destination node. Completing a successful facility loopback on this card eliminates the possibility that the destination node cabling, MIC card, or line interface is responsible for a faulty circuit.

Figure 12-17 Facility loopback on a destination XTC card



Caution

Performing a loopback on an in-service circuit is allowed but is service-affecting.



Note

Loopbacks operate only on in-service ports.

Procedure: Create the Facility Loopback on a Destination XTC Card

Step 1 Connect an electrical test set to the port you are testing. Use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the MIC connectors for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Adjust the test set accordingly.

Step 2 Set the port into facility loopback mode.



Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

Step 3 Proceed to the “Test the Destination Facility Loopback” procedure on page 12-31.

Procedure: Test the Destination Facility Loopback

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the loopback circuit. Clear the facility loopback. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

Step 4 If the test set indicates a faulty circuit, the problem may be a faulty MIC card, faulty cabling from the MIC card. Proceed to the “Test the DS-N Cabling” procedure on page 12-23.

Procedure: Test the DS-N Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the MIC ports) with a known-good cable.

Step 2 If a known-good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the MIC and connect the cable to the transmit (Tx) and receive (Rx) terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 3 Resend test-set traffic on the loopback circuit with a known-good cable installed.

Step 4 If the test set indicates a good circuit, the problem was probably the defective cable. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

- a. Make sure the faulty cable is replaced with known-good cable (such as the cable used for testing or another cable which has been tested before installation).
- b. Clear the loopback circuit before testing the next segment of the network circuit path.

Step 5 If the test set indicates a faulty circuit, the problem may be a faulty card. Proceed to the “Test the XTC Card” procedure on page 12-32.

Procedure: Test the XTC Card

- Step 1** Replace the suspect card with a known-good card.
- Step 2** Resend test-set traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- a. Make sure the faulty card is replaced with a known-good card (such as the card used for testing or another card that has been tested before installation).
 - b. Clear the loopback circuit. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- Step 4** If the test set indicates a faulty circuit, proceed to the “Test the MIC Card” procedure on page 12-32.
-

Procedure: Test the MIC Card

- Step 1** Replace the suspect card with a known-good card.
- Step 2** Resend test-set traffic on the loopback circuit with a known-good card installed.
- Step 3** If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the returned materials authorization (RMA) process. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- a. Make sure the faulty card is replaced with a known-good card (such as the card used for testing or another card that has been tested before installation).
 - b. Clear the loopback circuit. The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.
- Step 4** If the test set indicates a faulty circuit, contact the Cisco Technical Assistance Center.
-

12.11 Creating Diagnostic Files

When working with ONS 15327 customer support, you may need to record system information to a file and send it to technical personnel for diagnosis.

Procedure: Create a Diagnostic File

-
- Step 1** Log into the node where you will retrieve the diagnostic files.
 - Step 2** In node view, click the **Maintenance > Diagnostic** tabs.
 - Step 3** Click **Retrieve Diagnostics File**.
 - Step 4** In the Save dialog box, type a file name. Do not add an extension to the file name; the CTC extension is added automatically.
 - Step 5** Choose a directory where you want to save the file.
 - Step 6** Click **Save**. A dialog box confirms a successful file transfer. (The dialog box may take 20-30 seconds to display.)
 - Step 7** E-mail the diagnostic file to the address given to you by customer support.
-

12.12 Optic Fiber Cleaning

You can clean the optic fiber connected to an ONS 15327 node according to local site practice or by following the procedures below.



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.



Note

Replace all dust caps whenever the equipment will be unused for 30 minutes or more.

Procedure: Clean Fiber Connectors and Adapters with Alcohol and Dry Wipes

-
- Step 1** Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.
 - Step 2** Replace any damaged fiber connectors.
 - Step 3** Remove the dust cap from the fiber connector.
 - Step 4** Wipe the connector tip with the pre-moistened alcohol wipe.
 - Step 5** Blow dry using filtered air.
 - Step 6** Use an inspection microscope to inspect each fiber for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 3–5.
 - Step 7** Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.



Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a Cletop stick swab (14100400).

Procedure: Clean Fiber Connectors with Cletop

- Step 1** Using an inspection microscope, inspect each fiber connector for dirt, cracks, or scratches.
- Step 2** Replace any damaged fiber connectors.
- Step 3** Remove the dust cap from the fiber connector.
- Step 4** Press the lever down to open the shutter door. Each time you press the lever, you expose a clean wiping surface.
- Step 5** Insert the connector into the Cletop cleaning cassette slot, rotate one quarter turn, and gently swipe downwards.
- Step 6** Use an inspection microscope to inspect each fiber for dirt, cracks, or scratches. If the connector is not clean, repeat Steps 3–5.
- Step 7** Insert the fiber connector into the applicable adapter or attach a dust cap to the fiber connector.



Note If you must replace a dust cap on a connector, first verify that the dust cap is clean. To clean the dust cap, wipe the outside of the cap using a dry, lint-free wipe and the inside of the dust cap using a Cletop stick swab (14100400).

Procedure: Clean the Fiber Adapters

- Step 1** Remove the dust plug from the fiber adapter.
 - Step 2** Using an inspection microscope, inspect each adapter for dirt, cracks, or scratches.
 - Step 3** Insert a Cletop stick swab (14100400) into the adapter opening and rotate the swab.
 - Step 4** Use an inspection microscope to inspect each fiber for dirt, cracks, or scratches. If the connector is not clean, repeat Step 3.
 - Step 5** Place dust plugs on the fiber adapters when not in use.
-

12.13 Power Down the ONS 15327

The following procedure describe how to power down a Cisco ONS 15327.



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



The following procedure is designed to minimize traffic outages when powering down nodes, but traffic will be lost if you delete and recreate circuits that passed through a working node.



Always use the supplied ESD wristband when working with the Cisco ONS 15327.

Procedure: Power Down the ONS 15327

- Step 1** Identify the node that you want to power down. If no cards are installed, go to Step 11. If cards are installed, log into the node.
- Step 2** In network view, verify that the node is not connected to a working network:
- If the node is part of a working network, log out of the node and remove the node from the network and proceed to Step 3.
 - If the node is not connected to a working network and the current configurations are no longer required, proceed to Step 3.



Current configurations will be saved if Steps 3–11 are skipped.

- Step 3** In node view, click the **Circuits** tab and verify that no circuits are displayed. If no circuits are displayed, proceed to Step 4. If circuits are displayed, delete all the circuits that originate or terminate in the node:
- Click the circuits that need to be deleted and click **Delete**.
 - Click **Yes**.

Repeat until no circuits are displayed.

- Step 4** In node view, click the **Provisioning > Protection** tabs and verify that no protection groups are displayed. If no protection groups are displayed, proceed to Step 5. If protection groups are displayed, delete the protection groups:

- Click the protection group that needs to be deleted and click **Delete**.
- Click **Yes**.

Repeat until no protection groups are displayed.

- Step 5** In node view, click the **Provisioning > SONET DCC** tabs and verify that no SDCC terminations are displayed. If no SDCC terminations are displayed, proceed to Step 6. If SDCC terminations are displayed, delete the SDCC terminations:

- Click the SDCC Termination that needs to be deleted and click **Delete**.
- Click **Yes**.

Repeat until no SDCC Terminations are displayed.

- Step 6** For each installed card, place all ports in Out of Service status:
- a. In card view, click the **Provisioning > Line** tabs.
 - b. Click under the Status column for each port and choose **Out of Service**.
- Step 7** Remove all fiber connections to the cards.
- Step 8** In node view, right-click on an installed card and click **Delete**.
- Step 9** Click **Yes**.
- Step 10** After you have deleted the card, unscrew and open the card ejector and remove it from the node. Repeat Steps 6–10 for each installed card.
- Step 11** Shut off the power from the power supply that feeds the node.
- Step 12** Disconnect the node from its external fuse source.
- Step 13** Store all cards removed and update inventory records according to local site practice.
-



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 Chapter 1, “Hardware Installation.”



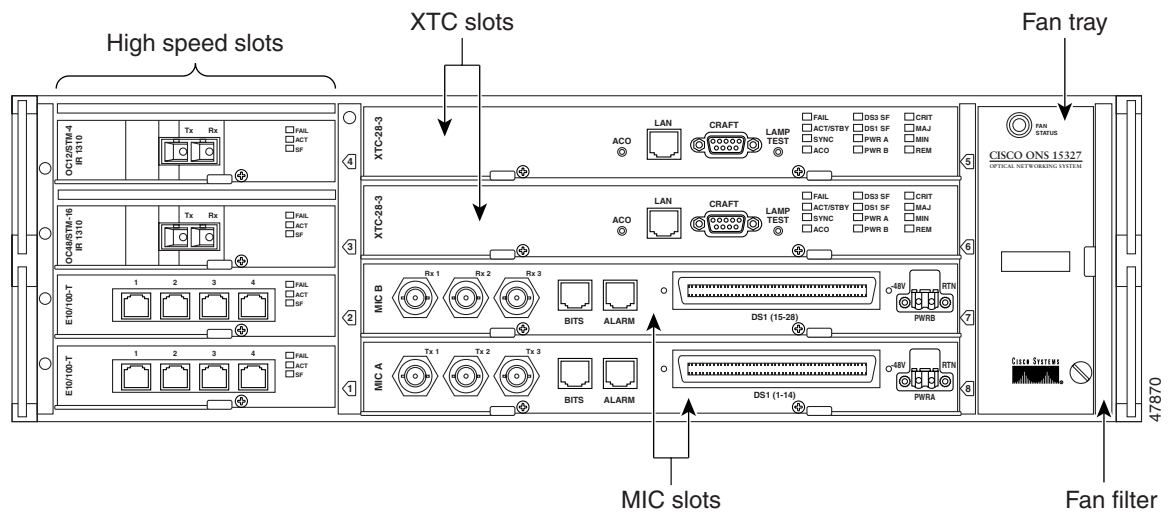
Note

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

13.1 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 13-1 shows the ONS 15327 slot assignments.

Figure 13-1 ONS 15327 slot assignments



13.1.1 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.

13.1.2 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.

13.1.3 Optical Cards

The optical cards include the OC3 IR 4 1310, OC12 IR 1310, OC12 LR 1550, OC48 IR 1310, and the OC48 LR 1550. The OC3 IR 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.

13.1.4 Ethernet Card

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

13.2 Card Protection

The ONS 15327 provides both optical and electrical protection methods. The XTC-14 card provides electrical-protection circuitry for DS-1s. The XTC-28-3 provides electrical-protection circuitry for DS-1s and DS-3s. The optical cards use 1+1 protection, in which one optical port protects another optical port of the same type. This section describes the protection options.

13.2.1 Unprotected

Unprotected cards are not included in a protection scheme; therefore, a card failure or a signal error causes lost data. Because no bandwidth is reserved for protection, unprotected schemes maximize the available ONS 15327 bandwidth. On the ONS 15327, only OC-N cards can run unprotected. DS-N cards are protected by default because of the automatically created protection group, XTCProtGroup.

13.2.2 Electrical Protection

The XTC cards provide protection for the DS-1 and DS-3 circuits and for each other when installed in a redundant configuration (when XTCs are installed in Slots 5 and 6). The ONS 15327 provides 1:1 protection by default. In 1:1 protection, a working card is paired with a protect card of the same type.

Electrical protection in the ONS 15327 is bidirectional; after a failure, automatic protection switching (APS) switches the traffic from the working card to the protect card, where the signal stays until it is manually switched back. In the ONS 15327, the working XTC card is installed in Slot 6, the protect XTC is installed in Slot 5. If any circuits fail on the working XTC, all functionality switches to the protect XTC card (not just the failed circuit).

13.2.3 Optical Card Protection

The ONS 15327 currently supports 1+1 protection to create redundancy for optical cards. Working and protection spans are defined by card slot pairs. The same optical cards in any two slots can be paired for protection. 1+1 protection pairs a single working card with a single dedicated protect card. If the working card fails, the protect card takes over.

13.2.4 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 non-revertive 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 non-revertive by default; revertive switching is easily provisioned using Cisco Transport Controller (CTC).

The ONS 15327 Release 3.3 supports unidirectional path switched ring (UPSR) and bidirectional line switched ring (BLSR) configurations, providing additional methods of optical protection.

13.3 XTC Cards (XTC-28-3/XTC-14)

This section describes the features and functions of the XTC cards.

13.3.1 XTC Card Description

The XTC cards perform system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection and resolution, SONET DCC 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 non-redundant configuration. Figure 13-2 shows the XTC-28-3 faceplate, Figure 13-3 shows the XTC-14 faceplate, and Figure 13-5 diagrams the functionality.

**Note**

You can connect to either the active or standby XTC using the LAN or CRAFT port, but 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 13-2 XTC-28-3 card faceplate

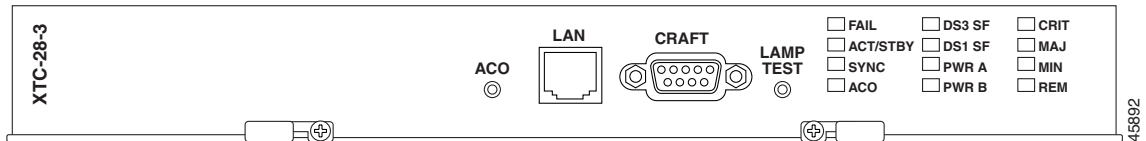
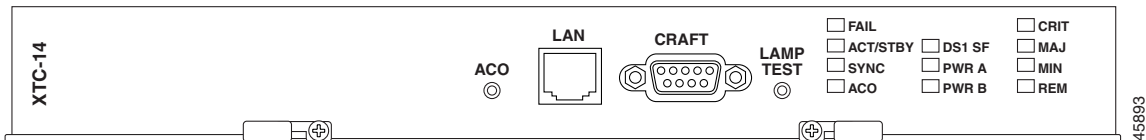


Figure 13-3 XTC-14 card faceplate



13.3.1.1 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 unit 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 (yellow).
- 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/problem with one or more of the DS-3 interfaces.
- The DS1 SF LED indicates a signal fail/problem 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.

13.3.1.2 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 VT1.5s and concatenates these virtual tributaries (VTs) into one STS-1. Full VT1.5 grooming is supported.

The physical connection points are located on the MIC cards. See the “MIC Description” section on page 13-9 for more information about physical connections.

13.3.1.3 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 non-redundant 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 Release 3.3 supports DCC tunneling of non-Cisco equipment.

The XTC cards also originate and terminate a cell bus carried over the SCI. The cell bus supports links between any two cards in the system, which is essential for peer-to-peer communication. Peer-to-peer communication accelerates protection switching for redundant cards.

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.

The node database, IP address, and system software are stored in XTC card non-volatile 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, 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.

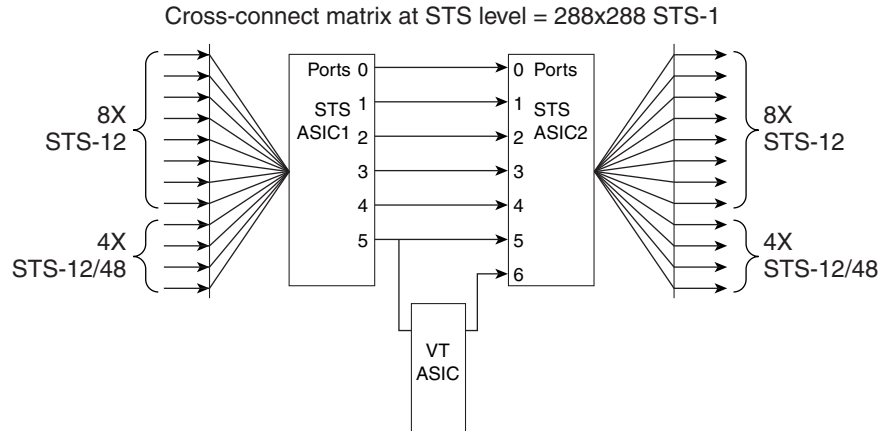
The XTC-cards feature an RJ-45 10Base-T LAN port and an EIA/TIA-232 DB9 type craft interface for user interfaces. The craft port runs at 9600 bps.

13.3.1.4 XTC Cross-Connect Functionality

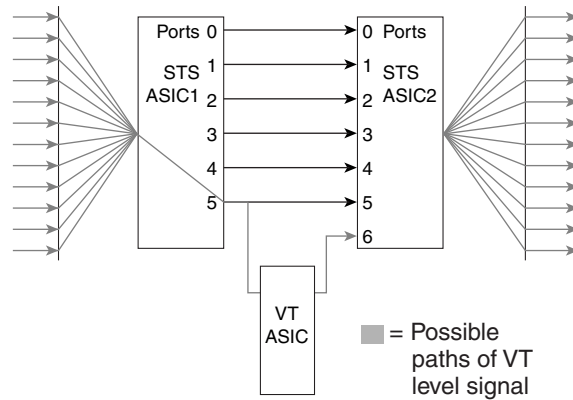
The XTC card is the central element for ONS 15327 switching. It establishes cross connections and performs time-division switching (TDS) at the STS-1 and VT1.5 level between ONS 15327 traffic cards.

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 non-blocking 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 13-4 shows the cross-connect matrix for the XTC card.

Figure 13-4 Cross-connect matrix



Cross-connect matrix at VT level = 336x336 bidirectional VT 1.5 bandwidth manager



50829

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.

13.3.2 VT Mapping

The Cisco ONS 15327 performs VT mapping according to Telcordia GR-253 standards. Table 13-1 shows the VT numbering scheme for the ONS 15327 as it relates to the Telcordia standard.

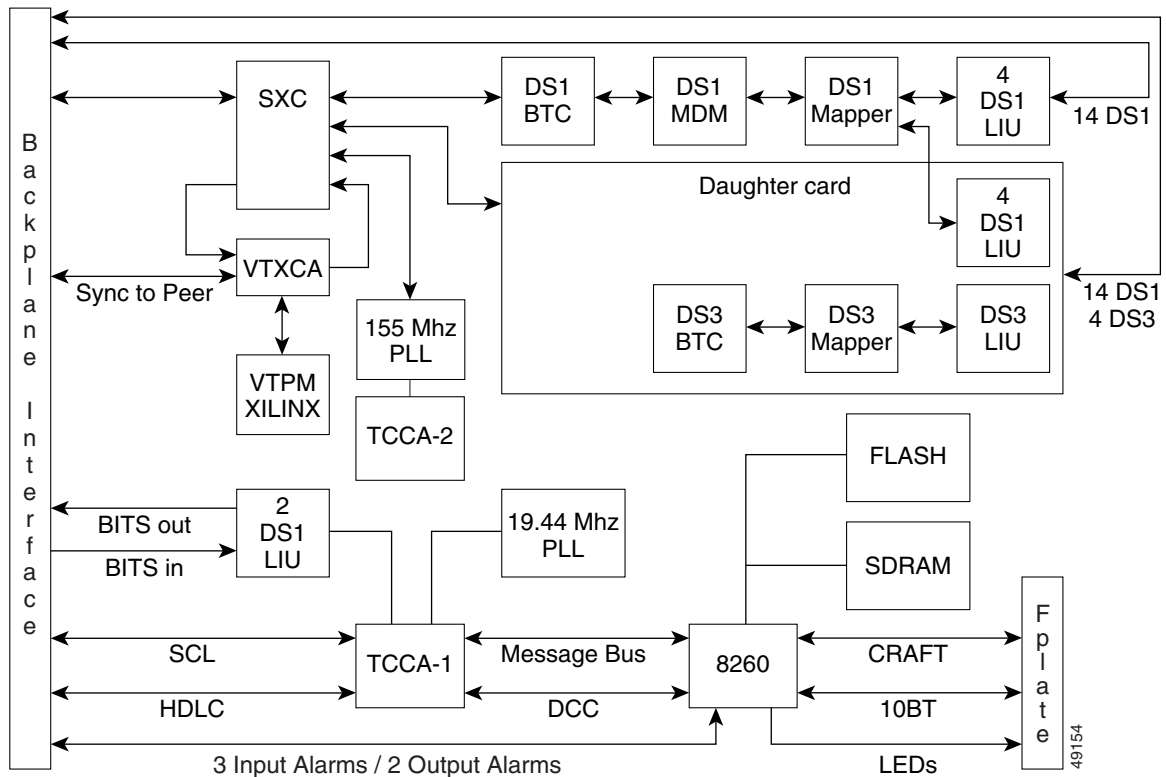
Table 13-1 ONS 15327 VT mapping

ONS 15327 VT Number	Telcordia Group/VT Number
VT1	Group1/VT1
VT2	Group2/VT1
VT3	Group3/VT1
VT4	Group4/VT1

Table 13-1 ONS 15327 VT mapping (continued)

ONS 15327 VT Number	Telcordia Group/VT Number
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 13-5 XTC block diagram



13.3.3 XTC Cards (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: 3.7×10^{-7} ppm/day, including temperature (< 255 slips in first 24 hours)
 - Reference: External BITS, line, internal
- Environmental
 - Operating Temperature: -40 to +65 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing
 - Power Consumption: 56 W maximum, 1.17 AMPS, 191 BTU/Hr
- Dimensions

- Height: 1.080 in.
- Width: 9.375 in.
- Depth: 9.172 in.

13.4 Mechanical Interface Cards

This section describes the features and functions of the MICs.

13.4.1 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 13-6 shows the MIC A faceplate. MIC A is keyed so that it can only be installed in Slot 8.

Figure 13-6 MIC A card faceplate

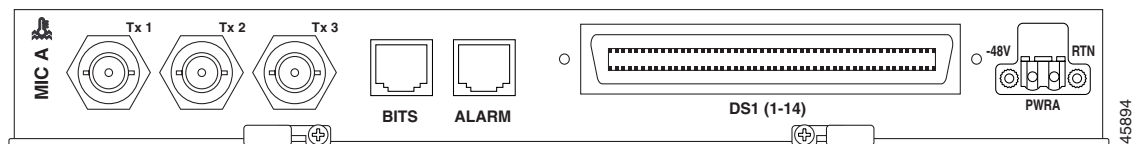
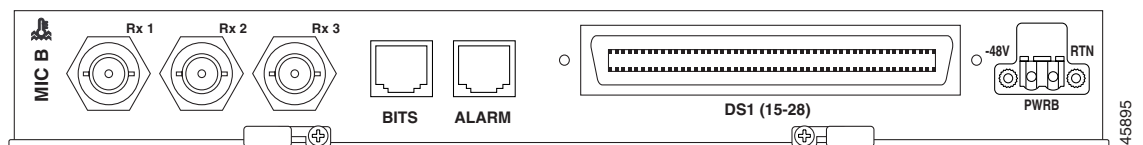


Figure 13-7 shows the MIC-28-3-B faceplate. MIC-B is keyed so that it can only be installed in Slot 7.

Figure 13-7 MIC B card faceplate



13.4.1.1 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 – 14, and MIC-28-3-B provides connection to DS-1s 15 – 28. The XTC cards house the electrical tributary circuitry for managing the individual DS-1s.

13.4.1.2 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.

13.4.1.3 Power Connection

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

13.4.1.4 Alarm Interface

Each MIC has one Form C discrete external control. Connection to the external control uses an RJ-45 connector. Two wires of the RJ-45 connector are used for the external control, which defaults to the open position. Each MIC also has three Form C discrete external alarm inputs. The alarm input connections are made using the same RJ-45 connector as the external control. Six wires of the RJ-45 connector are used for the external alarm input. Make the physical connections using the RJ-45 ALARM port on each MIC (for additional information, refer to the “Alarm Cable Installation” section on page 1-27).

In CTC you can provision the six external alarm inputs (three on each MIC) and the two external controls (one on each MIC), collectively referred to as alarm contacts. External alarm inputs are typically used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions. 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. For provisioning information about the external contacts, see the following section.

13.4.1.5 Provisioning I/O Alarm Contacts

You can program each of the six Form C external alarms (inputs) separately. They can be set to Alarm on Closure or Alarm on Open. The alarm severity can be set to any of the levels (Critical, Major, Minor, Not Alarmed, Not Reported). In addition to severity, you can set alarm type and virtual wire for alarm contacts 1 – 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 “Using Virtual Wires” section on page 7-17.

You can also program the two Form C external controls (outputs) separately. 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 (e.g. trigger when any Major alarm happens) 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 “Using Virtual Wires” section on page 7-17.

13.4.1.6 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.

13.4.2 MIC Specifications

- Environmental
 - Operating Temperature: -40 to +65 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing

- Power Consumption: 7 W, .15 AMPS, 24 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 9.375 in.
 - Depth: 9.172 in.

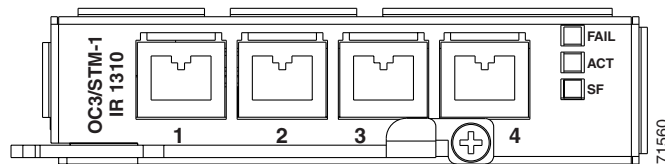
13.5 OC3 IR 4 1310 Card

This section describes the features and functions of the OC3 IR 4 1310 card. Refer to this section for general information about the OC3 IR 4 1310 card.

13.5.1 OC3 IR 4 1310 Card Description

The OC3 4 IR 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 non-concatenated or concatenated payloads for STS-1 or STS-3c. Figure 13-10 shows the OC3 IR 4 1310 faceplate and Figure 13-11 diagrams the card's functionality.

Figure 13-8 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 in 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) 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 13-3, 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. See Chapter 14, “Alarm Troubleshooting” for a description of these conditions. The card also counts section and line bit interleaved parity (BIP) errors.

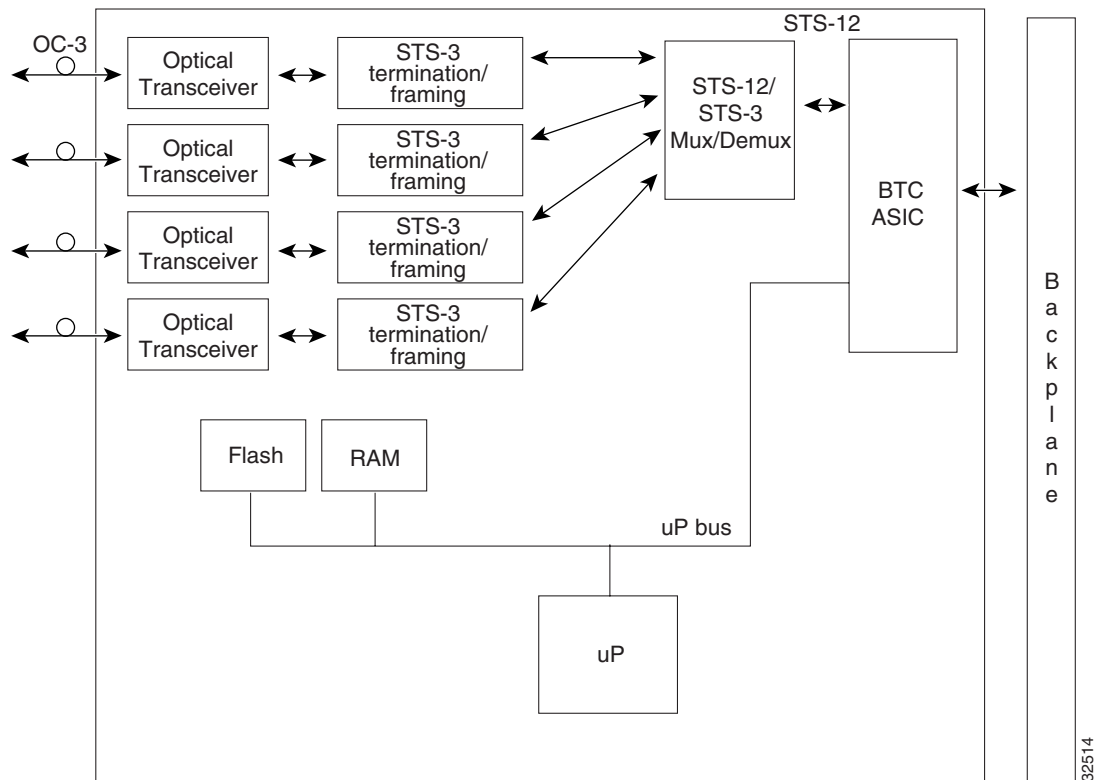
13.5.2 OC3 IR 4 1310 Card-Level Indicators

The OC3 IR 4 1310 card has three card-level LED indicators (Table 13-2).

Table 13-2 OC3 IR 4 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC3 IR 4/STM1 SH 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	The amber SF LED indicates a signal failure or condition such as LOS, LOF, AIS-L or high BER on one or more of the card's ports. The amber SF LED also illuminates when the transmit and receive fibers are incorrectly connected. When the fibers are properly connected, the light turns off.

Figure 13-9 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.

13.5.3 OC3 IR 4 1310 Card Specifications

- Line
 - Bit Rate: 155.52 Mbps
 - Code: Scrambled NRZ
 - Fiber: 1310 nm single-mode
 - Loopback Modes: Terminal and Facility
 - Connectors: LC
 - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
 - Max. Transmitter Output Power: -8 dBm
 - Min. Transmitter Output Power: -15 dBm
 - Center Wavelength: 1274 nm - 1356 nm
 - Nominal Wavelength: 1310 nm
 - Transmitter: Fabry Perot Laser
- Receiver
 - Max. Receiver Level: -8 dBm
 - Min. Receiver Level: -28 dBm
 - Receiver: InGaAs/InP photo detector
 - Link Loss Budget: 13 dB
- Environmental
 - Eye safety compliance: Class I
 - Operating Temperature: -40 to +65 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing
 - Power Consumption: 14 W, .29 AMPS, 48 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 4.280 in.
 - Depth: 9.172 in.

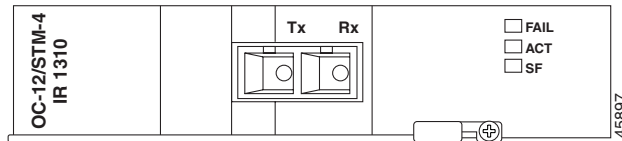
13.6 OC12 IR 1310 Card

This section describes the features and functions of the OC12 IR 1310 card. Refer to this section for general information about the OC12 IR 1310 card.

13.6.1 OC12 IR 1310 Card Description

The OC12 IR 1310 card provides one intermediate- or short-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 non-concatenated or concatenated payloads for STS-1, STS-3c, STS-6c, or STS-12c. Figure 13-10 shows the OC12 IR 1310 faceplate and Figure 13-11 diagrams the card's functionality.

Figure 13-10 OC12 IR 1310 card faceplate



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

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. See Chapter 14, “Alarm Troubleshooting” for a description of these conditions. The card counts section and line BIT errors.

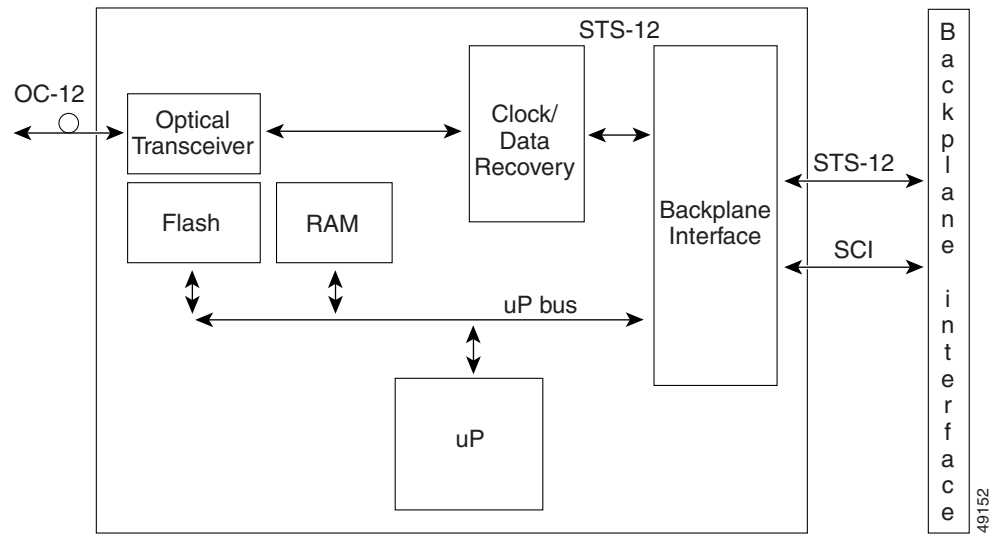
13.6.2 OC12 IR 1310 Card-Level Indicators

The OC12 IR 1310 card has three card-level LED indicators (Table 13-3).

Table 13-3 OC12 IR 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC12 IR/STM4 SH 1310 card is operational and is carrying traffic or is traffic-ready.
Amber SF LED	The 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. When the fibers are properly connected, the light turns off.

Figure 13-11 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.

13.6.3 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
 - Max. Transmitter Output Power: -8 dBm
 - Min. Transmitter Output Power: -15 dBm
 - Center Wavelength: 1274 nm - 1356 nm
 - Nominal Wavelength: 1310 nm
 - Transmitter: Fabry Perot Laser
- Receiver
 - Max. Receiver Level: -7 dBm
 - Min. Receiver Level: -29 dBm
 - Receiver: InGaAs/InP photo detector
 - Link Loss Budget: 14 dB
- Environmental

- Eye safety compliance: Class I
- Operating Temperature: -40 to +65 degrees Celsius
- Operating Humidity: 5 - 95%, non-condensing
- Power Consumption: 14 W, .29 AMPS, 48 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 4.280 in.
 - Depth: 9.172 in.

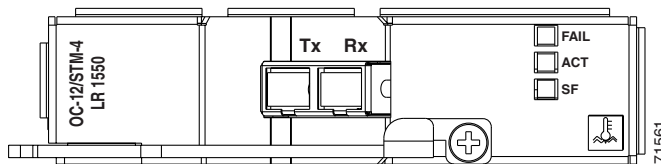
13.7 OC12 LR 1550 Card

This section describes the features and functions of the OC12 LR 1550 card. Refer to this section for general information about the OC12 LR 1550 card.

13.7.1 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 non-concatenated or concatenated payloads for STS-1, STS-3c, STS-6c, or STS-12c. Figure 13-12 shows the OC12 LR 1550 faceplate and Figure 13-13 diagrams the card's functionality.

