Cisco ONS 15454 User Documentation

Release 2.2.1
Last Updated: July 25, 2003

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

Customer Order Number: DOC-7811078=
Text Part Number: 78-11078-02

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.

Copyright © 2000, Cisco Systems, Inc. All rights reserved. Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, the 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, iQuick Study, iQ Readiness Scorecard, The iQ Logo, 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, 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, Stratm, SwitchProbe, TeleRouter, 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. (0008R)

Cisco ONS 15454 User Documentation, Release 2.2.1
Copyright © 2000, Cisco Systems, Inc.
All rights reserved.

About This Manual xxxv

Audience xxxv

Organization xxxv

Related Documentation xxxvi

Conventions xxxvi

Obtaining Documentation xxxvii

Obtaining Technical Assistance xxxviii
Contacting TAC by Using the Cisco TAC Website xxxviii
Contacting TAC by Telephone xxxix

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

1.3 Installation in a Rack 1-3
1.3.1 Reversible Mounting Bracket 1-4
Procedure: Reverse the Mounting Bracket 1-5
1.3.2 Mounting the ONS 15454 in a Rack 1-5
Procedure: Mount the Shelf Assembly in a Rack (One Person) 1-6
Procedure: Mount the Shelf Assembly in a Rack (Two People) 1-6
1.3.3 Multiple Installations in a Rack 1-6
Procedure: Mount Multiple ONS 15454s in a Rack 1-7

1.4 Equipment Access and Features 1-9
1.4.1 Front Door 1-10
Procedure: Open the Front Cabinet Compartment 1-10
Procedure: Remove the Front Door 1-11
1.4.2 Card Slots 1-12
1.4.3 Cable Management Facilities 1-12
1.4.4 Fan Tray Assembly 1-13
Procedure: Install or Replace the Fan Tray Air Filter Without the Bottom Brackets 1-14
Procedure: Install or Replace the Fan Tray Air Filter Using the Bottom Brackets 1-14
Procedure: Install the Fan Tray 1-16
Procedure: Remove the Fan Tray 1-16
1.4.5 LCD Screen 1-17
Procedure: View Alarms Counts on a Specific Slot and Port 1-17
1.4.6 LCD Alarm Functions 1-18
1.4.7 Backplane Covers 1-18
Procedure: Remove the Backplane Sheet Metal Covers 1-19
Procedure: Remove an EIA 1-23
Procedure: Install an EIA 1-24
Procedure: Access the Alarm Interface Panel, Alarm Pin Field or Power Terminals 1-25
Procedure: Replace the Alarm Interface Panel 1-25

1.5 Power and Ground Installation 1-25
Procedure: Install Redundant Power Feeds 1-26

1.6 Alarm Pin Field Connections 1-28
1.6.1 Alarm Installation 1-29
1.6.2 Timing Installation 1-30
1.6.3 LAN Installation 1-30
1.6.4 Craft Interface Installation 1-31
1.6.5 X.25 Installation 1-32
1.6.6 Modem Installation 1-32
1.6.7 TBOS Installation 1-32

1.7 Ferrite Installation 1-32

1.8 Card Installation and Turn-Up 1-35
Procedure: Install ONS 15454 Cards 1-35
1.8.1 Slot Requirements 1-36
1.8.2 Card Turn-Up 1-37
Procedure: Verify Successful Turn-Up of the AIC Card 1-37
Procedure: Verify Successful Turn-Up of the TCC/TCC+ and XC/XCVT Cards 1-38
Procedure: Verify Successful Turn-Up of All Other Cards 1-38
1.8.3 Card Software Installation 1-39
1.8.4 Gigabit Interface Converter 1-39
Procedure: Install Gigabit Interface Converters 1-40
Procedure: Remove a Gigabit Interface Converter 1-41

1.9 Cable Installation 1-41
1.9.1 Fiber Cable Installation 1-41
Procedure: Install and Route Fiber Optic Cables in the ONS 15454 1-41
Procedure: Install the Fiber Boot 1-43
1.9.2 Coaxial Cable Installation 1-43
Procedure: Install Coaxial Cable With BNC Connectors 1-44
Procedure: Install Coaxial Cable With High-density BNC Connectors 1-45
Procedure: Install SMB Type Connectors 1-45
1.9.3 DS-1 Cable Installation 1-46
Procedure: Install DS-1 Electrical Interface Adapters 1-47
Procedure: Install DS-1 Cables on the DS-1 Electrical Interface Adapters 1-48
Procedure: Install DS-1 AMP CHAMP Cables on the AMP CHAMP EIA 1-50

1.10 Cable Management 1-50
1.10.1 Optical Cable Management 1-50
Procedure: Route Optical Cables in the Shelf Assembly 1-51
1.10.2 Coaxial Cable Management 1-51
1.10.3 Twisted Pair Cable Management 1-52
1.10.4 AMP CHAMP Cable Management 1-53
1.10.5 Alarm Cable Management 1-53
1.10.6 BIC Rear Cover Installation 1-53
Procedure: Install the BIC Rear Cover 1-54

1.11 ONS 15454 Assembly Specifications 1-54
1.11.1 Bandwidth 1-54
1.11.2 Slot Assignments 1-55
1.11.3 Cards 1-55
1.11.4 Configurations 1-55

1.11.5 Cisco Transport Controller 1-56
1.11.6 External LAN Interface 1-56
1.11.7 TL1 Craft Interface 1-56
1.11.8 Modem Interface 1-56
1.11.9 Alarm Interface 1-56
1.11.10 EIA Interface 1-56
1.11.11 Database Storage 1-56
1.11.12 BITS Interface 1-56
1.11.13 System Timing 1-57
1.11.14 Power Specifications 1-57
1.11.15 Environmental Specifications 1-57
1.11.16 Dimensions 1-57

1.12 Node Turn-Up 1-57
1.12.1 Installation 1-57
1.12.2 Node Turn-Up 1-59

1.13 ONS 15454 Software and Hardware Compatibility Matrix 1-61

Card Reference 2-1

2.1 Overview 2-1
2.1.1 Common Control Cards 2-1
2.1.2 Electrical Cards 2-1
2.1.3 Optical Cards 2-1
2.1.4 Ethernet Card 2-2

2.2 Electrical Card Protection 2-2
2.2.1 1:1 Protection 2-2
2.2.2 1:N Protection 2-3
2.2.3 Electrical Card Protection and the Backplane 2-4

2.3 Optical Card Protection 2-5

2.4 Multiport Card Protection 2-5

2.5 Unprotected Cards 2-6

2.6 Timing Communication and Control (TCC/TCC+) Card 2-7
2.6.1 TCC/TCC+ Functionality 2-7
2.6.2 Unique TCC+ Functionality 2-8
2.6.3 TCC/TCC+ Card-Level Indicators 2-8
2.6.4 System Level Indicators 2-8
2.6.5 TCC/TCC+ Specifications 2-9

2.7 Cross Connect Card 2-11
2.7.1 XC Card-Level Indicators 2-12
2.7.2 XC Specifications 2-13

2.8 Cross Connect VT Card 2-14
2.8.1 VT Mapping 2-15
2.8.2 XCVT Hosting DS3XM-6 2-16
2.8.3 XCVT Card-Level Indicators 2-16
2.8.4 XC/XCVT Compatibility 2-16
2.8.5 XCVT Card Specifications 2-18

2.9 Alarm Interface Controller Card 2-19
2.9.1 Customer-Defined Alarms 2-19
2.9.2 Orderwire 2-20
2.9.3 AIC Specifications 2-22

2.10 EC1-12 Card 2-23
2.10.1 EC1-12 Card-Level Indicators 2-24
2.10.2 EC1-12 Port-Level Indicators 2-24
2.10.3 EC1-12 Specifications 2-24

2.11 DS1-14 Card 2-26
2.11.1 DS1-14 Card-Level Indicators 2-27
2.11.2 DS1-14 Port-Level Indicators 2-27
2.11.3 DS1-14 Specifications 2-27

2.12 DS1N-14 Card 2-29
2.12.1 DS1N-14 Card-Level Indicators 2-30
2.12.2 DS1N-14 Port-Level Indicators 2-30
2.12.3 DS1N-14 Specifications 2-30

2.13 DS3-12 Card 2-32
2.13.1 DS3-12 Card-Level Indicators 2-33
2.13.2 DS3-12 Port-Level Indicators 2-33
2.13.3 DS3-12 Specifications 2-33

2.14 DS3N-12 Card 2-35
2.14.1 DS3N-12 Card-Level Indicators 2-36
2.14.2 DS3N-12 Port-Level Indicators 2-36
2.14.3 DS3N-12 Card Specifications 2-36

2.15 DS3XM-6 Card 2-38
2.15.1 DS3XM-6 Hosted By XCVT 2-38
2.15.2 DS3XM-6 Card-Level Indicators 2-39
2.15.3 DS3XM-6 Port-Level Indicators 2-39
2.15.4 DS3XM-6 Card Specifications 2-39

2.16 OC3 IR 4 1310 Card 2-41
2.16.1 OC3 IR 4 1310 Card-Level Indicators 2-42
2.16.2 OC3 IR 4 1310 Port-Level Indicators 2-42
2.16.3 OC3 IR 4 1310 Card Specifications 2-43

2.17 OC12 IR 1310 Card 2-44
2.17.1 OC12 IR 1310 Card-Level Indicators 2-45
2.17.2 OC12 IR 1310 Port-Level Indicators 2-45
2.17.3 OC12 IR 1310 Card Specifications 2-45

2.18 OC12 LR 1310 Card 2-47
2.18.1 OC12 LR 1310 Card-Level Indicators 2-48
2.18.2 OC12 LR 1310 Port-Level Indicators 2-48
2.18.3 OC12 LR 1310 Card Specifications 2-48

2.19 OC12 LR 1550 Card 2-50
2.19.1 OC12 LR 1550 Card-Level Indicators 2-51
2.19.2 OC12 LR 1550 Port-Level Indicators 2-51
2.19.3 OC12 LR 1550 Card Specifications 2-51

2.20 OC48 IR 1310 Card 2-53
2.20.1 OC48 IR 1310 Card-Level Indicators 2-54
2.20.2 OC48 IR 1310 Port-Level Indicators 2-54
2.20.3 OC48 IR 1310 Card Specifications 2-54

2.21 OC48 LR 1550 Card 2-56
2.21.1 OC48 LR 1550 Card-Level Indicators 2-57
2.21.2 OC48 LR 1550 Port-Level Indicators 2-57
2.21.3 OC48 LR 1550 Card Specifications 2-57

2.22 OC48 ELR DWDM Cards 2-59
2.22.1 OC48 ELR Card-Level Indicators 2-60
2.22.2 OC48 ELR Port-Level Indicators 2-60
2.22.3 OC48 ELR Card Specifications 2-61

2.23 E100T-12 Card 2-62
2.23.1 E100T-12 Card-Level Indicators 2-63
2.23.2 E100T-12 Port-Level Indicators 2-63
2.23.3 E100T-12 Card Specifications 2-64

2.24 E1000-2 Card 2-65
2.24.1 E1000-2 Card-Level Indicators 2-66
2.24.2 E1000-2 Port-Level Indicators 2-66
2.24.3 E1000-2 Card Specifications 2-67

Using the Cisco Transport Controller 3-1

3.1 Overview 3-1

3.2 Preparing PCs to Run CTC 3-1
Procedure: Install Netscape Communicator (Windows) 3-2
Procedure: Install the Java Files (Windows) 3-2

3.3 Preparing Solaris Workstations to Run CTC 3-2
Procedure: Install qzip 3-3
Procedure: Install Netscape Navigator (Solaris) 3-3
Procedure: Install the Java Files (Solaris) 3-4

3.4 Connecting PCs to the ONS 15454 3-5
3.4.1 Direct Connections 3-5
Procedure: Setup a PC for Direct Connection 3-5
3.4.2 Local Area Network Connections 3-8
Procedure: Disable Proxy Service: Windows with Internet Explorer 3-8
Procedure: Disable Proxy Service: Windows with Netscape 3-9
3.4.3 Remote Access to the ONS 15454 3-9
3.4.4 Connecting to the ONS 15454 with TL1 Terminals 3-9

3.5 Logging into the ONS 15454 3-9
Procedure: Log into the ONS 15454 3-9

3.6 CTC Views 3-11
3.6.1 Node View 3-12
3.6.2 Network View 3-12
3.6.3 Card View 3-14

3.7 CTC Navigation 3-14

3.8 Viewing CTC Table Data 3-16

3.9 Viewing ONS 15454 Alarms 3-18
3.9.1 Controlling Alarm Display 3-19
3.9.2 Viewing Alarm History 3-19
3.9.3 Setting Up General Node Information 3-21
Procedure: Set Up General Node Information 3-21
Procedure: Convert Coordinates to Degrees, Minutes, and Seconds 3-21
3.9.4 Setting Up ONS 15454 Network Information 3-22
Procedure: Set Up Network Information 3-23
3.9.5 Setting Up ONS 15454 Security 3-24
Procedure: Create New Users 3-25
Procedure: Edit User Security 3-26
3.9.6 Creating Protection Groups 3-26
Procedure: Create Protection Groups 3-27
Procedure: Edit Protection Groups 3-28
Procedure: Delete Protection Groups 3-28
3.9.7 Setting Up ONS 15454 Timing 3-29
Procedure: Setup ONS 15454 Timing 3-31

3.10 Viewing ONS 15454 Inventory 3-33

3.11 Printing and Exporting CTC Data 3-34
Procedure: Print CTC Data 3-35
Procedure: Export CTC Data 3-35

3.12 Displaying CTC Data in Other Applications 3-36

Configuring Networks 4-1

4.1 Bidirectional Line Switched Rings 4-1
4.1.1 Sample BLSR Application 4-3
4.1.2 Setting Up BLSRs 4-6
Procedure: Install the Optical Carrier Cards 4-6
Procedure: Create the BLSR DCC Terminations 4-7
Procedure: Enable the Optical Card Ports 4-8
Procedure: Configure the BLSR 4-8
4.1.3 Adding and Dropping BLSR Nodes 4-10
Procedure: Add a BLSR Node 4-10
Procedure: Drop a BLSR Node 4-13
4.1.4 Moving BLSR Trunk Cards 4-14
Procedure: Move a BLSR Trunk Card 4-15

4.2 Unidirectional Path Switched Rings 4-17
4.2.1 Sample UPSR Application 4-19
4.2.2 Setting Up a UPSR 4-21
Procedure: Install the Optical Carrier Cards 4-21
Procedure: Configure the UPSR DCC Terminations 4-22
Procedure: Enable the UPSR Ports 4-23
4.2.3 Adding and Dropping UPSR Nodes 4-23
Procedure: Switch UPSR Traffic 4-24
Procedure: Add a UPSR Node 4-25
Procedure: Drop a Node 4-26

4.3 Subtending Rings 4-27
Procedure: Subtend a UPSR from a BLSR 4-29
Procedure: Subtend a BLSR from a UPSR 4-29

4.4 Creating a Linear ADM Configuration 4-30
Procedure: Create a Linear ADM 4-31
Procedure: Convert a Linear ADM to UPSR 4-32
Procedure: Convert a Linear ADM to a BLSR 4-35

4.5 Path Protected Mesh Networks 4-38

4.6 Creating and Provisioning Circuits 4-40
4.6.1 Cross Connect Card Capacities 4-40
4.6.2 VT Tunnels 4-41
Procedure: Create a Circuit 4-41
4.6.3 Creating Circuits With Multiple Drops 4-44
Procedure: Create a Circuit with Multiple Drops 4-44
4.6.4 Creating Monitor Circuits 4-45
Procedure: Set Up a Monitor Circuit 4-45
4.6.5 Editing UPSR Circuits 4-46
Procedure: Edit UPSR Circuits 4-46

4.7 DCC Tunneling 4-47
4.7.1 Creating DCC Tunnels 4-48
Procedure: Provision a DCC Tunnel 4-48

4.8 Loopbacks and Network Tests 4-50
4.8.1 Network Test Types 4-50
4.8.2 Network Test Procedures 4-51
Procedure: Perform a Facility Loopback on a Source DS-N Card 4-51
Procedure: Perform a Hairpin on a Source Node 4-54
Procedure: Perform a Hairpin on a Destination Node 4-56
Procedure: Perform a Terminal Loopback on a Destination DS-N Card 4-59
Procedure: Perform a Facility Loopback on a Destination DS-N Card 4-61

4.9 Managing Multiple ONS 15454 Rings 4-63
Procedure: Enable Multiple Ring Management 4-64

4.10 Creating Diagnostic Files 4-65
Procedure: Create a Diagnostic File 4-65

Provisioning Cards 5-1

5.1 Provisioning Electrical Cards 5-1
5.1.1 Card Settings 5-1
5.1.2 Provisioning DS3XM-6 Cards 5-4
Procedure: Set Up DS3XM-6 Protection Groups 5-5
Procedure: Provision the DS3XM-6 Ports 5-5

5.2 Provisioning Optical Cards 5-6

5.3 Provisioning the OC-3 Card for STM-1 5-8
Procedure: Provision the OC3 IR 4 1310 for STM-1 5-9

5.4 Provisioning the Alarm Interface Controller 5-9
5.4.1 Using Virtual Wires 5-11

Procedure: Provision External Alarms 5-11
Procedure: Provision External Controls 5-12
5.4.2 Provisioning AIC Orderwire 5-12
Procedure: Provision AIC Orderwire 5-13
5.4.3 Using the AIC Orderwire 5-14

5.5 Converting DS-1 and DS-3 Cards From 1:1 to 1:N Protection 5-14
Procedure: Convert DS1-14 Cards From 1:1 to 1:N Protection 5-14
Procedure: Convert DS3-12 Cards From 1:1 to 1:N Protection 5-16

5.6 Upgrading XC Cards to XCVT 5-18
Procedure: Upgrade XC Cards to XCVT 5-18

DWDM 6-1

6.1 DWDM Overview 6-1

6.2 DWDM Components 6-1
6.2.1 Optical Transmitters and Transponders 6-2
6.2.2 Optical Amplifiers 6-2
6.2.3 Optical Multiplexers and Demultiplexers 6-3
6.2.4 Optical Receivers 6-3
6.2.5 OADMs 6-3

6.3 DWDM Applications 6-3
6.3.1 Long Distance 6-3
6.3.2 Self-Healing Rings 6-3
6.3.3 Network Expansion 6-4

6.4 DWDM and the ONS 15454 6-4
6.4.1 ONS 15454 OC48 ELR ITU Optics 6-4
6.4.2 Using the ONS 15454 in a DWDM Network 6-4

Ethernet Applications 7-1

7.1 Ethernet over SONET Application 7-1

7.2 Router Aggregation Application 7-1

7.3 Transparent LAN Application 7-2

7.4 ONS 15454 Ethernet Cards 7-3
7.4.1 E100T 7-3
7.4.2 E1000-2 7-4

7.5 Virtual Local Area Networks (VLANs) 7-6
7.5.1 IEEE 802.1Q 7-6
7.5.2 IEEE 802.1Q Priority Queuing (formerly IEEE 802.1P) 7-8

7.6 Spanning Tree 7-10
Procedure: Enable Spanning Tree on Ethernet Ports 7-11
7.6.1 Spanning Tree Parameters 7-11
7.6.2 Spanning Tree Configuration 7-13
7.6.3 Viewing Spanning Tree 7-14
Procedure: View Spanning Tree 7-14

7.7 Multicard and Single-card EtherSwitch 7-15

7.8 ONS 15454 Ethernet Circuit Configurations 7-16
7.8.1 Multicard EtherSwitch Ethernet Circuit Provisioning 7-18
Procedure: Provision a Multicard Straight Ethernet Circuit 7-18
Procedure: Provision a Single Card Ethernet Straight Circuit 7-27
7.8.2 Shared Packet Ring Ethernet Circuit Provisioning 7-35
Procedure: Provision a Shared Packet Ring 7-35
7.8.3 Hub and Spoke Ethernet Circuit Provisioning 7-45
Procedure: Provision a Hub and Spoke Ethernet Circuit 7-46
7.8.4 Ethernet Manual Cross-Connects 7-54
Procedure: Provision a Single-card Etherswitch Manual Cross-Connect 7-54
Procedure: Provision a Multi-card Etherswitch Manual Cross-Connect 7-56

7.9 VLAN Membership and Ethernet Port Provisioning 7-59
Procedure: Provision Ethernet Ports for VLAN Membership 7-59
Procedure: Provision E1000-2 Ethernet Ports 7-61
Procedure: Provision E100T-12 Ethernet Ports 7-62

7.10 Ethernet Maintenance and Performance Screens 7-63
7.10.1 Statistics Screen 7-63
7.10.2 Line Utilization Screen 7-65
7.10.3 History Screen 7-65
7.10.4 Spanning Trees Screen 7-66
7.10.5 MAC Addresses Screen 7-67
7.10.6 Trunk Utilization Screen 7-68

7.11 Remote Monitoring Specification Alarm Thresholds 7-69
Procedure: Creating Ethernet Thresholds 7-71

7.12 Basic Ethernet Connectivity Testing 7-73
Procedure: Test Ethernet Connectivity 7-73

Network Management 8-1

8.1 Simple Network Management Protocol 8-1
8.1.1 SNMP Basic Components 8-2
8.1.2 SNMP Support 8-3
Procedure: Set up SNMP Support 8-3
8.1.3 SNMP MIBs 8-5
8.1.4 SNMP Traps 8-7
8.1.5 SNMP Community Names 8-8
8.1.6 SNMP Remote Network Monitoring 8-8

8.2 IP Address Entry Using Front Panel LCD 8-10
Procedure: Enter IP Address Using Front Panel LCD 8-10

8.3 Proxy ARP 8-12

8.4 IP Addressing and Subnets 8-13
8.4.1 Types of IP Addresses 8-14
8.4.2 Common IP Addressing Scenarios with the ONS 15454 8-14
Procedure: IP Checklist for Scenario 1 8-15
Procedure: IP Checklist for Scenario 2 8-16
Procedure: IP Checklist for Scenario 3 8-18
Procedure: IP Checklist for Scenario 4 8-20
Procedure: IP Checklist for Scenario 5 8-22

Procedure: IP Checklist for Scenario 6 8-24
Procedure: IP Checklist for Scenario 7 8-26

8.5 IP Troubleshooting 8-28

8.6 Static Route Provisioning 8-30
Procedure: Provision Static Routing to a Router Linked Workstation 8-30

CTC Alarms 9-1

9.1 Overview 9-1

9.2 AIS-L 9-5
9.2.1 OCN 9-5
9.2.2 EC-1 (AIS-L) 9-5

9.3 AIS-P 9-6
9.3.1 I/O 9-6

9.4 AISV 9-6
9.4.1 DS1, DS3XM-6 9-6

9.5 APSB 9-7
9.5.1 OCN 9-7

9.6 APSCIMP 9-7
9.6.1 OC-12 and OC-48 in BLSR 9-7

9.7 APSCM 9-8
9.7.1 OCN in linear mode 9-8

9.8 APSMM 9-9
9.8.1 OCN in linear mode 9-9

9.9 AUTORESET 9-9
9.9.1 Any Card 9-9

9.10 BKUPMEMP 9-10
9.10.1 TCC+ 9-10

9.11 BLSROOSYNC 9-11

9.12 CARLOSS 9-12
9.12.1 E100T-12, E1000-2 9-12

9.13 CONCAT 9-13
9.13.1 OCN 9-13

9.14 CONNLOS 9-14
9.14.1 OC-12 and OC-48 in BLSR 9-14

9.15 CONTBUS-A-X 9-15
9.15.1 Any Card 9-15

9.16 CONTBUS-A-18 9-16
9.16.1 TCC, TCC+ 9-16

9.17 CONTBUS-B-X 9-17
9.17.1 Any Card 9-17

9.18 CONTBUS-B-18 9-18

9.18.1 TCC/TCC+ 9-18

9.19 CTNEQPT-PBXPROT 9-19
9.19.1 I/O, XC/XCVT 9-19

9.20 CTNEQPT-PBXWORK 9-21
9.20.1 I/O, XC/XCVT 9-21

9.21 DATAFLT 9-23
9.21.1 TCC/TCC+ 9-23

9.22 DFLTK 9-23
9.22.1 OCN 9-23

9.23 DISCONNECTED 9-24

9.24 EOC 9-25
9.24.1 OCN 9-25

9.25 EQPT 9-26
9.25.1 Any Card 9-26

9.26 EXTERNAL 9-27
9.26.1 AIC 9-27

9.27 FAILTOSW-PATH 9-27
9.27.1 UPSR 9-27

9.28 FAN 9-29

9.29 FE-AIS 9-29
9.29.1 DS3XM-6 9-29

9.30 FE-DS1-MULTLOS 9-30
9.30.1 DS3XM-6 9-30

9.31 FE-DS1-SNGLLOS 9-31
9.31.1 DS3XM-6 9-31

9.32 FE-EQPT-FAIL-SA 9-31
9.32.1 DS3XM-6 9-31

9.33 FE-EQPT-NSA 9-32
9.33.1 DS3XM-6 9-32

9.34 FE-IDLE 9-32
9.34.1 DS3XM-6 9-32

9.35 FE-LOF 9-33
9.35.1 DS3XM-6 9-33

9.36 FE-LOS 9-33
9.36.1 DS3XM-6 9-33

9.37 FORCED-REQ 9-34
9.37.1 OCN in linear mode 9-34

9.38 FRNGSYNC 9-34

9.39 HITEMP 9-35

9.40 HLDOVERSYNC 9-35

9.41 IMPROPRMVL 9-36
9.41.1 Any Card 9-36

9.42 INCOMPATIBLE-SW 9-37

9.43 INCON 9-38
9.43.1 OC-12 and OC-48 in BLSR 9-38

9.44 LANOVERFLOW 9-38
9.44.1 TCC/TCC+ 9-38

9.45 LBKFACILITY 9-39
9.45.1 OCN 9-39

9.46 LPBKTERMINAL 9-39
9.46.1 OCN 9-39

9.47 LOCKOUTOFPR-RING 9-40
9.47.1 OC-12 and OC-48 in BLSR 9-40

9.48 LOF 9-41
9.48.1 DS3XM-6 9-41
9.48.2 TCC/TCC+ (LOF) 9-41
9.48.3 DS1 (LOF) 9-43
9.48.4 OCN (LOF) 9-44
9.48.5 EC-1 (LOF) 9-45

9.49 LOP 9-46
9.49.1 I/O 9-46

9.50 LOP-V 9-47
9.50.1 DS3XM-6, DS1 9-47

9.51 LOS 9-48
9.51.1 DS3, DS3XM-6, DS1 9-48
9.51.2 OCN (LOS) 9-49
9.51.3 EC-1 (LOS) 9-50

9.52 LPBKDS1FEAC 9-50
9.52.1 DS3XM-6 9-50

9.53 LPBKDS3FEAC 9-51
9.53.1 DS3XM-6 9-51

9.54 LPBKFACILITY 9-51
9.54.1 DS3, DS3XM-6 9-51
9.54.2 DS1 (LPBKFACILITY) 9-52

9.55 LPBKTERMINAL 9-53
9.55.1 DS3, DS3XM-6 9-53
9.55.2 DS1 (LPBKTERMINAL) 9-53

9.56 MANRESET 9-54
9.56.1 Any Card 9-54

9.57 MANUAL-REQ 9-54
9.57.1 OCN (Not OC3) 9-54
9.57.2 XC/XCVT (MANUAL-REQ) 9-55

9.58 MEA 9-56
9.58.1 XC, I/O 9-56

9.59 MEM-GONE 9-57
9.59.1 TCC/TCC+ 9-57

9.60 MEM-LOW 9-57
9.60.1 TCC/TCC+ 9-57

9.61 NODEMIS 9-58
9.61.1 OC-12 and OC-48 in BLSR 9-58

9.62 NOT-AUTHENTICATED 9-59

9.63 PDI-P 9-59
9.63.1 DS3, DS3XM-6, DS1 9-59

9.64 PLM-P 9-60
9.64.1 DS3, DS3XM-6, DS1 9-60

9.65 PLM-V 9-62
9.65.1 DS1, DS3XM-6 9-62

9.66 PWRRESTART 9-62

9.67 RAI 9-63
9.67.1 DS3XM-6 9-63

9.68 RCVRMISS 9-63
9.68.1 DS1 9-63

9.69 RFI-L 9-64
9.69.1 OCN, EC-1 9-64

9.70 RFI-P 9-64
9.70.1 DS3, DS3XM-6, DS1, E100-T12, E1000-2 9-64

9.71 RFI-V 9-65
9.71.1 DS3XM-6, DS1 9-65

9.72 SDBER 9-66
9.72.1 OCN 9-66

9.73 SFBER 9-67
9.73.1 OCN 9-67

9.74 SQUELCH 9-68

9.75 STU 9-68

9.76 SWTOPRI 9-69

9.77 SWTOSEC 9-69

9.78 SWTOTHIRD 9-69

9.79 SWTRANSFER 9-70
9.79.1 TCC/TCC+ 9-70

9.80 SYNCPRI 9-70
9.80.1 TCC/TCC+ 9-70

9.81 SYNCSEC 9-71
9.81.1 TCC/TCC+ 9-71

9.82 SYNCTHIRD 9-71
9.82.1 TCC/TCC+ 9-71

9.83 SYSBOOT 9-72
9.83.1 TCC/TCC+ 9-72

9.84 TRMTMISS 9-73
9.84.1 DS1 9-73

9.85 UNEQ-P 9-73
9.85.1 I/O 9-73

9.86 UNEQ-V 9-74
9.86.1 DS1, DS3XM-6 9-74

Maintenance 10-1

10.1 Air Filter Inspection 10-1
10.1.1 Reusable Air Filter 10-1
Procedure: Inspecting and Cleaning the Reusable Air Filter 10-2
10.1.2 Disposable Air Filter 10-3
Procedure: Inspecting and Replacing the Disposable Air Filter 10-3

10.2 System Reset 10-5
Procedure: Performing a Soft Reset 10-6
Procedure: Performing a Hard Reset 10-6

10.3 Database Backup and Restore 10-7
Procedure: Backup the Database 10-7
Procedure: Restoring the Database 10-8

10.4 Revert To Earlier Software Load 10-10
Procedure: Revert To Earlier Software Load 10-10

10.5 Card Replacement 10-11

10.6 TCC Card to TCC+ Card Upgrade 10-11
Procedure: Upgrade the TCC Card to the TCC+ Card 10-11

10.7 Electrical Interface Assembly Replacement 10-13
10.7.1 EIA Types 10-13
10.7.2 Replacement Procedures 10-14
Procedure: Remove the Backplane Cover or EIA 10-14
Procedure: Install the BNC EIAs 10-14

10.8 Fiber Cleaning 10-15

TL1 Reference 11-1

11.1 Overview 11-1

11.2 Craft Interface 11-1

11.3 TL1 Access using Telnet 11-1

11.4 Alarms 11-1

11.4.1 Equipment Alarms 11-2
11.4.2 OC-N Alarms 11-4
11.4.3 DS-3 Alarms 11-6
11.4.4 DS-1 Alarms 11-7
11.4.5 STS Alarms 11-8
11.4.6 VT Termination Alarms 11-9
11.4.7 BITS Alarms 11-9
11.4.8 Network Element Synch Ref Alarms 11-10

11.5 Autonomous Messages 11-11

11.6 Performance Monitoring 11-11
11.6.1 Performance Monitoring Statistics 11-11

11.7 TL1 Command Syntax 11-14

11.8 TL1 Command Privilege Map 11-14

11.9 TL1 Command List 11-15
11.9.1 Cross Connect 11-15
11.9.2 Environment 11-16
11.9.3 Equipment 11-16
11.9.4 Facility 11-16
11.9.5 Facility Protection 11-16
11.9.6 Fault 11-17
11.9.7 Log 11-17
11.9.8 Performance 11-17
11.9.9 Security 11-17
11.9.10 Switch 11-17
11.9.11 Synchronization 11-17
11.9.12 System 11-18
11.9.13 Testing 11-18
11.9.14 Other 11-18

11.10 TL1 Command Index 11-19

11.11 TL1 Command Description 11-21

11.12 Access Identifiers 11-92
11.12.1 bits 11-93
11.12.2 ds-1 11-93
11.12.3 env 11-93
11.12.4 eqpt 11-94
11.12.5 facility 11-94
11.12.6 sts 11-94
11.12.7 syn_src 11-95
11.12.8 sync_ref 11-95
11.12.9 vt1_5 11-95

11.13 Parameter Types 11-95
11.13.1 ATAG Description 11-95
11.13.2 CTAG Description 11-96
11.13.3 TID Description 11-96
11.13.4 ALL_MONTYPE 11-97
11.13.5 ALL_THR 11-98

11.13.6 CCT 11-99
11.13.7 COND_EFF 11-99
11.13.8 CONDITION 11-99
11.13.9 DIRECTION 11-107
11.13.10 DS3_FMT 11-107
11.13.11 DS_LINE_CODE 11-108
11.13.12 DS_LINE_TYPE 11-108
11.13.13 DX_MODE_OP 11-108
11.13.14 E_LBO 11-108
11.13.15 ENV_ALM 11-109
11.13.16 ENV_CTL 11-110
11.13.17 EQPT_TYPE 11-110
11.13.18 EQUIP 11-111
11.13.19 EQUIPMENT_TYPE 11-112
11.13.20 EXT_RING 11-112
11.13.21 FRAME_FORMAT 11-112
11.13.22 LINE_BUILDOUT 11-113
11.13.23 LINE_CODE 11-113
11.13.24 LOCATION 11-113
11.13.25 LPBK_TYPE 11-113
11.13.26 MOD2 11-114
11.13.27 MOD2ALM 11-114
11.13.28 MOD2B 11-115
11.13.29 MODIFIER 11-115
11.13.30 NOTIF_CODE 11-116
11.13.31 OCN_MONTYPE 11-116
11.13.32 OCN_TYPE 11-116
11.13.33 ON_OFF 11-117
11.13.34 OPTICAL_MODE 11-117
11.13.35 PRIVILEGE 11-117
11.13.36 PROT_MOD_OP 11-117
11.13.37 PROTECTION_GROUP 11-118
11.13.38 PST 11-118
11.13.39 REVERTIVE_TIME 11-118
11.13.40 REVERTIVE_TYPE 11-118
11.13.41 RNG_TYPE 11-118
11.13.42 SD_BER 11-119
11.13.43 SDCC_MODE 11-119
11.13.44 SERV_EFF 11-119
11.13.45 SF_BER 11-119
11.13.46 SIDE 11-119
11.13.47 STATE 11-120
11.13.48 STATUS 11-120
11.13.49 STM_TYPE 11-120
11.13.50 STS_MONTYPE 11-120
11.13.51 STS_PATH 11-121
11.13.52 SWITCH 11-121
11.13.53 SYNC_GENERATION 11-121
11.13.54 SYNC_MODE 11-121
11.13.55 SYNC_QUALITY_LEVEL 11-122
11.13.56 TIMING_MODE 11-122

11.13.57 TMG_REF 11-122
11.13.58 TMPR 11-123
11.13.59 USE_DST 11-123
11.13.60 VALIDITY 11-123
11.13.61 Performance Monitoring Parameters by Line Type 11-124

11.14 Errors 11-124

11.15 Echo 11-129

Regulatory and Compliance Requirements A-1

A.1 Overview A-1
A.1.1 Emissions/Immunity A-1
A.1.2 Safety A-1
A.1.3 Environmental/Mechanical A-1

Glossary B-1

Acronyms C-1

Index I-1

FIGURES

Figure 1-1 Dimensions 1-4

Figure 1-2 Rack Mount 1-5

Figure 1-3 Four Shelf System 1-8

Figure 1-4 Four Shelf ONS 15454 Bay Assembly 1-9

Figure 1-5 Front Door 1-10

Figure 1-6 Door Hinge 1-11

Figure 1-7 Erasable Label on the Inside Door 1-12

Figure 1-8 Front Panel Cable Management 1-13

Figure 1-9 Bottom Bracket Installation 1-15

Figure 1-10 Fan Tray Filter Replacement 1-15

Figure 1-11 Fan Tray Assembly 1-16

Figure 1-12 LCD Panel 1-17

Figure 1-13 Backplane Sheet Metal Covers 1-18

Figure 1-14 BNC Backplane 1-20

Figure 1-15 High-density BNC Backplane 1-21

Figure 1-16 SMB Backplane 1-22

Figure 1-17 AMP CHAMP Backplane 1-23

Figure 1-18 Lower Backplane Cover 1-24

Figure 1-19 Power Terminals 1-28

Figure 1-20 Pinouts 1-29

Figure 1-21 Ferrites for Power Cables 1-32

Figure 1-22 Ferrites for AMP CHAMP Connectors 1-33

Figure 1-23 Ferrites for Electrical Interface Assemblies (EIAs) or Baluns 1-33

Figure 1-24 Ferrites for SMB/BNC Connectors 1-34

Figure 1-25 Ferrites for Pin Field 1-34

Figure 1-26 Card Installation 1-35

Figure 1-27 Gigabit Interface Converter 1-39

Figure 1-28 GBIC Installation 1-40

Figure 1-29 Fiber Cable Connection 1-42

Figure 1-30 Fiber Boot Attachment 1-43

Figure 1-31 BNC Backplane Connection Using a Right Angle Connector 1-44

Figure 1-32 SMB Coaxial Cable Connections 1-46

Figure 1-33 Electrical Interface Adapter 1-47

Figure 1-34 Backplane With SMB EIA 1-48

Figure 1-35 Cable Routing 1-50
Figure 1-36 Fold-down Front Door of the Shelf Assembly 1-51
Figure 1-37 Backplane Cable Routing 1-52
Figure 1-38 Clear BIC Rear Cover 1-53
Figure 1-39 Backplane Attachment For BIC Cover 1-54
Figure 2-1 1:1 Protection Configuration 2-2
Figure 2-2 1:N Protection Configuration 2-3
Figure 2-3 Unprotected Configuration 2-6
Figure 2-4 TCC Faceplate 2-7
Figure 2-5 TCC Block Diagram 2-9
Figure 2-6 XC Card Faceplate 2-11
Figure 2-7 Cross-Connect Matrix 2-12
Figure 2-8 XC Block Diagram 2-13
Figure 2-9 XCVT Faceplate 2-14
Figure 2-10 XCVT Cross-Connect Matrix 2-15
Figure 2-11 XCVT Block Diagram 2-17
Figure 2-12 AIC Faceplate 2-19
Figure 2-13 AIC Block Diagram 2-22
Figure 2-14 EC1-12 Faceplate 2-23
Figure 2-15 EC1-12 Block Diagram 2-24
Figure 2-16 DS1-14 Faceplate 2-26
Figure 2-17 DS1-14 Block Diagram 2-27
Figure 2-18 DS1N-14 Faceplate 2-29
Figure 2-19 DS1N-14 Block Diagram 2-30
Figure 2-20 DS3-12 Faceplate 2-32
Figure 2-21 DS3-12 Block Diagram 2-33
Figure 2-22 DS3N-12 Faceplate 2-35
Figure 2-23 DS3N-12 Block Diagram 2-36
Figure 2-24 DS3XM-6 Faceplate 2-38
Figure 2-25 DS3XM-6 Block Diagram 2-39
Figure 2-26 OC3 IR 4 1310 Faceplate 2-41
Figure 2-27 OC3 IR 4 1310 Block Diagram 2-42
Figure 2-28 OC12 IR 1310 Faceplate 2-44
Figure 2-29 OC12 IR 1310 Block Diagram 2-45

Figure 2-30 OC12 LR 1310 Faceplate 2-47
Figure 2-31 OC12 LR 1310 Block Diagram 2-48
Figure 2-32 OC12 LR 1550 Faceplate 2-50
Figure 2-33 OC12 LR 1550 Block Diagram 2-51
Figure 2-34 OC48 IR 1310 Faceplate 2-53
Figure 2-35 OC48 IR 1310 Block Diagram 2-54
Figure 2-36 OC48 LR 1550 Faceplate 2-56
Figure 2-37 OC48 LR Block Diagram 2-57
Figure 2-38 OC48 ELR DWDM Card Faceplate 2-59
Figure 2-39 OC48 ELR Block diagram 2-60
Figure 2-40 E100T-12 Faceplate 2-62
Figure 2-41 E100T-12 Block Diagram 2-63
Figure 2-42 E1000-2 Card Faceplate 2-65
Figure 2-43 E1000-2 Block Diagram 2-67
Figure 3-1 Network Dialog 3-6
Figure 3-2 IP Address Window 3-7
Figure 3-3 TCP/IP Properties - Gateway Tab (Windows 95/98) 3-7
Figure 3-4 Login Screen 3-10
Figure 3-5 CTC Window Elements 3-11
Figure 3-6 Network View 3-13
Figure 3-7 Card View 3-14
Figure 3-8 CTC Popup Information 3-15
Figure 3-9 Table Column Shortcut Menu 3-17
Figure 3-10 Alarms Tab 3-18
Figure 3-11 History>Session Subtab 3-20
Figure 3-12 History>Node Subtab 3-20
Figure 3-13 Provisioning>Network Subtab 3-23
Figure 3-14 Create User Dialog 3-25
Figure 3-15 Create Protection Group Dialog (1+1) 3-27
Figure 3-16 Provisioning>Protection Subtab 3-28
Figure 3-17 ONS 15454 Timing Example 3-30
Figure 3-18 Provisioning>Timing Subtab 3-32
Figure 3-19 Inventory Tab 3-33
Figure 3-20 CTC Print Dialog 3-35

Figure 3-21 CTC Export Dialog 3-36
Figure 4-1 Four-Node, Two-Fiber OC-48 BLSR 4-2
Figure 4-2 BLSR Bandwidth Reuse 4-3
Figure 4-3 Sample BLSR Application 4-4
Figure 4-4 Sample Shelf Layout for Node 0 in Figure 4-3 4-5
Figure 4-5 Sample Shelf Layout for Nodes 1-4 in Figure 4-3 4-5
Figure 4-6 Two Node OC-48 BLSR 4-6
Figure 4-7 Sample Shelf Setup for Two Node BLSR 4-7
Figure 4-8 Line Subtab 4-8
Figure 4-9 Ring Subtab 4-9
Figure 4-10 Three Node BLSR Example 4-10
Figure 4-11 BLSR Example with Added Fourth Node 4-12
Figure 4-12 BLSR Trunk Card Switchover Example 4-14
Figure 4-13 Circuits Tab 4-16
Figure 4-14 Basic UPSR Configuration 4-18
Figure 4-15 UPSR Fiber Break 4-18
Figure 4-16 Sample OC-3 UPSR Application 4-19
Figure 4-17 Node ID 0 Layout for Sample OC-3 UPSR 4-20
Figure 4-18 Node ID 1-3 Layout for Sample OC-3 UPSR 4-20
Figure 4-19 Sample Two Node OC-48 UPSR 4-21
Figure 4-20 Sample Two Node OC-48 UPSR Shelf Setup 4-22
Figure 4-21 Three Node UPSR 4-23
Figure 4-22 Span Shortcut Menu 4-24
Figure 4-23 Circuits on Span Dialog 4-25
Figure 4-24 UPSR Example With Fourth Node 4-26
Figure 4-25 ONS 15454 With Multiple Subtending Rings 4-28
Figure 4-26 Multiple Subtending Rings 4-28
Figure 4-27 Create SDCC Termination dialog 4-29
Figure 4-28 Linear ADM 4-31
Figure 4-29 Maintenance>Protection Subtab 4-32
Figure 4-30 Provisioning>Protection Subtab 4-33
Figure 4-31 Linear to UPSR Conversion 4-33
Figure 4-32 Network View with Ring 4-35
Figure 4-33 Linear to BLSR Conversion 4-36

Figure 4-34 Path Protected Mesh Network Example 4-39
Figure 4-35 PPMN Virtual Ring 4-39
Figure 4-36 Circuit Creation Dialog 4-42
Figure 4-37 Circuit Path Selection Dialog 4-43
Figure 4-38 Monitor Circuit Example 4-45
Figure 4-39 Monitors Tab 4-45
Figure 4-40 Edit Circuit Dialog - UPSR Tab 4-46
Figure 4-41 DCC Tunnel Example 4-48
Figure 4-42 Create DCC Tunnel Connection Dialog 4-49
Figure 4-43 The facility loopback process 4-50
Figure 4-44 The terminal loopback process 4-50
Figure 4-45 The hairpin circuit process 4-51
Figure 4-46 Facility loopback on a source DS-N card 4-51
Figure 4-47 Performing a facility loopback 4-52
Figure 4-48 Hairpin on a source node 4-54
Figure 4-49 Hairpin on a destination node 4-56
Figure 4-50 Terminal loopback on a destination DS-N card 4-60
Figure 4-51 Facility loopback on a destination DS-N card 4-61
Figure 4-52 CTC Multiple Ring Management 4-64
Figure 5-1 Line Subtab 5-1
Figure 5-2 Port Provisioning (DS3XM-6 Card) 5-6
Figure 5-3 Thresholds Subtab - OC12 IR 1310 Card 5-7
Figure 5-4 AIC Alarm Input and Output 5-10
Figure 5-5 AIC Provisioning Tab - External Alarms Subtab 5-10
Figure 5-6 AIC Virtual Wire Example 5-11
Figure 5-7 AIC - Local Orderwire Subtab 5-13
Figure 5-8 Protection Group Slot Status 5-15
Figure 5-9 ONS 15454 with XC Cards 5-18
Figure 5-10 Active XC Card 5-19
Figure 5-11 XC Cards Subtab 5-19
Figure 6-1 DWDM System 6-2
Figure 6-2 DWDM Ring Application 6-5
Figure 6-3 Survivable Network 6-6
Figure 7-1 Router Aggregation Application 7-2

Figure 7-2 Transparent LAN Application 7-3
Figure 7-3 E100T Card, Front view 7-4
Figure 7-4 E1000-2 Card, Front view 7-5
Figure 7-5 Q-tag 7-7
Figure 7-6 Priority Queuing 7-9
Figure 7-7 Spanning Tree Blocked Path 7-10
Figure 7-8 Enabling Spanning Tree 7-11
Figure 7-9 Spanning Tree Parameters 7-12
Figure 7-10 Spanning Tree Configuration 7-13
Figure 7-11 Circuit Screen 7-14
Figure 7-12 Multicard EtherSwitch 7-15
Figure 7-13 Single-card EtherSwitch 7-15
Figure 7-14 Card Mode 7-16
Figure 7-15 Straight Circuit Configuration 7-17
Figure 7-16 Shared Packet Ring Ethernet Circuit Configuration 7-17
Figure 7-17 Hub and Spoke Ethernet Circuit Configuration 7-18
Figure 7-18 Multicard Straight Circuit 7-19
Figure 7-19 Card Mode Window 7-20
Figure 7-20 Circuit Attributes Dialog 7-21
Figure 7-21 Circuit Source 7-22
Figure 7-22 Circuit Destination 7-23
Figure 7-23 Define New VLAN Dialog 7-24
Figure 7-24 Circuit VLAN Selection 7-25
Figure 7-25 Circuit Confirmation 7-26
Figure 7-26 Single-card Straight Circuit 7-27
Figure 7-27 Single-card EtherSwitch Screen 7-28
Figure 7-28 Circuit AttributesDialog 7-29
Figure 7-29 Circuit Source 7-30
Figure 7-30 Circuit Destination 7-31
Figure 7-31 Define New VLAN Dialog 7-32
Figure 7-32 Circuit VLAN Selection 7-33
Figure 7-33 Circuit Confirmation 7-34
Figure 7-34 Shared Packet Ring 7-35
Figure 7-35 Multicard EtherSwitch Group 7-36

Figure 7-36 Circuit Attributes Dialog 7-37
Figure 7-37 Circuit Source Dialog 7-38
Figure 7-38 Circuit VLAN Selection 7-39
Figure 7-39 Circuit Path Selection 7-40
Figure 7-40 Circuit Path Selection (all spans) 7-41
Figure 7-41 Circuit Creation 7-42
Figure 7-42 Highlighted Circuit Path 7-43
Figure 7-43 Edit Circuit Dialog Box 7-44
Figure 7-44 Completed Shared Packet Ring Circuit 7-45
Figure 7-45 Hub and Spoke Ethernet Circuit 7-46
Figure 7-46 Single-card EtherSwitch Screen 7-47
Figure 7-47 Circuit Attributes Dialog 7-48
Figure 7-48 Circuit Source 7-49
Figure 7-49 Circuit VLAN Selection 7-50
Figure 7-50 Selected VLANs 7-51
Figure 7-51 Circuit Confirmation 7-52
Figure 7-52 Ethernet manual cross-connects 7-54
Figure 7-53 Creating an Ethernet circuit 7-54
Figure 7-54 Selecting VLANs 7-56
Figure 7-55 Creating an Ethernet circuit 7-57
Figure 7-56 Selecting VLANs 7-58
Figure 7-57 VLAN Port Provisioning Screen 7-60
Figure 7-58 Port Provisioning Screen 7-61
Figure 7-59 Port Provisioning Screen 7-62
Figure 7-60 Ethernet Statistics 7-64
Figure 7-61 Line Utilization 7-65
Figure 7-62 Ethernet History 7-66
Figure 7-63 Spanning Tree Topology 7-67
Figure 7-64 MAC Addresses Discovered 7-67
Figure 7-65 MAC Forwarding Table 7-68
Figure 7-66 Trunk Utilization 7-69
Figure 7-67 Ethernet Alarm Screen 7-71
Figure 7-68 Ethernet Alarm Thresholds 7-72
Figure 7-69 Ethernet Connectivity Reference 7-73

Figure 8-1 Basic Network Managed by SNMP 8-1
Figure 8-2 SNMP Operations 8-2
Figure 8-3 SNMP Components 8-3
Figure 8-4 Create SNMP Trap Destination Dialog 8-4
Figure 8-5 Trap Destinations Screen 8-5
Figure 8-6 Front Panel LCD 8-10
Figure 8-7 IP Address Option 8-10
Figure 8-8 IP Address LCD Screen 8-11
Figure 8-9 Save Configuration Option LCD Screen 8-11
Figure 8-10 Save and REBOOT LCD Screen 8-11
Figure 8-11 Saving Changes LCD Screen 8-11
Figure 8-12 ONS 15454 Network Using Proxy ARP 8-13
Figure 8-13 IP Addressing Scenario 1 8-15
Figure 8-14 IP Addressing Scenario 2 8-16
Figure 8-15 IP Addressing Scenario 3 8-18
Figure 8-16 IP Addressing Scenario 4 8-20
Figure 8-17 IP Addressing Scenario 5 8-22
Figure 8-18 IP Addressing Scenario 6 8-24
Figure 8-19 IP Addressing Scenario 7 8-26
Figure 8-20 Create Static Route Window 8-31
Figure 8-21 Static Route Window 8-32
Figure 10-1 Reusable Fan Tray Filter in an External Filter Bracket 10-2
Figure 10-2 Fan Tray Assembly 10-4
Figure 10-3 Air Filter 10-5
Figure 10-4 Soft Reset 10-6
Figure 10-5 Database Backup Screen 10-8
Figure 10-6 File Received Dialog 10-8
Figure 10-7 Database Backup Screen 10-9
Figure 10-8 File Transfer Dialog 10-9
Figure 10-9 Soft Reset 10-12
Figure 10-10 BNC Insertion and Removal Tool 10-15
Figure 11-1 Autonomous Alarm Message Format 11-11

TABLES

Table 1-1 External Timing Pin Assignments for BITS 1-30

Table 1-2 LAN Pin Assignments 1-31

Table 1-3 Craft Interface Pin Assignments 1-31

Table 1-4 Slot and Card Symbols 1-36

Table 1-5 Card Ports, Line Rates, and Connectors 1-37

Table 1-6 Available GBICs 1-39

Table 1-7 Pin Assignments for AMP Champ Connector 1-49

Table 1-8 Installation Checklist 1-57

Table 1-9 Node Turn Up Checklist 1-59

Table 1-10 ONS 15454 Software and Hardware Compatibility 1-61

Table 2-1 ONS 15454 VT Mapping 2-15

Table 3-1 Node View Card Colors 3-12

Table 3-2 Node View Tabs and Subtabs 3-12

Table 3-3 Node Status 3-13

Table 3-4 Network View Actions 3-13

Table 3-5 CTC Window Navigation 3-15

Table 3-6 Table Display Options 3-17

Table 3-7 Alarm Data 3-18

Table 3-8 Alarm Colors 3-19

Table 3-9 Alarm Display 3-19

Table 3-10 ONS 15454 Security Levels 3-24

Table 3-11 ONS 15454 Security Idle Times 3-25

Table 3-12 Protection Types 3-26

Table 3-13 SSM Generation 1 Message Set 3-30

Table 3-14 SSM Generation 2 Message Set 3-31

Table 3-15 CTC Table Data 3-34

Table 4-1 Two-Fiber BLSR Capacity 4-2

Table 4-2 XC and XCVT Card Capacity: STSs (Bidirectional) 4-40

Table 4-3 XC and XCVT Card Capacity: VT1.5s (Bidirectional) 4-40

Table 4-4 VT Use Example 4-41

Table 4-5 DCC Tunnels 4-47

Table 5-1 Line Settings - Electrical 5-2

Table 5-2 Threshold Settings - Electrical 5-2

Table 5-3 Threshold Settings - DS3XM-6 Card 5-4

Table 5-4 Line Settings - Optical 5-7
Table 5-5 Threshold Settings - Optical 5-8
Table 7-1 E100T Ethernet Port LED States 7-4
Table 7-2 E1000-2 Ethernet Port LED States 7-6
Table 7-3 Priority Queuing 7-8
Table 7-4 Spanning Tree Parameters 7-12
Table 7-5 Spanning Tree Configuration 7-13
Table 7-6 Port Settings 7-60
Table 7-7 Ethernet Parameters 7-64
Table 7-8 Ethernet Threshold Variables (MIBs) 7-70
Table 8-1 SNMP Manager Operations 8-6
Table 8-2 IETF Standard MIBs Implemented in the ONS 15454 SNMP Agent 8-6
Table 8-3 SNMP Trap Variable Bindings 8-7
Table 8-4 Generic Traps Supported in the ONS 15454 8-7
Table 8-5 IETF Traps Supported by the ONS 15454 8-8
Table 8-6 IP Troubleshooting Solutions 8-28
Table 9-1 Alarm Index 9-2
Table 9-2 Entity Alarms, Equipment Alarms and Common Equipment Alarms 9-76
Table 9-3 Threshold Crossing Events (EVTs) 9-79
Table 9-4 Additional Events (EVTs) 9-80
Table 10-1 EIA Configurations 10-13
Table 11-1 Equipment Alarms 11-2
Table 11-2 OC-N Alarms 11-4
Table 11-3 DS-3 Alarms 11-6
Table 11-4 DS-1 Alarms 11-7
Table 11-5 STS Alarms 11-8
Table 11-6 VT Termination Alarms 11-9
Table 11-7 Bits Alarms 11-9
Table 11-8 Synch Ref Alarms 11-10
Table 11-9 PM Statistics 11-11
Table 11-10 Command Access 11-15
Table 11-11 Security Idle Times 11-15
Table 11-12 Command Index 11-19
Table 11-13 Access Identifiers 11-92

Table 11-14 bits 11-93
Table 11-15 ds-1 11-93
Table 11-16 env 11-94
Table 11-17 eqpt 11-94
Table 11-18 facility 11-94
Table 11-19 sts 11-94
Table 11-20 sync_src 11-95
Table 11-21 sync_ref 11-95
Table 11-22 vt1_5 11-95
Table 11-23 ALL_MONTYPE Values 11-97
Table 11-24 ALL_THR Value 11-98
Table 11-25 CCT Values 11-99
Table 11-26 COND_EFF Values 11-99
Table 11-27 CONDITION Values 11-99
Table 11-28 DIRECTION Values 11-107
Table 11-29 DS3_FMT Values 11-107
Table 11-30 DS_LINE_CODE Values 11-108
Table 11-31 DS_LINE_TYPE Values 11-108
Table 11-32 DX_MODE_OP Values 11-108
Table 11-33 E_LBO Values 11-108
Table 11-34 ENV_ALM Values 11-109
Table 11-35 ENV_CTL Values 11-110
Table 11-36 EQPT_TYPE Values 11-110
Table 11-37 EQUIP Values 11-111
Table 11-38 EQUIPMENT_TYPE Values 11-112
Table 11-39 EXT_RING Values 11-112
Table 11-40 FRAME_FORMAT Values 11-112
Table 11-41 LINE_BUILDOUT Values 11-113
Table 11-42 LINE_CODE Values 11-113
Table 11-43 LOCATION Values 11-113
Table 11-44 LPBK_TYPE Values 11-113
Table 11-45 MOD2 Values 11-114
Table 11-46 MOD2ALM Values 11-114
Table 11-47 MOD2B Values 11-115

Table 11-48 MODIFIER Values 11-115
Table 11-49 NOTIF_CODE Values 11-116
Table 11-50 OCN_MONTYPE Values 11-116
Table 11-51 OCN_TYPE Values 11-116
Table 11-52 ON_OFF Values 11-117
Table 11-53 OPTICAL_MODE Values 11-117
Table 11-54 PRIVILEGE Values 11-117
Table 11-55 PROT_MOD_OP Values 11-117
Table 11-56 PROTECTION_GROUP Values 11-118
Table 11-57 PST Values 11-118
Table 11-58 REVERTIVE_TIME Values 11-118
Table 11-59 REVERTIVE_TYPE Values 11-118
Table 11-60 RNG_TYPE Values 11-118
Table 11-61 SD_BER Values 11-119
Table 11-62 SDCC_MODE Values 11-119
Table 11-63 SERV_EFF Values 11-119
Table 11-64 SF_BER Values 11-119
Table 11-65 SIDE Values 11-119
Table 11-66 STATE Values 11-120
Table 11-67 Status Values 11-120
Table 11-68 STM_TYPE Values 11-120
Table 11-69 STS_MONOTYPE Values 11-120
Table 11-70 STS_PATH Values 11-121
Table 11-71 SWITCH Values 11-121
Table 11-72 SYNC_GENERATION Values 11-121
Table 11-73 SYNC_MODE Values 11-121
Table 11-74 SYNC_QUALITY_LEVEL Values 11-122
Table 11-75 TIMING_MODE Values 11-122
Table 11-76 TMG_REF Values 11-122
Table 11-77 TMPR Values 11-123
Table 11-78 USE_DST Values 11-123
Table 11-79 VALIDITY Values 11-123
Table 11-80 Performance Monitoring Parameters by Line Type 11-124
Table 11-81 Error Codes 11-125

About This Manual

This section explains who should read the *Cisco ONS 15454 User Documentation Release 2.2.1*, how it is organized, related documentation, and document conventions.

Audience

This guide is for Cisco ONS 15454 installation technicians and administrators who are responsible for configuring, maintaining, and enhancing ONS 15454 networks.

Organization

Chapter	Title	Description
Chapter 1	Installation	Provides installation procedures for all ONS 15454 hardware components
Chapter 2	Card Reference	Describes all ONS 15454 cards, including their features, protection methods, and specifications
Chapter 3	Using the Cisco Transport Controller	Explains how to set up the ONS 15454 software
Chapter 4	Configuring Networks	Contains procedures for configuring ONS 15454 rings and circuits
Chapter 5	Provisioning Cards	Explains how to use the CTC to configure ONS 15454 electrical cards, optical cards, and the Alarm Interface Controller card
Chapter 6	DWDM	Provides a description of dense wavelength division multiplexing and explains how the ONS 15454 uses DWDM to increase bandwidth
Chapter 7	Ethernet Applications	Describes how to use the Ethernet features of the ONS 15454
Chapter 8	Network Management	Explains the different protocols used to manage ONS 15454 networks
Chapter 9	CTC Alarms	Lists the alarms generated by the ONS 15454 that can be viewed using the CTC
Chapter 10	Maintenance	Describes miscellaneous operations that the ONS 15454 requires after installation

Chapter	Title	Description
Chapter 11	TL1 Reference	Lists TL1 alarms, commands, and autonomous messages supported by the Cisco ONS 15454
Appendix A	Regulatory and Compliance Requirements	Lists customer, industry, and government requirements met by the Cisco ONS 15454
Appendix B	Glossary	Defines commonly-used terms
Appendix C	Acronyms	Defines commonly-used acronyms

Related Documentation

Cisco ONS 15454 Release 2.2.1 Release Notes

Cisco ONS 15454 Product Overview

Cisco Warranty Services for ONG Products

Cisco ONS 15454 Quick Configuration Guide

Cisco ONS 15454 Quick Installation Guide

Related products:

Installing the Cisco ONS 15516 DWDM Filters

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.

Tips 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
Italic	Field where the user enters a value

>	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 *Cisco ONS 15454 User Documentation, Release 2.2.1*, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM, a member of the Cisco Connection Family, is updated as required. Therefore, it might be more current than printed documentation. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www.europe.cisco.com.

Ordering Documentation

Cisco documentation is available in the following ways:

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

P1 and P2 level problems are defined as follows:

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

Installation

This chapter provides procedures for installing the Cisco ONS 15454. Chapter topics include installation equipment, rack installation, equipment access, power and ground installation, backplane interface connections (alarms, timing, craft interface, etc.), card turn-up procedures, cable installation, cable management, and hardware specifications.

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

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

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

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

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

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

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

1.1 Installation Overview

When installed in an equipment rack, the ONS 15454 assembly is typically connected to a fuse and alarm panel to provide centralized alarm connection points and distributed power for the ONS 15454 system. Fuse and alarm panels are third-party equipment and are not described in this documentation. If you are unsure about the requirements or specifications for a fuse and alarm panel, consult the documentation for the related equipment.

You can mount the ONS 15454 in a 19- or 23-inch rack. The shelf assembly weighs approximately 55 pounds with no cards installed. An ONS 15454 is installed in a rack using reversible mounting brackets on each side of the shelf. The ONS 15454 features a front door for added security, a fan tray module for cooling, and extensive fiber management space.

ONS 15454 optical cards have SC connectors on the card faceplate. Fiber optic cables are routed into the front of the destination cards.

DS-1, DS-3, DS3XM-6, and EC-1 units require special Electrical Interface Assemblies (EIAs) to provide the coaxial connection points for the shelf. In most cases, EIAs are ordered with the ONS 15454 and come pre-installed on the assembly backplane. See the "Backplane Covers" section on page 1-18 for more information about the EIAs. DS-1 units support wire wrap twisted pair connections or an AMP CHAMP EIA. DS-3, DS3XM-6, and EC-1 units support BNC or SMB EIAs on the assembly backplane.

The front door of the ONS 15454 shelf allows access to the shelf assembly, fan tray, and fiber management area. The back panel provides access to alarm contacts, external interface contacts, power terminals, and BNC/SMB connectors.

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

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

1.2 Installation Equipment

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

1.2.1 Included Materials

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

- #12-24 x 3/4 pan head phillips mounting screws (8)
- #12 -24 x 3/4 socket set screws (2)
- T-handle #12-24 hex tool for set screws (1)
- ESD wrist strap with 1.8 m (6 ft) coil cable (1)
- Tie wraps (10)
- Pinned Allen key for front door (1)

1.2.2 User-Supplied Materials

These materials and tools are recommended but are not supplied with the ONS 15454.

- Equipment rack (22 inches total width for a 19-inch rack; 26 inches total width for a 23-inch rack)
- Fuse panel
- Power cable (from fuse and alarm panel to assembly), #12-#14 AWG
- Ground cable #14 AWG (4.0 mm) stranded
- Alarm cable pairs for all alarm connections, #22 or #24 AWG, solid tinned
- Building Integrated Timing Supply (BITS) clock cable pair #22 or #24, solid tinned
- Single mode SC fiber jumpers with UPC polish (55 dB or better) for optical cards
- Shielded coaxial cable terminated with SMB or BNC connectors for DS-3 cards
- Shielded ABAM cable terminated with AMP CHAMP connectors or unterminated for DS-1 cards with #22 or #24 AWG ground wire (typically about two feet in length)
- Tie wraps and/or lacing cord
- Labels

1.2.2.1 Tools Needed

- #2 Phillips screw driver
- Medium slot head screw driver
- Small slot head screw driver
- Wire wrapper
- Wire cutters
- Wire strippers
- Crimp tool

1.2.2.2 Test Equipment

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

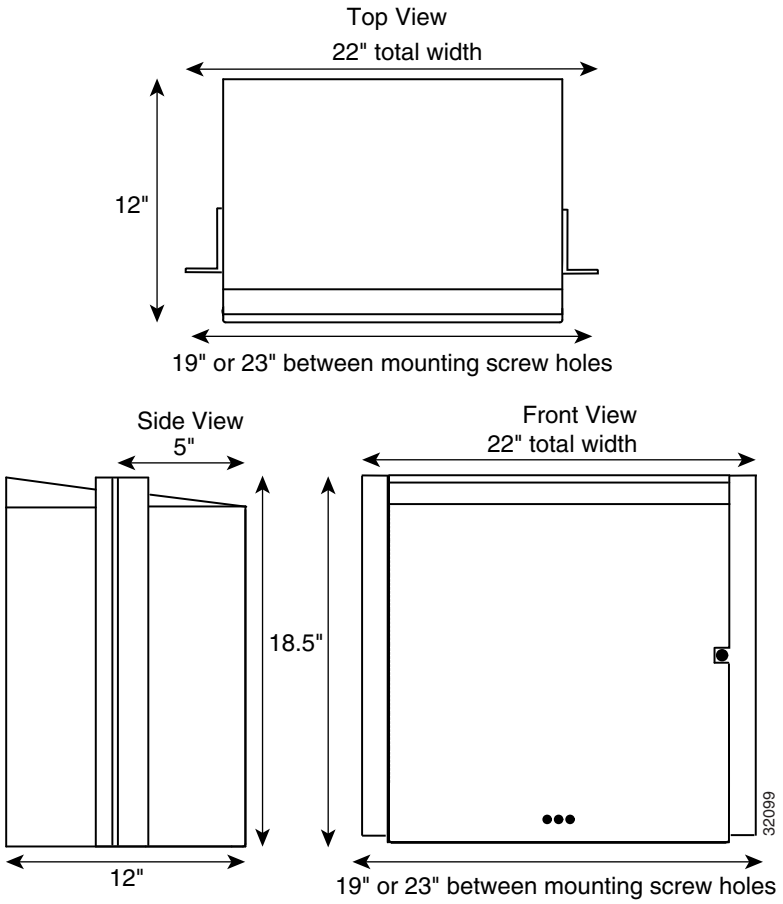
1.3 Installation in a Rack

The ONS 15454 is easily mounted in a 19- or 23-inch equipment rack. The shelf assembly projects 5 inches from the front of the rack. It mounts in both EIA-standard and Telcordia-standard racks. The shelf assembly is a total of 17 inches wide with no mounting ears attached. With the mounting ears attached, the shelf assembly is 19 inches wide. Ring runs are not provided by Cisco and may hinder side-by-side installation of shelves where space is limited.

The ONS 15454 measures 18.5 inches high, 19 or 23 inches wide (depending on which way the mounting ears are attached), and 12 inches deep (40.7 by 41.8 by 26.4 cm). You can install up to four ONS 15454 shelves in a seven-foot equipment rack. The ONS 15454 must have 1 inch of

airspace below the installed unit to allow air flow to the fan intake. If a second ONS 15454 is installed underneath the unit, the air ramp on top of the bottom unit provides the air spacing needed and should not be modified in any way. Figure 1-1 shows the dimensions of the ONS 15454 shelf assembly.

Figure 1-1 Dimensions



1.3.1 Reversible Mounting Bracket

Caution Use only the fastening hardware provided with the ONS 15454 to prevent loosening, deterioration, and electromechanical corrosion of the hardware and joined material.

Caution When mounting the ONS 15454 in a frame with a non-conductive coating (such as paint, lacquer, or enamel) either use the thread-forming screws provided with the ONS 15454 shipping kit, or remove the coating from the threads to ensure electrical continuity.

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

Procedure: Reverse the Mounting Bracket

Step 1 Remove the screws that attach the mounting bracket to the side of the shelf assembly unit.

Step 2 Flip the detached mounting bracket upside down. Text imprinted on the mounting bracket will now also be upside down.

Step 3 Place the widest side of the mounting bracket flush against the shelf assembly.

The narrow side of the mounting bracket should be towards the front of the shelf assembly. Text imprinted on the mounting bracket should be visible and upside down.

Step 4 Align the mounting bracket screw holes against the shelf assembly screw holes.

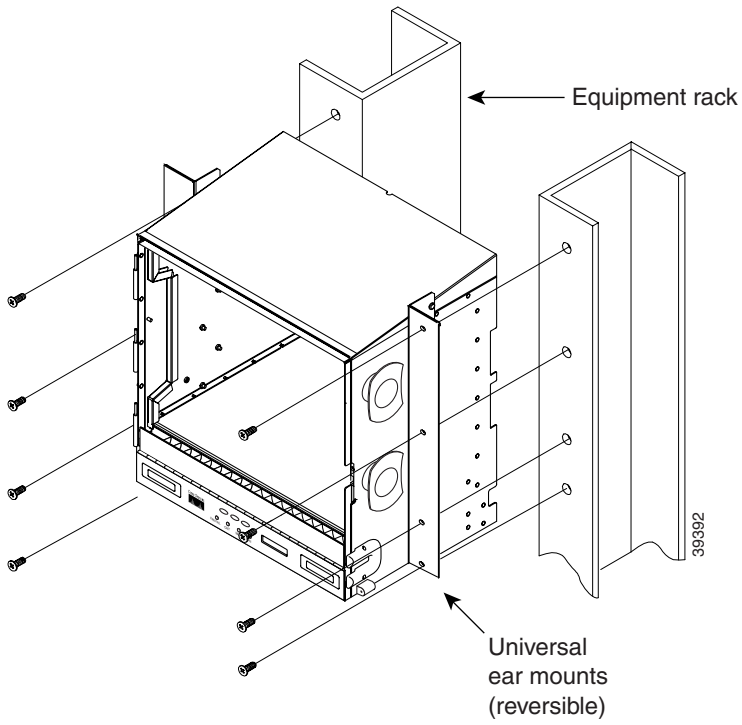
Step 5 Insert the screws that were removed in Step 1 and tighten them.

Step 6 Repeat the procedure for the mounting bracket on the opposite side.

1.3.2 Mounting the ONS 15454 in a Rack

Mounting the ONS 15454 in a rack requires a minimum of 18.5 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 1-2 shows the rack mounting position for the ONS 15454.

Figure 1-2 Rack Mount



Two people should install the ONS 15454 shelf assembly; however, one person can install the shelf assembly using the temporary set screws. Two hex head set screws are included for use when one person is installing the shelf assembly. The shelf should be empty for easier lifting. The door can also be removed to lighten the shelf (see the "Remove the Front Door" section on page 1-11).

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

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

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

Step 2 Install the set screws using the hex tool that shipped with the assembly.

Step 3 Place the shelf assembly on the set screws using the screw holes that will not be used to mount the shelf.

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

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

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

At least one set of the ONS 15454's horizontal screw slots should be used to prevent future slippage.

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

Step 8 Remove the temporary set screws.

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

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

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

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

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

At least one set of the ONS 15454's horizontal screw slots should be used to prevent future slippage.

Step 5 When the shelf is secured to the rack, install the remaining mounting screws.

1.3.3 Multiple Installations in a Rack

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

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

Procedure: Mount Multiple ONS 15454s in a Rack

Step 1 Install the fuse and alarm panel in the top space.

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

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

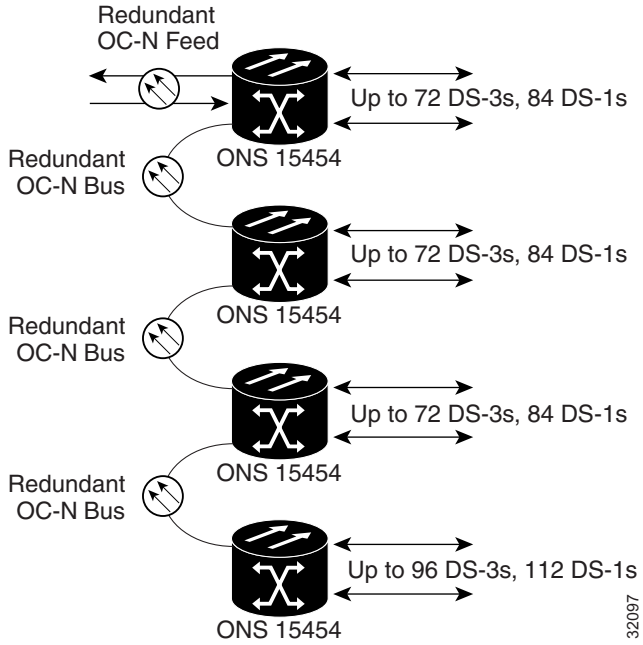
Note The ONS 15454 must have one inch of airspace below the installed unit to allow air flow to the fan intake. If a second ONS 15454 is installed underneath a unit, the air ramp on top of the bottom unit provides the desired space. However, if the ONS 15454 is installed above third party equipment, you must provide a minimum spacing of one inch between the third party unit and the bottom of the ONS 15454. The third party equipment must not generate heat upward into the ONS 15454.

1.3.3.1 Four Shelf System Example

A common application is linking multiple shelves with a fiber optic bus to accommodate more access traffic than a single shelf can support. For example, if you need to drop more than 112 DS-1s or 96 DS-3s (the maximum that can be aggregated in a single node), you can link the shelves. However, you cannot merge multiple shelves into a single node. You can link shelves with OC-12 or OC-48 fiber spans as you would link any other two network nodes. They can be co-located in a facility to aggregate more local traffic.

Figure 1-3 shows a four shelf system. Each shelf is identified as a separate node in the CTC, and traffic must be mapped using CTC cross-connect options. In the figure, each node uses redundant fiber optic cards. Node 1 uses redundant OC-N transport and OC-N bus cards for a total of four cards, with eight free slots remaining. Nodes 2 and 3 each use two redundant OC-N bus cards for a total of four cards, with eight free slots remaining. Node 4 uses redundant OC-12 bus cards for a total of two cards, with ten free slots remaining. The four shelf system example presented here is one of many ways to set up a multiple-shelf system.

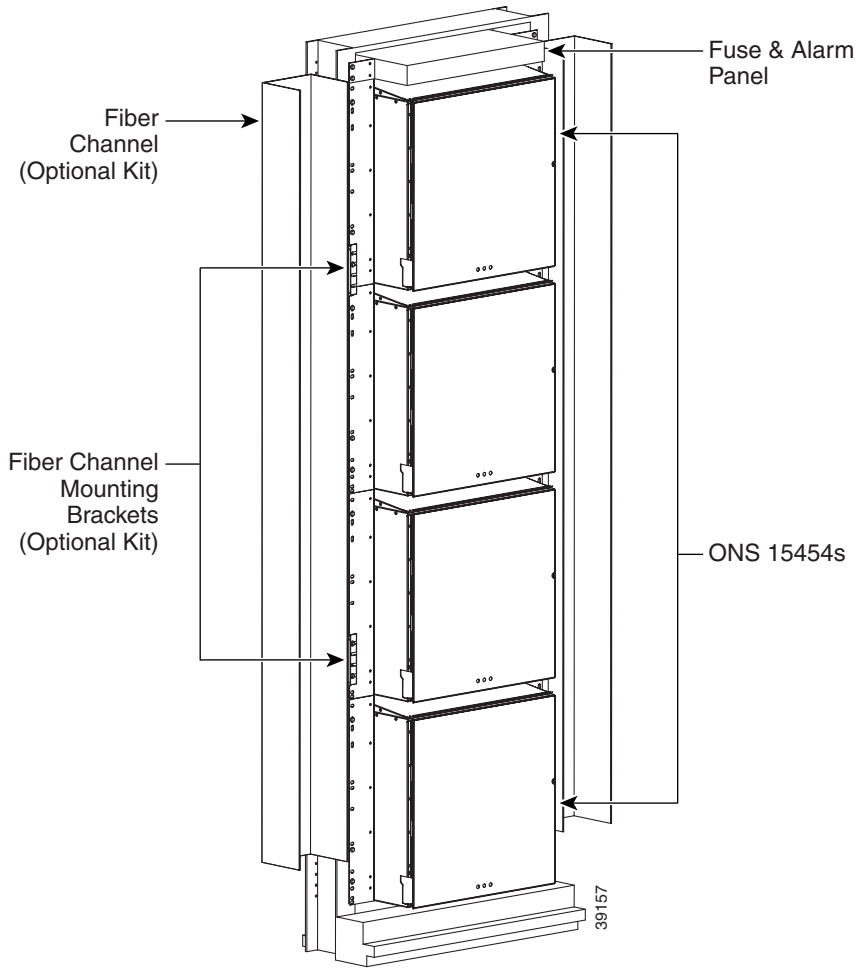
Figure 1-3 Four Shelf System



1.3.3.2 ONS 15454 Bay Assembly

The Cisco ONS 15454 Bay Assembly simplifies ordering and installing the ONS 15454. The ONS 15454 Bay Assembly allows you to order shelf assemblies pre-installed in a seven-foot rack. The Bay Assembly is available in a three- or four-shelf configuration. The three-shelf configuration includes three ONS 15454 shelf assemblies, a pre-wired fuse and alarm panel, and two fiber management trays. Optional fiber channels can be ordered. The four-shelf configuration includes four ONS 15454 shelf assemblies and a pre-wired fuse and alarm panel. Optional fiber channels can be ordered. A four shelf ONS 15454 Bay Assembly is shown in Figure 1-4.

Figure 1-4 Four Shelf ONS 15454 Bay Assembly



1.4 Equipment Access and Features

This section tells you how to access ONS 15454 equipment through the front door and backplane cover and describes the equipment features.

Note The ONS 15454 has an ESD plug input and is shipped with an ESD wrist strap. The ESD plug input is located on the outside edge of the shelf on the right hand side. It is labeled "ESD" on the top and bottom. Always wear an ESD wrist strap and connect the strap to the ESD plug when working on the ONS 15454.

Note The front door of the ONS 15454 is grounded to prevent the possibility of electrical shock.

1.4.1 Front Door

The ONS 15454 features a locked door to the front compartment and a screw-in panel over the backplane. A pinned Allen key that unlocks the front door ships with the ONS 15454. A button on the right side of the assembly releases the door. The front door (Figure 1-5) provides access to the ONS 15454 shelf assembly, cable management tray, fan tray assembly, and LCD screen (Figure 1-12).

Procedure: Open the Front Cabinet Compartment

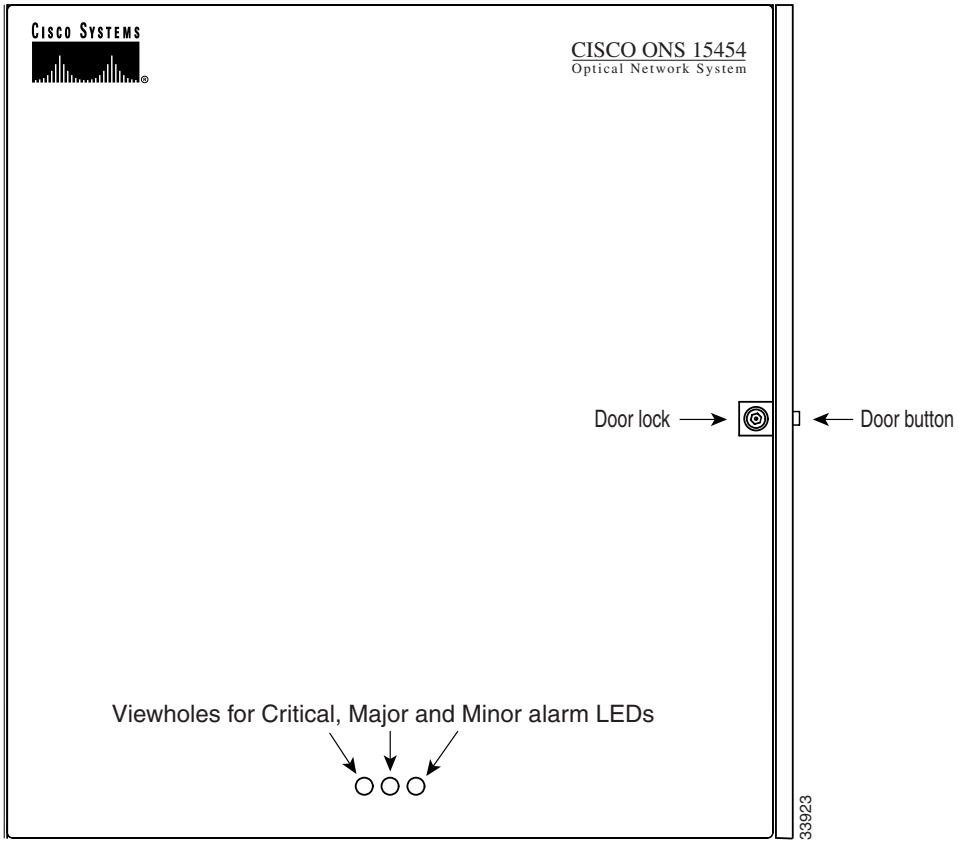
Step 1 Open the front door lock.

The ONS 15454 comes with a pinned hex key for locking and unlocking the front door. Turn the key counterclockwise to unlock the door and clockwise to lock it.

Step 2 Press the door button to release the latch.

Step 3 Swing the door open.

Figure 1-5 Front Door



The Critical, Major, and Minor alarm LEDs visible through the front door indicate whether a Critical, Major, or Minor alarm is present anywhere on the ONS 15454. These LEDs must be visible so technicians can quickly determine if any alarms are present. You can use the LCD to further isolate alarms. See the "LCD Alarm Functions" section on page 1-18 for more information.

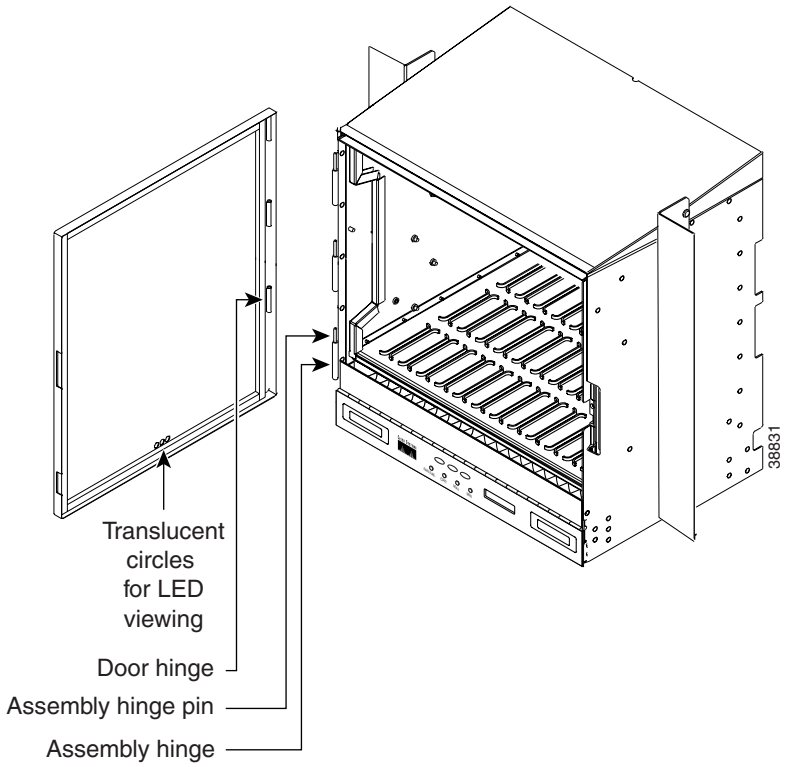
You can remove the front door of the ONS 15454 to provide unrestricted access to the front assembly.

Procedure: Remove the Front Door

Step 1 Open the door.

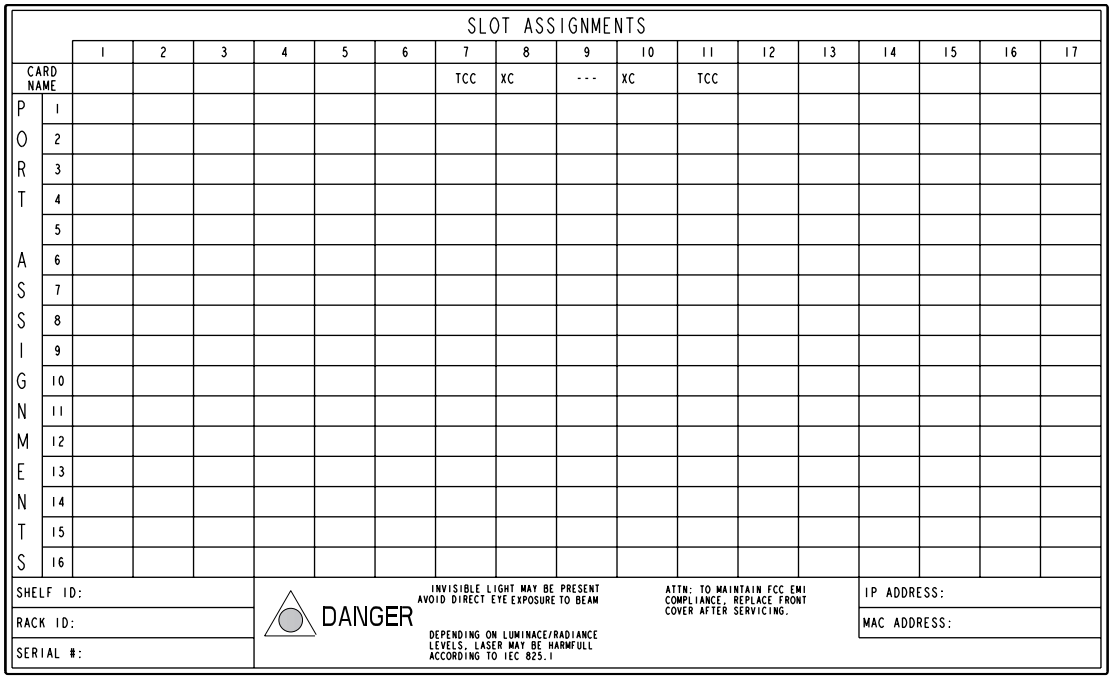
Step 2 Lift the door from its hinges from the top left corner of the door (Figure 1-6).

Figure 1-6 Door Hinge



An erasable label (Figure 1-7) is pasted on the inside of the front door. You can use the label to record slot assignment, port assignments, card types, node ID, rack ID, and serial number for the ONS 15454.

Figure 1-7 Erasable Label on the Inside Door



1.4.2 Card Slots

The ONS 15454 shelf assembly has 17 card slots numbered sequentially from left to right. Slots 1–4 and 14–17 are "multispeed" slots. They can host any ONS 15454 card except the OC-48. Slots 5, 6, 12 and 13 are "high-speed" slots. They can host any ONS 15454 card including OC-48 cards. Slots 7 and 11 are dedicated to timing communications and control (TCC) cards. Slots 8 and 10 are dedicated to cross-connect (XC and XCVT) cards. Slot 9 is reserved for the optional Alarm Interface Controller (AIC) card. Slots 3 and 15 can also host DS1N-14 and DS3N-12 cards that are used in 1:N protection. Each shelf assembly slot has a symbol that indicates the type of cards that can be installed in the slot (see the "Slot Requirements" section on page 1-36 for a list).

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

1.4.3 Cable Management Facilities

The ONS 15454 cable management facilities include the following:

- Cable management clips on optical card faceplates
- A cable routing channel that runs the width of the shelf assembly
- Fiber guides at each side opening of the cable routing channel

  The plastic horseshoe-shaped fiber guides ensure that the proper bend radius is maintained in the fibers. You can remove the fiber guide if necessary to create a larger opening (if you need to route copper Ethernet cables out the side, for example). It is removed by taking out the three screws that anchor it to the side of the shelf assembly.

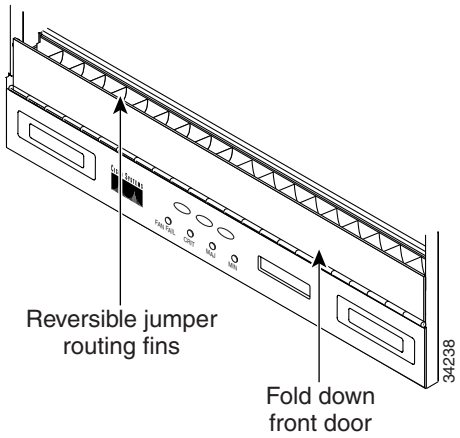
- A fold-down door
- Cable tie wrap facilities on EIAs
- Reversible jumper routing fins

  You can route cables out either side by positioning the fins as desired.
- Jumper slack storage reels (2) on each side panel

  These reels are used to reduce the amount of slack in cables that are connected to other devices. They are easily removed by taking out the screw in the center of each reel.

Figure 1-8 shows the cable management facilities in the shelf assembly that can be accessed through the fold-down front door of the shelf, including the cable routing channel and the jumper routing fins.

Figure 1-8 Front Panel Cable Management



See the "Cable Management" section on page 1-50 for more detailed cable management information.

1.4.4 Fan Tray Assembly

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

Note Install the fan tray filter before installing the fan tray assembly if you are not using the bottom brackets to install the filter on the shelf assembly.

To install or replace the fan tray assembly, it is not necessary to move any of the cable management facilities. You can remove the fan tray assembly using the retractable handles and replace it by pushing until it plugs into the receptacle on the back panel.

The fan tray assembly features an air filter at the bottom of the tray that can be installed and removed by hand. Remove and visually inspect this filter every 30 days. When the filter is dirty, remove the filter and clean it by either vacuuming the filter or running water through it. Because the filter

material is delicate, only a very low-power vacuum should be used. If you are cleaning with water, make sure the filter is completely dry before replacing it in the fan tray. Spare filters should be kept in stock.

The shelf assembly ships with a bottom bracket that can be used to install the filter. The bottom bracket consists of two grooved metal pieces that attach to the bottom of the shelf assembly using three screws each. When the fan tray air filter is installed using the bottom bracket, the filter can be installed and removed without first removing the fan tray assembly. The following two procedures describe both methods of filter installation.

Caution Do not force the fan tray assembly into place when installing a fan tray. 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 or Replace the Fan Tray Air Filter Without the Bottom Brackets

Step 1 Remove the fan tray assembly.

If you are replacing the filter, remove the old filter.

Step 2 Slide the filter into the shelf assembly.

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

Although the filter will work if installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

If the bottom bracket is used to install the fan tray air filter, the fan tray does not need to be removed to access the filter. Attach the brackets to the bottom of the shelf assembly before performing rack installation.

Procedure: Install or Replace the Fan Tray Air Filter Using the Bottom Brackets

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

Step 2 Locate the three screw holes that run along the left and right sides of the bottom of the shelf assembly.

Step 3 Secure each bracket to the bottom of the shelf assembly using the screws provided.

Each bracket has a filter stopper and a flange on one end. Make sure to attach the brackets with the stoppers and flanges at the rear of the shelf assembly (the top, if the ONS 15454 is face-down during installation).

Figure 1-9 illustrates bottom bracket installation and Figure 1-10 illustrates fan tray filter replacement when bottom brackets are used to install the filter.

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

Figure 1-9 Bottom Bracket Installation

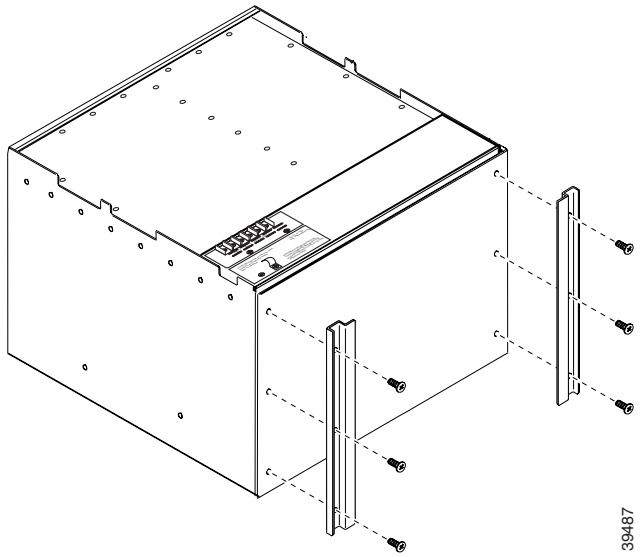
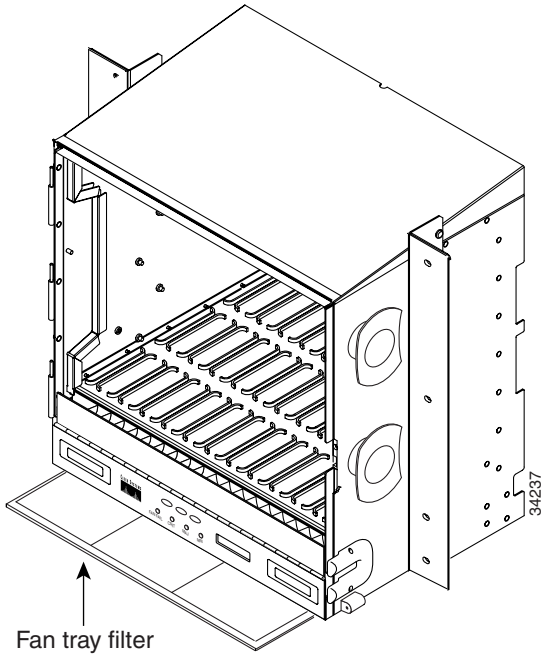


Figure 1-10 Fan Tray Filter Replacement



Procedure: Install the Fan Tray

Step 1 Remove the front door of the shelf assembly.

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

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

Procedure: Remove the Fan Tray

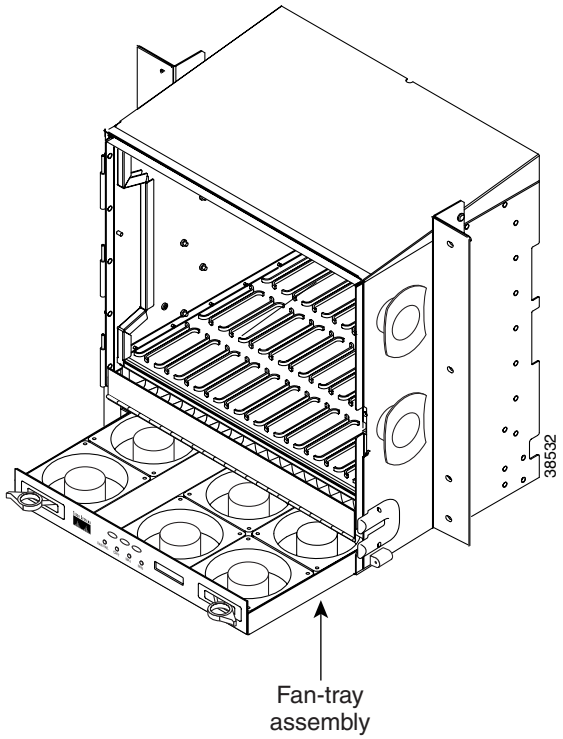
Step 1 Remove the front door of the shelf assembly.

Step 2 Fold out the retractable handles at each outside edge of the fan tray.

Step 3 Slide the fan tray out of the shelf by gently pulling on the handles.

Figure 1-11 shows the location of the fan tray. The filter will function no matter which side faces up but Cisco recommends that you install the filter with the metal bracing facing up against the fan tray.

Figure 1-11 Fan Tray Assembly



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

If one or more fans fail on the fan tray assembly, replace the entire assembly. You cannot replace individual fans. The red Fan Fail LED on the front of the fan tray illuminates when one or more fans fail. For fan tray replacement instructions, see the "Install the Fan Tray" section on page 1-16. The red Fan Fail LED clears after you install a working fan tray.

1.4.5 LCD Screen

The ONS 15454 LCD screen provides port-level information for all ONS 15454 card slots.

You can set the IP address, subnet mask, and default router for the node by using the LCD screen. This allows you to accomplish these basic operations without a computer. For instructions about using the LCD screen to set these parameters, see the "Enter IP Address Using Front Panel LCD" section on page 8-10.

Press the Slot, Port, or Status buttons to display status information for each ONS 15454 slot and port. The LCD displays the number of Critical, Major, and Minor alarms on a slot or port basis.

Procedure: View Alarms Counts on a Specific Slot and Port

Step 1 Use the Slot button to toggle to the desired slot number.

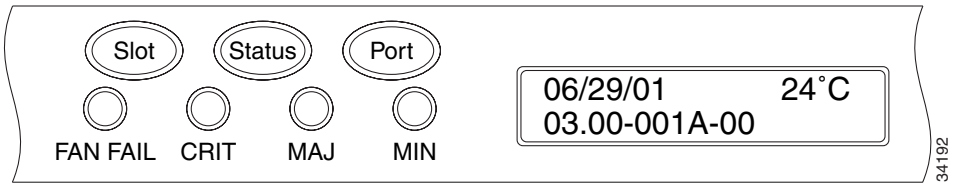
Set the slot number to Slot 0 to see a summary of alarms for the node.

Step 2 Use the Port button to toggle to the port.

Step 3 Use the Status button to toggle through all active alarms and conditions.

Figure 1-12 shows the LCD panel.

Figure 1-12 LCD Panel



By default, the LCD screen displays the ONS 15454 network element IP address. The Cisco Transport Controller needs this address to access the ONS 15454.

The LCD panel alternately displays the node name and the current date. The IP address alternates with the current software version on the LCD; the time and temperature also display alternately.

The information displayed on the LCD is determined by the software version you are currently running.

Caution If the ONS 15454 node connects to a LAN, change the default ONS 15454 IP address to an address that is compatible with the network. If you do not change the IP address, the network can be disrupted. For IP addressing procedures, see the "Setup a PC for Direct Connection" section on page 3-5.

1.4.6 LCD Alarm Functions

Note The Critical, Major and Minor alarm LEDs on the fan tray front panel indicate whether a critical, major, or minor alarm is present anywhere on the ONS 15454 assembly. These LEDs are viewable through the front door so that you can quickly determine if any alarms are present on the assembly. These LEDs are independent of the Card, Port, and Status indicators on the LCD. You can view specific alarm messages in the Alarms menu in the CTC.

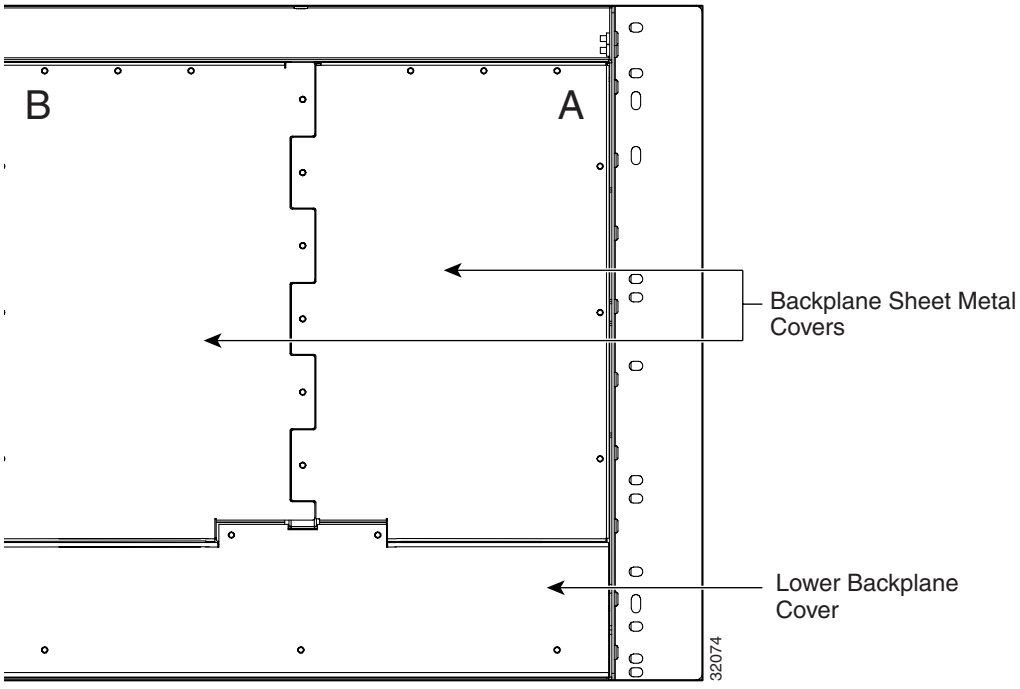
When you press the Slot, Port, or Status buttons, the LCD displays the selected slot and port and the number of Critical, Major, or Minor alarms.

See Chapter 2, "Card Reference," for descriptions of the port-level states supported by ONS 15454 cards.

1.4.7 Backplane Covers

To access the ONS 15454 backplane, remove the sheet metal on each side of the backplane (Figure 1-13). Each sheet metal panel is held in place with nine 6-32 x 3/8 inch Phillips screws.

Figure 1-13 Backplane Sheet Metal Covers



Before installing EIA(s), you need to prepare the backplane by removing the backplane sheet metal covers to expose the EIA backplane mating connectors.

Procedure: Remove the Backplane Sheet Metal Covers

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

Step 2 Loosen the nine perimeter screws that hold the backplane sheet metal cover(s) in place.

Step 3 Lift the panel by the bottom to remove it from the shelf assembly.

Step 4 Store the panel for later use. Attach the backplane sheet metal cover(s) whenever EIA(s) are not installed.

Figure 1-13 shows the sheet metal covers on the ONS 15454 backplane.

1.4.7.1 EIA Backplane Cover (Optional)

EIAs are typically pre-installed on the ONS 15454 when ordered with the system. EIAs must be ordered when using DS-1, DS-3, DS3XM-6, or EC-1 cards. Four different EIAs are available for the ONS 15454: BNC, High-density BNC, SMB, and AMP CHAMP. This section describes each EIA in detail.

EIAs host a special card that provides coaxial cable connection points (SMB or BNC) for the DS-3 or EC-1 cards. EIAs also host twisted pair wire-wrap adapters for SMB connectors or, for the DS-1 card, AMP CHAMP connectors. EIAs also feature a special backplane cover with cutouts over the cable connectors. You can install EIAs on one or both sides of the ONS 15454 backplane in any combination (in other words, AMP Champ on Side A and BNC on Side B or High-density BNC on side A and SMB on side B, and so forth).

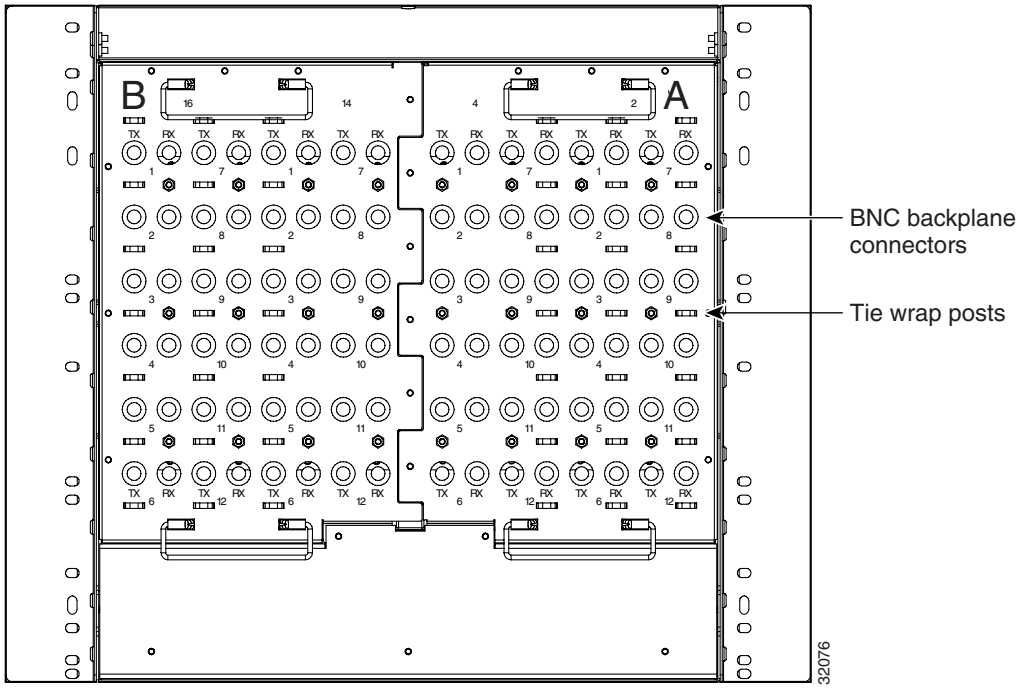
If you are installing EIAs after the ONS 15454 shelf assembly is installed, plug the EIA card into the backplane. The EIA has six electrical connectors that plug into six corresponding backplane connectors. The EIA must replace the standard sheet metal cover to provide access via the coaxial cable connectors. The EIA sheet metal covers use the same screw holes as the solid backplane panels, but they have 12 additional 6-32 x 1/2 inch Phillips screw holes so you can screw down the cover and the card using standoffs on the EIA card. For information about installing EIAs, see the "Install an EIA" section on page 1-24. To view a list of EIAs and their functions, see Table 10-1 on page 10-13.

1.4.7.2 BNC EIA

The ONS 15454 BNC EIA supports Trompeter UCBJ224 75 Ohm 4 leg connectors. You can use BNC EIAs for DS-3 (including the DS3XM-6) or EC-1 cards. Figure 1-14 shows the ONS 15454 with pre-installed BNC EIAs.

For instructions on installing coaxial cable with BNC connectors, see the "BNC Installation" section on page 1-43.

Figure 1-14 BNC Backplane



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

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

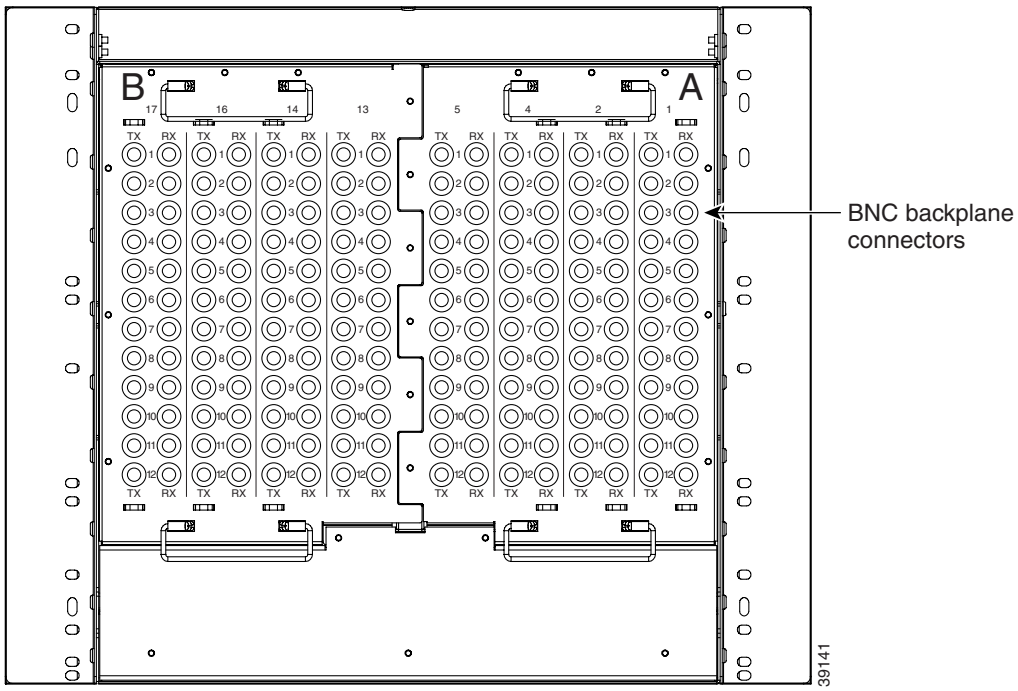
When BNC connectors are used and a DS3N-12 card is in Slot 3 or 15, the 1:N card protection extends only to the two slots adjacent to the 1:N card due to BNC wiring constraints.

1.4.7.3 High-Density BNC EIA

The ONS 15454 High-density BNC EIA supports Trompeter UCBJ224 75 Ohm 4 leg connectors. You can use High-density BNC EIAs for DS-3 (including the DS3XM-6) or EC-1 cards. Figure 1-15 shows the ONS 15454 with pre-installed High-density BNC EIAs.

For instructions on installing coaxial cable with High-density BNC connectors, see the “High-Density BNC Installation” section on page 1-45.

Figure 1-15 High-density BNC Backplane



The EIA side marked “A” hosts 48 pairs of BNC connectors. Each column of connector pairs is numbered and corresponds to the slot of the same number. The first column (12 pairs) of BNC connectors corresponds to Slot 1 on the shelf assembly, the second column to Slot 2, the third column to Slot 4 and the fourth column to Slot 5. The rows of connectors correspond to ports 1–12 of a 12-port card. The EIA side marked “B” provides an additional 48 pairs of BNC connectors. The first column (12 pairs) of BNC connectors corresponds to Slot 13 on the shelf assembly, the second column to Slot 14, the third column to Slot 16 and the fourth column to Slot 17. The rows of connectors correspond to ports 1–12 of a 12-port card. The BNC connector pairs are marked “Tx” and “Rx” to indicate transmit and receive cables for each port. The High-density BNC EIA supports both 1:1 and 1:N protection across all slots.

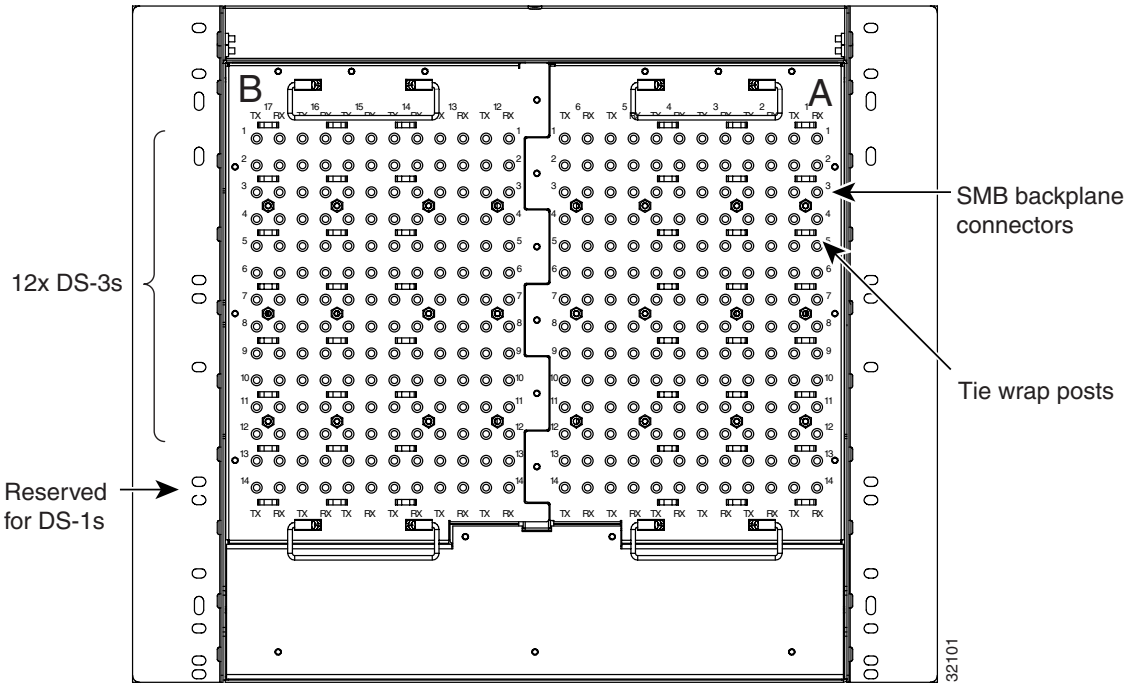
Install the High-density BNC EIA(s) after removing the backplane sheet metal covers or existing EIA(s).

1.4.7.4 SMB EIA

The ONS 15454 SMB EIA supports AMP 415484-1 75 Ohm 4 leg connectors. You can use SMB EIAs with DS-1, DS-3 (including the DS3XM-6), and EC-1 cards. If you use DS-1 cards, use the DS-1 electrical interface adapter to terminate the twisted pair DS-1 cable from the backplane. Figure 1-16 shows the ONS 15454 with pre-installed SMB EIAs and the sheet metal cover and screw locations for the EIA.

For instructions on installing SMB connectors, see the “SMB Installation” section on page 1-45.

Figure 1-16 SMB Backplane



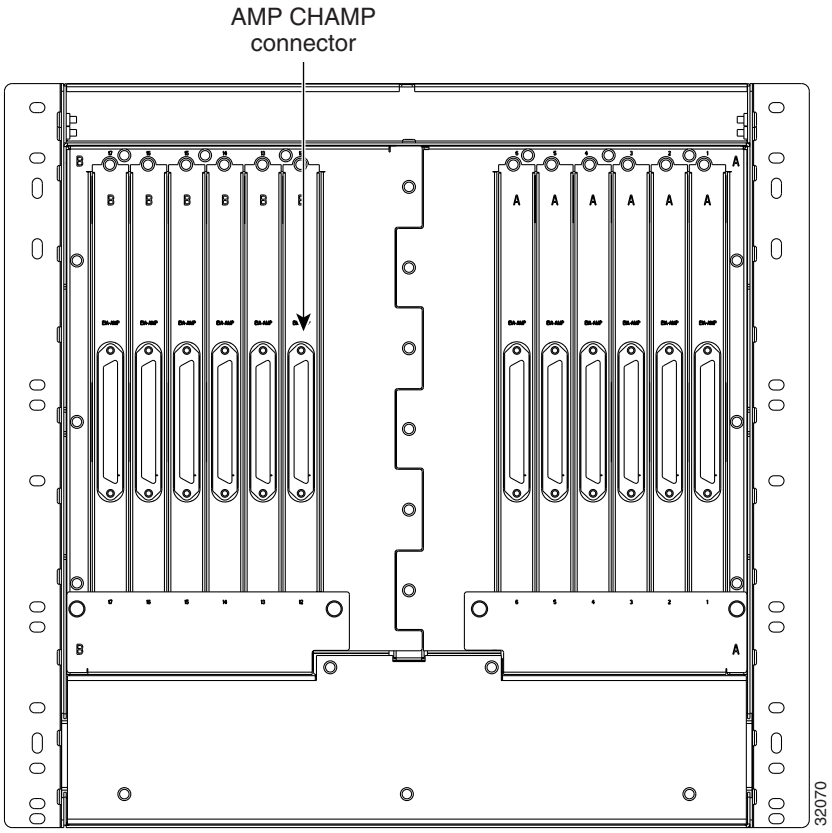
The EIA side marked "A" hosts 84 SMB connectors in six columns of 14 connectors. The "A" side columns are numbered 1-6 and correspond to Slots 1-6 on the shelf assembly. The EIA side marked "B" hosts an additional 84 SMB connectors in six columns of 14 connectors. The "B" side columns are numbered 12-17 and correspond to Slots 12-17 on the shelf assembly. The connector rows are numbered 1-14 and correspond to the 14 ports on a DS-1 card. If you use a DS-3 or EC-1 card, only ports 1-12 are active. If you use a DS3XM-6 card, only ports 1-6 are active. The SMB connector pairs are marked "Tx" and "Rx" to identify transmit and receive cables for each port. If you use SMB connectors, you can install DS-1, DS-3, or EC-1 cards in any multispeed slot.

1.4.7.5 AMP CHAMP EIA

The ONS 15454 AMP CHAMP EIA supports 64-pin (32 pair) AMP CHAMP connectors for each slot on both sides of the shelf assembly where the EIA is installed. Cisco AMP CHAMP connectors are female AMP # 552246-1 with AMP # 552562-2 bail locks. Each AMP CHAMP connector supports 14 DS-1 ports. You can use AMP CHAMP EIAs with DS-1 cards. Figure 1-17 shows the ONS 15454 with pre-installed AMP CHAMP EIAs and the corresponding sheet metal cover and screw locations for the EIA.

For instructions on installing AMP CHAMP connector DS-1 cables, see the "AMP CHAMP Installation" section on page 1-48.

Figure 1-17 AMP CHAMP Backplane



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

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

Procedure: Remove an EIA

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

Step 2 Loosen the nine perimeter screws that hold the EIA in place.

If you are removing an AMP CHAMP EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

Step 3 Lift the EIA handles and gently pull the EIA panel away from the backplane.

Procedure: Install an EIA

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

Step 2 Line up the connectors on the EIA with the mating connectors on the backplane.

Step 3 Gently push the EIA until both sets of connectors fit together snugly.

Step 4 Replace the nine perimeter screws that were removed with the backplane sheet metal cover.

Step 5 If you are installing an AMP CHAMP EIA, proceed to Step 6; if you are installing any other EIA, proceed to Step 7.

Step 6 Secure the AMP CHAMP EIA by attaching the fastening plate to the shelf assembly.

The fastening plate attaches over the EIA and to the shelf assembly using the integrated thumbscrews.

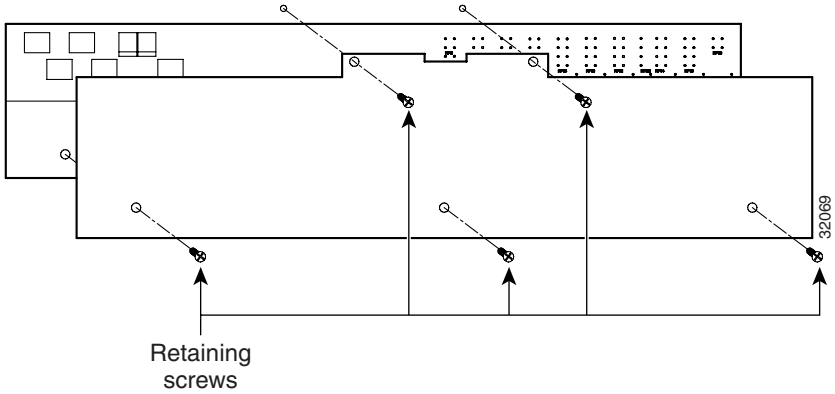
Step 7 Reattach the lower backplane cover.

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

1.4.7.6 Lower Backplane Cover

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

Figure 1-18 Lower Backplane Cover



Procedure: Access the Alarm Interface Panel, Alarm Pin Field or Power Terminals

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

Step 2 Grasp the Plexiglas cover at each side.

Step 3 Gently pull the cover away from the backplane (shown in Figure 1-18).

1.4.7.7 Alarm Interface Panel

The Alarm Interface Panel (AIP) is located above the alarm pin field on the lower section of the backplane (see the "Equipment Access and Features" section on page 1-9 for information about how to access the AIP). The AIP provides surge protection for the ONS 15454 shelf assembly. It also provides an interface from the backplane to the fan tray assembly and LCD. The AIP plugs into the backplane using a 96 pin DIN connector and is held in place with two retaining screws. The panel has a non-volatile memory chip that stores the unique node (MAC) address.

The MAC address identifies the nodes that support circuits. It allows the CTC to determine circuit sources, destinations, and spans. The TCC cards in the ONS 15454 also read the MAC address to store the node database. You can change the default IP address in CTC. See the "Set Up Network Information" section on page 3-23 for instructions.

If the AIP fails, a MAC Fail alarm displays on the CTC Alarms menu. See the "Viewing ONS 15454 Alarms" section on page 3-18 for more information about alarms.

Procedure: Replace the Alarm Interface Panel

Step 1 Remove the clear cover from the AIP.

Step 2 Unscrew the two screws that hold the AIP in place.

Step 3 Grip the panel on each side.

Step 4 Gently remove the panel from the backplane.

Step 5 Remove the fan tray assembly power cable.

Step 6 Attach the fan tray assembly power cable to the new AIP.

Step 7 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 8 Replace the screws that secure the panel to the backplane.

Step 9 Reset both TCCs, one at a time.

1.5 Power and Ground Installation

This section explains how to connect the ONS 15454 assembly to the power supply.

Warning Shut off the power from the power source before beginning work.

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

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

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

Use the following wiring conventions:

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

Note Use an external disconnect (minimum 15A fused) for service purposes. Install according to local site practice.

The ONS 15454 has redundant -48V DC #8 power terminals on the assembly backplane. The terminals are labeled BAT1, RET1, BAT2, and RET2 and are located on the lower section of the backplane behind a Plexiglas cover. See the "Equipment Access and Features" section on page 1-9 for information about accessing the power terminals.

To install redundant power feeds, use four power cables and one ground cable. For a single power feed, only two power cables and one ground cable are required. Use #12 or #14 AWG cable. Use a conductor with low impedance to ensure circuit overcurrent protection. However, the conductor must have the capability to safely conduct any fault current that might be imposed.

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

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

Procedure: Install Redundant Power Feeds

Step 1 Measure and cut the cables as needed to reach the ONS 15454 from the fuse panel. Use 15A fuses for each power lead. Figure 1-19 shows the ONS 15454 power terminals.

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

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

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

Note Use only listed compression type connectors when terminating the battery, battery return, and frame ground conductors.

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

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

Step 4 Strip 1/2 inch of insulation from all power cables that you will use. If you are using lugs, crimp the lugs onto the ends of all power leads.

Note When terminating battery and battery return connections as shown in Figure 1-19, follow a torque specification of 10 in-lbs. When terminating a frame ground, use the kep-nut provided with the ONS 15454 and tighten it to a torque specification of 31 in-lbs. The kep-nut provides a frame ground connection that minimizes the possibility of loosening caused by rotation during installation and maintenance activity. This type of prevention is inherently provided by the terminal block for battery and battery return connections.

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

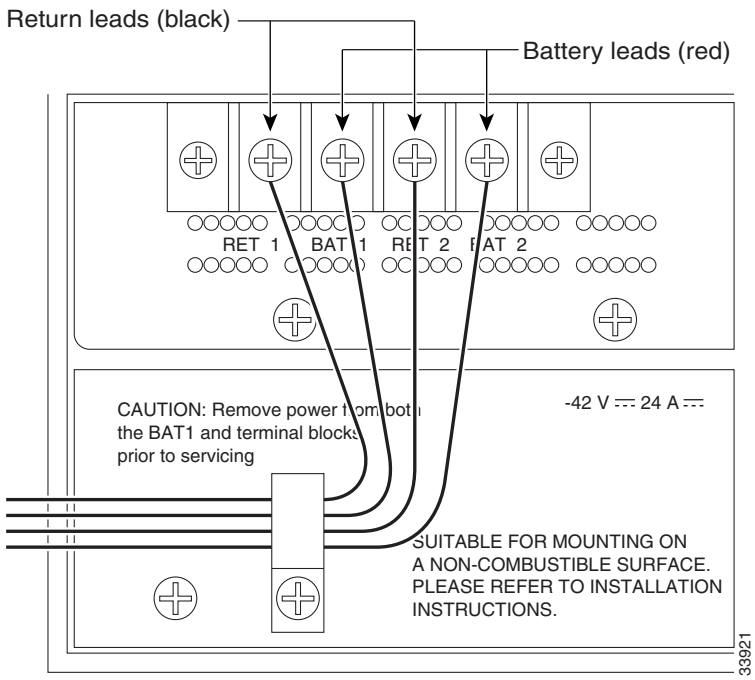
Warning Do not secure multiple connectors with the same bolt assembly.

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

Step 7 If you use redundant power leads, terminate the return 2 lead to the positive RET terminal on the ONS 15454. Terminate the negative 2 lead to the negative BAT2 terminal on the ONS 15454. Use oxidation-preventative grease to keep connections non-corrosive.

Step 8 Route the cables out using the plastic cable clamp below the power terminals.

Figure 1-19 Power Terminals



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

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

If the system loses power or both TCC cards are reset, you must reset the ONS 15454 clock. After powering down, the date defaults to January 1, 1970, 00:04:15.

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

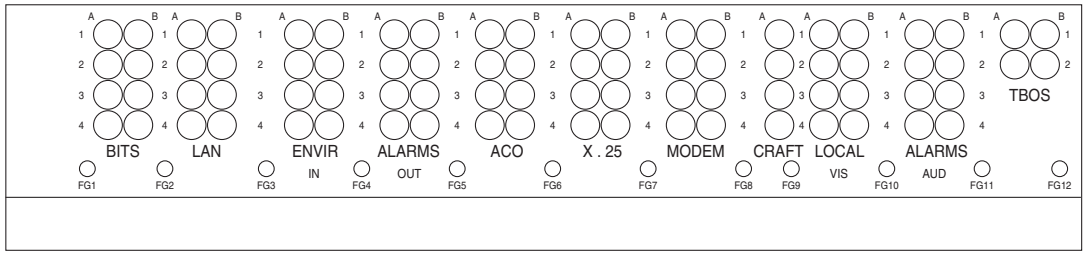
1.6 Alarm Pin Field Connections

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

The ONS 15454 backplane has an alarm pin field located at the bottom of the backplane. The alarm pin field provides 0.045 square inch wire-wrap pins for installing external alarms, timing input and output, and craft interface terminals. This section describes the alarm pin field and the pin assignments for the field. Figure 1-20 shows the wire-wrap pins on the alarm pin field. Beneath each wire-wrap pin is a frame ground pin. Frame ground pins are labeled FG1, FG2, FG3, etc. Install the ground shield of the cables connected to the backplane to the ground pin that corresponds to the pin field used. Figure 1-20 shows pinouts for the ONS 15454.

See the "Equipment Access and Features" section on page 1-9 for information about how to access the alarm pin field.

Figure 1-20 Pinouts



Field	Pin	Function
BITS	A1	BITS Output 2 negative (-)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (-)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (-)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (-)
	B4	BITS Input 1 positive (+)
LAN	Connecting to a hub, or switch	
	A1	RJ-45 pin 6 RX-
	B1	RJ-45 pin 3 RX+
	A2	RJ-45 pin 2 TX-
	B2	RJ-45 pin 1 TX+
	Connecting to a PC/Workstation or router	
	A1	RJ-45 pin 2 RX-
	B1	RJ-45 pin 1 RX+
	A2	RJ-45 pin 6 TX-
	B2	RJ-45 pin 3 TX+
ENVIR ALARMS IN	A1	Alarm input pair number 1: Reports closure on connected wires.
	B1	
	A2	Alarm input pair number 2: Reports closure on connected wires.
	B2	
	A3	Alarm input pair number 3: Reports closure on connected wires.
	B3	
	A4	Alarm input pair number 4: Reports closure on connected wires.
	B4	

Field	Pin	Function
ENVIR ALARMS OUT N/O	A1	Normally open output pair number 1
	B1	
	A2	Normally open output pair number 2
	B2	
	A3	Normally open output pair number 3
	B3	
	A4	Normally open output pair number 4
	B4	
ACO	A1	Normally open ACO pair
	B1	
CRAFT	A1	Receive (PC pin #2)
	A2	Transmit (PC pin #3)
	A3	Ground (PC pin #5)
	A4	DTR (PC pin #4)
LOCAL ALARMS AUD (Audible) N/O	A1	Alarm output pair number 1: Remote audible alarm.
	B1	
	A2	Alarm output pair number 2: Critical audible alarm.
	B2	
	A3	Alarm output pair number 3: Major audible alarm.
	B3	
	A4	Alarm output pair number 4: Minor audible alarm.
	B4	
LOCAL ALARMS VIS (Visual) N/O	A1	Alarm output pair number 1: Remote visual alarm.
	B1	
	A2	Alarm output pair number 2: Critical visual alarm.
	B2	
	A3	Alarm output pair number 3: Major visual alarm.
	B3	
	A4	Alarm output pair number 4: Minor visual alarm.
	B4	

38533

1.6.1 Alarm Installation

The alarm pin field supports up to 17 alarm contacts: four audible alarms, four visual alarms, one Alarm Cutoff (ACO), and four user-definable alarm inputs and outputs. Audible alarm contacts are in the LOCAL ALARM AUD pin field. Visual contacts are in the LOCAL ALARM VIS pin field. Both of these types of alarms fall into the LOCAL ALARMS category. User-definable contacts are in the ENVIR ALARM IN and ENVIR ALARM OUT pin fields. These two types of alarms fall into the ENVIR ALARMS category; you must have the AIC card installed in order to use the ENVIR ALARMS. The MODEM and X.25 pin fields are not currently used. Alarm contacts are Normally

Open (N/O), meaning that the system closes the alarm contacts when the corresponding alarm conditions are present. Each alarm contact consists of two wire-wrap pins on the assembly backplane. The alarm contacts are wired to the TCC card through the ONS 15454 backplane. Visual and Audible alarm contacts are classified as Critical, Major, Minor, and Remote. Refer to Figure 1-20 for alarm pin assignments.

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

To install alarm wires on the backplane, use #22 or #24 AWG alarm wires. Wrap the alarm wires on the appropriate wire-wrap pins according to local site practice. Each pin field has a frame ground pin beneath it.

1.6.2 Timing Installation

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

Table 1-1 External Timing Pin Assignments for BITS

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

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

To install timing wires on the backplane, use #22 or #24 AWG wire; wrap the clock wires on the appropriate wire-wrap pins according to local site practice. The BITS pin field (FG1) has a frame ground pin beneath it. Wrap the ground shield of the alarm cable to the frame ground pin. For more detailed information about timing, see the “Setting Up ONS 15454 Timing” section on page 3-29.

1.6.3 LAN Installation

You can use the Local Area Network (LAN) pins on the ONS 15454 backplane to connect the ONS 15454 to a PC or Ethernet LAN. You can use the LAN pin field to connect a LAN modem to the ONS 15454 for remote access to the node. You can also use the LAN port on the TCC faceplate to

connect a computer or to connect the ONS 15454 to the network. For more information about the ONS 15454 craft interface software and how to connect to a LAN modem, see Chapter 3, "Using the Cisco Transport Controller." Use the backplane pins and the LAN port on the TCC card to maintain two simultaneous craft interface connections. Table 1-2 shows the LAN pin assignments.

Table 1-2 LAN Pin Assignments

Pin Field	Backplane Pins	RJ-45 Pins
LAN 1 (Going to a router, hub, or switch)	B2	1
	A2	2
	B1	3
	A1	6
LAN 1 (Going to a PC/workstation)	B1	1
	A1	2
	B2	3
	A2	6

Note LAN 2 pins will be active in a future release.

To install LAN wires on the backplane, use #22 or #24 AWG wire. Wrap the wires on the appropriate wire-wrap pins according to local site practice. A frame ground pin is located beneath each pin field (FG2 for the LAN pin field). Wrap the ground shield of the LAN interface cable to the frame ground pin.

Warning You cannot have simultaneous connections to the front and back LAN ports. Attempting to connect to both the RJ-45 port in the front (on the TCC/TCC+ card) and the LAN pins in the back of the shelf assembly can result in loops.

1.6.4 Craft Interface Installation

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

You can use the CRAFT pins on the ONS 15454 backplane to connect a computer terminal to serve as a VT100-type craft interface. You can also use the RS-232 port on the TCC faceplate to connect a computer terminal to serve as a TL1 craft interface to the ONS 15454. Table 1-3 shows the pin assignments for the CRAFT pin field.

Table 1-3 Craft Interface Pin Assignments

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

To install craft interface wires on the backplane, use #22 or #24 AWG wire. Wrap the craft interface wires on the appropriate wire-wrap pins according to local site practice. A frame ground pin is located beneath each pin field (FG9 for the CRAFT pin field). Wrap the ground shield of the craft interface cable to the frame ground pin. Wrap the ground wire of your computer cable to pin A3 on the CRAFT pin field.

1.6.5 X.25 Installation

This pin field is not active.

1.6.6 Modem Installation

This pin field is not active.

1.6.7 TBOS Installation

This pin field is not active.

1.7 Ferrite Installation

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

Figure 1-21 shows the suggested method for attaching ferrites to power cabling. Use a single oval ferrite TDK ZCAT2035-0930 for both pair of cables and a block ferrite Fair Rite 0443164151 for each pair of cables. Wrap the cables once around and through the block ferrites and pull the cable straight through the oval ferrites. Place the oval ferrite between the ONS 15454 and the block ferrite as shown. Place the oval ferrite as close to the power terminals as possible and place the block ferrite within 5 to 6 inches of the power terminals.