Figure 13-12 OC12 LR 1550 card faceplate



You can install the OC12 LR 1550 card in any ONS 15327 high-speed card slot. You can provision the OC12 LR 1550 as part of a UPSR if desired. In ADM/TM configurations, you can provision the card as either an access tributary or a transport span-side interface.

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 protection and provisionable 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 Chapter 14, "Alarm Troubleshooting" for a complete description of alarm conditions). The OC12 LR 1550 counts path and line BIT errors.

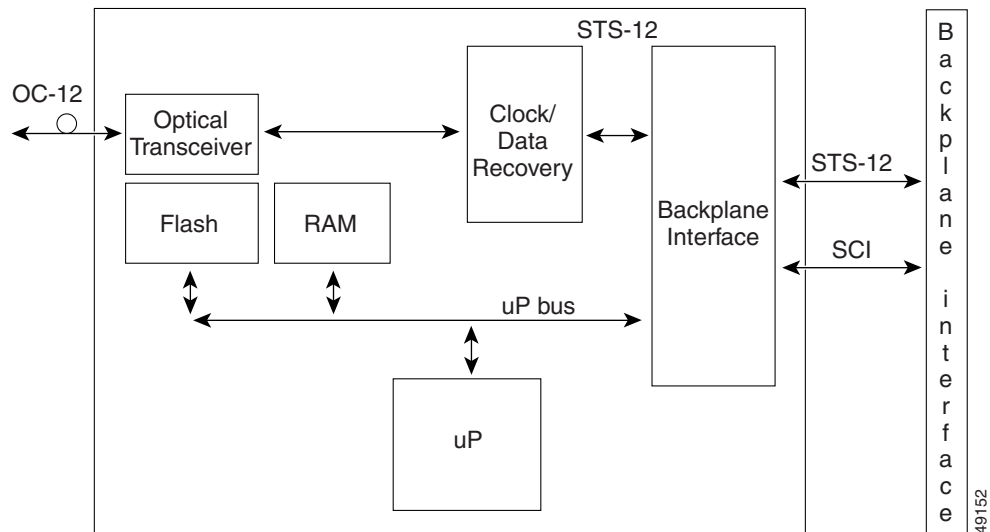
The OC12 LR 1550 extracts the K1 and K2 bytes from the SONET overhead to perform an appropriate protection switch. The DCC bytes are forwarded to the DCC-terminating XTC.

13.7.2 OC12 LR 1550 Card-Level Indicators

The OC12 LR 1550 card has three card-level LED indicators (Table 13-4).

Table 13-4 OC12 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC12 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	The 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. When the fibers are properly connected, the light turns off.

Figure 13-13 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.

13.7.3 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
 - Max. Transmitter Output Power: +2 dBm

- Min. Transmitter Output Power: -3 dBm
- Center Wavelength: 1480 nm - 1580 nm
- Nominal Wavelength: 1550 nm
- Transmitter: DFB Laser
- Receiver
 - Max. Receiver Level: -7 dBm
 - Min. Receiver Level: -29 dBm
 - Receiver: InGaAs/InP photo detector
 - Link Loss Budget: 26 dB
- Environmental
 - Eye safety compliance: Class I
 - Operating Temperature: -40 to +65 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing
 - Power Consumption: 14 W, .29 AMPS, 48 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 4.280 in.
 - Depth: 9.172 in.

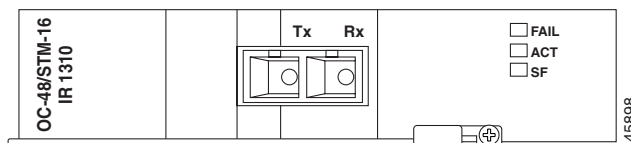
13.8 OC48 IR 1310 Card

This section describes the features and functions of the OC48 IR 1310 card. Refer to this section for general information about the OC48 IR 1310 card.

13.8.1 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 non-concatenated or concatenated payloads for STS-1, STS-3c, STS-6c, STS-12c, or STS-48c. Figure 13-14 shows the OC48 IR 1310 faceplate and Figure 13-15 diagrams the card's functionality.

Figure 13-14 OC48 IR 1310 faceplate



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. See Chapter 14, “Alarm Troubleshooting”, for a description of these conditions. The card also counts section and line BIT errors.

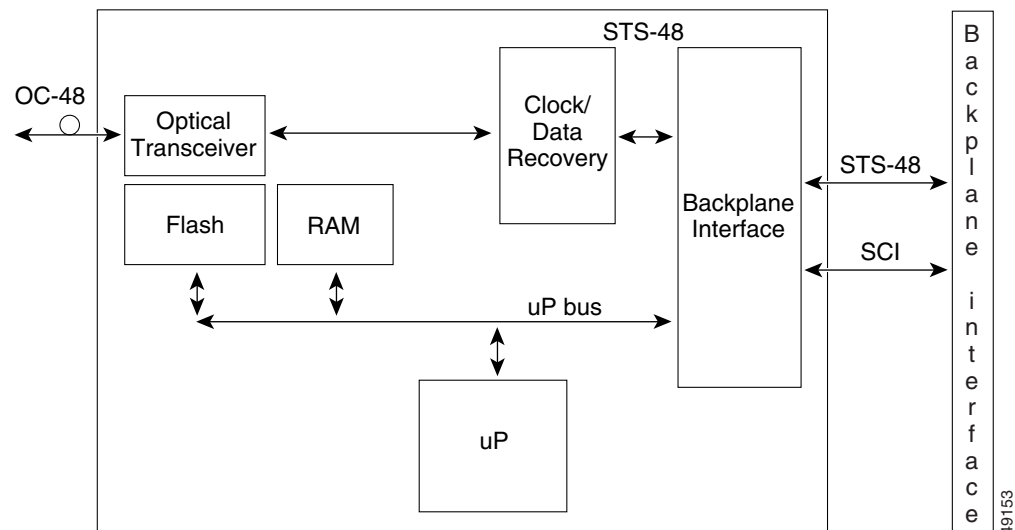
13.8.2 OC48 IR 1310 Card-Level Indicators

The OC48 IR 1310 card has three card-level LED indicators (Table 13-5).

Table 13-5 OC48 IR 1310 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card’s processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 IR 1310 card is carrying traffic or is traffic-ready.
Amber SF LED	The 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. When the fibers are properly connected, the light turns off.

Figure 13-15 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.

13.8.3 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
 - Max. Transmitter Output Power: 0 dBm
 - Min. Transmitter Output Power: -5 dBm
 - Center Wavelength: 1280 nm - 1350 nm
 - Nominal Wavelength: 1310 nm
 - Transmitter: Fabry Perot Laser
- Receiver
 - Max. Receiver Level: 0 dBm
 - Min. Receiver Level: -18 dBm
 - Receiver: InGaAs InP photo detector
 - Link Loss Budget: 13 dB min
- Environmental
 - Eye Safety Compliance: Class I
 - Operating Temperature: 0 to +55 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing
 - Power Consumption: 25 W, .52 AMPS, 85 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 4.280 in.
 - Depth: 9.172 in.

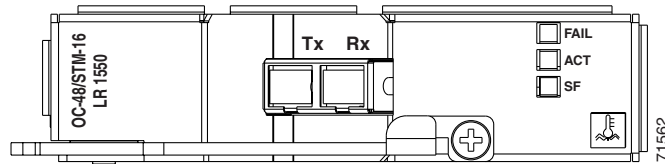
13.9 OC48 LR 1550 Card

This section describes the features and functions of the OC48 LR 1550 card. Refer to this section for general information about the OC48 LR 1550 card.

13.9.1 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 non-concatenated or concatenated payloads for STS-1, STS-3c, STS-6c, STS-12c, or STS-48c. Figure 13-16 shows the OC48 LR 1550 faceplate and Figure 13-17 diagrams the card's functionality.

Figure 13-16 OC48 LR 1550 faceplate



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 in an 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. See Chapter 14, “Alarm Troubleshooting” for a description of these conditions. The card also counts section and line BIT errors.

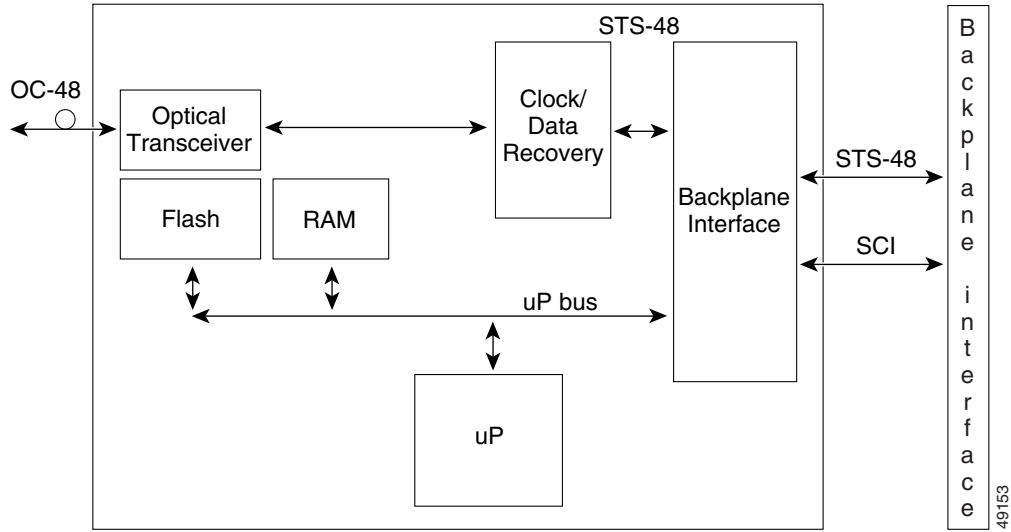
13.9.2 OC48 LR 1550 Card-Level Indicators

The OC48 LR 1550 card has three card-level LED indicators (Table 13-6).

Table 13-6 OC48 LR 1550 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The red FAIL LED indicates that the card's processor is not ready. Replace the card if the red FAIL LED persists.
Green ACT LED	The green ACT LED indicates that the OC48 LR 1550 card is carrying traffic or is traffic-ready.
Amber SF LED	The 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. When the fibers are properly connected, the light turns off.

Figure 13-17 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.

13.9.3 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
 - Max. Transmitter Output Power: +3dBm
 - Min. Transmitter Output Power: -2 dBm
 - Center Wavelength: 1520 nm - 1580 nm
 - Nominal Wavelength: 1550 nm
 - Transmitter: Fabry Perot Laser
- Receiver
 - Max. Receiver Level: -8 dBm
 - Min. Receiver Level: -28 dBm
 - Receiver: InGaAs InP photo detector
 - Link Loss Budget: 26 dB min., with 1 dB dispersion penalty

- Environmental
 - Eye Safety Compliance: Class I
 - Operating Temperature: -40 to +65 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing
 - Power Consumption: 25 W, .52 AMPS, 85 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 4.280 in.
 - Depth: 9.172 in.

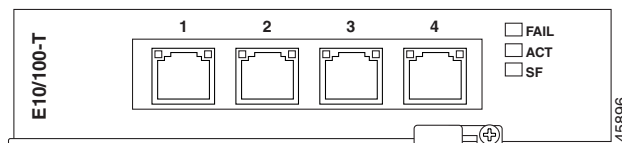
13.10 E10/100-4 Card

This section describes the features and functions of the ONS 15327 Ethernet card, called the E10/100-4 card. Refer to this section for information about the E10/100-4 card.

13.10.1 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 (auto-senses) and automatically connects at the appropriate speed. The ports auto-configure to operate at either half or full duplex and can determine whether to enable or disable flow control. You can manually set the ports' speed and duplex mode. The card's faceplate and functionality are shown in Figure 13-18 and Figure 13-19.

Figure 13-18 E10/100-4 faceplate



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 co-existence 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. 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 in the shelf assembly. 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 multi-card EtherSwitch mode.

13.10.2 E10/100-4 Card-Level Indicators

The E10/100-4 card faceplate has two card-level LED indicators (Table 13-7).

Table 13-7 E10/100-4 Card-Level Indicators

Card-Level Indicators	Description
Red FAIL LED	The 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	A 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 use.

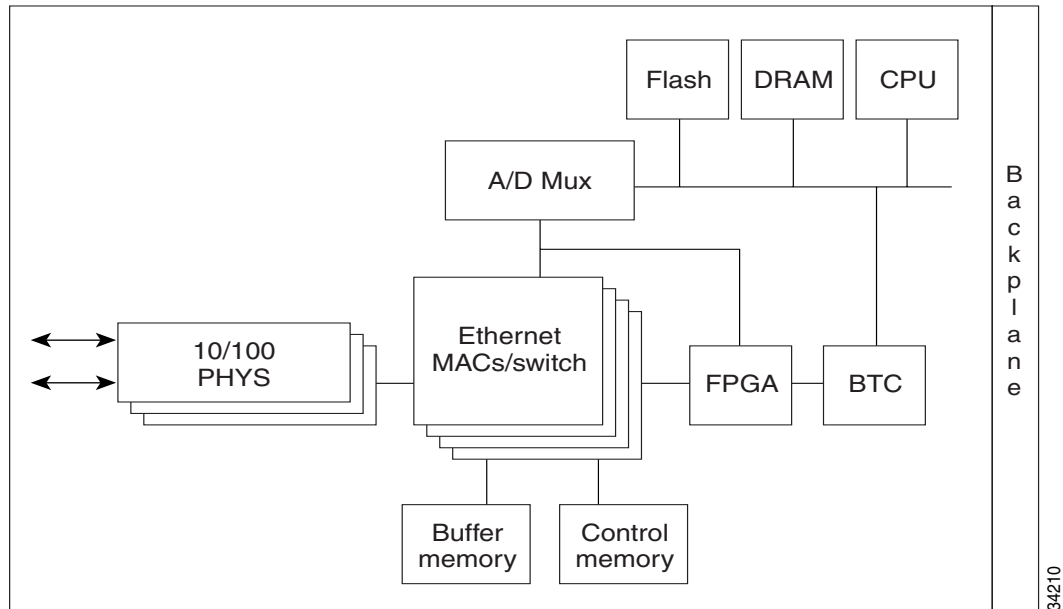
13.10.3 E10/100-4 Port-Level Indicators

The E10/100-4 card also has 4 pairs of LEDs (one pair for each port) to indicate port conditions (Table 13-8). See Chapter 14, "Alarm Troubleshooting" for a complete description of the alarm messages.

Table 13-8 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

Figure 13-19 E10/100-4 block diagram



13.10.4 E10/100-4 Card Specifications

- Environmental
 - Operating Temperature: 0 to +55 degrees Celsius
 - Operating Humidity: 5 - 95%, non-condensing
 - Power Consumption: 35 W, .73 AMPS, 120 BTU/Hr
- Dimensions
 - Height: 1.080 in.
 - Width: 4.280 in.
 - Depth: 9.172 in.



Alarm Troubleshooting

This chapter gives an alphabetical list of Cisco Transport Controller (CTC) alarm messages for the Cisco ONS 15327. It also lists the cards that host the alarms, and procedures to correct the alarms. The procedure to correct an alarm applies to the CTC and TL1 version of that alarm.

This chapter also includes a list of threshold-crossing events (EVTs). Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center for unresolved problems (1-800-553-2447).



Note

Some minor differences exist between TL1 error messages and CTC error messages for the ONS 15327. These discrepancies are resolved in an upcoming release of the ONS 15327. This chapter derives its text from the error messages as they appear in CTC. For a description of CTC, see Chapter 3, “Using Cisco Transport Controller.”



Note

At the CTC card view, ONS 15327 XTC alarms appear only on the active XTC card. The card- level view of the standby XTC card does not show these alarms.

This chapter gives descriptions, severities, and troubleshooting procedures for each Cisco ONS 15327 alarm. Table 14-1 on page 14-2 gives an alphabetical list of alarms that appear on the ONS 15327. Table 14-2 on page 14-3 gives a list of alarms organized by alarm type. Both lists cross-reference the alarm entry, which gives the severity, description, and troubleshooting procedure for each particular alarm.

The troubleshooting procedure for an alarm applies to both the CTC and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

The default standby severity for all ONS 15327 alarms is Minor, Non-Service-Affecting, as defined in Telcordia GR-474. All severities listed in the alarm entry are the default for the active card, if applicable.

This chapter provides a comprehensive list of alarms (conditions with a severity of Minor, Major or Critical). It also includes some conditions with severities of nonalarmed (NA) or not reported (NR), which are commonly encountered while troubleshooting major alarms. The default standby severity value for conditions with a severity of NA, Non-Service-Affecting (NSA) is NA, NSA. The default standby severity value for conditions with a severity of NR, NSA is NR, NSA. For a comprehensive list of all conditions, see the *Cisco ONS 15327 TL1 Command Guide*.

14.1 Alarm Index

Table 14-1 lists alarms by the name displayed on the CTC alarm pane in the conditions column.

Table 14-1 Alarm Index

AIS, page 14-9	FAILTOSWR, page 14-38	MEA (EQPT), page 14-62
AIS-L, page 14-9	FAILTOSWS, page 14-39	MEA (FAN), page 14-63
AIS-P, page 14-10	FAN, page 14-39	MEM-GONE, page 14-63
AIS-V, page 14-10	FANDEGRADE, page 14-40	MEM-LOW, page 14-63
APSB, page 14-11	FE-AIS, page 14-40	MFGMEM, page 14-64
APSCDFLTK, page 14-11	FE-DS1-MULTLOS, page 14-41	
APSC-IMP, page 14-12	FE-DS1-SNGLLOS, page 14-41	NOT-AUTHENTICATED, page 14-65
APSCINCON, page 14-13	FE-DS3-SA, page 14-42	
APSCM, page 14-14	FE-EQPT-NSA, page 14-42	PDI-P, page 14-65
APSCNMIS, page 14-14	FE-IDLE, page 14-42	PEER-NORESPONSE, page 14-67
APSM, page 14-15	FE-LOCKOUT, page 14-43	PLM-P, page 14-67
AUTORESET, page 14-16	FE-LOF, page 14-43	PLM-V, page 14-68
AUTOSW-AIS, page 14-16	FE-LOS, page 14-44	PRC-DUPID, page 14-68
AUTOSW-LOP (STSMON), page 14-16	FEPRLF, page 14-44	
AUTOSW-PDI, page 14-17	FORCED-REQ, page 14-44	RAI, page 14-69
AUTOSW-SDBER, page 14-17	FRNGSYNC, page 14-45	RCVR-MISS, page 14-69
AUTOSW-SFBER, page 14-17	FSTSYNC, page 14-45	RDI-P, page 14-70
AUTOSW-UNEQ (STSMON), page 14-17		RFI-L, page 14-70
AUTOSW-UNEQ (VT-MON), page 14-17	HITEMP, page 14-46	RFI-P, page 14-70
	HLDOVERSYNC, page 14-46	RFI-V, page 14-71
BKUPMEM, page 14-18		RING-MISMATCH, page 14-72
BLSROSYNC, page 14-19	IMPROPRMVL, page 14-47	
	INCOMPATIBLE-SW, page 14-48	SD-L, page 14-72
CARLOSS (EQPT), page 14-21	INVMACADDR, page 14-49	SD-P, page 14-73
CARLOSS (EQPT), page 14-21		SF-L, page 14-74
CLDRESTART, page 14-22	LOCKOUT-REQ, page 14-49	SF-P, page 14-75
CONCAT, page 14-23	LOF (BITS), page 14-49	SFTWDOWN, page 14-76
CONTBUS-A, page 14-23	LOF (DS1), page 14-50	SFTWDOWN-FAIL, page 14-76
CONTBUS-A-18, page 14-24	LOF (DS3), page 14-51	SNTP-HOST, page 14-77
CONTBUS-B, page 14-25	LOF (OC-N), page 14-51	SQUELCH, page 14-78
CONTBUS-B-18, page 14-26	LOGBUFR90, page 14-52	SSM-FAIL, page 14-79
CTNEQPT-PBPROT, page 14-27	LOGBUFROVFL, page 14-53	STU, page 14-79

Table 14-1 Alarm Index (continued)

CTNEQPT-PBWORK, page 14-28	LOP-P, page 14-53	SWTOPRI, page 14-80
	LOP-V, page 14-55	SWTOSEC, page 14-80
DATAFLT, page 14-30	LOS (BITS), page 14-56	SWTOTHIRD, page 14-80
DS3-MISM, page 14-30	LOS (DS-N), page 14-56	SYNCPRI, page 14-80
	LOS (OC-N), page 14-57	SYNCSEC, page 14-81
EOC, page 14-31	LPBKDS1FEAC, page 14-58	SYNCTHIRD, page 14-81
EQPT, page 14-32	LPBKDS1FEAC, page 14-58	SYSBOOT, page 14-82
EQPT-MISS, page 14-33	LPBKDS3FEAC, page 14-58	
E-W-MISMATCH, page 14-33	LPBKFACILITY (DS-N), page 14-58	TIM-P, page 14-82
EXCCOL, page 14-35	LPBKFACILITY (OC-N), page 14-59	TRMT, page 14-83
EXERCISE-RING-FAIL, page 14-35	LPBKTERMINAL (DS-N), page 14-60	TRMT-MISS, page 14-83
EXERCISE-SPAN-FAIL, page 14-36		
EXT, page 14-36	MANRESET, page 14-61	UNEQ-P, page 14-84
	MAN-REQ, page 14-61	UNEQ-V, page 14-85
FAILTOSW-PATH, page 14-36	MEA (AIP), page 14-61	

14.2 Alarm Index by Alarm Type

Table 14-2 gives the name and page number of every alarm in the chapter organized by alarm type.

Table 14-2 Alarm Index by Alarm Type

AIP:: INVMACADDR, page 14-49
AIP:: MEA (AIP), page 14-61
AIP:: MFGMEM, page 14-64
BITS:: AIS, page 14-9
BITS:: LOF (BITS), page 14-49
BITS:: LOS (BITS), page 14-56
BITS:: SSM-FAIL, page 14-79
BPLANE:: MEA (EQPT), page 14-62
BPLANE:: MFGMEM, page 14-64
DS1:: AIS, page 14-9
DS1:: LOF (DS1), page 14-50
DS1:: LOS (DS-N), page 14-56
DS1:: LPBKDS1FEAC, page 14-58
DS1:: LPBKFACILITY (DS-N), page 14-58
DS1:: LPBKTERMINAL (DS-N), page 14-60
DS1:: RCVR-MISS, page 14-69

Table 14-2 Alarm Index by Alarm Type (continued)

DS1::TRMT , page 14-83
DS1::TRMT-MISS , page 14-83
DS3::AIS , page 14-9
DS3::DS3-MISM , page 14-30
DS3::FE-AIS , page 14-40
DS3::FE-DS1-MULTLOS , page 14-41
DS3::FE-DS1-SNGLLOS , page 14-41
DS3::FE-DS3-SA , page 14-42
DS3::FE-EQPT-NSA , page 14-42
DS3::FE-IDLE , page 14-42
DS3::FE-LOF , page 14-43
DS3::FE-LOS , page 14-44
DS3::LOF (DS3) , page 14-51
DS3::LOS (DS-N) , page 14-56
DS3::LPBKDS1FEAC , page 14-58
DS3::LPBKDS3FEAC , page 14-58
DS3::LPBKFACILITY (DS-N) , page 14-58
DS3::LPBKTERMINAL (DS-N) , page 14-60
DS3::RAI , page 14-69
E100::CARLOSS (E-Series) , page 14-20
ENVALRM::EXT , page 14-36
EQPT::AUTORESET , page 14-16
EQPT::BKUPMEMP , page 14-18
EQPT::CARLOSS (EQPT) , page 14-21
EQPT::CLDRESTART , page 14-22
EQPT::CONTBUS-A-18 , page 14-24
EQPT::CONTBUS-A , page 14-23
EQPT::CONTBUS-B-18 , page 14-26
EQPT::CONTBUS-B , page 14-25
EQPT::CTNEQPT-PBPROT , page 14-27
EQPT::CTNEQPT-PBWORK , page 14-28
EQPT::EQPT , page 14-32
EQPT::EXCCOL , page 14-35
EQPT::FORCED-REQ , page 14-44
EQPT::HITEMP , page 14-46
EQPT::IMPROPRMVL , page 14-47
EQPT::LOCKOUT-REQ , page 14-49

Table 14-2 Alarm Index by Alarm Type (continued)

EQPT::MANRESET , page 14-61
EQPT::MEA (EQPT) , page 14-62
EQPT::MEM-GONE , page 14-63
EQPT::MEM-LOW , page 14-63
EQPT::PEER-NORESPONSE , page 14-67
EQPT::SFTWDOWN-FAIL , page 14-76
EQPT::SNTP-HOST , page 14-77
EXT-SREF::SWTOPRI , page 14-80
EXT-SREF::SWTOSEC , page 14-80
EXT-SREF::SWTOTHIRD , page 14-80
EXT-SREF::SYNCPRI , page 14-80
EXT-SREF::SYNCSEC , page 14-81
EXT-SREF::SYNCTHIRD , page 14-81
FAN::EQPT-MISS , page 14-33
FAN::FAN , page 14-39
FAN::MEA (FAN) , page 14-63
FAN::MFGMEM , page 14-64
NE::BLSROSYNC , page 14-19
NE::DATAFLT , page 14-30
NE::HITEMP , page 14-46
NE::PRC-DUPID , page 14-68
NE::RING-MISMATCH , page 14-72
NE::SYSBOOT , page 14-82
NE-SREF::FRNGSYNC , page 14-45
NE-SREF::FSTSYNC , page 14-45
NE-SREF::HLDOVERSYNC , page 14-46
NE-SREF::SWTOSEC , page 14-80
NE-SREF::SWTOTHIRD , page 14-80
NE-SREF::SYNCPRI , page 14-80
NE-SREF::SYNCSEC , page 14-81
NE-SREF::SYNCTHIRD , page 14-81
OCN::AIS-L , page 14-9
OCN::APSB , page 14-11
OCN::APSCDFLTK , page 14-11
OCN::APSC-IMP , page 14-12
OCN::APSCINCON , page 14-13
OCN::APSCM , page 14-14

Table 14-2 Alarm Index by Alarm Type (continued)

OCN::APSCNMIS, page 14-14
OCN::APSMM, page 14-15
OCN::AUTORESET, page 14-16
OCN::EOC, page 14-31
OCN::E-W-MISMATCH, page 14-33
OCN::FEPRLF, page 14-44
OCN::FORCED-REQ, page 14-44
OCN::LOCKOUT-REQ, page 14-49
OCN::LOF (OC-N), page 14-51
OCN::LOS (OC-N), page 14-57
OCN::LPBKFACILITY (OC-N), page 14-59
OCN::SD-L, page 14-72
OCN::SF-L, page 14-74
OCN::SQUELCH, page 14-78
OCN::SSM-FAIL, page 14-79
OCN::STU, page 14-79
STSMON::AIS-P, page 14-10
STSMON::CONCAT, page 14-23
STSMON::AUTOSW-AIS, page 14-16
STSMON::AUTOSW-LOP (STSMON), page 14-16
STSMON::AUTOSW-PDI, page 14-17
STSMON::AUTOSW-SDBER, page 14-17
STSMON::AUTOSW-SFBER, page 14-17
STSMON::AUTOSW-UNEQ (STSMON), page 14-17
STSMON::FORCED-REQ, page 14-44
STSMON::LOCKOUT-REQ, page 14-49
STSMON::LOP-P, page 14-53
STSMON::MAN-REQ, page 14-61
STSMON::PDI-P, page 14-65
STSMON::PLM-P, page 14-67
STSMON::RFI-P, page 14-70
STSMON::TIM-P, page 14-82
STSMON::UNEQ-P, page 14-84
STSTRM::LOP-P, page 14-53
STSTRM::PLM-P, page 14-67
STSTRM::SD-P, page 14-73
STSTRM::SF-P, page 14-75

Table 14-2 Alarm Index by Alarm Type (continued)

STSTRM::TIM-P , page 14-82
STSTRM::UNEQ-P , page 14-84
VT-MON::AIS-V , page 14-10
VT-MON::AUTOSW-AIS , page 14-16
VT-MON::AUTOSW-LOP (STSMON) , page 14-16
VT-MON::AUTOSW-PDI , page 14-17
VT-MON::AUTOSW-SDBER , page 14-17
VT-MON::AUTOSW-SFBER , page 14-17
VT-MON::AUTOSW-UNEQ (STSMON) , page 14-17
VT-MON::FORCED-REQ , page 14-44
VT-MON::LOCKOUT-REQ , page 14-49
VT-MON::LOP-V , page 14-55
VT-MON::UNEQ-V , page 14-85
VT-TERM::AIS-V , page 14-10
VT-TERM::LOP-V , page 14-55
VT-TERM::PLM-V , page 14-68
VT-TERM::RFI-V , page 14-71
VT-TERM::SD-P , page 14-73
VT-TERM::SF-P , page 14-75
VT-TERM::UNEQ-V , page 14-85

14.2.1 Alarm Type/Object Definition

Table 14-3 defines alarm types.

Table 14-3 Alarm Type/Object Definition

AIP	Auxiliary interface protection module.
BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
DS1	DS-1 ¹ line on an XTC-14 card or XTC-28-3 card.
DS3	DS-3 ² line on an XTC-28-3 card.
E100T	Ethernet line on an E10/100 card.
ENVALRM	Environmental alarm port on an MIC card.
EQPT	Card in any of the 17 card slots. This object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, STS ³ and VT ⁴ .
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
NE	The entire network element (SYSTEM).

Table 14-3 Alarm Type/Object Definition (continued)

NE-SREF	Represents the timing status of the NE.
OCN	OC-N line on an OC-N card.
RING	BLSR ⁵ number (STSRNG).
STSMON	STS alarm detection at the monitor point (upstream of cross-connect).
STSTRM	STS alarm detection at termination (downstream of cross-connect).
VT-MON	VT1 alarm detection at the monitor point (upstream of cross-connect).
VT-TERM	VT1 alarm detection at termination (downstream of cross-connect).

1. Digital Signal 1
2. Digital Signal 3
3. Synchronous Transport Signal
4. Virtual Tunnel
5. Bidirectional Line Switched Ring

14.3 Trouble Notifications

The ONS 15327 uses standard Telcordia categories to characterize levels of trouble. The ONS 15327 reports both alarmed trouble notifications, under the Alarms tab, and nonalarmed (NA) trouble notifications under the Conditions tab in CTC. Alarms signify a problem that the user needs to fix, such as a loss of signal (LOS). Conditions notify the user of an event which does not require action, such as a switch to a secondary timing reference (SWTOSEC) or a user-initiated manual reset (MANRESET).

Telcordia further divides alarms into Service-Affecting (SA) and Non-Service-Affecting (NSA) status. An SA failure affects a provided service or the network ability to provide service. For example, a missing transmitter (TRMT-MISS) alarm is characterized as an SA failure. TRMT-MISS occurs when the cable connector leading to a port on an active XTC card is removed. This affects a provided service, because traffic switches to the protect card. The high temperature (HITEMP) alarm, which means the ONS 15327 is hotter than 122 degrees Fahrenheit (50 degrees Celsius), is also an SA failure. Although for example a particular XTC port may not be affected, a high temperature affects the network ability to provide service.

14.3.1 Conditions

When an SA failure is detected, the ONS 15327 also sends an AIS downstream. When it receives the AIS, the receiving node sends a remote failure indication (RFI) upstream. AIS and RFI belong in the conditions category and show up on the Conditions window of the ONS 15327. However, unlike most conditions that are nonalarmed, Telcordia classifies these conditions as not reported (NR).

Both CTC and TL1 report NRs and NAs as conditions when conditions are retrieved. NAs are also reported as autonomous events under TL1 and under the History tab of CTC. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

14.3.2 Severities

The ONS 15327 uses Telcordia-standard severities: Critical (CR), Major (MJ), and Minor (MN). Critical indicates a severe, service-affecting alarm that needs immediate correction. Major is still a serious alarm, but the failure has less of an impact on the network. For example, with an XTC LOS, a Major alarm, 24 DS-0 circuits lose protection. But with a OC-192 LOS, a Critical alarm, over a hundred thousand DS-0 circuits lose protection.

Minor alarms, such as Fast Start Synchronization (FSTSYNC), do not have a serious effect on service. FSTSYNC lets you know that the ONS 15327 is choosing a new timing reference because the old reference failed. The loss of the prior timing source is something a user needs to look at, but it should not immediately disrupt service.

Telcordia standard severities are the default settings for the ONS 15327. A user may customize ONS 15327 alarm severities with the alarm profiles feature. For a description of alarm profiles, see Chapter 10, “Alarm Monitoring and Management”.

This chapter lists the default alarm severity for the active reporting card, if applicable. The default severity for alarms reported by standby cards is always Minor, NSA.

14.4 Alarm Procedures

This section lists alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, the description and the troubleshooting procedure accompany each alarm and condition.

14.4.1 AIS

- Not Reported (NR)

The ONS 15327 detects an AIS in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS. For example, this alarm occurs when the port on the reporting node is in service but the OC-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service or has an out-of-service port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node may not report any alarms that indicate it is at fault.

Procedure: Clear the AIS Condition

-
- | | |
|---------------|---|
| Step 1 | Check upstream nodes and equipment for alarms, especially for LOS and out-of-service ports. |
| Step 2 | Clear the upstream alarms. |
-

14.4.2 AIS-L

- Not Reported (NR)

The ONS 15327 detects an AIS in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS. For example, it is raised when the port on the reporting node is in service but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an LOS or has an out-of-service port. The AIS-L clears when you clear the primary alarm on the upstream node. However, the primary alarm node may not report any alarms that indicate it is at fault.

An AIS-L occurs at the line layer. The line layer refers to the segment between two SONET devices in the circuit and is also known as a maintenance span. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization.

Procedure: Clear the AIS-L Condition

-
- | | |
|---------------|---|
| Step 1 | Check upstream nodes and equipment for alarms, especially for LOS and an out-of-service port. |
| Step 2 | Clear the upstream alarms. |
-

14.4.3 AIS-P

- Not Reported (NR) (Condition)

The ONS 15327 detects an AIS in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. The AIS is caused by an incomplete circuit path. For example, it is raised when the port on the reporting node is in service, but a node upstream on the circuit does not have its port in service. The upstream node often reports a LOS or has an OC-N port out of service. The AIS-P clears when the primary alarm on the upstream node is cleared. However, the node with the primary alarm may not report any alarms to indicate it is at fault.

AIS-P occurs in each node on the incoming OC-N path. The path layer is the segment between the originating equipment and the terminating equipment. This path segment encompasses several consecutive line segments or segments between two SONET devices. The originating equipment puts bits together into a SONET payload and the terminating equipment breaks the bits apart again. SONET multiplexers, such as the ONS 15327, often perform the origination and termination tasks of the SONET payload.

Procedure: Clear the AIS-P Condition

-
- | | |
|---------------|---|
| Step 1 | Check upstream nodes and equipment for alarms, especially LOS and out-of-service ports. |
| Step 2 | Clear the upstream alarms. |
-

14.4.4 AIS-V

- Not Reported (NR)

The ONS 15327 detects an AIS in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS. For example, it is raised when the port on the reporting node is in service but a node upstream on the circuit does not

have its OC-N port in service. The upstream node often reports a LOS or has an out-of-service port. The AIS-V clears when the primary alarm is cleared. The node with the out-of-service port may not report any alarms to indicate it is at fault.

An AIS-V indicates that an upstream failure occurred at the VT layer. The VT, or electrical layer, is created when the SONET signal is broken down into an electrical signal. For example, it can be raised when an optical signal comes into an ONS 15327 OC-N card. If this optical signal is demultiplexed by the ONS 15327, and one of the channels separated from the optical signal is then cross connected into the XTC ports in the same node, that ONS 15327 reports an AIS-V alarm. An AIS-V error message on the electrical card is accompanied by an AIS-P error message on the cross connected OC-N card.

Procedure: Clear the AIS-V Condition on the XTC-14 Card or XTC-28-3 Card

-
- | | |
|---------------|---|
| Step 1 | Check upstream nodes and equipment for alarms, especially LOS and out-of-service ports. |
| Step 2 | Correct the upstream alarms. |
-

14.4.5 APSB

- Minor, Non-Service-Affecting

The channel byte failure alarm occurs when line-terminating equipment detects protection-switching byte failure in the incoming automatic protection switching (APS) signal. This happens when an inconsistent APS byte or invalid code is detected. Some older, non-Cisco SONET nodes send invalid APS codes if configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15327. These invalid codes raise an APSB on an ONS node.

Procedure: Clear the APSB Alarm on an OC-N Card

-
- | | |
|---------------|--|
| Step 1 | Examine the incoming SONET overhead with an optical test set to confirm inconsistent or invalid K bytes. |
| Step 2 | If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment may not interoperate effectively with the ONS 15327. For ONS 15327 protection switching to operate properly, the upstream equipment may need to be replaced. |
-

14.4.6 APSCDFLTK

- Minor, Non-Service-Affecting

The default K byte received (APSCDFLTK) alarm occurs when a BLSR is not properly configured. For example, it is raised when a four-node BLSR has one node configured as UPSR. A node in a UPSR or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

The alarm can also be caused when a new node is added but a new ring map has not been accepted. Troubleshooting for APSCDFLTK is often similar to troubleshooting for BLSROSYNC.

Procedure: Clear the APSCDFLTk Alarm

- Step 1** Prior to accepting a new mapping table, verify that each node has a unique node ID number:
- Login to a node on the ring.
 - Click the **Provisioning > Ring** tabs.
 - Record the node ID number.
 - Repeat Steps a–c for all nodes in the ring.
 - If two nodes have the same node ID number, change the ID number of one node so that each node has a unique node ID.
 - Click **Apply**.
- Step 2** Verify correct configuration of the east port and west-port optical fibers. (See the “E-W-MISMATCH” section on page 14-33.)
- Step 3** If it is a four-fiber BLSR system, make sure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if there is a working fiber incorrectly attached to a protection fiber.
- Step 4** Click **Yes** to accept the ring map.
- Step 5** If the alarm does not clear, check the ring map for each ONS 15327 in the network and verify that each node is visible to the other nodes:
- At the node (default) view, click the **Provisioning > Ring** tabs.
 - Highlight a BLSR.
 - Click **Ring Map**.
 - Verify that each node that is part of the ring appears on the ring map with a node ID and IP address.
 - Click **Close**.
- Step 6** If nodes are not visible, ensure that SONET Data Communications Channel (SDCC) terminations exist on each node:
- Click the **Provisioning > SONET DCC** tabs.
 - Click **Create**.
 - Click the OC-N card that links to the adjacent node.
 - Click **OK**.
- Step 7** If the alarm still does not clear, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
-

14.4.7 APSC-IMP

- Minor, Non-Service-Affecting

An improper SONET automatic protect switch code (APSC-IMP) alarm indicates invalid K bytes. This alarm occurs on OC-N cards in a BLSR configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa.

K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. APSCIMP occurs when these bits indicate a bad or invalid K byte. The alarm clears when the node receives valid K bytes.

**Caution**

Always use the supplied electrostatic discharge (ESD) wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the APSC-IMP Alarm

-
- Step 1** To determine the validity of the K byte signal, examine the received signal. Use an optical test set capable of viewing SONET overhead.
- Step 2** If the K byte is invalid, the problem lies in upstream equipment and not in the reporting ONS 15327. Troubleshoot the appropriate upstream equipment.
- Step 3** If the K byte is valid, verify that each node has a ring ID that matches the other node ring IDs:
- Using CTC, login to a node on the ring.
 - Click the **Provisioning > Ring** tabs.
 - Record the ring ID number.
 - Repeat Steps a–c for all nodes in the ring.
- Step 4** If a node has a ring ID number that does not match the other nodes, change the ring ID number of that node to match the other nodes in the ring.
- Step 5** Click **Apply**.
-

14.4.8 APSCINCON

- Minor, Service-Affecting

An inconsistent automatic protection switching (APS) alarm (APSCINCON) is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15327, to switch the SONET signal from a working to a protect path. An inconsistent APS code occurs when three consecutive frames do not contain identical APS bytes. Inconsistent APS bytes give the receiving equipment conflicting commands about switching.

Procedure: Clear the APSCINCON Alarm on an OC-N Card in a BLSR

-
- Step 1** Look for other alarms, especially LOS, loss of frame (LOF), or AIS. Clearing these alarms clears the APSCINCON alarm.
- Step 2** If an APSCINCON alarm occurs with no other alarms, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
-

14.4.9 APSCM

- Major, Service-Affecting

The APS Channel Mismatch (APSCM) alarm occurs when the ONS 15327 expects a working channel but receives a protection channel. In many cases, the working and protection channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM alarm only occurs on the ONS 15327 when 1+1 bidirectional protection is used on OC-N cards in a 1+1 configuration.



Warning

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



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the APSCM Alarm on an OC-N Card in 1+1 Mode

-
- Step 1** Verify that the working-card channel fibers connect directly to the adjoining node working-card channel fibers.
- Step 2** Verify that the protection-card channel fibers connect directly to the adjoining node protection-card channel fibers.
-

14.4.10 APSCNMIS

- Major, Service-Affecting

The APS node ID mismatch (APSCNMIS) alarm raises when the source-node ID contained in the K2 byte of the APS channel being received is not present in the ring map. This alarm may occur and clear when a BLSR is being provisioned. If so, the user can disregard the temporary occurrence. If an APSCNMIS raises and stays, the alarm clears when the receiving node receives or matches the expected K-byte. If the APSCNMIS is raised and stays, the alarm clears when a K byte with valid source-node ID in K2 is received.

Procedure: Clear the APSCNMIS Alarm

-
- Step 1** Verify that each node has a unique node ID number:
- Click the **Provisioning > Ring** tabs.
 - Click the BLSR row to highlight.
 - Click **Ring Map**.
 - If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.
 - Click **Close** on the Ring Map dialog box.

- Step 2** If two nodes have the same node ID number, change the ID number of one node so that each node has a unique node ID:
- Display the network view.
 - Login to one of the nodes that uses the repeated node ID recorded in Step 1.



Note If the node names shown on the network view do not correlate with the node IDs, login to each node and click the **Provisioning > Ring** tabs. This window displays the node ID of the node you are logged into.

- Click the Node ID table cell to reveal a drop-down menu.
- Select a unique node ID from the drop-down menu and click **Apply**.



Note Locking out and clearing the lockout on a span causes the ONS 15327 to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

- Step 3** If the alarm does not clear, lockout a span on the ring and then clear the lockout:
- Click the **Ring > Maintenance** tabs.
 - Click the table cell under the West Switch heading to reveal the drop-down menu.
 - Select **LOCKOUT SPAN** and click **Apply**.
 - Click **OK** on the BLSR Operations dialog box.
 - Click the same table cell under the West Switch heading to reveal the drop-down menu.
 - Select **CLEAR** and click **Apply**.
 - Click **OK** on the BLSR Operations dialog box.

14.4.11 APSMM

- Minor, Non-Service-Affecting

An APS mode mismatch failure (APSMM) alarm occurs when there is a mismatch of the protection-switching schemes at the two ends of the span. If one node is provisioned for bidirectional switching, the node at the other end of the span must also be provisioned for bidirectional switching. If one end is provisioned for bidirectional and the other is provisioned for unidirectional, an APSMM alarm occurs in the ONS node that is provisioned for bidirectional. This alarm occurs in a 1+1 configuration.

Procedure: Clear the APSMM Alarm in 1+1 Mode

- Step 1** For the reporting ONS 15327, display the CTC node view and click the **Provisioning > Protection** tabs.
- Step 2** Choose the 1+1 protection group configured for the OC-N cards.
This is the protection group optically connected (with DCC connectivity) to the far end.
- Step 3** Record whether the bidirectional switching box is checked.

- Step 4** Login to the far-end node and verify that the OC-N 1+1 protection group is provisioned. This is the protection group optically connected (with DCC connectivity) to the near end.
- Step 5** Verify that the bidirectional switching box matches the checked or unchecked condition of the box recorded in Step 3. If not, change it to match.
- Step 6** Click **Apply**.
-

14.4.12 AUTORESET

- Minor, Non-Service-Affecting

The AUTORESET alarm occurs when a card performs a warm reboot automatically. This happens when you change an IP address or perform any other operation that causes an automatic card-level reboot.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the AUTORESET Alarm

- Step 1** Check for additional alarms that may have triggered an automatic reset.
- Step 2** If the card automatically resets more than once a month with no apparent cause, replace it with a new card.



Note

When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.13 AUTOSW-AIS

- Not Reported (Condition)

The AUTOSW-AIS alarm indicates that automatic UPSR protection switching took place because of an AIS alarm. The UPSR is configured for revertive switching and switches back to the working path after the fault clears. Troubleshoot with the “AIS” section on page 14-9.

14.4.14 AUTOSW-LOP (STSMON)

- Not Alarmed (NA) (Condition)

The AUTOSW-LOP alarm indicates that automatic UPSR protection switching took place because of an LOP alarm. The UPSR is configured for revertive switching and switches back to the working path after the fault clears. Troubleshoot with the “LOP-P” section on page 14-53.

14.4.15 AUTOSW-LOP (VT-MON)

- Minor, Service-Affecting

The AUTOSW-LOP alarm indicates that automatic UPSR protection switching took place because of an LOP alarm. The UPSR is configured for revertive switching and switches back to the working path after the fault clears. Troubleshoot with the “LOP-P” section on page 14-53.

14.4.16 AUTOSW-PDI

- Not Alarmed (NA) (Condition)

The AUTOSW-PDI alarm indicates that automatic UPSR protection switching took place because of a PDI alarm. The UPSR is configured for revertive switching and switches back to the working path after the fault clears. Troubleshoot with the “PDI-P” section on page 14-65.

14.4.17 AUTOSW-SDBER

- Not Alarmed (NA) (Condition)

The AUTOSW-SDBER alarm indicates that automatic UPSR protection switching took place because of a signal degrade (SD) alarm. The UPSR is configured for revertive switching and has switched back to the working path. Troubleshoot with the “CLDRESTART” section on page 14-22.

14.4.18 AUTOSW-SFBER

- Not Alarmed (NA) (Condition)

The AUTOSW-SFBER alarm indicates that automatic UPSR protection switching took place because of a signal fail (SF) alarm. The UPSR is configured for revertive switching and switches back to the working path. Troubleshoot with the “SF-L” section on page 14-74.

14.4.19 AUTOSW-UNEQ (STSMON)

- Not Alarmed (NA) (Condition)

The AUTOSW-UNEQ alarm indicates that automatic UPSR protection switching took place because of an UNEQ alarm. The UPSR is configured for revertive switching and switches back to the working path after the fault clears. Troubleshoot with the “UNEQ-P” section on page 14-84.

14.4.20 AUTOSW-UNEQ (VT-MON)

- Minor, Service-Affecting

AUTOSW-UNEQ indicates that automatic UPSR protection switching took place because of an UNEQ alarm. The UPSR is configured for revertive switching and switches back to the working path after the fault clears. Troubleshoot with the “UNEQ-P” section on page 14-84.

14.4.21 BKUPMEMP

- Critical, Non-Service-Affecting

The BKUPMEMP alarm refers to a problem with the XTC card flash memory. The alarm occurs when the XTC card is in use and has one of four problems: the flash manager fails to format a flash partition; the flash manager fails to write a file to a flash partition; there is a problem at the driver level, or the code volume fails cyclic redundancy checking (CRC). CRC is a method to check for errors in data transmitted to the XTC.

The BKUPMEMP alarm also raises the EQPT alarm. In this instance, use the following procedure to clear the BKUPMEMP and the EQPT alarm.



Caution

It can take up to 30 minutes for software to be updated on a standby XTC card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

Procedure: Clear the BKUPMEMP Alarm

Step 1 Verify that both XTC cards are powered and enabled by confirming that the ACT/STBY LEDs on the XTC cards are lit.

Step 2 Reset the active XTC card to make the standby XTC card active:

- In CTC, display the node view.
- Position the cursor over the active XTC card slot.
- Right-click and choose **RESET CARD**.



Note

Ensure that the active green LED is lit before removing card.

Step 3 If the alarm clears, reseal the old XTC and allow it to boot up completely.

Step 4 Do a second reset, this time on the newly active XTC card to make the recently reseated standby XTC card active:

- In CTC, display the node view.
- Position the cursor over the active XTC card slot.
- Right-click and choose **RESET CARD**.

Step 5 If the alarm reappears after you perform the switch, replace the XTC card:

- Open the card ejectors.
- Slide the card out of the slot.
- Open the ejectors on the replacement card.
- Slide the replacement card into the slot along the guide rails.
- Close the ejectors.

**Note**

When replacing a card with an identical type of card, no additional CTC provisioning is required.

14.4.22 BLSROSYNC

- Major, Service-Affecting

The BLSR out of sync (BLSROSYNC) alarm occurs when the mapping table needs to be updated. To clear the alarm, a new ring map must be created and accepted. Before you create a new ring map, complete Steps 1 to 4 of the “Clear the BLSROSYNC Alarm” procedure on page 14-19.

Procedure: Clear the BLSROSYNC Alarm

-
- Step 1** Prior to accepting a new mapping table, verify that each node has a unique node ID number:
- Login to a node on the ring.
 - Click the **Provisioning > Ring** tabs.
 - Record the node ID number.
 - Repeat Steps a to c for all nodes in the ring.
 - If two nodes have the same node ID number, change one node ID number, so the node ID number is unique within that ring.
 - Click **Apply**.
- Step 2** Verify that each node has a ring ID that matches the other node ring IDs:
- Login to the next node on the ring.
 - Click the **Provisioning > Ring** tabs.
 - Record the ring ID number.
 - Repeat Steps a and b for all nodes in the ring.
 - If a node has a ring ID number that does not match the other nodes, change the ring ID to match all the other nodes in the ring.
 - Click **Apply**.
- Step 3** Verify correct configuration of the east port and west-port optical fibers. (See the “E-W-MISMATCH” section on page 14-33.)
- Step 4** If it is a four-fiber BLSR system, make sure that each protect fiber connects to another protect fiber, and each working fiber connects to another working fiber. The software does not report any alarm if there is a working fiber misconnected to a protect fiber.
- Step 5** If the east-to-west configuration changes, click **Apply**.
The BLSR Ring Map Change window appears.
- Step 6** Click **Yes** to accept the ring map.
- Step 7** If the alarm does not clear, check the ring map for each ONS 15327 in the network and verify that each node is visible to the other nodes.

- Step 8** If nodes are not visible, ensure that SDCC terminations exist on each node:
- Click the **Provisioning > SONET DCC** tabs.
 - Click **Create**.
 - Click the OC-N card that links to the adjacent node.
 - Click **OK**.
- Step 9** If alarms are raised when the DCCs are turned on, follow the “Clear the EOC Alarm on an OC-N Card” procedure on page 14-31.
- Step 10** If the alarm still does not clear, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
-

14.4.23 CARLOSS (E-Series)

- Major, Service-Affecting

A carrier loss on the LAN is the data equivalent of a SONET LOS alarm. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of this alarm are a disconnected cable or an improperly installed Ethernet card. Ethernet card ports must be enabled (put in service) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

This alarm also occurs after the restoration of a node database. In this instance, the alarm clears in approximately 30 seconds after spanning-tree protection reestablishes. This applies to the E-series Ethernet cards.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CARLOSS Alarm

-
- Step 1** Verify that the Ethernet cable is properly connected and attached to the correct port.
- Step 2** Verify that the Ethernet cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** Check that the transmitting device is operational. If not, troubleshoot the device.
- Step 4** Using a test set, determine that a valid signal is coming into the Ethernet port.
- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the Ethernet cable connecting the transmitting device to the Ethernet port.
- Step 6** If a valid Ethernet signal is present, physically reseal the Ethernet card.
- Step 7** If the alarm does not clear, replace the Ethernet card:
- Open the card ejectors.
 - Slide the card out of the slot.
 - Open the ejectors on the replacement card.
 - Slide the replacement card into the slot along the guide rails.
 - Close the ejectors.



Note When replacing a card with an identical type of card, no additional CTC provisioning is required.

- Step 8** If a CARLOSS alarm repeatedly appears and clears, examine the layout of your network to determine if or not the Ethernet circuit is part of an Ethernet manual cross-connect. If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm may be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, these steps do not apply.



Note A Ethernet manual cross-connect is used when equipment from another vendor sits between ONS 15327s, and the 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 is manually cross connected to an STS channel riding through the non-ONS network.

- a. Right-click anywhere on the row of the CARLOSS alarm.
 - b. Right-click or left-click the Select Affected Circuits dialog box that appears.
 - c. Record the information in the type and size columns of the highlighted circuit.
 - d. From the examination of the layout of your particular network, determine the ONS 15327 and card that host the Ethernet circuit at the other end of the Ethernet manual cross-connect.
 - e. Login to the ONS 15327 at the other end of the Ethernet manual cross-connect.
 - f. Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
 - g. Click the **Circuits** tab.
 - h. Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross connect. This circuit connects the Ethernet card to an OC-N card on the same node.
 - i. Determine if the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.
 - j. If one of the circuit sizes is incorrect, navigate to the incorrectly configured circuit.
 - k. Click the incorrectly configured circuit to highlight it and click **Delete**.
 - l. Click **Yes** at the Delete Circuit dialog box, and **OK** at the Confirmation dialog box.
 - m. Reconfigure the circuit with the correct circuit size. See Chapter 9, “Ethernet Operation” for procedures to provision Ethernet manual cross-connects.
-

14.4.24 CARLOSS (EQPT)

- Minor, Non-Service-Affecting

This carrier loss alarm means the ONS 15327 and the workstation hosting CTC do not have a TCP/IP connection. It is a problem involves the LAN or data circuit used by the RJ-45 connector on the XTC card or the LAN backplane pin connection on the back of the ONS 15327. It does not involve an Ethernet circuit connected to a port on Ethernet card. The problem is in the connection (usually a LAN problem) and not CTC or the ONS 15327.

Procedure: Clear the CARLOSS Alarm

-
- Step 1** Verify connectivity by pinging the ONS 15327 that is reporting the alarm:
- If you are using a Microsoft Windows operating system, click the Start button, then choose **Programs > Command Prompt**.
 - If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and click **Terminal**.
 - For both the Sun and Microsoft operating systems, at the prompt type:

```
ping [ONS 15327 IP address]
```

For example,

```
ping 192.168.0.0
```

If the workstation has connectivity to the ONS 15327, it displays “Reply from [IP Address]” after the ping. If the workstation does not have connectivity, a “Request timed out” message appears.

- Step 2** If the ping is successful, an active TCP/IP connection exists. Restart CTC.
- Step 3** If you are unable to establish connectivity, perform standard network/LAN diagnostics. For example, trace the IP route, check cables, and check any routers between the node and CTC.
-

14.4.25 CLDRESTART

- Not Alarmed (NA) (Condition)

A cold restart (CLDRESTART) is a cold boot of the reporting card. This alarm can occur when you physically remove and insert a card, power up an ONS 15327, or replace a card.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CLDRESTART Condition

-
- Step 1** If the alarm fails to clear after the card reboots, physically reseal the card.
- Step 2** If the alarm still fails to clear, replace the card.



Note

When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.26 CONCAT

- Critical, Service-Affecting

The STS concatenation error (CONCAT) alarm occurs when the transmitted STSc circuit is smaller than the provisioned STSc, which causes a mismatch of the circuit type on the concatenation facility. For example, an STS3c or STS1 is sent across a circuit provisioned for STS12c.

Either an incorrect circuit size was provisioned on the reporting node, or the circuit source is delivering the wrong circuit size. If a recently configured circuit reports this alarm, it is more likely that the provisioned circuit size is incorrect. If a previously configured circuit has been operating correctly for a period and then reports the alarm, it is more likely that a problem occurred with the circuit source.

Procedure: Clear the CONCAT Alarm

-
- Step 1** Check that the provisioned circuit size is correct:
- Click the **Circuits** tab.
 - Find the appropriate row using the circuit name and record the size listed in the size column.
 - Determine if the size listed matches the original network design plan.
- Step 2** If the circuit size listed does not match the original network design plan, delete the circuit:
- Click the circuit row to highlight it and click **Delete**.
 - Click **Yes** at the Delete Circuits dialog box.
 - Recreate the circuit with the correct circuit size.
- Step 3** Check that the size of the circuit source matches the correct circuit size:
- Measure the source signal with a test set to determine if the circuit size matches the provisioned circuit.
 - If the source circuit signal is a test set, check that the test set settings match the intended circuit size.
-

14.4.27 CONTBUS-A

- Major, Non-Service-Affecting

The communication failure XTC A to shelf slot (CONTBUS-A) alarm means the XTC card in Slot 5 has lost communication with a line card. Cards require frequent communication with the XTC card because the XTC performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SDCC termination, system fault detection, and other operations for the ONS 15327. The XTC card also ensures that the system maintains Telcordia timing requirements.

The CONTBUS-A alarm can appear briefly when the ONS 15327 switches to the standby XTC card. In this instance, the alarm clears after the cards establish communication with the new primary XTC card. In cases where the alarm persists, the problem lies in the physical path of communication from the XTC to the reporting card. The physical path of communication includes the XTC card, the card in Slot X and the backplane.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CONTBUS-A Alarm

-
- Step 1** Ensure that the reporting card is physically present. Record the card type.
- Step 2** Click the **Inventory** tab to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, complete the “Clear the MEA Alarm” procedure on page 14-62.
- Step 3** If only one card slot is reporting the alarm, perform a software reset of the traffic card:
- a. Display the CTC node view.
 - b. Position the cursor over the slot reporting the alarm.
 - c. Right-click and choose **RESET CARD**.
- Step 4** If the software reset does not clear the alarm, physically reseal the reporting card.
- Step 5** If all traffic cards report this alarm, perform a software reset of the active XTC card:
- a. Display the node view.
 - b. Position the cursor over the active XTC card slot.
 - c. Right-click and choose **RESET CARD**.
- Step 6** If the software reset does not clear the alarm, physically reseal the XTC card.
- Step 7** If the alarm still does not clear, replace the XTC card.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.28 CONTBUS-A-18

- Major, Non-Service-Affecting

The communication failure from XTC slot to XTC slot (CONTBUS-A-18) alarm means the main processor on the XTC card in Slot 5 has lost communication with the coprocessor on the second XTC card in Slot 6. The problem is with the physical path of communication from the XTC card to the reporting card. The physical path of communication includes the two XTC cards and the backplane.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CONTBUS-A-18 Alarm

-
- Step 1** Position the cursor over the XTC card in Slot 5.
 - Step 2** Right-click the mouse to reveal a menu.
 - Step 3** To clear the alarm, choose **RESET CARD** to make the standby XTC in Slot 6 the active XTC and clear the alarm.
 - Step 4** Wait approximately two minutes for the XTC in Slot 5 to reset as the standby XTC. Verify that the Standby LED is lit before proceeding to the next step.
 - Step 5** Position the cursor over the XTC card in Slot 6.
 - Step 6** Right-click the mouse to reveal a menu.
 - Step 7** Choose **RESET CARD** to make the standby XTC in Slot 5 the active XTC.
 - Step 8** If the alarm reappears when the XTC in Slot 5 reboots as the active XTC, the XTC card in Slot 5 is defective and must be replaced.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.29 CONTBUS-B

- Major, Non-Service-Affecting

The communication failure XTC B to shelf slot (CONTBUS-B) alarm means the XTC card in Slot 6 lost communication with a line card. Cards require frequent communication with the XTC card, because the XTC card performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SDCC termination, and system fault detection among other operations for the ONS 15327. The XTC card also ensures that the system maintains Telcordia timing requirements.

This alarm may appear briefly when the ONS 15327 switches over to the protect XTC card. In this instance, the alarm clears after the other cards establish communication with the new primary XTC card. In cases where the alarm persists, the problem lies in the physical path of communication from the XTC card to the reporting card. The physical path of communication includes the XTC card, the card in Slot X and the backplane.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CONTBUS-B

-
- Step 1** Ensure that the reporting card is physically present and that it matches the type of card identified in that slot on CTC.
 - Step 2** If this slot is the only one reporting the alarm, perform a software reset of the traffic card:
 - a. Display the CTC node view.

- b. Position the cursor over the slot reporting the alarm.
 - c. Right-click the mouse and choose **RESET CARD** to do a software reset.
- Step 3** If the software reset does not clear the alarm, physically reseal the reporting card.
- Step 4** If all cards with the exception of the active XTC report this alarm, perform a software reset of the active XTC:
- a. Display the CTC node view.
 - b. Position the cursor over the active XTC card slot.
 - c. Choose **RESET CARD**.
- Step 5** If the software reset does not clear the card, physically reseal the XTC card to perform a card pull.
- Step 6** If the alarm still does not clear, replace the XTC card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.30 CONTBUS-B-18

- Major, Non-Service-Affecting

The communication failure from XTC slot to XTC slot (CONTBUS-B-18) alarm means main processor on the XTC card in Slot 6 lost communication with the coprocessor on the XTC card in Slot 5. The problem is with the physical path of communication from the XTC card to the reporting XTC card. The physical path of communication includes the two XTC cards and the backplane.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the CONTBUS-B-18 Alarm on the XTC Card

- Step 1** Position the cursor over the XTC card in Slot 6.
- Step 2** Right-click and choose **RESET CARD** to make the XTC in Slot 6 the active XTC card.
- Step 3** Wait approximately two minutes for the XTC in Slot 5 to reset as the standby XTC card. Verify that the Standby LED is lit before proceeding to the next step.
- Step 4** Position the cursor over the XTC card in Slot 5.
- Step 5** Right-click and choose **RESET CARD** again to make the XTC in Slot 6 the active XTC card.
- Step 6** If the alarm reappears when the XTC in Slot 6 reboots as the active XTC, the XTC card in Slot 6 is defective and must be replaced.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.31 CTNEQPT-PBPROT

- Critical, Service-Affecting

The interconnection equipment failure protect payload bus (CTNEQPT-PBPROT) alarm indicates a failure of the main payload between the protect cross-connect XTC card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in either the reporting traffic card, the XTC card or the backplane.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



Note

If all traffic cards show this alarm, physically reseal the standby XTC card. If this fails to clear the alarm, replace the standby XTC card. Do not physically reseal an active XTC card. This disrupts traffic.



Caution

It can take up to 30 minutes for software to be updated on a standby XTC card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

Procedure: Clear the CTNEQPT-PBPROT Alarm

-
- Step 1** Perform a software reset on the standby cross-connect XTC card:
- Display the node view.
 - Position the cursor over the slot reporting the alarm.
 - Right-click and choose **RESET CARD**.
- Step 2** If the alarm persists, physically reseal the standby cross-connect card.
- Step 3** If the alarm persists and the reporting traffic card is the active card in the protection group, do a force switch to move traffic away from the card:
- At the node view, click the **Maintenance** tab then click the **Protection** tabs.
 - Double-click the protection group that contains the reporting card.
 - Click the Protect/Standby card of the selected groups.
 - Click **Force** and **OK**.
- Step 4** Perform a software reset on the reporting card:
- Display the CTC node view.
 - Position the cursor over the slot reporting the alarm.

- c. Right-click to choose **RESET CARD**.

Step 5 If the alarm persists, physically reseal the reporting card.

Step 6 Clear the force switch:

- a. At the node view, click the **Maintenance** tab, then click the **Protection** tabs.
- b. Double-click the protection group that contains the reporting card.
- c. Highlight either selected group.
- d. Click **Clear** and click **YES** at the confirmation dialog box.

Step 7 If the reporting traffic card is protect, perform a software reset on the reporting card:

- a. Display the CTC node view.
- b. Position the cursor over the slot reporting the alarm.
- c. Right-click and choose **RESET CARD**.

Step 8 If the alarm persists, physically reseal the reporting card.

Step 9 If the alarm persists, replace the standby cross-connect card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 10 If the alarm persists, replace the reporting traffic card.

14.4.32 CTNEQPT-PBWORK

- Critical, Service-Affecting

The interconnection equipment failure protect payload bus (CTNEQPT-PBWORK) alarm indicates a failure in the main payload bus between the active cross-connect XTC card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the reporting traffic card or the backplane.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly



Note

If all traffic cards show this alarm, do a forced side switch on the active XTC card, as shown in Step 1, and physically reseal this XTC card. If this fails to clear the alarm, replace the XTC card. Do not physically reseal an active XTC card; this disrupts traffic.

Procedure: Clear the CTNEQPT-PBWORK Alarm

Step 1 Do a side switch from the active cross-connect XTC card to the protect cross-connect card:

- a. Determine the active cross-connect card. The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is yellow.



Note You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

- b. In the node view, select the **Maintenance** tab, then click the **XC Cards** tab.
- c. Click **Switch**.
- d. Click **Yes** on the Confirm Switch dialog box.



Note After the active cross-connect goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

- Step 2** Perform a software reset on the reporting card:
- a. From the node view, position the cursor over the slot reporting the alarm.
 - b. Right-click to choose **RESET CARD**.
- Step 3** If the alarm persists, perform a card pull on the standby cross-connect card.
- Step 4** If the alarm persists and the reporting traffic card is the active card in the protection group, do a force switch to move traffic away from the card:
- a. At the node view, click the **Maintenance > Protection** tabs.
 - b. Double-click the protection group that contains the reporting card.
 - c. Click the Protect/Standby card of the selected groups.
 - d. Click **Force** and **OK**.
- Step 5** Perform a software reset on the reporting card:
- a. Display the CTC node view.
 - b. Position the cursor over the slot reporting the alarm.
 - c. Right-click to choose **RESET CARD**.
- Step 6** If the alarm persists, physically reseal the reporting card.
- Step 7** Clear the force switch:
- a. At the node view, click the **Maintenance > Protection** tabs.
 - b. Double-click the protection group that contains the reporting card.
 - c. Highlight either selected group.
- Step 8** Click **Clear** and click **YES** at the confirmation dialog box.
- Step 9** If the reporting traffic card is protect, perform a software reset on the reporting card:
- a. Display the CTC node view.
 - b. Position the cursor over the slot reporting the alarm.
 - c. Right-click to choose **RESET CARD**.
- Step 10** If the alarm persists, physically reseal the reporting card.
- Step 11** If the alarm persists, replace the cross-connect card. First, ensure that the card has been side switched from active to standby (Step 1).



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 12 If the alarm persists, replace the reporting traffic card.

14.4.33 DATAFLT

- Minor, Non-Service-Affecting

The software fault data integrity fault (DATAFLT) alarm means the database exceeded the capacity of the Flash memory on the XTC.



Caution When the system reboots, the last configuration entered is not saved.

Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.34 DS3-MISM

- Not Alarmed (NA) (Condition)

The DS-3 frame format mismatch (DS3-MISM) alarm indicates a frame format mismatch on the XTC-28-3 card. The condition occurs when the provisioned line type and incoming signal frame format type do not match. For example, if the line type is set to C-BIT for an XTC-28-3 card, and the incoming frame format of the incoming signal is detected as M23 or UNFRAMED, then the ONS 15327 reports a DS3-MISM alarm. The alarm is not raised when the line type is set to AUTOPROVISION or UNFRAMED.

The alarm or condition clears when the line type is set to AUTO PROVISION or UNFRAMED, the port state is set to OOS, or the correct frame format is set. Setting the line type to AUTO PROVISION causes the ONS 15327 to detect the received frame format and provision the port to use the matching frame format, either Unframed, M23 or C-bit.

Procedure: Clear the DS3-MISM Alarm on the XTC-28-3 Card

- Step 1** Go to the CTC card-level view for the reporting XTC-28-3.
- Step 2** Click the **Provisioning > Line** tabs.
- Step 3** For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal.
- Step 4** If the Line Type drop-down column does not match the expected incoming signal, select the correct Line Type on the pull down menu.
- Step 5** Click **Apply**.

- Step 6** If the alarm does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use a test set to verify that the actual signal coming into the ONS 15327 matches the expected incoming signal.

14.4.35 EOC

- Major, Non-Service-Affecting

The termination failure SDCC alarm means the ONS 15327 has lost its DCC. The DCC is three bytes, D1 through D3, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P.) The ONS 15327 uses the SDCC to communicate network management information.