Figure 1-21 Ferrites for Power Cables

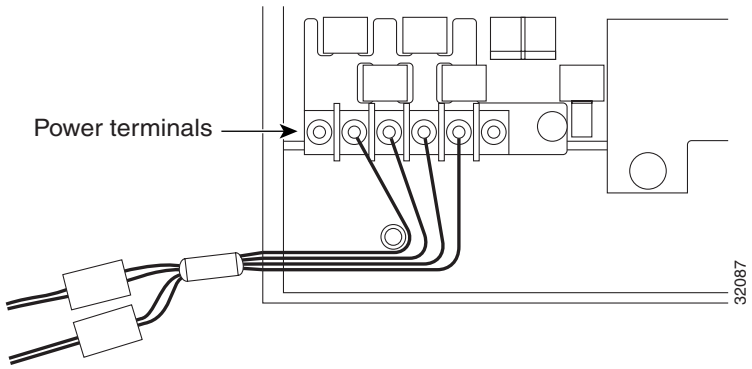


Figure 1-22 shows the suggested method for attaching the ferrites to AMP CHAMP connectors. Use a block ferrite Fair Rite 0443164151 for each cable.

Figure 1-22 Ferrites for AMP CHAMP Connectors

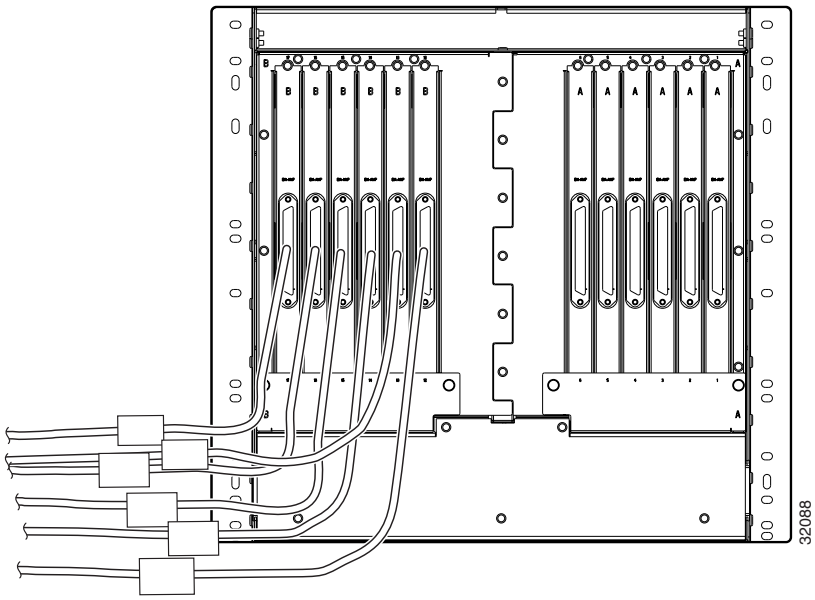


Figure 1-23 shows the suggested method for attaching the ferrites to EIAs or baluns. Use an oval ferrite TDK ZCAT 1730-0730 for each cable.

Figure 1-23 Ferrites for Electrical Interface Assemblies (EIAs) or Baluns

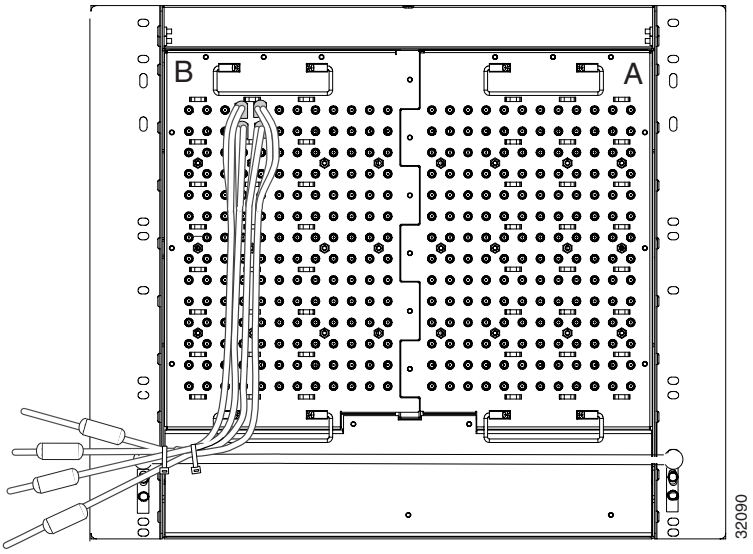


Figure 1-24 shows the suggested method for attaching the ferrites to SMB/BNC connectors. Use an oval ferrite TDK ZCAT1730-0730 for each cable and place the ferrite as close to the connector as possible.

Figure 1-24 Ferrites for SMB/BNC Connectors

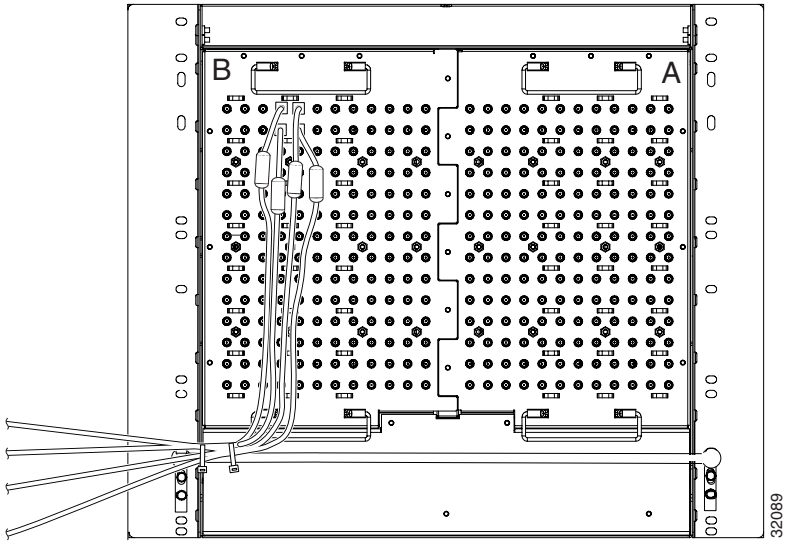
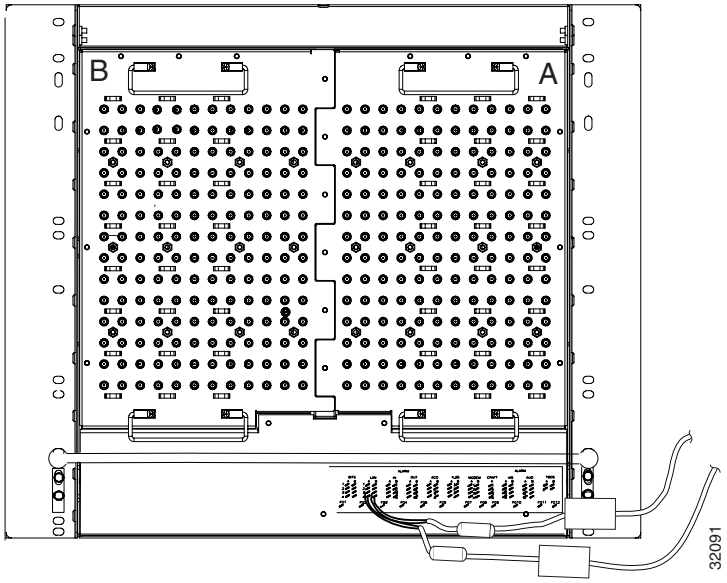


Figure 1-25 shows the suggested method for attaching the ferrites to wire-wrap pin fields. Use an oval ferrite TDK ZCAT1730-0730 and block ferrite Fair Rite 0443164151 for each pair of cables. Wrap the cables once around and through the block ferrites and pull the cables straight through the oval ferrites. Place the oval ferrite as close to the wire wrap pin field as possible and between the ONS 15454 and the block ferrite as shown. The block ferrite should be within 5 to 6 inches of the wire-wrap pin field.

Figure 1-25 Ferrites for Pin Field



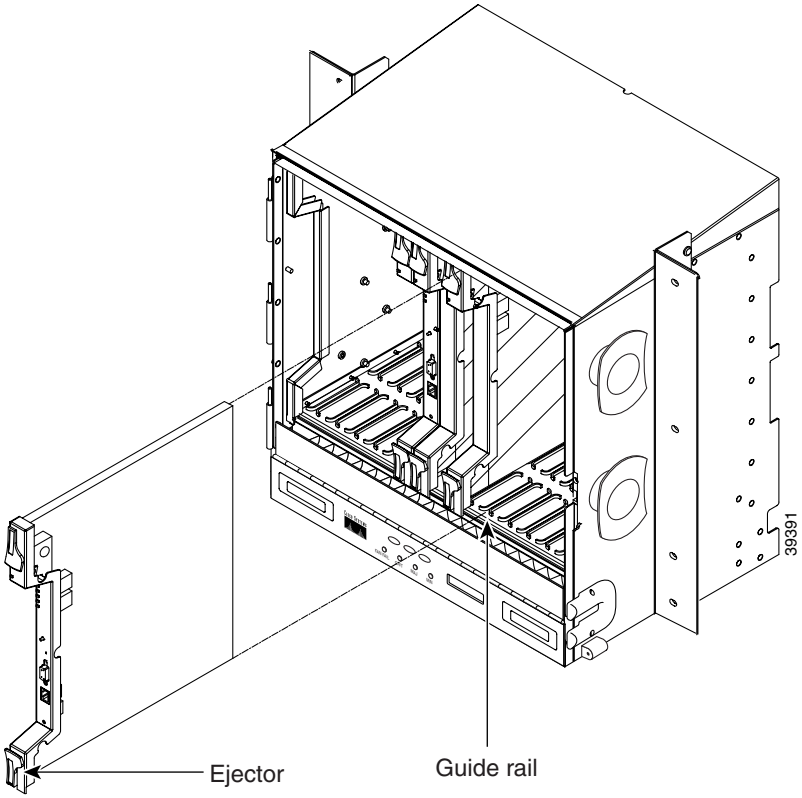
1.8 Card Installation and Turn-Up

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

ONS 15454 cards have electrical plugs at the back that plug into electrical connectors on the assembly backplane. When the ejectors are fully closed, the card plugs into the assembly backplane. Figure 1-26 shows card installation.

Warning The optical cards for the ONS 15454 are Class 1 laser products. These products have been tested and comply with Class 1 limits.

Figure 1-26 Card Installation



Procedure: Install ONS 15454 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.

1.8.1 Slot Requirements

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

- Multispeed slots have circle symbols. In these slots, only install ONS 15454 cards with a circle symbol on the faceplate.
- High-speed slots have a circle symbol and a triangle symbol. In these slots, only install ONS 15454 cards with a circle symbol or a triangle.
- TCC slots have a square symbol. In these slots, only install ONS 15454 cards with a square symbol.
- Cross-connect slots have a cross symbol. In these slots, only install ONS 15454 cards with a cross symbol.
- Protection slots have a P symbol. You can use these slots to supply 1:N protection for electrical cards.
- The AIC slot has a diamond. In this slot, only install cards with a diamond symbol in this slot.

Table 1-4 shows the slot-card symbol definitions.

Table 1-4 Slot and Card Symbols

Symbol	Color/Shape	Definition
●	Orange/Circle	Multispeed slot (all line cards except OC-48)
▲	Blue/Triangle	High speed slot (all line cards including OC-48)
■	Purple/Square	Timing, Communications, and Control (TCC/TCC+) slot
✚	Green/Cross	Cross-connect (XC/XCVT) slot
P	Red/P	Protection slot in 1:N protection schemes
◆	Red/Diamond	AIC Slot
★	Gold/Star	Multispeed slot - future

Table 1-5 lists the number of ports, line rates, connector options and connector locations for ONS 15454 optical and electrical cards.

Table 1-5 Card Ports, Line Rates, and Connectors

Card	Ports	Line Rate per Port	Connector Types	Connector Location
DS1-14	14	1.544 Mbps	SMB w/wire wrap adapter, AMP CHAMP Connector*	Backplane
DS1N-14	14	1.544 Mbps	SMB w/wire wrap adapter, AMP CHAMP Connector*	N/A
DS3-12	12	44.736 Mbps	SMB or BNC*	Backplane
DS3N-12	12	44.736 Mbps	SMB or BNC*	N/A
DS3XM-6	6	44.736 Mbps	SMB or BNC*	Backplane
EC1-12	12	51.84 Mbps	SMB or BNC*	Backplane
E100T-12	12	100 Mbps	RJ-45	Faceplate
E1000-2	2	1000 Mbps	SC (GBIC)	Faceplate
OC3 IR	4	155.52 Mbps (STS-3)	SC	Faceplate
OC-12 (IR/LR)	1	622.08 Mbps (STS-12)	SC	Faceplate
OC-48 (IR/LR/ELR)	1	2488.32 Mbps (STS-48)	SC	Faceplate

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

1.8.2 Card Turn-Up

The procedure for turning up ONS 15454 cards is nearly identical for each card. AIC card turn-up is slightly different from all other cards and is described in its own procedure, and the XC/XCVT and TCC/TCC+ turn up procedures are virtually identical and are described in one procedure. Turn up for all other cards is the same and is covered by one procedure.

Note Because all other cards boot from the active TCC/TCC+ card, at least one TCC/TCC+ card must be installed in order to boot any other cards.

Procedure: Verify Successful Turn-Up of the AIC Card

Step 1 Install the card in the correct slot.

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

Step 3 Verify that the red FAIL LED blinks for 30 to 45 seconds.

Step 4 Verify that after 30 to 45 seconds, all LEDs blink once and turn off.

Step 5 Verify that the ACT LED is on.

Step 6 Verify that the card appears in the correct slot on the CTC software screen.

Step 7 Verify that the card is white on the CTC software screen.

Procedure: Verify Successful Turn-Up of the TCC/TCC+ and XC/XCVT Cards

Step 1 Install the card in the correct slot (Slot 8 or 10 for the XC/XCVT and slot 7 or 11 for the TCC/TCC+).

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

Step 3 Verify that the red FAIL LED blinks for 30 to 45 seconds.

If the FAIL LED is displayed continuously on the TCC/TCC+ card, see the note below concerning TCC/TCC+ uploading.

Step 4 Verify that after 30 to 45 seconds, all LEDs blink once and turn off.

Step 5 Verify that the ACT/STBY LED is the correct color for the card (green for active, yellow for standby).

On the TCC/TCC+ card, the LED may take several minutes to illuminate while the DCC processor boots.

Step 6 Verify that the card appears in white in the correct slot on the CTC software screen.

Note This is not the procedure to use when upgrading from XC to XCVT cards. If you are performing an XC to XCVT upgrade, see the "Upgrade XC Cards to XCVT" section on page 5-18. If you are performing a TCC to TCC+ upgrade, see the "TCC Card to TCC+ Card Upgrade" section on page 10-11.

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

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

Procedure: Verify Successful Turn-Up of All Other Cards

Step 1 Install the card in the correct slot.

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

Step 3 Verify that the red FAIL LED blinks for 30 to 45 seconds.

Step 4 Verify that after 30 to 45 seconds, all LEDs blink once and turn off.

Step 5 Verify that the ACT LED is on. Note that the signal fail (SF) LED may persist until all card ports connect to their far end counterparts and signal is present.

Step 6 Verify that the card appears in the correct slot on the CTC software screen.

Step 7 Verify that the card is white on the CTC software screen.

1.8.3 Card Software Installation

After you install an ONS 15454 card in a valid card slot, the card's software automatically updates to the version that operates correctly with the system software installed on the TCC. To verify the current version of software installed on the XTC, click the Help menu and then click About CTC. See Chapter 5, "Provisioning Cards" for more information.

1.8.4 Gigabit Interface Converter

GBICs are hot-swappable input/output devices that plug into a Gigabit Ethernet port to link the port with the fiber optic network. Cisco provides two GBIC models: one for short reach applications (part number 15454-GBIC-SX) and one for long-reach applications (15454-GBIC-LX). The short reach, or "SX" model, connects to multimode fiber and the long reach, or "LX" model, requires single-mode fiber. Because the GBICs are very similar in appearance, check the label on the GBIC carefully before installing it. A GBIC is shown in Figure 1-27.

Figure 1-27 Gigabit Interface Converter

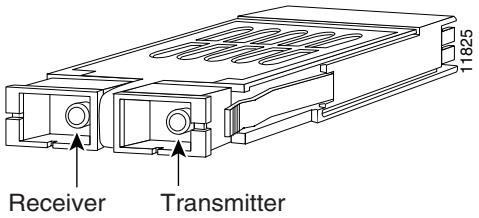


Table 1-6 shows the available GBICs.

Table 1-6 Available GBICs

GBIC	Product Number
Short wavelength (1000BaseSX)	15454-GBIC-SX
Long wavelength/long haul (1000BaseLX)	15454-GBIC-LX

- 15454-GBIC-SX

  The 15454-GBIC-SX operates on ordinary multi-mode fiber optic link spans of up to 550 m in length.

- 15454-GBIC-LX

  The 15454-GBIC-LX fully complies with the IEEE 802.3z 1000BaseLX standard. However, their higher optical quality allows them to reach 10km over single-mode fiber (SMF) versus the 5 km specified in the standard.

Procedure: Install Gigabit Interface Converters

Step 1 Remove the GBIC from its protective packaging.

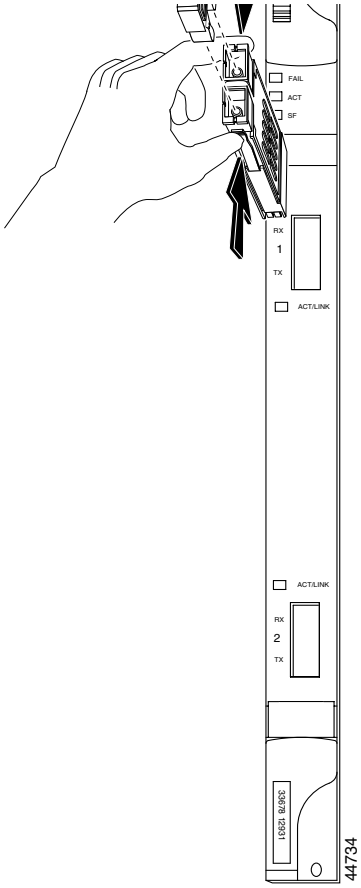
Step 2 Check the part number to verify that the GBIC is the correct type for your network.

Step 3 Grip the sides of the GBIC with your thumb and forefinger and insert it into the slot on the front panel of the Gigabit Ethernet card (shown in Figure 1-28).

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

Note GBICs are keyed to prevent incorrect installation.

Figure 1-28 GBIC Installation



Step 4 Slide the GBIC through the flap that is covering the opening until you hear a click.

The click indicates the GBIC is locked into the slot.

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

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

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

Procedure: Remove a Gigabit Interface Converter

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

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

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

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

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

1.9 Cable Installation

This section explains how to install fiber, coaxial, and DS-1 cables.

1.9.1 Fiber Cable Installation

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

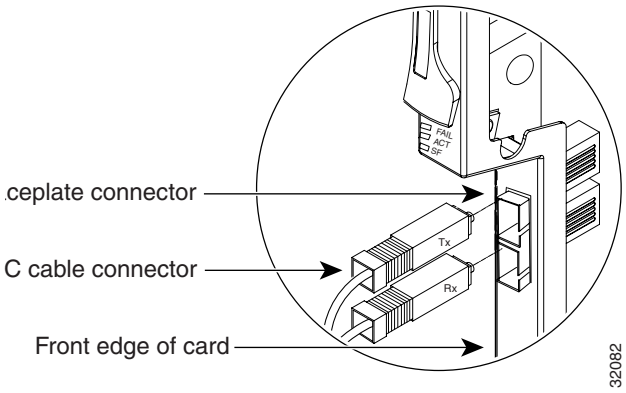
ONS 15454 fiber optic cards feature SC connectors. To install fiber optic cables in the ONS 15454, a fiber cable with the corresponding connector type must be connected to the transmit and receive ports on the ONS 15454 cards. On ONS 15454 optical card ports, the top connector is Transmit and the bottom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

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

Procedure: Install and Route Fiber Optic Cables in the ONS 15454

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 1-29 shows the cable location.

Figure 1-29 Fiber Cable Connection



Step 2 Align the keyed ridge of the cable connector with the receiving slot on the faceplate connection point.

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

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

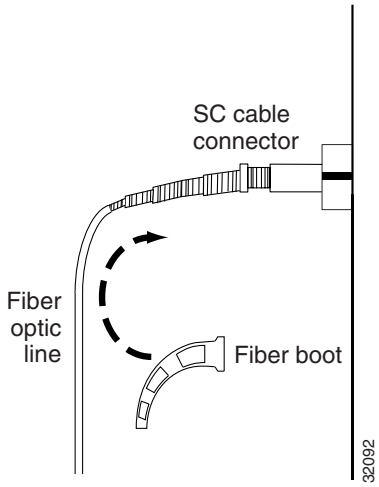
Step 5 From the cable management tray, route the fiber cables out the nearest side of the assembly through cutout holes.

See the "Cable Management Facilities" section on page 1-12 for more information about cable management.

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

Cisco provides clear plastic fiber boots for each optics card. The boots prevent hanging fibers from bending too sharply, which may degrade performance. The boots also prevent the front door from interfering with hanging fibers. Figure 1-30 shows the fiber boot attachment.

Figure 1-30 Fiber Boot Attachment



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

Procedure: Install the Fiber Boot

Step 1 Position the open slot of the fiber boot underneath the fiber cable.

Step 2 Push the fiber cable down into the fiber boot.

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

Step 4 Slide the fiber boot forward along the fiber cable until the fiber boot fits snugly onto the end of the SC cable connector.

1.9.2 Coaxial Cable Installation

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

When using ONS 15454 DS-3 electrical cables, the cables must terminate on a pre-installed EIA on the ONS 15454 backplane. EIAs are available with SMB and BNC type connectors. All DS-3 cables connected to the ONS 15454 DS-3 card must terminate with coaxial cables using the desired connector type in order to connect to the specified EIA. For information about physically installing an EIA in the field, see the "Backplane Covers" section on page 1-18.

1.9.2.1 BNC Installation

When EIAs are pre-installed on the backplane, a special backplane cover panel with cutouts over the coaxial cable connectors is provided. The BNC EIA supports 24 DS-3 circuits on each side of the ONS 15454 (24 transmit and 24 receive connectors). If you install BNC EIAs on both sides of the unit, the ONS 15454 hosts up to 48 circuits. The BNC connectors on the EIA are Trompeter UCBJ224 (75 Ohm) 4 leg connectors. Right angle mating connectors for the connecting cable are

AMP 413588-2 (75 Ohm) connectors. A straight connector of the same type can also be used, if preferred. Use RG-59/U cable to connect to the ONS 15454 BNC EIA. These cables are recommended to connect to a patch panel and are designed for long runs of up to 450 feet.

Procedure: Install Coaxial Cable With BNC Connectors

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

Figure 1-31 shows how to connect a coaxial cable to the BNC EIA using a right-angle BNC cable connector.

Step 2 Position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

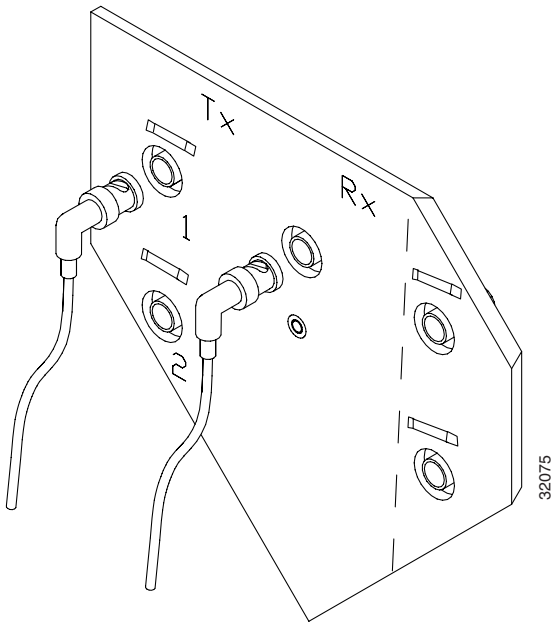
Step 3 Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector until the notch clicks into place.

Step 5 Tie wrap the cables to the EIA according to local site practice.

Step 6 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice. The rubber coated edges of the side cutouts prevent the cables from chafing.

Figure 1-31 BNC Backplane Connection Using a Right Angle Connector



Note Slots 1, 3, 15 and 17 are designated protection slots when BNC connectors are used. Slots 5, 6, 11, and 12 do not support DS3-12 cards when BNC connectors are used. A total of four DS3-12 cards may be used to carry traffic when BNC connectors are used.

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

1.9.2.2 High-Density BNC Installation

The High-density BNC EIA supports 48 DS-3 circuits on each side of the ONS 15454 (48 transmit and 48 receive connectors). If you install BNC EIAs on both sides of the unit, the ONS 15454 hosts up to 96 circuits. You must use straight connectors on RG-59/U cable to connect to the ONS 15454 High-density BNC EIA. Cisco recommends these cables for connection to a patch panel; they are designed for long runs of up to 450 feet.

Although not required, Cisco strongly recommends using the BNC insertion tool to connect cables to the EIA. See page 10-15 for more information about the insertion tool.

Procedure: Install Coaxial Cable With High-density BNC Connectors

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

Step 2 Using the insertions tool, position the cable connector so that the slot in the connector is over the corresponding notch at the backplane connection point.

Step 3 Gently push the connector down until the notch backplane connector slides into the slot on the cable connector.

Step 4 Turn the cable connector until the notch clicks into place.

Step 5 Tie wrap the cables to the EIA according to local site practice.

Step 6 Route the cables to the nearest side of the shelf assembly through the side cutouts according to local site practice.

The rubber coated edges of the side cutouts prevent the cables from chafing.

1.9.2.3 SMB Installation

The SMB backplane cover is similar to the BNC cover. The SMB EIA has 84 transmit and 84 receive connectors on each side of the ONS 15454 for a total of 168 SMB connectors (84 circuits). For DS-3 or EC-1, the EIA supports 72 transmit and 72 receive connectors, for a total of 144 SMB connectors (72 circuits.) The SMB connectors on the EIA are AMP 415504-3 (75 Ohm) 4 leg connectors. Right-angle mating connectors for the connecting cable are AMP 415484-2 (75 Ohm) connectors. Use RG-179/U cable to connect to the ONS 15454 EIA. Cisco recommends these cables for connection to a patch panel; they are not designed for long runs.

Procedure: Install SMB Type Connectors

Refer to Figure 1-32 when performing the following steps.

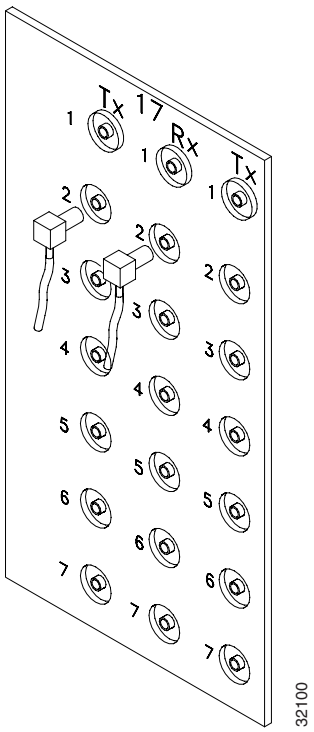
Step 1 Place the SMB cable connector over the desired connection point on the backplane.

Step 2 Gently push the connector until it clicks into place.

Step 3 Tie wrap the cables to the EIA according to local site practice.

Step 4 Route the cables to the nearest side of the shelf assembly into rack runs according to local site practice.

Figure 1-32 SMB Coaxial Cable Connections



Label the transmit, receive, working and protection cables at each end of the connection to avoid confusion with cables that are similar in appearance.

1.9.3 DS-1 Cable Installation

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

1.9.3.1 Twisted Pair Wire Wrap Installation

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

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

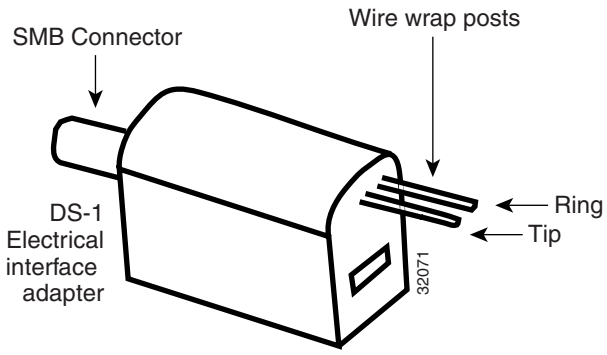
If you use DS-1 electrical twisted pair cables, equip the ONS 15454 with an SMB-based EIA on each side of the backplane where DS-1 cables will terminate. You must install special DS-1 electrical interface adapters on every transmit and receive connector for each DS-1 termination. See the "Install DS-1 Electrical Interface Adapters" section on page 1-47 for information about installing SMB backplane covers.

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

EIAs are special cards attached to the assembly backplane that provide cable connectors and a cover panel that features cutouts over the coaxial cable connectors. EIAs are available with SMB and BNC type connectors. You must use SMB EIAs for DS-1 twisted-pair cable installation.

If you install DS-1 cards in the ONS 15454, you must fit the corresponding transmit and receive SMB connectors on the EIA with a DS-1 electrical interface adapter. You can install the adapter on the SMB connector for the port. The adaptor has wire wrap posts for DS-1 transmit and receive cables. Figure 1-33 shows the DS-1 electrical interface adapter.

Figure 1-33 Electrical Interface Adapter



Each DS-1 electrical interface adapter, commonly referred to as a balun, has a female SMB connector on one end and a pair of .045 inch square wire wrap posts on the other end. The wire wrap posts are .200 inches apart.

Procedure: Install DS-1 Electrical Interface Adapters

Step 1 Attach the SMB connector on the adapter to the SMB connector for the port's transmit pair on the backplane.

Step 2 Attach the SMB connector on an adapter to the SMB connector for the port's receive pair on the backplane.

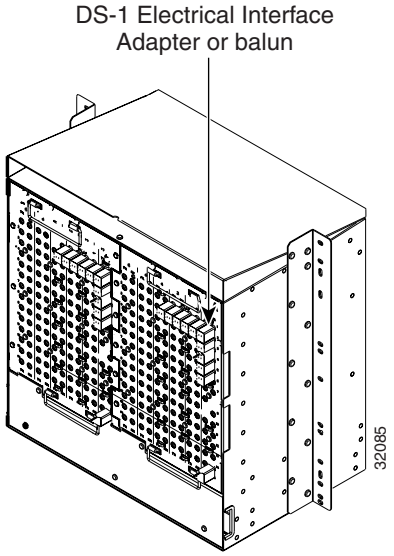
Step 3 Terminate the DS-1 transmit and receive cables for the port to the wire wrap posts on the adapter.

Make sure to install the electrical interface adapter with the wire wrap posts.

If you place DS1N-14 in Slots 3 and 15 to form 1:N protection groups, do not wire Slots 3 and 15 for DS-1 electrical interface adapters.

Figure 1-34 shows a ONS 15454 backplane with an SMB EIA with DS-1 electrical interface adapters attached on both sides of the shelf to create DS-1 twisted pair termination points.

Figure 1-34 Backplane With SMB EIA



All DS-1 cables connected to the ONS 15454 DS-1 ports must terminate with twisted-pair cables to connect to the DS-1 electrical interface adapter. The DS-1 electrical interface adapters project 1.72 inches beyond the SMB EIA.

Procedure: Install DS-1 Cables on the DS-1 Electrical Interface Adapters

Step 1 Using a wire-wrap tool, connect the receive cables to the receive adapter pins on the backplane connector for the desired port.

Step 2 Connect the transmit cables to the transmit adapter pins on the backplane connector for the desired port.

Step 3 Terminate the shield ground wire on the DS-1 cable to ground according to local site practice.

Step 4 If you place DS1N-14 cards in Slots 3 and 15 to form 1:N protection groups, do not wire Slots 3 and 15 for DS-1 electrical interface adapters.

1.9.3.2 AMP CHAMP Installation

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

Because each DS1-14 card supports 14 DS-1 ports, only 56 pins (28 pairs) of the 64-pin connector are used. Prepare one 56-wire cable for each DS-1 facility installed. Table 1-7 shows the pin assignments for the AMP CHAMP connectors on the ONS 15454 AMP CHAMP EIA. See the“AMP CHAMP EIA” section on page 1-22 for more information about the AMP CHAMP EIA.

Table 1-7 Pin Assignments for AMP Champ Connector

Signal/Wire	Pin	Pin	Signal/Wire	Signal/Wire	Pin	Pin	Signal/Wire
Tx Tip 1 white/blue	1	33	Tx Ring 1 blue/white	Rx Tip 1 yellow/orange	17	49	Rx Ring 1 orange/yellow
Tx Tip 2 white/orange	2	34	Tx Ring 2 orange/white	Rx Tip 2 yellow/green	18	50	Rx Ring 2 green/yellow
Tx Tip 3 white/green	3	35	Tx Ring 3 green/white	Rx Tip 3 yellow/brown	19	51	Rx Ring 3 brown/yellow
Tx Tip 4 white/brown	4	36	Tx Ring 4 brown/white	Rx Tip 4 yellow/slate	20	52	Rx Ring 4 slate/yellow
Tx Tip 5 white/slate	5	37	Tx Ring 5 slate/white	Rx Tip 5 violet/blue	21	53	Rx Ring 5 blue/violet
Tx Tip 6 red/blue	6	38	Tx Ring 6 blue/red	Rx Tip 6 violet/orange	22	54	Rx Ring 6 orange/violet
Tx Tip 7 red/orange	7	39	Tx Ring 7 orange/red	Rx Tip 7 violet/green	23	55	Rx Ring 7 green/violet
Tx Tip 8 red/green	8	40	Tx Ring 8 green/red	Rx Tip 8 violet/brown	24	56	Rx Ring 8 brown/violet
Tx Tip 9 red/brown	9	41	Tx Ring 9 brown/red	Rx Tip 9 violet/slate	25	57	Rx Ring 9 slate/violet
Tx Tip 10 red/slate	10	42	Tx Ring 10 slate/red	Rx Tip 10 white/blue	26	58	Rx Ring 10 blue/white
Tx Tip 11 black/blue	11	43	Tx Ring 11 blue/black	Rx Tip 11 white/orange	27	59	Rx Ring 11 orange/white
Tx Tip 12 black/orange	12	44	Tx Ring 12 orange/black	Rx Tip 12 white/green	28	60	Rx Ring 12 green/white
Tx Tip 13 black/green	13	45	Tx Ring 13 green/black	Rx Tip 13 white/brown	29	61	Rx Ring 13 brown/white
Tx Tip 14 black/brown	14	46	Tx Ring 14 brown/black	Rx Tip 14 white/slate	30	62	Rx Ring 14 slate/white
Tx Spare0+ N/A	15	47	Tx Spare0- N/A	Rx Spare0+ N/A	31	63	Rx Spare0- N/A
Tx Spare1+ N/A	16	48	Tx Spare1- N/A	Rx Spare1+ N/A	32	64	Rx Spare1- N/A

Shaded area corresponds to the white/orange binder group.

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

When using DS-1 AMP CHAMP cables, you must equip the ONS 15454 with an AMP CHAMP connector EIA on each side of the backplane where DS-1 cables will terminate. Each AMP CHAMP connector on the EIA corresponds to a slot in the shelf assembly and is numbered accordingly. The AMP CHAMP connectors have screw-down tooling at each end of the connector. See the "AMP CHAMP EIA" section on page 1-22 for information on AMP CHAMP backplane cover installation.

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

Step 1 Prepare a 56-wire cable for each DS-1 card you will install in the shelf assembly. See Table 1-7 on page 1-49 for the ONS 15454 AMP CHAMP connector pin assignments.

Step 2 Connect the male AMP CHAMP connector on the cable to the female AMP CHAMP connector on the ONS 15454 backplane.

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

The female connector has grooves on the outside edge for snapping the clips into place.

1.10 Cable Management

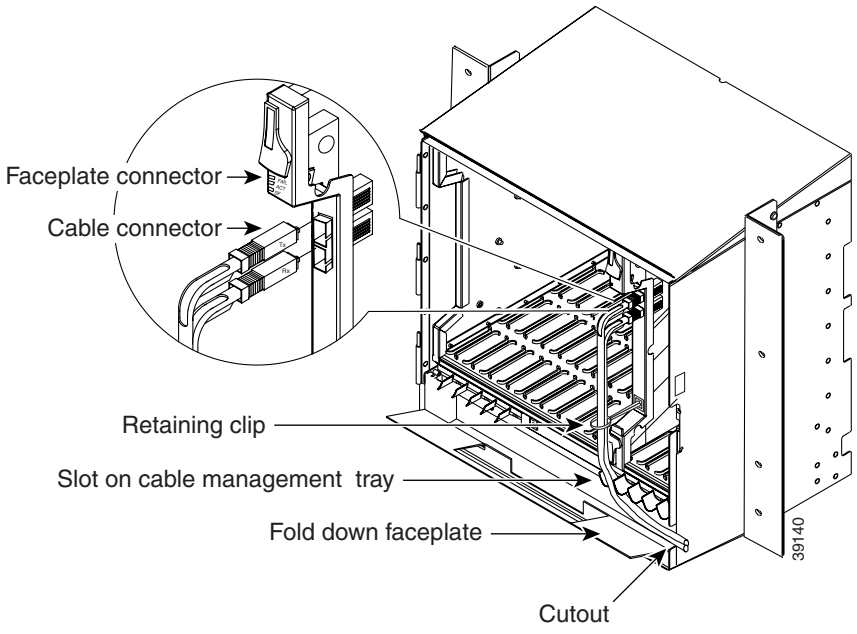
ONS 15454 cable management components include cable management clips on the optical card faceplates, a cable management tray in the front cabinet compartment, and cable tiewrap facilities on the EIAs.

1.10.1 Optical Cable Management

Optical cables connect to the SC connectors on the faceplate of the optical cards as described in the "Fiber Cable Installation" section on page 1-41. Route optical cables down through the fiber management clips on the optical card faceplate (shown in Figure 1-35).

Route optical cables from the fiber management clips into the cable management area of the shelf assembly, through a cutout in the nearest side of the assembly, and onto the side of the assembly. A hinged panel on the front of the shelf assembly folds down to provide access to the cable management tray. Figure 1-36 shows the fold-down panel and cable management tray.

Figure 1-35 Cable Routing



Procedure: Route Optical Cables in the Shelf Assembly

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

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

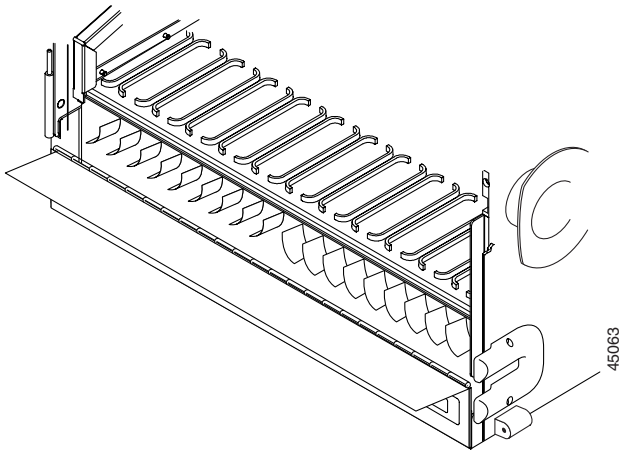
Step 3 Route the cables into the cable management tray.

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

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

Figure 1-36 shows the fold-down front door of the shelf assembly open to display the cable routing channel.

Figure 1-36 Fold-down Front Door of the Shelf Assembly



1.10.2 Coaxial Cable Management

Coaxial cables connect to the BNC type or SMB type EIAs on the ONS 15454 backplane using cable connectors. The BNC type EIAs support up to 48 transmit and receive coaxial connectors on each side of the ONS 15454 backplane for a total of up to 96 connectors (48 circuits). The SMB type EIAs support up to 84 transmit and receive coaxial connectors on each side of the ONS 15454 for a total of up to 168 connectors (84 circuits).

When EIAs are used, the backplane cover uses cutouts over the cable connectors. Incoming cables terminated with the corresponding connector type (SMB or BNC) can be connected directly onto the backplane through the cover cutouts.

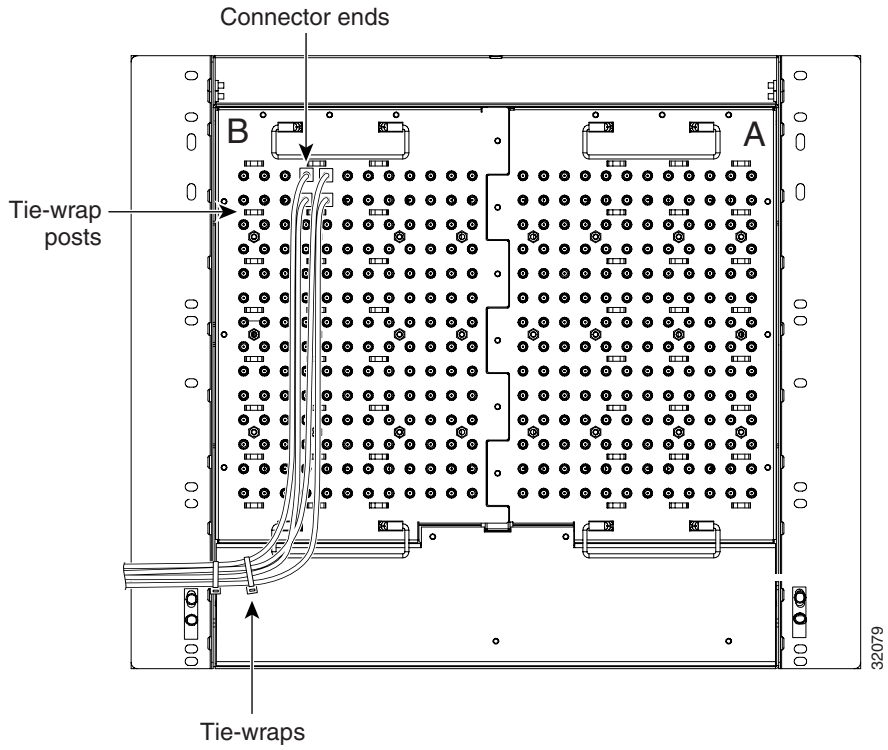
EIAs feature cable management eyelets for tie wrapping or lacing cables to the cover panel. Tiewrap or lace the coaxial cables according to local site practice and route the cables through the side cutouts on either side of the ONS 15454 assembly. The rubber coated edges of the side cutouts prevent the cables from chafing.

When using the RG179 cable with SMB connectors, remember that the maximum distance available with the RG179 cable is less than the maximum distance available with standard RG59 cable. If you only use the RG179, the maximum available distance is 100 feet versus the 450 feet available with the larger RG59 cable.

Use short lengths of "pigtail" RG179 to terminate the shelf, and use standard RG59 connected to the RG179 for the remainder of the cable run. When using a 10-foot section of the RG179, you can attach a maximum length of 437 feet of RG59. When using a 30-foot section of RG179, you can attach a maximum length of 311 feet of RG59.

The shorter maximum distance available with the RG179 is due to a higher attenuation rate for the thinner cable. The attenuation rate for RG59 cable (based on testing with Belden 923, the equivalent of 328A cable) is ~1.0 dB/100 feet at 22 Mhz (DS-3 data rate). The attenuation rate of RG179 is 6.3 db/100 feet. Use a figure of 5.0 for total cable loss when making calculations. Figure 1-37 shows one side of the ONS 15454 backplane with SMB EIAs and the coaxial cables properly routed.

Figure 1-37 Backplane Cable Routing



1.10.3 Twisted Pair Cable Management

Connect twisted pair/DS-1cables to SMB EIAs on the ONS 15454 backplane using cable connectors and DS-1 electrical interface adapters. The SMB type EIAs support up to 84 transmit and receive SMB connectors on each side of the ONS 15454 for a total of up to 168 connectors (84 circuits).

When using DS-1 twisted pair cables, the backplane cover features cutouts over the SMB cable connectors. You must install DS-1 electrical interface adapters on every transmit and receive connector for DS-1 ports. Incoming cables terminated can be connected directly onto the backplane using the wire wrap posts on the DS-1 electrical interface adapters.

SMB EIAs feature cable management eyelets for tie wrapping or lacing cables to the cover panel. Tie wrap or lace the twisted pair cables according to local site practice and route the cables into the side cutouts on either side of the ONS 15454 assembly.

1.10.4 AMP CHAMP Cable Management

AMP CHAMP cables connect to the EIAs on the ONS 15454 backplane using AMP CHAMP cable connectors. The AMP CHAMP EIAs support up to six AMP CHAMP connectors on each side of the ONS 15454 backplane for a total of up to 12 connectors.

EIAs have cable management eyelets to tiewrap or lace cables to the cover panel. Tiewrap or lace the AMP CHAMP cables according to local site practice and route the cables. If you configure the ONS 15454 for a 23-inch rack, two additional inches of cable management area are available on each side of the assembly. See the“AMP CHAMP EIA” section on page 1-22 and the “AMP CHAMP Installation” section on page 1-48 and the for more information.

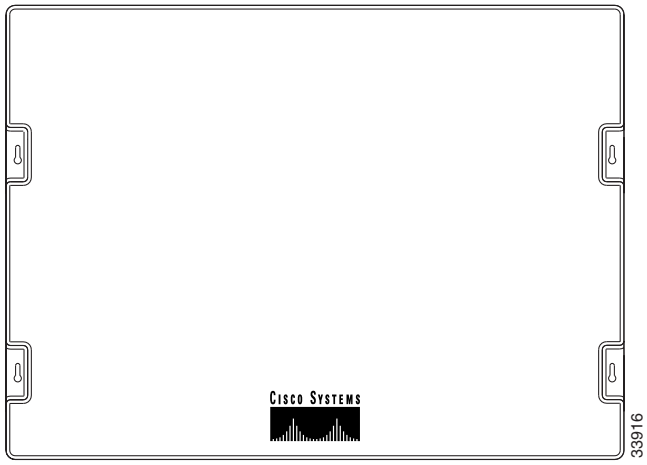
1.10.5 Alarm Cable Management

Route alarm cables out the nearest side of the shelf assembly through the space provided. Tiewrap eyelets below the alarm pin field can be used to manage alarm cables. Cutouts are protected to prevent chaffing of the cables.

1.10.6 BIC Rear Cover Installation

The ONS 15454 has an optional backplane interface connector (BIC) rear cover. This clear plastic cover provides additional protection for the cables and connectors on the backplane (Figure 1-38).

Figure 1-38 Clear BIC Rear Cover



Procedure: Install the BIC Rear Cover

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

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

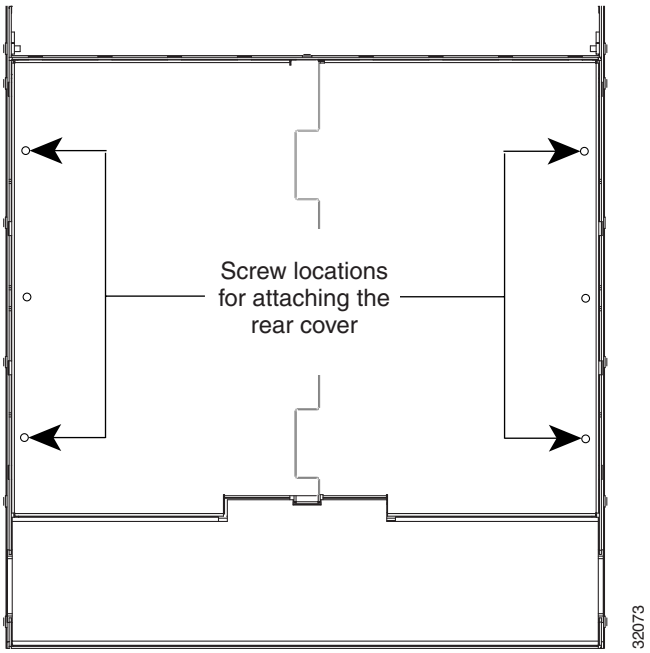
Step 2 Loosen the top and bottom screws on one edge of the backplane to provide room to slide the mounting brackets into place using the u-shaped screw slots on each end.

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

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

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

Figure 1-39 Backplane Attachment For BIC Cover



1.11 ONS 15454 Assembly Specifications

1.11.1 Bandwidth

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

1.11.2 Slot Assignments

- Total card slots: 17
- Universal slots (any traffic card except OC-48): slots 1–4, 14–17
- High speed slots (any traffic card including OC-48): slots 5, 6, 12, 13
- TCC (Timing, Communication and Control): slots 7, 11
- XC/XCVT (Cross Connect): slots 8, 10
- AIC (Alarm Interface Card): 9

1.11.3 Cards

- TCC
- TCC+
- XC
- XCVT
- AIC
- EC1-12
- E100T-12
- DS1-14
- DS1N-14
- DS3-12
- DS3N-12
- DS3XM-6
- OC3 IR 4 1310
- OC12 IR 1310
- OC12 LR 1310
- OC12 LR 1550
- OC48 IR 1310
- OC48 LR 1550
- OC48 ELR DWDM

1.11.4 Configurations

- Terminal mode
- Add-drop multiplexer
- Regenerator mode
- Two fiber BLSR ring
- Two fiber UPSR ring
- Path protected mesh network (PPMN)

1.11.5 Cisco Transport Controller

- 10 Base-T
- TCC access: RJ-45 connector
- Backplane access: LAN pin field

1.11.6 External LAN Interface

- 10 Base-T Ethernet
- Backplane access: LAN pin field

1.11.7 TL1 Craft Interface

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

1.11.8 Modem Interface

- Hardware flow control
- TCC: RS-232 DB-9 type connector
- Backplane access: MODEM pin field

1.11.9 Alarm Interface

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

1.11.10 EIA Interface

- SMB: AMP #415504-3 75 Ohm 4 leg connectors
- BNC: Trompeter #UCBJ224 75 Ohm 4 leg connector
- AMP CHAMP: AMP#552246-1 with #552562-2 bail locks

1.11.11 Database Storage

- Nonvolatile memory: 32MB, 3.0V FLASH memory

1.11.12 BITS Interface

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

- Backplane access: BITS pin field

1.11.13 System Timing

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

1.11.14 Power Specifications

- Input power: -48V DC
- Power consumption: 55W (fan tray only); 650W (maximum draw w/cards)
- Power Requirements: -42 to -57 VDC
- Power terminals: #8 Lug

1.11.15 Environmental Specifications

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

1.11.16 Dimensions

- Height: 18.5 inches (40.7 cm)
- Width: 19 or 23 inches (41.8 or 50.6 cm) with mounting ears attached
- Depth: 12 inches (26.4 cm), 5-inch projection from rack
- Weight: 55 lbs. (empty)

1.12 Node Turn-Up

This section provides the steps required for the basic turn-up of the ONS 15454 shelf assembly. The section assumes that individual cards will either be used with their default provisioning values or will be provisioned by local technicians as required by the site.

1.12.1 Installation

Table 1-8 lists the steps needed to verify a successful installation of the ONS 15454.

Table 1-8 Installation Checklist

Description	Check
ONS 15454 mounted securely in rack.	
ONS 15454 grounded with rack ground.	

Table 1-8 Installation Checklist (continued)

Description	Check
Power runs to the ONS 15454.	
Visual and Audible alarm pins connect to central alarm collection equipment.	
If used, BITS, LAN, Alarm, ACO and CRAFT pins connect to corresponding cables.	
If used, BITS, LAN, Alarm, ACO and CRAFT cables are tiewrapped and routed under screw holes.	
Preferred EIAs are installed.	
Coaxial and/or DS-1 cables installed on back of unit.	
Laced or tiewrapped coaxial cables run onto the sides of the ONS 15454.	
Power connections fused properly (15A recommended).	
-48V DC (tolerance -42 to -56V DC) power present at DC A and DC B terminals (if used) when power applied.	
Fan tray filter installed in fan tray with flow direction arrow on filter frame pointing up.	
Fan tray assembly installed. When installed, fans will run on high speed with no TCCs installed.	
If used, Ethernet patch cords are connected to Ethernet cards.	
Fiber optic and/or Ethernet patchcords route through the faceplate clips, into the fiber management tray, through the side cutout and along the sides of the ONS 15454.	
Fiber management tray able to swing up and down without disturbing fiber or Ethernet patchcords.	
Fan tray assembly able to be removed without disturbing fiber or Ethernet patchcords.	
LCD functions. (Use LCD buttons to toggle through slots, ports and states of cards).	
Door mounted with hinges on hinge pins.	
Doors open and close without disturbing fiber or Ethernet patchcords.	

1.12.2 Node Turn-Up

Table 1-9 lists the steps necessary to successfully turn-up an ONS 15454 node. Each step references the page number where the procedure for completing the step can be found. You must complete the steps listed in Table 1-8 before you begin node turn up.

Table 1-9 Node Turn Up Checklist

Description	Check
Configure computer	
Verify that the computer has a 486 or higher processor and 128 Megabytes or more of RAM. The operating system should be Windows 95/98, NT, or UNIX. The browser should either be Netscape Navigator 4.08 or higher or Microsoft Internet Explorer 4.0 or higher. Netscape Navigator can be installed from the Cisco ONS 15454 system software CD shipped with the system.	
Verify that a straight-through CAT 4 or CAT 5 cable with RJ-45 connectors on each end is used to connect the computer to the LAN port on the TCC card.	
Verify that the computer TCP/IP connection is installed on the computer. If the computer has never been connected to a network, see the Control Panel>Network>Configuration screen on Windows 95/98 to verify TCP/IP installation.	
Install Cards	
Install TCC/TCC+ and XC/XCVT cards. Slots 7 and 11 hold redundant TCC cards. Slots 8 and 10 hold redundant XC/XCVT cards. Install one TCC and let it initialize before installing any additional cards. The red Fail LED on the TCC will flash for approximately 30 seconds and all remaining LEDs will blink once in sequence. The ACT/STBY LED will be green/amber when the card is initialized. The IP address for the node, the temperature of the ONS 15454, and the time of day will be displayed on the LCD. Default time of day is 12:00 AM, January 1, 1970	
Verify that each card turns up successfully. For more information, see the “Card Turn-Up” section on page 1-37.	
Ensure that transmit and receive fiber patchcords are correctly connected to the optic cards.	
Verify that TCC/TCC+ cards and XC/XCVT cards are installed in the ONS 15454 in the correct slots. Do not operate the ONS 15454 with only one TCC/TCC+ or one XC/XCVT card installed. Always use redundant cards.	
Connect computer	
When connecting through a LAN, you must first obtain a valid IP address from your network administrator. After obtaining a valid IP address, connect directly to the ONS 15454 through either the LAN port on the TCC or the LAN pins on the rear of the shelf. In the CTC, go to the Provisioning>Network tabs and set the IP address, subnet mask, and default router address. You can also use the buttons on LCD panel to set your IP address, subnet mask, and default router address.	
Connect the computer LAN cable to the RJ-45 port marked “LAN” on the faceplate of a TCC card.	
Get the IP address for the node from the LCD screen on the ONS 15454. Record the IP address for future reference.	
Open the Internet browser to connect with the network element.	
Enter the ONS 15454's IP address in the address field of the browser program. Press Return.	
Log into the CTC	
A log in screen appears. No password is required for the first log in. Network administrators should set up a new user name and a password for security. User names and passwords are case sensitive.	
The CTC main screen appears. The screen graphically depicts the ONS 15454 shelf assembly.	

Table 1-9 Node Turn Up Checklist (continued)

Description	Check
Verify that the TCC and XC/XCVT card(s) are correctly installed. The cards appear in the graphic depiction of the shelf assembly as white when successfully installed. The card name and slot numbers where the cards are installed should be identical to the physical installation.	
Set up security	
To set up user security accounts, go to the Provisioning>Security screen. Superusers can add and modify other accounts.	
Set up accounts for users as required for the local site.	
Provision node	
Go to the Provisioning>General screen. The Node Name, Contact, and Description are displayed. Set the node name.	
In the Provisioning>General screen, set the time zone, date, and time options as desired.	
Go to the Provisioning>Ring screen. Configure the Node ID to Ring Disabled, or to the desired ring number in a BLSR ring configuration.	
Connect to the ONS 15454 over a Local Area Network (LAN)	
Change the ONS 15454 IP address to a valid local LAN network IP address in the Provisioning>Network screen.	
Select the subnet mask.	
Enter a valid default router, if applicable.	
Click Apply to reboot the TCC card and activate the new address.	
Change TCP/IP settings on the PC connected to the ONS 15454 so that it is on the same subnet as the Gateway network element.	
Verify that the Netmask field on the PC's TCP/IP settings match the ONS 15454's subnet mask.	
Restart the PC, if necessary.	
After restart, open the browser software and enter the new IP address assigned to the ONS 15454.	
Select Provisioning>SonetDCC to view the DCCs over SONET links. DCCs are disabled by default. Select and enable desired DCCs.	
Provision Timing References	
Set timing references for the shelf assembly. Select Provisioning>Timing.	
For an external BITS clock, set the Timing Mode to External Time.	
For Synchronous Status Messaging (SSM), the SSM Message Set field displays clock specifications.	
Set Quality of RES to the Quality of the timing reference being received, if applicable.	
Set BITS 1 and BITS 2 to In Service. The Coding and Framing fields display clock specifications.	
Check the Sync Messaging Enabled box if you are using SSM.	
Set the AIS Threshold if AIS should be inserted on the BITS. (Not supported when SSM is enabled.)	
Set NE Reference 1 and NE Reference 2 to BITS 1 and BITS 2, respectively.	
Set BITS 1 Out and BITS 2 Out as desired to provide timing output using the timing output pins on the ONS 15454 backplane.	
Install any service cards to be used in the ONS 15454. Slot restrictions may apply.	
Verify that when a card is installed, the Fail LED blinks for over 30 seconds and then the remaining LEDs each flash once in sequence.	

Table 1-9 Node Turn Up Checklist (continued)

Description	Check
Verify that the green ACT LED turns on for active cards and the yellow STBY LED turns on for standby cards. The yellow SF LED may persist if far-end ports are not all connected.	
Verify that all cards are installed in the correct slots and are white on the main CTC craft interface screen. This confirms that each card is installed successfully.	
Go to the Alarms screen and verify that no equipment alarms are issued against the installed cards.	
Connect all cables (near end and far end) for each installed service card port.	
Provision Ports	
Go to the service card's Provisioning screen for all connected ports and set the ports to In Service.	
For ports that use concatenation, set concatenation as needed within the Circuit provisioning screen.	
Check Enabled Sync Messages box to use SSM on each port, if applicable.	
Ensure that all links are active to external network elements where cross-connects will be mapped.	
Map cross-connects to the Circuits tab and create cross-connects as needed.	
Verify Protection and Save the Database	
Remove active cards to verify that standby cards become active.	
Save the network element database. Record the location of the saved database file for future reference.	

1.13 ONS 15454 Software and Hardware Compatibility Matrix

Table 1-10 provides a matrix showing software and hardware compatibility for ONS 15454 Releases 2.0, 2.1, and 2.2.0.

Table 1-10 ONS 15454 Software and Hardware Compatibility

Hardware	2.00.0x (2.0)	2.10.0x (2.1)	2.20.0x (2.2.0)
TCC	Fully compatible	Fully Compatible	Fully Compatible
TCC+	Not Supported	Not Supported	Fully Compatible
XC	Fully Compatible	Fully Compatible	Fully Compatible
XCVT	Fully Compatible	Fully Compatible	Fully Compatible
AIC	Fully Compatible	Fully Compatible	Fully Compatible
EC1-12	Fully Compatible	Fully Compatible	Fully Compatible
E100T-12	Fully Compatible	Fully Compatible	Fully Compatible
E1000-2	Not Supported	Not Supported	Fully Compatible
DS1-14	Fully Compatible	Fully Compatible	Fully Compatible
DS1N-14	Fully Compatible	Fully Compatible	Fully Compatible
DS3-12	Fully Compatible	Fully Compatible	Fully Compatible
DS3N-12	Fully Compatible	Fully Compatible	Fully Compatible
DS3XM-6	Fully Compatible	Fully Compatible	Fully Compatible
OC3 IR 4 1310	Fully Compatible	Fully Compatible	Fully Compatible
OC12 IR 1310	Fully compatible	Fully Compatible	Fully Compatible

Table 1-10 ONS 15454 Software and Hardware Compatibility (continued)

OC12 LR 1310	Fully compatible	Fully Compatible	Fully Compatible
OC12 LR 1550	Fully compatible	Fully Compatible	Fully Compatible
OC48 IR 1310	Fully compatible	Fully Compatible	Fully Compatible
OC48 LR 1550	Fully compatible	Fully Compatible	Fully Compatible
OC48 ELR 1550	Not Supported	Fully Compatible	Fully Compatible

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

Card Reference

This chapter describes the Cisco ONS 15454 cards. It includes descriptions, hardware specifications, and block diagrams for each card. For installation and turn-up procedures, see Chapter 1, "Installation."

2.1 Overview

The cards for the ONS 15454 include common control cards, electrical cards, optical cards, and an Ethernet/Fast Ethernet card. Each card is marked with a symbol that corresponds to a slot (or slots) on the ONS 15454 shelf assembly. The cards are then installed into slots displaying the same symbols (see the "Slot Requirements" section on page 1-36 for a list of slots/symbols). This overview provides a summary of the cards.

2.1.1 Common Control Cards

The four common control cards are the Timing Communications and Control (TCC/TCC+) card, the Cross Connect (XC) card, the VT1.5 Capable Cross Connect (XCVT) card, and the Alarm Interface Controller (AIC) card. The TCC is the main processing center of the ONS 15454 and provides system initialization, provisioning, alarm reporting, maintenance, and diagnostics. The XC/XCVT card is the central element for switching; it establishes connections and performs time division switching (TDS). The AIC card provides customer-definable alarms with its additional input/output alarm contact closures.

2.1.2 Electrical Cards

The electrical cards are the EC1-12, DS1-14, DS1N-14, DS3-12, DS3N-12, and the DS3XM-6 (Transmux). The EC1-12 card provides twelve STS-1 electrical interfaces. The DS1-14 card provides 14 DS-1 interfaces. The DS1N-14 card provides 14 DS-1 interfaces but can also provide 1:N protection when necessary. The DS3-12 card has 12 DS-3 interfaces and the DS3N-12 card has 12 DS-3 interfaces and 1:N protection capability. The DS3XM-6 card can convert six framed DS-3 network connections into 168 VT1.5s.

2.1.3 Optical Cards

The optical cards include the OC3IR 4 1310, the OC12IR 1310, the OC12 LR 1310, the OC12 LR 1550, the OC48 IR 1310, and the OC48 LR 1550 cards. The OC3IR 4 1310 card provides four intermediate or short-range OC-3 interfaces. The OC12IR 1310 card provides one intermediate or short range OC-12 interface. The OC12 LR 1310 card and the OC12 LR 1550 card each have one

long-range OC-12 interface but operate at different wavelengths (1310 nm and 1550 nm, respectively). The OC48 IR 1310 card and the OC48 LR 1550 card each provide one long-range OC-48 interface and, like the OC12 LR cards, operate at different wavelengths (1310 nm and 1550 nm, respectively). The OC48 Extended Long Reach (ELR) cards provide the dense wavelength division multiplexing (DWDM) solution for the ONS 15454. There are eighteen OC48 ELR cards; nine operate in the red band on different wavelengths and nine operate in the blue band on different wavelengths.

2.1.4 Ethernet Card

The E100T-12 card provides twelve switched, autosensing, 10/100 Base-T Ethernet interfaces. The Ethernet card reduces the need for certain external Ethernet aggregation equipment such as hubs or switches.

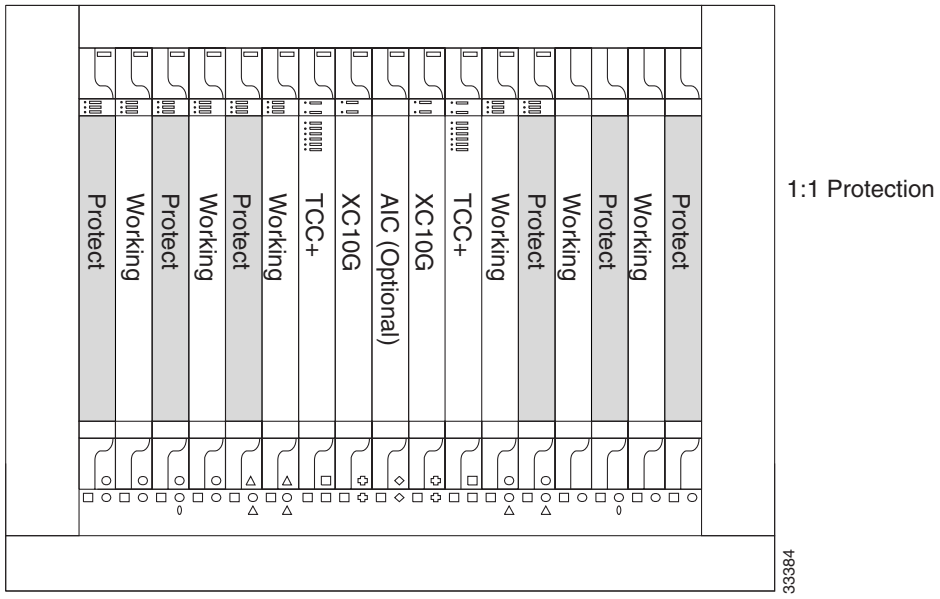
2.2 Electrical Card Protection

The ONS 15454 provides a variety of electrical card protection methods. This section describes the protection options. Figure 2-3 shows a 1:1 protection scheme and Figure 2-2 shows a 1:N protection scheme.

2.2.1 1:1 Protection

In 1:1 protection, a working card is paired with a protect card of the same type. If the working card fails, the traffic from the working card switches to the protect card. By default, the switched traffic stays on the protect card. Figure 2-1 shows the ONS 15454 in a 1:1 protection configuration; Slot 1 is protecting Slot 2, Slot 3 is protecting Slot 4, Slot 5 is protecting Slot 6, Slot 17 is protecting Slot 16, Slot 15 is protecting Slot 14, and Slot 13 is protecting Slot 12. Each working card is paired with a protect card.