Warning

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



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the EOC Alarm on an OC-N Card

- Step 1** If an LOS alarm is also reported, first resolve the LOS alarm by following the troubleshooting procedure given for that alarm.
- Step 2** On the node reporting the alarm, check the physical connections from the cards to the fiber-optic cables that are configured to carry DCC traffic.
- Step 3** Verify that both ends of the fiber span have in-service ports by checking that the ACT LED on each OC-N card is illuminated.
- Step 4** Verify that the DCC is provisioned for the ports at both ends of the fiber span.
- Under the node view, click the **Provisioning > SONET DCC** tabs.
 - If the slot and port are listed under **SDCC Terminations**, the DCC is provisioned.
 - If the slot and port are not listed under the **SDCC Terminations**, click **Create**.
 - Click the OC-N card that links to the adjacent node.
 - Click **OK**.
 - Repeat Steps a to e at the adjacent nodes.
- Step 5** Verify that the OC-N port is active and in service:
- Confirm that the OC-N card shows a green LED by viewing CTC or viewing the physical card.
A green LED indicates an Active card. A yellow LED indicates a Standby card.
 - To determine whether or not the OC-N port is in In Service, double-click the card in CTC to display the card-level view.
 - Click the **Provisioning > Line** tabs.

- d. Verify that the Status column lists the port as in service.
- e. If the Status column lists the port as out of service, click the column and select **In Service**. Click **Apply**.

Step 6 Using a test set, check for signal failures on fiber terminations.



Caution Using a test set disrupts service on the OC-N card. It may be necessary to manually switch traffic carrying circuits to a protection path.

Step 7 Measure power levels to verify that the budget loss is within the parameters of the receiver.



Note After measuring power levels, clean fibers according to site practice.

Step 8 Ensure that fiber connectors are securely fastened and properly terminated.

Step 9 Reset the active XTC using the “Card Turn-Up” section on page 1-18.



Note Ensure that the active green LED is lit before removing card.

Resetting the active XTC switches the traffic to the standby XTC. If the alarm clears when the ONS 15327 switches to the standby XTC, the user can assume that the original active XTC is the cause of the alarm.

Step 10 Replace the original active XTC with a new XTC card.



Caution Resetting the active XTC can result in loss of traffic.

Step 11 Delete and recreate the problematic SDCC termination:

- a. Click the **Provisioning > SONET DCC** tabs.
- b. Highlight the problematic SDCC termination.
- c. Click **Delete**.
- d. Click **Yes** at confirmation dialog box.

Step 12 Verify that both ends of the SDCC have been recreated at the optical ports.

Step 13 Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.36 EQPT

- Critical, Service-Affecting

An equipment failure (EQPT) alarm indicates that a hardware failure has occurred on the reporting card.

If the EQPT alarm occurs with a BKUPMEMP alarm, follow the procedure “Clear the BKUPMEMP Alarm” section on page 14-18. This procedure also clears the EQPT alarm.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the EQPT Alarm

- Step 1** Perform a software reset on the reporting card:
- Display the CTC node view.
 - Position the CTC cursor over the slot reporting the alarm.
 - Right-click **RESET CARD**.
- Step 2** If the software reset fails to clear the alarm, physically reseal the card.
- Step 3** If the physical reseal of the card fails to clear the alarm, replace the card.

**Note**

When replacing a card with an identical type of card, no additional CTC provisioning is required.

14.4.37 EQPT-MISS

- Critical, Service-Affecting

The replaceable equipment unit is missing (EQPT-MISS) alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly unit is missing or not fully inserted.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the EQPT-MISS Alarm

- Step 1** If the alarm is reported against the fan object, check that the fan-tray assembly is present.
- Step 2** If the fan-tray assembly is present, use the retractable handles embedded in the front of the fan tray to pull the fan-tray assembly forward several inches and then push the fan-tray assembly firmly back into the ONS 15327 shelf assembly and close the retractable handles.
- Step 3** If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the fan-tray assembly installation information in Chapter 1, Hardware Installation.

14.4.38 E-W-MISMATCH

- Major, Service-Affecting

A procedural error misconnect east/west direction (E-W-MISMATCH) alarm occurs when nodes in a ring have an east slot/port misconnected to another east slot/port or a west slot/port misconnected to another west slot/port. In most cases, the user did not hook up the fibers correctly, or the ring provisioning plan was flawed. You can physically reconnect the cable to the correct slot/ports to clear the E-W-MISMATCH alarm. Alternately, you can delete and recreate the span in CTC to change the west line and east line designations. The CTC method clears the alarm, but may change the traditional east-west node connection pattern of the ring.

**Note**

The E-W-MISMATCH alarm also appears during the initial set up of a ring with its East-West slot/ports configured correctly. In this instance, the alarm clears itself shortly after the ring setup is complete.

**Note**

The lower-numbered slot on a node is traditionally labelled as the west slot and the higher numbered slot is labelled as the east slot. For example, Slot 6 is west and Slot 12 is east.

Procedure: Clear the E-W-MISMATCH Alarm with a Physical Switch

- Step 1** Diagram the ring setup, including nodes and spans, on a piece of paper or white board.
- Step 2** Display the CTC network view and label each of the nodes on the diagram with the same name that appears on the window network map.
- Step 3** Double-click each span to reveal the node name/slot/port for each end of the span.
- Step 4** Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1 - Node2/Slot6/Port1 (2F BLSR OC48, Ring ID=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/ Port 1.
- Step 5** Repeat Steps 3 and 4 for each span on your diagram.
- Step 6** Label the highest slot at each node *east* and the lowest slot at each node *west*.
- Step 7** Look at the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span.
- Step 8** If any span has an east-to-east or west-to-west connection, physically switch the fiber connectors from the card that does not fit the pattern to the card that continues the pattern. This should clear the alarm.

**Note**

The above physical switch procedure is the recommended method of clearing this alarm. This method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slot/ports as east and west. This is useful when the misconnected node is not geographically near the troubleshooter.

Procedure: Clear the E-W-MISMATCH Alarm with the CTC

- Step 1** Login to the misconnected node. This is the node with both ring fibers misconnected; it is in the middle of the two nodes that have one of two ring fibers misconnected.
- Step 2** Click the **Provisioning > Ring** tabs.

-
- Step 3** From the row of information for the fiber span, write down the node ID, ring ID, and the slot and port in the east line list and west line list.
 - Step 4** Click the row from Step 3 to select it and click **Delete**.
 - Step 5** Click **Create**.
 - Step 6** Fill in the ring ID and node ID from the information collected in Step 3.
 - Step 7** Change the West line drop-down menu to the slot/port you recorded for the East line in Step 3.
 - Step 8** Change the East line drop-down menu to the slot/port you recorded for the West line in Step 3.
 - Step 9** Click **OK**.
 - Step 10** Click **Yes** at the Ring Map Change dialog box.
 - Step 11** Click **Accept** at the new ring map.
-

14.4.39 EXCCOL

- Minor, Non-Service-Affecting

The excess collisions on the LAN (EXCCOL) alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15327 unit and the CTC may be affected. The network management LAN is the data network connecting the workstation running the CTC software to the XTC card. This problem is external to the ONS 15327.

Procedure: Clear the EXCCOL Alarm

Troubleshoot the network management LAN connected to the XTC card for excess collisions. You may need to contact the system administrator of the network management LAN to accomplish the following steps:

-
- Step 1** Verify that the network device port connected to the XTC card has a flow rate set to 10 Mb, half-duplex.
 - Step 2** Troubleshoot the network device connected to the XTC card and the network management LAN.
-

14.4.40 EXERCISE-RING-FAIL

- Not Alarmed (NA) (Condition)

The exercise-ring command issues ring-protection switching of the requested channel without completing the actual bridge and switch. The exercise-ring-failed (EXERCISE-RING-FAIL) alarm is raised if the command was issued but the exercise did not take place.

Procedure: Clear the EXERCISE-RING-FAIL Condition

-
- Step 1** Check for any LOS, LOF, or BLSR service-affecting alarms.

Step 2 Lookup and troubleshoot any of these alarms, then reissue the Exercise-Ring command.

14.4.41 EXERCISE-SPAN-FAIL

- Not Alarmed (NA) (Condition)

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The exercise-span-fail (EXERCISE-SPAN-FAIL) alarm is raised if the command was issued but the exercise did not take place.

Procedure: Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Check for any LOS, LOF, or BLSR service-affecting alarms.

Step 2 Lookup and troubleshoot any of these alarms, then reissue the Exercise Span command.

14.4.42 EXT

- Minor, Service-Affecting

An external facility (EXT) alarm is detected external to the node because an environmental alarm is present, for example, a door is open or flooding has occurred.

Procedure: Clear the EXT Alarm

Step 1 Open the MIC card maintenance window to gather further information about this alarm.

Step 2 Perform your standard operating procedure for this environmental condition.

14.4.43 FAILTOSW-PATH

- Not Alarmed (NA) (Condition)

The fail to switch path (FAILTOSW-PATH) alarm means the working path did not switch to the protection path on a UPSR. Common causes of this alarm include a missing or defective protection card or a lockout set on one of the UPSR nodes.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the FAILTOSW-PATH on a UPSR Configuration

- Step 1** Ensure that a lockout is not set on the UPSR:
- Display the CTC network view.
 - Right-click the span (the line between the nodes).
 - Click **Circuits**.
 - Under Switch State, confirm that Clear appears.
 - If Clear does appear, perform Steps a – d at the next span.
 - If Clear still does not appear, click the **Switch all UPSR- circuits away** menu.
 - Choose **Clear** and click **Apply**.
 - Click **Yes** at the Confirm UPSR Switch Are You Sure? dialog box.
 - Click **OK** at the next dialog box.
- Step 2** Check the fiber connections to ensure that they are securely fastened and intact.
- Step 3** Ensure that the OC-N cards are active and in service.
- Step 4** Verify that the protect OC-N card paired with the active reporting OC-N card is the same type and in service.
- Step 5** If the alarm persists and the reporting traffic card is active, do a manual switch to move traffic away from the card:
- At the node view, click the **Maintenance > Protection** tabs.
 - Double-click the protection group that contains the reporting card.
 - Click the Protect/Standby card of the selected groups.
 - Click **Manual** and **OK**.
- Step 6** Perform a software reset on the reporting card:
- Display the CTC node view.
 - Position the cursor over the slot reporting the alarm.
 - Right-click to choose **RESET CARD**.
 - If the alarm persists, physically reseal the reporting card.
- Step 7** If the traffic does not switch over, right-click the protect card and click **Reset**.
- Step 8** Attempt another manual switch after the protect cards have booted up completely.
- Step 9** If you are still unable to perform a switch, reseal the protect card.
- Step 10** Attempt another manual switch.
- Step 11** Clear the manual switch:
- At the node view, click the **Maintenance > Protection** tabs.
 - Double-click the protection group that contains the reporting card.
 - Highlight either selected group.
 - Click **Clear** and click **YES** at the confirmation dialog box.
- Step 12** If the alarm persists, replace the protect card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 13 Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.44 FAILTOSWR

- Not Alarmed (NA) (Condition)

This fail to switch ring signals an automatic protection switching (APS) ring switch failure (FAILTOSWR) alarm clears when one of the following actions occurs: a higher priority event, such as a user-switch command occurs, the next ring switch succeeds, or the cause of the APS switch (such as an SF or SD alarm) clears.



Warning

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam 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.

Procedure: Clear the FAILTOSWR on a Four-Fiber BLSR Configuration

- Step 1** Check to see that every node expected to be part of the ring is listed in the ring map:
- Click the **Provisioning > Ring** tabs.
 - Highlight the row of the affected ring.
 - Click **Ring Map**.
 - Verify that a node ID appears in the Ring map for every node expected to be part of the ring.
- Step 2** Display the CTC network view.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** Login to the near-end node and click the **Ring > Provisioning** tabs.
- Step 5** Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards are active and in service.
- Step 6** Verify fiber continuity to the ports on the recorded cards.
- Step 7** Verify that the correct port is in service.



Caution Using a test set disrupts service on the optical card. It may be necessary to manually switch traffic carrying circuits over to a protection path.

- Step 8** Use an optical test set to verify that a valid signal exists on the line.
Test the line as close to the receiving card as possible.

- Step 9** Clean the fiber:
- a. Clean fiber according to local site practice.
 - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 10** Verify that the power level of the optical signal is within the OC-N card receiver specifications.
- Step 11** Repeat Steps 1 to 5 for any other ports on the card.
- Step 12** Replace the protect standby OC-N card.
- Step 13** If the alarm does not clear after you replace the BLSR cards on this node one by one, follow Steps 4 to 14 for each of the nodes in the ring.
- Step 14** Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
-

14.4.45 FAILTOSWS

- Not Alarmed (NA) (Condition)

This failure to switch to protection span signals an APS span switch (FAILTOSWS) alarm occurs for a four-fiber BLSR if a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS alarm does not appear. If the ring switch does not occur, the FAILTOSWS alarm appears. FAILTOSWS clears when one of the following actions occur: a higher priority event, such as a user-switch command occurs, the next ring switch succeeds, or the cause of the APS switch (such as an SF or SD alarm) clears. Follow the procedure for “Clear the FAILTOSWR on a Four-Fiber BLSR Configuration” section on page 14-38.

14.4.46 FAN

- Critical, Service-Affecting

The failure of the cooling fan-tray alarm indicates a problem with the fan-tray assembly. When the fan is not fully functional, the temperature of the ONS 15327 can rise above its normal operating range. The fan tray contains six fans and needs a minimum of five working fans to properly cool the ONS 15327. However, even with five working fans, the fan tray can need replacement because a sixth working fan is required for extra protection against overheating.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the FAN Alarm

- Step 1** Check the condition of the air filter to see if it needs replacement.
- Step 2** If the filter is clean, take the fan-tray assembly out of the ONS 15327.
- Step 3** Reinsert the fan tray making sure the back of the fan tray connects to the rear of the ONS 15327.



Note The fan should run immediately when correctly inserted.

- Step 4** If the fan does not run or the alarm persists, replace the fan tray.
- Step 5** If the replacement fan tray does not operate correctly, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
-

14.4.47 FANDEGRADE

- Major, Non-Service-Affecting

The degrade of the cooling fan-tray alarm indicates a problem with the fan-tray assembly. When the fan is not fully functional, the temperature of the ONS 15327 can rise above its normal operating range. The fan tray contains six fans and needs a minimum of five working fans to properly cool the ONS 15327. However, even with five working fans, if a fan tray is not working properly, it may need to be replaced.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the FANDEGRADE Alarm

-
- Step 1** Check the condition of the air filter to see if it needs replacement.
- Step 2** If the filter is clean, take the fan-tray assembly out of the ONS 15327.
- Step 3** Reinsert the fan tray making sure the back of the fan tray connects to the rear of the ONS 15327.



Note The fan should run immediately when correctly inserted.

- Step 4** If the fan does not run or the alarm persists, replace the fan tray.
-

14.4.48 FE-AIS

- Not Alarmed (NA) (Condition)

The far end AIS (FE-AIS) alarm means the far-end node XTC card is reporting an AIS. The prefix FE in an alarm message means the main alarm is occurring at the far-end node and not at the node reporting this FE-AIS alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both the alarms clear when the main alarm clears.

Procedure: Clear the FE-AIS Condition on the XTC-28-3 Cards in C-bit Format

-
- Step 1** To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm.
- Step 3** Clear the main alarm.
-

14.4.49 FE-DS1-MULTLOS

- Not Alarmed (NA) (Condition)

The far end multiple DS-1 LOS detected on XTC-14 or XTC-28-3 (FE-DS1-MULTLOS) condition means multiple inputs detect a loss on the far end. The prefix FE in an alarm/condition message means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTLOS alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-MULTLOS Condition on the XTC-14 Card or XTC-28-3 Card

-
- Step 1** To troubleshoot an FE condition/alarm, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE condition/alarm.
- Step 3** Look up and troubleshoot the main alarm.
-

14.4.50 FE-DS1-SNGLLOS

- Not Alarmed (NA) (Condition)

The far end single DS-1 LOS on the XTC-14 (FE-DS1-SNGLLOS) condition means one of the XTC inputs on the far end detects an LOS. The prefix FE in an alarm/condition means the main alarm is occurring at the far-end node and not at the node reporting this FE-EQPT-FAILSA alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-DS1-SNGLLOS Condition on the XTC-14

-
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm.
- Step 3** Look up and troubleshoot the main alarm.
-

14.4.51 FE-DS3-SA

- Not Alarmed (NA) (Condition)

The far end DS-3 equipment failure service-affecting (FE-DS3-SA) alarm means a far-end DS-3 equipment failure is occurring. The prefix FE in an alarm/condition means the main alarm is occurring at the far-end node and not at the node reporting the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-DS3-SA Condition on the XTC28-3 Card in C-bit Format

-
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm/condition.
- Step 3** Clear the main alarm.
-

14.4.52 FE-EQPT-NSA

- Not Alarmed (NA) (Condition)

The far end common equipment failure non-service-affecting (FE-EQPT-NSA) condition means a non-service-affecting equipment failure is detected in the far-end DS-3. The prefix FE in an alarm/condition message means that the main alarm is occurring at the far-end node, not the node reporting this FE-EQPT-NSA alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the FE-EQPT-NSA Condition on the XTC28-3 Card in C-bit Format

-
- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm/condition.
- Step 3** Look up and troubleshoot the main alarm.
-

14.4.53 FE-IDLE

- Not Alarmed (NA) (Condition)

The far end idle (FE-IDLE) condition means a far-end node detects an idle DS-3 signal. The prefix FE in an alarm/condition means that the main alarm is occurring at the far-end node, not the node reporting this FE-IDLE alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Procedure: Clear the FE-IDLE Condition on the XTC28-3 Card in C-bit Format

- Step 1** To troubleshoot the FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm/condition.
- Step 3** Clear the main alarm.
-

14.4.54 FE-LOCKOUT

- Not Alarmed (NA) (Condition)

The far-end lockout (FE-LOCKOUT) condition raises whenever the Lockout Protection Span command is entered from any other node. This alarm indicates the prevention of any ring switch requests. The alarm clears when the lock out is removed.

Procedure: Clear the FE-LOCKOUT Condition on a BLSR

- Step 1** Display CTC network view.
- Step 2** Find the node reporting the LOCKOUT-REQ.
- Step 3** Login to the node reporting the LOCKOUT-REQ.
- Step 4** Follow the “Clear the Lockout Switch Request and the LOCKOUT-REQ Condition on an OC-N Card” procedure on page 14-49.
-

14.4.55 FE-LOF

- Not Alarmed (NA) (Condition)

The far-end LOF (FE-LOF) condition means a far-end node reports a DS-3 LOF. The prefix FE in an alarm/condition means that the main alarm is occurring at the far-end node, not the node reporting this FE-LOF alarm. Troubleshoot the FE alarm/condition by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-LOF Condition on the XTC28-3 Card in C-bit Format

- Step 1** To troubleshoot an FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm.

Step 3 Look up and troubleshoot the main alarm.

14.4.56 FE-LOS

- Not Alarmed (NA) (Condition)

The far end LOS (FE-LOS) condition means a far-end node reports a DS-3 LOS. The prefix FE in an alarm/condition message means that the main alarm is occurring at the far-end node, and not at the node reporting this FE-LOS alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarm/conditions clear when the main alarm clears.

Procedure: Clear the FE-LOS Condition on the XTC28-3 Card in C-bit Format

- Step 1** To troubleshoot the FE alarm/condition, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm.
- Step 3** Clear the main alarm.
-

14.4.57 FEPRLF

- Minor, Non-Service-Affecting

The far end protection line failure (FEPRLF) alarm means that there was an APS switching channel failure of signal on the protect card coming into the node.



Note

The FEPRLF alarm only occurs on the ONS 15327 when 1+1 bidirectional protection is used on optical cards in a 1+1 configuration.

Procedure: Clear the FEPRLF Alarm on a Four-Fiber BLSR

- Step 1** To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm.
- Step 2** Login to the node that links directly to the card reporting the FE alarm.
- Step 3** Look up and troubleshoot the main alarm.
-

14.4.58 FORCED-REQ

- Not Alarmed (NA) (Condition)

The force switch request on facility or equipment (FORCED-REQ) alarm means a user entered the force command on a span or card to force traffic from a working card or working span to a protection card or protection span or vice versa. You do not need to clear this alarm if you want the force switch to remain in place. To clear this alarm, clear the force command.

Procedure: Clear the FORCED-REQ on an OC-N Card

- Step 1** Click the **Maintenance** tab.
 - Step 2** Click the **Protection** tab for a card or span switch.
 - Step 3** At **Operation**, click the drop-down arrow.
 - Step 4** Choose **Clear** and click **Apply**.
-

14.4.59 FRNGSYNC

- Major, Service-Affecting

The free-running synchronization mode (FRNGSYNC) alarm means the reporting ONS 15327 is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the ONS 15327 has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips may begin to occur on an ONS 15327 relying on an internal clock.

Procedure: Clear the FRNGSYNC Alarm

- Step 1** If the ONS 15327 is configured to operate from its own internal clock, disregard this alarm.
 - Step 2** If the ONS 15327 is configured to operate off an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards.
 - Step 3** Find and troubleshoot alarms related to the failures of the primary and secondary reference sources, such as SYNCPRI and SYNCSEC.
-

14.4.60 FSTSYNC

- Minor, Non-Service-Affecting

A fast-start synchronization mode (FSTSYNC) alarm raises when the ONS 15327 is choosing a new timing reference. The previous timing reference has failed. This alarm disappears after approximately 30 seconds.



Note This is an informational alarm.

14.4.61 HITEMP

- Critical, Service-Affecting (NE)
- Minor, Non-Service-Affecting (EQPT)

The equipment failure high temperature (HITEMP) alarm means the temperature of the ONS 15327 is above 50 degrees Celsius (122 degrees Fahrenheit).



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the HITEMP Alarm

-
- Step 1** Check the temperature of the ONS 15327 on the front panel LCD.
- Step 2** Check that the temperature of the room is not abnormally high.
- Step 3** Ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15327.
- Step 4** Ensure that blank faceplates fill the ONS 15327 empty slots. Blank faceplates help airflow.
- Step 5** Check the condition of the air filter to see if it needs replacement.
- Step 6** If the filter is clean, take the fan-tray assembly out of the ONS 15327.
- Step 7** Reinsert the fan tray, making sure the back of the fan tray connects to the rear of the ONS 15327.



Note The fan should run immediately when correctly inserted.

- Step 8** If the fan does not run or the alarm persists, replace the fan tray.
- Step 9** If the replacement fan tray does not operate correctly, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
-

14.4.62 HLDOVERSYNC

- Major, Service-Affecting

Loss of the primary/secondary timing reference raises the holdover synchronization mode (HLDOVERSYNC) alarm. Timing reference loss occurs when line coding on the timing input is different from the configuration on the ONS 15327. It also usually occurs during the selection of a new node reference clock. This alarm indicates that the ONS 15327 has gone into holdover and is using the ONS 15327 internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

Procedure: Clear the HLDOVERSYNC Alarm

-
- Step 1** Check for additional alarms that relate to timing.

Step 2 Reestablish a primary and secondary timing source according to local site practice.

14.4.63 IMPROPRMVL

- Critical, Service-affecting

The procedural error improper removal (IMPROPRMVL) alarm means a card was physically removed from its slot before the card was deleted in CTC. The card does not need to be in service to cause this alarm, it only needs to be recognized by CTC and the XTC card. This alarm does not appear if you delete the card from CTC before you physically remove the card from the node.



Caution

Do not pull a card during a card reboot. If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



Note

CTC gives the user approximately 15 seconds to physically remove the card before the CTC begins a card reboot.



Caution

It can take up to 30 minutes for software to be updated on a standby XTC card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

Procedure: Clear the IMPROPRMVL Alarm

Step 1 Right-click the card reporting the IMPROPRMVL.

Step 2 Choose **Delete**.



Note

CTC does not allow you to delete this card if the card is in service, has a circuit mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

Step 3 If the card is in service, take the facility out of service:



Caution

Before taking the facility out of service, ensure that no live traffic is present on the facility.

- In CTC, double-click the reporting card to display the card view.
- Click the **Provisioning** tab.
- Click the **Status** of any in service ports.

- d. Choose **Out of Service** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, delete the circuit:



Caution Before deleting the circuit, ensure that the circuit does not carry live traffic.

- a. At the node view, click the **Circuits** tab.
- b. Click the applicable circuit, i.e., the circuit that connects to the reporting card.
- c. Click **Delete**.

Step 5 If the card is paired in a protection scheme, delete the protection group:

- a. Click the **Provisioning > Protection** tabs.
- b. Click the protection group of the reporting card.
- c. Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning:

- a. Click the **SONET DCC > Provisioning** tabs.
- b. Click the slots and ports listed in SDCC terminations.
- c. Click **Delete** and click **Yes** in the dialog box that appears.

Step 7 If the card is used as a timing reference, change the timing reference:

- a. Click the **Provisioning > Timing** tabs.
- b. Click the **Ref-1** menu.
- c. Change Ref-1 from the listed OC-N card to Internal Clock.
- d. Click **Apply**.

Step 8 Right-click the card reporting the IMPROPRMVL and choose **Delete**.

14.4.64 INCOMPATIBLE-SW

- Minor, Non-Service-Affecting

The incompatible software (INCOMPATIBLE-SW) alarm means the CTC software version loaded on the connecting workstation and the CTC software version loaded on the XTC card are incompatible. This occurs when the XTC software is upgraded but the PC has not yet upgraded the compatible CTC jar file. INCOMPATIBLE-SW also occurs when CTC logs into a node with compatible software but encounters another node in the network that has a newer version of CTC.

Procedure: Clear the INCOMPATIBLE-SW Alarm

- Step 1** Exit the current CTC session and completely close the browser.
- Step 2** Start the browser.
- Step 3** Type the ONS 15327 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Login to CTC. The browser downloads the jar file from CTC.

14.4.65 INVMACADDR

- Major, Non-Service-Affecting

The equipment failure invalid Media Access Control (MAC) address (INVMACADDR) alarm means the ONS 15327 MAC address is invalid. The MAC Address is permanently set into the ONS 15327 chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADDR. Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447)

Procedure: Clear the INVMACADDR Alarm

This is not a user-serviceable problem. Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.66 LOCKOUT-REQ

- Not Alarmed (NA) (Condition)

The lockout-switch request on facility/equipment (LOCKOUT-REQ) alarm occurs when a user initiates a lockout-switch request for an OC-N card or a lockout-switch request on a UPSR at the path level. A lockout prevents protection switching from occurring. Clearing the lockout again allows protection switching to take place. Clearing the lockout-switch request clears the LOCKOUT-REQ alarm. This is an informational alarm.

Procedure: Clear the Lockout Switch Request and the LOCKOUT-REQ Condition on an OC-N Card

-
- Step 1** Display the CTC network view.
- Step 2** Click **Circuits** tab and highlight the circuit.
- Step 3** Click **Edit** and click the **UPSR** tab.
- Step 4** From the Switch State menu, highlight **Clear**.
- Step 5** Click **Apply** and click **Close**.
-

14.4.67 LOF (BITS)

- Major, Service-Affecting

The LOF alarm means a port on the XTC BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15327 has lost frame delineation in the incoming data.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

**Note**

The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turn-up.

Procedure: Clear the LOF Alarm

- Step 1** Verify that the line framing and line coding match between the BITS input and the XTC:
- In CTC node view or card view, note the slot and port reporting the alarm.
 - Find the coding and framing formats of the external BITS timing source. This should be in the user documentation for the external BITS timing source or on the timing source itself.
 - Click the **Provisioning > Timing** tabs to display the General Timing window.
 - Verify that **Coding** matches the coding of the BITS timing source (either B8ZS or AMI).
 - If the coding does not match, click **Coding** to reveal a menu. Choose the appropriate coding.
 - Verify that **Framing** matches the framing of the BITS timing source (either ESF or SF [D4]).
 - If the framing does not match, click **Framing** to reveal the menu. Choose the appropriate framing.

**Note**

On the timing tab, the B8ZS coding field is normally paired with ESF in the Framing field, and the AMI coding field is normally paired with SF (D4) in the Framing field.

- Step 2** If the alarm does not clear when the line framing and line coding match between the BITS input and the XTC, replace the XTC card.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.68 LOF (DS1)

- Major, Service-Affecting

The LOF alarm indicates that the receiving ONS 15327 has lost frame delineation in the incoming data. If the LOF appears on the XTC-14 card, the transmitting equipment may have its framing set to a format that differs from the receiving ONS 15327.

Procedure: Clear the LOF Alarm on the XTC-14 Card

- Step 1** Verify that the line framing and line coding match between the XTC-14 port and the signal source:
- In CTC, note the slot and port reporting the alarm.

- b. Find the coding and framing formats of the signal source for the card reporting the alarm. You may need to contact your network administrator for this information.
- c. Display the card-level view of the reporting card.
- d. Click the **Provisioning > Line** tabs.
- e. Verify that the line type of the reporting port matches the line type of the signal source.
- f. If the signal source line type does not match the reporting port, click **Line Type** to reveal a menu. Choose the matching type.
- g. Verify that the reporting Line Coding matches the signal source line type.
- h. If the signal source line coding does not match the reporting port, click **Line Coding** to reveal the menu. Choose the matching type and click **Apply**.



Note On the Line tab, the B8ZS coding field is normally paired with ESF in the Framing field. AMI coding is normally paired with SF (D4) in the Framing field.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.69 LOF (DS3)

- Critical, Service-Affecting

The LOF alarm indicates that the receiving ONS 15327 lost frame delineation in the incoming data. The framing of the transmitting equipment may be set to a format that differs from the receiving ONS 15327. On XTC-28-3 cards, the alarm occurs only on cards with the provisionable framing format set to C-bit or M23, not on cards with the provisionable framing format is set to unframed.

Procedure: Clear the LOF Alarm on the XTC-28-3 Card

Change the line type of the non-ONS equipment attached to the reporting card to C-bit.

14.4.70 LOF (OC-N)

- Critical, Service-Affecting

The LOF alarm means a port on the reporting OC-N card has an LOF condition. LOF indicates that the receiving ONS 15327 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for three milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

LOF on an OC-N card is sometimes an indication that the OC-N card reporting the alarm expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the LOF Alarm on an OC-N Card

- Step 1** The LOF should trigger an automatic protection switch away from the working card that reported the alarm. If it did not, do a manual switch to move traffic away from the reporting card:
- At the node view, click the **Maintenance > Protection** tabs.
 - Double-click the protection group that contains the reporting card.
 - Click the Protect/Standby card of the selected groups.
 - Click **Manual** and **OK**.

**Note**

If you do not have a protect card for the reporting card, create a new circuit on the reporting card to achieve the same effect.

- Step 2** Clear the manual switch:
- At the node view, click the **Maintenance > Protection** tabs.
 - Double-click the protection group that contains the reporting card.
 - Highlight either selected group.
 - Click **Clear** and click **YES** at the confirmation dialog box.

Step 3 Verify that the OC-N port on the upstream node is in service.

Step 4 If you continue to receive the LOF alarm, login to <http://www.cisco.com/TAC> for information on obtaining a return materials authorization (RMA) for the AIP or call the Cisco Technical Assistance Center (1-800-553-2447).

14.4.71 LOGBUFR90

- Major, Service-Affecting

The log buffer 90% full (LOGBUFR90) alarm means that the memory buffer holding the alarms seen on the Alarms pane in CTC is 90% full. If the buffer continues to fill, a LOGBUFROVFL alarm is reported. The LOGBUFROVFL alarm means the memory buffer is full, and any new alarms occurring on the ONS 15327 do not display on the CTC alarms pane. The CTC receives alarms from all ONS nodes on the network, even if the CTC is set to the node or card-level view.

Procedure: Clear the LOGBUFR90 Alarm

- Step 1** Click the close button on the upper right corner of the CTC window.
- Step 2** Click the close button on the upper right corner of the browser window.

Step 3 Log back into the ONS 15327. The LOGBUFR90 alarm should clear after an approximately one minute delay.

Exiting CTC and logging back into the ONS 15327 removes any cleared alarms from the log buffer and resynchronizes the alarm pane to show any alarms that were not displayed as a result of a full log buffer.



Note Checking the AutoDelete Cleared Alarms checkbox on the Alarms panel helps prevent log buffer overflow.

14.4.72 LOGBUFROVFL

- Major, Service-Affecting

The log buffer overflow (LOGBUFROVFL) alarm means the memory buffer is full, and any new alarms occurring on the ONS 15327 do not display on the CTC alarms pane. The CTC receives alarms from all ONS nodes on the network, even if the CTC is set to the node or card-level view.

Procedure: Clear the LOGBUFROVFL Alarm

Step 1 Click the close button on the upper-right corner of the CTC window.

Step 2 Click the close button on the upper-right corner of the browser window.

Step 3 Log back into the ONS 15327. The LOGBUFROVFL alarm should clear after an approximately one minute delay.

Exiting CTC and logging back into the ONS 15327 removes any cleared alarms from the log buffer and resynchronizes the alarm pane to show any alarms not displayed as a result of a full log buffer.



Note Checking the AutoDelete Cleared Alarms checkbox on the Alarms panel helps prevent log buffer overflow.

14.4.73 LOP-P

- Critical, Service-Affecting

This loss of pointer path (LOP-P) alarm indicates a loss of pointer at the path level. LOP occurs when valid H1/H2 pointer bytes are missing from the SONET overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP alarm means that eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

One of the conditions that can cause this alarm is a transmitted STSc circuit that is smaller than the provisioned STSc. This condition causes a mismatch of the circuit type on the concatenation facility. For example, if an STS-3c or STS-1 is sent across a circuit provisioned for STS-12c, a LOP alarm occurs.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the LOP-P Alarm

Step 1 Verify the cabling and physical connections on the reporting card.

Step 2 Perform a soft reset on the reporting card:

- a. Display the CTC node view.
- b. Position the cursor over the slot reporting the alarm.
- c. Right-click to choose **RESET CARD**.

Step 3 Do a manual switch (side switch) to move traffic away from the card:

- a. At the node view, click the **Maintenance > Protection** tabs.
- b. Double-click the protection group that contains the reporting card.
- c. Click the Protect/Standby card of the selected groups.
- d. Click **Manual** and **OK**.

**Note**

If you do not have a protect card for the reporting card, create a new circuit on the reporting card to achieve the same effect.

Step 4 Clear the manual switch:

- a. At the node view, click the **Maintenance > Protection** tabs.
- b. Double-click the protection group that contains the reporting card.
- c. Highlight either selected group.
- d. Click **Clear** and click **YES** at the confirmation dialog box.

Step 5 If the alarm persists, the problem is at the far-end node. Verify the stability of the cabling and physical connections that connect to the far-end card.

Step 6 Perform a soft reset on the far-end card:

- a. Display the CTC node view.
- b. Position the cursor over the slot reporting the alarm.
- c. Right-click and choose **RESET CARD**.

Step 7 Perform a soft reset on the reporting card:

- a. Display the CTC node view.
- b. Position the cursor over the slot reporting the alarm.
- c. Right-click and choose **RESET CARD**.

Step 8 Switch from the far-end working card to the far-end protect card.

Step 9 If the alarm persists, replace the far-end card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.74 LOP-V

- Major, Service-Affecting

The loss of pointer VT (LOP-V) alarm indicates a loss of pointer at the VT level. The VT, or electrical, layer occurs when the SONET signal is broken down into an electrical signal, for example, when an optical signal comes into an ONS 15327. The ONS 15327 demultiplexes this optical signal. One of the channels separated from the optical signal cross connects into an ONS 15327 XTC card port. The ONS 15327 reports the LOS-V alarm.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the LOP-V Alarm on the XTC Card

Step 1 Verify the stability of the cabling and physical connections on the reporting card.

Step 2 Perform a software reset on the reporting card:

- Display the CTC node view.
- Position the cursor over the slot reporting the alarm.
- Right-click and choose **RESET CARD**.

Step 3 Perform a manual switch to move traffic away from the card:

- At the node view, click the **Maintenance > Protection** tabs.
- Double-click the protection group that contains the reporting card.
- Click the Protect/Standby card of the selected groups.
- Click **Manual** and **OK**.



Note If you do not have a protect card for the reporting card, create a new circuit on the reporting card to achieve the same effect.

Step 4 Clear the manual switch:

- At the node view, click the **Maintenance > Protection** tabs.
- Double-click the protection group that contains the reporting card.
- Highlight either selected group.
- Click **Clear** and click **YES** at the confirmation dialog box.

Step 5 If the alarm persists, the problem is at the far-end node. Verify the cabling and physical connections that connect to the far-end card.

- Step 6** Perform a soft reset on the far-end card.
- Step 7** Switch from the far-end working card to the far-end protect card.
-

14.4.75 LOS (BITS)

- Major, Service-Affecting

The XTC card has a loss of signal (LOS) from the BITS timing source. An LOS alarm occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (BITS-N) means the BITS clock or the connection to the BITS clock failed.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the LOS Alarm

- Step 1** Verify the wiring connection from the ONS 15327 backplane BITS clock pin fields to the timing source.
- Step 2** Check that the BITS clock is operating properly.
-

14.4.76 LOS (DS-N)

- Critical, Service-Affecting

The LOS is alarm indicates a loss of signal at the card for an XTC card port. LOS occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the LOS Alarm on the XTC Card

- Step 1** Verify cabling continuity to the port.
- Step 2** Verify that the correct port is in service.
- Step 3** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible.
- Step 4** Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.
- Step 5** If there is a valid signal, replace the DS-N connector on the ONS 15327.

- Step 6** Repeat Steps 1 to 5 for another port on the card.
- Step 7** Look for another alarm that may identify the source of the problem.
- Step 8** Replace the reporting card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.77 LOS (OC-N)

- Critical, Service-Affecting

A port on the reporting OC-N card has a loss of signal (LOS) condition. An LOS occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS means the upstream transmitter has failed. If an OC-N LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. The condition clears when two consecutive valid frames are received.



Warning

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



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the LOS Alarm on an OC-N Card

- Step 1** Verify fiber continuity to the port.
- Step 2** Verify that the correct port is in service.
- Step 3** Use an optical test set to verify that a valid signal exists on the line.
Test the line as close to the receiving card as possible.
- Step 4** Clean the fiber:
- a. Clean fiber according to local site practice.
 - b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 5** Verify that the power level of the optical signal is within the OC-N card receiver specifications.
- Step 6** If there is a valid signal, replace the connector on the backplane.
- Step 7** Repeat Steps 1 to 5 for another port on the card.
- Step 8** Replace the OC-N card.

14.4.78 LPBKDS1FEAC

- Not Alarmed (NA) (Condition)

A loopback due to FEAC command DS1 (LPBKDS1FEAC) condition on the XTC card means a DS-1 loopback signal is received from the far-end node due to a Far-End Alarm and Control (FEAC) command. An FEAC command is often used with loopbacks.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. A troubleshooter can compare the quality of the sent signal and the returned signal to determine the condition of an isolated circuit. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information about loopbacks, see the “Network Tests” section on page 12-19.



Caution

The CTC permits loopbacks on an in-service circuit. This operation is service-affecting.



Note

This is an informational alarm.

14.4.79 LPBKDS3FEAC

- Not Alarmed (NA) (Condition)

A loopback due to FEAC command DS-3 (LPBKDS3FEAC) condition means an XTC-28-3 loopback signal is received from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. This condition is only reported by the XTC-28-3 card. An XTC-28-3 card both generates and reports FEAC alarm/conditions.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. A troubleshooter can compare the quality of the sent signal and the returned signal to determine the condition of this isolated circuit. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information about loopbacks, see the “Network Tests” section on page 12-19.



Caution

The CTC permits loopbacks on an in-service circuit. This operation is service-affecting.



Note

This is an informational alarm.

14.4.80 LPBKFACILITY (DS-N)

- Not Alarmed (NA) (Condition)

A loopback facility (LPBKFACILITY) alarm means a software facility loopback is active for a port on the reporting card. Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically narrow down the source of the problem. For more information on loopbacks, see “Network Tests” section on page 12-19.

There are two types of loopbacks: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far-end equipment. You can provision loopbacks through CTC.

**Caution**

The CTC permits loopbacks to be performed on an in-service circuit. This operation is service-affecting.

**Note**

XTC-28-3 cards only support facility loopbacks on DS-1 circuits.

Procedure: Clear the LBKFACILITY Condition on the XTC-28-3 Card

-
- Step 1** Double-click the reporting card in CTC or right-click the reporting card in CTC and choose **Open** from the menu.
- Step 2** Click the **Maintenance** tab:
- a. If the condition is reported against an XTC-28-3 card, also click the **DS1** tab.
 - b. If a Loopback Type column cell that displays Facility (Line) is not shown under the **DS1** tab, then click the **DS3** tab to reveal a Loopback Type column cell that displays Facility (Line).
- Step 3** Click the Loopback Type column cell that displays Facility (Line).
- Step 4** Click **None**, and click **Apply**.
-

14.4.81 LPBKFACILITY (OC-N)

- Not Alarmed (NA) (Condition)

A loopback facility (LPBKFACILITY) alarm means a software facility loopback is active for a port on the reporting card. Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or part of the network and returned to the sending device. A troubleshooter can compare the quality of the sent signal and the returned signal to determine the condition of an isolated circuit. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter can logically isolate the source of the problem. For more information on loopbacks, see the “Network Tests” section on page 12-19.

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far end equipment. You provision loopbacks using CTC.

**Caution**

Before performing a facility loopback on an OC-N card, make sure there is another SDCC path to the ONS 15327 containing the OC-N card being put in loopback. A second SDCC path is necessary so you have a non-looped back path to login to the ONS 15327 containing the OC-N card being put in loopback and remove the facility loopback. This is not necessary if you are directly connected to the ONS 15327 with the OC-N card in facility loopback.

Procedure: Clear the LBKFACILITY Condition on the OC-N Card

-
- Step 1** To remove the loopback alarm, double-click or right-click the reporting card in the CTC. Choose **Open** from the list of options.
- Step 2** Click the **Maintenance** tab.
- Step 3** Click the Loopback Type column and choose **None** from the menu.
- Step 4** Click **Apply**.
-

14.4.82 LPBKTERMINAL (DS-N)

- Not Alarmed (NA) (Condition)

A loopback terminal (LPBKTERMINAL) alarm means a software terminal loopback is active for a port on the reporting card. Loopback is a commonly used troubleshooting technique. When a port is set in terminal loopback the outgoing signal (Ethernet or DS-N) being transmitted is fed back into the receive direction on the same port and the externally received signal is ignored. On the DS-N card the outgoing signal continues to be transmitted and then returned in the receiving direction of the sending device. A troubleshooter can compare the quality of the sent signal and the returned signal to determine the condition of an isolated circuit. By setting up loopbacks on various parts of the network and excluding other parts, a troubleshooter logically isolates the source of the problem. For more information on loopbacks, see the “Network Tests” section on page 12-19.

Two types of loopbacks are available: Facility and Terminal. Facility loopbacks troubleshoot ports only and are generally performed locally or at the near end. Terminal loopbacks test ports and spans and are often used for remote sites or far-end equipment. Loopbacks are provisioned using CTC. Terminal loopback is not supported at the DS1 level for the XTC-28-3 card.

**Caution**

CTC permits loopbacks on an in-service circuit. This operation is service-affecting.

Procedure: Clear the LPBKTERMINAL Condition on an XTC Card

-
- Step 1** To remove the loopback alarm, double-click the reporting card in CTC, or right-click the reporting card and choose **Open** from the list of options.
- Step 2** Click the **Maintenance** tab.
- Step 3** Choose the Loopback Type column and choose **None** from the menu.

Step 4 Click **Apply**.

14.4.83 MANRESET

- Not Alarmed (NA) (Condition)

A manual system reset (MANRESET) condition means a user performed a manual system reset by right-clicking a card and chose **Reset**. Resets performed during a software upgrade also prompt the alarm. This condition clears automatically, when the card finishes resetting.

14.4.84 MAN-REQ

- Not Alarmed (NA) (Condition)

The manual switch request on a facility/equipment (MAN-REQ) alarm occurs when a user initiates a manual switch request on an OC-N card or UPSR path. Clearing the manual switch clears the MANUAL-REQ alarm.

Procedure: Clear the Manual Switch and the MAN-REQ Condition on an OC-N Card

- Step 1** From network view, click the **Circuits** tab.
- Step 2** Highlight the circuit.
- Step 3** Click **Edit** and click the **UPSR** tab.
- Step 4** From the Switch State menu, highlight **Clear**.
- Step 5** Click **Apply** and click **Close**.
-

14.4.85 MEA (AIP)

- Critical, Service-Affecting

If the mismatch between entity/equipment type and provisioned attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board may have blown, and the AIP needs replacement.

Procedure: Clear the MEA Alarm on the AIP

- Step 1** The fuse in the AIP board may be blown and the board needs to be replaced. Login to <http://www.cisco.com/TAC> for information on obtaining a return materials authorization (RMA) for the AIP or call the Cisco Technical Assistance Center (1-800-553-2447).
-

14.4.86 MEA (EQPT)

- Critical, Service-Affecting

The mismatch between entity/equipment type and provisioned attributes (MEA) alarm occurs when the physical card inserted in a slot does not match the card type that is provisioned for that slot in CTC. The alarm clears when the provisioned card type and the physical card type match.

Procedure: Clear the MEA Alarm

-
- Step 1** Physically verify the type of card that sits in the slot reported in the object column of the MEA row on the alarms window.
- Step 2** Click the **Inventory** tab to reveal the provisioned card type.
- Step 3** If you prefer the card type depicted by CTC, physically insert that type of card (provisioned for that slot).
- Step 4** If you prefer the card that physically occupies the slot, put the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.



Note If the card is in service, has a circuit mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, then CTC does not allow you to delete the card.

- Step 5** If the card is in service, take the facility out of service:



Caution Before taking the facility out of service, ensure that no live traffic exists on the facility.

- Double-click the reporting card to display the card view.
- Click the **Provisioning** tab.
- Click the **Status** of any in-service ports.
- Choose **Out of Service** to take the ports out of service.

- Step 6** If a circuit has been mapped to the card, delete the circuit:



Caution Before deleting the circuit, ensure that no live traffic exists on the facility.

- On the node view, click the **Circuits** tab.
- Choose the applicable circuit (the one that connects to the reporting card).
- Click **Delete**.

- Step 7** If the card is paired in a protection scheme, delete the protection group:

- Click the **Provisioning > Protection** tabs.
- Choose the protection group of the reporting card.
- Click **Delete**.

- Step 8** Right-click the card reporting the IMPROPRMVL.
- Step 9** Choose **Delete**.
-

14.4.87 MEA (FAN)

- Critical, Service-Affecting

The mismatch between entity/equipment type and provisioned attributes (MEA) alarm is reported against the fan tray when an older ONS 15327 fan-tray assembly (FTA2) is used with certain cards that require the newer fan-tray assembly (15327-FTA3). The 10 Gbps compatible shelf assembly (15327-SA-10G) and fan-tray assembly (15327-FTA3) are required with the ONS 15327 XTC, E10/100-4, and OC-48 cards.

Procedure: Clear the MEA Alarm on the Fan-Tray Assembly

- Step 1** At the CTC shelf view, click the **Inventory** tab.
- Step 2** Under the Hardware Part # column, if the number is 800-19856-XX, then you have a 10 Gbps compatible shelf assembly (15327-SA-10G). See Chapter 1, Hardware Installation for procedures to install a new fan-tray assembly (15327-FTA3).
- Step 3** Under the Hardware Part # column, if the number is not 800-19856-01, then you are using an earlier shelf assembly. This is shelf assembly is not compatible with the XTC, E10/100-4 or OC-48 cards. Remove the incompatible cards to clear the alarm.
-

14.4.88 MEM-GONE

- Major, Non-Service-Affecting

The memory gone (MEM-GONE) alarm occurs when data generated by software operations exceeds the memory capacity of the XTC card. CTC does not function properly until this alarm clears. The alarm clears when additional memory becomes available.

Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.89 MEM-LOW

- Minor, Non-Service-Affecting

The free memory of card almost gone (MEM-LOW) alarm occurs when data generated by software operations is close to exceeding the memory capacity of the XTC card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the XTC card is exceeded, CTC ceases to function.

Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.90 MFGMEM

- Critical, Service-Affecting

The manufacturing data memory failure (MFGMEM) alarm raises if the ONS 15327 cannot access the data in the erasable programmable read-only memory (EPROM). Either the memory module on the component failed or the XTC lost the ability to read that module. The EPROM stores manufacturing data that is needed for both compatibility and inventory issues. The EPROM on the alarm interface panel (AIP) also stores the MAC address. An inability to read a valid MAC address disrupts IP connectivity and gray out the ONS 15327 icon on the CTC network view.

Procedure: Clear the MFGMEM Alarm on the AIP, Fan Tray, or Backplane

-
- Step 1** Do a software-initiated system reset on the XTC by referring to the “Perform a Software Reset” procedure on page 12-5.
- Step 2** If the alarm does not clear, do a card pull reset on the XTC by referring to the “Perform a Card Pull” procedure on page 12-5.
- Step 3** If the alarm does not clear, physically replace the standby XTC card on the ONS 15327 with a new XTC card:
- Open the XTC card ejectors.
 - Slide the card out of the slot. This raises the IMPROPRMVL alarm which clears when the upgrade is complete.
 - Open the ejectors on the XTC card.
 - Slide the XTC card into the slot along the guide rails.
 - Close the ejectors.



Note It takes approximately 30 minutes for the active XTC to transfer the system software to the newly installed XTC. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the LEDs on the XTC flash Fail and then the Active/Standby LED flashes. When the transfer completes, the XTC reboots and goes into Standby mode after approximately three minutes.

Step 4 Right-click the active XTC card to reveal a drop-down menu.

Step 5 Click **Reset Card**.

Wait for the XTC to reboot. The ONS 15327 switches the standby XTC card to active mode.

Step 6 Verify that the remaining XTC card is now in standby mode (the ACT/STBY LED changes to amber).

Step 7 Physically replace the remaining XTC card with the second XTC card.

- Open the XTC card ejectors.
- Slide the card out of the slot.
- Open the ejectors on the XTC card.
- Slide the XTC card into the slot along the guide rails.
- Close the ejectors.

The ONS 15327 boots up the second XTC card. The second XTC must also copy the system software, which can take up to twenty minutes.

- Step 8** If the MFGMEM alarm continues to report after replacing the XTC cards, the problem lies in the EPROM.
- Step 9** If the MFGMEM is reported from the fan tray, replace the fan tray.
- Step 10** If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan tray is replaced, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center (1-800-553-2447).
-

14.4.91 NOT-AUTHENTICATED

- Minor, Non-Service-Affecting

This not authenticated (NOT-AUTHENTICATED) alarm indicates that the username and password entered do not match the information stored in the XTC. All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes.

**Note**

For initial logon to the ONS 15327, type the user name `CISCO15` and click **Login** (no password is required).

Procedure: Clear the NOT-AUTHENTICATED Alarm on the XTC Card

- Step 1** If you have an alternate username and a password available to access the system:
- Use the alternate username and password to access the ONS node.
 - Click the **Provisioning > Security** tabs.
 - Look under the Users field to find the username that raised the alarm.
 - If the username that raised the alarm is listed, then highlight the username to reveal the associated password. Record the correct password.
 - If the username is not listed, then click **Create**.
 - Fill in the fields on the Create User dialog box with the username and password that raised the alarm then click **OK**.
- Step 2** If you do not have an alternate username and password available, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447). TAC can issue a new username and password.
-

14.4.92 PDI-P

- Not Alarmed (NA) (Condition)

A payload defect indication path (PDI-P) alarm indicates a signal label mismatch failure (SLMF). An invalid C2 byte in the SONET path overhead causes an SLMF. The C2 byte is the signal label byte. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. It enables a SONET device to transport multiple types of services.

The ONS 15327 encounters an SLMF when the payload, such as an ATM, does not match what the signal label is reporting. An AIS alarm often accompanies the PDI-P alarm. If the PDI-P is the only alarm reported with the AIS, clear the PDI-P alarm to clear the AIS alarm. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid alarm.

**Warning**

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

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the PDI-P Condition

-
- Step 1** Verify that all circuits terminating in the reporting card are in an active state:
- a. Click the **Circuits** tab.
 - b. Verify that the State column lists the port as **ACTIVE**.
 - c. If the State column lists the port as **INCOMPLETE**, wait 10 minutes for the ONS 15327 to fully initialize. If **INCOMPLETE** does not change after full initialization, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

Step 2 After determining that the port is active, verify the signal source to the card reporting the alarm.

Step 3 If traffic is affected, delete and recreate the circuit.



Caution Deleting a circuit may affect traffic.

Step 4 Check the far-end OC-N card that provides STS payload to the reporting card.

Step 5 Confirm the cross-connect between the OC-N card and the reporting card.

Step 6 Clean the far-end optical fiber:

- a. Clean the fiber according to local site practice.
- b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 7 Replace the optical/electrical cards.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.93 PEER-NORESPONSE

- Major, Non-Service-Affecting

The switch agent raises a peer card not responding (PEER-NORESPONSE) alarm if either traffic card in a protection group does not receive a response to the peer-status request message. This is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Procedure: Clear the PEER-NORESPONSE Alarm Reported on XTC or OC-N Card

-
- Step 1** Right-click the card reporting the alarm.
- Step 2** Click **Reset Card** and **OK** on the confirmation dialog.
- Step 3** Wait for the card to reset.
- Step 4** At reset, the green Act LED on the card is replaced on the CTC by a white Ldg LED. When the card finishes resetting, the green Act LED reappears.
- Step 5** Right-click the peer card of the card reporting the alarm.
- Step 6** Click **Reset Card** and **OK** on the confirmation dialog.
-

14.4.94 PLM-P

- Critical, Service-Affecting

A payload label mismatch path (PLM-P) alarm indicates an SLMF. An invalid C2 byte in the SONET path overhead causes an SLMF. The C2 byte is the signal label byte. This byte tells the equipment what the SONET payload envelope contains and how it is constructed. It enables a SONET device to transport multiple types of services.

The ONS 15327 encounters an SLMF when the payload, such as a DS-3 signal, does not match what the signal label is reporting. An AIS alarm often accompanies the PLM-P alarm. If the PLM-P is the only alarm reported with the AIS, clearing the PLM-P alarm clears the AIS alarm.



Warning

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



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the PLM-P Alarm Reported on the XTC Card

-
- Step 1** Verify that all circuits terminating in the reporting card are active:
- Click the **Circuits** tab.
 - Verify that the State column lists the port as ACTIVE.

- c. If the State column lists the port as INCOMPLETE, wait 10 minutes for the ONS 15327 to fully initialize. If INCOMPLETE does not change after full initialization, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

Step 2 After determining the port is active, verify the signal source to the traffic card reporting the alarm.

Step 3 If traffic is being affected, delete and recreate the circuit.



Caution Deleting a circuit may affect traffic.

Step 4 Check the far-end OC-N card that provides STS payload to the XTC card.

Step 5 Verify the cross-connect between the OC-N card and the XTC card.

Step 6 Clean the far-end optical fiber:

- a. Clean the fiber according to local site practice.
- b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

Step 7 Replace the OC-N/XTC cards.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.95 PLM-V

- Minor, Service-Affecting

A VT-payload label mismatch (PLM-V) alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. This alarm occurs when ONS nodes interoperate with equipment that performs bit-synchronous mapping for DS-1. ONS nodes use asynchronous mapping.

Procedure: Clear the PLM-V Alarm on the XTC-14 or XTC-28-3 Card

Step 1 Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.

Step 2 Verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

14.4.96 PRC-DUPID

- Major, Service-Affecting

The procedural error duplicate node ID (PRC-DUPID) alarm indicates that two identical node IDs exist in the same ring. The ONS 15327 requires each node in the ring to have a unique node ID.

Procedure: Clear the PRC-DUPID Alarm on an OC-N Card in a BLSR

-
- Step 1** Find the nodes with identical node IDs.
- Login to a node on the ring.
 - Click the **Provisioning > Ring** tabs.
 - Record the node ID number.
 - Repeat Steps a to c for all nodes in the ring.
- Step 2** If two nodes have an identical node ID number, change the node ID number of one node.
- Login to a node that has an identical node ID number.
 - Click the **Provisioning > Ring** tabs.
 - Change the number in the Node ID field to a unique number between 0 and 31.
 - Click **Apply**.
-

14.4.97 RAI

- Not Alarmed (NA) (Condition)

The remote alarm indication condition (RAI) signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other.

RAI on the XTC card indicates that far-end node is receiving a DS-3 AIS.

Procedure: Clear the RAI Condition on XTC-28-3 Cards in C-bit Format

Use the AIS procedure to troubleshoot the far-end DS-3 node for RAI.

14.4.98 RCVR-MISS

- Major, Service-Affecting

A facility-termination equipment receiver missing (RCVR-MISS) alarm occurs when the facility-termination equipment detects an incorrect amount of impedance on its backplane connector. This usually occurs when a missing receive cable on the XTC-14 port or a possible mismatch of backplane equipment, for example, an SMB connector or a BNC connector is connected to an XTC-14 card.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.



Note

DS-1s are four-wire circuits and need a positive (tip) and negative (ring) connection for both transmit and receive.

Procedure: Clear the RCVR-MISS Alarm on the XTC-14 Port

-
- | | |
|---------------|--|
| Step 1 | Ensure that the device attached to the XTC-14 port is operational. |
| Step 2 | Verify that the cabling is securely connected. |
| Step 3 | Verify that the pinouts are correct. |
| Step 4 | Replace the receive cable if Steps 1 – 3 do not clear the alarm. |
-

14.4.99 RDI-P

See the RFI-P, page 14-70.

14.4.100 RFI-L

- Not Reported (NR)

A remote-fault indication (RFI) alarm occurs when the ONS 15327 detects a remote-fault indication (RFI) in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L alarm in the reporting node.

RFI-L indicates that the alarm is occurring at the line level. The line layer is the segment between two SONET devices in the circuit and is also known as a maintenance span. The line layer deals with SONET payload transport. The line layer functions include multiplexing and synchronization.

Procedure: Clear the RFI-L Condition on the OC-N Card

-
- | | |
|---------------|---|
| Step 1 | Login to the far-end node from the reporting ONS 15327. |
| Step 2 | Check for alarms in the far-end node, especially LOS. |
| Step 3 | Resolve alarms in the far-end node. |
-

14.4.101 RFI-P

- Not Reported (NR)

A remote failure indication path (RFI-P) alarm occurs when the ONS 15327 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P alarm in the reporting node.

RFI-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. This segment may encompass several consecutive line segments. The originating equipment puts bits together into a SONET payload and the terminating equipment breaks the bits apart again. SONET multiplexers, such as the ONS 15327, often perform the origination and termination tasks of the SONET payload.

An RFI-P error message on the ONS 15327 indicates that the node reporting the RFI-P is the terminating node on that path segment.

**Note**

Any disruptions to the Ethernet or XTC card can cause an outage of Ethernet traffic for up to 10 minutes. During this period, convergence occurs and Ethernet traffic is restored.

Procedure: Clear the RFI-P Condition on the XTC or E10/100-4 Card

-
- Step 1** Verify that the ports are enabled and in service on the reporting ONS 15327.
- Step 2** To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.
- Step 3** Check for alarms in the node with the failure, especially UNEQ-P or UNEQ-V.
- Step 4** Resolve alarms in that node.
-

14.4.102 RFI-V

- Not Reported (NR)

A remote-fault indication VT (RFI-V) alarm occurs when the ONS 15327 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V alarm in the reporting node.

RFI-V indicates that an upstream failure has occurred at the VT layer. The VT (electrical) layer is created when the SONET signal is broken down into an electrical signal, for example when an optical signal comes into an ONS 15327. If this optical signal is demultiplexed and one of the channels separated from the optical signal is cross connected into the XTC-14 port in the ONS 15327, the ONS 15327 reports an RFI-V alarm.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the RFI-V Condition on the XTC Card

-
- Step 1** Check connectors to ensure that they are securely fastened and connected to the correct slot/port.
- Step 2** Verify that the XTC-14 port is active and in service.
- Step 3** Check the signal source for errors.
- Step 4** Login to the far-end node from the reporting ONS 15327.
- Step 5** Check for alarms in the far-end node, especially UNEQ-P or UNEQ-V.
- Step 6** Find and troubleshoot the far-end node alarms.
-

14.4.103 RING-MISMATCH

- Major, Service-Affecting

A procedural error mismatch ring (RING-MISMATCH) alarm occurs when the ring ID of the ONS 15327 that is reporting the alarm does not match the ring ID of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical ring IDs to function.

Procedure: Clear the RING-MISMATCH Alarm

-
- Step 1** Click the **Provisioning > Ring** tabs.
- Step 2** Note the number in the Ring ID field.
- Step 3** Login to the next ONS node in the BLSR.
- Step 4** Verify that the ring ID number matches the ring ID number of the reporting node:
- If the ring ID matches the ring ID in the reporting ONS node, login to the next ONS node in the BLSR.
 - If the ring ID does not match the ring ID in the reporting ONS node, change the ring ID to match the ring ID of the reporting node and click **Apply**.
 - Click **Yes** on the Accept Ring Map Changes dialog box.
 - Verify that the ring map is correct.
 - Click **Accept** for the new BLSR ring map.
- Step 5** Repeat Step 4 for all ONS nodes in the BLSR.
-

14.4.104 SD-L

- Not Alarmed (NA) (Condition)

A signal degrade (SDFL) alarm occurs when the quality of the signal is so poor that the bit error rate (BER) on the incoming optical line passed the SD threshold. Signal degrade is defined by Telcordia as a “soft failure” condition. SD and SF both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF. The BER threshold on the ONS 15327 is user provisionable and has a range for SD from 10^{-9} to 10^{-5} . SD-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SD alarm travels on the B2 byte of the SONET overhead.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.



Warning

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



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SD-L Condition on an OC-N Card

-
- Step 1** Verify that the user-provisionable BER threshold is set at the expected level:
- From the CTC node view, double-click the card reporting the alarm to bring up the card view.
 - Click the **Provisioning > Line** tabs.
 - Under the SD BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.
 - If the entry is consistent with what the system was originally provisioned for, continue with Step 2.
 - If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
 - Click **Apply**.
- Step 2** With an optical test set, measure the power level of the line to ensure it is within guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Clean the fibers at both ends for a line signal degrade:
- Clean the fiber according to local site practice.
 - If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 5** Verify that single-mode fiber is used.
- Step 6** Verify that a single-mode laser is used at the far end.
- Step 7** If the problem persists, the transmitter at the other end of the optical line may be failing and require replacement.
-

14.4.105 SD-P

- Not Alarmed (NA) (Condition)

A signal degrade (SDFP) alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal degrade (SD) threshold. Signal degrade is defined by Telcordia as a “soft failure” condition. SD and signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF. SD causes the card to switch from working to protect. The BER threshold on the ONS 15327 is user provisionable and has a range for SD from 10^{-9} to 10^{-5} . SD-P causes a switch from the working card to the protect card at the path (STS) level. A path or STS level SD alarm travels on the B3 byte of the SONET overhead. The ONS 15327 detects path SD on the STS level, not the VT level.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.



Warning

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

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SD-P Condition on an OC-N Card

-
- Step 1** Verify that the user-provisionable BER threshold is set at the expected level:
- From the CTC node view, double-click the card reporting the alarm to bring up the card view.
 - Click the **Provisioning > Line** tabs.
 - Under the SD BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-7.
 - If the entry is consistent with what the system was originally provisioned for, continue with Step 2.
 - If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
 - Click **Apply**.
- Step 2** With an optical test set, measure the power level of the line to ensure it is within guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Verify that single-mode fiber is being used.
- Step 5** Verify that a single-mode laser is being used at the far end.
- Step 6** If the problem persists, the transmitter at the other end of the optical line may be failing and require replacement.
-

14.4.106 SF-L

- Not Alarmed (NA) (Condition)

A signal failure (SFL) alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure (SF) threshold. Signal failure is defined by Telcordia as a “hard failure” condition. SD and SF both monitor the incoming BER error rate and are similar alarms, but SF is triggered at a higher BER than SD. The BER threshold on the ONS 15327 is user provisionable and has a range for SF from 10^{-5} to 10^{-3} . SF-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SF alarm travels on the B2 byte of the SONET overhead.

SF causes a card to switch from working to protect at either the path or line level. The SF alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

**Warning**

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

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SF-L Condition on an OC-N Card

-
- Step 1** Verify that the user-provisionable BER threshold is set at the expected level:
- From the CTC node view, double-click the card reporting the alarm to bring up the card view.
 - Click the **Provisioning > Line** tabs.
 - Under the SF BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-4.
 - If the entry is consistent with what the system was originally provisioned for, continue with Step 2.
 - If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
 - Click **Apply**.
- Step 2** Using an optical test set, measure the power level of the line and ensure it is within the guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Clean the fibers at both ends for a line signal fail:
- Clean the fiber according to local site practice.
 - If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 5** Verify that single-mode fiber is being used.
- Step 6** Verify that a single-mode laser is being used at the far-end node.
- Step 7** If the problem persists, the transmitter at the other end of the optical line may be failing and need replacement.
-

14.4.107 SF-P

- Not Alarmed (NA) (Condition)

A signal failure (SFP) alarm occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the signal failure (SF) threshold. Signal failure is defined by Telcordia as a “hard failure” condition. SD and SF both monitor the incoming BER error rate and are similar alarms, but SF is triggered at a higher BER than SD. The BER threshold on the ONS 15327 is user provisionable and has a range for SF from 10^{-5} to 10^{-3} . SF-P causes a switch from the working card to the protect card at the path (STS) level. A path or STS level SF alarm travels on the B3 byte of the SONET overhead. The ONS 15327 detects path SF on the STS level, not the VT level.

The SF alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

**Warning**

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

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SF-P Condition on an OC-N Card

-
- Step 1** Verify that the user-provisionable BER threshold is set at the expected level:
- a. From the CTC node view, double-click the card reporting the alarm to bring up the card view.
 - b. Click the **Provisioning > Line** tabs.
 - c. Under the SF BER column on the Provisioning pane, check that the cell entry is consistent with what the system was originally provisioned for. The default setting is 1E-4.
 - d. If the entry is consistent with what the system was originally provisioned for, continue to step 2.
 - e. If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the entry that is consistent with what the system was originally provisioned for.
 - f. Click **Apply**.
- Step 2** Using an optical test set, measure the power level of the line and ensure it is within the guidelines.
- Step 3** Verify that optical receive levels are within the acceptable range.
- Step 4** Verify that single-mode fiber is being used.
- Step 5** Verify that a single-mode laser is being used at the far-end node.
- Step 6** If the problem persists, the transmitter at the other end of the optical line may be failing and need replacement.
-

14.4.108 SFTWDOWN

- Minor, Non-Service-Affecting

A software download in progress (SFTWDOWN) alarm occurs when the XTC is downloading or transferring software. No action is necessary. Wait for the transfer or the software download to complete.

**Caution**

It can take up to 30 minutes for software to be updated on a standby XTC card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

14.4.109 SFTWDOWN-FAIL

- Minor, Non-Service-Affecting

The software download fail alarm (SFTWDOWN-FAIL) indicates the download from the XTC card to the ONS 15327 failed. The problem lies in the XTC card.

**Caution**

It can take up to 30 minutes for software to be updated on a standby XTC card. Wait the full time period before removing the card. Premature removal can cause flash corruption.

Procedure: Clear the SFTWDOWN-FAIL Alarm on the XTC Card

Step 1 Attempt the download again by clicking the **Maintenance > Software** tabs.

Step 2 Click the **Download** button.

Step 3 If the download fails, reset the active XTC:



Note Ensure that the active green LED is lit before removing card.

- a. Right-click the XTC.
- b. Select **Reset Card** from the drop-down menu.

Step 4 Attempt the download again by clicking the **Maintenance > Software** tabs.

Step 5 Click the **Download** button.

Step 6 If the download is successful, replace the standby XTC.

Step 7 If the download fails again, replace the active XTC.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 8 Attempt the download again by clicking the **Maintenance > Software** tabs.

Step 9 Click the **Download** button.

Step 10 If the download fails again, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).