Figure 2-1 1:1 Protection Configuration



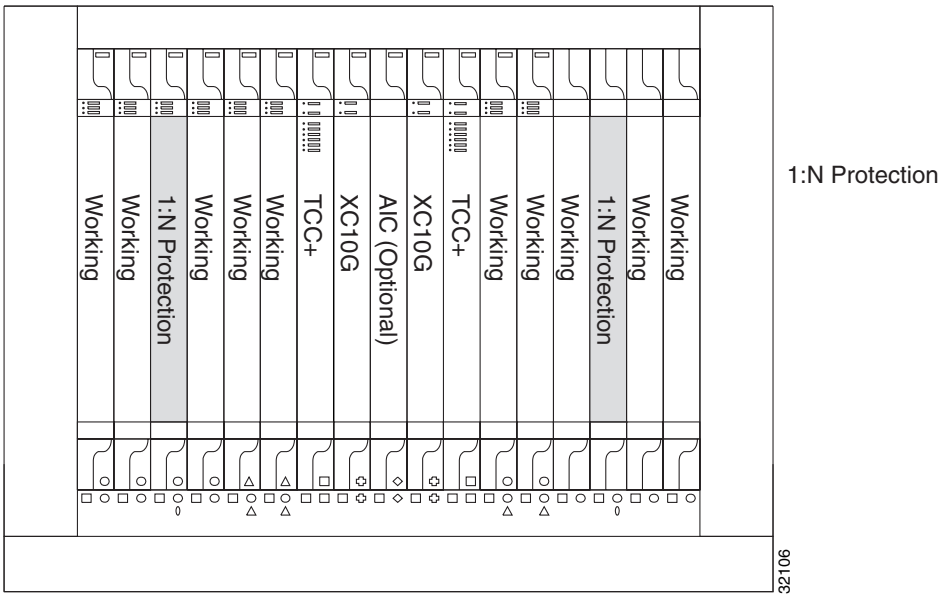
2.2.2 1:N Protection

1:N protection allows a single card to protect several working cards. A DS1N-14 card provides protection for up to five DS1-14 cards, and a DS3N-12 card protects up to five DS3-12 cards. With the 1:1 protection offered by a standard DS1-14 card or DS3-12 card, protection extends only to the single working card paired with the standard protection card.

Currently, 1:N protection operates only at the DS-1 and DS-3 levels. 1:N protect cards must match the levels of their working cards. For example, a DS1N-14 protects only DS1-14 or other DS1N-14 cards, and a DS3N-12 protects only DS3-12 or other DS3N-12 cards. 1:N cards have added circuitry to act as the protection card in a 1:N protection group. Otherwise, the card is identical to the standard card and can serve as a normal working card.

The physical DS-1 or DS-3 interfaces on the ONS 15454 backplane use the working card until the working card fails. When the system detects this failure, the protection card takes over the physical DS-1 or DS-3 electrical interfaces through the relays and signal bridging on the backplane. Figure 2-2 shows the ONS 15454 in a 1:N protection configuration. Each side of the shelf has only one card protecting all of the cards on that side.

Figure 2-2 1:N Protection Configuration



2.2.2.1 Revertive Switching

1:N protection supports revertive switching. Revertive switching sends the electrical interfaces back to the original working card after the card comes back online. Detecting an active working card triggers the reversion process. There is a variable time period for the lag between detection and reversion, called the revertive delay, which you can set using the Cisco Transport Controller (CTC). (For instructions, see the "Configure the BLSR" section on page 4-8 and the "Create a Circuit" section on page 4-41.) All cards in a protection group share the same reversion settings. 1:N protection groups default to automatic reversion.

2.2.2.2 1:N Protection Guidelines

Several rules apply to 1:N protection groups in the ONS 15454:

- Working and protect card groups must reside in the same card bank (A or B).
- The 1:N protect card must reside in Slot 3 for side A and Slot 15 for side B.
- Empty slots or non-protection group cards must not separate the cards in a protection group.
- Working cards may sit on either or both sides of the protect card.

The ONS 15454 supports 1:N equipment protection for all add-drop multiplexer configurations (ring, linear, and terminal), as specified by GR-253-CORE.

The ONS 15454 automatically detects and identifies a 1:N protection card when the card is installed in Slot 3 or Slot 15. However, the slot containing the 1:N card in a protection group must be manually provisioned as a protect slot because by default all cards are working cards.

For detailed procedures on setting up DS-1 and DS-3 protection groups, see the "Converting DS-1 and DS-3 Cards From 1:1 to 1:N Protection" section on page 5-14.

2.2.3 Electrical Card Protection and the Backplane

Protection schemes for electrical cards differ slightly depending on the Electrical Interface Assembly (EIA) type used on the ONS 15454 backplane. The difference is due to the varying connector size. For example, because BNC connectors are larger, fewer DS3-12 cards can be supported when using a BNC connector.

Caution When a protection switch moves traffic from the DS3-12 working/active card to the DS3-12 protect/standby card, ports on the new working/standby card cannot be taken out of service. Lost traffic can result when a port is taken out of service even if the DS3-12 working/standby card no longer carries traffic.

2.2.3.1 BNC Protection

When you use BNC connectors, the ONS 15454 supports 1:1 protection or 1:N protection for a total of four working DS-3 electrical cards. If you are using EC-1 electrical cards with the BNC EIA, the ONS 15454 supports 1:1 protection and a total of four working cards. Slots 2, 4, 14 and 16 are designated working slots. These slots are mapped to a set of 12 BNC connectors on the EIA. These slots can be used without protection for unprotected DS-3 access. With 1:N or 1:1 protection, slots 1, 3, 15 and 17 are designated for protection when BNC connectors are used. With 1:N protection, Slots 3 and 15 are also designated for protection when BNC connectors are used. Slots 5, 6, 12, and 13 do not support DS3-12 cards when you use the regular BNC EIA.

2.2.3.2 High-Density BNC Protection

When you use the High-density BNC EIA, the ONS 15454 supports 1:1 protection or 1:N protection for eight total working DS-3 electrical cards. If you are using EC-1 electrical cards with the BNC EIA, the ONS 15454 supports 1:1 protection and a total of eight working cards. Slots 1, 2, 4, 5, 13, 14, 16, and 17 are designated working slots. These slots are mapped to a set of 12 BNC type connectors on the EIA. These slots can be used without protection for unprotected DS-3 or EC-1 access. Slots 3 and 15 are designated for 1:N protection slots when BNC connectors are used with the High-density BNC EIA. Slots 6 and 12 do not support DS-3 or EC-1 cards when you use the High-density BNC EIA.

2.2.3.3 SMB Protection

When you use SMB connectors, the ONS 15454 supports 1:1 or 1:N protection. 1:1 and 1:N protection are available for the DS-1 and the DS-3 electrical cards. If you are using EC-1 cards with the SMB EIA, the ONS 15454 supports 1:1 protection. Working and protection electrical cards are defined by card slot pairs (note that the same card is used for working and protect modules; the protection of the card is defined by the slot in which it is housed). Each slot maps to a set of 12 or 14 SMB connectors on the EIA depending on the number of ports on the corresponding card. Any slot can be used without protection for unprotected DS-1, DS-3, or EC-1 access.

The DS1N-14 card can be a working or protect card in 1:1 or 1:N protection schemes. When used with 1:N protection, the DS1N-14 card can protect up to five DS1-14 plug-ins using the SMB connectors with the DS-1 electrical interface adapters.

2.2.3.4 AMP CHAMP Protection

When you use AMP CHAMP connectors, the ONS 15454 supports 1:1 or 1:N protection. Working and protection spans are defined by card slot pairs.

The DS1N-14 card can be a working or protect card in 1:1 or 1:N protection schemes. When used with 1:N protection, the DS1N-14 card can protect up to five DS1-14 plug-ins using the AMP CHAMP EIA.

2.3 Optical Card Protection

The ONS 15454 currently supports 1+1 span protection to create redundancy for optical cards. Working and protection spans are defined by card slot pairs. 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.

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

2.4 Multiport Card Protection

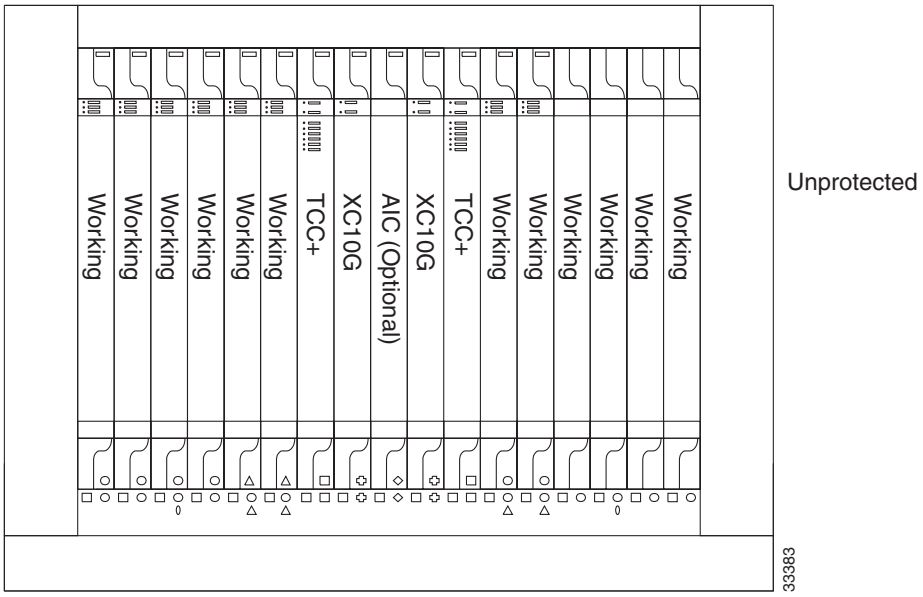
For multiport cards such as the DS3-12 and the OC-3, the ports on the card in the protection slot support the card in the working slot. With 1:1 or 1:N protection (electrical cards), the protect card must protect an entire slot. In other words, all the ports on the protect card will be used in the protection scheme. With 1+1 protection (optical cards), protection can be assigned on a per-port basis. In other words, any number of ports can be assigned as protection ports. On a four-port card, for example, you could assign one port as a protection port (protecting the corresponding port on the active card) and leave three ports unprotected. Conversely, you could assign three ports as protection ports and leave one port unprotected.

Protection schemes can be modified using the CTC software. See the “Creating Protection Groups” section on page 3-26 for more information.

2.5 Unprotected Cards

Unprotected cards are not included in a protection scheme; therefore, a card failure or a signal error results in lost data. Because no bandwidth lies in reserve for protection, unprotected schemes maximize the available ONS 15454 bandwidth. Figure 2-3 shows the ONS 15454 in an unprotected configuration. All cards are in a Working state.

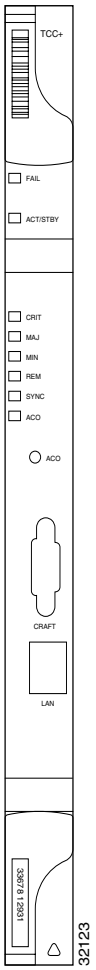
Figure 2-3 Unprotected Configuration



2.6 Timing Communication and Control (TCC/TCC+) Card

The TCC/TCC+ performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET Data Communications Channel (DCC) termination, and system fault detection for the ONS 15454. The TCC/TCC+ also ensures that the system maintains Telcordia timing requirements. The TCC and the TCC+ perform essentially identical functions but are not identical cards. The TCC+ is intended as a migration vehicle to future software releases. Figure 2-4 shows the TCC faceplate and Figure 2-5 shows a block diagram of the card.

Figure 2-4 TCC Faceplate



2.6.1 TCC/TCC+ Functionality

The TCC/TCC+ supports multichannel, high-level data link control (HDLC) processing for the DCC. Up to 48 DCCs can be routed over the Serial Communication Interface (SCI) and terminated at the TCC/TCC+. The TCC/TCC+ selects and processes ten DCCs to facilitate remote system management interfaces.

The TCC/TCC+ also originates and terminates 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 node database, IP address, and system software are stored in TCC/TCC+ non-volatile memory, which allows quick recovery in the event of a power or card failure.

The TCC/TCC+ performs all system-timing functions for each ONS 15454. The TCC/TCC+ monitors the recovered clocks from each traffic card and two DS-1 (BITS) interfaces for frequency accuracy. The TCC/TCC+ selects a recovered clock, a BITS, or an internal Stratum 3 reference as the system-timing reference. You can provision any of the clock inputs as primary or secondary timing sources. A slow-reference tracking loop allows the TCC/TCC+ to synchronize to the recovered clock, which provides holdover if the reference is lost.

Install TCC/TCC+ cards in Slots 7 and 11 for redundancy. If the active TCC/TCC+ fails, traffic switches to the protect TCC/TCC+. All TCC/TCC+ protection switches conform to protection switching standards when the BER counts are not in excess of E10-3 and completion time is less than 50 ms.

The TCC/TCC+ features an RJ-45 10Base-T LAN port and an RS-232 DB9 type craft interface for user interfaces. The craft port runs at 9600 bps.

Caution Cisco does not recommend operating the ONS 15454 with only one TCC/TCC+ card. To safeguard your system, always operate in a redundant configuration.

2.6.2 Unique TCC+ Functionality

The TCC+ is a memory-enhanced version of the first generation Timing Communication and Control card. The TCC+ will allow the ONS 15454 to scale from a multiservice OC-48 platform to a multiservice OC-192 platform in future releases without the need for an additional processor upgrade.

The enhanced memory of the TCC+ enable it to support the added features that future releases bring. Software Release 2.1 recognizes both processors; therefore, if a mixture of processors exist on the same shelf, the mismatch is flagged by the system. The TCC and the TCC+ can coexist on a network level but not on a shelf level. An upgrade to Release 2.2.0 software is required before you can install the TCC+.

2.6.3 TCC/TCC+ Card-Level Indicators

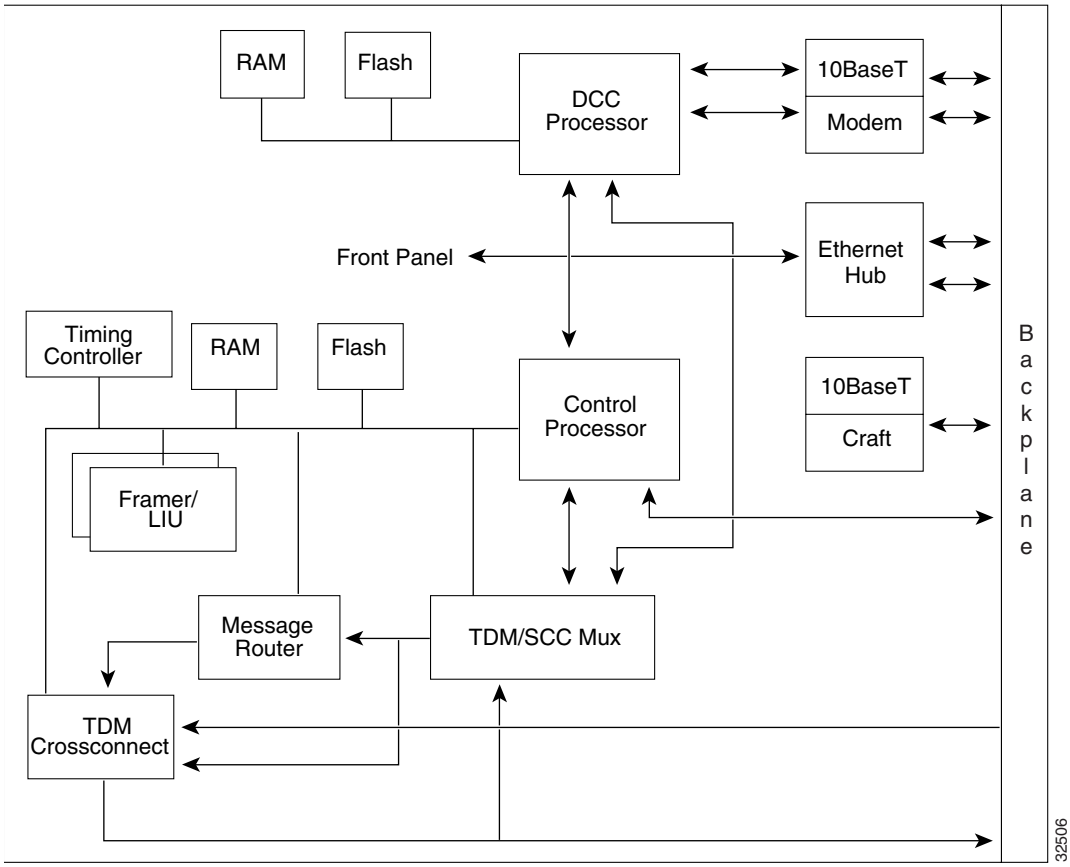
The TCC faceplate has eight LEDs. The first two LEDs are card-level indicators. The red FAIL LED indicates a TCC hardware problem. Replace the unit if the FAIL LED persists. The ACT/STBY (Active/Standby) LED indicates whether the TCC is active and providing the timing reference and shelf control (green), or is in standby to the active TCC (yellow).

2.6.4 System Level Indicators

The two red LEDs, CRIT and MAJ, indicate critical and major alarms in the system at the local terminal. The yellow MIN LED indicates a minor alarm. To provide first-level alarm isolation, the red REM LED illuminates when an alarm is present in one or several of the remote terminals. The green SYNC LED indicates that system timing is synchronized to an external reference.

Press the alarm cutoff (ACO) button to open the audible closure on the backplane. When the ACO function is activated, the green ACO LED illuminates. ACO state is stopped if a new alarm occurs. After the originating alarm is extinguished, the ACO LED and audible alarm control are reset.

Figure 2-5 TCC Block Diagram



2.6.5 TCC/TCC+ Specifications

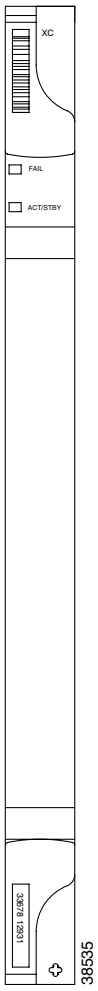
- CTC Software
  - Interface: 10 Base-T LAN
  - Backplane access: wire wrap
- TL1 Craft Interface
  - Speed: 9600 baud
  - Front panel access: RS-232 DB9 type connector
- Synchronization
  - Stratum 3 per Telcordia GR-253-CORE
  - Free running access: accuracy 4.6 ppm
  - Holdover Stability: 3.7 $x10^{-7}$ppm/day including temperature (<255 slips in first 24 hours)
  - Reference: External BITS, line, internal

- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 20W
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.7 Cross Connect Card

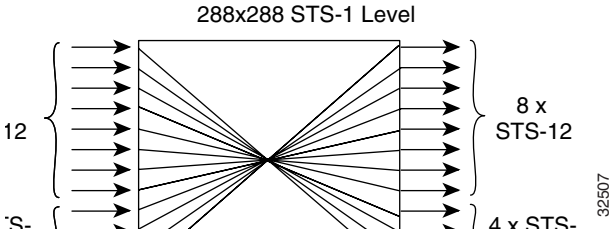
The Cross Connect (XC) card is the central element for ONS 15454 switching. It establishes connections and performs time division switching (TDS) at the STS-1 level between ONS 15454 traffic cards. The XC card faceplate, cross-connections, and functions are shown in Figure 2-6, Figure 2-7, and Figure 2-8.

Figure 2-6 XC Card Faceplate



The switch matrix on the XC card consists of 288 bidirectionsal 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 fully crosspoint, 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 2-7 Cross-Connect Matrix



The XC card has 12 input ports and 12 output ports. Four input and output ports operate at either STS-12 or STS-48 rates. The remaining eight input and output ports operate at the STS-12 rate. An STS-1 on any of the input ports can be mapped to an STS-1 output port, thus providing full STS-1 time slot assignments (TSA).

The XC card works with the TCC/TCC+ card to maintain connections and set up cross-connects within the ONS 15454. Either the XC or XCVT is required to operate the ONS 15454. You establish cross-connect and provisioning information through the user interface on the TCC/TCC+. The TCC/TCC+ establishes the proper internal cross-connect information and relays the set-up information to the XC card.

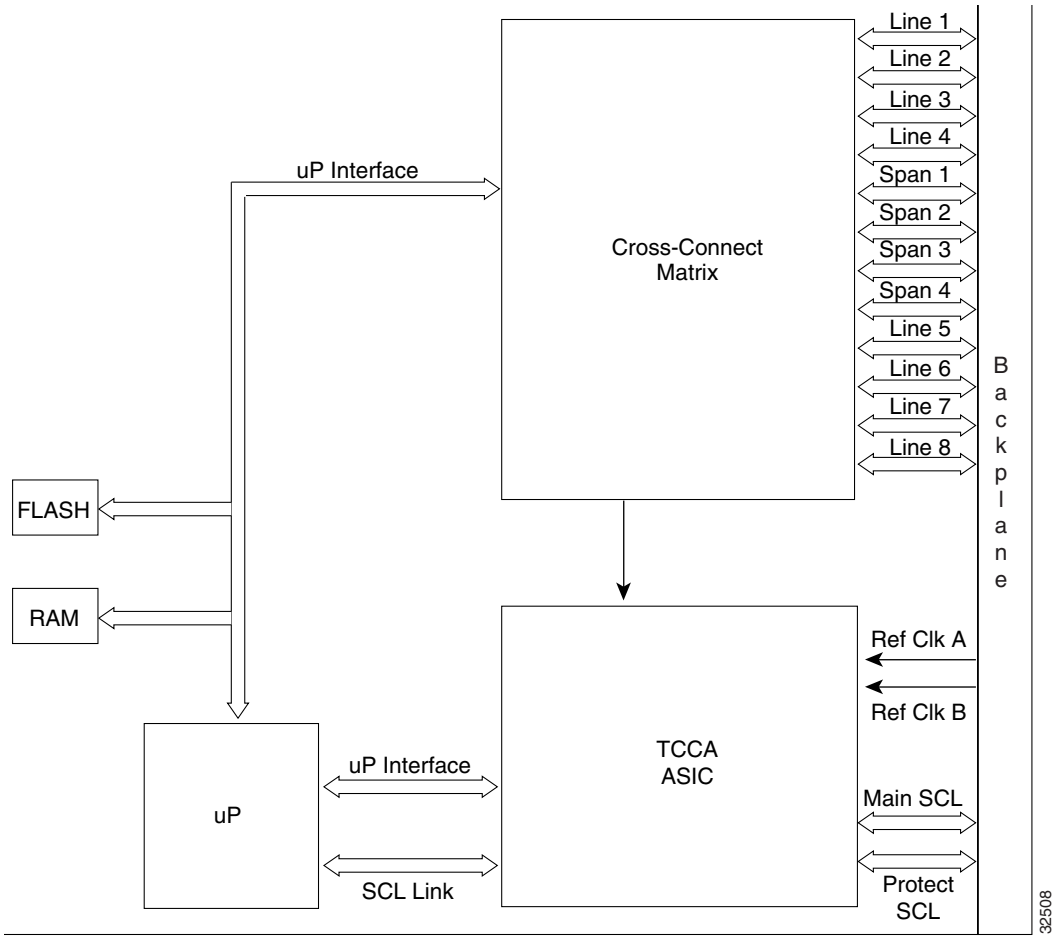
For simplex operation, you can install a single XC card in Slots 8 or 10. A second XC can be added for redundancy. The card has no external interfaces. All card interfaces are provided through the ONS 15454 backplane.

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

2.7.1 XC Card-Level Indicators

The XC faceplate has two card-level LEDs. The red FAIL LED indicates a hardware problem. If the FAIL LED persists, replace the card. The ACT/STBY LED indicates whether the XC is active and carrying traffic (green) or in standby mode to the active XC (yellow).

Figure 2-8 XC Block Diagram



2.7.2 XC Specifications

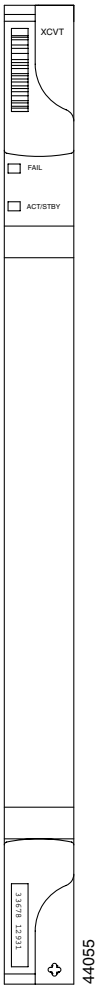
- Cross-Connect
  - Connection Setup Time: 5 ms
  - Latency: 270 ns
- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 16 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.8 Cross Connect VT Card

The XCVT card (Figure 2-9) provides the same STS capability as a standard XC card. It provides non-blocking STS-48 capacity to all of the high-speed slots and non-bidirectional blocking STS-12 capacity to all low-speed slots. This creates a fully non-blocking, 288-port, STS-1 matrix.

The XCVT faceplate, cross-connections, and functions are shown in Figure 2-9, Figure 2-10, and Figure 2-11.

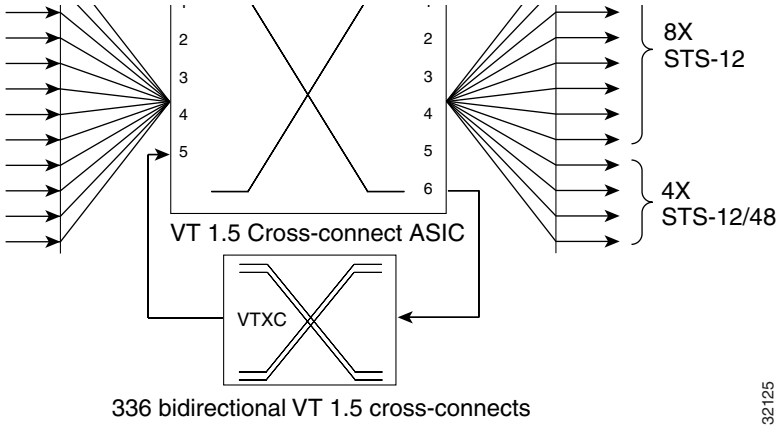
Figure 2-9 XCVT Faceplate



The XCVT card adds VT1.5 cross-connect capability to the standard STS-level capability. This allows the XCVT card to manage up to 336 bidirectional VT1.5s or the equivalent of a bidirectional STS-12. The VT1.5-level signals can be cross connected, dropped, or rearranged. The TCC assigns bandwidth to each slot on a per STS-1 or per VT1.5 basis.

The XCVT card works with the TCC card to maintain connections and set up cross-connects within the system. Either the XCVT or XC is required to operate the ONS 15454. You can establish cross-connect and provisioning information through the user interface on the TCC. The TCC establishes the proper internal cross-connect information and relays the setup information to the XCVT card.

Figure 2-10 XCVT Cross-Connect Matrix



2.8.1 VT Mapping

The Cisco ONS 15454 performs Virtual Tributary (VT) mapping according to Telcordia GR-253 standards. Table 2-1 shows the VT numbering scheme for the ONS 15454 as it relates to the Telcordia standard.

Table 2-1 ONS 15454 VT Mapping

ONS 15454 VT Number	Telcordia Group/VT Number
VT1	Group1/VT1
VT2	Group2/VT1
VT3	Group3/VT1
VT4	Group4/VT1
VT5	Group5/VT1
VT6	Group6/VT1
VT7	Group7/VT1
VT8	Group1/VT2

Table 2-1 ONS 15454 VT Mapping (continued)

ONS 15454 VT Number	Telcordia Group/VT Number
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

2.8.2 XCVT Hosting DS3XM-6

The XCVT card works with DS3XM-6 (transmux) cards. A single DS3XM-6 can demultiplex, or map down to a lower rate, six DS-3 signals into 168 VT1.5s that the XCVT card manages and cross connects. XCVT cards host a maximum of 336 VT1.5s. In most network configurations, two DS3XM-6 cards are paired as working and protect cards.

2.8.3 XCVT Card-Level Indicators

The XCVT faceplate has two card-level LEDs. The red FAIL LED indicates a hardware problem. Replace the unit if the red FAIL LED persists. The ACT/STBY (Active/Standby) LED indicates whether the XCVT is active and carrying traffic (green) or in standby mode to the active XCVT card (yellow).

2.8.4 XC/XCVT Compatibility

The XCVT supports run-time compatibility with the XC cross-connect both within a single node and within a ring of mixed XCVT and XC nodes. However, working and protect cards within a single ONS 15454 must be either two XC cards or two XCVT cards. If an XC card and an XCVT card are used together as a working and protect pair, the XCVT acts as an XC card. Both XC and XCVT systems are supported in unidirectional path switched ring (UPSR) and bi-directional line switched ring (BLSR) configurations. VT and STS-level cross-connect and protection management are also

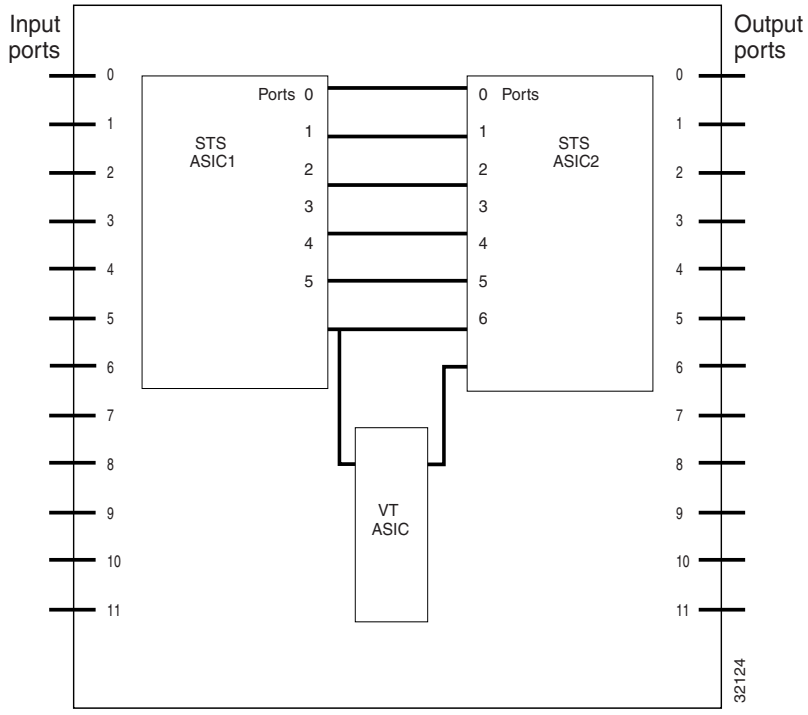
supported in either type of ring. Nodes that rearrange or drop VTs must use an XCVT. Nodes that only rearrange or drop STSs can use an XC. You do not need to upgrade STS-only nodes to XCVT in a ring that can handle both VT and STS drop/rearrangement. In this scenario, however, the XC must run Software Release 2.0 or higher.

When upgrading from XC to XCVT cards, the first XCVT card installed acts as an XC card until the second XCVT card is installed. For more information, see the "Upgrade XC Cards to XCVT" section on page 5-18.

If you want to create an STS-capable ring that allows VT drops at some nodes, all of the nodes in the ring must run Release 2.0 software or higher. The nodes that allow VT drops must use XCVT cards, and the nodes that do not allow VT drops can use any type of XC card.

When upgrading a system or ring to use the release 2.0 XCVT card, you must first upgrade the software to Release 2.0.

Figure 2-11 XCVT Block Diagram



VT cross-connects go to internal port 5 only, which bridges the signal into the VT ASIC. Port 5 supports 48 STSs, but only the last 24 STSs map VT-level signals.

2.8.5 XCVT Card Specifications

- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 50 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.9 Alarm Interface Controller Card

The Alarm Interface Controller (AIC) card is an optional card that expands system management capabilities for customer-defined alarm I/O and orderwire. Figure 2-12 shows the AIC faceplate and Figure 2-13 shows a block diagram of the card.

Figure 2-12 AIC Faceplate

2.9.1 Customer-Defined Alarms

The AIC card provides additional input/output alarm contact closures. You can define up to four input and four output contacts. The physical connections are made using the backplane wire-wrap field. The alarms are defined using the CTC (for instructions see the "Provisioning the Alarm Interface Controller" section on page 5-9). Each alarm contact has a corresponding LED on the front panel of the AIC that indicates the status of the alarm. Input alarms are typically used for external sensors such as open doors, temperature sensors, flood sensors, and other environmental conditions. Output contacts 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.

2.9.1.1 Provisioning I/O Alarm Contacts

You can program each of the four Form A input alarm contacts 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). The alarm service level can be programmed to Service Affecting or Non-Service Affecting. A 63-character alarm description can be assigned for display by the CTC in the alarm log. The fan tray abbreviation for the alarm is not assignable. It reflects the generic name of the input contacts. The alarm condition remains until the external input stops driving the contact and you clear the alarm in CTC.

You can also program the Form A output alarm contacts 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 15454 alarm condition including the user-defined input alarms, or triggering based on severity (i.e. trigger when any Major alarm happens), or remote alarm. You use pull-down menus in CTC to provision alarm-to-output-contact association; CTC organizes the alarms by category or by individual alarm. The output contact electrical interface is 50V, 100mA.

2.9.1.2 Provisionable Items

You can provision several items within the customer-defined alarms. You can provision up to four OC-N facilities for each local orderwire (LOW) and express orderwire (EOW) as orderwire paths. External alarm input contacts on the AIC can be provisioned for type, severity, service affecting status, contact normal, virtual wire, and description. External control output contacts on the AIC can be provisioned for trigger and local description.

The provisionable triggers cause normally open relay contacts to close. The user-provisionable triggers consist of the following:

- Local NE alarm severity: A hierarchy of non-reported, non-alarmed, minor, major, or critical alarm severity that can be set to cause output closure. For example, if the trigger is set to minor, a minor alarm or above is the trigger.
- Remote NE alarm severity: Same as the Local NE alarm severity but applies to remote alarms only.
- Virtual wire entities: A raised signal on external outputs 1 through 4 can be provisioned as triggers to cause output closure.

In addition to provisionable triggers, the CTC allows you to manually force each external output contact to open or close. Manual operation takes precedence over any provisioned triggers that might be present.

2.9.2 Orderwire

Orderwire allows a craftsperson to plug a phoneset into an ONS 15454 and communicate with craftspeople working at other ONS 15454s. The orderwire is a pulse code modulation (PCM) encoded voice channel that uses E1 or E2 bytes in section/line overhead.

The AIC allows simultaneous use of both local (section overhead signal) and express (line overhead channel) orderwire channels on a SONET ring or particular optics facility. Local orderwire also allows communication at regeneration sites when the regenerator is not a Cisco device.

You can provision orderwire functions with the CTC. This is similar to the current provisioning model for DCC channels. In CTC you provision the orderwire communications network during ring turn-up so that all NEs on the ring can reach one another. Orderwire terminations (i.e. the optics facilities that receive and process the orderwire channels) are provisionable. Both express and local orderwire can be configured as on or off on a particular SONET facility. The system supports up to

4 orderwire channel terminations per shelf. This allows linear, single ring, dual ring, and small hub-and-spoke configurations. Keep in mind that orderwire is not protected in ring topologies such as BLSR and UPSR.

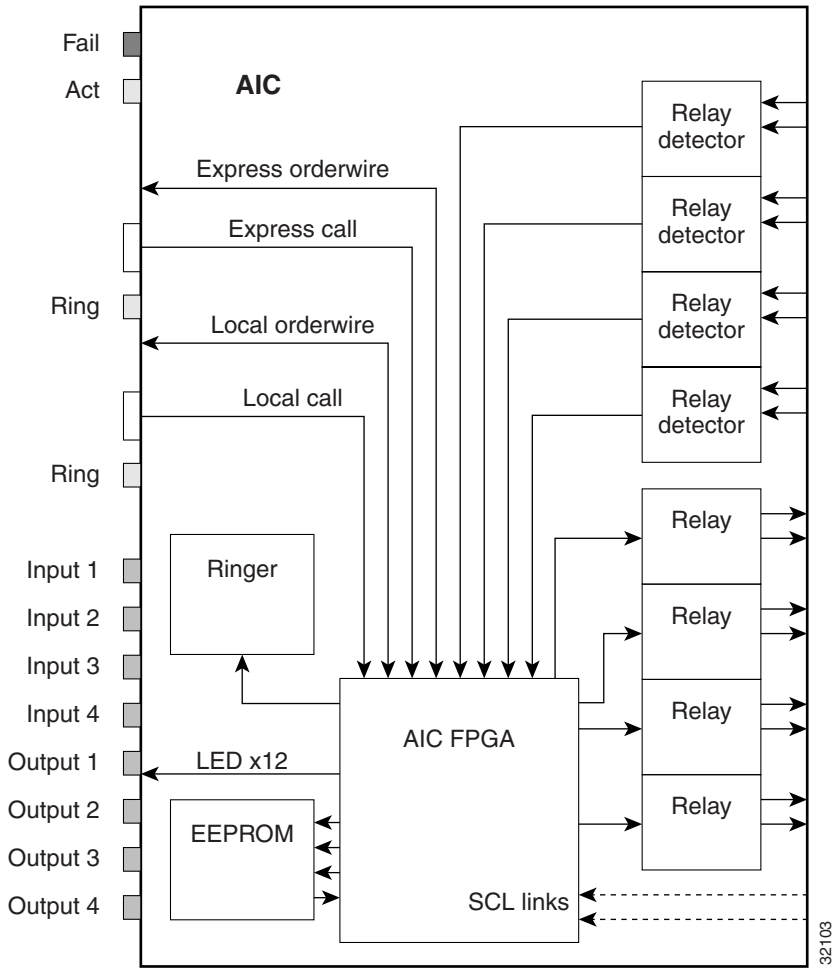
Caution Do not configure orderwire loops. Orderwire loops cause feedback that disables the orderwire channel.

The ONS 15454 implementation of both local and express orderwire is broadcast in nature. The line acts as a party line. There is no signalling for private point-to-point connections. Anyone who picks up the orderwire channel can communicate with all other participants on the connected orderwire subnetwork. The local orderwire party line is separate from the express orderwire party line. Up to four OC-N facilities for each local and express orderwire are provisionable as orderwire paths. The AIC supports a "call" button on the module front panel which, when pressed, causes all ONS 15454 AICs on the orderwire subnetwork to "ring." The ringer/buzzer resides on the AIC. There is also a "ring" LED that mimics the AIC ringer. It flashes when any "call" button is pressed on the orderwire subnetwork. The "call" button and ringer/LED allow a remote craftsperson to get the attention of the craftspeople across the network.

When provisioning the orderwire subnetwork, make sure that an orderwire loop does not exist. Loops cause oscillation and an unusable orderwire channel.

Note Only Ports 1 and 3 are valid when using the orderwire function.

Figure 2-13 AIC Block Diagram



2.9.3 AIC Specifications

- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 16 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.10 EC1-12 Card

The EC1-12 card provides 12 Telcordia-compliant, GR-253 STS-1 electrical interfaces per card. Each interface operates at 51.840 Mbps over a single 75 ohm 728A or equivalent coaxial span. Figure 2-14 shows the EC1-12 faceplate and Figure 2-15 shows a diagram of the card.

Figure 2-14 EC1-12 Faceplate

STS path selection for UNEQ-P, AIS-P, UPSR using BER thresholds, etc. is done on the SONET ring interfaces in conjunction with the STS cross-connect. The EC1-12 terminates the twelve selected working STS-1 signals from the backplane. The EC1-12 maps each of the twelve received EC1 signals into 12 STS-1s with visibility into the SONET path overhead.

You can install the EC1-12 card in any ONS 15454 multispeed or high-speed card slot. Each EC1-12 interface features DSX-level outputs supporting distances up to 450 feet depending on facility conditions.

An EC1-12 card can be 1:1 protected with another EC1-12 card but cannot protect more than one EC1-12 card. It must be installed in an even-numbered slot to serve as a working card and an odd-numbered slot to serve as a protect card.

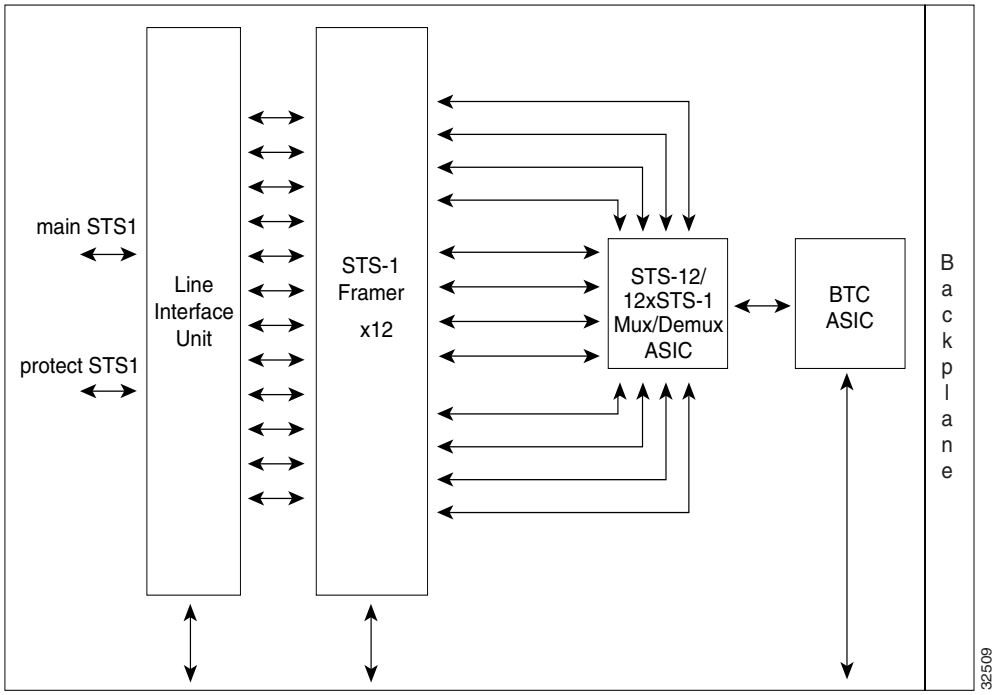
2.10.1 EC1-12 Card-Level Indicators

The EC1-12 card faceplate has three card-level LEDs. The red FAIL LED signifies a hardware problem on the EC1-12 card. Replace the unit if the FAIL LED persists. The green ACT LED means that the EC1-12 card is operational and ready to carry traffic. The yellow SF LED indicates a signal failure or condition such as loss of signal (LOS), loss of frame (LOF), or high bit error rate (BER) on one or more of the card's EC1-12 ports.

2.10.2 EC1-12 Port-Level Indicators

You can obtain the status of the EC1-12 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-15 EC1-12 Block Diagram



2.10.3 EC1-12 Specifications

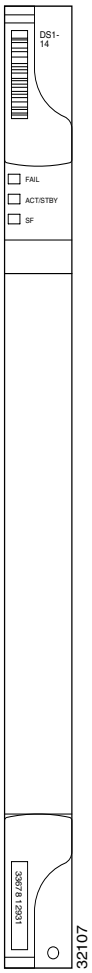
- EC1-12 Input
  - Bit Rate: 51.84 Mb/s +/- 20ppm
  - Frame Format: SONET
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%

  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 100 ft. RG179
  - AIS: TR-TSY-000191-compliant
- EC1-12 Output
  - Bit Rate: 51.84 Mb/s +/- 20ppm
  - Frame Format: SONET
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 100 ft. RG179
  - AIS: TR-TSY-000191-compliant
  - Power Level: -1.8 - +5.7 dBm
  - Pulse Shape: ANSI T1.102-1988 Figure 8
  - Pulse amplitude: 0.36 - 0.85 V peak to peak
  - Loopback Modes: Terminal and Facility
  - Line Build Out: 0-225 ft.; 226-450 ft.
- EC1-12 Electrical Interface
  - Connectors: BNC or SMB
- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 40 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.11 DS1-14 Card

The ONS 15454 DS1-14 card provides 14 Telcordia-compliant, GR-499 DS-1 interfaces. Each interface operates at 1.544 Mbps over a 100Ω twisted pair copper cable. The DS1-14 card can function as a working or protect card in 1:1 protection schemes and as a working card in 1:N protection schemes. Figure 2-16 shows the DS1-14 faceplate and Figure 2-17 shows a block diagram of the card.

Figure 2-16 DS1-14 Faceplate



You can install the DS1-14 card in any ONS 15454 multispeed or high-speed card slots. Each DS1-14 interface has DSX-level outputs supporting distances up to 655 feet.

The DS1-14 card supports 1:1 protection. The DS1-14 can be a working card in a 1:N protection scheme with the proper backplane EIA and wire-wrap or AMP CHAMP connectors. You can also provision the DS1-14 to monitor for line and frame errors in both directions.

You can group and map DS1-14 card traffic in STS-1 increments to any other card in an ONS 15454. Each DS-1 is asynchronously mapped into a SONET VT1.5 payload and the card carries a DS-1 payload intact in a VT1.5. For performance monitoring purposes, you can gather bidirectional DS-1 frame-level information (loss of frame, parity errors, CRC errors, etc.). All 14 VT1.5 payloads from a DS1-14 card are carried in a single STS-1 to the XC or XCVT card where the payload may be further aggregated for efficient STS-1 transport.

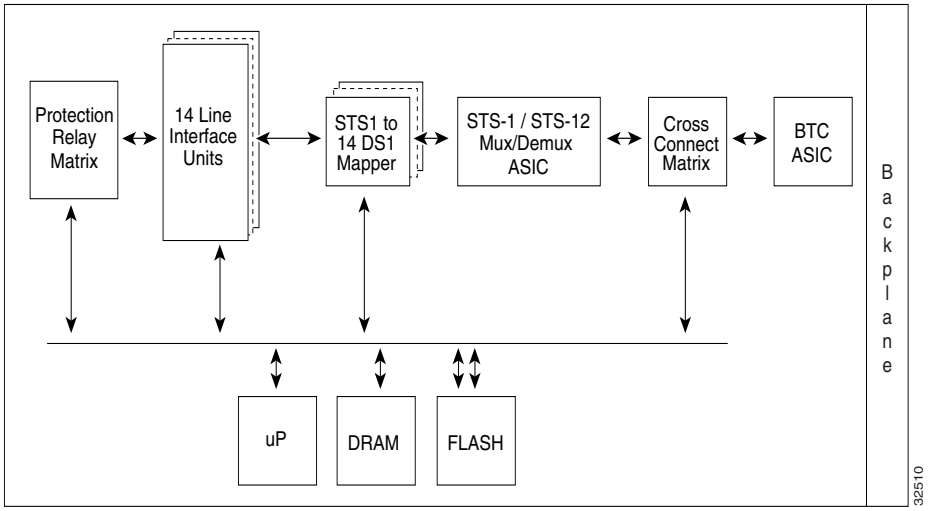
2.11.1 DS1-14 Card-Level Indicators

The DS1-14 card faceplate has three LEDs. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The green/yellow ACT/STBY LED indicates whether the DS1-14 card is operational and ready to carry traffic (green), or in standby mode (yellow). The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on one or more of the DS1-14 ports.

2.11.2 DS1-14 Port-Level Indicators

You can obtain the status of the DS1-14 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-17 DS1-14 Block Diagram



2.11.3 DS1-14 Specifications

- DS1-14 Input
  - Bit Rate: 1.544 Mb/s +/- 32ppm
  - Frame Format: Off, SF (D4), ESF
  - Line Code: AMI, B8ZS
  - Termination: Wire-Wrap, AMP CHAMP
  - Input Impedance:100 Ohms
  - Cable Loss: Max 655 ft. ABAM #22 AWG
  - AIS: TR-TSY-000191-compliant
- DS1-14 Output
  - Bit Rate: 1.544 Mb/s +/- 32ppm
  - Frame Format: Off, SF (D4), ESF

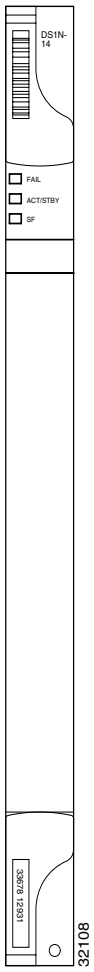
- Line Code: AMI, B8ZS
- Termination: Wire-Wrap, AMP CHAMP
- Input Impedance:100 Ohms
- Cable Loss: Max 655 ft. ABAM #22 AWG
- AIS: TR-TSY-000191-compliant
- Power Level: 12.5 to 17.9 dBm centered @ 772 KHz, -16.4 to -11.1 dBm centered at 1544 KHz
- Pulse Shape: GR-499-CORE Figure 9-5
- Pulse Amplitude: 2.4- 3.6 V peak-to-peak
- Loopback Modes: Terminal and Facility

- Environmental
  - Surge Protection: GR-1089
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 25 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.12 DS1N-14 Card

The DS1N-14 card provides 14 Telcordia-compliant, GR-499 DS-1 interfaces. Each DS1N-14 interface operates at 1.544 Mbps over a 100Ω twisted-pair copper cable. Figure 2-18 shows the DS1N-14 faceplate and Figure 2-19 shows a block diagram of the card.

Figure 2-18 DS1N-14 Faceplate



Each DS1N-14 interface features DSX-level outputs supporting distances up to 655 feet depending on facility conditions.

The DS1N-14 card supports 1:N (N≤5) protection with the proper backplane EIA and wire-wrap or AMP CHAMP connectors. You can also provision the DS1N-14 to monitor line and frame errors in both directions.

The DS1N-14 card can function as a working or protect card in 1:1 or 1:N protection schemes. If you use the DS1N-14 as a standard DS-1 card in a 1:1 protection group, you can install the DS1N-14 card in any ONS 15454 multispeed or high-speed card slot. If you use the card's 1:N functionality, you must install a DS1N-14 card in Slots 3 and 15.

You can group and map DS1-14 card traffic in STS-1 increments to any other card in an ONS 15454 system. Each DS-1 is asynchronously mapped into a SONET VT1.5 payload and the card carries a DS-1 payload intact in a VT1.5. For performance monitoring purposes, you can gather bidirectional

DS-1 frame-level information (loss of frame, parity errors, or CRC errors, for example). All 14 VT1.5 payloads from a DS1-14 card are carried in a single STS-1 to the XC or XCVT card where they can be further aggregated for efficient STS-1 transport.

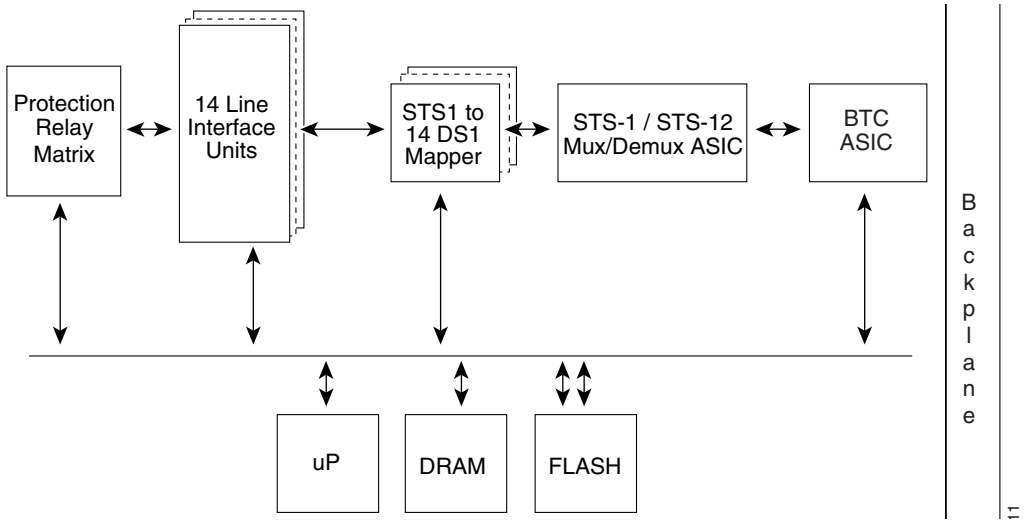
2.12.1 DS1N-14 Card-Level Indicators

The DS1N-14 card faceplate has three LEDs. The red FAIL LED indicates a hardware problem. Replace the card if the FAIL LED persists. The green/yellow, ACT/STBY LED indicates when green that the DS1N-14 card is operational and ready to carry traffic, or when yellow that the card is in standby mode. The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on one or more of the DS-1 ports on the card.

2.12.2 DS1N-14 Port-Level Indicators

You can obtain the status of the 14 DS-1 ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, “CTC Alarms,” for a complete description of the alarm messages.

Figure 2-19 DS1N-14 Block Diagram



2.12.3 DS1N-14 Specifications

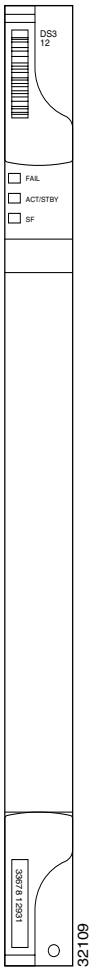
- DS1N-14 Input
  - Bit Rate: 1.544 Mb/s +/- 32ppm
  - Frame Format: Off, SF (D4), ESF
  - Line Code: AMI, B8ZS
  - Termination: Wire-Wrap, AMP CHAMP
  - Input Impedance:100 Ohms
  - Cable Loss: Max 655 ft. ABAM #22 AWG
  - AIS: TR-TSY-000191-compliant

- DS1N-14 Output
  - Bit Rate: 1.544 Mb/s +/- 32ppm
  - Frame Format: Off, SF (D4), ESF
  - Line Code: AMI, B8ZS
  - Termination: Wire-Wrap, AMP CHAMP
  - Input Impedance:100 Ohms
  - Cable Loss: Max 655 ft. ABAM #22 AWG
  - AIS: TR-TSY-000191-compliant
  - Power Level: 12.5 to 17.9 dBm centered @ 772 KHz, -16.4 to -11.1 dBm centered at 1544 KHz
  - Pulse Shape: GR-499-CORE Figure 9-5
  - Pulse Amplitude: 2.4- 3.6 V peak-to-peak
  - Loopback Modes: Terminal and Facility
- Environmental
  - Surge Protection: GR-1089
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 25 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.13 DS3-12 Card

The ONS 15454 DS3-12 card provides twelve Telcordia-compliant, GR-499 DS-3 interfaces per card for the ONS 15454. Each interface operates at 44.736 Mbps over a single 75Ω 728A or equivalent coaxial span. The DS3-12 card operates as a working or protect card in 1:1 protection schemes and as a working card in 1:N protection schemes. Figure 2-20 shows the DS3-12 faceplate, and Figure 2-21 shows a block diagram of the card.

Figure 2-20 DS3-12 Faceplate



You can install the DS3-12 card in any ONS 15454 multispeed or high-speed card slot. Each DS3-12 interface features DSX-level outputs supporting distances up to 450 feet depending on facility conditions.

The DS3-12 card supports 1:1 protection with the proper backplane EIA. EIAs are available with BNC or SMB connectors.

Warning When a protection switch moves traffic from the DS3-12 working/active card to the DS3-12 protect/standby card, ports on the now working/standby card cannot be taken out of service. Lost traffic can result if you take a port out of service even if the DS3-12 working/standby card no longer carries traffic.

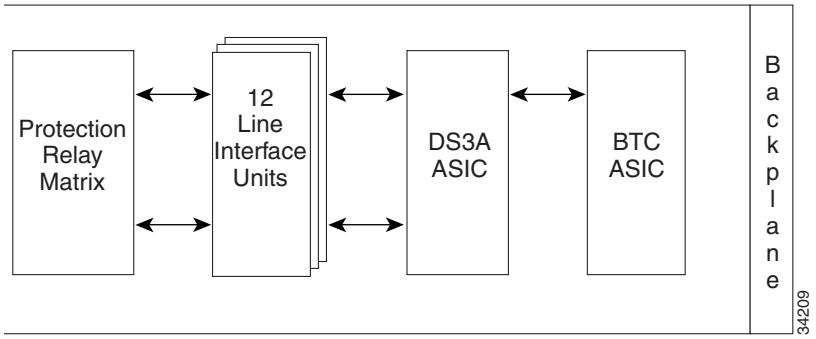
2.13.1 DS3-12 Card-Level Indicators

The DS3-12 card faceplate has three LEDs. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on one or more of the DS-3 ports on the card. The green ACT LED indicates that the DS3-12 card is operational and ready to carry traffic.

2.13.2 DS3-12 Port-Level Indicators

You can find the status of the 12 DS3-12 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-21 DS3-12 Block Diagram



2.13.3 DS3-12 Specifications

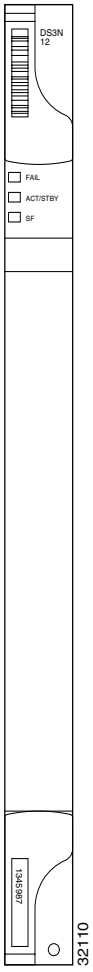
- DS3-12 Input
  - Bit Rate: 44.736 Mb/s +/- 20ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 100 ft. RG179
  - AIS: TR-TSY-000191-compliant

- DS3-12 Output
  - Bit Rate: 44.736 Mb/s +/- 20ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 100 ft. RG179
  - AIS: TR-TSY-000191-compliant
  - Power Level: -1.8 - +5.7 dBm
  - Pulse Shape: ANSI T1.102-1988 Figure 8
  - Pulse amplitude: 0.36 - 0.85 V peak-to-peak
  - Loopback Modes: Terminal and Facility
- DS3-12 Electrical Interface
  - Connectors: BNC or SMB
- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 28 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.14 DS3N-12 Card

The ONS 15454 DS3N-12 card provides twelve Telcordia-compliant, TR499 DS-3 interfaces per card. Each interface operates at 44.736 Mbps over a single 75 ohm 785A or equivalent coaxial span. Figure 2-22 shows the DS3N-12 faceplate and Figure 2-23 shows a diagram of the card.

Figure 2-22 DS3N-12 Faceplate



You can install the DS3N-12 card in any ONS 15454 multispeed or high-speed card slot. Each DS3N-12 interface features DSX-level outputs supporting distances up to 450 feet depending on facility conditions. With the proper backplane EIA, the card supports BNC or SMB connectors.

The DS3N-12 can operate as the protect card in a 1:N (1<=N<=5) DS-3 protection group. It has additional circuitry not present on the basic DS3-12 card that allows it to protect up to 5 working DS3-12 cards. The basic DS3-12 card can only function as the protect card for one other DS3-12 card. Other than the protection capabilities, the DS3-12 and DS3N-12 cards are identical.

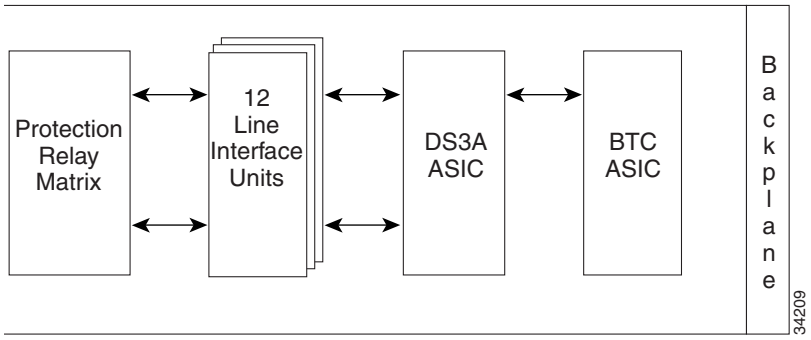
2.14.1 DS3N-12 Card-Level Indicators

The DS3N-12 card faceplate has three LEDs. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The green ACT/STBY LED indicates that the DS3N-12 card is operational and ready to carry traffic. The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on one or more of the DS-3 ports on the card.

2.14.2 DS3N-12 Port-Level Indicators

You can find the status of the 12 DS3N-12 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-23 DS3N-12 Block Diagram



2.14.3 DS3N-12 Card Specifications

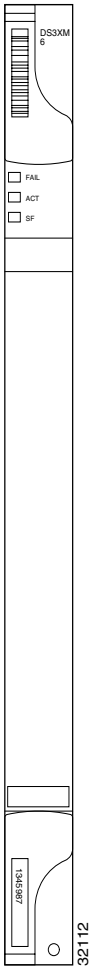
- DS3N-12 Input
  - Bit Rate: 44.736 Mb/s +/- 20ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 79 ft. RG179
  - AIS: TR-TSY-000191-compliant

- DS3N-12 Output
  - Bit Rate: 44.736 Mb/s +/- 20ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 79 ft. RG179
  - AIS: TR-TSY-000191-compliant
  - Power Level: -1.8 - +5.7 dBm
  - Pulse Shape: ANSI T1.102-1988 Figure 8
  - Pulse amplitude: 0.36 - 0.85 V peak-to-peak
  - Loopback Modes: Terminal and Facility
  - Line Build Out: 0-225 ft.; 226-450 ft.
- DS3N-12 Electrical Interface
  - Connectors: BNC or SMB
- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 30 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.15 DS3XM-6 Card

The DS3XM-6 card, commonly referred to as a transmux card, provides six Telcordia-compliant, GR-499-CORE M13 multiplexing functions. The DS3XM-6 converts six framed DS-3 network connections to 28x6 or 168 VT1.5s. Figure 2-24 shows the DS3XM-6 card faceplate and Figure 2-25 shows a block diagram of the card.

Figure 2-24 DS3XM-6 Faceplate



You can install the DS3XM-6 in any ONS 15454 multispeed or high-speed card slot. Each DS3XM-6 interface features DSX-level outputs supporting distances up to 450 feet depending on facility conditions.

The DS3XM-6 card supports 1:1 protection with the proper backplane EIA. EIAs are available with BNC or SMB connectors.

2.15.1 DS3XM-6 Hosted By XCVT

The DS3XM-6 card works in conjunction with the XCVT card. A single DS3XM-6 can demultiplex, or map down to a lower rate, six DS-3 signals into 168 VT1.5s that the XCVT card then manages and cross connects. XCVT cards host a maximum of 336 VT1.5s or two DS3XM-6 cards. In most network configurations, two DS3XM-6 cards are paired together as working and protect cards.

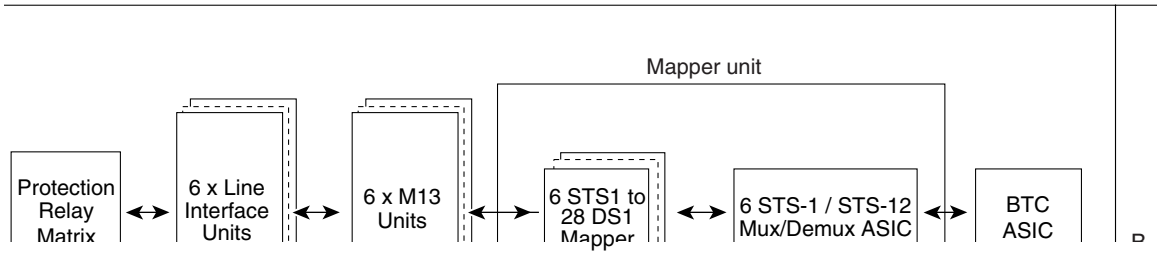
2.15.2 DS3XM-6 Card-Level Indicators

The DS3XM-6 card faceplate has three LEDs. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The green ACT LED indicates that the DS3XM-6 card is operational and ready to carry traffic. The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on one or more of the DS3XM-6 card ports.

2.15.3 DS3XM-6 Port-Level Indicators

You can find the status of the six DS3XM-6 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-25 DS3XM-6 Block Diagram



2.15.4 DS3XM-6 Card Specifications

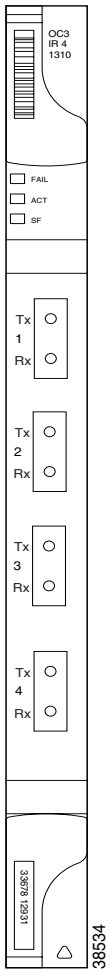
- DS3XM-6 Input
  - Bit Rate: 44.736 Mb/s +/- 20ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 100 ft. RG179
  - AIS: TR-TSY-000191-compliant

- DS3XM-6 Output
  - Bit Rate: 44.736 Mb/s +/- 20ppm
  - Frame Format: DS-3 ANSI T1.107-1988
  - Line Code: B3ZS
  - Termination: Unbalanced coaxial cable
  - Input Impedance: 75 ohms +/-5%
  - Cable Loss: Max 450 ft. 734A, RJ59, 728A/Max 100 ft. RG179
  - AIS: TR-TSY-000191-compliant
  - Power Level: -1.8 - +5.7 dBm
  - Pulse Shape: ANSI T1.102-1988 Figure 8
  - Pulse amplitude: 0.36 - 0.85 V peak-to-peak
  - Loopback Modes: Terminal and Facility
  - Line Build Out: 0-225 ft.; 226-450 ft.
- DS3XM-6 Electrical Interface
  - Connectors: BNC or SMB
- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 40 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.16 OC3 IR 4 1310 Card

The OC3 IR 4 1310 card provides four intermediate or short range, Telcordia-compliant, GR-253 SONET OC-3 interfaces. Each interface operates at 155.52 Mbps over a single-mode fiber span and supports VT payloads and non-concatenated or concatenated payloads on a per STS-1 or STS-3c basis. Figure 2-26 shows the OC3 IR 4 1310 faceplate and Figure 2-27 shows a diagram of the card.

Figure 2-26 OC3 IR 4 1310 Faceplate



You can install the OC3 IR 4 1310 card in any ONS 15454 multispeed or high-speed card slot. The OC3IR 4 1310 card can be provisioned as part of a UPSR or in an ADM/TM configuration. Each interface features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC3 IR 4 1310 uses SC connectors.

The OC3 IR 4 1310 card supports 1+1 unidirectional protection and bi-directional protection switching. You can provision protection on a per port basis.

The OC3 IR 4 1310 detects LOS, LOF, Loss of Pointer (LOP), line Alarm Indication Signal (AIS-L), and line Remote Defect Indication (RDI-L) conditions (see Chapter 9, “CTC Alarms,” for a description of these conditions). The card also counts section and line BIP errors.

To enable automatic protection switching, the OC3 IR 4 1310 extracts the K1 and K2 bytes from the SONET overhead to perform appropriate protection switches. The DCC bytes are forwarded to the DCC-terminating TCC.