14.4.110 SNTP-HOST

- Minor, Non-Service-Affecting

The SNTP (Simple Network Timing Protocol) host failure (SNTP-HOST) alarm indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. This failure can result from two causes: either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

Procedure: Clear the SNTP-HOST Alarm

-
- Step 1** Contact the network administrator that manages the IP network supplying the SNTP information to the proxy and determine if the network is experiencing problems which may affect the SNTP server/ router connecting to the proxy ONS 15327.
- Step 2** On the ONS node serving as the proxy, click the **CTC Provisioning > General** tabs.
- Step 3** Ensure that the **Enable Proxy** check box is checked.
- Step 4** If the **Enable Proxy** check box is not checked, check this box.
- Step 5** Refer to the ONS 15454 Reference Manual for more information on SNTP Host.
-

14.4.111 SQUELCH

- Not Alarmed, Non-Service-Affecting (Condition)

The ring is squelching traffic (SQUELCH) alarm occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance force ring commands. The isolation or failure of the node disables the circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The AIS-P alarm also appears on all nodes in the ring, except the isolated node.



Warning

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



Warning

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam 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.



Caution

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SQUELCH Condition

-
- Step 1** Determine the isolated node:
- Display the CTC network view.
 - The grayed out node with red spans is the isolated node.
- Step 2** Verify fiber continuity to the ports on the isolated node.
- Step 3** Verify that the proper ports are in service.
- Step 4** Use an optical test set to verify that a valid signal exists on the line.

Test the line as close to the receiving card as possible.

- Step 5** Verify that the power level of the optical signal is within the optical card receiver specifications. Each individual card section in Chapter 4 lists the receiver specifications for that card.
- Step 6** Ensure that the optical transmits and receives are connected properly.
- Step 7** Replace the OC-N card.
-

14.4.112 SSM-FAIL

- Minor, Non-Service-Affecting

The failed to receive synchronization status message (SSM-FAIL) alarm means the synchronization status messaging (SSM) received by the ONS 15327 failed. The problem is external to ONS 15327. The ONS 15327 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

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.

Procedure: Clear the SSM-FAIL Alarm

- Step 1** Check that SSM is enabled on the external timing source.
- Step 2** Use a test set to determine that the external timing source is delivering SSM.
-

14.4.113 STU

- Not Alarmed (NA) (Condition)

The synchronization traceability unknown (STU) alarm occurs when the reporting node is timed to a reference that does not support synchronization status messaging (SSM), but the ONS 15327 has SSM support enabled. STU can also be raised if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15327.

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. SSM enables SONET devices to automatically choose the highest quality timing reference and to avoid timing loops.

Procedure: Clear the STU Condition

- Step 1** Click the **Provisioning > Timing** tabs.
- Step 2** If **Sync Messaging** is checked, uncheck the box.
- Step 3** If **Sync Messaging** is unchecked, check the box.
- Step 4** Click **Apply**.
-

14.4.114 SWTOPRI

- Not Alarmed (NA) (Condition)

The synchronization switch to primary reference (SWTOPRI) condition occurs when the ONS 15327 switches to the primary timing source (reference 1). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

**Note**

This is a condition and not an alarm. It is for information only and does not require troubleshooting.

14.4.115 SWTOSEC

- Not Alarmed (NA) (Condition)

The synchronization switch to secondary reference (SWTOSEC) condition occurs when the ONS 15327 has switched to the secondary timing source (reference 2). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOSEC Condition

Find and troubleshoot alarms related to failures of the primary source, such as the SYNCPRI alarm.

14.4.116 SWTOTHIRD

- Not Alarmed (NA) (Condition)

The synchronization switch to third reference (SWTOTHIRD) condition occurs when the ONS 15327 has switched to the third timing source (reference 3). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOTHIRD Condition

Find and troubleshoot alarms related to failures of the primary and secondary reference source, such as the SYNCPRI and SYNCSEC alarms.

14.4.117 SYNCPRI

- Minor, Non-Service-Affecting

A loss of timing on primary reference (SYNCPRI) alarm occurs when the ONS 15327 loses the primary timing source (reference 1). The ONS 15327 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15327 should switch to its secondary timing source (reference 2). This switch also triggers the SWTOSEC alarm.

Procedure: Clear the SYNCPRI Condition on the XTC Card

-
- Step 1** From the node view, click the **Provisioning > Timing** tabs.
 - Step 2** Check the current configuration for the REF-1 of the NE Reference.
 - Step 3** If the primary reference is a BITS input, follow the procedure in the “LOS (BITS)” section on page 14-56.
 - Step 4** If the primary reference clock is an incoming port on the ONS 15327, follow the procedure in the “LOS (OC-N)” section on page 14-57.
-

14.4.118 SYNCSEC

- Minor, Non-Service-Affecting

A loss of timing on secondary reference (SYNCSEC) alarm occurs when the ONS 15327 loses the secondary timing source (reference 2). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15327 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15327. This switch also triggers the SYNCTHIRD alarm.

Procedure: Clear the SYNCSEC Alarm on the XTC Card

-
- Step 1** From the node view, click the **Provisioning > Timing** tabs.
 - Step 2** Check the current configuration of the REF-2 for the NE Reference.
 - Step 3** If the secondary reference is a BITS input, follow the procedure in the “LOS (BITS)” section on page 14-56.
 - Step 4** If the secondary timing source is an incoming port on the ONS 15327, follow the procedure in the “LOS (OC-N)” section on page 14-57.
-

14.4.119 SYNCTHIRD

- Minor, Non-Service-Affecting

A loss of timing on third reference (SYNCTHIRD) alarm occurs when the ONS 15327 loses the third timing source (reference 3). The ONS 15327 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCTHIRD occurs and the ONS 15327 uses an internal reference for source three, then the XTC card may have failed. The ONS 15327 often reports either FRNGSYNC or HLDOVERSYNC alarms after a SYNCTHIRD alarm.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the SYNCTHIRD Alarm on the XTC Card

-
- Step 1** From node view, click the **Provisioning > Timing** tabs.
- Step 2** Check the current configuration of the REF-3 for the NE reference.
- Step 3** If the third timing source is a BITS input, follow the procedure in the “LOS (BITS)” section on page 14-56.
- Step 4** If the third timing source is an incoming port on the ONS 15327, follow the procedure in the “LOS (OC-N)” section on page 14-57.
- Step 5** If the third timing source uses the internal ONS 15327 timing, perform a software reset on the XTC card:
- a. Display the CTC node view.
 - b. Position the cursor over the slot reporting the alarm.
 - c. Right-click and choose **RESET CARD**.
- Step 6** If this fails to clear the alarm, physically reseal the XTC card.
- Step 7** If the reset fails to clear the alarm, replace the XTC card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

14.4.120 SYSBOOT

- Major, Service-Affecting

The system reboot (SYSBOOT) alarm indicates that new software is booting on the XTC card. This is an informational alarm. No action is required. The alarm clears when all cards finish rebooting the new software.



Note The XTC reboot takes up to 30 minutes.

14.4.121 TIM-P

- Minor, Service-Affecting

The STS path trace identifier mismatch path (TIM-P) alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to manual or Auto for this alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the New Expected String field for the receiving port. This string must match the string typed into the New Transmit String field for the sending port. If these fields do not match, the TIM-P alarm occurs. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, this means the circuit path changed or someone typed and entered a new incorrect value into the New Transmit String field. Follow the procedure below to clear either instance.

This alarm also occurs on a port that has previously been operating without alarms if someone switches or removes the DS-3 cables or optical fibers that connect the ports. This TIM-P occurrence is usually accompanied by other alarms, such as LOS, UNEQ-P, or PLM-P. In this case, reattach or replace the original cables/fibers to clear the alarm.

Procedure: Clear the TIM-P Alarm

-
- Step 1** Login to the circuit source node and select the **Circuits** tab.
 - Step 2** Select the circuit reporting the alarm, then click **Edit**.
 - Step 3** At the bottom of the Edit Circuit window, check the **Show Detailed Map** box.
 - Step 4** On the detailed circuit map, right-click the source circuit port and select **Edit Path Trace** from the shortcut menu.
 - Step 5** On the detailed circuit map, right-click the drop/destination circuit port and select **Edit Path Trace** from the shortcut menu.
 - Step 6** Compare the New Transmit String and the New Expected String entries in the Path Trace Mode dialog box.
 - Step 7** If the strings differ, correct the Transmit or Expected strings and click **Apply**.
 - Step 8** Click **Close**.
-

14.4.122 TRMT

- Major, Service-Affecting

A facility-termination equipment transmit failure (TRMT) alarm occurs when there is a transmit failure on the XTC card because of an internal hardware failure. The card must be replaced.

Procedure: Clear the TRMT Alarm on the XTC-14 Card

-
- Step 1** Replace the XTC-14 card reporting the failure.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 2** Login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).
-

14.4.123 TRMT-MISS

- Major, Service-Affecting

A facility-termination equipment transmitter missing (TRMT-MISS) alarm occurs when the facility-termination equipment detects an incorrect amount of impedance on its backplane connector. This means transmit cable is missing on the XTC-14 port or the backplane does not match the inserted card; for example, an SMB connector or a BNC connector connects to an XTC-14 card instead of an XTC-28-3 card.

**Note**

DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

Procedure: Clear the TRMT-MISS Alarm

-
- Step 1** Check that the device attached to the XTC-14 port is operational.
 - Step 2** Verify that the cabling is securely connected.
 - Step 3** Verify that the pinouts are correct.
 - Step 4** If Steps 1 to 3 do not clear the alarm, replace the transmit cable.
-

14.4.124 UNEQ-P

- Critical, Service-Affecting

A signal label mismatch failure unequipped path ((UNEQ-P) alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

UNEQ-P occurs in the node that terminates a path. The path layer is the segment between the originating equipment and the terminating equipment. This segment can encompass several consecutive line segments. The originating equipment puts bits together into a SONET payload and the terminating equipment breaks the bits apart again. SONET multiplexers, such as the ONS 15327, often perform the origination and termination tasks of the SONET payload. A UNEQ-P error message on the ONS 15327 indicates that the node reporting the RFI-P is the terminating node on that path segment.

**Caution**

Deleting a circuit affects traffic.

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

**Note**

If you have created a new circuit but it has no signal, an UNEQ-P alarm is reported on the OC-N cards and an AIS-P alarm is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Procedure: Clear the UNEQ-P Alarm on the Line Card

-
- Step 1** Display the CTC network view and right-click the span reporting UNEQ-P.

- Step 2** Select **Circuits** from the menu.
- Step 3** If the specified circuit is a VT tunnel, check for VTs assigned to the VT tunnel.
- Step 4** If the VT tunnel has no assigned VTs, delete the VT tunnel from the list of circuits.
- Step 5** If you have complete visibility to all nodes, check for incomplete circuits such as stranded bandwidth from circuits that were not deleted completely.
- Step 6** If you find incomplete circuits, verify whether they are working circuits and if they are still passing traffic.
- Step 7** If the incomplete circuits are not needed or are not passing traffic, delete them and log out of CTC. Log back in and check for incomplete circuits again. Recreate any needed circuits.
- Step 8** Verify that all circuits terminating in the reporting card are active:
- Click the **Circuits** tab.
 - Verify that the State column lists the port as ACTIVE.
 - If the State column lists the port as INCOMPLETE. If INCOMPLETE does not change after a full initialization, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- Step 9** After you determine that the port is active, verify the signal source received by the card reporting the alarm.
- Step 10** Check the far-end OC-N card that provides STS payload to the card.
- Step 11** Verify the far-end cross-connect between the OC-N card and the DS-N card.
- Step 12** Clean the far-end optical fiber:
- Clean the fiber according to local site practice.
 - If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.

14.4.125 UNEQ-V

- Major, Service-Affecting

A signal label mismatch failure unequipped path (UNEQ-V) alarm indicates that the node is receiving SONET path overhead with bits 5, 6, and 7 of the V5 overhead byte all set to zeros. The source of the problem is the node that is transmitting the VT-level signal into the node reporting the UNEQ-P. The problem node is the next node upstream that processes the signal at the VT level.

The V in UNEQ-V indicates that the failure has occurred at the VT layer. The VT (electrical) layer is created when the SONET signal is broken down into an electrical signal, for example, when an optical signal comes into an ONS 15327, the optical signal is demultiplexed and one of the channels separated from the optical signal is cross connected into an ONS 15327 cross-connect (XC/XCVT/XC10G) card and the corresponding DS-N card.



Warning

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

**Caution**

Always use the supplied ESD wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located on the lower-right outside edge of the shelf assembly.

Procedure: Clear the UNEQ-V Alarm on the XTC-14 and XTC-28-3 Card

- Step 1** Verify that all circuits terminating in the reporting card are active:
- Click the **Circuits** tab.
 - Verify that the State column lists the port as ACTIVE.
 - If the State column lists the port as INCOMPLETE. If INCOMPLETE does not change after full initialization, login to <http://www.cisco.com/TAC> for more information or call the Cisco Technical Assistance Center to report a service-affecting problem (1-800-553-2447).
- Step 2** After you determine that the port is active, verify the signal source being received by the DS-N card reporting the alarm.
- Step 3** If traffic is being affected, delete and recreate the circuit.

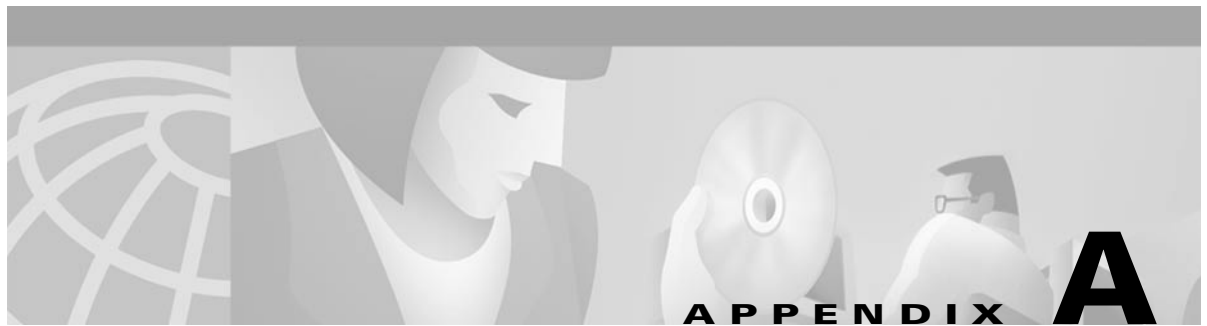
**Caution**

Deleting a circuit can be service-affecting.

- Step 4** Check the far-end OC-N card that provides STS payload to the XTC card.
- Step 5** Verify the cross-connect between the OC-N card and the XTC card.
- Step 6** Clean the far-end optical fiber:
- Clean the fiber according to local site practice.
 - If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product.
- Step 7** Replace OC-N/XTC cards.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.



Acronyms

A

ACO	Alarm Cutoff
ACT/STBY	Active/Standby
ADM	Add-Drop Multiplex
AIC	Alarm Interface Controller
AID	Access Identifier
AIS	Alarm Indication Signal
AIS-L	Line Alarm Indication Signal
AMI	Alternate Mark Inversion
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
ATAG	Autonomous Message Tag
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge

B

B8ZS	Bipolar 8 Zero Substitution
BER	Bit Error Rate
BIC	Backplane Interface Connector

BIP	Bit Interleaved Parity
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switched Ring
BML	Business Management Layer
BNC	Bayonet Neill-Concelman (coaxial cable bayonet locking connector)
BPDU	Bridge Protocol Data Unit
BTC	Bridging Transmission Convergence ASIC

C

CAT 5	Category 5 (cabling)
CCITT	Consultative Committee International Telegraph and Telephone (France)
CEO	Central Office Environment
CEV	Controlled Environment Vaults
CLEI	Common Language Equipment Identification
CLNP	Correctionless Network Protocol
CMIP	Common Management Information Protocol
CMS	Cerent Management System (now CTC)
cm	centimeter
COE	Central Office Environment
CORBA	Common Object Request Broker Architecture
CPE	Customer Premise Environments
CTAG	Correlation Tag
CTC	Cisco Transport Controller

D

DCC	Data Communications Channel
DCN	Data Communications Network
DCS	Distributed Communications System

DIN	Deutsche Institut fur Normung (German Institute for Standardization)
DRAM	Dynamic Random Access Memory
DS-1	Digital Signal Level One
DS-3	Digital Signal Level Three
DS1-14	Digital Signal Level One (14 ports)
DS1N-14	Digital Signal Level One (N-14 ports)
DS3-12	Digital Signal Level Three (12 ports)
DS3N-12	Digital Signal Level Three (N-12 ports)
DS3XM-6	Digital Service Level 3 Trans Multiplexer (6 ports)
DSX	Digital Signal Cross Connect frame
DWDM	Dense wavelength division multiplexing

E

EDFA	Erbium Doped Fiber Amplifier
EEE	Electronic Equipment Enclosures
EFI	Engineer furnish and install
EFT	Electrical Fast Transient/Burst
EIA	Electrical Interface Assemblies
ELR	Extended Long Reach
EMI	Electromagnetic interface
EML	Element Management Layer
EMS	Element Management System
EOW	Express Orderwire
ESD	Electrostatic Discharge
ESF	Extended Super Frame
ETSI	European Telecommunications Standards Institute

F

FCC	Federal Communications Commission
FCD	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FG1	Frame Ground #1(pins are labeled “FG1,” “FG2,” etc.)
FSB	Field Service Bulletin

G

Gbps	Gigabits per second
GB	Gigabyte
GBps	Gigabytes per second
GBIC	Gigabit Interface Converter
GHz	gigahertz
GR-253-CORE	General Requirements #253 Council Of Registrars
GR-1089	General Requirements #1089
GTL	Gunning Transistor Logic
GUI	Graphical User Interface

H

HDLC	High-Level Data Link Control
HTML	Hypertext Markup Language
HW Part #	Hardware Part Number

I

ID	Identifier
IF	Intermediate frequency
IEC	InterExchange Carrier

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
I/O	Input/Output
IP	Internet Protocol
IR	Intermediate reach
ITU-T	International Telephone Union- Telecommunication Standards Sector

J

JRE	Java Runtime Environment
------------	--------------------------

K

K	Kilo
Kb	Kilobit
kbps	kilobits per second
KB	kilobyte
kBps	kilobytes per second
kHz	kilohertz
km	kilometer

L

LAN	Local Area Network
LCD	Liquid Crystal Display
LDCC	Line Data Communications Channel
LOP	Loss of Pointer
LOS	Loss of Service
LOF	Loss of Frame
LOW	Local Orderwire

LTE	Line Terminating Equipment
LVDS	Low Voltage Differential Signal

M

MAC	Media Access Control
Mbps	Million bits per second, or Million bytes per second
Mhz	Megahertz
MIB	Management Information Bases
MIC	Mechanical Interface card
MIME	Multipurpose Internet Mail Extensions
Mux/Demux	Multiplexer/Demultiplexer

N

N	Any digit
NE	Network Element
NEL	Network Element Layer
NEBS	Network Equipment-Building Systems
NML	Network Management Layer
NMS	Network Management System

O

OAM&P	Operations, Administration, Maintenance, and Provisioning
OC	Optical Carrier
OC-3	Optical Carrier Level Three
OC-12	Optical Carrier Level 12
OC-48	Optical Carrier Level 48
OOS AS	Out of Service Assigned
OS	Operating System

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operations Support System
OSS/NMS	Operations Support System/Network Management System

P

P	Protection
PC	Personal Computer
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCN	Product Change Notices
PDI-P	STS Payload Defect Indication-Path
PMP	Point to Multipoint
POP	Point of Presence
PPMN	Path Protected Mesh Network
PSA	Product Specification Agreement

R

RAM	Random Access Memory
RDI-L	Remote Defect Indication Line
RES	Reserved
RJ45	Registered Jack #45 (8 pin)
RMA	Return Material Authorization
RMON	Remote Network Monitoring
RS232	Recommended Standard #232 (ANSI Electrical Interface for Serial Communication)
Rx	Receive

S

SCI	Serial Communication Interface
SCL	System Communications Link
SDBER	Signal Degrade Bit Error Rate
SDCC	Section Data Communications Channel
SDH/SONET	Synchronous Digital Hierarchy/Synchronous Optical Network
SELV	Safety Extra Low Voltage
SF	Super Frame
SFBER	Signal Failure Bit Error Rate
SML	Service Management Layer
SMF	Single-Mode Fiber
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SONET	Synchronous Optical Network
SPE	Synchronous Payload Envelope
SSM	Synchronous Status Messaging
STA	Spanning Tree Algorithm
STP	Shielded Twisted Pair
STS-1	Synchronous Transport Signal Level 1
SWS	SONET WAN Switch
SXC	SONET Cross Connect ASIC

T

TAC	Technical Assistance Center
TBOS	Telemetry Byte Oriented Serial protocol
TCC	Timing Communications and Control Card (Cisco ONS 15454)
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplex

TDS	Time Division Switching
TID	Target Identifier
TL1	Transaction Language 1
TLS	Transparent LAN service
TM	Terminal Mode
TMN	Telecommunications Management Network
TSA	Time Slot Assignment
TSI	Time-Slot Interchange
Tx	Transmit

U

UTC	Universal Time Coordinated
UDP/IP	User Datagram Protocol/Internet Protocol
UID	User Identifier
UL	Underwriter's Laboratories
UPSR	Unidirectional Path Switched Ring
UTP	Unshielded Twisted Pair

V

VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VT1.5	Virtual Tributary equals 1.544 megabits per second

W

WAN	Wide Area Network
W	Watts

X

XCON	Cross-Connect Card (pronounced “Ex-Con”)
XC	Cross Connect
XCVT	Cross Connect Virtual Tributary
XTC	Integrated Cross-Connect, Timing, and Control card
X.25	Protocol providing devices with direct connection to a packet switched network

Numerics

10BaseT	standard 10 megabit per second local area network over unshielded twisted pair copper wire
100BaseT	standard 100 megabit per second ethernet network
100BaseTX	specification of 100BaseT that supports full duplex operation



Regulatory Compliance and Safety Requirements for the *Cisco ONS 15327*

This document provides international regulatory compliance and safety information for the Cisco Optical Networking System (ONS) 15327. Use this document in conjunction with the *Cisco Optical Networking System 15327 User Documentation*.

Contents

- Japan and Korea Approvals, page B-1
- Regulatory Compliance, page B-4
- Class A Notice, page B-5
- Installation Warnings, page B-6
- Related Documentation, page B-16

Japan and Korea Approvals

Japan

Table B-1 Card Approvals

Card	Certificate Number
MIC-28-3-A/B	L01-0055
OC12 IR 1310	L01-0052
OC48 IR 1310	L01-0053

Label Requirements

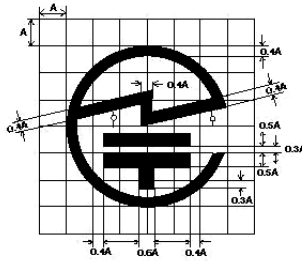
The following labels are applicable for use in Japan

Optical Card OC3 IR 4 1310.



Size: 30 x 10 mm
Base Color: Silver
Printing Color: Black
Adhesive: Parmanet Acrylic resin
Material: Chrome mylar
JATE Mark Diameter: 6mm
Placement: On the board
(Reverse side)

JATE Mark (A=1mm)



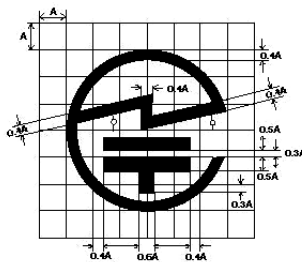
71766

Optical Card OC12 IR 1310.



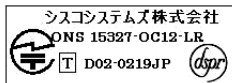
Size: 30 x 10 mm
Base Color: Silver
Printing Color: Black
Adhesive: Parmanet Acrylic resin
Material: Chrome mylar
JATE Mark Diameter: 6mm
Placement: On the board
(Reverse side)

JATE Mark (A=1mm)



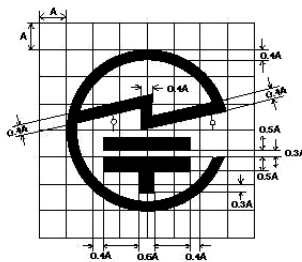
71768

Optical Card OC12 LR 1550



Size: 30 x 10 mm
Base Color: Silver
Printing Color: Black
Adhesive: Parmanet Acrylic resin
Material: Chrome mylar
JATE Mark Diameter: 6mm
Placement: On the board
(Reverse side)

JATE Mark (A=1mm)



71769

Optical Card OC48 IR 1310



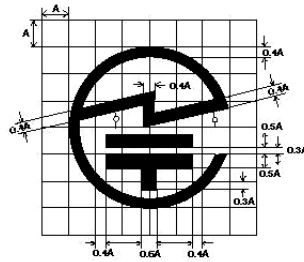
55356

Optical Card OC48 LR 1550



Size: 30 x 10 mm
 Base Color: Silver
 Printing Color: Black
 Adhesive: Parmanet Acrylic resin
 Material: Chrome mylar
 JATE Mark Diameter: 6mm
 Placement: On the board
 (Reverse side)

JATE Mark (A=1mm)



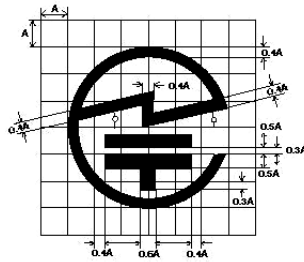
71770

Mechanical Interface Card (MIC) (DS1, DS3) MIC-28-3-A/B




Size: 30 x 10 mm
 Base Color: Silver
 Printing Color: Black
 Adhesive: Parmanet Acrylic resin
 Material: Chrome mylar
 JATE Mark Diameter: 6mm
 Placement: On the board
 (Reverse side)

JATE Mark (A=1mm)



71767

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。 VCCI-A

- 
1. 기기명(모델명): Cisco ONS 15327
 2. 인증번호: T-C99-01-0266
 3. 인증받은 자의 상호: Cisco Systems, Inc.
 4. 제조년월일:
 5. 제조자/제조국가: Cisco Systems, Inc / 미국

47-11054-01 Rev A0

55355

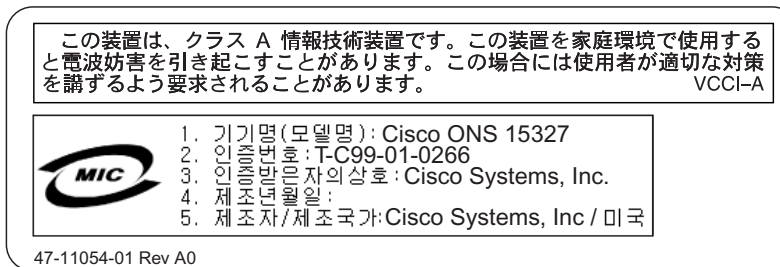
Korea

Table B-2 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/I00T-4	

Label Requirements

The following label is applicable for use in Korea.



Regulatory Compliance

Table B-3 Standards

Discipline	Country	Specification
EMC Emissions	Canada	ICES-003 Issue 3, 1997 Bellcore GR-1089-CORE
	USA	47CFR15 Bellcore GR-1089-CORE
	Japan	VCCI V-3/2000.04
	Korea	CISPR22

Table B-3 Standards

Discipline	Country	Specification
EMC Immunity	Canada	Bellcore GR-1089-CORE
	USA	Bellcore GR-1089-CORE
	Japan	Not applicable
	Korea	CISPR24
Safety	Canada	CAN/CSA-C22.2 No. 950-95, 3 rd Ed Bellcore GR-1089-CORE Bellcore GR-63-CORE
	USA	UL 1950, Third Edition Bellcore GR-1089-CORE Bellcore GR-63-CORE
	Japan	EN60950 (to A4)
	Korea	EN60950 (to A4)
	Telecom	Canada
	USA	Not applicable
	Japan	Blue Book 1996, Green Book 1997
	Korea	OC-12, OC-48
Environmental	Canada	Bellcore GR-63-CORE NEBS
	USA	Cisco Mechanical Environmental Design and Qualification Guideline ENG-3396
Structural Dynamics (Mechanical)	Canada	Bellcore 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 Equipment Requirements

Class A Notice



Warning

This is a Class A Information Product. When used in residential environment, it may cause radio frequency interference. Under such circumstances, the user may be requested to take appropriate countermeasures.

警告使用者

這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

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、インストラクションについての説明書を必ずお読みください。

DC Power Disconnection Warning



Warning

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

Waarschuwing

Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.

Varoitus

Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.

Attention

Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifiez que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.

Warnung

Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.

Avvertenza

Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata (OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.

Advarsel

Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.

Aviso

Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.

- ¡Advertencia!** Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).
- Varning!** Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.

DC Power Connection Warning



Warning

After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.

- Waarschuwing** Nadat de bedrading van de gelijkstroom voeding aangebracht is, verwijder 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).
- Warning!** När du har kopplat ledningarna till strömförsörjningsenheten för inmatad likström tar du bort tejpén från överspänningsskyddets omkopplare och slår på strömmen igen genom att ställa överspänningsskyddets omkopplare i TILL-läget.

Power Supply Disconnection Warning



Warning

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

- Waarschuwing** Voordat u aan een frame of in de nabijheid van voedingen werkt, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen; voor gelijkstroom toestellen dient u de stroom uit te schakelen bij de stroomverbreker.
- Varoitus** Kytke irti vaihtovirtalaitteiden virtajohto ja katkaise tasavirtalaitteiden virta suojakytkimellä, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.
- Attention** Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif ; couper l'alimentation des unités en courant continu au niveau du disjoncteur.
- Warnung** Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw. schalten Sie bei Gleichstromeinheiten den Strom am Unterbrecher ab.
- Avvertenza** Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all'interruttore automatico sulle unità CC.
- Advarsel** Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut på vekselstrømsenheter og strømmen kobles fra ved strømbryteren på likestrømsenheter.
- Aviso** Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada; desligue a corrente no disjuntor nas unidades de corrente contínua.
- ¡Advertencia!** Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA); cortar la alimentación desde el interruptor automático en los equipos de corriente continua (CC).
- Warning!** 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。

Circuit Breaker (30A) Warning



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 30A U.S. (240 VAC, 20A international) is used on the phase conductors (all current-carrying conductors).

Waarschuwing

Dit produkt is afhankelijk van de installatie van het gebouw voor kortsluit-(overstroom)beveiliging. Controleer of er een zekering of stroomverbreker van niet meer dan 120 Volt wisselstroom, 30 A voor de V.S. (240 Volt wisselstroom, 20 A internationaal) gebruikt wordt op de fasegeleiders (alle geleiders die stroom voeren).

Varoitus

Tämä tuote on riippuvainen rakennukseen asennetusta oikosulkusuojauksesta (ylivirtasuojauksesta). Varmista, että vaihevirtajohtimissa (kaikissa virroitetuissa johtimissa) käytetään Yhdysvalloissa alle 120 voltin, 30 ampeerin ja monissa muissa maissa 240 voltin, 20 ampeerin sulaketta tai suojakytkintä.

Attention

Pour ce qui est de la protection contre les courts-circuits (surtension), ce produit dépend de l'installation électrique du local. Vérifier qu'un fusible ou qu'un disjoncteur de 120 V alt., 30 A U.S. maximum (240 V alt., 20 A international) est utilisé sur les conducteurs de phase (conducteurs de charge).

Warnung

Dieses Produkt ist darauf angewiesen, daß im Gebäude ein Kurzschluß- bzw. Überstromschutz installiert ist. Stellen Sie sicher, daß eine Sicherung oder ein Unterbrecher von nicht mehr als 240 V Wechselstrom, 20 A (bzw. in den USA 120 V Wechselstrom, 30 A) an den Phasenleitern (allen stromführenden Leitern) verwendet wird.

Avvertenza

Questo prodotto dipende dall'installazione dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Verificare che un fusibile o interruttore automatico, non superiore a 120 VCA, 30 A U.S. (240 VCA, 20 A internazionale) sia stato usato nei fili di fase (tutti i conduttori portatori di corrente).

Advarsel

Dette produktet er avhengig av bygningens installasjoner av kortslutningsbeskyttelse (overstrøm). Kontroller at det brukes en sikring eller strømbryter som ikke er større enn 120 VAC, 30 A (USA) (240 VAC, 20 A internasjonalt) på faselederne (alle strømførende ledere).

Aviso

Este produto depende das instalações existentes de protecção contra curto-circuito (sobrecarga). Assegure-se de que um fusível ou disjuntor não superior a 240 VAC, 20A é utilizado nos condutores de fase (todos os condutores de transporte de corrente).

- ¡Advertencia!** Este equipo utiliza el sistema de protección contra cortocircuitos (o sobrecorrientes) del propio edificio. Asegurarse de que se utiliza un fusible o interruptor automático de no más de 240 voltios en corriente alterna (VAC), 20 amperios del estándar internacional (120 VAC, 30 amperios del estándar USA) en los hilos de fase (todos aquéllos portadores de corriente).
- Varning!** Denna produkt är beroende av i byggnaden installerat kortslutningsskydd (överströmsskydd). Kontrollera att säkring eller överspänningsskydd används på fasledarna (samtliga strömförande ledare) för internationellt bruk max. 240 V växelström, 20 A (i USA max. 120 V växelström, 30 A).

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.

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 possui uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.

- ¡Advertencia!** Esta unidad ha sido diseñada para instalarse en áreas de acceso restringido. Área de acceso restringido significa un área a la que solamente tiene acceso el personal de servicio mediante la utilización de una herramienta especial, cerradura con llave, o algún otro medio de seguridad, y que está bajo el control de la autoridad responsable del local.
- Varning!** Denna enhet är avsedd för installation i områden med begränsat tillträde. Ett område med begränsat tillträde får endast tillträdas av servicepersonal med ett speciellt verktyg, lås och nyckel, eller annan säkerhetsanordning, och kontrolleras av den auktoritet som ansvarar för området.

Ground Connection Warning



Warning

When installing the unit, always make the ground connection first and disconnect it last.

- Waarschuwing** Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.
- Varoitus** Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.
- Attention** Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.
- Warnung** Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.
- Avvertenza** In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.
- Advarsel** Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.
- Aviso** Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.
- ¡Advertencia!** Al instalar el equipo, conectar la tierra la primera y desconectarla la última.
- Varning!** Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.

Qualified Personnel Warning



Warning

Only trained and qualified personnel should be allowed to install or replace this equipment.

Waarschuwing	Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.
Varoitus	Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.
Avertissement	Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.
Achtung	Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.
Avvertenza	Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.
Advarsel	Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.
Aviso	Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.
¡Atención!	Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.
Varning	Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.