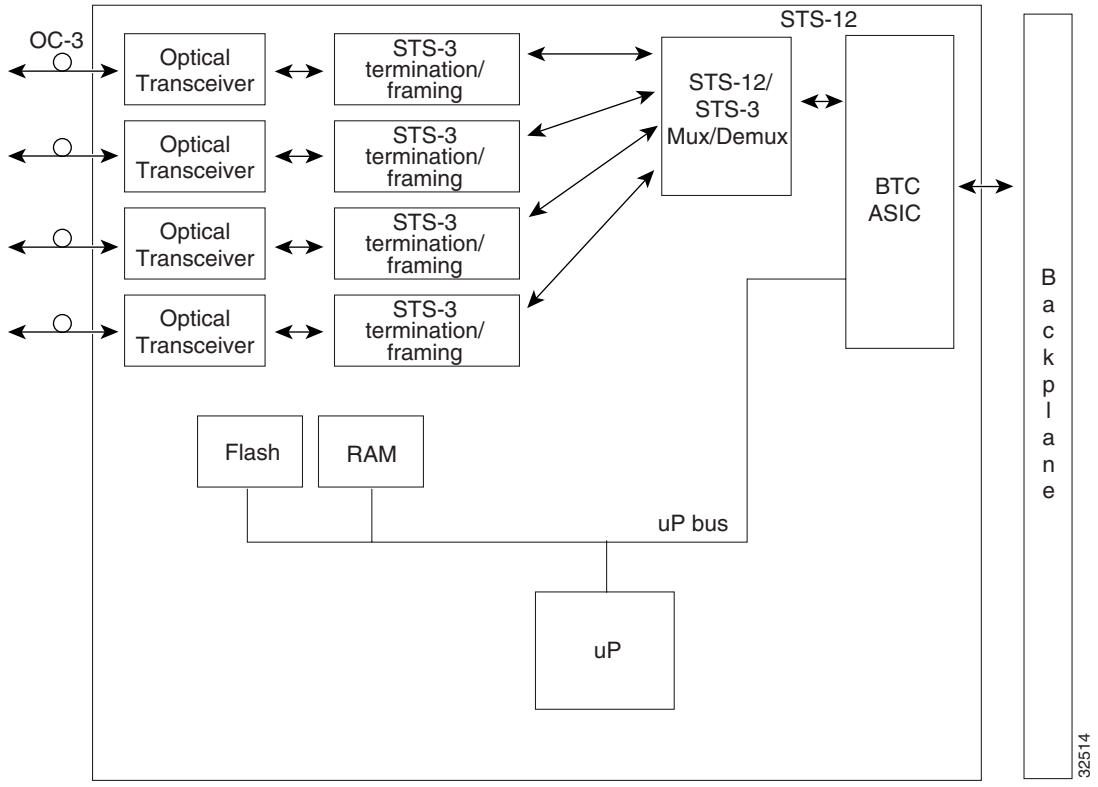
2.16.1 OC3 IR 4 1310 Card-Level Indicators

The OC3 IR 4 1310 card has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, AISL, or high BER) on one or more of the card's OC-3 ports. The green ACT LED indicates the OC3 IR 4 1310 card is carrying traffic or is traffic-ready.

2.16.2 OC3 IR 4 1310 Port-Level Indicators

You can find the status of the 4 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-27 OC3 IR 4 1310 Block Diagram



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

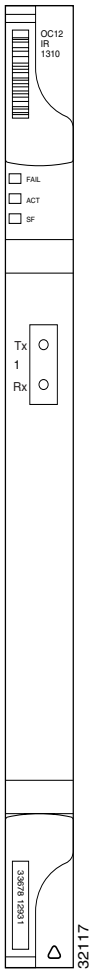
2.16.3 OC3 IR 4 1310 Card Specifications

- Line
  - Bit Rate:155.52 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310nm Single Mode
  - Loopback Modes: Terminal and Facility
  - Connector: 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: 1310nm
  - 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: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 20 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.17 OC12 IR 1310 Card

The OC12 IR 1310 card provides one intermediate or short range, 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 on a per STS-1, STS-3c, STS-6c, or STS-12c basis. Figure 2-28 shows the OC12 IR 1310 faceplate and Figure 2-29 shows a block diagram of the card.

Figure 2-28 OC12 IR 1310 Faceplate



You can install the OC12 IR 1310 card in any ONS 15454 multispeed or high-speed card slot. You can provision the OC12 IR 1310 as part of a BLSR or UPSR. In ADM/TM configurations, you can provision the card as either an access tributary or a transport span-side interface.

The OC12 IR 1310 interface features a 1310 nm laser and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 IR 1310 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 9, “CTC Alarms,” for a description of these conditions). The card counts section and line BIT errors.

To enable automatic protection switching, the OC12 IR 1310 extracts the K1 and K2 bytes from the SONET overhead and processes them to switch accordingly. The DCC bytes are forwarded to the DCC-terminating TCC.

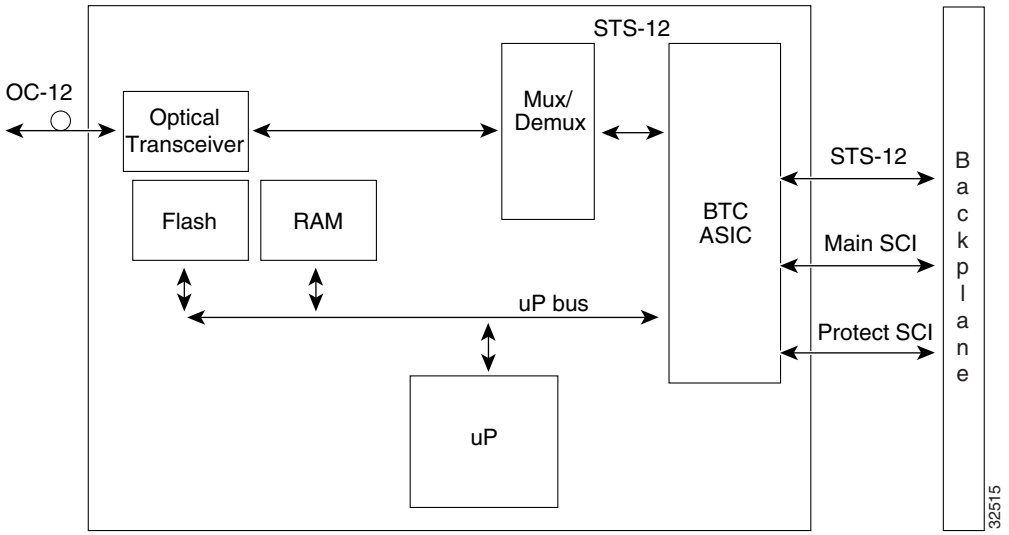
2.17.1 OC12 IR 1310 Card-Level Indicators

The OC12 IR 1310 card has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, AIS-L, or high BER) on the OC-12 interface. The green ACT LED indicates that the OC12 IR 1310 card is operational and is carrying traffic or is traffic-ready.

2.17.2 OC12 IR 1310 Port-Level Indicators

You can find the status of the OC-12 card port using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-29 OC12 IR 1310 Block Diagram



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

2.17.3 OC12 IR 1310 Card Specifications

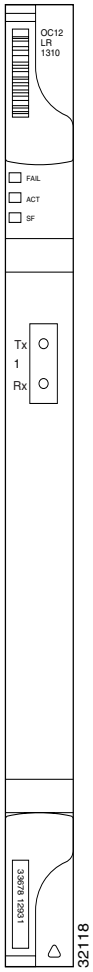
- Line
  - Bit Rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310nm Single Mode
  - Loopback Modes: Terminal and Facility

  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253
- Transmitter
  - Max. Transmitter Output Power: -8 dBmn
  - 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: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 14 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.18 OC12 LR 1310 Card

The OC12 LR 1310 card provides one long-range, Telcordia-compliant, GR-253 SONET OC12 interface per card. The interface operates at 622.08 Mbps over a single-mode fiber span. The OC12 LR 1310 supports non-concatenated or concatenated payloads on a per STS-1, STS-3c, STS-6c, or STS-12c basis and reports VT payloads. Figure 2-30 shows the OC12 LR 1310 faceplate and Figure 2-31 shows a block diagram of the card.

Figure 2-30 OC12 LR 1310 Faceplate



You can install the OC12 LR 1310 card in any ONS 15454 multispeed or high-speed card slot. You can provision the OC12 LR 1310 as part of a BLSR or UPSR. In ADM/TM configurations, you can provision the card as either an access tributary or a transport span-side interface.

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

The OC12 LR 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions (see Chapter 9, “CTC Alarms,”for a description of these conditions). The card also counts section and line BIT errors.

To enable automatic protection switching (APS), the OC12 LR 1310 extracts the K1 and K2 bytes from the SONET overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC, which terminates the DCC.

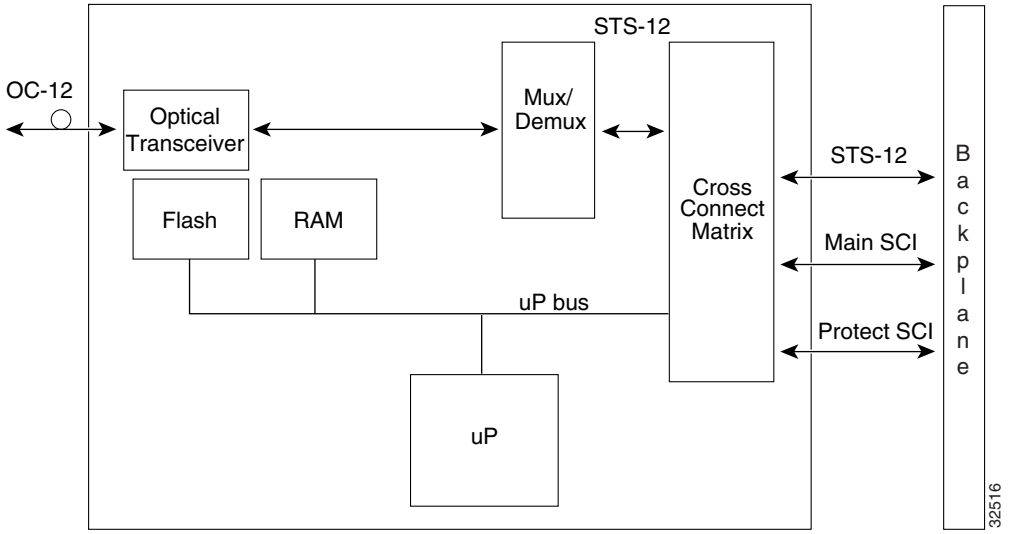
2.18.1 OC12 LR 1310 Card-Level Indicators

The OC12 LR 1310 card has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, AIS-L, or high BER) on the OC-12 interface. The green ACT LED indicates that the OC12 LR 1310 card is operational and is carrying traffic or is traffic-ready.

2.18.2 OC12 LR 1310 Port-Level Indicators

You can find the status of the OC12 LR 1310 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-31 OC12 LR 1310 Block Diagram



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

2.18.3 OC12 LR 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-253-CORE
- Transmitter
  - Max. Transmitter Output Power: +2 dBm
  - Min. Transmitter Output Power: -3 dBm
  - Center Wavelength: 1280 nm – 1335 nm
  - Nominal Wavelength: 1310nm
  - Transmitter: Distributed Feedback Laser
- Receiver
  - Max. Receiver Level: -8 dBm
  - Min. Receiver Level: -28 dBm
  - Receiver: InGaAs/InP photo detector
  - Link Loss Budget: 25 dB
- Environmental
  - Eye safety compliance: Class I
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 14 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.19 OC12 LR 1550 Card

The OC12 LR 1550 card provides one long-range, Telcordia-compliant, GR-253 SONET OC-12 interface per card. The interface operates at 622 Mbps over a single-mode fiber span and supports concatenated STS, non-concatenated STS, and VT payloads. Figure 2-32 shows the OC12 LR 1550 faceplate and Figure 2-33 shows a block diagram of the card.

Figure 2-32 OC12 LR 1550 Faceplate

You can install the OC12 LR 1550 card in any ONS 15454 general purpose card slot. The OC12 LR 1550 can be provisioned as part of a BLSR, UPSR, or ADM/TM.

The OC12 LR 1550 uses long reach optics centered at 1550 nm and contains a transmit and receive connector (labeled) on the card faceplate. The OC12 LR 1550 uses SC optical connections and supports 1+1 unidirectional protection or provisionable bidirectional or unidirectional switching.

The OC12 LR 1550 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions (see Chapter 9, “CTC Alarms,” for a description of these conditions). The card also counts section and line BIT errors.

To enable automatic protection switching, the OC12 LR 1550 extracts the K1 and K2 bytes from the SONET overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC, which terminates the DCC.

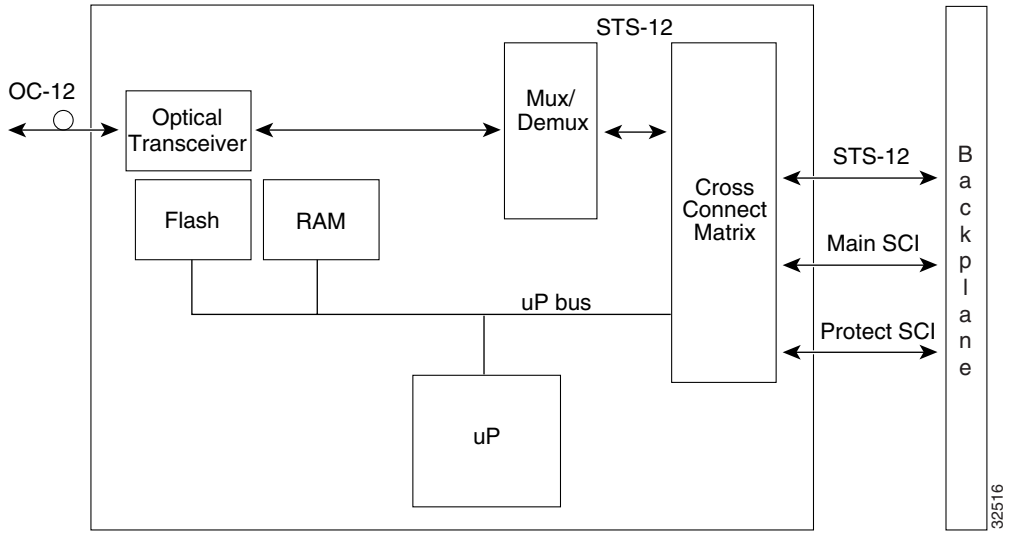
2.19.1 OC12 LR 1550 Card-Level Indicators

The OC12 LR 1550 card has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, AIS-L, or high BER) on the OC-12 interface. The green ACT LED indicates that the OC12 LR 1550 card is operational and ready to carry traffic.

2.19.2 OC12 LR 1550 Port-Level Indicators

You can find the status of the OC12 LR 1550 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-33 OC12 LR 1550 Block Diagram



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

2.19.3 OC12 LR 1550 Card Specifications

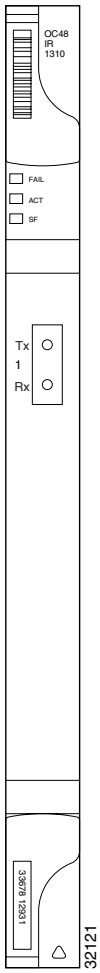
- Line
  - Bit Rate: 622.08 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm Single Mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-253-CORE

- Transmitter
  - Max. Transmitter Output Power: +2 dBm
  - Min. Transmitter Output Power: -3 dBm
  - Center Wavelength: 1480 nm – 1580 nm
  - Nominal Wavelength: 1550 nm
  - Transmitter: Distributed Feedback Laser
- Receiver
  - Max. Receiver Level: -8 dBm
  - Min. Receiver Level: -28 dBm
  - Receiver: InGaAs/InP photo detector
  - Link Loss Budget: 25 dB
- Environmental
  - Eye safety compliance: Class I
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 14 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.20 OC48 IR 1310 Card

The OC48 IR 1310 card provides one intermediate-range, 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 on a per STS-1, STS-3c, STS-6c STS-12c, or STS-48c basis. Figure 2-34 shows the OC48 IR 1310 faceplate and Figure 2-35 shows a block diagram of the card.

Figure 2-34 OC48 IR 1310 Faceplate



You can install the OC48 IR 1310 card in any ONS 15454 high-speed card slot. You can provision the OC48 IR 1310 as part of a BLSR or UPSR or, in an ADM/TM configuration, as either an access tributary or a transport span interface.

The OC-48 interface 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 OC48 IR 1310 card supports 1+1 unidirectional protection and provisionable bidirectional switching.

The OC48 IR 1310 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions (see Chapter 9, “CTC Alarms,” for a description of these conditions). The card also counts section and line BIT errors.

To enable automatic protection switching, the OC48 IR 1310 extracts the K1 and K2 bytes from the SONET overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC. The TCC terminates the DCC.

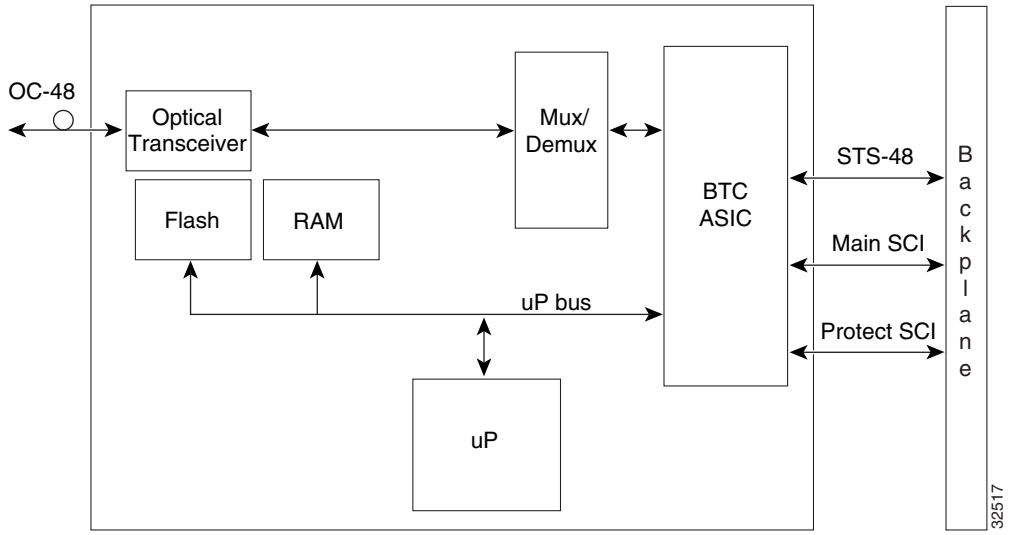
2.20.1 OC48 IR 1310 Card-Level Indicators

The OC48 IR 1310 card has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, AIS-L, or high BER) on the OC-48 interface. The green ACT LED indicates that the OC48 IR 1310 card is carrying traffic or is traffic-ready.

2.20.2 OC48 IR 1310 Port-Level Indicators

You can find the status of the OC48 IR 1310 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-35 OC48 IR 1310 Block Diagram



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

2.20.3 OC48 IR 1310 Card Specifications

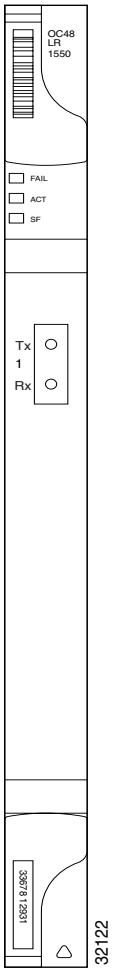
- Line
  - Bit Rate: 2488.320 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1310 nm Single Mode
  - Loopback Modes: Terminal and Facility

  - 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: 1310nm
  - 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 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.21 OC48 LR 1550 Card

The OC48 LR 1550 card provides one long-range, 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 on a per STS-1, STS-3c, STS-6c, STS-12c, or STS-48c basis. Figure 2-36 shows the OC48 LR 1550 faceplate and Figure 2-37 shows a block diagram of the card.

Figure 2-36 OC48 LR 1550 Faceplate



You can install OC48 LR cards in any ONS 15454 high-speed slot. You can provision the OC48 LR cards as part of a BLSR or UPSR or, in an ADM/TM configuration, as either an access tributary or a transport span interface.

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

The OC48 LR 1550 detects LOS, LOF, LOP, AIS-L, and RDI-L conditions (see Chapter 9, “CTC Alarms,” for a description of these conditions). The card also counts section and line BIT errors.

To enable automatic protection switching, the OC48 LR 1550 extracts the K1 and K2 bytes from the SONET overhead and processes them to switch accordingly. The DCC bytes are forwarded to the TCC.

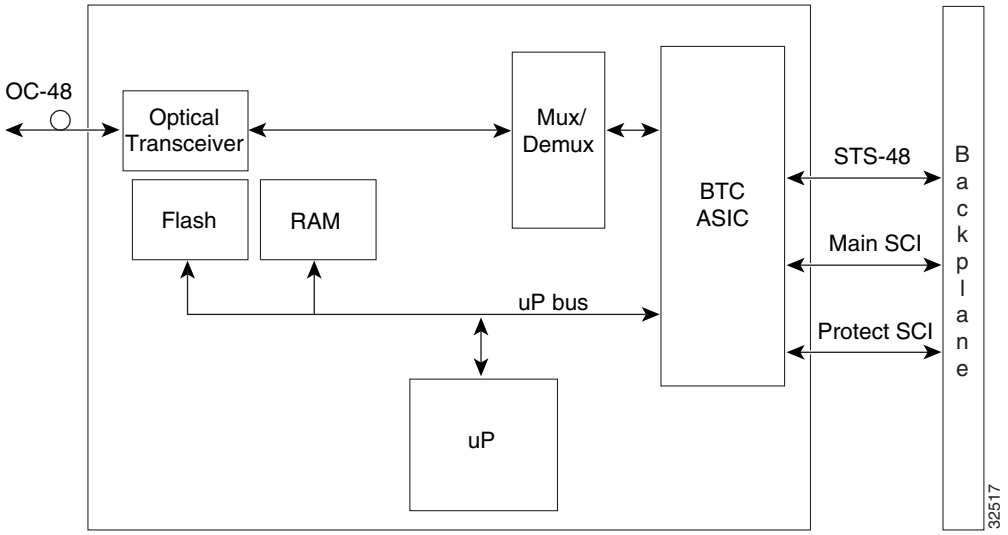
2.21.1 OC48 LR 1550 Card-Level Indicators

The OC48 LR 1550 card has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on the OC-48 interface. The green ACT LED indicates that the OC48 LR 1550 card is carrying traffic or is traffic-ready.

2.21.2 OC48 LR 1550 Port-Level Indicators

You can find the status of the OC48 LR 1550 card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, "CTC Alarms," for a complete description of the alarm messages.

Figure 2-37 OC48 LR Block Diagram



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

2.21.3 OC48 LR 1550 Card Specifications

- Line
  - Bit Rate: 2488.320 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: +3 dBm
  - Min. Transmitter Output Power: -2 dBm
  - Center Wavelength: 1520 nm – 1580 nm
  - Nominal Wavelength: 1550 nm
  - Transmitter: Distributed Feedback Laser
- Receiver
  - Max. Receiver Level: -8 dBm
  - Min. Receiver Level: -28 dBm
  - Receiver: InGaAs APD photo detector
  - Link Loss Budget: 26 dB min, with 1 dB dispersion penalty
- Environmental
  - Eye Safety Compliance: Class I
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 25 Watts
- Dimensions
  - Height:12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.22 OC48 ELR DWDM Cards

18 distinct OC-48 ITU 200GHz dense wavelength division multiplexing (DWDM) cards provide the ONS 15454 DWDM channel plan. Each OC48 DWDM card provides one Telcordia-compliant, GR-253 SONET OC-48 interface. The interface operates at 2.48 Gbps over a single-mode fiber span and carries both concatenated and non-concatenated payloads on an STS-1 or VT basis. Figure 2-38 shows the OC48 ELR faceplate and Figure 2-39 shows a block diagram of the card.

Figure 2-38 OC48 ELR DWDM Card Faceplate

Nine of the cards operate in the blue band with spacing of 200 GHz on the ITU grid (1530.33 nm, 1531.90 nm, 1533.47 nm, 1535.04 nm, 1536.61 nm, 1538.19 nm, 1539.77 nm, 1541.35 nm, 1542.94 nm), while the other nine operate in the red band with spacing of 200 GHz on the ITU grid (1547.72 nm, 1549.32 nm, 1550.92 nm, 1552.52 nm, 1554.13 nm, 1555.75 nm, 1557.36 nm, 1558.98 nm, 1560.61 nm).

You can install the OC48 ELR cards in any ONS 15454 high-speed slot. You can provision the OC48 ELR cards as part of a BLSR or UPSR or, in an ADM/TM configuration, as either an access tributary or a transport span interface.

Each OC48 DWDM card uses extended long reach optics operating individually within the ITU-T 200 GHz grid. The OC48 DWDM cards are intended to be used in applications with very long unregenerated spans of up to 200 km (with mid-span amplification). These transmission distances are achieved through the use of inexpensive optical amplifiers (flat gain amplifiers) such as erbium

doped fiber amplifiers (EDFAs). Using co-located amplification, distances up to 200 km can be achieved for a single channel (160 km for 8 channels). Maximum system reach in filterless applications without the use of optical amplifiers or regenerators is 24 dB or approximately 80 km, depending on the condition of the facilities, number of splices and connectors, or other performance-affecting factors. The OC48 DWDM cards feature wavelength stability of +/- 0.25 nm. Each interface contains a transmitter and receiver.

The OC48 DWDM cards are the first in a family of cards meant to support extended long reach applications in conjunction with optical amplification. Using electro-absorption technology, the OC48 DWDM cards provide a solution at the lower-extended long reach distances.

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

The OC48 ELR cards detect LOS, LOF, LOP, AIS-L, and RDI-L conditions (see Chapter 9, “CTC Alarms,” for a description of these conditions). The cards also count section and line BIT errors.

To enable APS, the OC48 ELR cards extract the K1 and K2 bytes from the SONET overhead and process them to switch accordingly. The DCC bytes are forwarded to the TCC.

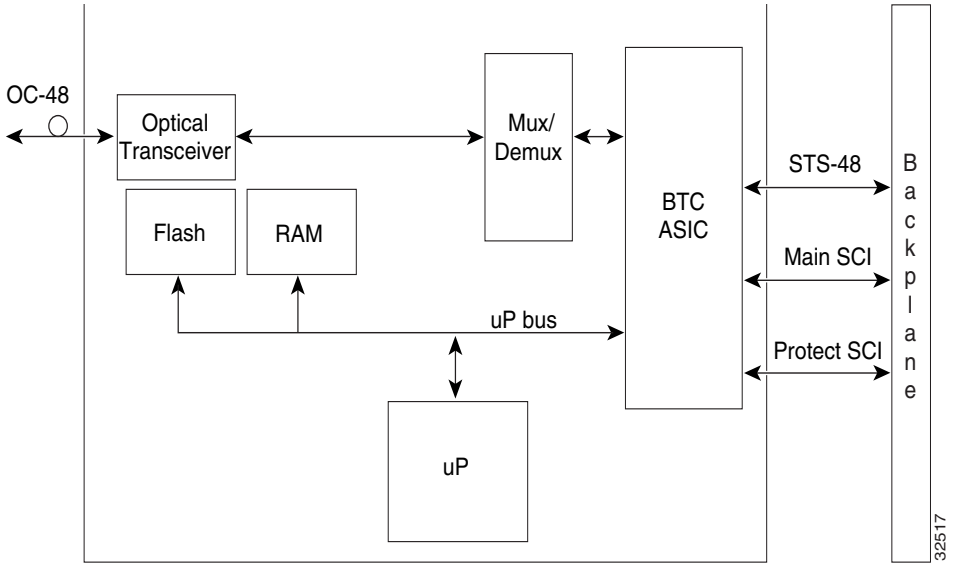
2.22.1 OC48 ELR Card-Level Indicators

The OC48 ELR cards have three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. The yellow SF LED indicates a signal failure or condition (LOS, LOF, or high BER) on the OC-48 interface. The green ACT LED indicates that the card is carrying traffic or is traffic-ready.

2.22.2 OC48 ELR Port-Level Indicators

You can find the status of the OC48 ELR card ports using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, “CTC Alarms,” for a complete description of the alarm messages.

Figure 2-39 OC48 ELR Block diagram



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

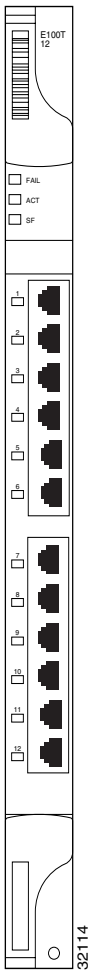
2.22.3 OC48 ELR Card Specifications

- Line
  - Bit Rate: 2488.320 Mbps
  - Code: Scrambled NRZ
  - Fiber: 1550 nm Single Mode
  - Loopback Modes: Terminal and Facility
  - Connectors: SC
  - Compliance: Telcordia SONET, GR-GSY-00253, ITU-T G692, ITU-T G958
- Transmitter
  - Max. Transmitter Output Power: 0 dBm
  - Min. Transmitter Output Power: -2 dBm
  - Center Wavelength: ±.25 nm
  - Transmitter: Electro-absorption laser
- Receiver
  - Max. Receiver Level: -8 dBm
  - Min. Receiver Level: -28 dBm
  - Receiver: InGaAs APD photo detector
  - Link Loss Budget: 26 dB min, with 1 dB dispersion penalty
- Environmental
  - Eye Safety Compliance: Class I
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 25 Watts
- Dimensions
  - Height:12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.23 E100T-12 Card

The E100T-12 card provides twelve ports of IEEE 802.3-compliant, 10/100 interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 200 Mbps per port and 2.4 Gbps per card. Each port independently detects 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. The card's faceplate and functionality are shown in Figure 2-40 and Figure 2-41.

Figure 2-40 E100T-12 Faceplate



The E100T-12 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 are provided.

The E100T-12 eliminates the need for external aggregation equipment such as routers or Ethernet switches, remote headends, or distributed point of presences (POPs).

Each E100T-12 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). 802.1p priority is also supported in order to provide multiple classes of service.

You can install the E100T-12 card in any general-purpose slot in the shelf assembly. Multiple Ethernet cards installed in an ONS 15454 act as a single switch supporting a variety of SONET port configurations. You can create logical SONET ports by provisioning a number of STS channels to the packet switch entity within the ADM. Logical ports can be created with a bandwidth granularity of STS-1. The ONS 15454 supports STS-1, STS-3c, STS-6c, or STS-12c configurations.

2.23.1 E100T-12 Card-Level Indicators

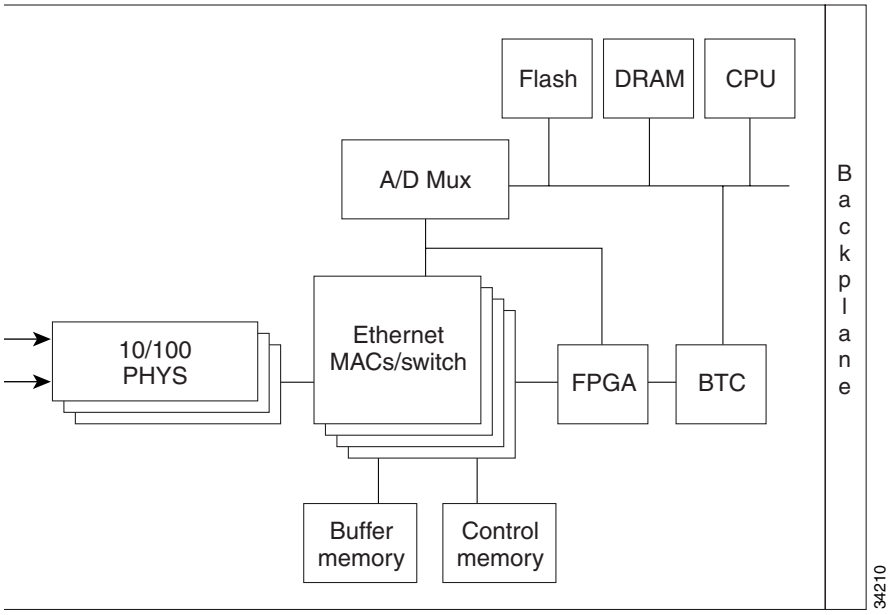
The E100T-12 card faceplate has three card-level LED indicators. The red FAIL LED indicates a hardware problem. Replace the card if the red FAIL LED persists. An ACT LED indicates the status of the E100T-12. The SF LED is reserved for future options.

2.23.2 E100T-12 Port-Level Indicators

The E100T-12 card also has twelve pairs of LEDs (one pair for each port) to indicate port conditions. A green LINK LED indicates link has been detected: ON means an active connection and OFF means no active connection.

You can find the status of the E100T-12 card port using the LCD screen on the fan tray assembly of the ONS 15454 shelf. Use the LCD to access quickly the status of any port or card slot; the screen displays the number and severity of alarms for a given port or slot. See Chapter 9, “CTC Alarms,” for a complete description of the alarm messages.

Figure 2-41 E100T-12 Block Diagram



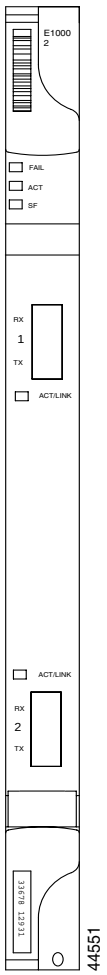
2.23.3 E100T-12 Card Specifications

- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5 - 95%, non-condensing
  - Power Consumption: 40 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

2.24 E1000-2 Card

The E1000-2 card provides two ports of IEEE-compliant, 1000 Mbps interfaces. Each interface supports full-duplex operation for a maximum bandwidth of 2 Gbps per port and 4 Gbps per card. Each port auto-configures for full duplex and 802.3x flow control. The E1000-2 card uses GBIC modular receptacles for the optical interfaces. For Release 2.2.0, two GBIC modules are offered as separate orderable products for maximum customer flexibility: An IEEE 1000Base-SX compliant, 850 nm optical module and an IEEE 1000Base-LX-compliant, 1300 nm optical module. The 850 nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300 nm LX optics are designed for single-mode fiber and distances of up to five kilometers. Other GBIC modules for long reach 1550 nm and twisted-pair copper will be offered for use with the E1000 card when those components become available. The card's faceplate and functionality are shown in Figure 2-42 and Figure 2-43.

Figure 2-42 E1000-2 Card Faceplate



The E1000-2 Gigabit Ethernet card provides high-throughput, low-latency packet switching of Ethernet encapsulated traffic (IP and other layer 3 protocols) across a SDH/SONET network while providing a greater degree of reliability through SONET "self-healing" protection services. This enables network operators to provide multiple 1000 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.

The E1000-2 card eliminates the need for external aggregation equipment such as routers, Ethernet or ATM switches at the customer site, remote headends, or distributed POPs.

Each E1000-2 card supports standards-based, layer 2+ Ethernet switching between its Ethernet interfaces and any other Ethernet or SONET trunk interfaces on the ONS 15454. 802.1q tag and port-based VLANS are supported in order to logically isolate traffic (typically subscribers). 802.1p priority is also supported in order to provide multiple classes of service.

You can install the E1000-2 card into any general-purpose slot in the shelf assembly for a total shelf capacity of 20 Gigabit Ethernet ports. Multiple Ethernet cards installed in an ONS 15454 can act as either a single switching entity or as a single switch supporting a variety of SONET port configurations. You can create logical SONET ports by provisioning a number of STS channels to the packet switch entity within the Cisco ADM. Logical ports can be created with a bandwidth granularity of STS 1. In a single or multicard configuration, the ONS 15454 can support the following unstitched STS configurations: 1 STS-12c, 2 STS-6c, 4 STS-3c, or 12 STS-1 and the following stitched configurations: 2 STS-6c, 4 STS-3c, or 12 STS-1s.

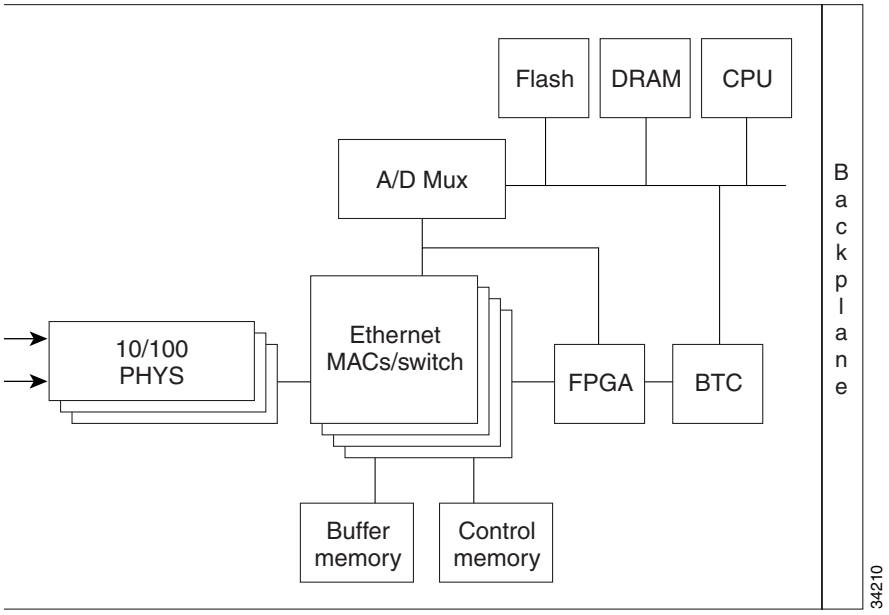
2.24.1 E1000-2 Card-Level Indicators

The E1000-2 card faceplate has two card-level LED indicators. The red FAIL LED indicates a hardware problem or catastrophic software failure on the E1000-2 card. As part of the boot sequence, the FAIL LED is turned on until the software deems the card operational. A green ACT LED provides the operational status of the E1000-2. When the ACT LED is green it indicates that the E1000-2 card is active and the software is operational.

2.24.2 E1000-2 Port-Level Indicators

The E1000-2 card also has one bi-color LED per port. The green LINK LED indicates whether linkbeat has been detected (ON), meaning that an active network cable is installed, or if an active network cable is not plugged into the port (OFF). The amber port ACT LED flashes at a rate proportional to the level of traffic being received and transmitted over the port.

Figure 2-43 E1000-2 Block Diagram



2.24.3 E1000-2 Card Specifications

- Environmental
  - Operating Temperature: 0 to +55 degrees Celsius
  - Operating Humidity: 5- 95%, non-condensing
  - Power Consumption: 40 Watts
- Dimensions
  - Height: 12.650 in.
  - Width: 0.716 in.
  - Depth: 9.000 in.

Using the Cisco Transport Controller

This chapter explains how to connect computers to the Cisco ONS 15454 and set up the ONS 15454 using the Cisco Transport Controller (CTC) software.

3.1 Overview

CTC is a Java application that is downloaded from the Timing Communications and Control (TCC) card to your computer when you connect to the ONS 15454. CTC allows you to provision and manage the ONS 15454 using Netscape Navigator or Microsoft® Internet Explorer. You can also use TL1 commands to communicate with the ONS 15454 through VT100 terminals, VT100 emulation software, or you can Telnet to the node using TL1 port 2361.

To use CTC, your computer needs a web browser and appropriate versions of the Java Runtime Environment (JRE) and Java plug-ins. Netscape Communicator and required Java files are provided on the Cisco ONS 15454 software CD. You can install Netscape and the Java files using procedures in the following sections.

Each time you connect to an ONS 15454, a CTC launcher is downloaded from the ONS 15454 TCC card to your computer. The launcher verifies that the computer has a CTC version that matches the version on the TCC. If the computer does not have CTC, or if the version on the TCC is a later release, the launcher downloads the CTC application to the temporary directory designated by your computer's operating system. (For a detailed description of the TCC card, see the "Timing Communication and Control (TCC/TCC+) Card" section on page 2-7.)

3.2 Preparing PCs to Run CTC

The following minimum requirements are needed to run CTC from personal computers:

- 486 processor
- 128 megabytes of RAM
- LAN connection (to access the ONS 15454 through a LAN)
- Windows 95, Windows 98, or Windows NT (Windows NT is recommended)
- Any one of the following:
  - Netscape Navigator 4.08 or higher
  - Netscape Communicator 4.61 or higher, or
  - Internet Explorer 4.0 (service pack 2) or higher

Netscape Communicator is included on the Cisco ONS 15454 software CD. Internet Explorer 5.0 is included with Windows 98 second edition.

- Java Runtime Environment 1.2.2 with Java 1.2 plug-in (included on CTC software CD)
- User-supplied category 5 cable with RJ-45 connectors on each end

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

Procedure: Install Netscape Communicator (Windows)

If a web browser is not installed, install Netscape Communicator or Microsoft Internet Explorer using procedures provided by those vendors. Netscape Communicator is provided on the Cisco ONS 15454 software CD. To install it:

Step 1 Insert the Cisco ONS 15454 software CD into your PC's CD drive.

Step 2 In the Windows/Netscape directory, double click **n32e461.exe** and follow the on-screen instructions.

Procedure: Install the Java Files (Windows)

Step 1 Insert the ONS 15454 software CD into your PC's CD drive.

Step 2 In the Windows/Jre1.2.2 folder, double click **jre1_2_2-win.exe** and follow the on-screen instructions.

Step 3 In the Windows folder, double click **JavaPolicyInstall.bat**.

A message displays on the DOS screen stating the installation was successful.

Step 4 Enable the JRE 1.2 plug-in:

(a) From the Windows Start menu, select **Programs>Java Plug-in Control Panel**.

(b) On the Java Plug-in Properties dialog, click the **Advanced** tab.

(c) Under Java Run Time Environment, choose **JRE 1.2**.

(d) Click **Apply**. Close the Java Plug-in Properties dialog.

3.3 Preparing Solaris Workstations to Run CTC

To install CTC Release 2.2.0 software on Solaris workstations, the workstation must have Solaris 2.6 or 2.7 installed, with a minimum 128 megabytes of RAM. Use the following procedures to install Netscape and the appropriate Java files on the Solaris workstation.

Note Solaris installation instructions use "CD/" instead of an actual CD-ROM path. Remember to substitute the path to your CD-ROM drive.

Procedure: Install qzip

To install Netscape, you need qzip. If qzip is not installed:

Step 1 Insert the Cisco Transport Controller Release 2.2.0 CD into your CD-ROM drive. If the directory of the CD does not open automatically, open it.

Step 2 Extract the files from the CD/Solaris/files.tar archive to a temporary directory on your hard drive by typing:

```
cd /var/tmp
tar xvf /CD/solaris/files.tar
```

Step 3 Copy qzip from the /var/tmp/Solaris/Netscape to /usr/local/bin (you may need to create /usr/local/bin and add it to your path). Type:

```
mkdir -p /usr/local/bin
cp /var/tmp/Solaris/Netscape/qzip /usr/local/bin
```

Step 4 Add /usr/local/bin and /opt/NSCPcom to your search path by typing:

```
csh: % set path = ( /usr/local/bin /opt/NSCPcom $path )
sh or ksh: # PATH=/usr/local/bin:/opt/NSCPcom:$PATH
# export PATH
```

Step 5 Set the environment variable in the startup files in each user's home directory: .cshrc for csh and .profile for sh or ksh.

Procedure: Install Netscape Navigator (Solaris)

If Netscape Navigator 4.08 or Netscape Communicator 4.61 or later is not installed on the workstation, install it from the CTC Release 2.2.0 CD:

Step 1 Insert the Cisco Transport Controller Release 2.2.0 CD into your CD-ROM drive. If the directory of the CD does not open automatically, open it.

Step 2 Extract the files from the CD/Solaris/files.tar archive (if not extracted in a previous procedure) to a temporary directory on your hard drive by typing:

```
cd /var/tmp
tar xvf /CD/solaris/files.tar
```

Step 3 Go to /var/tmp/Solaris/Netscape and type:

```
tar xvf navigator-v408-export.sparc-sun-solaris2.5.1.tar
```

Step 4 Follow the instructions in: /var/tmp/Solaris/Netscape/navigator-v408.sparc-sun-solaris2.5.1/README.install.

When prompted for the Netscape Communicator software location, type:

```
/opt/NSCPcom
```

Netscape Communicator is installed in [/opt/netscape]: /opt/NSCPcom.

Procedure: Install the Java Files (Solaris)

If JRE 1.2.2.2_05 with Java 1.2 plug-in is not installed on the workstation, complete Steps 1-8 to install it from the CTC Release 2.2.0 CD. If JRE 1.2.2.2_05 with 1.2 plug-in is installed, skip to Step 9.

Step 1 Insert the Cisco Transport Controller Release 2.2.0 CD into your CD-ROM drive. If the directory of the CD does not open automatically, open it.

Step 2 Extract the files from the CD/Solaris/files.tar archive (if not extracted in a previous procedure) to a temporary directory on your hard drive by typing:

```
cd /var/tmp
tar xvf /CD/solaris/files.tar
```

Step 3 Go to the /var/tmp/Solaris/Jre1.2.1_05/ directory and unpack the appropriate tar archive:

- For Solaris 2.6, unpack the *.6.tar archive
- For Solaris 2.7, unpack the *.7.tar archive

Step 4 Un-compress each patch file by typing:

```
cd /var/tmp/Solaris/Jre1.2.1_05
tar -xvf 1.2.1_03_patches_sparc_5.6.tar# or ...5.7.tar
cd 5.6 or 5.7
uncompress *
```

Step 5 For each un-compressed tar file, unpack the archive, enter the directory, and follow the instructions, for example:

```
tar xvf 105181-11.tar
```

Step 6 Remove the intermediate tar files, for example:

```
rm *.tar
```

Step 7 Add each patch using /usr/sbin/patchadd, for example:

```
/usr/sbin/patchadd 105181-11
```

Note Refer to http://java.sun.com/products/jdk/1.2.1/install-solaris-patches.html for more information on installing Solaris patches.

Step 8 Install the Java 1.2 plug-in using /usr/sbin/pkgadd, for example,

```
cd /var/tmp/Solaris/Jre1.2.1_03
tar xvf plugin-12-sparc.tar
pkgadd -d . SUNWj2pi
```

This installs javaplugin.so into /opt/NSCPcom/plugins. If Netscape was installed under /opt/NSCPcom, the plug-in is installed in the Netscape directory. If so, copy javaplugin.so to <Netscape-directory>/plugins. For more information about installing the JRE, see:

```
http://java.sun.com/products/jdk/1.2/runtime_solaris.html
```

Step 9 Modify *java.policy* to allow the CTC launcher to write to the workstation's hard drive:

(a) Exit Netscape if a Netscape session is running.

(b) Modify *java.policy*:

- To enable the applet for all users, copy the lines from: /CD/Cerent/LAUNCHER.policy to /opt/NSCPcom/j2pi/lib/security/java.policy.

Otherwise:

- If your home directory has a .java.policy file, copy the lines from /CD/Cerent/LAUNCHER.policy to that file.
- If your home directory does not have a .java.policy file, copy the /CD/Cerent/LAUNCHER.policy file to your home directory and rename it .java.policy.

Note The per-user .java.policy has a leading period (.) while the system-wide file does not.

Step 10 Use Netscape to launch and run CTC. (Before launching Netscape, make sure to put /opt/NSCPcom/j2pi/bin in your path.)

Step 11 Clean up the temporary files by typing:

```
cd /var/tmp
rm -fr Solaris
```

Step 12 Type `eject cdrom` to remove the CTC CD from your CD-ROM drive.

3.4 Connecting PCs to the ONS 15454

You can connect a PC to the ONS 15454 using the RJ-45 LAN port on the TCC or the LAN 1 pins on the ONS 15454 backplane. For initial setup, use the front panel RJ-45 port. For long-term connections, Cisco recommends using the LAN pins to keep the front panel area uncluttered. For a list of LAN pin assignments, see Table 1-2 on page 1-31.

Each ONS 15454 must have a unique Internet Protocol (IP) address that you use to access the ONS 15454. The address is displayed on the front panel's liquid crystal display (LCD) at turn-up. The initial IP address, 192.1.0.2, is a generic default address for ONS 15454 access and configuration.

Each computer used to communicate with the ONS 15454 should have only one IP address.

Note Do not use dual Network Interface Cards or an enabled NIC card and dial-up adapter at the same time; this hampers communication between the CTC and ONS 15454s.

3.4.1 Direct Connections

Use the following procedures to connect a PC running Windows 95, Windows 98, or Windows NT directly to an ONS 15454.

Procedure: Setup a PC for Direct Connection

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

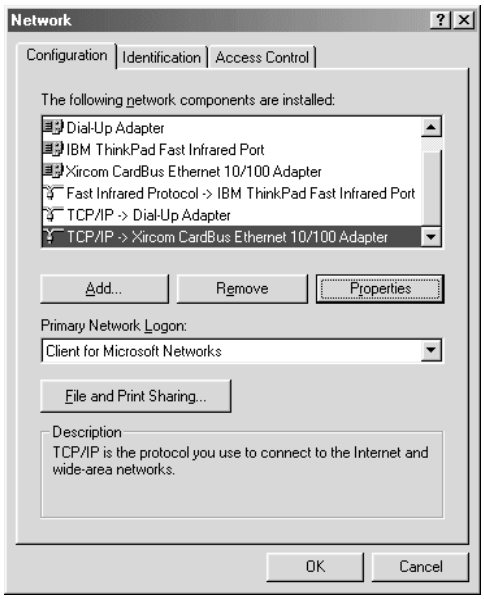
Step 2 On the Control Panel dialog, click the **Network** icon.

Step 3 On the Network dialog, shown in Figure 3-1, select the following:

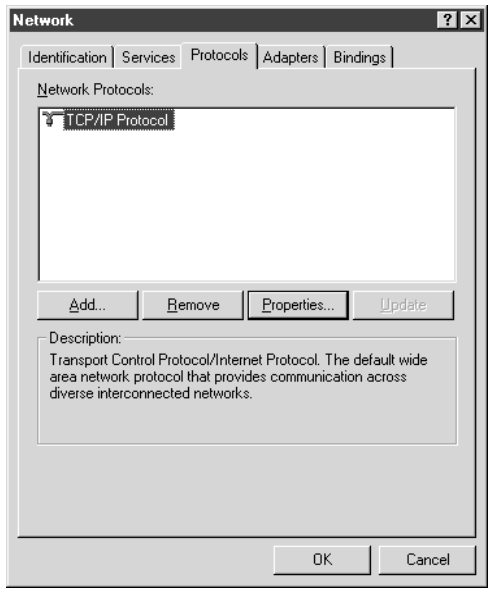
- Windows 95/98: select TCP/IP for your PC Ethernet card, then click **Properties**.
- Windows NT: choose the **Protocols** tab, select **TCP/IP Protocol**, and click **Properties**.

Figure 3-1 Network Dialog

Windows 95/98



Windows NT



34330

Step 4 (Windows 95/98 only) On the TCP/IP Properties dialog:

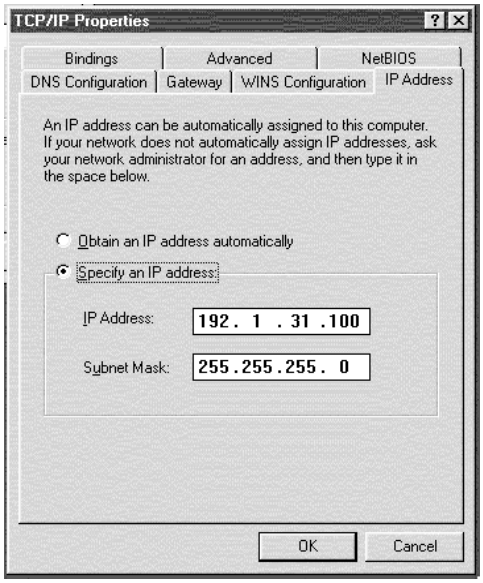
(a) Click the **DNS Configuration** tab and select **Disable DNS**.

(b) Click the **WINS Configuration** tab and select **Disable WINS Resolution**.

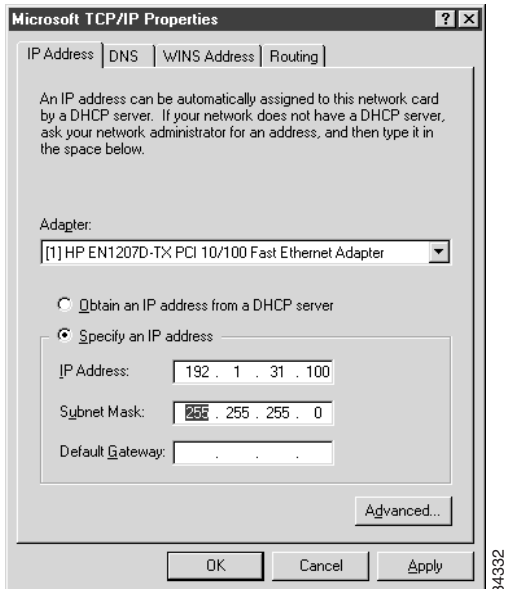
Step 5 Click the **IP Address** tab to open the IP Address window (Figure 3-2).

Figure 3-2 IP Address Window

Windows 95/98



Windows NT



Step 6 Click **Specify an IP address**.

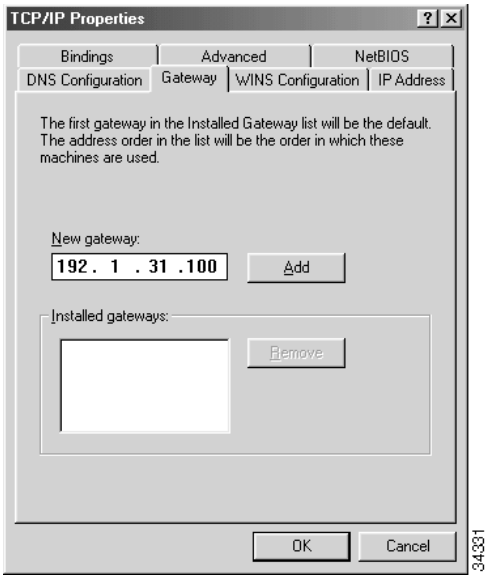
Step 7 In the *IP Address* field, enter an IP address identical to the ONS 15454 (the ONS 15454 IP address is shown on the front LCD panel) except for the last three digits. The last three digits must be between 1 and 254. This places the PC on the same subnet as the ONS 15454.

Step 8 Type 255.255.255.0 in *Subnet Mask*.

Step 9 Click **OK**.

Step 10 (Windows 95/98) Click the **Gateway** tab (Figure 3-3).

Figure 3-3 TCP/IP Properties - Gateway Tab (Windows 95/98)



Step 11 This step defines the ONS 15454 as the default gateway for the PC. In *New Gateway* (Windows 95/98) or *Default Gateway* (Windows NT), type the ONS 15454 IP address. For initial setup, this is the default address that ships with the ONS 15454 (192.1.0.2).

Step 12 Click **Apply** (Windows NT) or **Add** (Windows 95/98). For Windows 95/98, verify that the IP address displays in the *Installed Gateways* field.

Step 13 If your PC runs on Windows 95/98, you will be prompted to restart your PC. Click **Yes**. If your PC runs on Windows NT, you do not need to restart your computer.

Step 14 Test the connection:

(a) Start Netscape Navigator or Windows Explorer.

(b) Enter the ONS 15454 IP address in the Web address (URL) field. Within 30 seconds, the CTC login screen displays. If it does not appear, continue with Steps c and d.

(c) From the Windows Start menu, choose MS-DOS prompt.

(d) At the DOS prompt, type `ping [ONS 15454 IP address]`, for example, `ping 192.1.0.2`. If your computer is connected to the ONS 15454, a `reply from [IP address]` message displays.

If your PC is not connected, a `Request timed out` message displays. If this occurs, check that the cables connecting the PC to the ONS 15454 are securely attached. Check the Link Status LED on the PC NIC card. Repeat Steps 1-14, verifying IP and submask information.

3.4.2 Local Area Network Connections

To access the ONS 15454 from a local area network (LAN):

- The ONS 15454 IP address must be changed to a LAN-compatible IP address.
- The ONS 15454 must be physically connected to the LAN (typically using cross-over cable to a router, hub, or switch).
- If the PC Network settings were changed for direct access to the ONS 15454, change the settings back to LAN access. Usually this means setting the IP Address on the TCP/IP dialog back to "Obtain an IP address automatically." If your LAN requires that DNS or WINS is enabled, change the setting on the DNS Configuration or WINS Configuration tab of the TCP/IP dialog.
- If your computer is connected to a proxy server, disable proxy service or add the ONS 15454 nodes as exceptions.

If these conditions have been met, to access the ONS 15454, start your web browser and type the ONS 15454 IP address in the URL field.

Procedure: Disable Proxy Service: Windows with Internet Explorer

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

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

Step 3 From the Internet Properties dialog, select the **Connections** tab and click **LAN Settings**.

Step 4 On the Local Area Network (LAN) Settings dialog do one of the following:

- Deselect "Use a proxy server" to disable the service, or

- Leave "User a proxy server" selected and click **Advanced**. On the Proxy Setting dialog under *Exceptions*, enter the IP addresses of ONS 15454 nodes that you will access. Separate each address with a semi colon. You can insert an asterisk for the host number to include all the ONS 15454s on your network. Click **OK** to close each open dialog.

Procedure: Disable Proxy Service: Windows with Netscape

Step 1 Open Netscape.

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

Step 3 In the Preferences dialog under Category, select **Advanced>Proxies**.

Step 4 On the right side of the Preferences dialog under Proxies, do one of the following:

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

3.4.3 Remote Access to the ONS 15454

You can remotely access an ONS 15454 node using a LAN modem. The LAN modem must be connected to the RJ-45 port on a TCC card or to the LAN pins on the ONS 15454 backplane. The LAN modem must be properly configured for use with the ONS 15454. When the modem is installed, dial-up access to the ONS 15454 is available using a personal computer modem.

3.4.4 Connecting to the ONS 15454 with TL1 Terminals

Although the ONS 15454 is designed to be used with CTC, you can communicate with the ONS 15454 using TL1 commands or Telnet to port 2361. To connect a TL1 terminal (or a PC running terminal emulation software) to the ONS 15454, use the DB-9 plug on the front panel of the TCC or the CRAFT pins on the backplane. For a list of CRAFT pin assignments, see Table 1-3 on page 1-31. For information about TL1 commands that can be used with the ONS 15454, see Chapter 11, "TL1 Reference."

3.5 Logging into the ONS 15454

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

Procedure: Log into the ONS 15454

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

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

When the PC connects to the ONS 15454, the login window displays (Figure 3-4).

Figure 3-4 Login Screen

Step 3 Type a valid user name and password. For initial setup, type the user name "CISCO15" and click **Login** (no password is required).

Note CISCO15 is the default user name provided with every ONS 15454. This user name has Superuser rights and privileges so you can set up other ONS 15454 users. The CISCO15 user is delivered without a password. To assign a password, click the **Provisioning>Security** tabs and change the Superuser password. In addition to CISCO15 user, a "cerent454" user is provided for compatibility with previous CTC releases. For more information about ONS 15454 security, see the "Setting Up ONS 15454 Security" section on page 3-24.

After logging in, the CTC node view (Figure 3-5) appears. From here, you can navigate to other CTC views to perform the ONS 15454 operations, administration, maintenance, and provisioning tasks described in the following sections.

Note The term "node" refers to a single ONS 15454. See the glossary for a detailed definition.

3.6 CTC Views

The CTC window includes a menu bar and a top and bottom pane. CTC provides three ONS 15454 views:

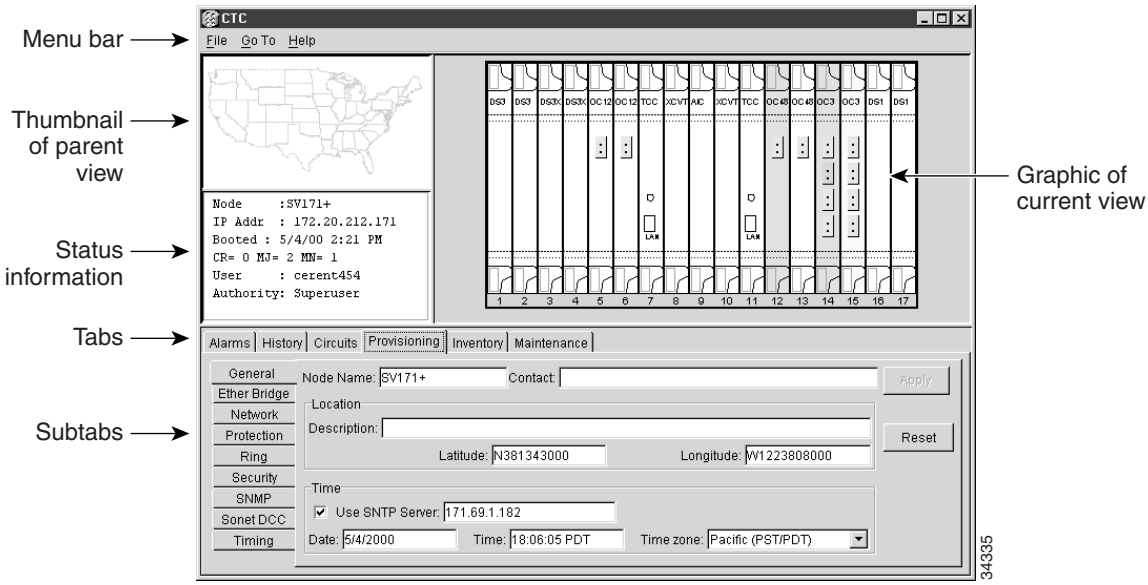
- *Network view*—displays information about the ONS 15454 network. You perform ONS 15454 network management tasks in this view.
- *Node view*—displays information about one ONS 15454 node. You perform node management tasks in this view.
- *Card view*—displays information about individual ONS 15454 cards. You perform card management tasks in this view.

A graphic of the current view appears in the upper right portion of the CTC window. The node view displays the ONS 15454 shelf. The network view displays a background map with ONS 15454 nodes represented by colored squares. The card view displays a graphic of the selected card.

A thumbnail of the parent view is displayed in the upper left corner of the CTC window. Parent view is the level above the current view. For example, network view is the parent of node view, and node view is the parent of card view. Below the thumbnail, status information for the current view is shown. In node view, the Node name; IP address; session boot date and time; a summary of critical (CR), major (MJ), and minor (MN) alarms; the name of the user who is logged in; and the user's security level are shown. In network view, the status of the selected node or span is shown.

The middle of the CTC window provides tabs to access CTC functions. Some CTC tabs have subtabs, which are used to access subfunctions. The tabs that are displayed depend on the view. In node view, six tabs are displayed: Alarms, History, Circuits, Provisioning, Inventory, and Maintenance. In network view, only the Alarms, History, and Circuits tabs are displayed. CTC window elements are shown in Figure 3-5.

Figure 3-5 CTC Window Elements



3.6.1 Node View

The CTC node view (Figure 3-5) is displayed each time you log into CTC. Node view shows a real-time depiction of the ONS 15454 shelf. The colors of the cards, shown in Table 3-1, indicate the status of the physical card and slot.

Table 3-1 Node View Card Colors

Card Color	Status
Grey	slot is not provisioned; no card is installed
Blue	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

Node view provides six tabs to access node information and perform node maintenance and provisioning tasks. Some tabs have subtabs. Figure 3-5 shows the CTC Node view with the Provisioning subtabs displayed. Node view tabs and subtabs are shown in Table 3-2.

Table 3-2 Node View Tabs and Subtabs

Tab	Description	Subtabs
Alarms	Lists current alarms for 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 since the software installation.	Session, Node
Circuits	Allows you to create, delete, edit, and map circuits	none
Provisioning	Provision the ONS 15454 node	General, Ether Bridge, Network, Protection, Ring, Security, SNMP, Sonet DCC, Timing
Inventory	Provides inventory information (part number, serial number, CLEI codes) for cards installed in the node	none
Maintenance	Allows you to perform maintenance tasks for the node	Database, Ether Bridge, Protection, Ring, Software, XC cards, Timing, Diagnostic

3.6.2 Network View

Network view (Figure 3-6) displays information about the ONS 15454 network. You perform network provisioning and management tasks in this view. A United States map is displayed and the ONS 15454 nodes are represented by colored squares. The color of the square indicates the status of the node. Table 3-3 shows the colors and their corresponding status.

Figure 3-6 Network View

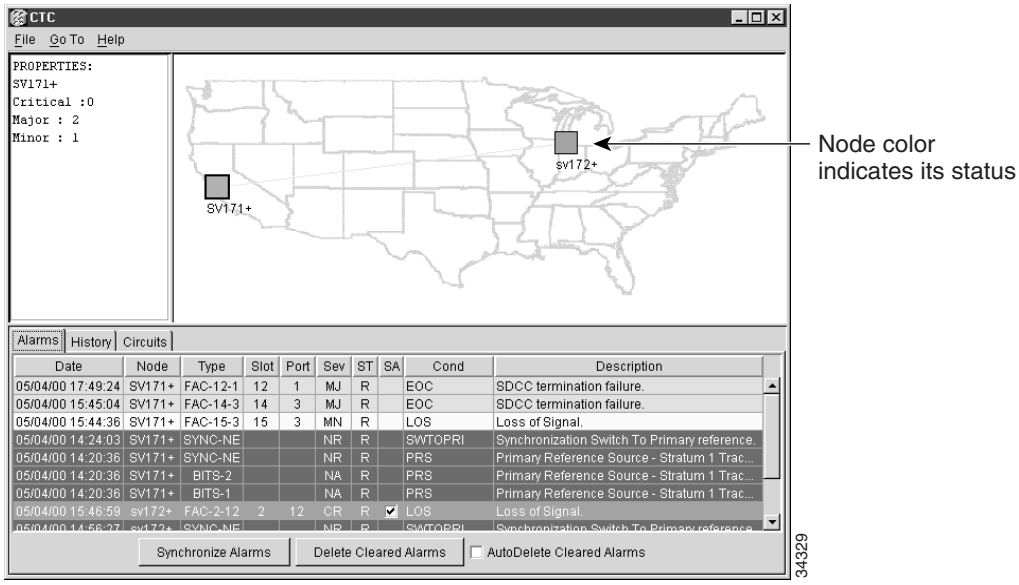


Table 3-3 Node Status

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

The network view tabs display network alarms and alarm history and allow you to set up and edit network circuits. In addition, you can click spans (the lines connecting the nodes) and node icons on the network map to quickly view circuit properties, provision circuits, and perform protection switches. Table 3-4 shows the actions that you can perform in network view.

Table 3-4 Network View Actions

Action	Procedure
Open a node	Any of the following: • Double click the node icon • Right-click the icon, choose Open from the shortcut menu • From the CTC Go To menu, choose Other Node, then choose the node from the Select Node dialog
Move a node icon	Pressing the Control <Ctrl> and left mouse buttons, drag the node icon to a new location.
Reset node icon position	Right click a node and choose Reset Position from the shortcut menu. The node icon moves to the position defined by the longitude and latitude fields on the General subtab.
Display span properties	Click a network span. Properties display in the upper left corner of the window.

Table 3-4 Network View Actions (continued)

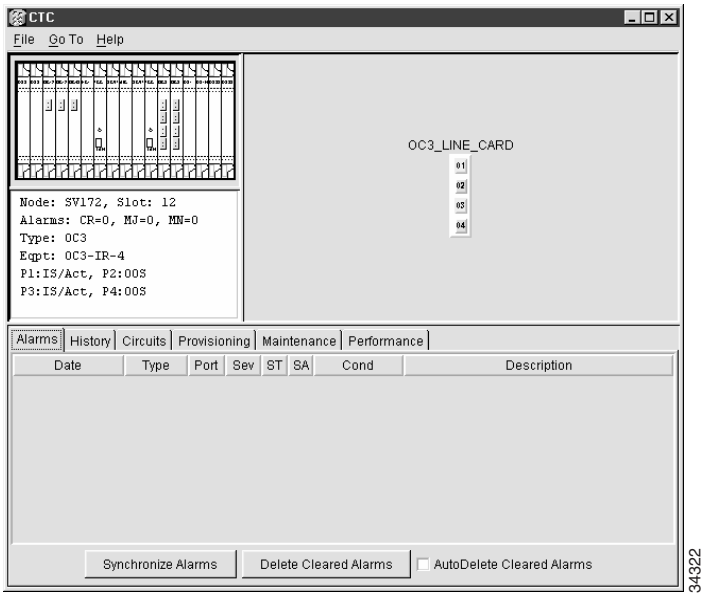
Action	Procedure
Perform a UPSR protection switch for an entire span	Right click a network span and click Circuits. See the "Switch UPSR Traffic" section on page 4-24 for UPSR protection switch procedures.
Provision a circuit	Right click a node and choose Provision Circuit from the shortcut menu. For circuit procedures, see the "Create a Circuit" section on page 4-41.
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 the new node.

3.6.3 Card View

Card view displays information about individual ONS 15454 cards. (Figure 3-7 shows an OC3 IR 4 1310 in card view.) You perform card-specific maintenance and provisioning tasks in card view. The information that is displayed and the tasks you can perform depend on the card. CTC displays a card view for all ONS 15454 cards except the TCC, XC, and XCVT cards.

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

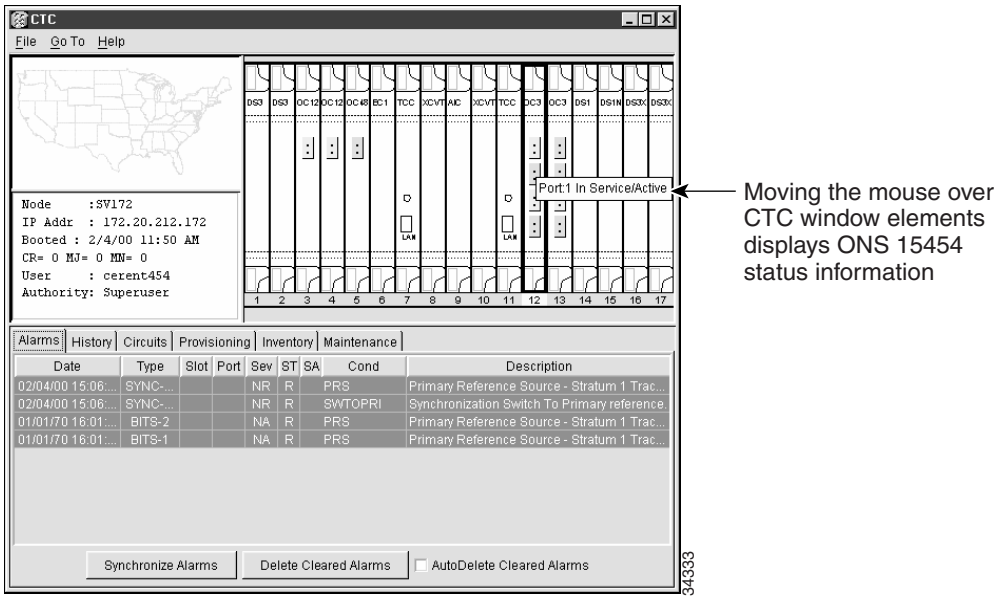
Figure 3-7 Card View



3.7 CTC Navigation

You can use different methods to navigate to views within the CTC window. You can select views from the Go To menu. You can also double click or right click objects in the window. Moving the mouse over nodes, cards, and card ports displays popup information about the node, card, or port. Figure 3-8 shows an example.

Figure 3-8 CTC Popup Information



Moving the mouse over CTC window elements displays ONS 15454 status information

Different methods for navigating within the CTC window are shown in Table 3-5.

Table 3-5 CTC Window Navigation

Technique	Description
Go To menu	
• Network View	Displays the network view
• Parent View	Displays the parent of the currently selected view; in card view, node view will be displayed. In node view, the network view will display.
• Selected object	Displays the currently selected object; if you select a card on the node view shelf, the card view for the selected card will display. If you select a node on the network view map, the node view for the node will display.
• Other Node	Displays a dialog where you can select any node within the current network.
Double Click	
• Network Thumbnail	Displays the network view
• Node Thumbnail	Displays the node view
• Node on the network view map	Displays the node in node view
• Card in node view	Displays the card in card view
Right Click	
• Node in network view	Displays a menu from which you can: 1) open the node, 2) provision the circuits, 3) update circuits with a new node, and 4) reset the node icon position to the longitude and latitude provisioned for the node on the Provisioning>General tabs.
• Span in network view	Displays a menu from which you can 1) view information about the source and destination slots, ports, the span's protection scheme and optical or electrical level, and 2) display a Circuits on Span dialog. This dialog displays additional span information and allows you to perform UPSR protection switching.

Table 3-5 CTC Window Navigation (continued)

Technique	Description
• Card in card view	Displays a menu from which you can: 1) open the card, 2) delete the card, and 3) reset the card.
Move Mouse Cursor	
• Over node in network view	Displays a summary of node alarms and provides a warning if the node icon has been moved out of the map range
• Over span in network view	Displays circuit (node, slot, port) and protection information
• Over card in node view	Displays card type and card status
• Over card port in node view	Displays port number and port status

3.8 Viewing CTC Table Data

Much of the ONS 15454 data that CTC displays, such as alarms, alarm history, circuits, and node 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 except Inventory.)
- Export CTC table data to spreadsheets and database management programs to perform additional data manipulation. For exporting procedures, see the "Printing and Exporting CTC Data" section on page 3-34.

To change CTC table display, left-click or right-click a table column header. Right clicking a column header displays a shortcut menu, shown in Figure 3-9, with table column display options.

Figure 3-9 Table Column Shortcut Menu

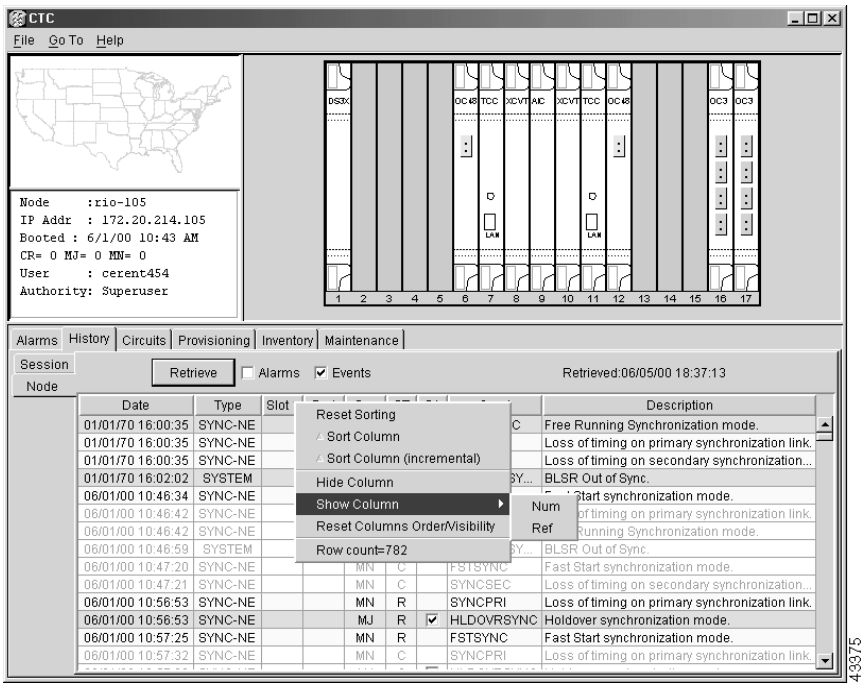


Table 3-6 lists the options that you can use to customize information display in CTC tables.

Table 3-6 Table Display Options

Task	Click	Right Click Shortcut Menu
Rearrange column order	Drag column header right or left	N/A
Reset column order	N/A	Select Reset Columns Order/Visibility
Hide column	N/A	Select Hide Column
Resize column	Position cursor over the column border and drag right or left	N/A
Display a hidden column	N/A	Select Show Column>[column name]
Display all hidden columns	N/A	Select Reset Columns Order/Visibility
Sort table (primary)	Click a column header; each click changes sort order (ascending or descending)	Select Sort Column
Sort table (secondary sorting keys)	Pressing Shift, click column header	Select Sort Column (incremental)
Reset sorting	N/A	Select Reset Sorting
View table row count	N/A	Table row count is the last item on the shortcut menu

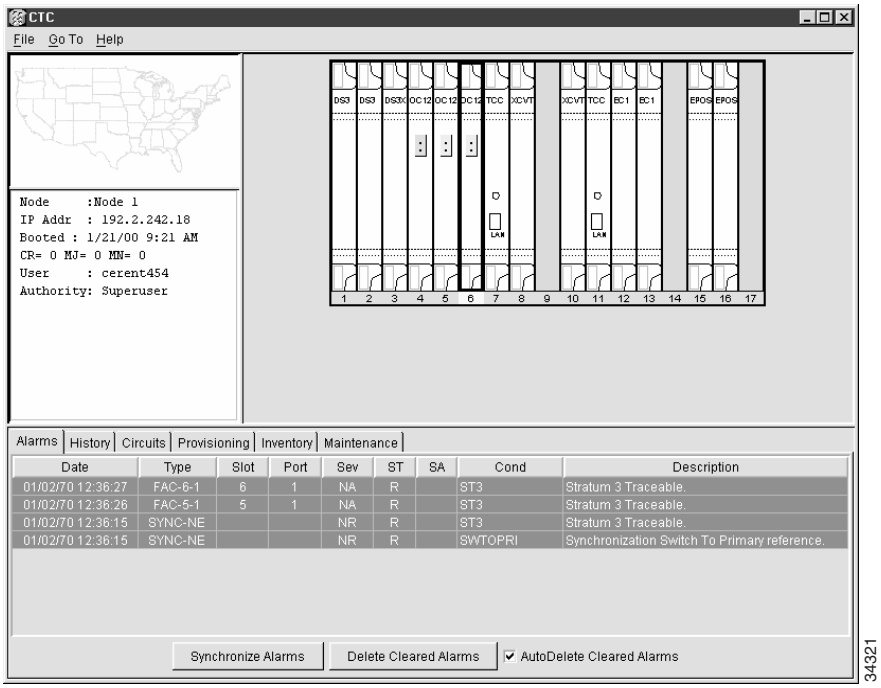
3.9 Viewing ONS 15454 Alarms

Select the Alarms tab (Figure 3-10) to display current and cleared alarms generated on the node. Table 3-7 shows the information that is displayed for each ONS 15454 alarm.

Table 3-7 Alarm Data

Column	Description
Num	Unique, per-node alarm identifier (this column is hidden by default)
Ref	If an alarm references another alarm, the number of the referenced alarm (this column is hidden by default)
Date	Date and time of the alarm
Node	Node where the alarm occurred, based on the active TCC (displays in network view only)
Type	Type of alarm, based on circuit type
Slot	Slot where the alarm occurred
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)
SA	When checked, indicates the alarm is service affecting
Cond	The error message code. See Chapter 9, “CTC Alarms” for troubleshooting procedures
Description	Description of the alarm

Figure 3-10 Alarms Tab



Alarms are displayed in one of five background colors, listed in Table 3-8, to quickly communicate the alarm severity. For information about troubleshooting alarms, see Chapter 9, “CTC Alarms.”

Table 3-8 Alarm Colors

Color	Description
Red	Critical Alarm
Orange	Major Alarm
Yellow	Minor Alarm
Blue	Event Notification (not an alarm)
White	Cleared alarm or event

3.9.1 Controlling Alarm Display

You can control the display of alarms on the Alarms tab. Table 3-9 shows the actions you can perform from the Alarms tab.

Table 3-9 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
Checkbox	
AutoDelete Cleared Alarms	If checked, automatically deletes cleared alarms

3.9.2 Viewing Alarm History

The History tab displays historical alarm data. The History tab also shows the events (that is, non-reported activities) that occur in addition to the alarms. For example, protection switching events or performance monitoring threshold crossings appear here. The History tab presents two alarm history views:

- The Session subtab (Figure 3-11) presents alarms and events for the current CTC session. (Events are non-reported activities, such as timing changes and threshold crossings.) When you log off, the alarms disappear.
- The Node subtab (Figure 3-12) shows the alarms and events that occurred at the node since the CTC software installation. The ONS 15454 can store up to 256 critical alarms, 256 major alarms, 256 minor alarms, and 256 events. When the limit is reached, the ONS 15454 discards the oldest alarms and events.

Tip Double click an alarm in the alarm table 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 3-11 History>Session Subtab

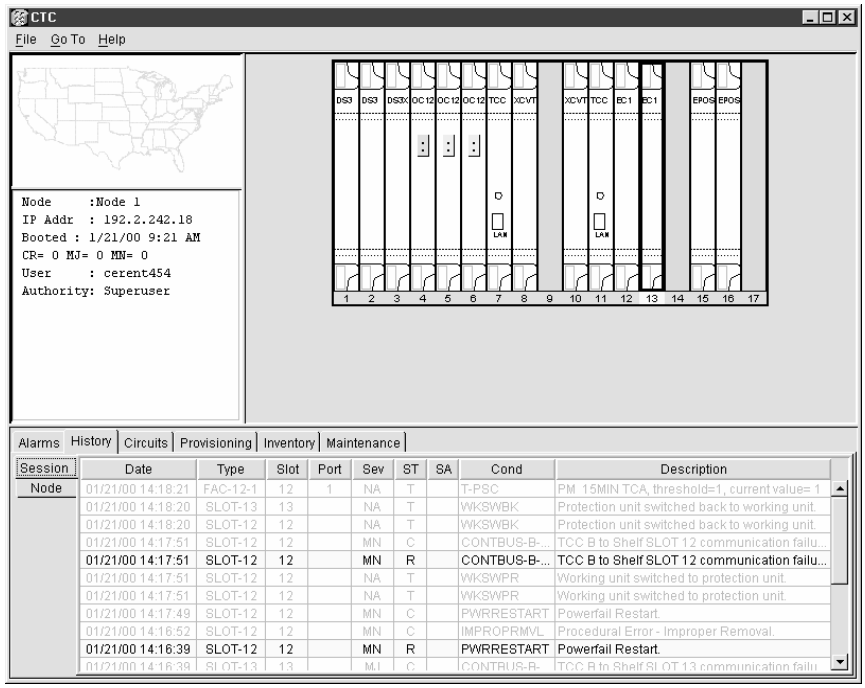
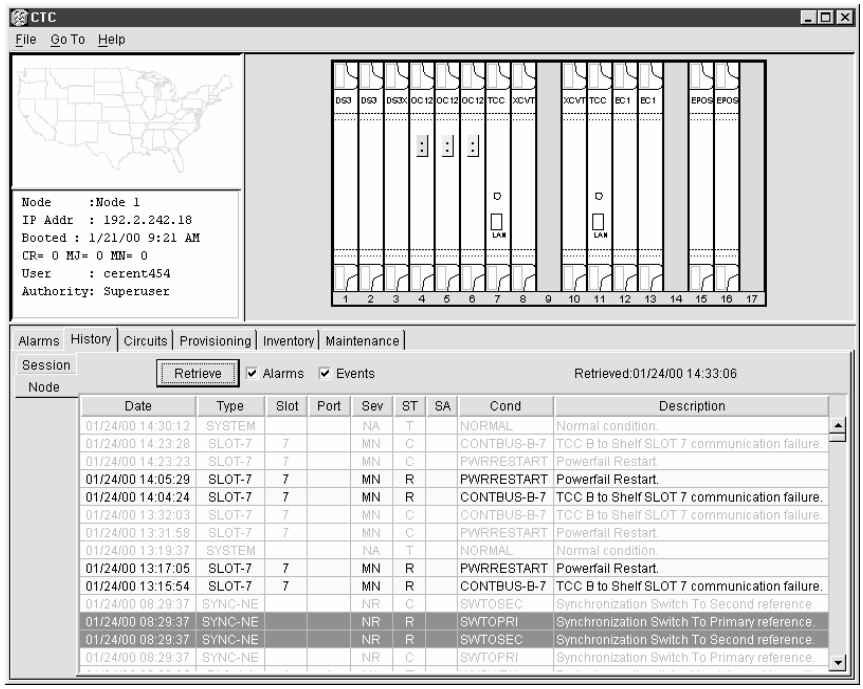


Figure 3-12 History>Node Subtab



3.9.3 Setting Up General Node Information

The first ONS 15454 provisioning task you will perform is setting up basic node information. If the node is to be connected to a LAN or other ONS 15454s, the information that you enter for the node, such as node name and IP address, must be coordinated with your network administrator.

Procedure: Set Up General Node Information

Step 1 Log into the ONS 15454 node.

Step 2 From node view, click the **Provisioning** tab.

Step 3 In the **General** subtab, type the following:

- *Node Name*—type a name for the node.
- *Contact*—type the contact person's name for the node contact and the phone number (optional).
- *Location*—type the node's location (optional).
- *Latitude*—type the node's latitude in the format Nddmmssfff, where d=degrees, m=minutes, s=seconds, and f=fractional seconds.
- *Longitude*—type the node's longitude in the format Wdddmmssfff, where d=degrees, m=minutes, s=seconds, and f=fractional seconds.

CTC uses the latitude and longitude to place node icons on the network view map. To convert longitudes and latitudes given in degrees to degrees, minutes, and seconds, see the "Convert Coordinates to Degrees, Minutes, and Seconds" section on page 3-21.

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

Step 4 Click **Apply**.

CTC uses the longitude and latitude you enter on the General subtab to place node icons on the network view map. You can obtain the longitude and latitude for cities and Zip Codes from the US Census Bureau U.S. Gazetteer website (www.census.gov/cgi-bin/gazetteer). Coordinates are generally provided in degrees. CTC requires that you enter coordinates in degrees, minutes, and seconds. Use the following procedure to convert coordinates.

Procedure: Convert Coordinates to Degrees, Minutes, and Seconds

Step 1 Find the location's longitude and latitude. For example, Petaluma, California is 38.250739 N, 122.615536 W.

Step 2 Use the appropriate directional letter plus the first two digits of latitude and first three digits of longitude with no conversion. For Petaluma, this is N38 (latitude) and W122 (longitude).

Step 3 Using the unconverted longitude and latitude, multiply the number after the decimal by 60 to convert it to minutes. For example, .250739 x 60 is 15.0443, and .615536 x 60 is 36.93216. Use the whole numbers for the minutes (in the example, 15 and 36).

Step 4 Multiply the number after the decimal from Step 3 by 60 to convert it to seconds. In the example, .0443 x 60 is 2.6580, and .93216 x 60 is 55.9296. Use the whole numbers of the total (in the example, 02 and 55) for the seconds. If the whole number for either minutes or seconds is less than ten, add a zero to the left of the number, for example 2 is entered as 02.

Step 5 Use zeros for fractional seconds, because the values are not significant for node positioning on the CTC network view map.

Step 6 Convert the latitude, originally given in degrees, to the format Nddmmssfff, where d=degrees, m=minutes, s=seconds, and f=fractional seconds. In this example, 38.257039 N = N381502000.

Step 7 Convert the longitude, originally given in degrees, to the format Wdddmmssfff. In the example, 122.615536 = W1223655000. Enter zeros if degrees are less than 100, for example, 98 degrees is entered 098.

3.9.4 Setting Up ONS 15454 Network Information

Before you connect an ONS 15454 to other ONS 15454s or to a LAN, you must change the default IP address that is shipped with the ONS 15454 (192.1.0.2). IP addresses are unique identifiers for nodes or hosts connected to a network using TCP/IP. Each address consists of a network number and a host number. The network numbers are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and host information from the IP address.

IP addresses are 32-bit binary numbers. However, to make IP addresses easier to work with, they are represented as four decimal values, each representing eight bits in the range 0 to 255 (known as octets) separated by decimal points. For example, the following IP address is in binary format:

```
10001100.10110011.11011100.11001000
```

The same address, represented as four decimal values, is:

```
140.179.220.200
```

Because the IP addresses that you work with represent binary addresses, changing an address is not always straightforward. Therefore, before you change the ONS 15454 IP addresses, consult your LAN administrator or someone knowledgeable in TCP/IP to ensure addresses are suitable to your network. Additional information about ONS 15454 network management and Ethernet applications is provided in Chapters 7 and 8.

Use the following procedure to set up networking information for the ONS 15454. If the ONS 15454 or the computer used to access the ONS 15454 is linked to a network router, you should create a static route, which can be provisioned using the Static Route fields.

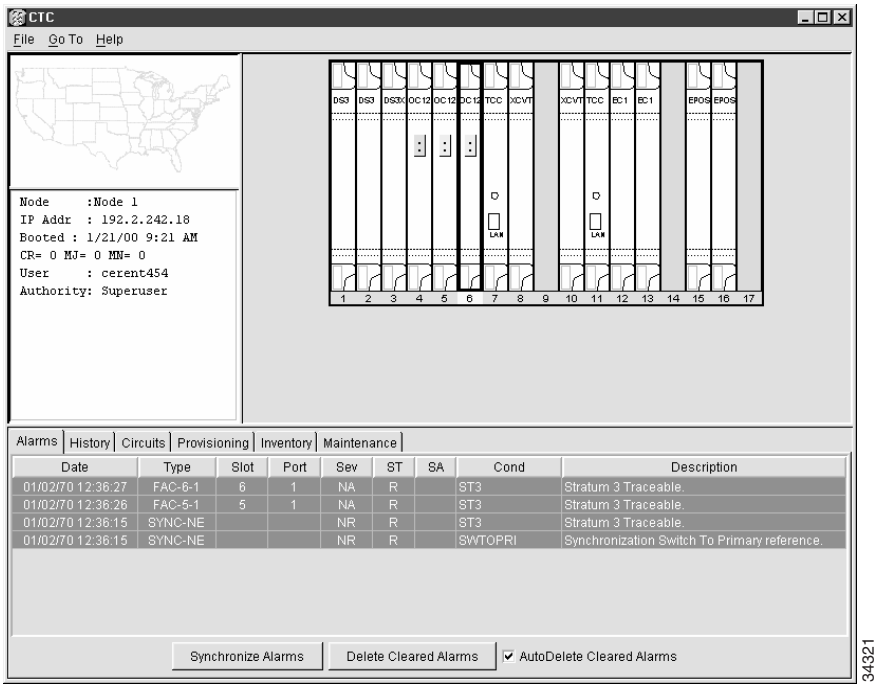
Procedure: Set Up Network Information

Step 1 From the CTC node view, click the **Provisioning** tab.

Step 2 Click the **Network** subtab (Figure 3-13) and complete the following:

- *IP Address*—type the node IP address.
- *Prevent LCD IP Config*—if checked, prevents the ONS 15454 IP address from being changed using the LCD. See the "IP Address Entry Using Front Panel LCD" section on page 8-10.
- *Default Router*—if the ONS 15454 must communicate with a device that has an IP address that the ONS 15454 is not routed to, it forwards the packets to the default router. Type the address of the router in this field. If the ONS 15454 is not connected to a LAN, leave this field blank.
- *Subnet Mask Length*—type the subnet mask length (decimal number representing the subnet mask length in bits), or click the arrows, to adjust the subnet mask length.
- *MAC Address* (read only)—displays the ONS 15454 address as it is identified on the Media Access Control layer.
- *Static Routes*—static routes permit multiple CTC sessions with different destination IP addresses on the same subnet. For static route provisioning procedures, see the "Static Route Provisioning" section on page 8-30.

Figure 3-13 Provisioning>Network Subtab



Step 3 Click **Apply**.

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

The TCCs will reboot, one at a time.

3.9.5 Setting Up ONS 15454 Security

The ONS 15454 has four security levels that limit the functions users can perform: Retrieve, Maintenance, Provisioning, and Superuser. A Retrieve user can retrieve and view CTC information but cannot set or modify parameters. A Maintenance user can access only Maintenance options. A Provisioning user can access only Provisioning and Maintenance options. A Superuser, usually the network element administrator, can perform all of the functions of the other security levels as well as set names, passwords, and security levels for other users. A list of CTC actions that can be performed at each security level is shown in Table 3-10.

Table 3-10 ONS 15454 Security Levels

CTC Tab	Subtab	Actions	Retrieve	Maintenance	Provisioning	Superuser
Alarms	n/a	Delete cleared alarms	X	X	X	X
History	Session	Read only				
	Node	Retrieve	X	X	X	X
Circuits	n/a	Create/Delete/Edit/ VLAN			X	X
		Map	X	X	X	X
Provisioning	General	All				X
	EtherBridge	All			X	X
	Sonet DCC	All				X
	Timing	All			X	X
	SNMP	Create/Delete/Edit				X
		Browse traps	X	X	X	X
	Security	Create/Delete				X
		Change password	same user	same user	same user	X
	Ring	All (BLSR)			X	X
	Protection	Create/Delete/Edit			X	X
		Browse groups	X	X	X	X
	Network	Modify mask/IP/Route				X
Inventory	n/a	Delete			X	X
		Reset		X	X	X
Maintenance	Database	Backup/Restore				X
	EtherBridge	Read only				
	Protection	Operation on protection groups		X	X	X
	Ring	BLSR maintenance		X	X	X
	Software	Upgrade/Activate/ Revert				X
	XC Cards	Protection switches		X	X	X
	Diagnostic	Retrieve				X
	Timing	Read-only				
	Audit	Retrieve	X	X	X	X

Note In order for users to access multiple nodes, the same user name and password must exist on each node.

Security levels also limit the amount of time a user can leave the system idle before the CTC window is locked to prevent unauthorized users from making changes. Higher security levels have shorter idle times. Table 3-11 shows CTC security levels and their idle times.

Table 3-11 ONS 15454 Security Idle Times

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

Procedure: Create New Users

Step 1 From the CTC window, click the **Provisioning** tab.

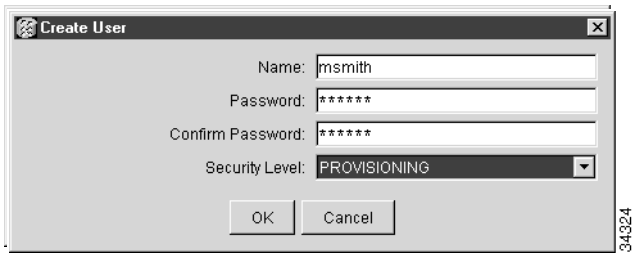
Step 2 Click the **Security** subtab.

Step 3 On the Security pane, click **Create**.

Step 4 In the Create User dialog (Figure 3-14), enter the following:

- *Name*— type the user name.
- *Password*—type the user password. The password must contain at least six characters and can be any letter or number (a-z, A-Z, 0-9).
- *Confirm Password*—type the password again to confirm it.
- *Security Level*—select the user's security level.

Figure 3-14 Create User Dialog



Step 5 Click **OK**.

Note CTC users must be added to each node where they need access. Users are not automatically added to other network nodes.

Procedure: Edit User Security

Step 1 From the CTC window, click the **Provisioning** tab.

Step 2 Click the **Security** subtab.

Step 3 On the Security pane, click the user you want to edit.

Step 4 On the right portion of the Security pane, enter new security information for the user: 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 password.)

Step 5 Click **Apply**.

Note Changing user permissions and access levels does not take effect while the user is logged into CTC. The changes take effect the next time the user logs into CTC. If the user has access to more than one node, you must change the user settings at each node.

3.9.6 Creating Protection Groups

The ONS 15454 provides several card protection methods. When you set up protection for ONS 15454 cards, you must choose between maximum protection and maximum card slot availability. The highest protection reduces the number of available card slots; the highest card slot availability reduces the protection. Table 3-12 shows the protection types that can be set up for ONS 15454 cards.

Table 3-12 Protection Types

Type	Cards	Description
1:1	Any electrical	Pairs one working card with one protect card. Protect cards must be placed in an odd-numbered slot and the working card must be placed in an even-numbered slot that follows the protect slot, for example, protect in Slot 1, working in Slot 2 and protect in Slot 3, working in Slot 4.
1:N	DS-1 and DS-3 cards	Assigns one protect card for several working cards. The maximum is 1:5. Protect cards (DS1N-14, DS3N-12) must be installed in Slots 3 or 15 and the cards they protect must be on the same side of the shelf. Protect cards must match the cards they protect. For example, a DS1N-14 can only protect DS1-14 or DS1N-14 cards. If a failure occurs, traffic reverts back when the working card comes back online after the time indicated in the reversion has elapsed.
1+1	Any optical	Pairs an 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.
Unprotected 0:1	Any	Unprotected cards may 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 xxx available for use on the ONS 15454. Unprotected is the default protection type.

Procedure: Create Protection Groups

Step 1 From the CTC window, click the **Provisioning** tab.

Step 2 Click the **Protection** subtab.

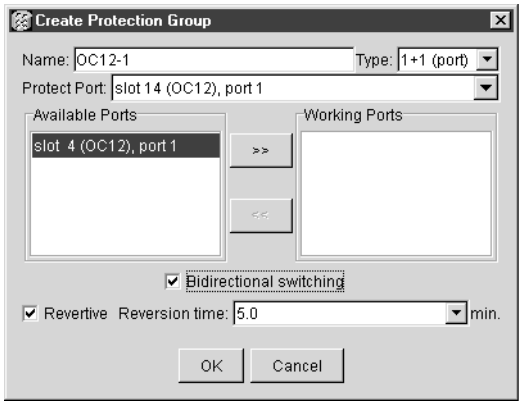
Step 3 Under Protection Groups, click **Create**.

Step 4 In the Create Protection Group dialog (Figure 3-15), enter the following:

- *Name*—type a name for the protection group, up to 32 alpha-numeric characters.
- *Type*—choose the protection type: 1:1, 1:N, or 1+1. The protection selected determines the cards that are available to serve as protect and working cards. For example, if you choose 1:N protection, only DS-1N and DS-3N cards are displayed.
- *Protect Card or Port*—choose the protect card (if using 1:1 or 1:N) or protect port (if using 1+1) from the list.

Based on these selections, a list of available working cards or ports is displayed under Available Cards or Available Ports.

Figure 3-15 Create Protection Group Dialog (1+1)



Step 5 From the Available Cards or Available Ports list, choose the card or port that you want to be the working card or port (the card(s) or port(s) that will be protected by the card or port selected in Protect Cards or Protect Ports). Select the top arrow button to move them to the Working Cards or Working Ports list.

Step 6 Complete the remaining fields:

- *Bidirectional switching*—(optical cards only) click if you want both transmit and receive channels to switch if a failure occurs to one.
- *Revertive*—if checked, the ONS 15454 reverts back to the working card or port after failure conditions are corrected.
- *Reversion time*—if *Revertive* is checked, enter the amount of time following failure condition correction that the ONS 15454 should switch back to the working card or port.

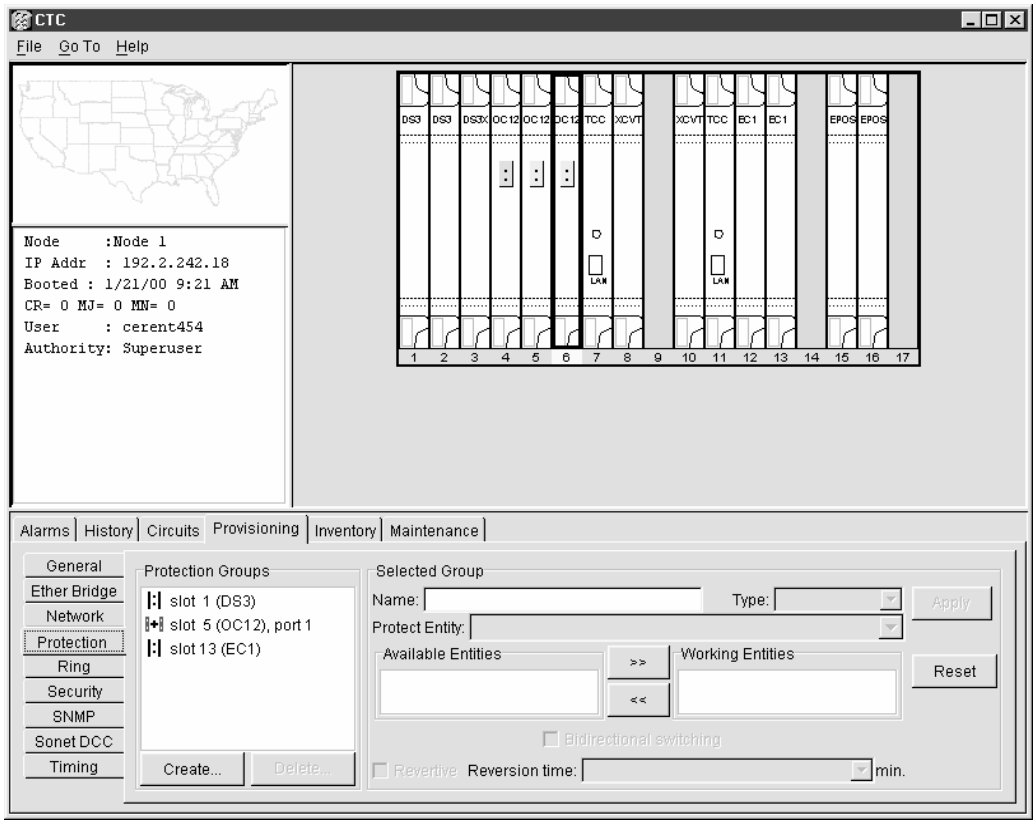
Step 7 Click **OK.**

Procedure: Edit Protection Groups

Step 1 From the CTC window, click the **Provisioning** tab.

Step 2 Click the **Protection** subtab (Figure 3-16).

Figure 3-16 Provisioning>Protection Subtab



Step 3 Under Protection Groups, choose a protection group.

Step 4 Under Selected Group, edit the fields as appropriate. (For field descriptions, see the "Create Protection Groups" section on page 3-27.)

Step 5 Click **Apply**.

Procedure: Delete Protection Groups

Step 1 Log in to CTC.

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

(a) Click the **Maintenance>Protection** tabs.

(b) Under Protection Groups, choose the group you want to delete.

(c) Under Selected Group, verify that the protect card is in standby mode. If it is in standby mode, continue with Step 3. If it is active, manually switch traffic back to the working card. Verify that the protect card is in standby mode, then 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 CTC window, click the **Provisioning>Protection** tabs.

Step 4 Under Protection Groups, click a protection group.

Step 5 Click **Delete**.

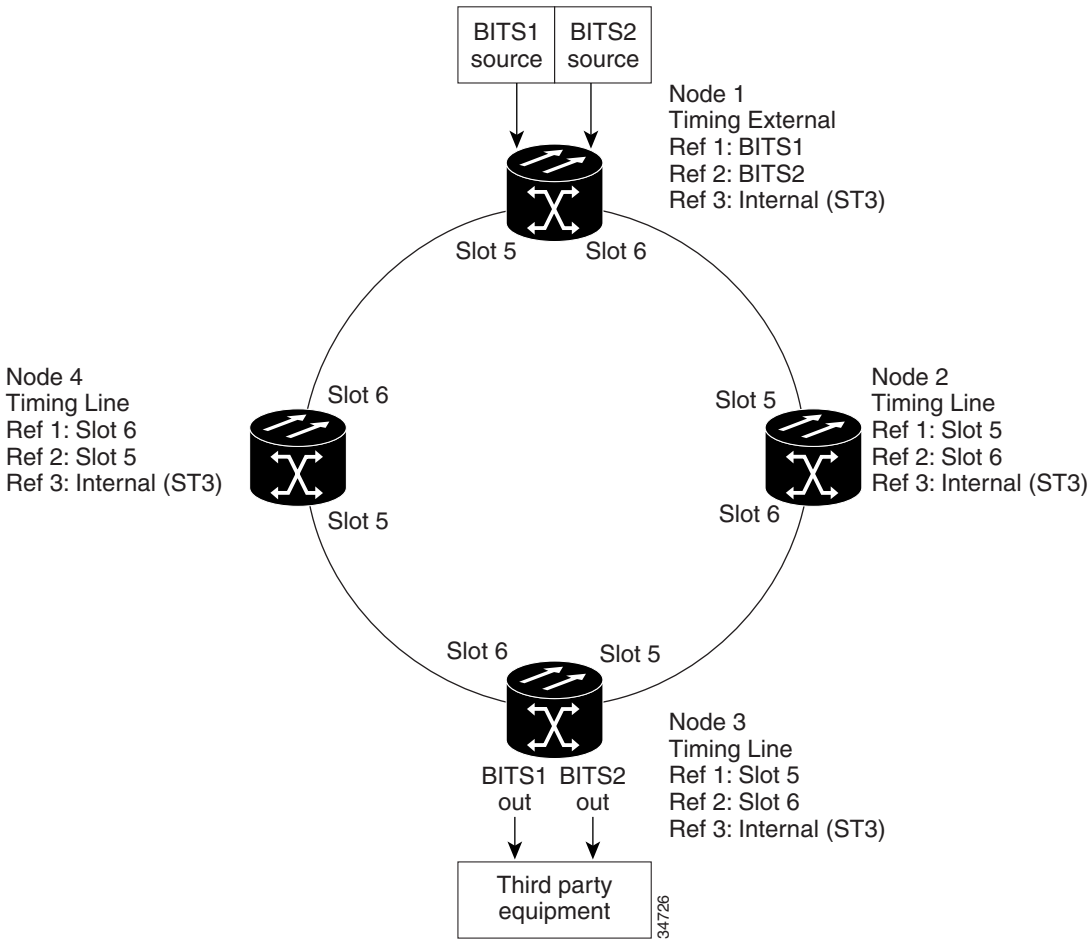
3.9.7 Setting Up ONS 15454 Timing

You must set the SONET timing parameters for each ONS 15454. ONS 15454 timing is set to one of two modes: external or line. In typical ONS 15454 networks, at least one node is set to external and the other nodes are set to line. The external node derives its timing from a Building Integrated Timing Supply (BITS) source wired to the BITS backplane pins. (Figure 1-20 shows a diagram of the BITS pin location.) The BITS source, in turn, derives its timing from a Primary Reference Source (PRS) such as a Stratum 1 clock or GPS signal. The line nodes derive timing from Optical Carrier cards.

For protection, up to three timing references can be identified. These are typically two BITS-level or line-level sources and an internal reference. The internal reference is the Stratum 3 (ST3) clock provided on every ONS 15454 TCC card.

Figure 3-17 shows an ONS 15454 network timing setup example. Node 1 is set to external timing. Two references are set to BITS. These are Stratum 1 timing sources wired to the node's BITS input pins on the ONS 15454 backplane. Its third reference is set to internal. The BITS output pins on the backplane of Node 3 are used to provide timing to outside equipment, such as a Digital Access Line Access Multiplexer.

Figure 3-17 ONS 15454 Timing Example



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

SSM messages are either Generation 1 or Generation 2. Generation 1 is the first and most widely deployed SSM message set. Generation 2 is a newer version. If you enable SSM for the ONS 15454, consult your timing reference documentation to determine which message set to use. Table 3-13 and Table 3-14 show the Generation 1 and Generation 2 message sets.

Table 3-13 SSM Generation 1 Message Set

Message	Quality	Description
PRS	1	Primary reference source - Stratum 1
STU	2	Sync traceability unknown
ST2	3	Stratum 2
ST3	4	Stratum 3
SMC	5	SONET minimum clock
ST4	6	Stratum 4
DUS	7	Do not use for timing synchronization

Table 3-13 SSM Generation 1 Message Set (continued)

Message	Quality	Description
RES		Reserved; quality level set by user

Table 3-14 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: Setup ONS 15454 Timing

Step 1 Log into the node and click the **Provisioning** tab.

Step 2 Click the **Timing** subtab (Figure 3-18) and complete the following:

- *Timing Mode*—set to External if timing is derived from an external BITS source wired to the backplane pins; set to Line if timing is derived from an Optical Carrier card.
- *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, a ST3E message becomes a ST3.
- *Quality of RES*—if your timing source supports the reserve 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 3-13 and Table 3-14 for more information.
- *Revertive*—if checked, the ONS 15454 reverts back to a primary reference source after the conditions that caused it to switch to a secondary timing reference are corrected.
- *Revertive Time*—If *Revertive* is checked, indicate the amount of time the ONS 15454 will wait before reverting back to its primary timing source.

The BITS Facilities section sets the parameters used by your BITS1 and BITS2 timing references. Many of these settings are determined by the timing source manufacturer.

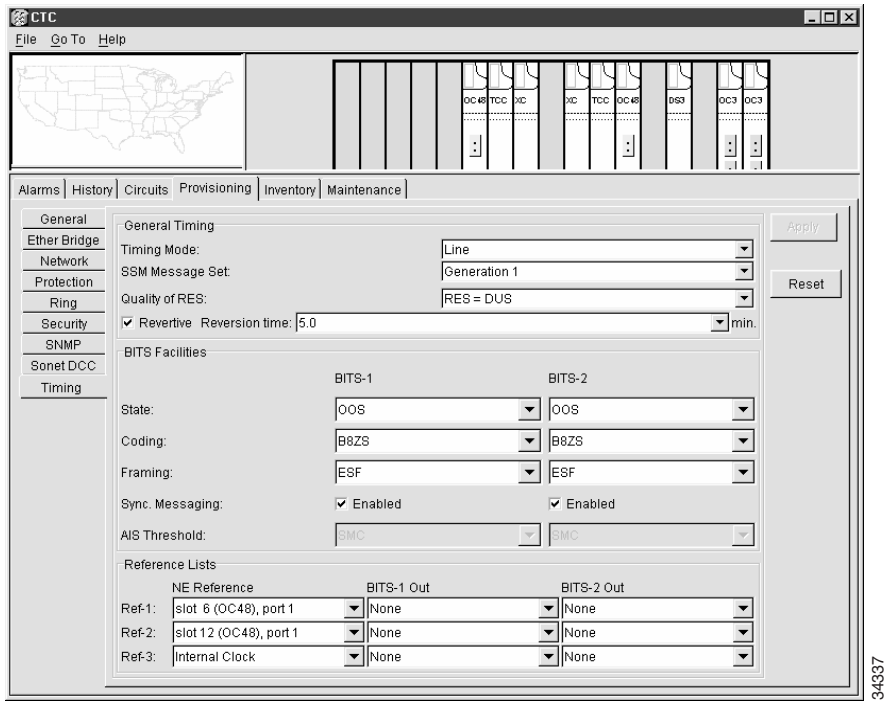
- *State*—set the BITS reference to IS (In Service) or OOS (Out of Service). For nodes set to Line timing, set *State* to OOS; for nodes using external timing, or nodes using the external BITS out, set *State* to IS.
- *Coding*—set to the coding used by your BITS reference, either B8ZS or AMI.

- *Framing*—set to the framing used by your BITS reference, either ESF (Extended Super Frame, or SF (D4)(Super Frame). Synchronization Status Messaging is not available with Super Frame.
- *Sync Messaging*—check to enable Synchronization Status Messaging.
- *AIS Threshold*—sets the quality level where a node sends an AIS from the BITS 1 Out and BITS 2 Out backplane pins. When a node times at or below the *AIS Threshold* quality, AIS is sent (used when SSM is disabled or frame is SF).

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

- *NE Reference*—defines up to three network element (the current node) references (Ref 1, Ref 2, Ref3). The options displayed depend on the node's timing mode. If the timing mode is External, the options are BITS1, BITS2, and Internal. If the timing mode is Line, the node's working optical cards are displayed. In this case, select optical ports on cards that are directly or indirectly connected to a BITS timed source, that is, the node's trunk cards.
- *BITS 1 Out/BITS 2 Out*—define the timing references for equipment wired to the BITS Out backplane pins. Normally, BITS Out is used with Line nodes, so the options displayed are the working optical cards.

Figure 3-18 Provisioning>Timing Subtab

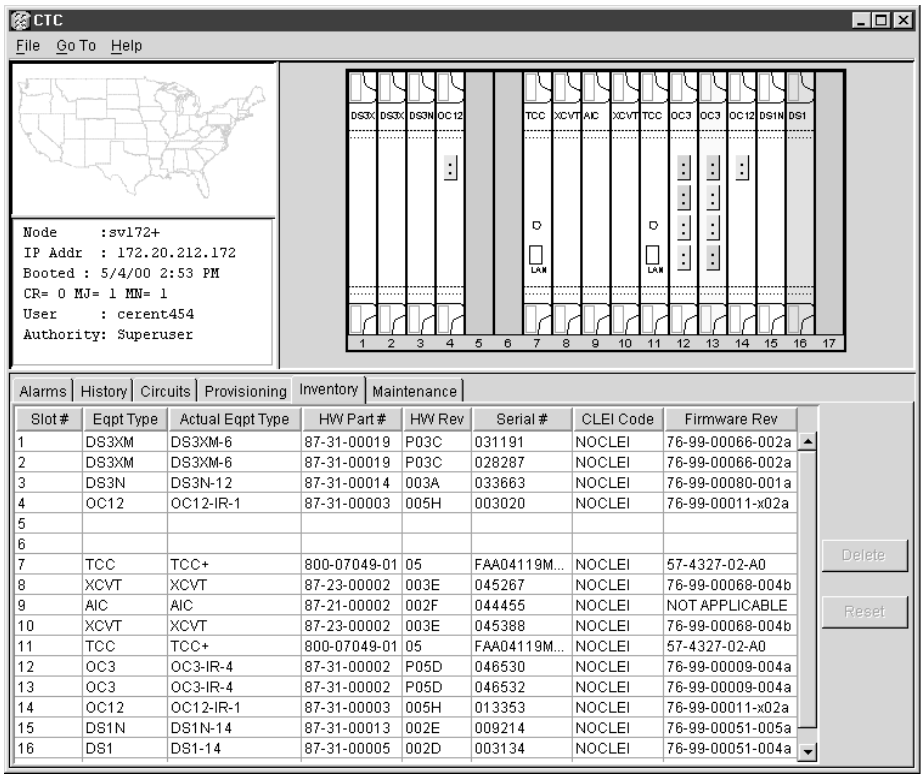


Step 3 Click **Apply**.

3.10 Viewing ONS 15454 Inventory

The Inventory tab (Figure 3-19) displays information about cards installed in the ONS 15454 node including part numbers, serial numbers, hardware revisions, and equipment types. The tab provides a central location to obtain information and to determine applicability of ONS 15454 Product Change Notices (PCNs) and Field Service Bulletins (FSBs). Using the ONS 15454 export feature, you can export inventory data from ONS 15454 nodes into spreadsheet and database programs, where information can be consolidated for network inventory management and reporting.

Figure 3-19 Inventory Tab



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

- *Slot #*—the slot where the card is installed.
- *Eqpt Type*—equipment type the slot is provisioned for, for example, OC-12 or DS-1.
- *Actual Eqpt Type*—the actual card that is installed in the slot, for example, OC12 IR 4 1310 or DS1N-14.

Note While an ONS 15454 slot is provisioned by the card that is installed in the slot, 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

3.11 Printing and Exporting CTC Data

You can print CTC windows and you can print CTC data that is displayed in columns, such as alarms and inventory. You can also export CTC table data in formats that can be used use by other applications such as spreadsheets, word processors, and database management applications. Table 3-15 shows CTC data that can be exported.

Table 3-15 CTC Table Data

View	Tab	Subtab
Node	Alarms	
	History	Node/Session
	Provisioning	Ether Bridge
		Network (Static Routes)
	Maintenance	Ether Bridge
	Inventory	
Network	Alarms	
	History	
	Circuits	
OC Cards	Alarms	
	Circuits	
	Provisioning	Line/Threshold/STS
	Maintenance	
	Performance	
DS Cards	Alarms	
	Circuits	
	Provisioning	Line
AIC Card	Alarms	
	Circuits	
	Maintenance	
EC1-12	Alarms	
	Circuits	
	Provisioning	Line/Threshold/STS
	Maintenance	
	Performance	
DS3XM-6	Alarms	
	Circuits	
	Provisioning	Line
	Maintenance	DS-1/DS-3/Performance

Procedure: Print CTC Data

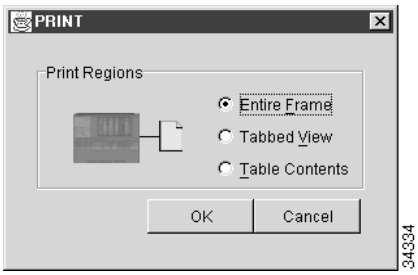
Use the following procedure to print CTC screens and data. Before you start, make sure your PC is connected to a printer.

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

Step 2 In the Print dialog (Figure 3-20) 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 Table 3-15)

Figure 3-20 CTC Print Dialog



Step 3 Click **OK**.

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

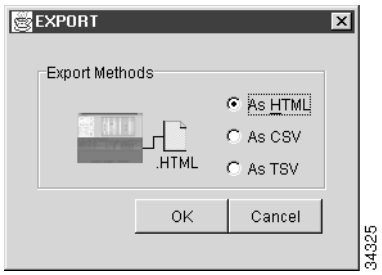
Procedure: Export CTC Data

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

Step 2 In the Export dialog (Figure 3-21) choose an option:

- *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 3-21 CTC Export Dialog



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**.

3.12 Displaying CTC Data in Other Applications

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

You can display CTC data exported as comma separated values (CSV) or tab separated values (TSV) 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.

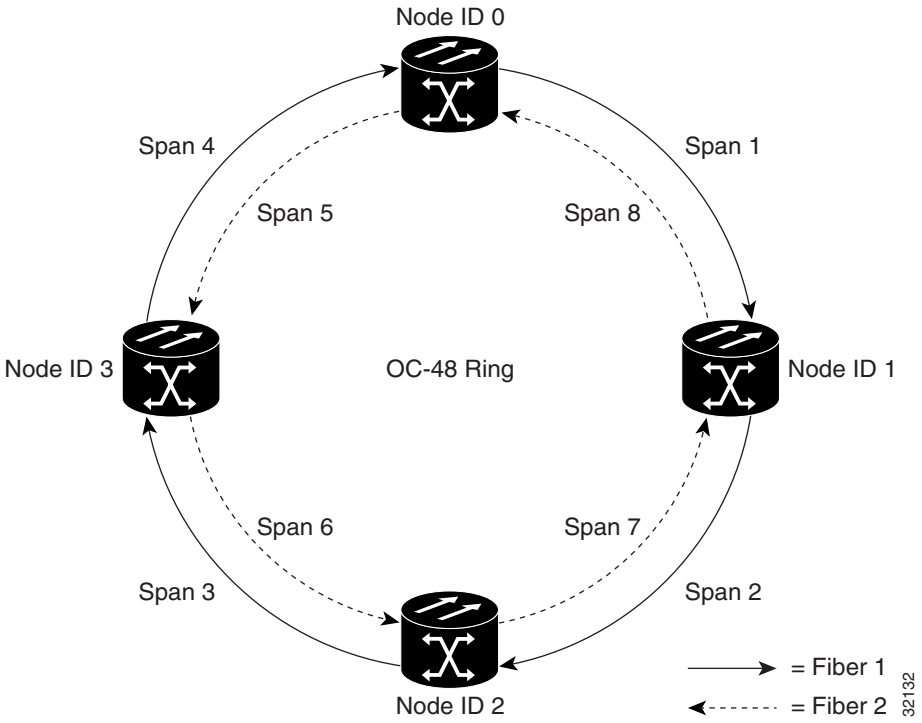
Configuring Networks

This chapter provides procedures for configuring ONS 15454 rings and circuits including Bidirectional Line Switched Rings (BLSRs), Unidirectional Path Switched Rings (UPSRs), linear add-drop multiplexers (ADMs), circuits, Data Communication Channel (DCC) tunnels, and loopbacks.

4.1 Bidirectional Line Switched Rings

The ONS 15454 supports two-fiber BLSRs with up to 16 ONS 15454 nodes. BLSRs allocate half the available fiber bandwidth for protection. In an OC-48 BLSR, for example, STSs 1–24 are allocated to working traffic, and STSs 25–48 are allocated for protection. If a break occurs on one fiber, working traffic switches to the protection bandwidth (STSs 25–48) on the other fiber. Working traffic travels in one direction on STSs 1–24 on one fiber, and on STSs 1–24 in the opposite direction on the second fiber. Because the working and protection bandwidths must be equal, you can create only OC-12 and OC-48 BLSRs. Figure 4-1 shows a two-fiber OC-48 BLSR.

Figure 4-1 Four-Node, Two-Fiber OC-48 BLSR



SONET sends BLSR protection information over the K1 and K2 overhead bytes. The K bytes communicate failure conditions and actions taken between different nodes in the ring. Receiving nodes monitor the K bytes to determine when to switch the SONET signal to an alternate physical path. BLSRs are limited to a maximum of 16 nodes due to K byte node addressing requirements.

BLSR rings work well for distributed "mesh" and node-to-node traffic applications, such as interoffice networks and access networks. A BLSR node can terminate traffic fed from either side of the ring. Protection is provided by BLSR "standby bandwidth." Table 4-1 shows the bidirectional bandwidth capacities of two-fiber BLSRs.

Table 4-1 Two-Fiber BLSR Capacity

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

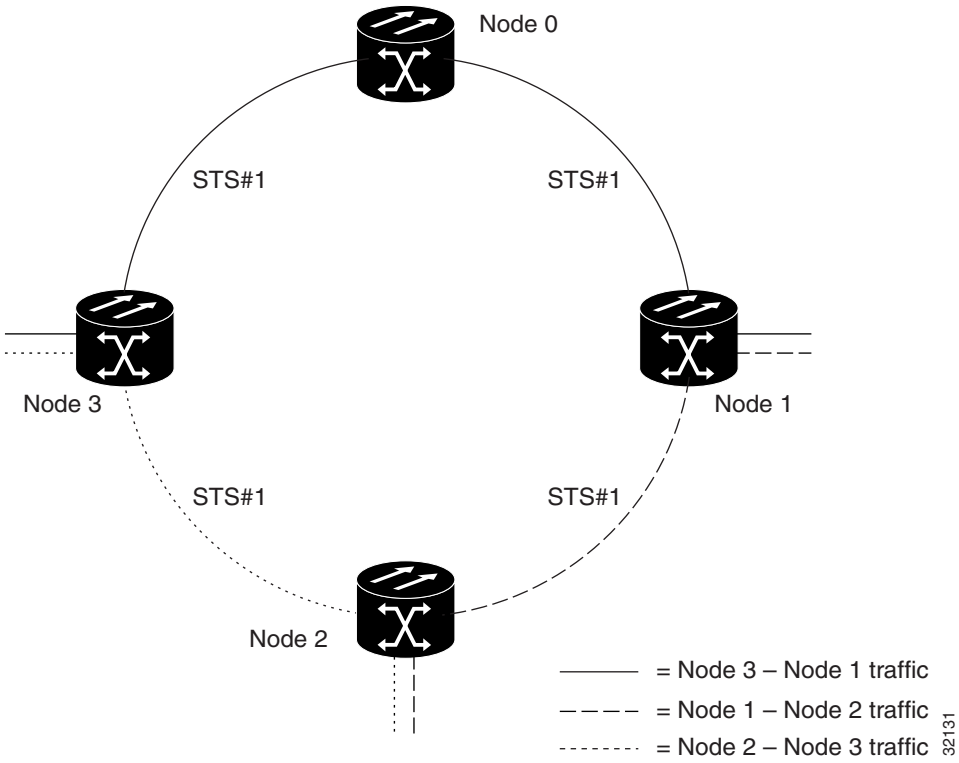
* N equals the number of ONS 15454 nodes configured as BLSR nodes.

† PT equals the number of STS-1 circuits passed through an ONS 15454 node (capacity can vary depending on the traffic pattern).

In BLSRs, bandwidth can be reused around the ring. The ONS 15454 can carry more traffic in networks with a distributed traffic pattern than a network with traffic flowing through one central hub. With a distributed traffic pattern, a BLSR can carry more traffic than a UPSR operating at the same optical rate.

Figure 4-2 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 4-2 BLSR Bandwidth Reuse



4.1.1 Sample BLSR Application

Figure 4-3 shows a sample BLSR implementation. A regional long-distance network connects to other carriers at Node 0. Traffic is delivered to the service provider's major hubs.

- Carrier 1 delivers six DS-3s over two OC-3 spans to Node 0. Carrier 2 provides twelve DS-3s directly. Node 0 receives the signals and delivers them around the ring to the appropriate node.
- The ring also brings 14 DS-1s back from each remote site to Node 0. Intermediate nodes serve these shorter regional connections.
- The ONS 15454 OC-3 module supports a total of four OC-3 ports, so that two additional OC-3 spans can be added at little cost.

Figure 4-3 Sample BLSR Application

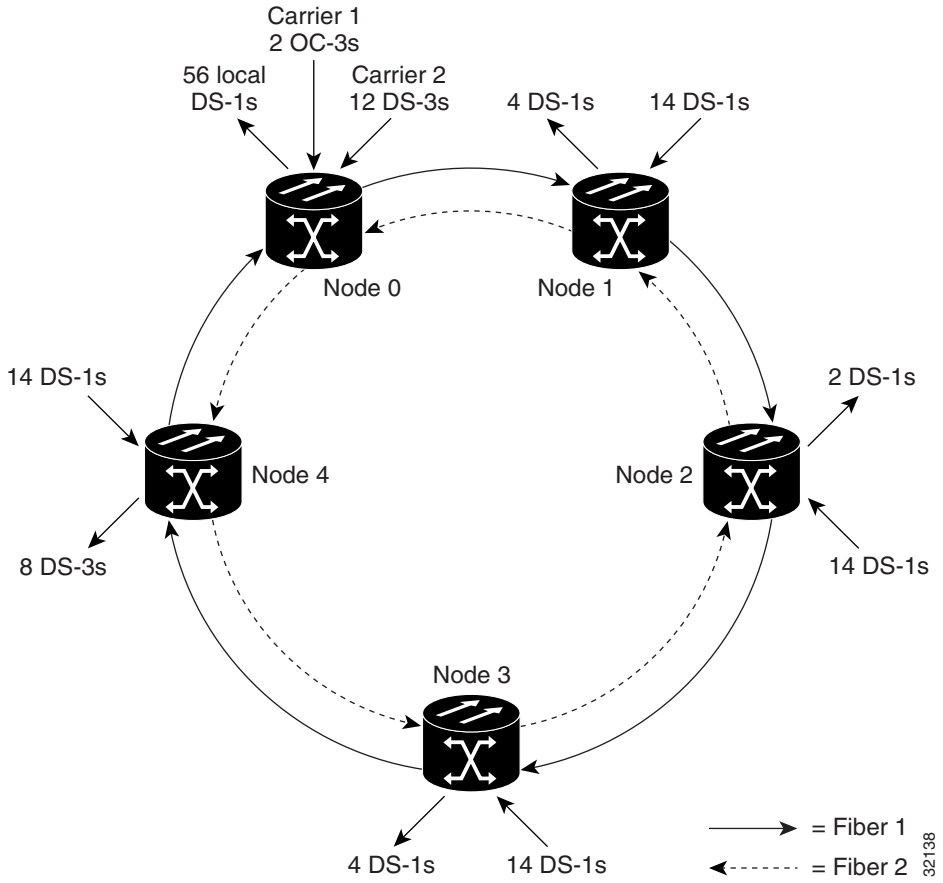


Figure 4-4 shows the shelf layout for Node 0, which has one free slot. Figure 4-5 shows the shelf layout for the remaining sites in the ring. In this BLSR configuration, an additional eight DS-3s at Node IDs 1 and 3 can be activated. An additional four DS-3s can be added at Node ID 4, and ten DS-3s can be added at Node ID 2. Each site has free slots for future traffic needs.

Figure 4-4 Sample Shelf Layout for Node 0 in Figure 4-3

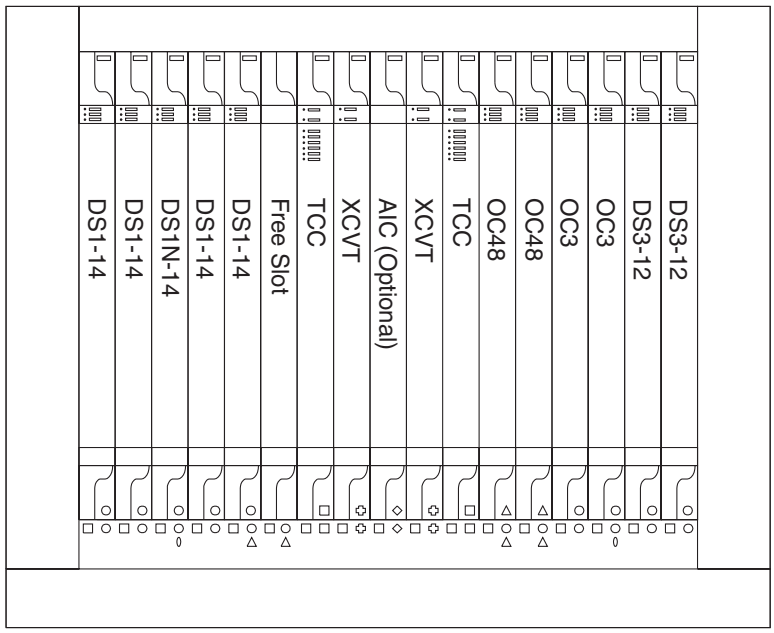
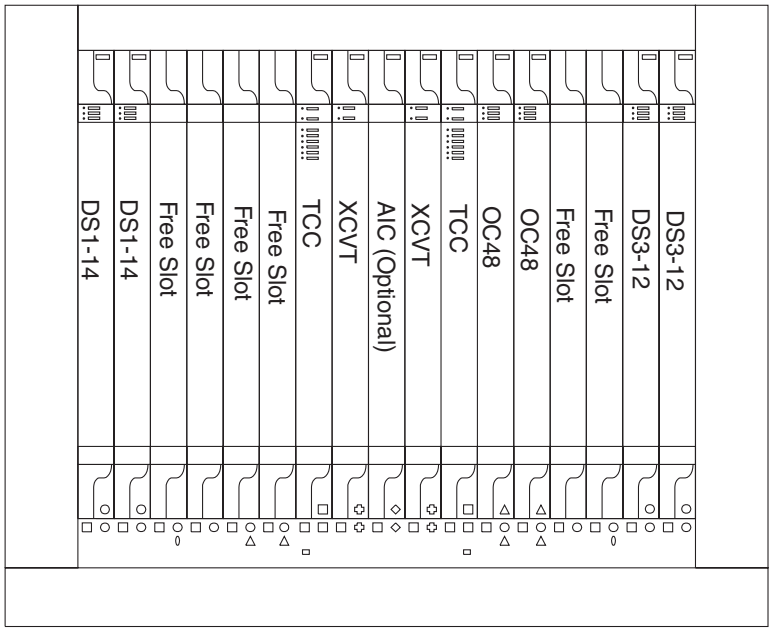


Figure 4-5 Sample Shelf Layout for Nodes 1-4 in Figure 4-3



4.1.2 Setting Up BLSRs

To set up a BLSR, you perform five basic procedures:

- Install the Optical Carrier cards and attach the fibers
- Create the BLSR DCC terminations
- Enable the BLSR ports
- Set up BLSR timing
- Configure the BLSR ring

The BLSR setup procedures in this section are for a two-fiber, two-node BLSR. However, you can apply the same setup principles to larger rings.

Procedure: Install the Optical Carrier Cards

Step 1 Use the procedures in the "Card Installation and Turn-Up" section on page 1-35 to install the OC-12 or OC-48 cards.

You can install the OC-12 cards in any slot, but the OC-48 cards can only be installed in Slots 5, 6, 12, or 13. Figure 4-6 shows a sample OC-48 BLSR. Figure 4-7 shows a sample card installation for a two-node, OC-48 BLSR.

Figure 4-6 Two Node OC-48 BLSR

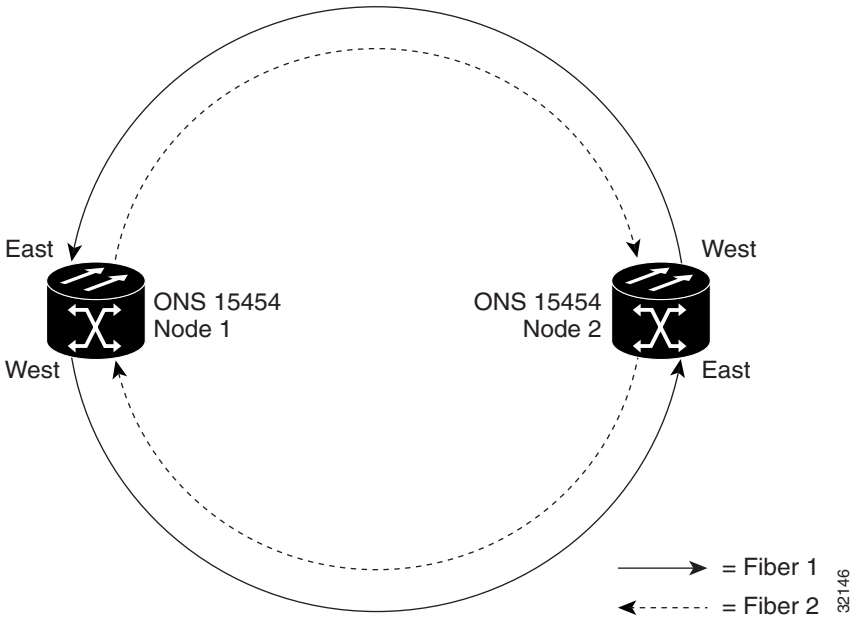
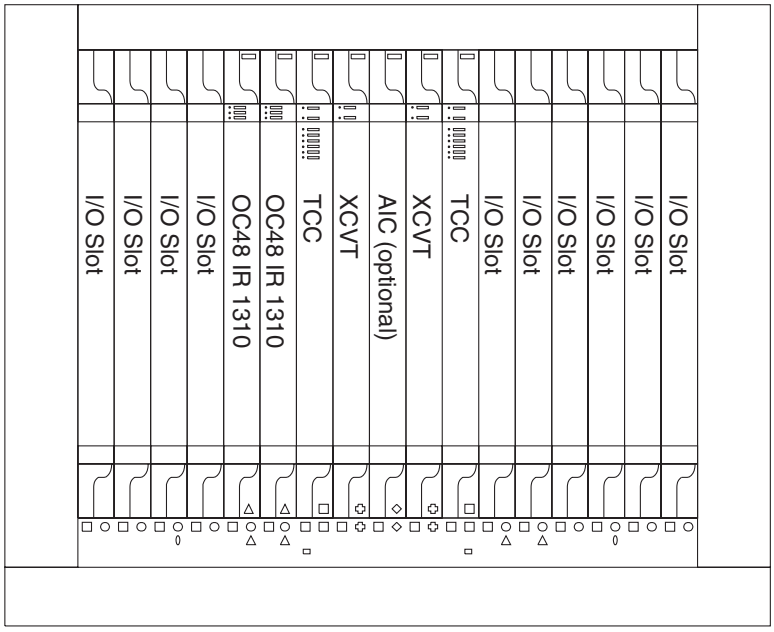


Figure 4-7 Sample Shelf Setup for Two Node BLSR



Step 2 Allow the cards to boot.