Invisible Laser Radiation Warning (other versions available)



Warning

Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

Waarschuwing	Omdat er onzichtbare laserstraling uit de opening van de poort geëmitteerd kan worden wanneer er geen kabel aangesloten is, dient men om blootstelling aan laserstraling te vermijden niet in de open openingen te kijken.
Varoitus	Kun porttiin ei ole kytketty kaapelia, portin aukosta voi vuotaa näkymätöntä lasersäteilyä. Älä katso avoimiin aukkoihin, jotta et altistu säteilylle.
Attention	Etant donné qu'un rayonnement laser invisible peut être émis par l'ouverture du port quand aucun câble n'est connecté, ne pas regarder dans les ouvertures béantes afin d'éviter tout risque d'exposition au rayonnement laser.

Warnung	Aus der Öffnung des Ports kann unsichtbare Laserstrahlung austreten, wenn kein Kabel angeschlossen ist. Kontakt mit Laserstrahlung vermeiden und nicht in offene Öffnungen blicken.
Avvertenza	Poiché quando nessun cavo è collegato alla porta, da quest'ultima potrebbe essere emessa radiazione laser invisibile, evitare l'esposizione a tale radiazione e non fissare con gli occhi porte a cui non siano collegati cavi.
Advarsel	Usynlige laserstråler kan sendes ut fra åpningen på utgangen når ingen kabel er tilkoblet. Unngå utsettelse for laserstråling og se ikke inn i åpninger som ikke er tildekket.
Aviso	Evite uma exposição à radiação laser e não olhe através de aberturas expostas, porque poderá ocorrer emissão de radiação laser invisível a partir da abertura da porta, quando não estiver qualquer cabo conectado.
¡Advertencia!	Quando 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.
Warning!	Osynliga laserstrålar kan sändas ut från öppningen i porten när ingen kabel är ansluten. Undvik exponering för laserstrålning och titta inte in i ej täckta öppningar.

More Than One Power Supply



Warning

This unit has more than one power supply connection; all connections must be removed completely to completely remove power from the unit.

Waarschuwing	Deze eenheid heeft meer dan één stroomtoevoerverbinding; alle verbindingen moeten volledig worden verwijderd om de stroom van deze eenheid volledig te verwijderen.
Varoitus	Tässä laitteessa on useampia virtalähdekytkentöjä. Kaikki kytkennät on irrotettava kokonaan, jotta virta poistettaisiin täysin laitteesta.
Attention	Cette unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.
Warnung	Diese Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.
Avvertenza	Questa unità ha più di una connessione per alimentatore elettrico; tutte le connessioni devono essere completamente rimosse per togliere l'elettricità dall'unità.
Advarsel	Denne enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.

- Aviso** Este dispositivo possui mais do que uma conexão de fonte de alimentação de energia; para poder remover a fonte de alimentação de energia, deverão ser desconectadas todas as conexões existentes.
- ¡Advertencia!** Esta unidad tiene más de una conexión de suministros de alimentación; para eliminar la alimentación por completo, deben desconectarse completamente todas las conexiones.
- Varning!** Denna enhet har mer än en strömförsörjningsanslutning; alla anslutningar måste vara helt avlägsnade innan strömtillförseln till enheten är fullständigt bruten.

Related Documentation

- Cisco ONS 15327 User Documentation, DOC-7811719=
- Cisco ONS 15327 Product Overview, DOC-7811788=

Release-Specific Documents

- Release 1.0 ONS 15327 Release Notes

Obtaining Documentation

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

World Wide Web

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

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

Optical Networking Group CD-ROM

Optical networking-related documentation, including the *Cisco ONS 15327 Release Notes*, is available in a CD-ROM package that ships with your product. The Optical Networking Product CD-ROM, a member of the Cisco Connection Family, is updated as required. Therefore, it might be more current than printed documentation. To order additional copies of the Optical Networking Product CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www.europe.cisco.com>.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation, including the Optical Networking Products CD-ROM, from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

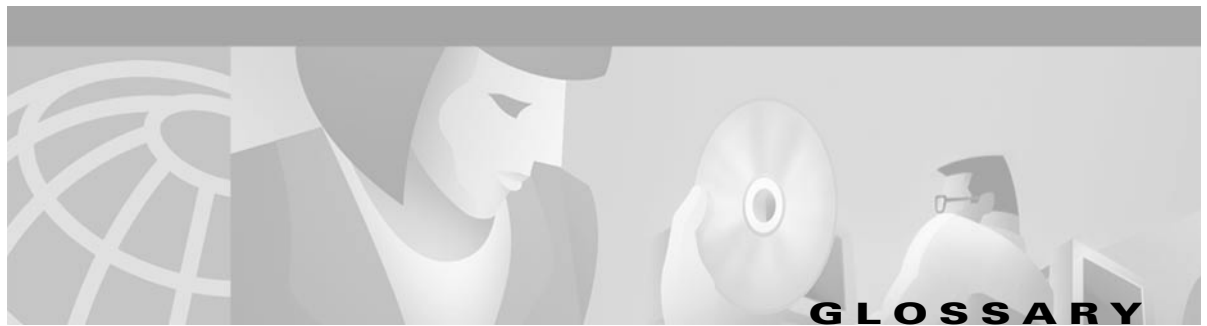
This document is to be used in conjunction with the Cisco ONS 15327 User Documentation.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, CiscoLink, the Cisco NetWorks logo, Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQ Logo, iQ Readiness Scorecard, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, WebViewer, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press,

Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0010R)

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.



Numerics

1:1 protection

A card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot. If the working card fails, the traffic from the working card switches to the protect card. When the failure on the working card is resolved, traffic reverts back to the working card if this option is set. This protection scheme is specific to electrical cards.

1:N protection

An electrical-card protection scheme that allows a single card to protect several working cards. When the failure on the working card is resolved, traffic reverts back to the working card.

1+1 protection

An optical-card protection scheme that pairs a single working card with a single dedicated protect card.

A

Access drop

Points where network devices can access the network.

Address mask

Bit combination used to describe the portion of an IP address that refers to the network or subnet and the part that refers to the host. Sometimes referred to as mask. See also *subnet mask*.

ADM

Add/drop multiplexer. ADM allows a signal to be added into or dropped from a SONET span.

Agent

1. Generally, software that processes queries and returns replies on behalf of an application.
2. In a network management system, a process that resides in all managed devices and reports the values of specified variables to management stations.

AID

Access Identifier. An access code used in TL1 messaging that identifies and addresses specific objects within ONS nodes. These objects include individual pieces of equipment, transport spans, access tributaries, and others.

AMI

Alternate Mark Inversion. Line-code format used on T1 circuits that transmits Ones by alternate positive and negative pulses. Zeroes are represented by 01 during each bit cell and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary-coded alternate mark inversion.

APS

Automatic Protection Switching. SONET switching mechanism that routes traffic from working lines to protect lines if a line card failure or fiber cut occurs.

ATAG

Autonomous Message Tag. ATAG is used for TL1 message sequencing.

ATM

Asynchronous Transfer Mode. International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.

B**B8ZS**

Binary 8-zero Substitution. A line-code type, used on T1 circuits, that substitutes a special code whenever 8 consecutive zeros are sent over the link. This code is then interpreted at the remote end of the connection. This technique guarantees Ones density independent of the data stream. Sometimes called bipolar 8-zero substitution.

Backbone

Part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.

Bandwidth reuse

A synchronous transfer signal that carries different sets of traffic on different spans at the same time.

BER

Bit Error Rate. Ratio of received bits that contain errors.

BLSR

Bidirectional Line Switched Ring. SONET ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically routed onto the protection fiber.

Bit rate

Speed at which bits are transmitted, usually expressed in bits per second.

BITS

Building Integrated Timing Supply. A single building master timing supply that minimizes the number of synchronization links entering an office. Sometimes referred to as a Synchronization Supply Unit.

Blue band

Dense wavelength division multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

Bridge

Device that connects and passes packets between two network segments that use the same communications protocol. In general, a bridge will filter, forward, or flood an incoming frame based on the MAC address of that frame.

Broadcast

Data packet that is sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*. See also *Broadcast address*.

Broadcast address

Special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones.

Broadcast storm

Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

Bus

Common physical signal path composed of wires or other media across which signals can be sent from one part of a computer to another.

C**C2 byte**

The C2 byte is the signal label byte in the STS path overhead. This byte tells the equipment what the SONET payload envelope contains and how it is constructed.

Cell

Basic Unit of ATM switching and multiplexing. Cells contain identifiers that specify the data stream where they belong.

CEV

Controlled environment vault. An underground room that houses electronic and/or optical equipment in controlled temperature and humidity.

Collision

In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.

Concatenation

A mechanism for allocating contiguous bandwidth for payload transport. Through the use of concatenation pointers, multiple OC-1s can be linked together to provide contiguous bandwidth through the network, from end to end.

Crosspoint

A set of physical or logical contacts that operate together to extend the speech and signal channels in a switching network.

CTAG

Correlation tag. A unique identifier given to each input command by the TL1 operator. When an ONS 15327 or ONS 15454 system responds to a specific command, it includes the command's CTAG in the reply. This eliminates discrepancies about which response corresponds to which command.

CMS

The previous name of the Cisco Transport Controller (CTC).

CTC

Cisco Transport Controller. A Java-based program that allows a user to provision and manage ONS 15327s and ONS 15454s using an Internet browser.

CTM

Cisco Transport Manager. A Java-based network management tool used to support large networks of Cisco 15000-class equipment.

D**DCC**

Data communications channel. Used to transport information about operation, administration, maintenance, and provisioning (OAM&P) over a SONET interface. DCCs can be located in section DCC (SDCC) or line overhead (LDCC).

Demultiplex

Separates multiple multiplexed input streams from a common physical signal back into multiple output streams. See also *Multiplexing*.

DSX

Digital signal cross-connect frame. A manual bay or panel where different electrical signals are wired. A DSX permits cross-connections by patch cords and plugs.

DWDM

Dense Wave Division Multiplexing. A technology that increases the information carrying capacity of existing fiber optic infrastructure by transmitting and receiving data on different light wavelengths. Many of these wavelengths can be combined on a single strand of fiber.

E**EDFA**

Erbium Doped Fiber Amplifier. A form of fiber optical amplification that transmits a light signal through a section of erbium-doped fiber and amplifies the signal with a laser pump diode. EDFA is used in transmitter booster amplifiers, in-line repeating amplifiers, and in receiver preamplifiers.

EMI

Electromagnetic Interference. Interference by electromagnetic signals can reduce data integrity and increase error rates on transmission channels.

Encapsulation

The wrapping of data in a particular protocol header.

Envelope

The part of messaging that varies in composition from one transmittal step to another. It identifies the message originator and potential recipients, documents its past, directs its subsequent movement by the message transfer system (MTS), and characterizes its content.

EOW

Express Orderwire. A permanently-connected voice circuit between selected stations for technical control purposes.

Ethernet switch

An Ethernet data switch. Ethernet switches increase the aggregate LAN bandwidth by allowing simultaneous switching of packets between switch ports. Ethernet switches subdivide previously-shared LAN segments into multiple networks with fewer stations per network.

External timing reference

A timing reference obtained from a source external to the communications system, such as one of the navigation systems. Many external timing references are referenced to Coordinated Universal Time (UTC).

F**Falling threshold**

A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, this triggers an event to reset the rising threshold. See also *rising threshold*.

FDDI

Fiber Distributed Data Interface. LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber-optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

Frame

Logical grouping of information sent as a data-link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control that surrounds the user data contained in the unit.

Free run synchronization mode

Occurs when the external timing sources have been disabled and the ONS node is receiving timing from its Stratum 3 level internal timing source.

G**GBIC**

Gigabit Interface Converter. A hot-swappable input/output device that plugs into a Gigabit Ethernet port to link the port with the fiber optic network.

H**Hard reset**

The physical removal and insertion of a card.

HDLC

High Level Data Link Control. Bit-oriented, synchronous, data-link layer protocol developed by ISO. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

Host number

Part of IP address used to address an individual host within the network or subnetwork.

Hot swap

The process of replacing a failed component while the rest of the system continues to function normally.

Hub

1. Hardware or software device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat, but merely split, signals sent through them).

2. In Ethernet and IEEE 802.3, an Ethernet multiport repeater, sometimes called a concentrator.

I**Input alarms**

Used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions.

Interface

1. Connection between two systems or devices.

2. In routing terminology, a network connection.

IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IP address

32-bit address assigned to host using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number.

J**Java**

Object-oriented programming language developed at Sun Microsystems to solve a number of problems in modern programming practice. The Java language is used extensively on the World Wide Web, particularly for applets.

K**K bytes**

Automatic protection switching bytes. K bytes are located in the SONET line overhead and monitored by equipment for an indication to switch to protection.

L**LAN**

Local Area Network. High-speed, low error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. Ethernet, FDDI, and Token Ring are widely used LAN technologies.

LCD

Liquid Crystal Display. An alphanumeric display using liquid crystal sealed between two pieces of glass. LCDs conserve electricity.

Learning bridge

Bridge that performs MAC address learning to reduce traffic on the network. Learning bridges manage a database of MAC addresses and the interfaces associated with each address. See also *MAC address learning*.

Line layer

Refers to the segment between two SONET devices in the circuit. The line layer deals with SONET payload transport, and its functions include multiplexing and synchronization. Sometimes called a maintenance span.

Line timing mode

A node that derives its clock from the SONET lines.

Link budget

The difference between the output power and receiver power of an optical signal expressed in dB. Link refers to an optical connection and all of its component parts (optical transmitters, repeaters, receivers, and cables).

Link integrity

The network communications channel is intact.

Loopback test

Test that sends signals then directs them back toward their source from some point along the communications path. Loopback tests are often used to test network interface usability.

LOW

Local Orderwire. A communications circuit between a technical control center and selected terminal or repeater locations.

M**MAC address**

Standardized data-link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as the hardware address, MAC-layer address, and physical address.

MAC address learning

Service that stores the source MAC address of each received packet so that future packets destined for that address can be forwarded only to the bridge interface where that address is located. This scheme helps to minimize traffic on the attached LANs. See also *learning bridge* and *MAC address*.

Maintenance user

A security level that limits user access to maintenance options only. See also *Superuser*, *Provisioning User*, and *Retrieve User*.

Managed device

A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers.

Managed object

In network management, a network device that can be managed by a network management protocol. Sometimes called an MIB object.

Mapping

A logical association between one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.

MIB

Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Multicast

Single packets copied by the network and sent to a specific subset of network addresses.

Multiplex payload

Generates section and line overhead, and converts electrical/optical signals when the electrical/optical card is transmitting.

Multiplexing

Scheme that allows multiple logical signals to be transmitted simultaneously across a single physical channel. Compare with *Demultiplex*.

N**NE**

Network Element. In an Operations Support System (OSS), a single piece of telecommunications equipment used to perform a function or service integral to the underlying network.

Network management

Generic term used to describe systems or actions that help maintain, characterize, or troubleshoot a network.

Network number

Part of an IP address that specifies the network where the host belongs.

NMS

Network Management System. System that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.

Node

Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes, which vary in routing and other functional capabilities, can be interconnected by links, and serve as control points in the network. Node is sometimes used generically to refer to any entity that can access a network. In this manual the term “node” usually refers to an ONS 15327.

O**OAM&P**

Operations, Administration, Maintenance, and Provisioning. Provides the facilities and personnel required to manage a network.

OC

Optical Carrier. Series of physical protocols (OC-1, OC-2, OC-3, and so forth), defined for SONET optical signal transmissions. OC signal levels put Synchronous Transport Signal (STS) frames onto fiber-optic lines at a variety of speeds.

Optical amplifier

A device that amplifies an optical signal without converting the signal from optical to electrical and back again to optical energy.

Optical receiver

An opto-electric circuit that detects incoming lightwave signals and converts them to the appropriate signal for processing by the receiving device.

Orderwire

Equipment that establishes voice contact between a central office and carrier repeater locations.

Output contacts

Used to drive visual or audible devices such as bells and lights. Output contacts can control other devices such as generators, heaters, and fans.

P**Packet**

Logical grouping of information that includes a header containing control information and (usually) user data. Packets are most often used to refer to network-layer units of data. The terms datagram, frame, message, and segment are also used to describe logical information groupings.

Passive devices

Components that do not require external power to manipulate or react to electronic output. Passive devices include capacitors, resistors, and coils.

Path Layer

The segment between the originating equipment and the terminating equipment. This path segment can encompass several consecutive line segments or segments between two SONET devices.

Payload

Portion of a cell, frame, or packet that contains upper-layer information (data).

PCM

Pulse Code Modulation. Transmission of analog information in digital form through sampling and encoding with a fixed number of bits.

Ping

Packet internet grouper. ICMP echo message and its reply. Often used in IP networks to test the connection to a network device.

PPMN

Path-protected mesh network. PPMN extends the protection scheme of a unidirectional path switched ring (UPSR) beyond the basic ring configuration to the meshed architecture of several interconnecting rings.

Priority queuing

Routing feature that divides data packets into two queues: one low-priority and one high-priority.

Provisioning user

A CTC security level that allows the user to perform provisioning and maintenance options only. See also *Superuser*, *Maintenance user*, and *Retrieve user*.

Q**Queue**

In routing, a backlog of packets waiting to be forwarded over a router interface.

R**Retrieve user**

A CTC security level that allows the user to retrieve and view information but not set or modify parameters. See also *Superuser*, *Maintenance user*, and *Provisioning user*.

Revertive switching

A process that sends electrical interfaces back to the original working card after the card comes back online.

Rising threshold

The number of occurrences (collisions) that must be exceeded to trigger an event.

RMON

Remote Network Monitoring. Allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

Router

Network layer device that uses one or more metrics to determine the optimal path that network traffic should use. Routers forward packets from one network to another based on network-layer information.

S**Self-healing**

The ability of SONET rings to provide automatic network backup with 100% redundancy so if a point of failure occurs on the fiber ring, the service continues.

Signal degrade

Errors in the SONET signal exceed the threshold for normal operations but are less than the threshold for signal failure.

Signal failure

Errors in the SONET signal exceed the threshold defined for failure.

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP monitors and controls network devices and manages configurations, statistics collection, performance, and security.

SNTP

Simple Network Time Protocol. Using an SNTP server ensures that all ONS network nodes use the same date and time reference. The server synchronizes alarm timing during power outages or software upgrades.

Soft reset

A soft reset reloads the operating system, application software, etc., and reboots the card. It does not initialize the ONS 15327 ASIC hardware.

SONET

Synchronous Optical Network. High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

Spanning tree

Loop-free subset of a network topology. See also *STA* and *STP*.

SPE

Synchronous Payload Envelope. A SONET term describing the envelope that carries the user data or payload.

SSM

Synchronous Status Messaging. A SONET protocol that communicates information about the quality of the timing source using the S1 byte of the line overhead.

STA

Spanning-Tree Algorithm. An algorithm used by the spanning tree protocol to create a spanning tree. See also *Spanning tree* and *STP*.

Standing alarms

Alarms that are currently active.

Static route

A route that is manually entered into a routing table. Static routes take precedence over routes chosen by all dynamic routing protocols.

STP

Spanning Tree Protocol. Bridge protocol that creates a spanning tree to enable a learning bridge to work dynamically around loops in a network topology. See also *Spanning tree*, *STA*, and *Learning bridge*.

STS-1

Synchronous Transport Signal 1. Basic building block signal of SONET, operating at 51.84 Mbps for transmission over OC-1 fiber. Faster SONET rates are defined as STS-*n*, where *n* is a multiple of 51.84 Mbps. See also *SONET*.

Subnet mask

32-bit address mask used in IP to indicate the bits of an IP address that are used for the subnet address. Sometimes referred to simply as mask. See also *IP address mask* and *IP address*.

Subnetting

A technique used to maximize the number of networks available within a range (class) of addresses. See also *Subnetwork*.

Subnetwork

In IP networks, a network confined to a particular subnet address. Subnetworks are networks segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. Sometimes called a subnet.

Subtending rings

SONET rings that incorporate nodes that are also part of an adjacent SONET ring.

Superuser

A security level that can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. A superuser is usually the network element administrator. See also *Retrieve user*, *Maintenance user*, and *Provisioning user*.

Switch

Network device that filters, forwards, and floods frames based on the destination address of each frame.

T**T1**

T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network using AMI or B8ZS coding. See also *AMI*, *B8ZS*, and *DS-1*.

Tag

Identification information, including a number plus other information.

TDM

Time Division Multiplexing. Allocates bandwidth on a single wire for information from multiple channels based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

Telcordia

Telcordia Technologies, Inc., formerly named Bellcore. Eighty percent of the U.S. telecommunications network depends on software invented, developed, implemented, or maintained by Telcordia.

TID

Target Identifier. Identifies the particular network element (in this case, the ONS 15327) where each TL1 command is directed. The TID is a unique name given to each system at installation.

TLS

Transparent LAN Service. Provides private network service across a SONET backbone.

Trap

Message sent by an SNMP agent to an NMS (CTM), console, or terminal to indicate the occurrence of a significant event, such as an exceeded threshold.

Tributary

The lower-rate signal directed into a multiplexer for combination (multiplexing) with other low-rate signals to form an aggregate higher rate level.

Trunk

Network traffic travels across this physical and logical connection between two switches. A backbone is composed of a number of trunks. See also *Backbone*.

Tunneling

Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. See also *encapsulation*.

U**Unicast**

The communication of a single source to a single destination.

Unprotected card

Cards that are not included in a protection scheme. An unprotected card failure or a signal error results in lost data.

UPSR

Unidirectional Path Switched Ring. Path-switched SONET rings that employ redundant, fiber-optic transmission facilities in a pair configuration. One fiber transmits in one direction and the backup fiber transmits in the other. If the primary ring fails, the backup takes over.

Upstream

Set of frequencies used to send data from a subscriber to the headend.

UTC

Coordinated Universal Time. Time zone at zero degrees longitude.

V**Virtual fiber**

Converts each fiber into multiple fibers to allow signals that are carried at different rates use the same fiber-optic cable.

Virtual ring

Entity in a source-route bridging (SRB) network that logically connects two or more physical rings together either locally or remotely. The concept of virtual rings can be expanded across router boundaries.

Virtual wires

Virtual wires route external alarms to one or more alarm collection centers across the SONET transport network.

VLAN

Virtual LAN. Group of devices located on a number of different LAN segments that are configured (using management software) to communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPN

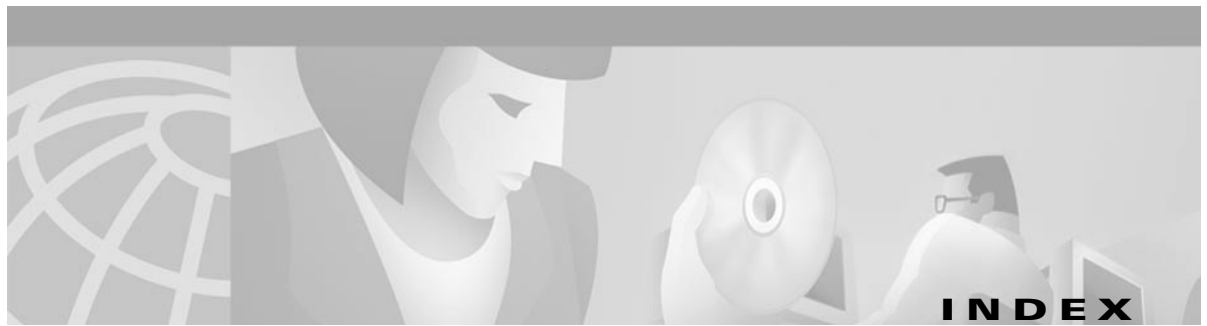
Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level. (See also *Tunneling*.)

VT

Virtual Tributary. A structure designed for the transport and switching of sub-DS3 payloads.

VT layer

The VT layer or electrical layer occurs when the SONET signal is broken down into an electrical signal.



Numerics

- 1+1 optical card protection
 - description **3-8**
 - creating linear ADMs **5-34**
- 1:1 electrical card protection
 - description **3-8**

A

- ACO *see* XTC cards
- add-drop multiplexer *see* linear ADM
- add node
 - BLSR **5-11**
 - current session **2-36**
 - groups (domain) **2-33**
 - UPSR **5-27**
- ADM *see* linear ADM
- air filter
 - description **1-7**
 - inspection and replacement **12-2**
 - replacing **1-7**
- AIS **3-14**
- AIS (alarm) **14-9**
- AIS-L (alarm) **14-9**
- AIS-P (alarm) **14-10**
- AIS-V (alarm) **14-10**
- alarm cutoff *see* alarms
- alarm indication signal **14-9**
- alarm indication signal *see* AIS
- alarm profiles
 - description **10-7**
 - comparing **10-8**
 - creating **10-7**
 - list by node **10-8**
 - loading **10-8**
 - saving **10-8**
- alarms
 - alarm cutoff on XTC **1-14**
 - cable installation **1-26**
 - changing default severities *see* alarm profiles
 - creating profiles *see* alarm profiles
 - deleting **10-3**
 - history **10-4, 10-6**
 - interface specifications **1-29**
 - LEDs **13-4**
 - severities **10-2, 10-6**
 - suppressing **10-11**
 - synchronize **10-3**
 - TL1 **14-1**
 - TL1 and CTC differences **14-1**
 - traps *see* SNMP
 - user-provisionable
 - cable installation **1-26**
 - external alarm input **7-17**
 - external controls **7-19**
 - physical description **13-10**
 - virtual wires **7-17**
 - viewing **10-1**
- alarm settings
 - Ethernet RMON thresholds **9-33**
 - XTC DS-1 card **7-8**
 - XTC DS-3 card **7-10**
 - XTC DS-N cards, general **7-3**
- APS **13-3**
- APSB (alarm) **14-11**

APSCDFLTK (alarm) **14-11**
 APSCIMP (alarm) **14-12**
 APSCINCON (alarm) **14-13**
 APSCM (alarm) **14-14**
 APSCNMIS (alarm) **14-14**
 APSMM (alarm) **14-15**
 APS *see* protection switching
 area range table (OSPF) **4-31**
 automated circuit creation **6-3, 6-6**
 automatic protection switching *see* protection switching
 automatic reset **14-16**
 AUTORESET (alarm) **14-16**
 AUTOSW-AIS (alarm) **14-16**
 AUTOSW-LOP (alarm) **14-16, 14-17**
 AUTOSW-PDI (alarm) **14-17**
 AUTOSW-SDBER (alarm) **14-17**
 AUTOSW-SFBER (alarm) **14-17**
 AUTOSW-UNEQ (alarm) **14-17**

B

bandwidth

circuit percentage used **9-31**
 line percentage used **9-30**
 two-fiber BLSR capacity **5-4**

bidirectional line switched ring *see* BLSR

bidirectional switching *see* switching

bipolar violations

DS1 CV-L **8-17**
 DS3 CV-L **8-23**

BITS

and BLSR setup **5-16**
 and pin assignments **1-27**
 and timing installation **1-14**
 BITS out references **3-14**
 cable installation **1-27**
 external node timing source **3-11**
 external timing pin assignments **1-14**
 facilities **3-14, 3-16**

loss of frame **14-49**

specifications **1-29**

BKUPMEMP (alarm) **14-18**

BLSR

adding a node **5-12**

alarms **5-10**

bandwidth capacity **5-4**

choosing properties **5-9**

DCC terminations **5-8**

deleting circuits **5-19**

enabling ports **5-8**

far-end protection line failure **14-44**

fiber configuration example **5-7**

improper configuration (alarms) **14-11**

increasing the traffic speed **12-12**

lockout protection span alarm **14-43**

manual speed upgrade **12-15**

maximum node number **5-1**

moving trunk cards **5-16**

planning fiber connections **5-7**

provisioning **5-9**

PSC **8-31, 8-36**

removing a node **5-15**

ring switch failure **14-38**

set up procedures **5-7**

squelch alarm **14-78**

subtending a BLSR **5-32**

subtending a UPSR **5-30**

testing **5-11**

timing **5-9**

two-fiber description **5-2**

two-fiber ring example **5-5**

VT1.5 capacity **6-15**

BLSROSYNC (alarm) **14-11, 14-19**

BPV *see* bipolar violations

broadcast domains **9-21**

C

- cable guides **1-20**
- cables
 - alarm installation **1-26**
 - coaxial installation **1-23**
 - connect PC to ONS 15454 **2-13**
 - DS-1 installation **1-24**
 - fiber-optic installation **1-22**
 - ground **1-9**
 - installation overview **1-20**
 - type descriptions **1-20**
 - CHAMP **1-20**
 - coaxial **1-20**
 - optical **1-20**
 - twisted-pair **1-20**
- card protection
 - creating a protection group **3-8**
 - default electrical protection **3-8**
 - deleting a protection group **3-10**
 - description
 - electrical (DS-1, DS-3) **13-2**
 - optical cards **13-3**
 - editing a protection group **3-9**
 - Ethernet (spanning tree) **9-27**
- card provisioning **7-1 to 7-21**
 - CTC card view **2-36**
 - electrical cards **7-2**
 - IPPM **7-15**
 - optical cards **7-10**
- cards
 - individual cards are indexed by name*
 - colors onscreen **2-29**
 - common control, overview **13-2**
 - Ethernet, overview **13-2**
 - improper removal **14-47**
 - installing **1-15**
 - inventory **3-16**
 - MIC, overview **13-2**
 - optical, overview **13-2**
 - part number **3-17**
 - protection *see* card protection
 - revision number **3-17**
 - serial number **3-17**
 - slots illustration **13-1**
 - turn-up **1-17**
 - XTC *see* XTC cards
- card slots **1-15**
- CARLOSS (alarm) **14-20**
- carrier loss **14-20**
- CHAMP connectors *see* cables, DS-1 installation
- circuits **6-1 to 6-15**
 - definition **6-2**
 - adding a node **2-32**
 - attributes **6-1**
 - automatic routing restraints **6-4, 6-7**
 - auto ranged **6-2, 6-3, 6-6**
 - bidirectional **6-3, 6-6**
 - creating automated circuits **6-2**
 - creating manual circuits **6-6**
 - deleting and recreating circuits for a linear to ring conversion **5-39, 5-41**
 - deleting and recreating for a linear to ring conversion **5-39**
 - displaying span properties **2-32**
 - editing UPSR circuits **6-10 to 6-12**
 - fully-protected path **6-4**
 - manual Ethernet cross-connects **9-16**
 - monitoring **6-9**
 - names **6-2, 6-6**
 - nodal diversity **6-7**
 - number of circuits **6-3, 6-6**
 - path diversity **6-4**
 - point-to-point Ethernet circuit **9-6**
 - protected drops **6-3**
 - protection for DS-1 and DS-3 circuits **13-2**
 - provisioning with a shortcut **2-32**
 - review routes **6-5**

- route automatically **6-4, 6-7**
- searching **6-10**
- shared packet ring Ethernet circuit **9-9**
- size **6-3**
- type **6-2, 6-6**
- unidirectional with multiple drops **6-8**
- upgrading a span **2-32**
- use secondary destination **6-4**
- use secondary source **6-4**
- virtual UPSR **6-4, 6-7**
- VT tunnels versus STS capacity **6-19**
- Cisco Transport Controller *see* CTC
- cleaning optical fibers *see* fibers, optical
- CLEI code **3-17**
- clock
 - set **3-3**
- CMS *see* CTC
- coding violations **7-13**
- colors
 - cards **2-29**
 - nodes **2-31**
- computer requirements **2-2**
- CONCAT (alarm) **14-23**
- conditions **10-2, 14-8**
- connected rings **5-29**
- CONTBUS-A-18 (alarm) **14-24**
- CONTBUS-A-X (alarm) **14-23**
- CONTBUS-B-18 (alarm) **14-26**
- CONTBUS-B-X (alarm) **14-25**
- controls *see* external controls
- CORBA **2-28**
- corporate LAN **2-10, 2-18**
- cost **4-26, 4-30**
- craft connection **2-10**
- cross-connect
 - card capacities **6-15**
 - definition **6-2**
 - Ethernet **9-16**
 - see also* circuits
 - see also* XTC cards
- CTC
 - installing **2-1 to 2-28**
 - alarms
 - colors **10-3**
 - deleting **10-3**
 - history **10-6**
 - profiles **10-7**
 - see also* alarms
 - viewing **10-1**
 - card inventory **3-16**
 - card protection setup **3-8**
 - changing format of data **2-41**
 - computer requirements **2-2**
 - connecting PCs **2-9, 2-20**
 - database backup **12-7**
 - firewall access **2-27**
 - hardware specifications **1-29**
 - installation wizard (UNIX) **2-6**
 - LAN connections **2-22**
 - logging in **2-24**
 - login node groups **2-25**
 - loss of TCP/IP connection **14-21**
 - navigation **2-37**
 - node setup **3-2**
 - PC requirements **2-4**
 - printing **2-41**
 - remote site access **2-19, 2-23**
 - setup wizard **2-4**
 - timing setup **3-11**
 - TL1 access **2-23**
 - true revert to earlier software **12-8**
 - Unix workstation requirements **2-6**
 - views
 - description **2-28**
 - card view **2-36**
 - network *see* network view
 - node *see* node view
- CTC Installation wizard (CTC) **2-4**