Step 3 Attach the fiber to the cards. When the ACT LED on the card you installed turns green, use the steps in the following procedure to configure the 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 Under SDCC Terminations, click **Create**.

Step 4 On the Create SDCC Terminations dialog, press Control and click the two slots/ports that will serve as the BLSR ring ports at the node. For example, Slot 6 (OC-48)/Port 1 and Slot 12 (OC-48)/ Port 1.

Note The ONS 15454 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs; therefore, the Line DCCs are available to tunnel DCCs from third-party equipment across ONS 15454 networks. For more detail, see the "Provision a DCC Tunnel" section on page 4-48.

Step 5 Click **OK.**

The slots/ports display under SDCC Terminations.

Step 6 Complete Steps 2 – 5 at each node that will be in the BLSR.

Procedure: Enable the Optical Card Ports

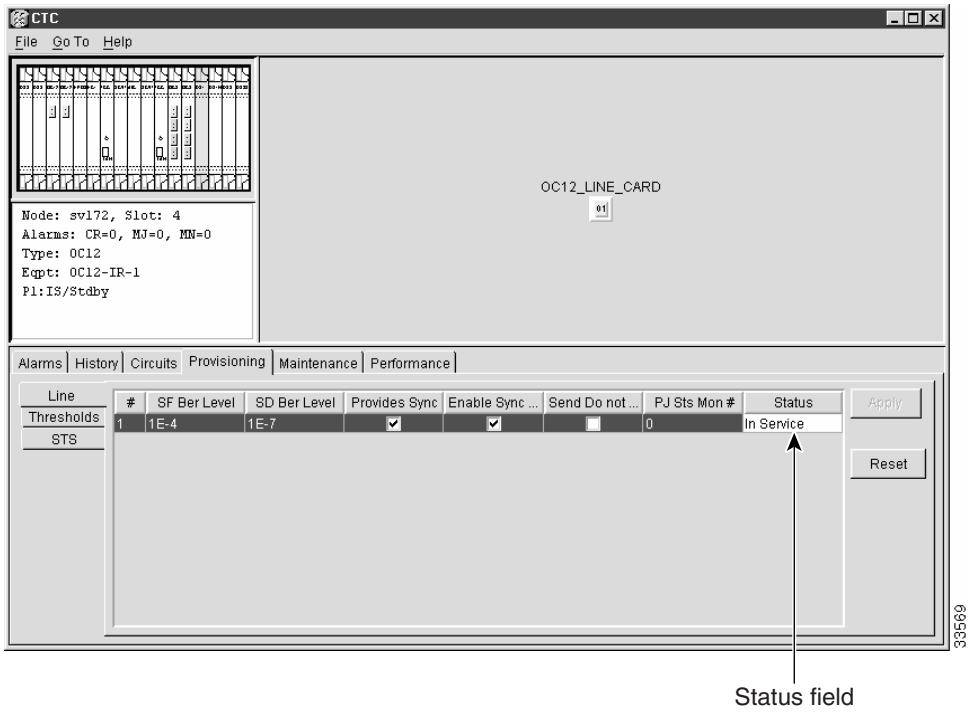
Step 1 Open one of the nodes that will be in the BLSR.

Step 2 Double click one of the optical cards that you configured as an SDCC termination.

Step 3 Click the **Provisioning>Line** tabs.

Step 4 Click **Status** (Figure 4-8) and choose In Service.

Figure 4-8 Line Subtab



Step 5 Repeat Steps 2 – 4 for the other optical card configured as a SDCC termination.

Step 6 Repeat Steps 2 – 5 for each node that will be in the BLSR.

After configuring the SONET DCC, you set the timing for the node. For procedures, see the "Setup ONS 15454 Timing" section on page 3-31. For general information about ONS 15454 timing, including Synchronization Status Messaging, see the "Setting Up ONS 15454 Timing" section on page 3-29. After you configure the BLSR timing you can enable the BLSR ports, which is described in the following procedure.

Procedure: Configure the BLSR

Step 1 Log into one BLSR node.

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

Step 3 On the **Ring** subtab under BLSR, assign a Node ID in the *NODE ID* field.

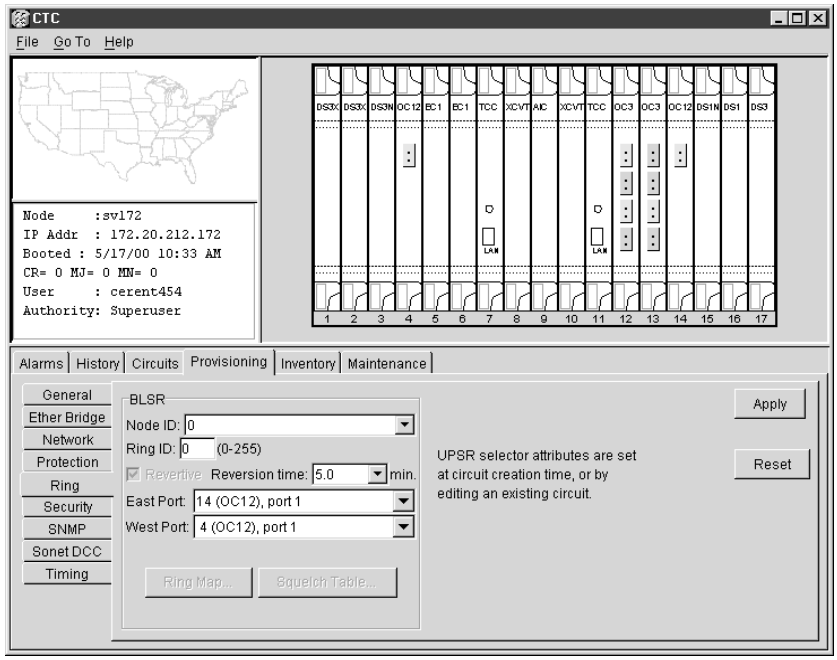
The Node ID identifies the node to the BLSR. Nodes in your BLSR must have different Node IDs. After you select a Node ID, the other BLSR fields are displayed.

Step 4 Set the BLSR properties:

- *Ring ID*—assign a ring ID (a number between 0 and 255). You must use the same Ring ID for all nodes in the same BLSR.
- *Reversion time*—set the amount of time after which the working traffic will revert back to the original working path. The default is 5 minutes.
- *East Port*—assign the east port from the pull-down menu.
- *West Port*—assign the west port from the pull-down menu.

The east and west ports must be ports where you created SDCC terminations in the "Create the BLSR DCC Terminations" section on page 4-7. The fiber of the east port must plug into the fiber of the west port on an adjacent node, and the fiber of the east port must plug into the port of a west port. To avoid errors, use a system to assign BLSR ports. A common practice is to make the east port the furthest slot to the right and the west port the farthest left. For example, if you use Slots 4 and 14, Slot 14 is the east port and Slot 4 is the west port. Figure 4-9 shows the Ring subtab with the east and west ports selected.

Figure 4-9 Ring Subtab



Step 5 Click **Apply**.

Step 6 When the BLSR Map Ring Change dialog displays, click **Yes**.

Step 7 On the BLSR Ring Map dialog, click **Accept**.

The node is added to the BLSR ring map. However, Default K alarms will display until all nodes in the ring are configured.

Step 8 Complete Steps 2 – 7 at each node that you are adding to the BLSR.

Step 9 When all nodes are added to the BLSR, switch to network view to verify that span lines appear between all BLSR nodes and that the Default K alarms are cleared.

Step 10 Test the BLSR using testing procedures normal for your site. Here are a few steps you can use:

(a) Log into a node, click the **Maintenance>Ring** tabs, and choose **MANUAL RING** from East Operation. Click **Apply**. Verify that traffic switches normally.

(b) Choose **Clear** from East Operation and click **Apply**.

(c) Repeat Steps a and b for West Operation.

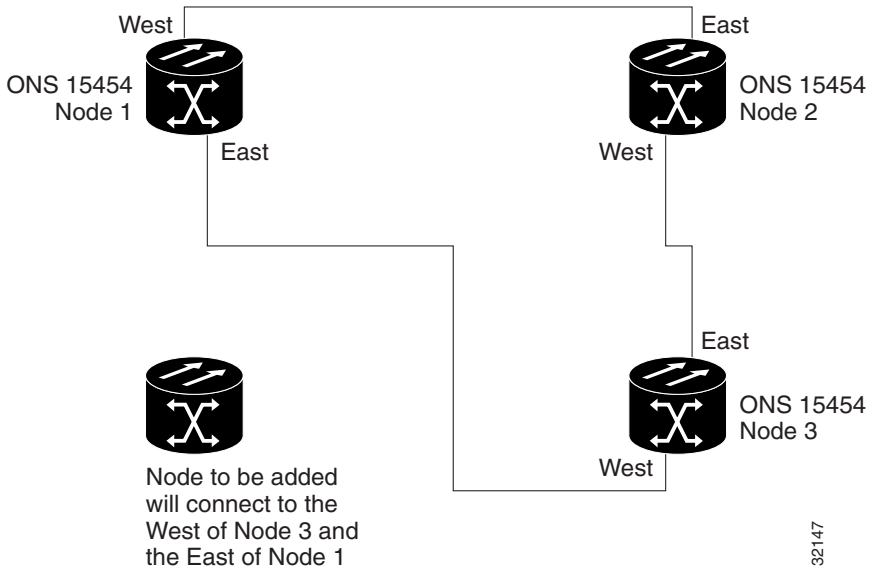
(d) Pull fibers at one node and verify that traffic switches normally.

4.1.3 Adding and Dropping BLSR Nodes

This section provides procedures for adding and dropping BLSR nodes. To add or drop a node, you force a protection switch to route traffic away from the span where service will be performed. Figure 4-10 shows a three-node BLSR before the new node is added.

Note You can only add one node at a time to an ONS 15454 BLSR.

Figure 4-10 Three Node BLSR Example



Procedure: Add a BLSR Node

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

Step 1 Install the optical cards in the ONS 15454 that you will add to the BLSR. Make sure fiber cables are available to connect to the cards. Run test traffic through the node to ensure the cards are functioning properly.

Step 2 Log into the node that will connect to the new node through its east port (Node 1 in the example shown in Figure 4-10).

Step 3 Manually switch protection on the east port:

(a) Click the **Maintenance>Ring** tabs.

(b) From East Operation, choose **FORCE RING**.

(c) Click **Apply**.

Performing a manual switch generates a manual equipment request alarm. This is normal.

Caution Traffic is unprotected during a protection switch.

Step 4 Log into the node that will connect to the new node through its west port (Node 3 in the example).

Step 5 Manually switch protection on the west port:

(a) Click the **Maintenance>Ring** tabs.

(b) From West Operation, choose **FORCE RING**.

(c) Click **Apply**.

Step 6 Log into the new node and complete the BLSR setup procedures in the "Setting Up BLSRs" section on page 4-6:

- Provision the SONET DCC
- Configure the BLSR timing
- Enable the BLSR ports
- Configure the BLSR

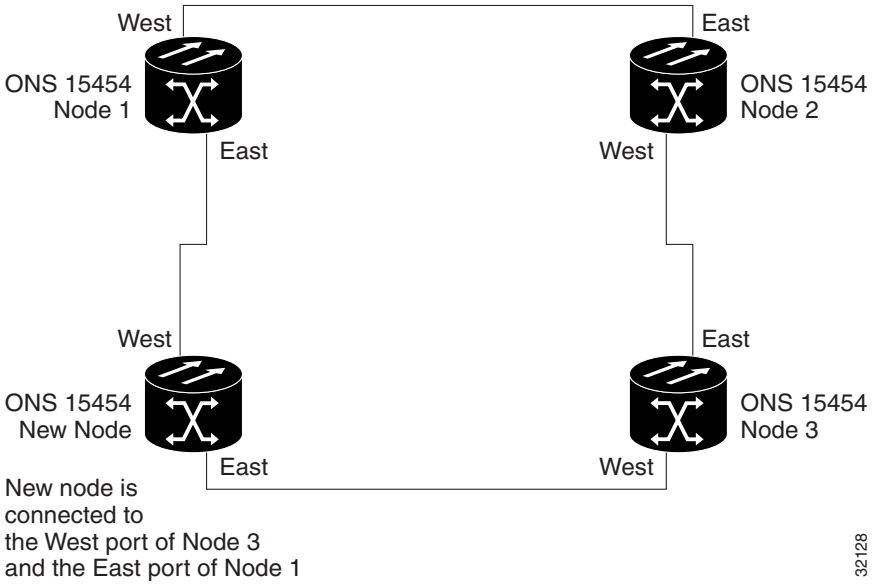
Step 7 Remove the fiber connections from the two nodes that will connect directly to the new node.

(a) Remove the east fiber from the node that will connect to the west port of the new node.

(b) Remove the west fiber from the node that will connect to the east port of the new node.

Step 8 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, as shown in Figure 4-11.

Figure 4-11 BLSR Example with Added Fourth Node



Step 9 Log out of CTC and then log back in. Wait for the BLSR Ring Map Change dialog to display. (If the ring map does not display, select the **Provisioning>Ring** tabs and click **Ring Map**.)

Step 10 When the BLSR Map Ring Change dialog displays, click **Yes**.

Step 11 On the BLSR Ring Map dialog, click **Accept**.

Step 12 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 13 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 is correct.

Step 14 Select the **Circuits** tab and verify that no incomplete circuits are present.

Step 15 Clear the protection switch. Do this for the node that is using its east port to connect to the new node, and for the node that is using its west port to connect to the new node.

(a) To clear the protection switch from the east port, display the **Maintenance>Ring** tabs. From East Operation choose **CLEAR**. Click **Apply**.

(b) To clear the protection switch from the west port, click West Operation and choose **CLEAR**. Click **Apply**.

Procedure: Drop a BLSR Node

Caution The following procedure minimizes traffic outages during node deletions, but traffic will be lost when you delete and recreate circuits that passed through the deleted node.

Step 1 In the node that will be removed, 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.

(b) Select the circuits that you need to delete, then 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.

Note Do not log into the node that is being removed.

Step 2 Manually switch traffic away from the ports of neighboring nodes that will be disconnected when the node is removed:

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

(b) Click the **Maintenance>Ring** tabs and choose **FORCE** from East Operation. Click **Apply.**

(c) Open the node that is connected through its west port to the removed node.

(d) From West Operation choose **FORCE**. Click **Apply.**

Caution Traffic is unprotected during the protection switch.

Step 3 Remove all fiber connections between the node being removed and the two nodes where it is still connected.

Step 4 Reconnect the two neighboring nodes.

Step 5 Wait for the BLSR Map Ring Change dialog to display. If the dialog does not display, select the **Provisioning>Ring** tabs and click **Ring Map**.

Step 6 When the BLSR Map Ring Change dialog displays, click **Yes**.

Step 7 On the BLSR Ring Map dialog, click **Accept**.

Step 8 Delete, then recreate each circuit that passed through the deleted node. Do this one circuit at a time.

Step 9 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 East Operation. Click **Apply**.

(a) Open the node with the protection switch on its west port.

(b) Click the **Maintenance>Ring** tabs and choose **CLEAR** from West Operation. Click **Apply.**

Step 10 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 from which all other nodes will derive their timing.

Step 11 Select the **Circuits** tab and verify that incomplete circuits are not present.

Step 12 Recreate all circuits deleted in Step 1 that passed through the dropped node.

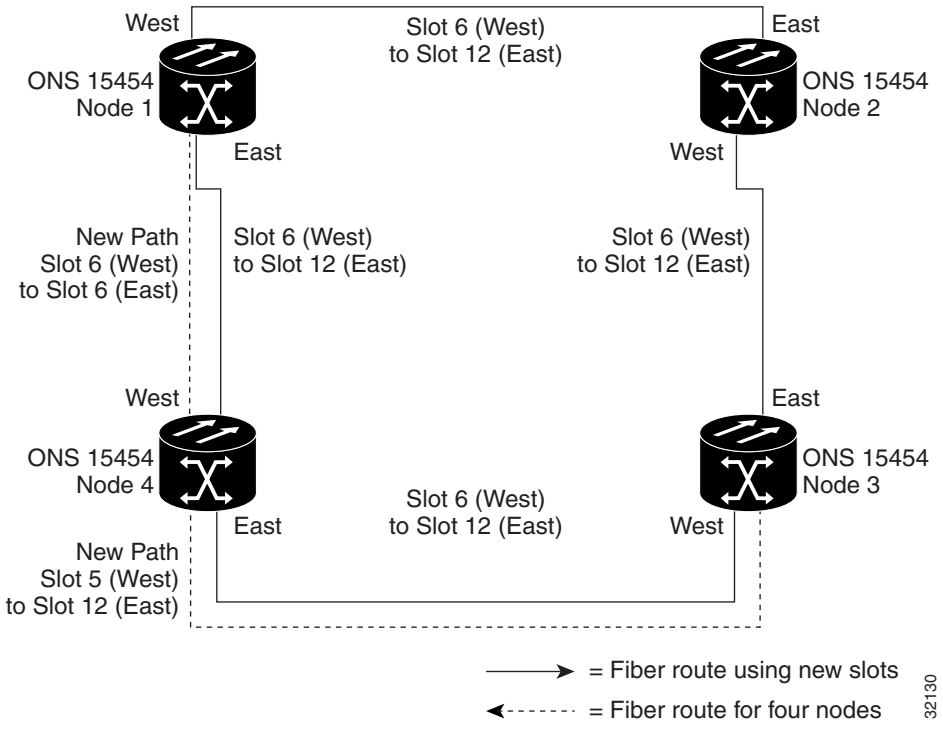
4.1.4 Moving BLSR Trunk Cards

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

Caution To arrange the trunk cards, you will drop one node at a time from the current BLSR ring. 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 4-12 shows a four node OC-48 BLSR made up of Node 1, Node 2, Node 3, and Node 4. Node 4 is temporarily removed from the active BLSR, while the OC-48 card in Slot 6 moves to Slot 5 and the OC-48 card in Slot 12 moves to Slot 6.

Figure 4-12 BLSR Trunk Card Switchover Example



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 15454 nodes must have CTC Release 2.0 or later and cannot have active alarms for the OC-48 or OC-12 cards or the BLSR configuration.

Step 1 Switch traffic away from the node where the trunk card will be switched:

(a) Log into the node connected through its east port to the node where the trunk card will be moved. Click the **Maintenance>Ring** tabs.

(b) From East Operation, choose **FORCE RING**.

(c) Click **Apply**.

When you perform a manual switch, a manual equipment request alarm is generated. This is normal.

Caution Traffic is unprotected during a protection switch.

(d) Log into the node that is connected through its west port to the node where the trunk card will be moved. Click the **Maintenance>Ring** tabs.

(e) From West Operation, choose **FORCE RING**.

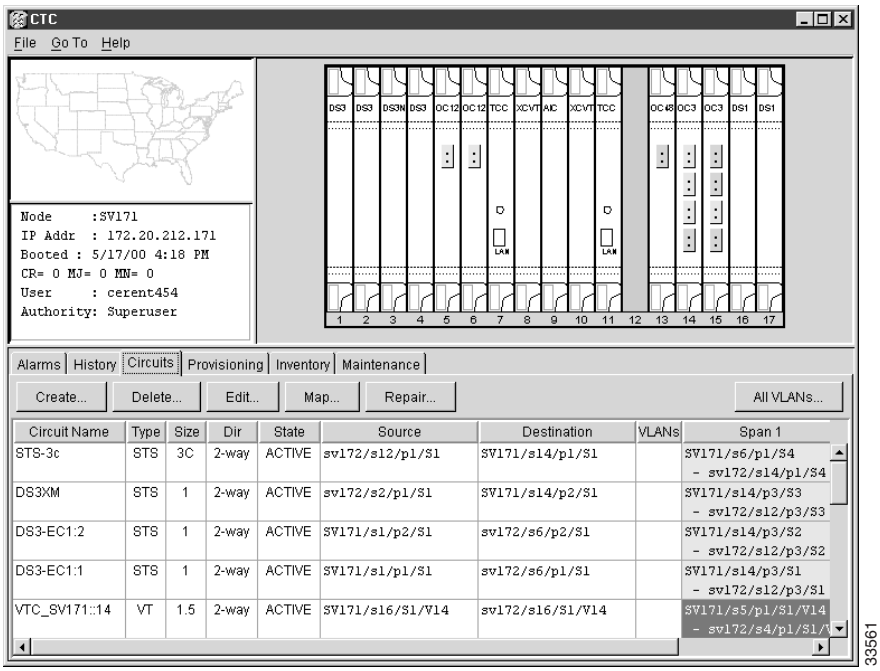
(f) Click **Apply**.

Step 2 Log into the node where the trunk card you will move is installed.

Step 3 Click the **Circuits** tab (Figure 4-13).

Step 4 Record the provisioning information of the affected circuits. You will need this information later to restore the circuits.

Figure 4-13 Circuits Tab



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, click **Yes.**

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

(a) Click the **Provisioning>Sonet DCC** tabs.

(b) Under SDCC Terminations, click the Sonet DCC you need to delete and click **Delete**.

Step 7 Disable the ring on the current node:

(a) Click the **Provisioning>Ring** tabs.

(b) From Node ID and choose **Ring Disabled**.

(c) Click **Apply**.

Step 8 If the OC card is a timing source, select the **Provisioning>Timing** tabs and set timing to Internal.

Step 9 Place the ports on the card out of service:

(a) Double click the card.

(b) On the **Provisioning>Line** tabs under Status, choose **Out of Service** for each port.

Step 10 Physically remove the card.

Step 11 Insert the card into its new slot and wait for the card to boot.

Step 12 To delete the card from its former slot, right click the card in node view and select **Delete** from the list of options.

Step 13 Place the port(s) back in service:

(a) To open the card, double click or right click the card and select **Open**.

(b) Click the **Provisioning** tab.

(c) From Status choose **In Service**.

(d) Click **Apply**.

Step 14 Follow the steps described in the "Setting Up BLSRs" section on page 4-6 to reenable the ring using the same cards (in their new slots) and ports for east and west.

Step 15 Manually reenter the circuits that were deleted.

For more information about circuit provisioning, see the "Creating and Provisioning Circuits" section on page 4-40.

Step 16 If you use line timing and the card you are moving is a timing reference, reenable the timing parameters on the card.

4.2 Unidirectional Path Switched Rings

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

Figure 4-14 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 4-15), Node ID 2 switches its active receiver to the protect signal coming through Node ID 3.

Figure 4-14 Basic UPSR Configuration

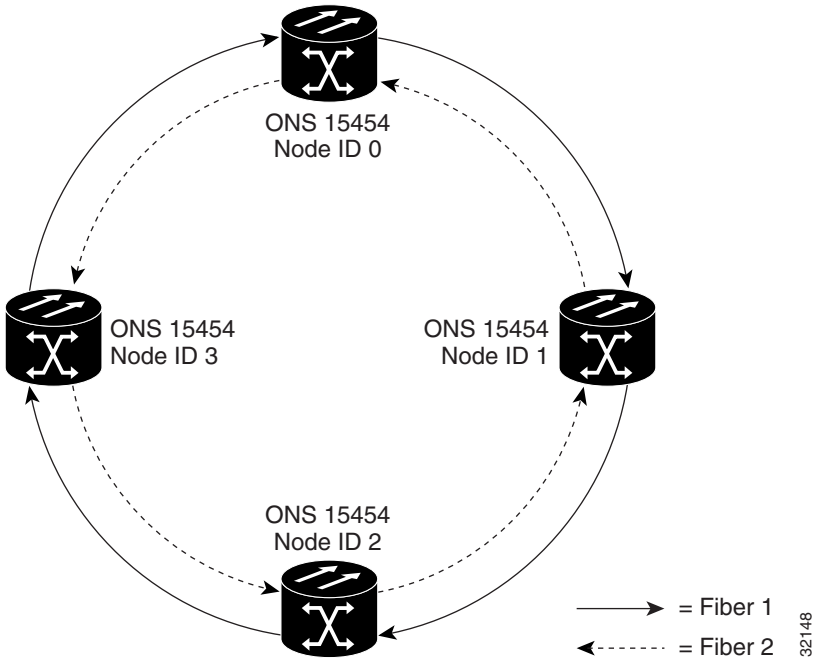
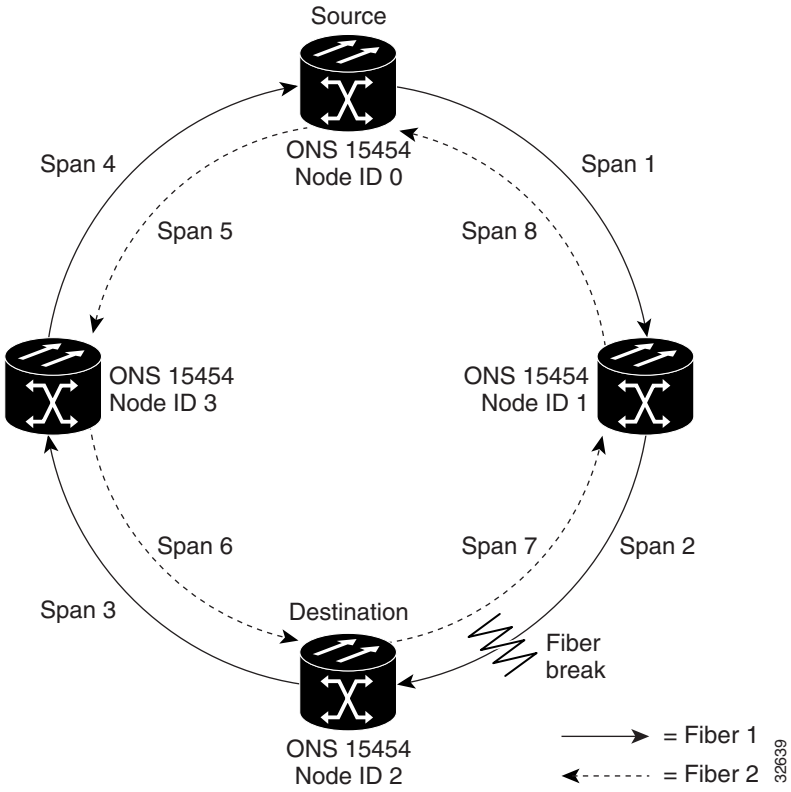


Figure 4-15 UPSR Fiber Break



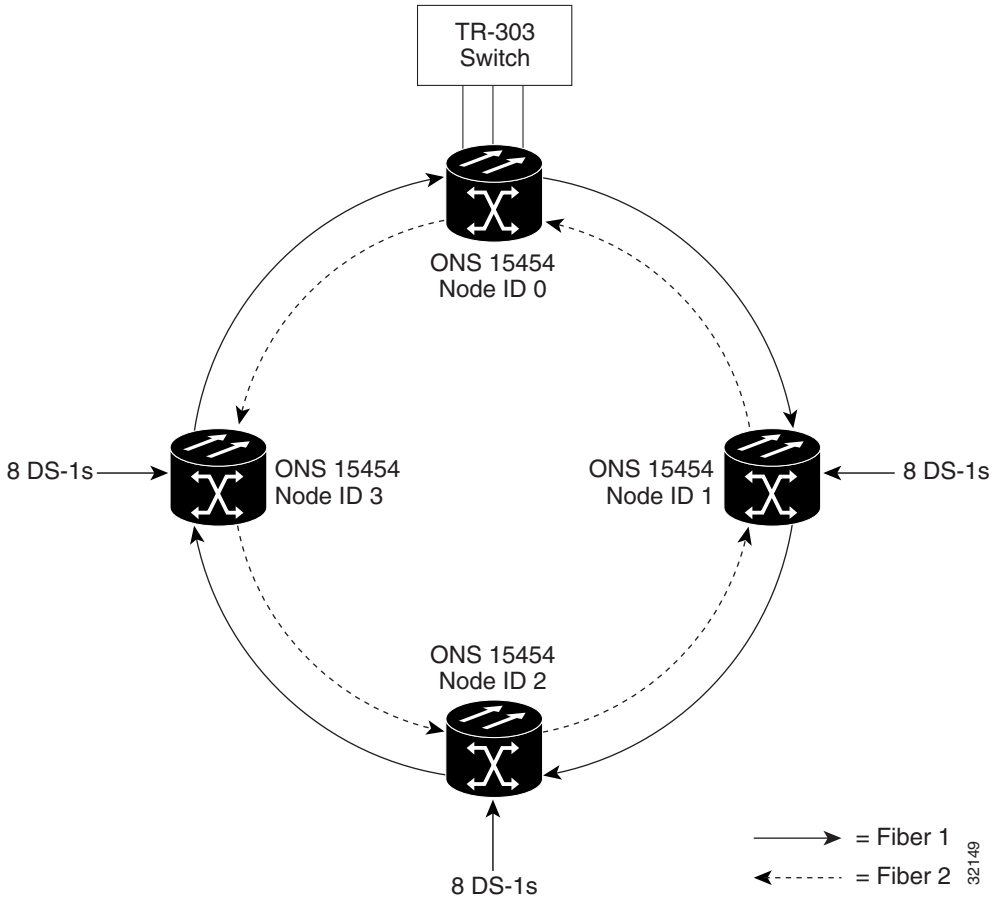
Because each traffic path is transported around the entire ring, UPSRs are best suited for networks where traffic concentrates at one or two locations and is not widely distributed. UPSR ring capacity is equal to its bit rate. Services can originate and terminate on the same UPSR, or they can be passed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

CTC automates ring configuration. UPSR traffic is defined within the ONS 15454 on a circuit-by-circuit basis. If a path-protected circuit is not defined within a 1+1 or BLSR line protection scheme and path protection is available and specified, CTC uses UPSR as the default.

4.2.1 Sample UPSR Application

Figure 4-16 shows a common UPSR application. OC-3 optics provide remote switch connectivity to a host TR-303 switch. In the example, each remote switch requires eight DS-1s to return to the host switch. Figure 4-17 and Figure 4-18 show the shelf layout for each site.

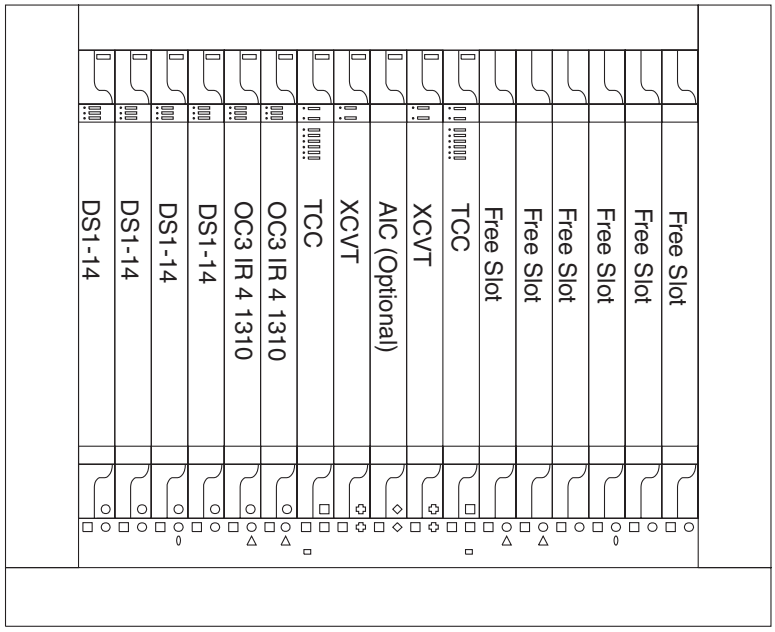
Figure 4-16 Sample OC-3 UPSR Application



Node ID 0 has four DS1-14 cards to provide 56 active DS-1 ports. The other sites only require two DS1-14 cards to handle the eight DS-1s to and from the remote switch. You can use the other half of each ONS 15454 shelf to provide support for a second or third ring to other existing or planned remote sites.

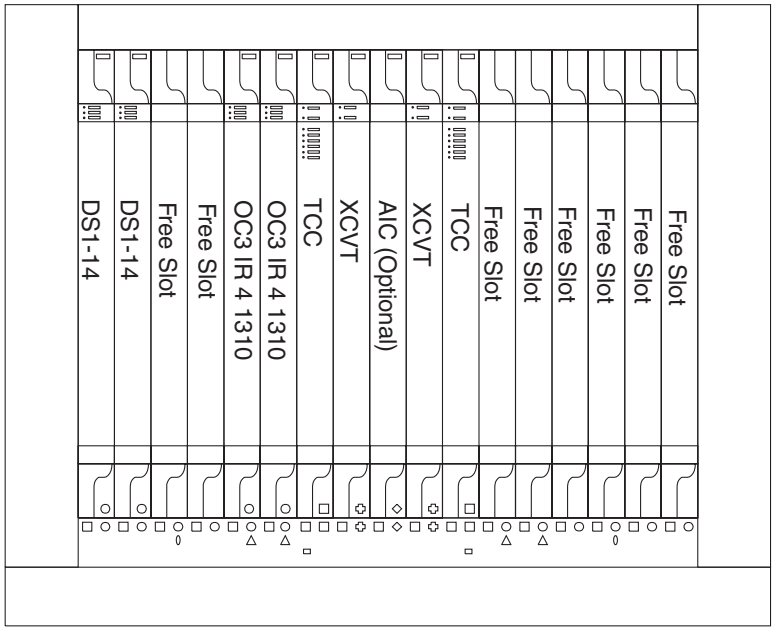
In this sample OC-3 UPSR, Node 0 contains four DS1-14 cards and two OC3 IR 4 1310 cards. Six free slots also exist in this setup and can be provisioned with cards or left empty. Figure 4-17 shows the shelf setup for these cards.

Figure 4-17 Node ID 0 Layout for Sample OC-3 UPSR



In this sample OC-3 UPSR, Nodes 1 to 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 4-18 shows the shelf setup for this configuration sample.

Figure 4-18 Node ID 1-3 Layout for Sample OC-3 UPSR



4.2.2 Setting Up a UPSR

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

- Install the Optical Carrier cards and attach the fiber
- Create the UPSR DCC terminations
- Configure the timing
- Enable the ports

After you enable the ports, you set up the UPSR circuits. UPSR signal thresholds are set at the circuit level. For procedures on creating UPSR circuits, see the "Creating and Provisioning Circuits" section on page 4-40.

Procedure: Install the Optical Carrier Cards

Step 1 Use the procedures in Chapter 1 to install the Optical Carrier cards. If you use OC-48 cards, make sure they are installed in Slots 5, 6, 12, or 13.

Step 2 When the ACT LED turns green, log into the node. Figure 4-19 shows a sample two-node OC-48 UPSR, and Figure 4-20 shows a sample shelf setup for the two-node, OC-48 UPSR.

Figure 4-19 Sample Two Node OC-48 UPSR

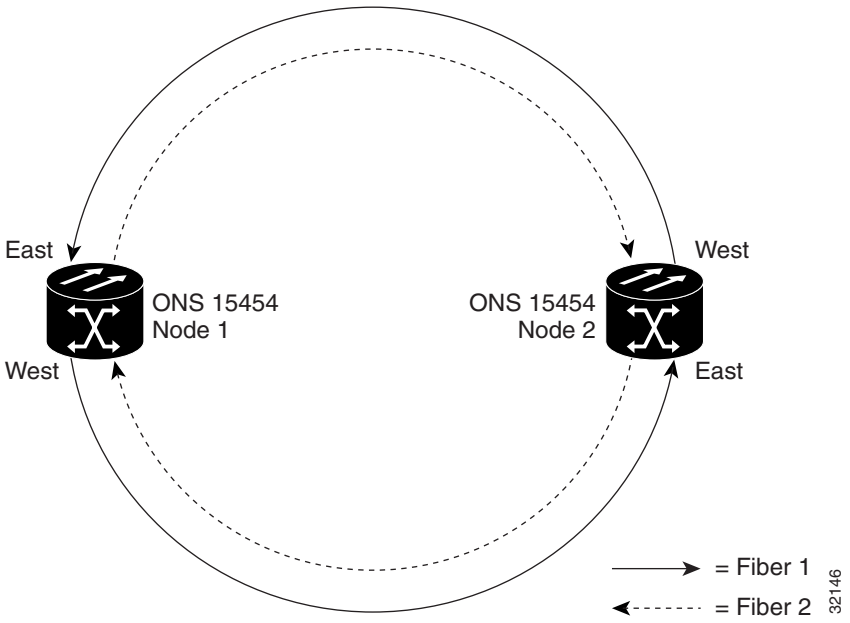
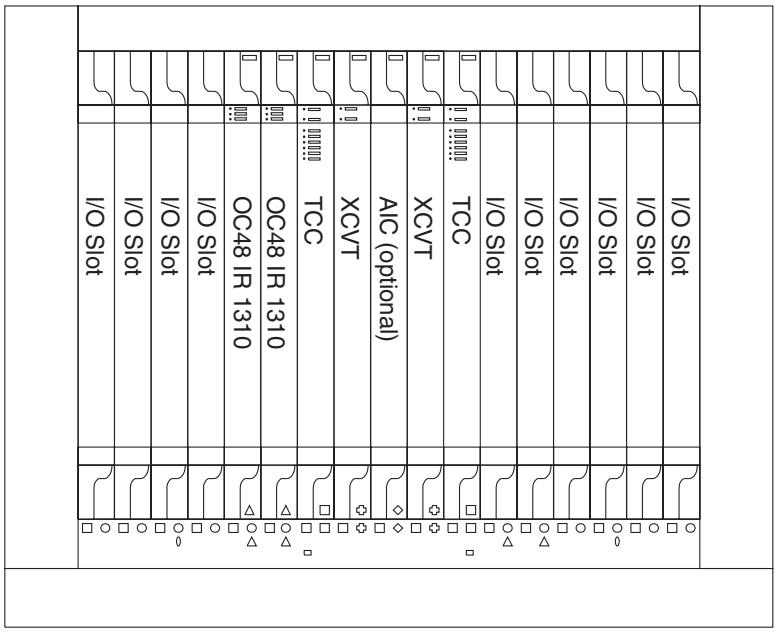


Figure 4-20 Sample Two Node OC-48 UPSR Shelf Setup



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 Under SDCC Terminations, click **Create**.

Step 4 On the Create SDCC Terminations dialog, press Control and click the two slots/ports that will serve as the UPSR ring ports at the node. For example, Slot 6 (OC-48)/Port 1 and Slot 12 (OC-48)/Port 1.

Note The ONS 15454 uses the SONET Section layer DCC (SDCC) for data communications. It does not use the Line DCCs. These can be used to tunnel DCCs from third party equipment across ONS 15454 networks. For procedures, see the "Provision a DCC Tunnel" section on page 4-48.

Step 5 Click **OK.**

The slots/ports display under SDCC Terminations.

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 "Setup ONS 15454 Timing" section on page 3-31. For general information about ONS 15454 timing, see the "Setting Up ONS 15454 Timing" section on page 3-29. After configuring the timing, enable the UPSR ports as described in the following procedure.

Procedure: Enable the UPSR Ports

Step 1 Open one of the UPSR nodes.

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.

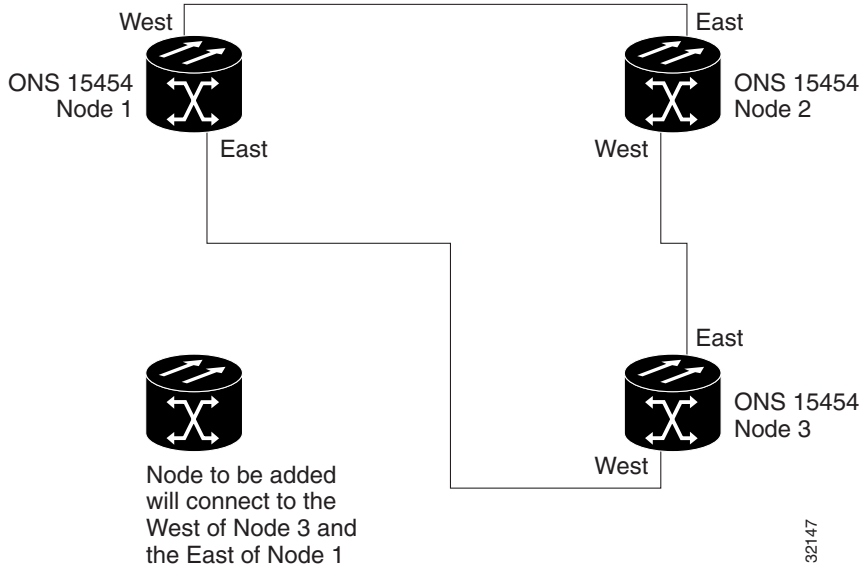
Step 5 Click **Apply**.

You configured a UPSR for one node. Use the same procedure to configure the additional nodes. To create path protected mesh networks, see the "Path Protected Mesh Networks" section on page 4-38. To create circuits, see the "Creating and Provisioning Circuits" section on page 4-40.

4.2.3 Adding and Dropping UPSR Nodes

This section provides procedures for adding and dropping nodes in an ONS 15454 UPSR configuration. To add or drop a node, you manually switch traffic on the affected spans to route traffic away from the area of the ring where service will be performed. Use the selector maintenance option to switch traffic from a UPSR span at different protection levels. The selector maintenance option is useful when you need to temporarily reroute traffic from a UPSR span to add or drop nodes, perform maintenance, or perform other operations. Figure 4-21 shows a three-node UPSR before a fourth node is added.

Figure 4-21 Three Node UPSR

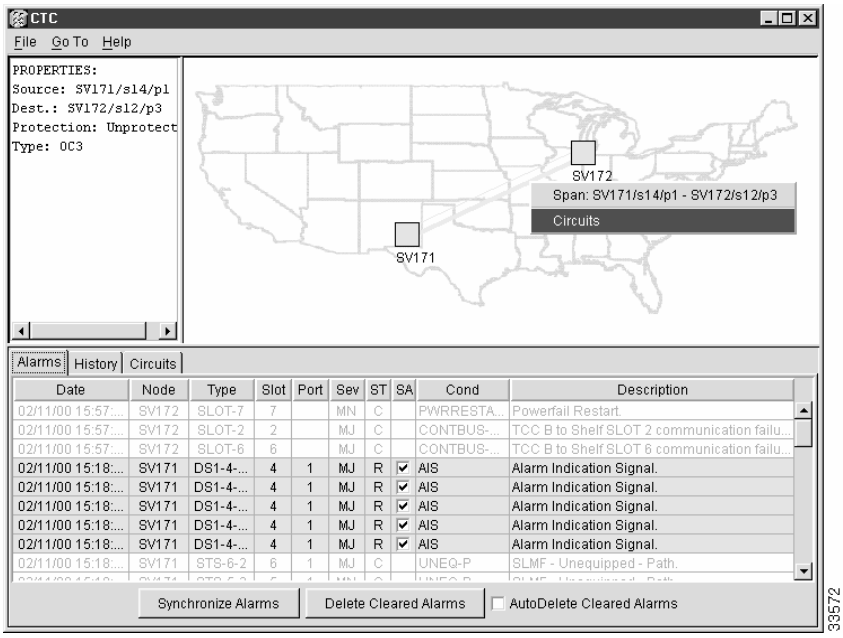


Procedure: Switch UPSR Traffic

Step 1 Go to the CTC network view.

Step 2 Right click the span that will be cut to add the new node and select **Circuits** from the shortcut menu (Figure 4-22).

Figure 4-22 Span Shortcut Menu

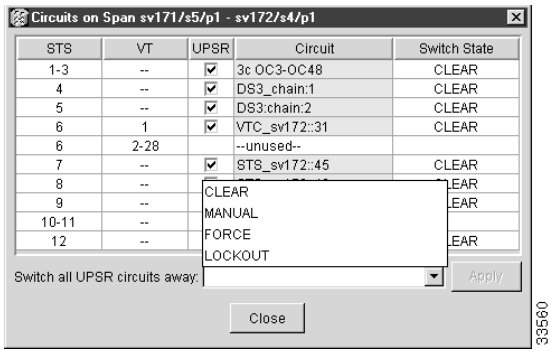


Step 3 On the Circuits on Span dialog (Figure 4-23), select the protection from the **Switch all UPSR circuits away** menu:

- CLEAR removes a previously-set switch command.
- MANUAL (recommended) 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 might cause line outages.

Figure 4-23 Circuits on Span Dialog



Step 4 Click **Apply.**

Step 5 When the confirmation dialog 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 At the node that will be added to the UPSR:

- Verify that the Optical Carrier 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.
- Provision the new node following the procedures listed in the "Setting Up a UPSR" section on page 4-21.

Step 2 Log into one of the nodes that will directly connect to the new node.

Step 3 Use the procedures in the "Switch UPSR Traffic" section on page 4-24 to switch traffic away from the span that will connect to the new node.

Caution Traffic is not protected during a protection switch.

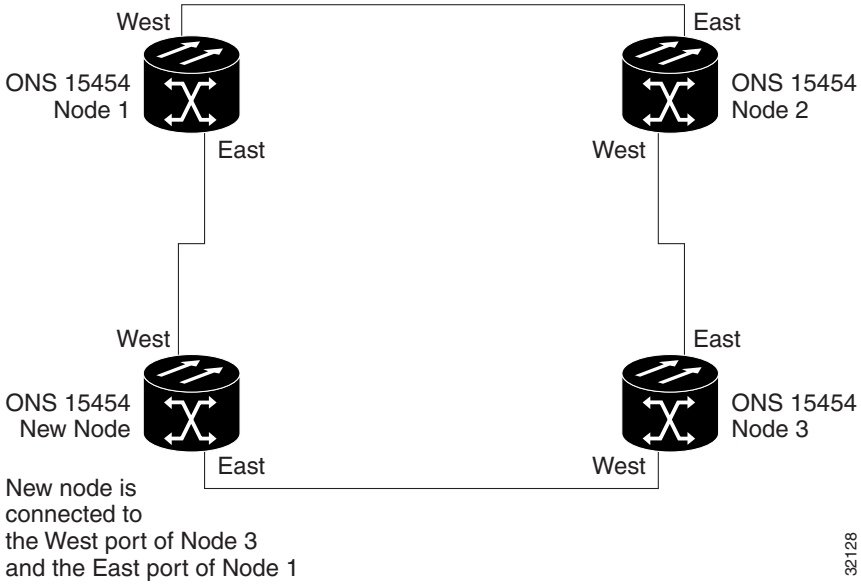
Step 4 Two nodes will connect directly to the new node; remove their fiber connections:

(a) Remove the east fiber connection from the node that will connect to the west port of the new node (Node 1 in the example shown in Figure 4-21).

(b) Remove the west fiber connection from the node that will connect to the east port of the new node (Node 3 in the Figure 4-21 example).

Step 5 Replace the removed fiber connections with connections from the new node. Connect the west port to the east port and the east port to the west port as shown in Figure 4-24.

Figure 4-24 UPSR Example With Fourth Node



Note Perform this step on site at the new node.

Step 6 Log out of CTC and then log back in.

Step 7 Go to 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 8 Click the **Circuits** tab and wait for all the circuits to appear, including spans. The affected circuit will display as "incomplete." One span will be missing until you update the circuit with the new node (Step 9). All other spans should be present.

Step 9 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 to appear. Verify that the number of updated circuits displayed in the dialog is correct.

Step 10 Select the **Circuits** tab and verify that no incomplete circuits are displayed. If incomplete circuits are displayed, run the **Update** command again.

Step 11 Use the procedures in the "Switch UPSR Traffic" section on page 4-24 to clear the protection switch.

Procedure: Drop a Node

Caution The following procedure is designed to minimize traffic outages during node deletions, but traffic will be lost when you delete and recreate circuits that passed through the deleted node.

Step 1 Use the procedures in the "Switch UPSR Traffic" section on page 4-24 to switch traffic away from the node you are dropping. Do this on all spans connected to the node you are deleted.

Caution Traffic is not protected during a force protection switch.

Step 2 In the node that will be removed, delete circuits that originate or terminate in that node. (If a circuit has multiple drops, delete only the drops that terminate on the node you are deleting.)

(a) Click the **Circuits** tab.

(b) Select the circuit(s) to delete. To select multiple circuits, press the Shift or Ctrl key.

(c) Click **Delete**.

(d) Click **Yes** when prompted.

Step 3 From the node that will be deleted, remove the east and west span fibers. At this point, the node should no longer be a part of the ring.

Step 4 Reconnect the span fibers of the nodes remaining in the ring.

Step 5 Open the Alarms window of each newly-connected node and verify that the span cards are free of alarms. Resolve any alarms before proceeding.

Step 6 One circuit at a time, delete and recreate each circuit that passed through the deleted node.

Note If the removed node was the BITS timing source, select a new node as the BITS source, or select another node as the master timing node.

Step 7 Verify the network map and circuits:

(a) Switch to network view.

(b) Select the **Circuits** tab, then select each circuit and click **Map**.

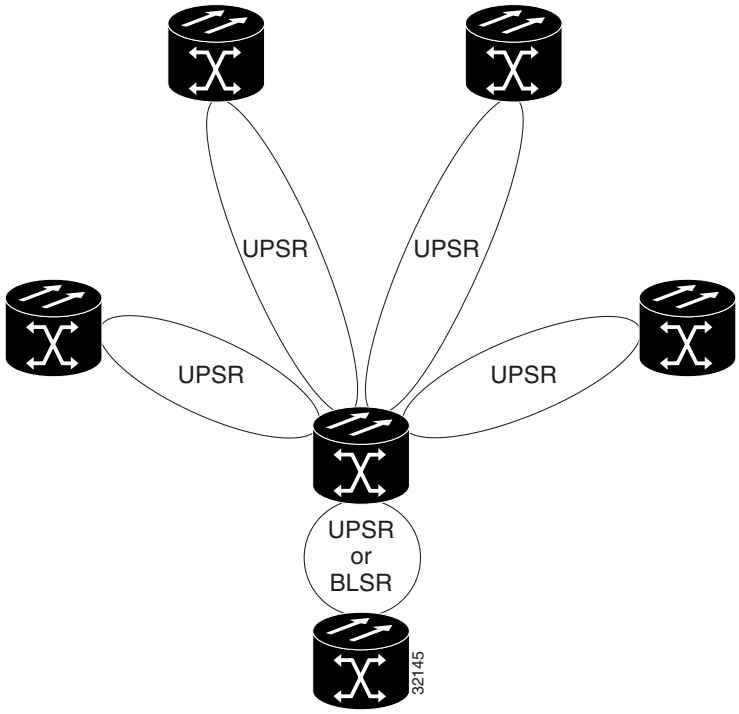
(c) Verify that all circuits are correct and no incomplete circuits are displayed.

4.3 Subtending Rings

Because the ONS 15454 supports up to ten SONET DCCs, one ONS 15454 can terminate and groom five UPSR rings or four UPSR rings and one BLSR ring. (If you tunnel DCCs, this number drops by one ring for each DCC tunnel. See the "DCC Tunneling" section on page 4-47.) Subtending rings from a single ONS 15454 reduces the number of shelves and cards required, and reduces external shelf-to- shelf cabling. Figure 4-25 shows an ONS 15454 with multiple subtending rings.

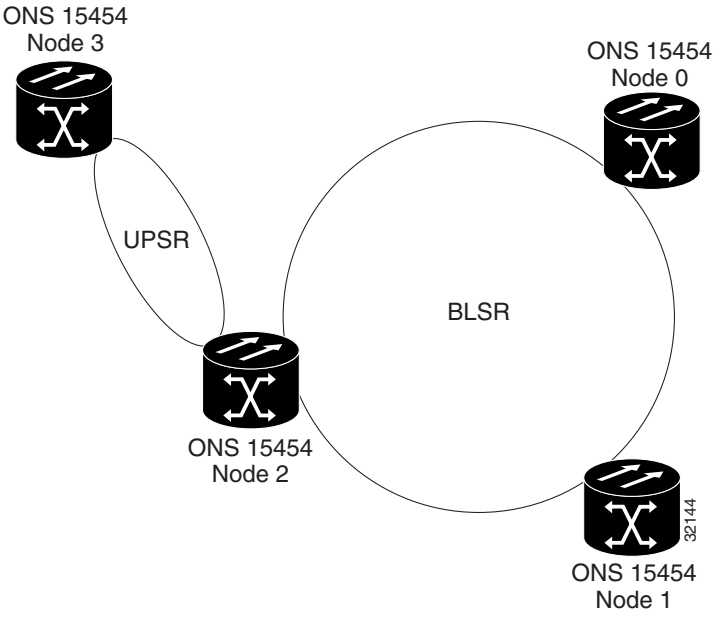
Note You cannot nest rings on the same ONS 15454 nodes. For example, if a UPSR is set up on Nodes 1 – 4, you cannot run a BLSR on the same nodes.

Figure 4-25 ONS 15454 With Multiple Subtending Rings



This section shows how to subtend a UPSR from a BLSR. To subtend multiple rings, repeat the following procedure for each ring. Figure 4-26 shows a UPSR subtending from a BLSR. In this example, Node 2 is the only node serving both the BLSR and UPSR. Some Node 2 slots are dedicated to BLSR and others to UPSR.

Figure 4-26 Multiple Subtending Rings



Procedure: Subtend a UPSR from a BLSR

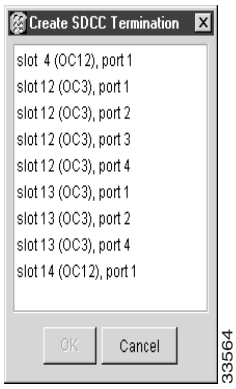
Step 1 Fill the optical slots with the number of optical cards needed for your application.

Step 2 From the Node view, click the **Provisioning>Sonet DCC** tabs.

Step 3 Click **Create**.

The Create SDCC Termination dialog is displayed (Figure 4-27).

Figure 4-27 Create SDCC Termination dialog



Step 4 In the Create SDCC Terminations dialog, click the slot and port that will carry the UPSR.

Step 5 Click **OK**.

Step 6 Repeat Steps 3 – 5 for all optical slots/ports that will carry the UPSR.

The selected slots/ports are displayed under SDCC Terminations.

Step 7 Put the ports that you will use in service:

(a) In the node view, double click the desired optical card.

(b) Select the **Provisioning>Line** tabs. Under Status, choose **In Service**.

(c) Click **Apply**.

Step 8 Repeat Step 7 for all ports/slots that will carry the UPSR.

Step 9 Follow Steps 1 – 8 for the other nodes you will use for the UPSR.

Step 10 Go to the network view to view the subtending ring.

Procedure: Subtend a BLSR from a UPSR

Step 1 Fill the optical slots with the number of optical cards needed for your application.

Step 2 From the Node view, click the **Provisioning>Sonet DCC** tabs.

Step 3 Click **Create**.

The Create SDCC Termination dialog is displayed.

Step 4 In the Create SDCC Terminations dialog, click the slot and port that will carry the BLSR.

Step 5 Click **OK**.

Step 6 Repeat Steps 3 – 5 for all optical slots/ports that will carry the BLSR.

The selected slots/ports are displayed under SDCC Terminations.

Step 7 Configure the BLSR:

(a) Click the **Provisioning>Ring** tabs.

(b) On the **Ring** subtab under BLSR, assign a Node ID in the *NODE ID* field.

The Node ID identifies the node to the BLSR. Nodes in your BLSR must have different Node IDs. After you select a Node ID, the other BLSR fields are displayed.

(c) Set the BLSR properties:

- *Ring ID*—assign a ring ID (a number between 0 and 255). You must use the same Ring ID for all nodes in the same BLSR.
- *Reversion time*—set the amount of time after which the working traffic reverts back to the original working path. The default is 5 minutes.
- *East Port*—assign the east port from the pull-down menu.
- *West Port*—assign the west port from the pull-down menu.

(d) Click **Apply**.

Step 8 Put the ports that you will use in service:

(a) In the node view, double click the desired optical card.

(b) Select the **Provisioning>Line** tabs. Under Status, choose **In Service**.

(c) Click **Apply**.

(d) When the BLSR Map Ring Change dialog displays, click **Yes**.

(e) On the BLSR Ring Map dialog, click **Accept**.

Step 9 Repeat Step 8 for all ports/slots that will carry the BLSR.

Step 10 Follow Steps 1 – 9 for the other nodes you will use for the BLSR.

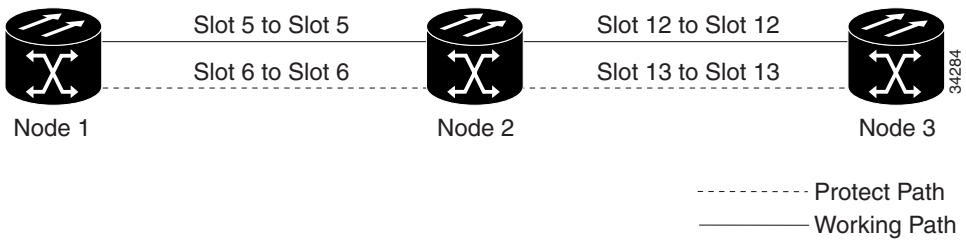
Step 11 Go to the network view to see the subtending ring.

4.4 Creating a Linear ADM Configuration

You can configure ONS 15454s as a line of add-drop multiplexers (ADMs) by configuring one set of optical cards as the working path and a second set as the protect path. Unlike rings, linear ADMs require that the optical 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 4-28 shows three ONS 15454s in a linear ADM configuration. Working traffic flows from Slot 6 of Node 1 to Slot 6 of Node 2, and from Slot 12 of Node 2 to Slot 12 of Node 3. You create the protect path by placing Slot 6 in a 1+1 protection with Slot 5 at Nodes 1 and 2, and Slot 12 in 1+1 protection with Slot 13 at Nodes 2 and 3.

Figure 4-28 Linear ADM



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 General Node Information" section on page 3-21.

Step 2 Set up the network information for the node. For procedures, see the "Setting Up ONS 15454 Network Information" section on page 3-22.

Step 3 Set up 1+1 protection for the optical cards in the ADM. In Figure 4-28, Slots 6 and 12 are the working ports and Slots 5 and 13 are the protect ports. In this example, you would set up one protection group for Node 1 (Slots 5 and 6), two for Node 2 (Slots 5 and 6, and 12 and 13) and one for Node 3 (Slots 12 and 13). For procedures on creating protection groups, see the "Creating Protection Groups" section on page 3-26.

Step 4 For optical ports connecting ONS 15454s, set the SONET Data Communications Channel terminations:

(a) Log into a linear ADM node and select the **Provisioning>Sonet DCC** tabs.

(b) Under SDCC Terminations, click **Create.**

(c) On the Create SDCC Terminations dialog, select the working port. Click **OK.**

Note Terminating nodes (Nodes 1 and 3 in Figure 4-28) will have one SDCC, and intermediate nodes (Node 2 in Figure 4-28) will have two SDCCs.

Step 5 Use the procedures provided in the "Setting Up ONS 15454 Timing" section on page 3-29 to set up the node timing. If a node is using line timing, set the working optical card as the timing source.

Step 6 Place the optical ports in service:

(a) Open an optical card that is connected to the linear ADM.

(b) On the **Provisioning>Line** tabs under Status, select **In Service**.

(c) Click **Apply**.

Repeat Step 6 for each optical card connected to the linear ADM.

Procedure: Convert a Linear ADM to UPSR

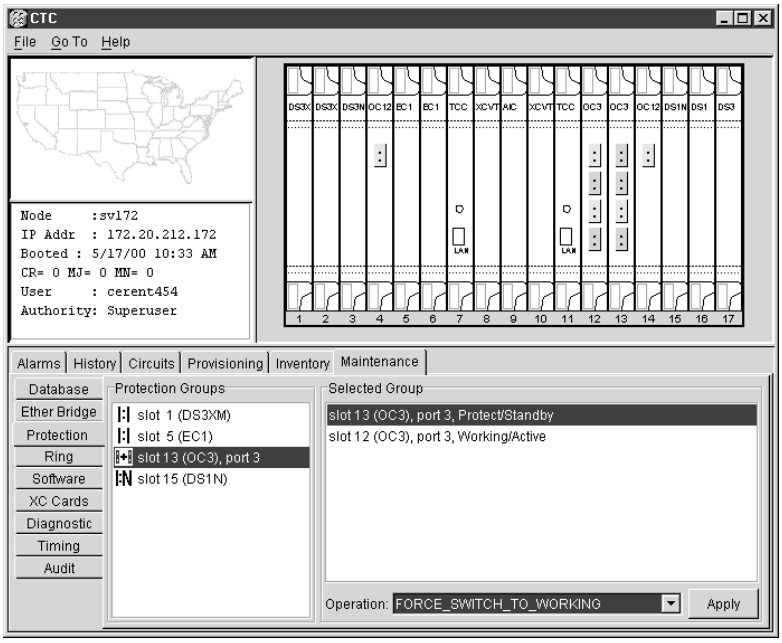
The following procedures describe how to convert a three-node linear ONS 15454 ADM to a UPSR.

Caution This procedure affects service.

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 4-29).

Figure 4-29 Maintenance>Protection Subtab



Step 3 Select the 1+1 protection group (that is, the group supporting the 1+1 span cards). Verify that the working slot is active. For example, under *Selected Group*, the working port should be shown as "Working/Active." If the slot says "Working/Standby," manually switch traffic to the working slot:

(a) In **Operations**, select Manual_Switch_to_Working. Click **Apply**.

(b) Click **Yes** on the confirmation dialog.

(c) Verify that the working slot is carrying traffic. If it is, continue to Step (d). If not, clear the conditions that prevent the card from carrying working traffic before proceeding.

(d) In **Operations**, select Clear. Click **Apply.**

(e) Click **Yes** on the confirmation dialog.

Repeat Step 3 for each group listed in Protection Groups.

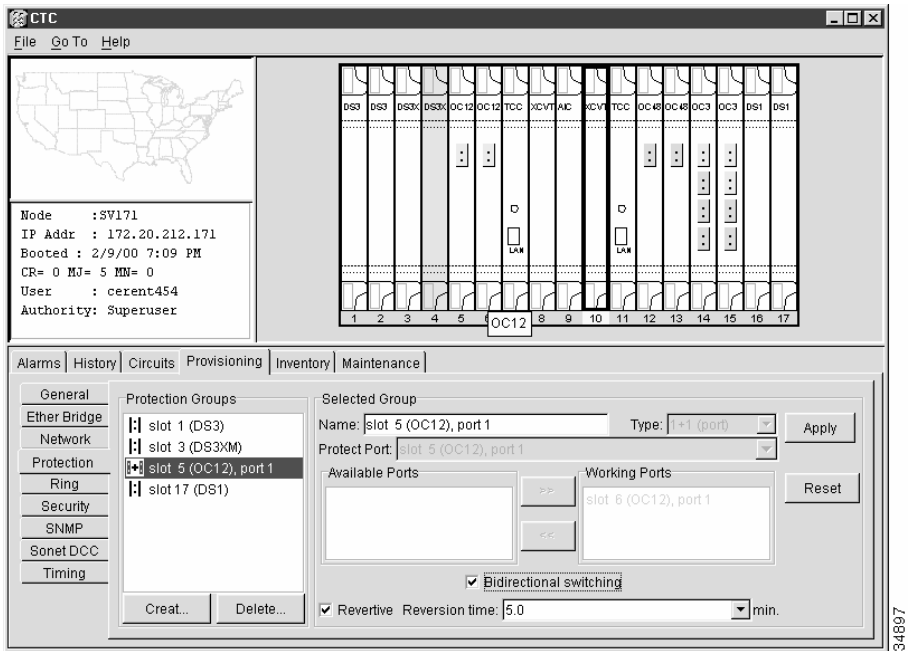
Step 4 For each node, delete the 1+1 OC-N protection group that supports the linear ADM span:

(a) Click the **Provisioning>Protection** tabs.

(b) In Protection Groups, select the group you want to delete (shown in Figure 4-30). Click **Delete**.

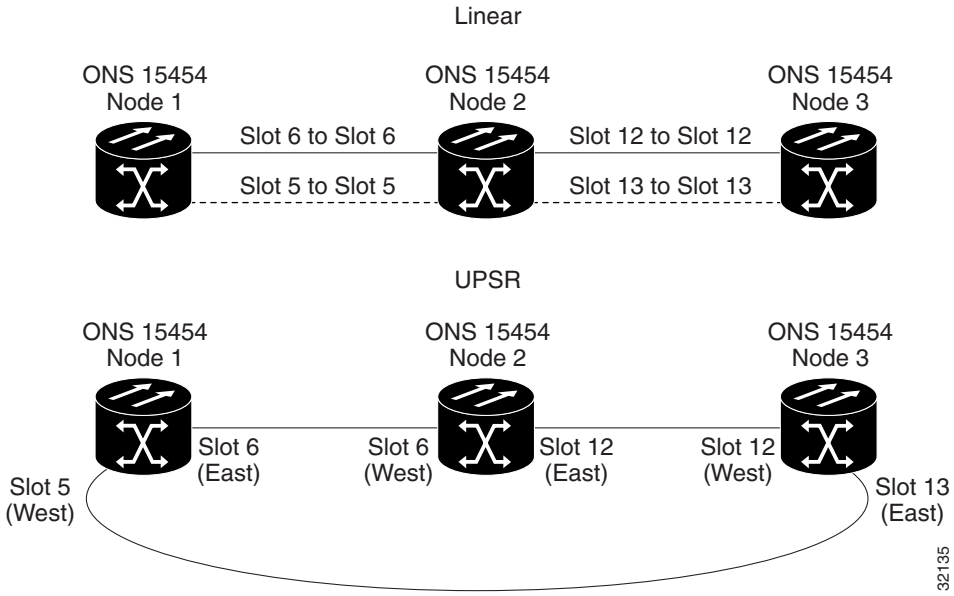
(c) Click **Yes** on the confirmation dialog.