CTNEQPT-PBX PROT (alarm) **14-27**

CTNEQPT-PBXWORK (alarm) **14-28**

CV-L parameter

OC-12 and OC-48 cards **8-30, 8-33, 8-35, 8-38**

OC-3 card **8-25, 8-27**

CV parameter, provisioning **7-13**

CV-S parameter

OC-12 and OC-48 cards **8-30, 8-35**

OC-3 card **8-24**

CV-V parameter

XTC DS1 cards **8-20**

cyclic redundancy checking **14-18**

D

database

memory exceeded **14-30**

version **3-17**

database backup

procedure **12-6**

XTC card **13-5**

Data Communications Channel *see* DCC

data export **2-41**

DATAFLT (alarm) **14-30**

datagrams **4-23**

date

setting **3-3**

DCC

definition **6-20**

and APS **13-16**

and routing **13-5**

and the XTC **13-3**

and true revert **12-8**

capacity **5-29**

channel lost **14-31**

exclude autodiscovery **2-25**

in domains **2-33**

metric (OSPF) **4-30**

OSPF Area ID **4-30**

terminations for BLSR **5-8**

terminations for UPSR **5-23, 5-24**

tunneling **6-20 to 6-22**

viewing connections **2-30**

DCC tunneling **13-5**

DCS **5-31**

dead interval **4-32**

default IP address **2-20**

default K alarm **14-11**

default router **3-3**

default thresholds **7-1**

destination

host **4-23**

IP addresses **4-19**

routing table **4-38**

DHCP **2-20, 3-4, 4-22**

diagnostic files, creating **12-33**

DISCONNECTED (alarm) **14-21**

DNS configuration **2-13, 2-14, 2-16, 2-18**

documentation

online **2-4**

domains

description **2-33**

changing background color **2-34**

creating **2-33**

opening **2-34**

removing **2-34**

renaming **2-34**

drop

creating multiple drops **6-8**

definition **6-2**

drop port **6-12, 6-14**

nodes **6-11, 6-15**

protected drops **6-3, 6-6**

DS1 CV-L parameter **8-17**

DS1 ES-L parameter **8-17**

DS1 LOSS-L parameter **8-17**

DS-1 port

VT1.5 circuit example **6-16**

DS1 Rx AISS-P parameter **8-18**
 DS1 Rx CV-P parameter **8-18**
 DS1 Rx ES-P parameter **8-18**
 DS1 Rx SAS-P parameter **8-18**
 DS1 Rx SES-P parameter **8-18**
 DS1 Rx UAS-P parameter **8-18**
 DS1 SES-L parameter **8-17**
 DS1 Tx AISS-P parameter **8-19**
 DS1 Tx CV-P parameter **8-19**
 DS1 Tx ES-P parameter **8-19**
 DS1 Tx SAS-P parameter **8-19**
 DS1 Tx SES-P parameter **8-19**
 DS1 Tx UAS-P parameter **8-19**
 DS3 card
 performance monitoring **8-21**
 DS3 CV-L parameter **8-23**
 DS3 ES-L parameter **8-23**
 DS3FF-MISM (alarm) **14-30**
 DS3 LOSS-L parameter **8-23**
 DS3 SES-L parameter **8-23**
 dynamic host configuration protocol *see* DHCP

E

E10/100-4 card **9-2, 13-23**
 card-level LEDs **13-24**
 port-level LEDs **13-24**
 specifications **13-25**
 east port **5-7, 5-10**
 electrical cards
 see cards indexed by name
 see XTC cards
 enterprise LAN *see* corporate LAN
 environmental specifications **1-30**
 environment variable **2-8**
 EOC (alarm) **14-31**
 EQPT (alarm) **14-18, 14-32, 14-33**
 equipment failure **14-32, 14-33, 14-42**
 ES-L parameter
 OC-12 and OC-48 cards **8-30, 8-33, 8-35, 8-38**
 OC-3 card **8-25, 8-27**
 XTC cards **8-17**
 XTC DS3 cards **8-23**
 ES parameter, provisioning **7-13**
 ES-S parameter
 OC-12 and OC-48 cards **8-30, 8-35**
 OC-3 card **8-24**
 ES-V parameter
 XTC DS1 cards **8-20**
 Ethernet **9-1 to 9-34**
 card *see* E10/100-4
 carrier loss **14-20**
 circuits
 hub-and-spoke **9-13**
 manual cross-connects **9-16**
 multicard and single-card EtherSwitch
 point-to-point **9-6**
 shared packed ring circuit **9-9**
 collision monitoring (RMON) **9-31**
 EtherSwitch **9-4 to 9-5**
 history window **9-30**
 line utilization window **9-30**
 MAC address screen **9-30**
 port provisioning
 E10/100-4 card **9-3**
 VLAN membership **9-3**
 priority queuing **9-24**
 router aggregation **9-1**
 spanning tree protection **9-26**
 statistics window **9-29**
 threshold variables (MIBs) **9-32**
 trunk utilization window **9-31**
 utilization formula **9-30**
 VLANs **9-21**
 EtherSwitch
 multicard **9-4**
 ONS 15327 circuit combinations **9-5**
 single-card **9-4**

- events **10-3, 10-6**
 - E-W-MISMATCH (alarm) **14-33**
 - examples
 - adding a BLSR node **5-11**
 - BLSR bandwidth reuse **5-4**
 - converting degrees to degrees and minutes **3-2**
 - creating a VT1.5 circuit on an XTC card **6-16**
 - creating login node groups **2-25**
 - creating VT1.5 circuits **6-15**
 - DCC tunnel **6-20**
 - moving a BLSR trunk card **5-18**
 - network timing **3-11**
 - PPMN **5-42**
 - removing a BLSR node **5-15, 5-17**
 - subtending BLSRs **5-31**
 - two-fiber BLSR **5-5**
 - UPSR **5-22**
 - VT tunnel **6-18**
 - EXCCOL (alarm) **14-35**
 - excess collisions **14-35**
 - EXERCISE-RING-FAIL (alarm) **14-35**
 - EXERCISE-SPAN-FAILED (alarm) **14-36**
 - EXT (alarm) **14-36**
 - external alarm inputs **1-26, 7-17, 13-10**
 - external controls **1-26, 7-19, 13-10**
 - external timing **3-11**
-
- F**
- facility loopback
 - definition **12-20**
 - test a destination XTC DS-N card **12-30**
 - FAILTOSW-PATH (alarm) **14-36**
 - FAILTOSWR (alarm) **14-38**
 - FAILTOSWS (alarm) **14-39**
 - failure count, provisioning **7-13**
 - FAN (alarm) **14-39, 14-40**
 - fan-tray assembly
 - air filter *see* air filter
 - description **1-7**
 - error **14-39, 14-40**
 - fan failure **1-9**
 - install **1-8**
 - removal **1-8**
 - fast Ethernet *see* E10/100-4 card
 - FC-L parameter
 - OC-12 and OC-48 cards **8-30, 8-33, 8-35, 8-38**
 - OC-3 card **8-25, 8-28**
 - FE-AIS (alarm) **14-40**
 - FE-DS1-MULTLOS (alarm) **14-41**
 - FE-DS1-SNGLLOS (alarm) **14-41**
 - FE-EQPT-FAIL-SA (alarm) **14-42**
 - FE-EQPT-NSA (alarm) **14-42**
 - FE-IDLE (alarm) **14-42**
 - FE-LOCKOUT (alarm) **14-43**
 - FE-LOF (alarm) **14-43**
 - FE-LOS (alarm) **14-44**
 - FEPRLF (alarm) **14-44**
 - ferrites
 - attaching to power cables **1-14**
 - fibers, optical
 - cable installation **1-22**
 - cleaning **12-33**
 - protection **1-20**
 - filter *see* air filter
 - firewalls **2-27**
 - FORCED-REQ (alarm) **14-44**
 - framing **3-14**
 - free run synchronization **14-45**
 - FRNGSYNC (alarm) **14-45**
 - front panel **1-2**
 - FSTSYNC (alarm) **14-45**
 - fully-protected path **6-7**
-
- G**
- gateway **4-19**
 - default **4-22, 4-24**

on routing table **4-38**
 proxy ARP-enabled **4-23**
 returning MAC address **4-23**

H

hairpin circuit

create on a destination node **12-26**
 create on a source node **12-24**
 definition **12-20**

hard reset *see* resets

hello interval **4-31, 4-32**

HITEMP (alarm) **14-46**

HLDOVERSYNC (alarm) **14-46**

holdover synchronization **14-46**

hop **4-26**

hosts **3-3**

hub-and-spoke **9-13**

I

idle time **3-6**

IEEE 802.1Q (priority queuing) **9-24**

IIOIP **2-27, 2-28**

IMPROPRMVL (alarm) **14-47**

INCOMPATIBLE-SW (alarm) **14-48**

installation

tasks (hardware) **1-2**

installation wizard (UNIX) **2-6**

installing the ONS 15327

cables **1-22**

cards **1-15**

equipment **1-2**

fan-tray assembly **1-7**

overview **1-2**

power **1-9**

reversing the mounting bracket **1-4**

see also shelf assembly

integrated cross-connect card *see* XTC cards

intermediate-path performance monitoring *see* IPPM

Internet Explorer

disable proxy service **2-19**

Internet Inter-ORB Protocol *see* IIOIP

internet protocol *see* IP

interoperability

JRE compatibility **2-2**

ONS node Ethernet circuit combinations **9-5**

inventory **3-16**

INVMACADR (alarm) **14-49**

IP

address change for LAN connection **2-22**

address definition **3-3**

address description **2-20**

addressing scenarios *see* IP addressing scenarios **4-20**

address initial configuration **2-13, 2-16**

default address **2-20**

environments **4-19**

networking **4-19 to 4-39**

requirements **4-20**

select address for log in **2-25**

subnetting **4-19**

IP addressing scenarios **4-20**

CTC and nodes connected to router **4-22**

CTC and nodes on same subnet **4-21**

default gateway on CTC workstation **4-24**

OSPF **4-27**

proxy ARP and gateway **4-23**

static routes connecting to LANs **4-25**

IPPM

description **8-12**

provisioning **7-15**

J

J1 bytes **6-12**

J1 path trace **6-12 to 6-15**

automatic **6-12**

- manual **6-12**
 - Java
 - and CTC, overview **2-1**
 - console window **2-24**
 - java.policy file **2-2**
 - java runtime environment *see* JRE
 - JRE
 - install (Solaris) **2-7**
 - install (Windows) **2-6**
 - location **2-2**
 - modify policy file (Solaris) **2-8**
 - modify policy file (Windows) **2-6**
 - patches **2-8**
 - patch requirement **2-4**
 - reference **2-9**
-
- K**
- k bytes **5-3, 14-11, 14-12**
-
- L**
- LAN
 - accessing the ONS 15454 **2-22**
 - external interface specifications **1-29**
 - modems **2-19, 2-23**
 - OSPF activity **4-30**
 - latitude **2-35**
 - layer 2 switching **9-4**
 - linear ADM
 - description **5-34**
 - converting to BLSR **5-39**
 - converting to UPSR **5-35**
 - creating **5-35**
 - increasing the traffic speed **12-12**
 - OC-12 cards **13-14**
 - OC-3 card **13-11**
 - OC-48 cards **13-18, 13-21**
 - see also* 1+1 optical card protection
 - line timing **3-11**
 - listener port **2-28**
 - lock on **12-18**
 - lock out **12-18**
 - LOCKOUT-REQ (alarm) **14-49**
 - LOF (alarm)
 - BITS **14-49**
 - OC-N **14-51**
 - XTC (DS-1) **14-50**
 - XTC (DS-3) **14-51**
 - logging in **2-24**
 - login node groups
 - creating **2-25**
 - network view **2-30**
 - viewing **2-25**
 - longitude **2-35**
 - loopback
 - alarms **14-58, 14-59, 14-60**
 - see also* facility loopback
 - see also* terminal loopback
 - LOP-P (alarm) **14-53**
 - LOP-V (alarm) **14-55**
 - LOS (alarm)
 - BITS **14-56**
 - OC-N **14-57**
 - XTC (DS-N) **14-56**
 - loss of frame *see* LOF
 - loss of pointer *see* LOP
 - LPBKDS1FEAC (alarm) **14-58**
 - LPBKDS3FEAC (alarm) **14-58**
 - LPBKFACILITY (alarm)
 - DS-N **14-58**
 - OC-N **14-59**
 - LPBKTERMINAL (alarm)
 - XTC **14-60**

M

MAC address **4-23**
 clear table **3-6**
 data memory failure **14-64**
 definition **9-30**
 in CTC **9-30**
 invalid **14-49**
 retrieve table **3-6**
 viewing on node **3-4**

maintenance
see database backup and restore
see diagnostic files
see fibers, optical
see network tests

management information base *See* MIB

MAN-REQ (alarm) **14-61**

MANRESET (alarm) **14-61**

map (network) **2-35**

MEA (alarm) **14-62**

Mechanical Interface Card *see* MIC

MEM-GONE (alarm) **14-63**

MEM-LOW (alarm) **14-63**

MFGMEM (alarm) **14-64**

MIB
 description **11-3**
 Ethernet **9-32**
 groups **11-7**
see also SNMP

MIC
 description **13-9**
 alarm interface **13-10**
 and cable installation **1-21**
 BITS interface **13-10**
 card view **2-36**
 DS-1 physical interfaces **13-9**
 DS-3 physical interfaces **13-9**
 MIC A and MIC B differences **13-9**
 power connection **13-10**

specifications **13-10**
 turn-up **1-18**

Microsoft Internet Explorer **2-1**

modem interface specifications **1-29**

modems
 LAN **2-23**

monitor circuits **6-9**

monitoring
 circuits *see* monitor circuits

multicard Etherswitch **9-4**

multiple drops **6-8**

N

navigating in CTC **2-37**

Netscape Communicator **2-5, 2-7**
 obtaining **2-2**
 running the CTC setup wizard **2-4**

Netscape Navigator
 CTC browser **2-1**
 disable proxy service **2-19**
 disabling proxy service **2-23**
 testing the node connection **2-17, 2-21**

network interface cards **2-20**

networks
 default configuration *see* UPSR
 IP networking **4-19 to 4-39**
 setting up basic information **3-3**
 SONET topologies **5-1 to 5-44**
 timing example **3-11**

network tests **12-19**
 facility loopback on a destination XTC card **12-30**
 facility loopback on a source XTC card **12-21**
 hairpin circuit on a source node XTC card **12-24**
 hairpin on a destination node XTC card **12-26**
see hairpin circuits
see loopback
 terminal loopback on a destination XTC card **12-28**
 types **12-19**

- network view
 - description **2-30**
 - adding nodes to map *see* domains
 - changing the background color **2-34**
 - changing the background image (map) **2-35**
 - creating new users **3-6**
 - login node groups **2-30**
 - moving node positions **2-32, 2-35**
 - tasks **2-32**
 - NIC **2-20**
 - node view
 - description **2-29**
 - card colors **2-29**
 - creating protection groups **3-8**
 - creating users **3-5**
 - setting up basic network information **3-3**
 - setting up basic node information **3-2**
 - setting up timing **3-13**
 - tabs list **2-30**
 - viewing popup information **2-30**
 - NOT-AUTHENTICATED (alarm) **14-65**
 - NPJC-Pdet parameter
 - description **8-14**
 - OC-12 and OC-48 cards **8-31, 8-36**
 - OC-3 card **8-26**
 - provisioning **7-14**
 - NPJC-Pgen parameter **8-14**
 - OC-12 and OC-48 cards **8-31, 8-36**
 - OC-3 card **8-26**
 - provisioning **7-14**
-
- O**
- OAM&P access **2-28**
 - OC12 IR 1310 card
 - description **13-13, 13-16**
 - card-level LEDs **13-16**
 - LEDs **13-14**
 - slot requirements **13-14**
 - specifications **13-12, 13-15, 13-17**
 - OC3 IR 1310 card
 - description **13-11**
 - OC3 IR 4 1310 card
 - LEDs **13-11**
 - OC48 IR 1310 card
 - description **13-18, 13-21**
 - card-level LEDs **13-21**
 - LEDs **13-19**
 - specifications **13-20, 13-22**
 - OC48 LR 1550 card
 - LEDs **13-21**
 - OC-N cards
 - BLSR trunk cards **5-7**
 - creating protection groups **3-8**
 - data export **2-41**
 - modifying transmission quality **7-10**
 - moving BLSR trunk cards **5-18**
 - path trace **6-12**
 - performance monitoring for OC-12 and OC-48 cards **8-29, 8-34**
 - performance monitoring for OC-3 **8-24**
 - provision line transmission settings **7-11**
 - provision threshold settings **7-12**
 - timing **3-11**
 - upgrading to a higher rate while in-service **12-12**
 - UPSR trunk cards **5-23**
 - online documentation **2-4**
 - Open Shortest Path First *see* OSPF
 - optical carrier cards *see* OC-N cards
 - optical transmission quality **7-11**
 - orderwire pass-through **7-20**
 - express **7-20**
 - local **7-20**
 - OSPF
 - area range table **4-31**
 - connecting nodes to CTC **4-25**
 - DCC OSPF area **4-30**
 - definition **4-27 to 4-30**

intervals **4-31**
 LAN activity **4-30**
 priority level **4-31**

P

passwords **2-24, 3-7**
 path-protected mesh network *see* PPMN
 path trace **6-12 to 6-15, 14-82**
 path trace mode
 auto **6-14**
 manual **6-14**
 PC
 connect to ONS 15454 using a craft connection **2-10**
 connect to ONS 15454 with LAN **2-18**
 connect with Windows 2000 **2-13, 2-14, 2-16**
 connect with Windows 95/98 **2-13, 2-14, 2-16**
 connect with Windows NT **2-13, 2-14, 2-16**
 PDI-P **6-3, 6-7**
 PDI-P (alarm) **14-65**
 PEER-NORESPONSE (alarm) **14-67**
 performance monitoring **8-1 to 8-38**
 15-minute intervals **8-4**
 clear count displayed **8-8**
 clear count stored **8-9**
 DS1 and DS1N parameters **8-16**
 DS3 and DS3N parameters **8-21**
 Ethernet **9-34**
 IPPM **8-12**
 line-level thresholds for electrical cards, setting **7-2**
 OC-12 and OC-48 cards **8-29, 8-34**
 OC3 parameters **8-24**
 path-level thresholds for DS-1 traffic, setting **7-2**
 path-level thresholds for DS-3 traffic, setting **7-2**
 path-level thresholds for STS/VT1.5 traffic, setting **7-2**
 thresholds **8-2**
 ping **4-20**
 PLM-P (alarm) **14-67**
 PLM-V (alarm) **14-68**
 pointer justification counts **8-13**
 point-to-point
 see Ethernet circuits
 see linear ADM
 popup data **2-30**
 port filtering **2-27**
 ports
 drop **6-12**
 enable for BLSR **5-8**
 enable for UPSR **5-25**
 enabling, general **3-9**
 Ethernet **9-3**
 filtering **2-27**
 IIOP port **2-27**
 listener port **2-28**
 path trace source and drop **6-12**
 protection **3-8**
 RJ-45 on XTC **2-20**
 status **2-36**
 TL1 port **2-2**
 power specifications **1-30**
 PPJC-Pdet parameter
 description **8-14**
 OC-12 and OC-48 cards **8-31, 8-36**
 OC-3 card **8-26**
 provisioning **7-14**
 PPJC-Pgen parameter
 OC-12 and OC-48 cards **8-31, 8-36**
 OC-3 card **8-26**
 provisioning **7-14**
 description **8-14**
 PPMN **5-42**
 PRC-DUPID (alarm) **14-68**
 Preface **xliii**
 printing **2-41**
 priority queuing **9-23**
 protection
 protection groups **3-8**
 see protection switching

- see* SONET topologies
- protection switching
 - APS channel mismatch **14-14**
 - APS mode mismatch failure **14-15**
 - byte failure (alarm) **14-11**
 - count *see* PSC
 - duration **7-14**
 - duration parameter (PSD) **8-26**
 - duration *see* PSD
 - editing a UPSR circuit **6-11**
 - inconsistent APS code **14-13**
 - invalid k bytes in APS **14-12**
 - lock on **12-18**
 - lock out **12-18**
 - lockout switch alarm **14-49**
 - reversion time **6-3, 6-7**
 - revertive **6-3, 6-7**
 - ring switch failure **14-38**
 - span switch failure **14-39**
 - UPSR alarms **14-16, 14-17**
- protocols
 - DHCP **3-4**
 - proxy ARP *see* proxy ARP
 - SNMP *see* SNMP
 - SNTP **3-2**
 - spanning tree *see* spanning tree protocol
 - SSM **3-12**
- proxy ARP
 - description **4-19**
 - enabling an ONS 15454 gateway **4-23**
- proxy service **2-23**
 - disable **2-19**
- PSC parameter
 - 1+1 protection **8-26, 8-31, 8-36**
 - BLSR **8-31, 8-36**
 - provisioning **7-14**
 - provisioning PSC-R **7-15**
 - provisioning PSC-S **7-15**
 - provisioning PSC-W **7-14**

- PSC-W (working) **8-32, 8-37**

PSD parameter

- definition **8-26**

- OC-12 and OC-48 cards **8-32, 8-36**

- provisioning PSD-L **7-14**

- provisioning PSD-R **7-15**

- provisioning PSD-S **7-15**

- provisioning PSD-W **7-15**

- PSD-W (working) **8-32, 8-37**

Q

- Q-tagging **9-22**

- queuing **9-23**

R

- RAI (alarm) **14-69**

- RCVRLMISS (alarm) **14-69**

- Related Documentation **xliv**

- remote fault indication *see* RFI

- resets **12-5**

- hard **12-5**

- soft **12-5**

- reversion time **5-10, 6-3**

- revertive switching **6-3, 6-7**

- revertive switching *see also* switching

- RFI (alarm)

- line level **14-70**

- path level **14-70**

- VT level **14-71**

- RING-MISMATCH (alarm) **14-72**

- rings

- converting from linear **5-35, 5-39**

- ID mismatch **14-72**

- maximum per node **5-1**

- see* BLSR

- see* UPSR

subtended **5-29**
 virtual **5-43**
 RJ-45 **2-20**
 and BITS interface **13-10**
 and twisted-pair cables **1-26, 1-27**
 external alarms **13-10**
 LAN connection on the XTC **13-2**
 pins **1-27**
 see also BITS, pin assignments
 RMON
 description **11-7**
 Ethernet alarm thresholds **9-31**
 MIB Groups **11-7**
 routing table **4-38**

S

SC connectors *see* cables
 SCI **13-5**
 SD BER **7-11**
 SDBER (alarm) **14-72, 14-73**
 SD threshold **6-3, 6-7**
 security
 setting up **3-5**
 tasks per level **3-5**
 viewing **2-29**
 SEFS-S parameter
 OC-12 and OC-48 cards **8-30, 8-35**
 OC-3 card **8-25**
 Serial Communication Interface *see* SCI
 SES-L parameter
 OC-12 and OC-48 cards **8-30, 8-33, 8-35, 8-38**
 OC-3 card **8-25, 8-27**
 SES parameter, provisioning **7-13**
 SES-S parameter
 OC-12 and OC-48 cards **8-30, 8-35**
 OC-3 card **8-25**
 SES-V parameter
 XTC DS1 cards **8-20**
 severities, alarm **14-9**
 SFBER (alarm) **14-74, 14-75**
 SF BER parameter, provisioning **7-11**
 SF threshold **6-3, 6-7**
 SFTWDWN-FAIL (alarm) **14-76, 14-77**
 shared packet ring **9-9**
 shelf assembly
 installing multiple nodes in a rack **1-7**
 installing one node in a rack **1-6**
 measurements **1-4**
 reversible mounting bracket **1-4**
 shells **2-9**
 shortest path **5-2**
 signal degrade (alarm) **14-17**
 signal failure **14-74, 14-75**
 signal failure (alarm) **14-17**
 signal label mismatch failure *see* SMLF **14-67**
 simple network management protocol *see* SNMP
 simple network time protocol *see* SNTP
 single-card Etherswitch **9-4**
 SLMF **14-67**
 SNMP **11-1 to 11-8**
 description **11-1**
 MIBs **11-3**
 remote network monitoring (RMON) **11-7**
 setting up **11-3**
 traps **11-5**
 SNTP **3-2**
 soft resets *see* resets
 software
 see CTC
 finding the version number **3-17**
 installation **2-1**
 software revert **12-8**
 Solaris
 CTC set up **2-8**
 disable proxy service **2-19, 2-23**
 JRE patch requirement **2-4**
 remote access **2-23**

- running the CTC setup wizard **2-4**
- SONET
 - and Ethernet **9-1**
 - Data Communication Channels *see* DCC
 - improper APS alarm **14-12**
 - K1 and K2 bytes **5-3**
 - line layer (maintenance span) **14-10**
 - path layer **14-10**
 - synchronization status messaging **3-12**
 - timing parameters **3-11**
 - topologies **5-1**
 - VT layer **14-11, 14-55**
- source **6-2**
- span
 - line appearance on map **2-33**
 - upgrade **2-32**
 - view properties **2-32**
- spanning tree protocol
 - configuration **9-28**
 - description **9-26**
 - multi-instance **9-27**
 - parameters **9-27**
- span upgrades
 - description **12-12**
 - manual upgrades **12-15 to 12-18**
 - wizard **12-13 to 12-15**
- SPE *see* synchronous payload envelope
- SQUELCH (alarm) **14-78**
- SSM
 - description **3-12**
 - enabling **3-14, 7-11**
 - failure **14-79**
 - message set **3-13**
 - synchronization traceability alarm **14-79**
- SSM-FAIL (alarm) **14-79**
- ST3 clock **3-11**
- standard constant **2-28**
- static routes **4-19**
 - connecting to LANs **4-25**
- STP *see* spanning tree protocol
- string **6-12**
- STS-1 cross-connects **13-5**
- STS concatenation error **14-23**
- STS CV-P parameter
 - monitored IPPMs **8-13**
 - OC-12 and OC-48 cards **8-32, 8-37**
 - OC-3 card **8-27**
 - XTC DS1 cards **8-21**
 - XTC DS3 cards **8-23**
- STS ES-P parameter
 - monitored IPPMs **8-13**
 - OC-12 and OC-48 cards **8-32, 8-37**
 - OC-3 card **8-27**
 - XTC DS1 cards **8-21**
 - XTC DS3 cards **8-23**
- STS FC-P parameter
 - monitored IPPMs **8-13**
 - OC-12 and OC-48 cards **8-32, 8-37**
 - OC-3 card **8-27**
 - XTC DS1 cards **8-21**
 - XTC DS3 cards **8-23**
- STS SES-P parameter
 - monitored IPPM **8-13**
 - OC-12 and OC-48 cards **8-33, 8-37**
 - OC-3 card **8-27**
 - XTC DS1 cards **8-21**
 - XTC DS3 cards **8-23**
- STS UAS-P parameter
 - monitored IPPM **8-13**
 - OC-12 and OC-48 cards **8-33, 8-37**
 - OC-3 card **8-27**
 - XTC DS1 cards **8-21**
 - XTC DS3 cards **8-23**
- STU (alarm) **14-79**
- subnet
 - CTC and nodes on different subnets **4-22**
 - CTC and nodes on same subnet **4-21**
 - multiple subnets on the network **4-24**

- using static routes **4-25**
- with proxy ARP **4-23**
- subnet mask **3-3**
 - 24-bit **4-39**
 - 32-bit **4-39**
- access to nodes **4-26**
- destination host or network **4-38**
- OSPF area range table **4-31**
- Windows setup **2-13, 2-16**
- subnetting **3-3**
- subtending rings **5-29**
 - subtend a BLSR from a BLSR **5-32**
 - subtend a BLSR from a UPSR **5-31**
- SWFTDWN (alarm) **14-76**
- switching
 - and Ethernet **9-1**
 - bidirectional **3-9**
 - non-revertive **13-3**
 - revertive **3-9, 13-3**
 - see* protection switching
 - see* traffic switching
 - time division switching **13-5**
 - XTC process **13-5**
- SWTOPRI (alarm) **14-80**
- SWTOSEC (alarm) **14-80**
- SWTOTHIRD (alarm) **14-80**
- synchronization status messaging *see* SSM **3-12**
- synchronous payload envelope
 - clocking differences **8-13**
 - OC-12 **8-31**
 - OC-12 and OC-48 cards **8-36**
 - OC-3 card **8-26**
- SYNCPRI (alarm) **14-80**
- SYNCSEC (alarm) **14-81**
- SYNCTHIRD (alarm) **14-81**
- SYSBOOT (alarm) **14-82**

T

- tables
 - display hidden columns **2-40**
 - exporting data **2-41, 2-43**
 - printing data **2-42**
 - rearranging columns **2-39**
 - resizing columns **2-40**
 - sorting **2-40**
- tabs
 - overview **2-28**
 - in card view **2-36**
 - node view - alarms **2-30**
 - node view - circuits **2-30**
 - node view - conditions **2-30**
 - node view - history **2-30**
 - node view - Inventory **3-16**
 - node view - inventory **2-30**
 - node view - maintenance **2-30**
 - node view - provisioning **2-30**
- TCA **8-4**
 - 15-minute interval **8-4**
 - 24-hour interval **8-5**
 - changing thresholds **8-10**
 - IPPM paths **8-13**
 - threshold guidelines **7-1**
- TCP/IP **2-13, 2-14, 2-16**
- TDM **6-15, 9-1**
- Telcordia
 - alarm severities **10-1**
 - default alarm severities **10-7**
 - default card thresholds **7-1**
 - default severities **14-1**
 - performance monitoring **8-1**
 - signal degrade definition **14-72, 14-73**
 - signal failure definition **14-74, 14-75**
 - trouble categories **14-8**
- temperature
 - fan-tray assembly alarm **14-39, 14-40**

- node alarm **14-46**
- terminal loopback
 - test on a destination DS-N card **12-28**
- testing
 - see also* performance monitoring
 - test set **5-35**
- third-party equipment **6-1, 6-20**
- threshold crossing alert *see* TCA
- thresholds
 - card **8-12**
 - Ethernet **9-34**
 - MIBs **9-31**
 - optical cards **7-12**
 - performance monitoring **8-10**
 - XTC DS-1 card **7-4**
 - XTC DS-3 card **7-8**
- Time Division Multiplexing *see* TDM
- time zone **3-3**
- timing **7-11**
 - and BITS **13-10**
 - BITS *see* BITS
 - installation **1-14**
 - internal **3-15**
 - parameters **3-11**
 - set node clock **3-3**
 - setting up **3-13**
 - specifications **1-30**
 - XTC process **13-5**
- timing alarms
 - loss of primary reference **14-80**
 - loss of third reference **14-81**
 - switching to secondary timing source **14-80**
 - switching to third timing source **14-80**
 - synchronization **14-45, 14-46**
- TIM-P (alarm) **14-82**
- TL1
 - AID in CTC **10-2, 10-5**
 - and CTC error messages **14-1**
 - commands **2-2**
 - connecting to the ONS 15454 **2-23**
 - craft interface specifications **1-29**
- TLS *see* VLAN
- topology hosts **2-25**
- traffic
 - cards *see also* DS-N/OC-N cards
 - outages when removing a node **5-15**
 - outages when removing UPSR nodes **5-28**
 - see also* circuits
 - switching *see* traffic switching
 - switching UPSR traffic **5-25**
- traffic monitoring **6-12**
- traffic switching
 - adding and removing UPSR nodes **5-25**
 - moving a BSLR trunk card **5-18**
 - multicard Etherswitch **9-4**
 - removing a BSLR node **5-16**
 - single-card Etherswitch **9-4**
- transmission failure **14-83**
- TRMT (alarm) **14-83**
- TRMTMISS (alarm) **14-83**
- troubleclearing *see* troubleshooting
- troubleshooting
 - see* alarms
 - conditions **14-8**
 - see* diagnostic files
 - severities **14-9**
 - trouble notifications **14-8**
- trunk cards
 - BLSR **5-7, 5-16**
 - moving **5-18**
 - UPSR **5-23**
- tunnel
 - see* DCC
 - see* VT tunnel
- turn-up
 - see* cards, turn-up
- twisted-pair cables *see* cables
- two-fiber BLSR *see* BLSR

U

UAS-L parameter

OC-12 and OC-48 cards **8-30, 8-33, 8-35, 8-38**OC-3 card **8-25, 8-28**UAS parameter **7-13**

UAS-V parameter

XTC DS1 cards **8-20**UNEQ-P (alarm) **14-84**unequipped path **14-17**UNEQ-V (alarm) **14-85**unidirectional path switched rings *see* UPSR

upgrade

cards

XTC-14 to XTC-28 **12-10**spans **12-12**

UPSR

adding nodes **5-25, 5-27**AIS alarm **14-16**circuit editing **6-10**converting from linear ADM **5-35, 5-39**DCC terminations **5-24**description **5-20**enabling ports **5-25**example **5-22**failed APS *see* FAILTOSW-PATHincreasing the traffic speed **12-12**LOP alarm **14-16, 14-17**PDI alarm **14-17**removing nodes **5-25, 5-28**SD alarm **14-17**set up procedures **5-23**signal failure alarm **14-17**speed upgrade **12-16**subtending a BLSR **5-31**switch protection paths **6-10**timing **5-25**traffic switch **5-25**user *see* securityuser setup **3-5****V**views *see* CTCvirtual link table (OSPF) **4-31**virtual local area network *see* VLANvirtual rings **5-43**virtual wires *see* alarms

VLAN

and MAC addresses **9-31**number supported **9-21**provisioning Ethernet ports **9-3**spanning tree **9-27**

VT1.5

see also circuitscross-connect capacity on XTC **6-15**cross-connect requirements **6-15**tunneling **6-18**VT mapping **6-16, 13-6**VT tunnels **6-18****W**WAN **4-19**west port **5-7, 5-10**Windows 2000 **2-13, 2-14, 2-16**Windows 95/98 **2-13, 2-14, 2-16**Windows NT **2-13, 2-14, 2-16**WINS configuration **2-13, 2-14, 2-16, 2-18**workstation requirements **2-2****X**XTC-14 card *see* XTC cardsXTC-28-3 card *see* XTC cards

XTC cards

(DS1-14) in a facility loopback **12-19**

- (DS1-14) modify line and threshold settings **7-4**
- (DS1-14) performance monitoring **8-16**
- (DS-1 and DS-3) circuitry **13-4**
- (DS3-12) modify line and threshold settings **7-8**
- (DS-N) creating protection groups **3-8**
- (DS-N) modifying transmission settings **7-4 to 7-8**
- description **13-3**
- alarm cutoff **1-14**
- alarm interface specifications *see* alarms
- and cable installation **1-21**
- and VT mapping **13-6**
- capacities **6-15**
- database backup **12-6**
- exporting data **2-42**
- flash memory problems **14-18**
- front panel **13-4**
- LEDs **13-4**
- low memory **14-63**
- LPBKTERMINAL alarm **14-60**
- memory capacity exceeded **14-63**
- path trace **6-12**
- resetting **12-5**
- see also* cross-connect
- software installation overview **2-1**
- specifications **13-8**
- timing and control functions **13-5**
- turn-up **1-19**
- upgrade **12-10**
- XTC-28-3 card and XTC-14 card differences **13-4**
- XTC front panel *see* XTC cards
- XTCPROTGRP *see* card protection