Figure 4-30 Provisioning>Protection Subtab



Step 5 Physically remove one of the protect fibers running between the middle and end nodes. In the Figure 4-31 example, the fiber running from Slot 13/Node 2 to Slot 13/Node 3 is removed.

Figure 4-31 Linear to UPSR Conversion



Step 6 Physically reroute the other protect fiber to connect the two end nodes. In the Figure 4-31 example, the fiber between Node 1/Slot 5 and Node 2/ Slot 5 is rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

Step 7 In the middle node, remove the optic cards that are no longer connected to end nodes and delete their equipment records. (If you are leaving the optic cards in place, skip this step and go to Step 9.) In this example, cards in Node 2/Slots 5 and 13 are removed:

(a) Double click the first card (Slot 5, in the example).

(b) In the **Provisioning>Line** tabs under Status, select **Out of Service.**

(c) From the Go To menu, select **Parent View.**

(d) Right click the card you just placed out of service (e.g. Slot 5) and select **Delete Card**. (You can also go to the **Inventory** tab, select the card, and click **Delete**.)

(e) Click **Yes** on the confirmation dialog.

(f) Repeat (a) through (e) for the second card (e.g. Slot 13).

(g) Record all information for each cross-connect in the linear configuration.

Step 8 Go to one of the end nodes.

Step 9 Select the **Provisioning>Sonet DCC** tabs.

Step 10 Under SDCC Terminations, click **Create.**

Step 11 Highlight the slot that is not already in the SDCC Terminations list (in this example, port 1 of Slot 5 (OC-48).

Step 12 Click **OK.**

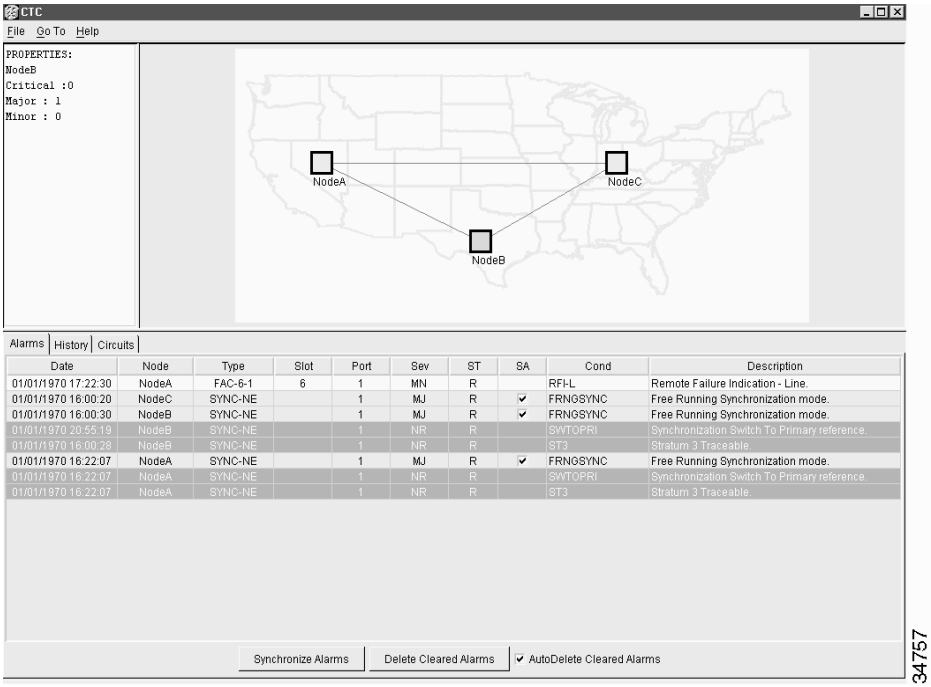
Step 13 Go to the node on the opposite end (Node 3 in Figure 4-31) and repeat Steps 9 – 12.

Step 14 Delete and reenter the circuits one at a time. (See the "Creating and Provisioning Circuits" section on page 4-40.)

Note Deleting circuits affects traffic.

Step 15 Go to the network map to view the newly-created ring (Figure 4-32).

Figure 4-32 Network View with Ring



Procedure: Convert a Linear ADM to a BLSR

The following procedures describe how to convert a three-node linear ONS 15454 ADM to a BLSR.

Caution This procedure affects service.

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 Select the 1+1 protection group (that is, the group supporting the 1+1 span cards). Verify that the working slot is active. For example, under Selected Group, the working port should be "Working/Active." If the slot says "Working/Standby," manually switch traffic to the working slot:

(a) In Operations, select **Manual_Switch_to_Working**. Click **Apply**.

(b) Click **Yes** on the confirmation dialog.

(c) Verify that the working slot is carrying traffic. If it is, continue to Step d. If not, before proceeding clear the conditions that prevent the card from carrying working traffic.

(d) In Operations, select **Clear**. Click **Apply.**

(e) Click **Yes** on the confirmation dialog.

Repeat Step 3 for each group listed in Protection Groups.

Step 4 For each node, delete the 1+1 OC-N protection group that supports the linear ADM span:

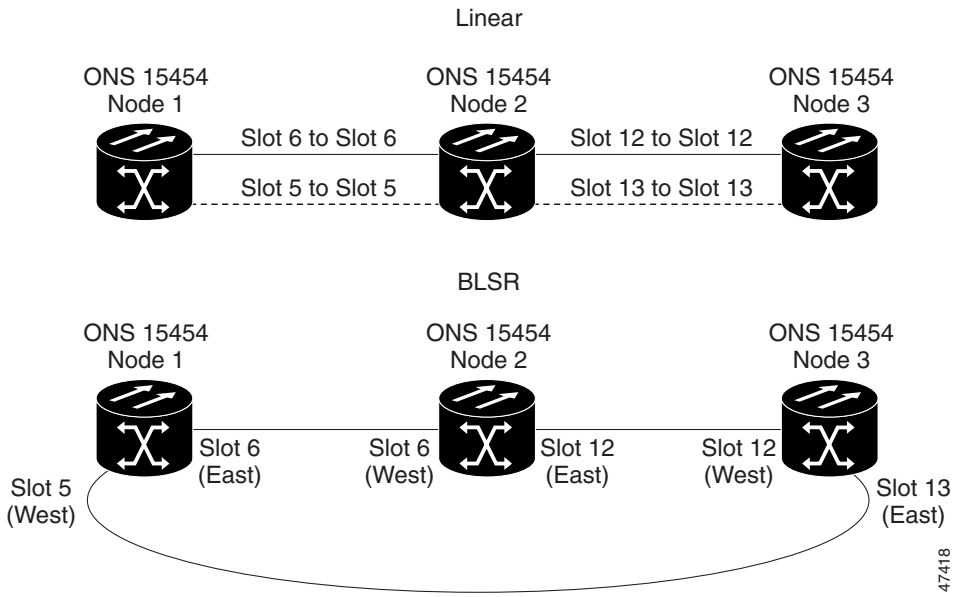
(a) Click the **Provisioning>Protection** tabs.

(b) In Protection Groups, select the group you want to delete. Click **Delete**.

(c) Click **Yes** on the confirmation dialog.

Step 5 Physically remove one of the protect fibers running between the middle and end nodes. In the Figure 4-33 example, the fiber running from Slot 13/Node 2 to Slot 13/Node 3 is removed.

Figure 4-33 Linear to BLSR Conversion



Step 6 Physically reroute the other protect fiber so it connects the two end nodes. In the Figure 4-33 example, the fiber between Node 1/Slot 5 and Node 2/Slot 5 is rerouted to connect Node 1/Slot 5 to Node 3/Slot 13.

Step 7 In the middle node, remove the optic cards that are no longer connected to end nodes and delete their equipment records. (If you are leaving the optic cards in place, skip this step and go to Step 9.) In this example, cards in Node 2/Slots 5 and 13 are removed:

(a) Double click the first card (Slot 5, in the example).

(b) In the **Provisioning>Line** tabs under Status, select **Out of Service.**

(c) From the Go To menu, select **Parent View.**

(d) Right click the card you just placed out of service (Slot 5 in the example) and select **Delete Card**. (Or, you can go to the **Inventory** tab, select the card, and click **Delete**.)

(e) Click **Yes** on the confirmation dialog.

(f) Repeat (a) through (e) for the second card (Slot 13 in the example).

(g) Select the **Provisioning>Line** tabs and record the circuit information for the linear configuration. To export the circuit information, select **Export** from the File menu. (For more information about exporting CTC data, see the "Printing and Exporting CTC Data" section on page 3-34.)

Step 8 Go to one of the end nodes.

Step 9 Select the **Provisioning>Sonet DCC** tabs.

Step 10 Under SDCC Terminations, click **Create.**

Step 11 Highlight the slot that is not already in the SDCC Terminations list (in this example, port 1 of Slot 5 (OC-48) on Node 1.

Step 12 Click **OK.**

Step 13 Go to the node on the opposite end (Node 3 in Figure 4-33) and repeat Steps 9 – 12.

Step 14 For circuits running on a BLSR protect STS (STSs 7-12 for an OC-12 BLSR, STSs 25-48 for an OC-48 BLSR), delete and recreate the circuit:

(a) Delete the first circuit.

(b) Recreate the circuit on STSs 1– 6 (for an OC-12 BLSR) or 1 – 24 (for an OC-48 BLSR) on the fiber that served as the protect fiber in the linear ADM. Before creating the circuit, deselect "Route Automatically" and "Fully Protected Path" on the Circuit Creation dialog box. Follow procedures in the "Creating and Provisioning Circuits" section on page 4-40 to provision the circuit.

(c) Repeat Steps (a) and (b) for each circuit residing on a BLSR protect STS.

Note Deleting circuits affects traffic.

Step 15 Configure the BLSR:

(a) Click the **Provisioning>Ring** tabs.

(b) On the **Ring** subtab under BLSR, assign a Node ID in the *NODE ID* field.

The Node ID identifies the node to the BLSR. Nodes in your BLSR must have different Node IDs. After you select a Node ID, the other BLSR fields are displayed.

(c) Set the BLSR properties:

- *Ring ID*—assign a ring ID (a number between 0 and 255). You must use the same Ring ID for all nodes in the same BLSR.
- *Reversion time*—set the amount of time after which the working traffic reverts back to the original working path. The default is 5 minutes.
- *East Port*—assign the east port from the pull-down menu.
- *West Port*—assign the west port from the pull-down menu.

(d) Click **Apply**.

(e) When the BLSR Map Ring Change dialog displays, click **Yes**.

(f) On the BLSR Ring Map dialog, click **Accept**.

Step 16 Go to the network map to view the newly-created ring.

4.5 Path Protected Mesh Networks

ONS 15454 networks give you the option to set up path protected mesh networks (PPMN). PPMN extends the protection scheme of UPSR from the basic ring configuration to the meshed architecture of several interconnecting rings. Typical UPSR protection creates two separate routes between source and destination nodes on a single UPSR. PPMN does this for source and destination nodes that do not lie on the same ring but link together through a network of meshed connections. When applied to a single ring, PPMN uses the same paths as the Telcordia-specified UPSR.

PPMN connects the source and destination of a circuit over two diverse paths through a network of single or multiple meshed rings. These two routes form a circuit-level UPSR. The source sends traffic on each of the diverse routes to the destination node, where the destination node uses the active route or switches to the standby route.

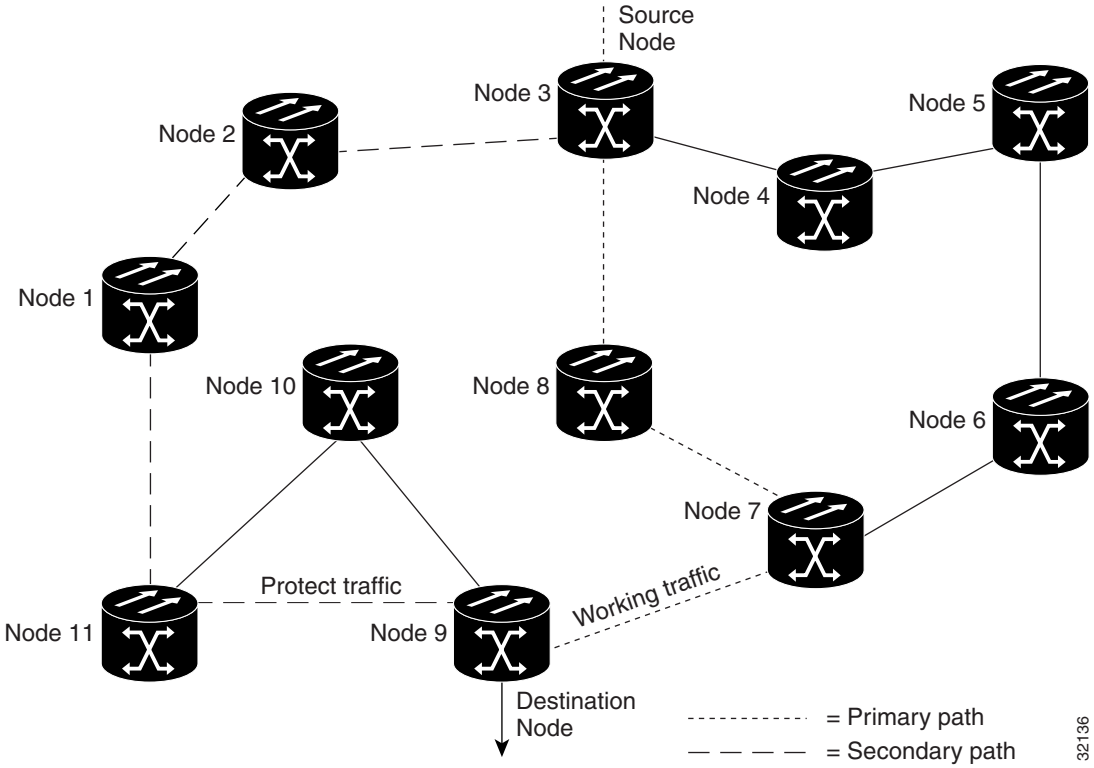
Note The primary and secondary routes are guaranteed to be link and span diverse, but not node diverse.

When you check the “Fully protect path” box during the normal A to Z provisioning process, PPMN provisions automatically in CTC. Choosing this option establishes an alternate route for the circuit in addition to the normally provisioned route. The second route or the protected path follows a unique second path through the network between the source and destination and sets up a second set of cross-connections. You can do this routing manually as well.

Figure 4-34 shows an example of PPMN. In the example, A to Z provisioned Node 3 as the source node and Node 9 as the destination node. The ONS 15454 CTC determined that the shortest route between the two end nodes passes through Node 8 and Node 7, shown by the dotted line. A to Z provisioning then automatically created cross-connections at each of the four nodes, 3, 8, 7, and 9, to provide the route for working traffic.

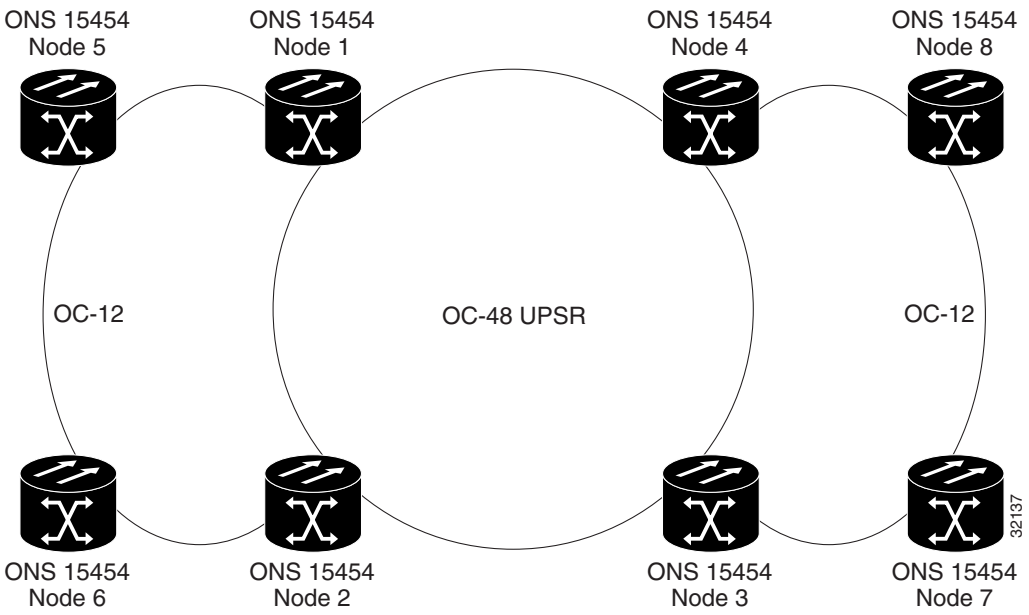
When the protected circuit box is checked, PPMN establishes a second unique route between Nodes 3 and 9 and automatically creates cross-connections at each of the five nodes, 3, 2, 1, 11, and 9 as illustrated by the dashed line. If a signal failure occurs on the primary path, traffic switches to the second, or protected 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 milliseconds.

Figure 4-34 Path Protected Mesh Network Example



PPMN also allows spans of different SONET line rates to be mixed together in "virtual rings." Figure 4-35 shows Nodes 1, 2, 3, and 4 forming 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 – 8 uses both OC-48 and OC-12.

Figure 4-35 PPMN Virtual Ring



4.6 Creating and Provisioning Circuits

You can create STS, VT1.5, and Ethernet circuits across and within ONS 15454 nodes and assign. circuits different attributes. For example, you can:

- Create one-way, two-way, or multicast 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.

Note Procedures for creating Ethernet circuits are provided in the "ONS 15454 Ethernet Circuit Configurations" section on page 7-16.

- Route circuits automatically or manually.
- Set an attribute so that CTC routes circuits only on protected paths.
- Set a filter to prevent you from attaching circuits to unprotected cards.
- Define a secondary circuit source or destination that allows you to interoperate an ONS 15454 UPSR with third-party equipment UPSRs.

4.6.1 Cross Connect Card Capacities

The ONS 15454 XC and XCVT cards perform the port-to-port time division multiplexing. XC cards perform STS switching; XCVT cards perform STS and VT1.5 switching. All TDM traffic consumes XC and XCVT bandwidth, even traffic that originates and terminates on the same ONS 15454. For example, each OC-12 card and the 12-port DS3-12 card consume 12 STS ports.

Table 4-2 shows the terminating STS and STS port-connection capacities of the XC and XCVT cards. Table 4-3 shows the terminating STS and VT1.5 connection capacities.

Table 4-2 XC and XCVT Card Capacity: STSs (Bidirectional)

Card	Terminating STSs	Connections between STS ports (1 to 1)
XC	288	144
XCVT	288	144

Table 4-3 XC and XCVT Card Capacity: VT1.5s (Bidirectional)

Card	Terminating STSs	Connections between VT1.5 ports
XC	0	0
XCVT	24 (672 VT1.5s)	336

When VT1.5 circuits are routed through ONS 15454 nodes, the number of VTs used within the XCVT cross-connect matrix depends on the protection scheme of the node. VT use is slightly higher at the source and drop nodes in 1+1 protection and in UPSRs than in BLSRs. Table 4-4 shows an example of VT use within an XCVT at the source and drop nodes.

Table 4-4 VT Use Example

Protection	VT ports Used Within XCVT Matrix per circuit	Description
1 + 1	3*	1) I/O card 2) Trunk card (working) 3) Trunk card (protect)
UPSR	3*	1) I/O card 2) Trunk card (working) 3) Trunk card (protect)
BLSR	2	1) I/O card 2) Trunk card (working)

* Source and drop nodes; two VT ports are used at pass-through nodes

4.6.2 VT Tunnels

You can tunnel VT1.5 circuits through ONS 15454 nodes. VT1.5 tunnels provide two benefits:

- VT1.5 tunnels allow you to route VT1.5 circuits through ONS 15454s with XC cards. (VT1.5 circuits require XCVT cards at the source and drop nodes.)
- When tunneled through nodes with XCVT cards, VT1.5 tunnels do not use VT connection capacity, thereby freeing the XCVT card's capacity for other VT1.5 circuits.

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 Node 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 VT1.5s between these nodes is close to 28),
- Node 2 or Node 3 have XC cards, or
- XCVT cards at Node 2 and Node 3 have reached full VT cross-connection capacity.

However, if the Node 1 - Node 4 tunnel carries only a few VT1.5 circuits, creating a regular VT1.5 circuit between Nodes 1, 2, 3, and 4 might maximize STS capacity.

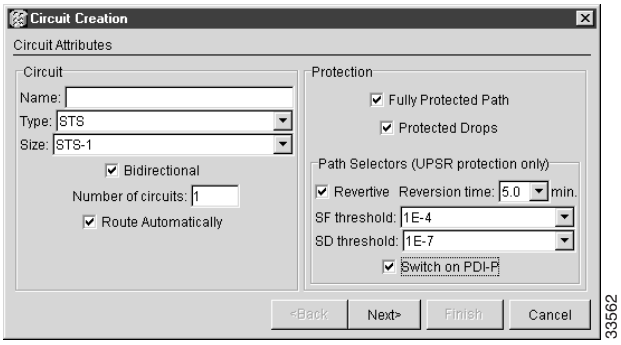
When you create a VT1.5 circuit, CTC checks to see whether a tunnel already exists between source and drop nodes. If a tunnel exists, CTC checks the tunnel capacity. If capacity is sufficient, CTC routes the circuit on the existing tunnel. If a tunnel does not exist, or if an existing tunnel does not have sufficient capacity, CTC displays a dialog 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, manually routing a circuit might make more sense than creating a new tunnel.

Procedure: Create a Circuit

Step 1 Log into CTC and click the **Circuits** tab.

Step 2 Click **Create**. The Circuit Creation dialog (Figure 4-36) displays.

Figure 4-36 Circuit Creation Dialog



Step 3 In the Circuit Creation dialog, complete the following fields:

- *Name*—assign a name to the circuit. The name can be alphanumeric and up to 32 characters (including spaces).
- *Type*—select the type of circuit you want to create: STS, VT (VT1.5), or VT tunnel. The circuit type you select determines the circuit-provisioning options that are displayed.
- *Size*—select the circuit size.
- *Bidirectional*—check this box if you want to create a two-way circuit; uncheck it to create a one-way circuit.
- *Number of circuits*—type the number of circuits you want to create. If you enter more than 1, CTC returns to the Circuit Source dialog after you create each circuit until you finish creating the number of circuits you specified here.
- *Route Automatically*—check this box if you want the CTC to choose the circuit path automatically. If it is not checked, you must provision the circuit spans and set the circuit paths manually.
- *Fully Protected Path*—check this box if you want CTC to route circuits only on protected paths. In other words, if a path cannot be a BLSR, UPSR, linear ADM, or PPM protected, CTC will not allow it to be used in the circuit if this box is checked.
- *Protected Drops*—If this box is checked, CTC only displays cards residing in 1:1, 1:N, or 1+1 protection for circuit source and destination selections.

Step 4 If the circuit is on a UPSR, set the UPSR Selector Defaults:

- *Revertive*—check this box if you want working traffic to revert back to its original path when the conditions that diverted it to the protect path are repaired. If it is not checked, working traffic remains on the protect path.
- *Reversion time*—if Revertive is checked, set the reversion time. This is the amount of time after which the traffic reverts back to the original working path when conditions causing the switch are cleared (the default is 5 minutes).
- *SF threshold*—set the UPSR Path-level signal failure BER thresholds.
- *SD threshold*—set the UPSR Path-level signal degrade BER thresholds.
- *Switch on PDI-P*—check this box if you want traffic to switch when an STS payload defect indicator is received.

Step 5 Click **Next**.

Step 6 In the Circuit Source dialog, set the circuit source.

Options include node, slot, port, STS, and VT/DS-1. The options displayed depend on the circuit type and circuit properties you selected and the cards installed in the node. For example, if the node does not have an XCVT card, VT circuits are not available for selection. For Ethergroups, see the "ONS 15454 Ethernet Circuit Configurations" section on page 7-16.

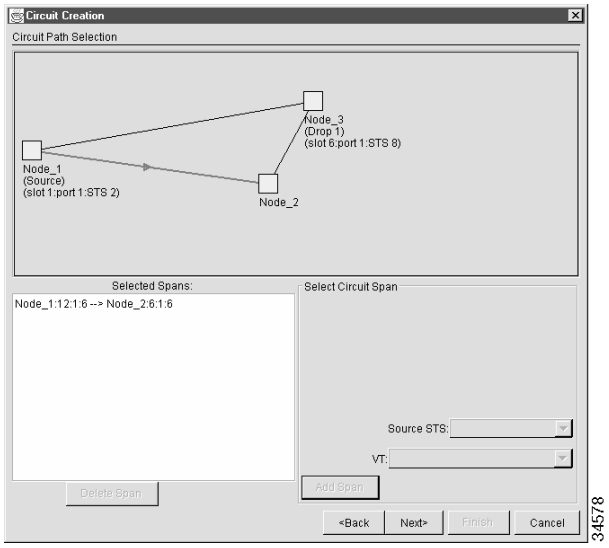
Click **Use Secondary Source** if you need to create a UPSR bridge/selector circuit entry point in a multivendor UPSR ring.

Step 7 Click **Next.**

Step 8 In the Circuit Destination dialog, enter the appropriate information for the circuit destination. Click **Use Secondary Destination** if you need to create a UPSR bridge/selector circuit destination point in a multivendor UPSR ring.

Step 9 Click **Next**. If you checked Route Automatically in Step 3, go to Step 10. If you did not check Route Automatically in Step 3, the Circuit Creation dialog is displayed (Figure 4-37). Follow Steps a – e to manually route your circuit path.

Figure 4-37 Circuit Path Selection Dialog



(a) Click the line of the span that will carry the circuit (the span turns white) and move the arrow so that it points from the source to the destination. To change the direction of the arrow, click the selected line again.

(b) Click **Source STS** or **VT** and select the source STS or VT.

(c) Click **Add Span**.

The span turns blue.

(d) Verify that the spans are correctly provisioned. The spans in the *Selected Spans* were added.

When provisioning a BLSR circuit, you only need to select one BLSR path from the source to the drop. If you are provisioning a UPSR, you can only select unprotected spans as paths. BLSR and 1+1 protected spans are not allowed. When selecting UPSR spans, select two different paths from source to drop. In Figure 4-37, the arrows would point from Node_1 to Node_2, Node_2 to Node_3, and from Node_1 to Node_3 (protect span).

Caution The ONS 15454 allows BLSR traffic to pass through an intermediate node on different STSs (for example, incoming traffic on STS-1, outgoing traffic on STS-2). However, if a pass-through node with incoming and outgoing traffic on different STSs becomes isolated (that is, multiple failures occur), the traffic supported by these STSs is not protected by the protection switch. Therefore, use the same STS/VT when passing traffic through a BLSR node.

(e) Click **Next**.

Step 10 In the Confirm Circuit Creation dialog, verify the circuit information.

Step 11 If the information is correct, click **Finish**.

If you entered more than 1 in *Number of Circuits* in the Circuit Attributes dialog, the Circuit Source dialog is displayed so you can create the remaining circuits. Otherwise, you are finished provisioning a circuit.

Note Ports must be placed in service before the circuits can carry traffic.

4.6.3 Creating Circuits With Multiple Drops

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.

Note When you create a unidirectional circuit, the card that does not have its backplane Rx input terminated with a valid input signal generates an LOS alarm. You cannot mask the alarm through CTC or through an internal hairpin connection. This will be addressed in a future release.

Procedure: Create a Circuit with Multiple Drops

Step 1 Create a unidirectional circuit by using the procedures in the "Create a Circuit" section on page 4-41. (To create a unidirectional circuit, deselect *Bidirectional* on the Circuit Creation dialog.)

Step 2 On the Circuits window, select the circuit and click **Edit**.

Step 3 On the Drops tab of the Edit Circuits dialog, select the circuit and click **Create**.

Step 4 On the Define New Drop dialog, complete the appropriate fields to define the new circuit drop: *Node, Slot, Port, STS, VT* (if applicable).

Step 5 Click **OK**.

Step 6 If you need to create additional drops, repeat Steps 3 – 5. If not, click **Close**.

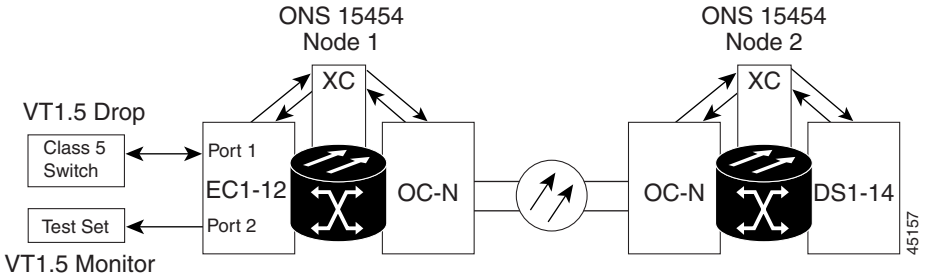
Step 7 Verify the new drops appear under the circuit's Destination column on the Circuits window.

4.6.4 Creating Monitor Circuits

You can set up secondary circuits to monitor traffic on primary circuits. You can create monitor circuits for bidirectional circuits only. For unidirectional circuits, simply create a drop to the port where the test equipment is attached. Figure 4-38 shows an example. At Node 1, a VT1.5 is dropped from Port 1 of an EC1-12 card. To monitor the VT1.5 traffic, test equipment is plugged into Port 2 of the EC1-12 and CTC is used to provision a circuit monitor to Port 2. Circuit monitors are one-way. The monitor in Figure 4-38 shows VT1.5 traffic received by the EC1-12. To monitor traffic sent from Node 1, a circuit monitor needs to be set up at Node 2.

Note Monitor circuits cannot be used with stitched Ethernet circuits.

Figure 4-38 Monitor Circuit Example



Procedure: Set Up a Monitor Circuit

Step 1 Log into CTC.

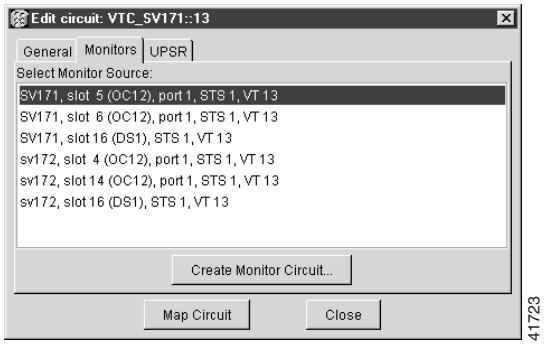
Step 2 In node view, select the **Circuits** tab.

Step 3 Select the circuit that you want to monitor. Click **Edit.**

Step 4 On the Edit Circuit dialog, select the **Monitors** tab (Figure 4-39).

The Monitors tab displays ports that you can use to monitor the circuit selected in Step 3.

Figure 4-39 Monitors Tab



Step 5 On the Monitors tab, select a port, then click **Create Monitor Circuit.**

Step 6 On the Circuit Creation dialog, select the destination node, slot, port, and STS for the monitored circuit. Click **Next.**

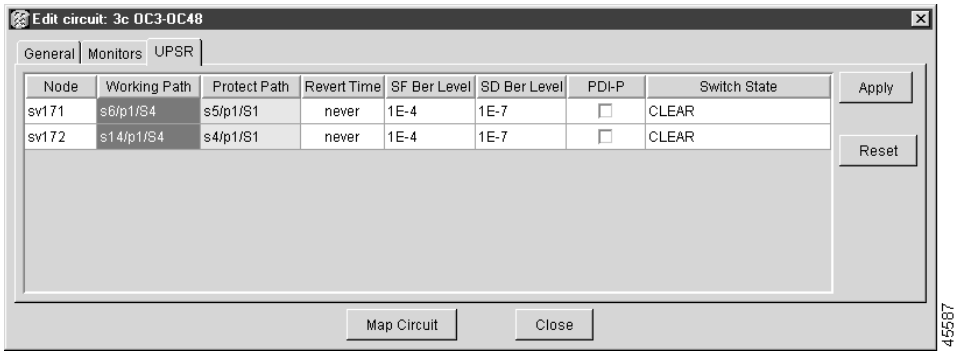
Step 7 On the Circuit Creation dialog confirmation, review the monitor circuit information. Click **Finish.**

Step 8 On the Edit Circuit dialog, click **Close.** The new monitor circuit displays on the Circuits tab.

4.6.5 Editing UPSR Circuits

To change UPSR selectors and switch protection paths, use the Edit Circuits dialog (Figure 4-40). You can view the UPSR circuit's working and protection paths, edit the reversion time, edit the Signal Fail/Signal Degrade thresholds, turn PDI-P on or off, and perform maintenance switches on the circuit selector. You can also display a map of the UPSR circuits to better see circuit flow between nodes.

Figure 4-40 Edit Circuit Dialog - UPSR Tab



Procedure: Edit UPSR Circuits

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 dialog, click the **UPSR** tab.

Step 5 Edit the UPSR selectors:

- *Reversion Time*—controls whether or not working traffic reverts back 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 after which traffic reverts back to the working path following repair of the working path.
- *SF BER Level*—sets the UPSR signal failure bit error rate threshold.
- *SD BER Level*—sets the UPSR signal degrade bit error rate threshold.
- *PDI-P*—when checked, traffic switches on STS payload defect indication path.
- *Switch State*—switches circuit traffic between the working and protect paths. The color of the Working Path and Protect Path fields indicate 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 FORCE and LOCKOUT commands override normal protective switching mechanisms. Applying these commands incorrectly might cause circuit outages.

Step 6 Click **Apply**.

Step 7 Click **Close.**

4.7 DCC Tunneling

SONET provides four data communications channels (DCCs) for network element operations, administration, maintenance, and provisioning: one on the SONET Section layer and three on the SONET Line layer. The ONS 15454 uses the Section DCC (SDCC) for ONS 15454 management and provisioning.

You can use the Line DCCs (LDCCs) and the SDCC (when the SDCC is not used for ONS 15454 DCC terminations) to tunnel third-party SONET equipment SDCCs across ONS 15454 networks. To create a DCC tunnel, you connect the tunnel end points from one ONS 15454 optical port to another. DCC traffic is forwarded transparently, byte-for-byte, across the ONS 15454 network. Each ONS 15454 can support up to 32 DCC tunnel connections. Table 4-5 shows the DCC tunnels that you can create.

Table 4-5 DCC Tunnels

DCC	SONET Layer	SONET Bytes	OC-3 (Ports 1 & 3)*	OC-12 (all ports)	OC-48 (all ports)
SDCC	Section	D1 - D3	Yes	Yes	Yes
Tunnel 1	Line	D4 - D6	No	Yes	Yes
Tunnel 2	Line	D7 - D10	No	Yes	Yes
Tunnel 3	Line	D11 - D12	No	Yes	Yes

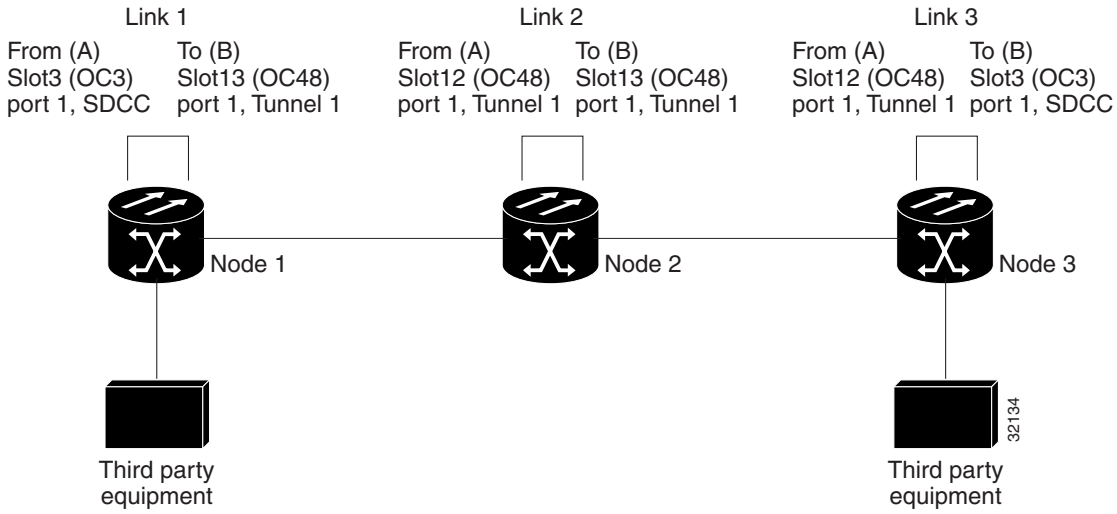
* You cannot use Ports 2 and 4 on OC-3 cards for DCC tunnels.

4.7.1 Creating DCC Tunnels

A DCC tunnel is a series of connection points that map a third-party equipment SDCC to ONS 15454 LDCCs. DCC tunnel end points are defined by slot, port, and DCC type (SDCC, Tunnel 1, Tunnel 2, or Tunnel 3). 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.

Figure 4-41 shows a DCC tunnel example. Third-party equipment is connected to OC-3 cards at Node 1, Slot 3, Port 1, and Node 3, Slot 3, Port 1. Each ONS 15454 node is connected by OC-48 trunk cards. In the example, three tunnel connections are created, one at Node 1 (OC-3 to OC-48), one at Node 2 (OC-48 to OC-48), and one at Node 3 (OC-48 to OC-3).

Figure 4-41 DCC Tunnel Example



Procedure: Provision a DCC Tunnel

Step 1 Log into an ONS 15454 that is connected to the non-ONS 15454 network.

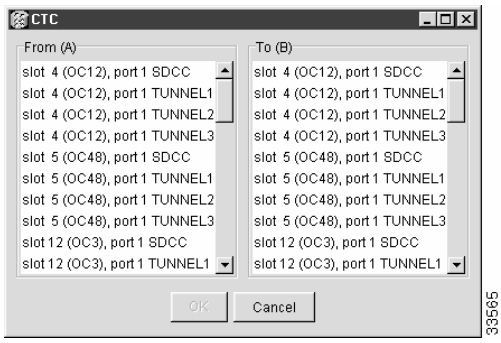
Step 2 Click the **Provisioning>Sonet DCC** tabs.

Step 3 Beneath the DCC Tunnel Connections area (bottom right of the screen), click **Create**.

Step 4 In the Create DCC Tunnel Connection dialog (Figure 4-42), 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 screen) for tunnel connections. These are used for ONS 15454 SDCCs.

Figure 4-42 Create DCC Tunnel Connection Dialog



Step 5 Click **OK**.

Step 6 The ports hosting the a DCC tunnel are not in service:

(a) Double click the card hosting the DCC in the shelf graphic or right click the card and select **Open**.

(b) Click the **Provisioning>Line** tabs.

(c) Under Status, select **In Service**.

(d) Click **Apply**.

DCC Provisioning is now complete for one slot/port. Repeat these steps for all slots/ports that are part of the DCC tunnel, including any intermediate nodes that will pass traffic through third party equipment. The procedure is confirmed when the third party network elements successfully communicate over the newly established DCC tunnel.

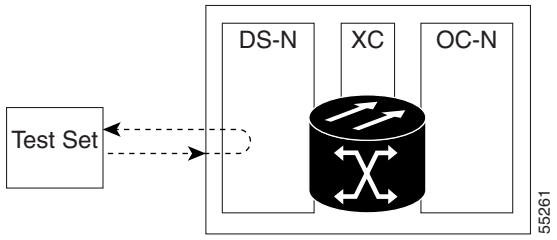
4.8 Loopbacks and Network Tests

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 15454 I/O cards, except Ethernet cards, allow loopbacks and hairpins.

4.8.1 Network Test Types

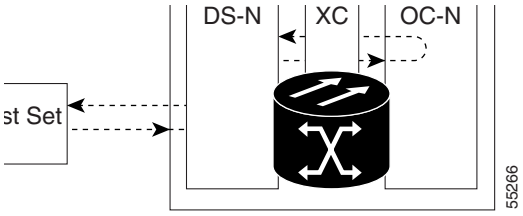
Facility loopbacks test the line interface unit (LIU) of a card, the backplane, and cabling. You put a facility loopback on a card and use a test set to run traffic over the loopback. A successful facility loopback eliminates the LIU of the card, backplane, and cabling plant as the cause or potential cause of a network problem. Figure 4-43 shows a facility loopback on a DS-N card.

Figure 4-43 The facility loopback process



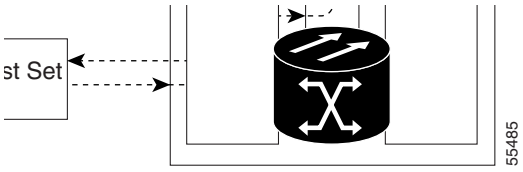
Terminal loopbacks test a circuit path through the XC card and loop back from the card that the terminal loopback is testing. Figure 4-44 shows a terminal loopback set on an OC-N card. The test set traffic comes in on the DS-N card and goes through the XC card to the OC-N card. The terminal loopback on the OC-N card turns the signal around before it reaches the LIU and sends it through the XC card to the DS-N card. This test verifies that the XC card and circuit paths are valid, but does not test the LIU on the OC-N card. To test the LIU 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 4-44 The terminal loopback process



Hairpin circuits bring 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 loopback, which would drop all traffic on the OC-N port. The hairpin allows you to test a circuit on nodes running live traffic.

Figure 4-45 The hairpin circuit process



4.8.2 Network Test Procedures

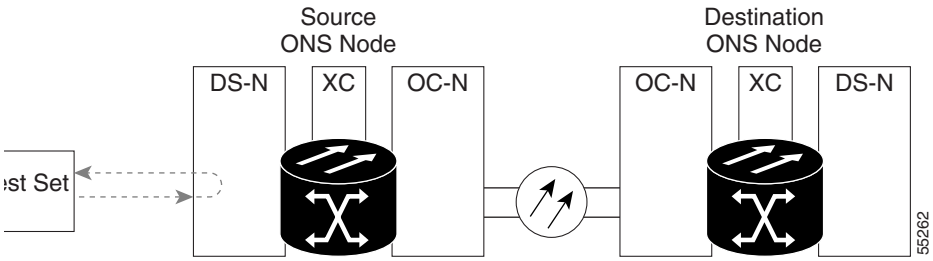
Facility loopbacks, terminal loopbacks, and hairpin circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a network test at each point along the circuit path systematically eliminates possible points of failure. In our example, we test a DS-N circuit on a two node BLSR. Using a series of facility loopbacks, terminal loopbacks, and hairpins, we trace the path of the circuit and eliminate possible points of failure.

A logical progression of five network test procedures apply to this scenario: a facility loopback on the source node DS-N card, a hairpin on the source node DS-N card, a hairpin on the destination node OC-N card, a terminal loopback to the destination node DS-N card, and a facility loopback to the destination DS-N card.

Procedure: Perform a Facility Loopback on a Source DS-N Card

The first loopback test is a facility test performed on the first card in the circuit; in this example, the DS1-14 card in source node. Completing a successful facility loopback on this card eliminates the cabling, DS-N card, and the backplane as possible failure points.

Figure 4-46 Facility loopback on a source DS-N card



Caution Performing a loopback on an in-service circuit is service affecting.

Note Loopbacks operate only on in-service ports.

Step 1 Test the test set with a hard loop.

To perform a hard loop, bridge the test set transmit (Tx) and receive (Rx) terminals with a cable and send traffic across this loop to ensure that the test set works.

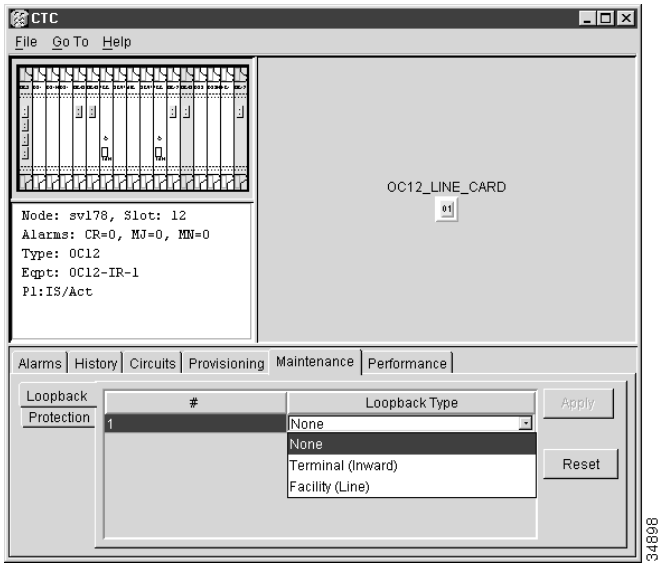
Step 2 Use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals of the test set to the backplane connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Setup the test set accordingly.

Step 3 In node view, double-click the loopback card where you will perform the loopback.

Step 4 Click the **Maintenance > Loopback** tabs.

Step 5 On the Loopback subtab, select **Facility (Line)** from the Loopback Type column for the port being tested.

Figure 4-47 Performing a facility loopback



Step 6 Click **Apply**.

Step 7 On the confirmation dialog box, click **Yes.**

Note It is normal for an alarm to appear during loopback setup. The alarm clears when you remove the loopback.

Step 8 If the test set is not already sending traffic, send test set traffic on the loopback circuit.

Step 9 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 10 If the test set indicates a good circuit:

(a) Clear the Facility Loopback:

- On the Loopback subtab, select **None** from the Loopback Type column.
- Click **Apply**.

(b) Skip to the second procedure (the "Perform a Hairpin on a Source Node" section on page 4-54).

Step 11 A faulty circuit signifies a problem with the DS-N card, the cabling from the DS-N card to the DSx panel, or the backplane. Test the DS-N cabling, the DS-N card, and then the backplane.

Step 12 To test the cabling:

(a) Replace the suspect cabling (the cables from the test set to the backplane ports) with a known good cable.

(b) If a known good cable is not available, test the suspect cable with a test set. Remove the suspect cable from the backplane and connect the cable to the transmit (Tx) and receive (Rx) of the test set. Run traffic to determine whether the cable is good or suspect.

(c) Resend test set traffic on the loopback circuit with a known good cable installed.

(d) If the circuit is now good, the problem was probably the defective cable. Replace this cable and skip to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 4-59.

Step 13 To test the card:

(a) Replace the suspect card with a known good card.

(b) Resend test set traffic on the loopback circuit with a known good card.

(c) If the circuit is now good, the problem was probably the defective card. Replace the suspect card and skip to the"Perform a Terminal Loopback on a Destination DS-N Card" section on page 4-59.

(d) 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.

Step 14 If the loopback test fails with a known good cable and a known good card, then the backplane is suspect.

(a) Repeat the facility loopback test for the DS-N card, but use a different port. This requires setting up a new facility loopback on CTC for the new port and running cables from the test set to the new port.

(b) If the loopback test on the new port fails, the entire backplane is suspect.

(c) If the loopback test succeeds on the new port, the backplane problem may be limited to the original port.

(d) No user-serviceable operations exist for the backplane. Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case for the backplane. Tell them whether the entire backplane is suspect or only specific ports.

(e) Replace the backplane.

(f) Resend test set traffic on the loopback circuit with known good cabling, a known good card, and the replacement backplane.

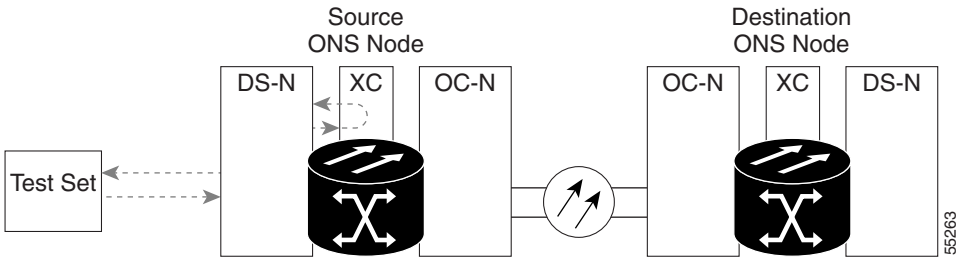
(g) If the circuit is now good, the problem was probably the defective backplane. Skip to the "Perform a Hairpin on a Source Node" section on page 4-54.

Step 15 Clear any loopback before testing the next segment of the circuit path.

Procedure: Perform a Hairpin on a Source Node

The second loopback test is a hairpin circuit performed on the first XC card in the circuit. Completing a successful loopback through this card eliminates the possibility that the source XC card is the reason for the faulty circuit.

Figure 4-48 Hairpin on a source node



Note The ONS 15454 does not support simplex operation on the XC/XCVT card. Two XC/XCVT cards must be installed for each node.

Step 1 Test the test set with a hard loop if you have not already done so.

To perform a hard loop, bridge the test set transmit (Tx) and receive (Rx) terminals with a cable and send traffic across this loop to make the test set work.

Step 2 If you just completed the prior procedure, Perform a Facility Loopback on a Source DS-N Card, page 4-51, leave the electrical test set hooked up to the DS-N card.

Step 3 If you are starting the current procedure without the electrical test set hooked up to the DS-N card, use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the backplane connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Set up the test set accordingly.

Step 4 Click the **Circuits** tab and click the **Create** button.

Step 5 Give the circuit an easily-identifiable name, such as hairpin1.

Step 6 Set the Circuit **Type** and **Size** to your normal preferences.

Step 7 Uncheck the **Bidirectional** check box and click **Next**.

Step 8 In the Circuit Source dialog box, fill in the same card and port where you performed the first loopback test. The DS-N card in the source node.

Step 9 Click **Next**.

Step 10 In the Circuit Destination dialog box, use the same card and port used for the source information.

Step 11 Click **Finish**.

Step 12 Confirm that the newly-created circuit appears with a direction column noting that this circuit is 1-way.

Step 13 If the test set is not already sending traffic, send test set traffic on the loopback circuit.

Step 14 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 15 If the test set indicates a good circuit, skip to the "Perform a Hairpin on a Destination Node" section on page 4-56.

Step 16 If the test traffic is not received or is poor quality, there may be a problem with the XC card.

Caution XC manual switches (side switches) are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

Step 17 Perform a software reset on the standby XC/XCVT card:

(a) Determine the standby XC card. On both the physical node and the CTC screen, the ACT/STBY LED of the standby XC card is yellow, and the ACT/STBY LED of the active XC card is green.

(b) Position the cursor over the standby XC/XCVT card.

(c) Right-click to choose **RESET CARD**.

Step 18 Do a manual switch (sideswitch) of the XC cards and retest the circuit:

(a) Determine the standby XC card. The ACT/STBY LED of the standby XC card is yellow, and the ACT/STBY LED of the active XC card is green.

Note Place the cursor on top of the card graphic to display a dialog. This display identifies the card as *XC: Active* or *XC: Standby.*

(b) In the node view, select the **Maintenance > XC/XCVT Cards** tabs.

(c) From the Cross Connect Cards menu, choose **Switch**.

(d) Click **Yes** on the Confirm Switch dialog box.

Note After the active XC/XCVT goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

(e) Resend test set traffic on the loopback circuit.

Now the test set traffic goes through the alternate XC card.

(f) 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.

(g) If the signal received by the test set is still faulty or non-existent, assume the XC card is not causing the problem. Skip to Step j of this procedure.

(h) If the circuit is now good, the problem could be a defective card. To confirm a defective original XC card:

- Redo the manual switch (sideswitch) procedure to make the original active XC card again the active card.
- Resend test set traffic on the loopback circuit.
- If the signal received by the test set is still faulty or non-existent, return the defective card to Cisco. Call the Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.

- If the circuit is now good, the XC card may have had a temporary problem that was cleared by the sideswitch.

(i) Replace the defective XC card.

(j) Click the **Circuits** tab.

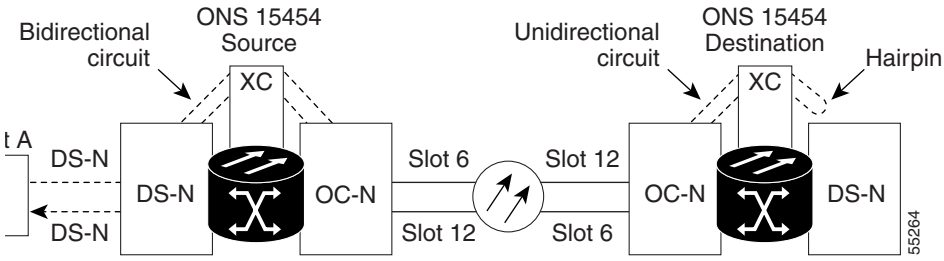
(k) Highlight the newly-created hairpin circuit and click **Delete**.

(l) Go to the "Perform a Hairpin on a Destination Node" section on page 4-56.

Procedure: Perform a Hairpin on a Destination Node

The third test is a hairpin circuit on the XC card in the destination node. To perform this test, first create a bidirectional circuit from the source DS-N 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 destination XC card, or the fiber span is responsible for the faulty circuit.

Figure 4-49 Hairpin on a destination node



Step 1 Test the test set with a hard loop if you have not done so.

Note To perform a hard loop, bridge the test set transmit (Tx) and receive (Rx) terminals with an appropriate cable and send traffic across this loop to ensure the test set works.

Step 2 If you are starting the current procedure with the electrical test set hooked up to the DS-N card, leave the test set hooked up.

Step 3 If you are starting the current procedure without the electrical test set hooked up to the DS-N card, use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the backplane connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Set up the test set accordingly.

Step 4 To create the first circuit, click the **Circuits** tab and click the **Create** button.

Step 5 Give the circuit an easily-identifiable name, such as bidirectional1.

Step 6 Select the appropriate circuit type, VT or STS-1.

Step 7 Leave the **Bidirectional** check box checked and click **Next**.

Step 8 In the Circuit Source dialog box, fill in the same card and port where you performed the first loopback test (the DS-N card in the source node).

Step 9 Click **Next**.

Step 10 In the Circuit Destination dialog box, use the source node OC-N card and port.

Step 11 Click **Next** and **Finish**.

Step 12 Confirm that the newly-created circuit appears with a direction column showing a 2-way circuit.

Step 13 Log into the destination node.

Step 14 For the second circuit, click the **Circuits** tab and click the **Create** button.

Step 15 Give the circuit an easily-identifiable name, such as hairpin2.

Step 16 Set Circuit **Type** and **Size** to your normal preferences.

Step 17 Uncheck the **Bidirectional** check box and click **Next**.

Step 18 In the Circuit Source dialog box, fill in the destination OC-N card and port.

Step 19 Click **Next**.

Step 20 In the Circuit Destination dialog box, use the same card and port from the Circuit Source dialog box.

Step 21 Click **Finish**.

Step 22 Confirm that the second newly-created circuit appears with a direction column noting a 1-way circuit.

Step 23 Double-click the circuit to display the network view.

Step 24 Verify that the circuits connect to the correct slots. For example, source node/Slot 6 (east slot) to destination node/Slot 12(west slot). If two east 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 25 If the test set is not already sending traffic, send test set traffic on the loopback circuit.

Step 26 Examine the test traffic received by the test set. Look for errors or any other signal information indicated by the test set.

Step 27 If the test set indicates a good circuit, skip to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 4-59.

Step 28 If the test traffic is not received or is poor quality, a problem may exist with the destination XC card, the source or destination OC-N card, or the fiber span. Test the destination XC card, then the OC-N cards, and then test the fiber span.

Caution XC manual switches (side switches) are service-affecting. Any live traffic on any card in the node will endure a hit of up to 50 ms.

Step 29 Perform a software reset on the standby XC/XCVT card:

(a) Determine the standby XC card. On both the physical node and the CTC screen, the ACT/STBY LED of the standby XC card is yellow, and the ACT/STBY LED of the active XC card is green.

(b) Position the cursor over the standby XC/XCVT card.

(c) Right-click to choose **RESET CARD**.

Step 30 Do a manual switch (sideswitch) of the XC cards and retest the circuit:

(a) In the node view, select the **Maintenance > XC/XCVT Cards** tabs.

(b) From the Cross Connect Cards menu, choose **Switch**.

(c) Click **Yes** on the Confirm Switch dialog box.

Note After the active XC/XCVT goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

(d) Resend test set traffic on the loopback circuit.

Now the test set traffic routes through the alternate XC card.

(e) 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.

(f) If the signal received by the test set is still faulty or non-existent, assume the XC card is not causing the problem. Skip to Step k of this procedure.

(g) If the circuit is now good, the problem could be a defective card. To confirm a defective original XC card:

- Redo the manual switch (sideswitch) procedure to make the original active XC card again the active card.
- Resend test set traffic on the loopback circuit.
- If the signal received by the test set is still faulty or non-existent, return the defective card to Cisco. Call the Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- If the circuit is now good, the XC card may have had a temporary problem that was cleared by the sideswitch.

(h) Replace the defective XC card.

(i) Click the **Circuits** tab.

(j) Resend test set traffic on the loopback circuit.

The test set traffic routes through the alternate XC card rather than the original XC card.

(k) Examine the received test set traffic. Look for errors or any other signal information that the test set is capable of indicating.

(l) If the signal received by the test set is still faulty or non-existent, assume the problem does not lie in a faulty XC card and skip to Step 31 of this procedure.

(m) If the circuit is now good, the problem could be a defective card. To confirm a defective original XC card:

- Repeat the manual switch (side switch) procedure to make the original active XC card again the active card.
- Resend test set traffic on the loopback circuit.
- If the signal received by the test set is still faulty or non-existent, return the defective card to Cisco. Call the Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.
- If the circuit is now good, the XC card may have had a temporary problem that is now cleared by the sideswitch.

(n) Replace the defective XC card.

(o) Click **Apply** and click the **Circuits** tab.

Step 31 To eliminate the possibility of faulty OC-N cards:

(a) Replace the suspect source OC-N card with a known good card.

(b) Resend test set traffic on the loopback circuit with a known good card.

(c) If the circuit is now good, the problem was probably the defective card. Return the defective card to Cisco. Call the Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.

(d) Repeat steps a – b for the suspect destination OC-N card.

(e) Skip to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 4-59.

If the test traffic is not received or is poor quality and the OC-N card is a known good card, then the fiber span is suspect.

Step 32 If you now have a valid fiber span, resend test set traffic on the loopback circuit.

Step 33 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 34 If you do not have a valid test signal or a valid fiber span, try to obtain access to another known good span, hook the source and destination OC-N cards to the known good span, and resend the test signal.

Step 35 If you do not have a valid signal with a known good span, valid OC-N cards, and a valid XC card, repeat the "Perform a Hairpin on a Destination Node" section on page 4-56 to try and determine the problem or call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368 and explain the situation.

Step 36 If you have a valid test signal with the known good span, replace or fix the original fiber span to obtain a valid circuit. Then, go to "Perform a Hairpin on a Destination Node" section on page 4-56

Step 37 Highlight the newly-created hairpin circuit.

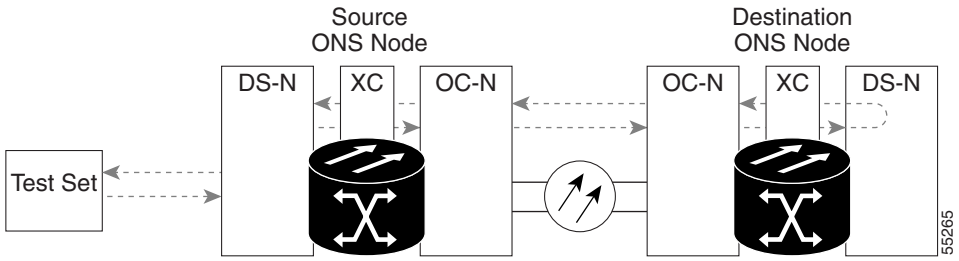
Step 38 Click **Delete**.

Step 39 Go to the "Perform a Terminal Loopback on a Destination DS-N Card" section on page 4-59.

Procedure: Perform a Terminal Loopback on a Destination DS-N Card

The fourth test is a terminal loopback performed on the fourth I/O card in the circuit; in this example the DS-N card in the destination node. 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 DS-N card eliminates the possibility that this card is responsible for the faulty circuit.

Figure 4-50 Terminal loopback on a destination DS-N card



Caution Performing a loopback on an in-service circuit is service affecting.

Step 1 Test the test set with a hard loop if you have not already done so.

To perform a hard loop, bridge the test set transmit (Tx) and receive (Rx) terminals with an appropriate cable and send traffic across the loop to ensure the test set works.

Step 2 If you are starting the current procedure with the electrical test set hooked up to the DS-N card in the source node, leave the test set hooked up.

Step 3 If you are starting the current procedure without the electrical test set hooked up to the DS-N card in the source node, use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the backplane connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Setup the test set accordingly.

Step 4 Click the **Circuits** tab and click the **Create** button.

Step 5 Give the circuit an easily-identifiable name, such as DSNtoDSN.

Step 6 Set Circuit **Type** and **Size** to your normal preferences.

Step 7 Leave the **Bidirectional** check box checked and click **Next**.

Step 8 In the Circuit Source dialog box, fill in the same card and port where you performed the first loopback test (the DS-N card in the source node).

Step 9 Click **Next**.

Step 10 In the Circuit Destination dialog box, use the DS-N card and port in the destination node.

Step 11 Click **Finish**.

Step 12 Confirm that the newly created circuit appears on a Circuits screen row with a direction column that shows a 2-way circuit.

Step 13 In node view, double-click the card that requires the loopback. In this example, the DS-N card in the destination node.

Step 14 Click the **Maintenance > Loopback** tabs.

Step 15 On the Loopback subtab, select **Terminal (Inward)** from the Loopback Type column.

Step 16 Click **Apply**.

Step 17 On the confirmation dialog box, click **Yes.**

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 18 If the test set is not already sending traffic, send test set traffic on the loopback circuit.

Step 19 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 20 If the test set indicates a good circuit, skip to the "Perform a Facility Loopback on a Destination DS-N Card" section on page 4-61.

Step 21 If the test traffic is not received or is poor quality, then test the DS-N card.

(a) Replace the suspect card with a known good card.

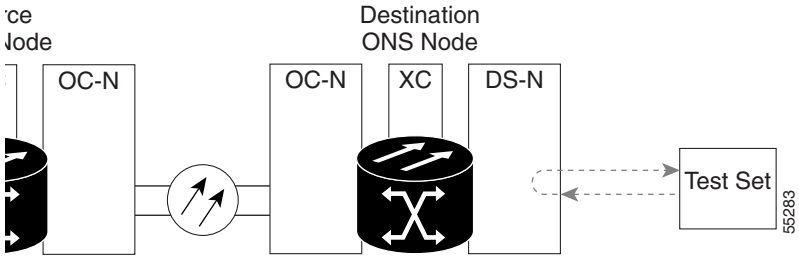
(b) Resend test set traffic on the loopback circuit with a known good card.

(c) If the circuit is now good, the problem was probably the defective card. Replace the suspect card and return the defective card to Cisco. Call the Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.

Procedure: Perform a Facility Loopback on a Destination DS-N Card

The final test is a facility loopback performed on the last card in the circuit; in this case the DS-N card in the destination node. Completing a successful facility loopback on this card eliminates the possibility that the destination node cabling, DS-N card, LIU, or backplane is responsible for a faulty circuit.

Figure 4-51 Facility loopback on a destination DS-N card



Caution Performing a loopback on an in-service circuit is allowed but is service affecting.

Note Loopbacks operate only on in-service ports.

Step 1 Test the test set with a hard loop if you have not already done so.

To perform a hard loop on the test set, bridge the test set transmit (Tx) and receive (Rx) terminals with an appropriate cable and send traffic across this loop to make the test set works.

Step 2 Use appropriate cabling to attach the electrical test set transmit (Tx) and receive (Rx) terminals to the backplane connectors or DSx panel for the port you are testing. Both transmit (Tx) and receive (Rx) connect to the same port. Set up your test set accordingly.

Step 3 In node view, double-click the card where you will perform the loopback.

Step 4 Click the **Maintenance > Loopback** tabs.

Note Loopbacks operate only on in-service ports.

Step 5 On the Loopback subtab, select **Facility (Line)** from the Loopback Type column for the port being tested.

Step 6 Click **Apply**.

Step 7 On the confirmation dialog box, click **Yes.**

Note It is normal for an alarm to appear during loopback. The alarm clears when you remove the loopback.

Step 8 If the test set is not already sending traffic, send test set traffic on the loopback circuit.

Step 9 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 10 If the test set indicates a clean circuit:

(a) Clear the Facility Loopback:

- On the Loopback subtab, select **None** from the Loopback Type column.
- Click **Apply**.

(b) The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

Step 11 If the test traffic is not received or is poor quality, there is a problem with the DS-N card, the cabling from the DS-N card, or the backplane. Test the DS-N cabling first, the DS-N card next, and the backplane last.

Step 12 To test the cabling:

(a) Replace the suspect cabling (the cables from the test set to the backplane ports) with a known good cable.

(b) If a known good cable is not available, you can test the suspect cable with a test set. Remove the suspect cable from the backplane and connect the cable to the transmit (Tx) and receive (Rx) of the test set. Run traffic to determine whether this is a good cable.

(c) Resend test set traffic on the loopback circuit with a known good cable installed.

(d) If the circuit is now good, the problem was probably the defective cable. Replace this cable.

(e) Skip to Step 14.

Step 13 To test the card:

(a) Replace the suspect card with a known good card.

(b) Resend test set traffic on the loopback circuit with a known good card.

(c) If the circuit is now good, the problem was probably the defective card. Replace the defective card.

(d) Return your defective card to Cisco. Call the Technical Assistance Center (TAC) at 1-877-323-7368 to open an RMA case.

Step 14 If the loopback test fails with a known good cable and known good card, then the backplane is suspect.

(a) Repeat the facility loopback test for the DS-N card, but use a different port. This will require setting up a new facility loopback on CTC for the new port and running cables from the test set to the new port.

(b) If the loopback test on the new port fails, the entire backplane is suspect.

(c) If the loopback test succeeds on the new port, the backplane problem may be limited to the original port.

(d) No user-serviceable operations exist for the backplane. Call the Cisco technical assistance center (TAC) at 1-877-323-7368 to open an RMA case on the backplane. Make sure to include whether the entire backplane is suspect or only specific ports.

(e) Replace the backplane.

(f) Resend test set traffic on the loopback circuit with known good cabling, a known good card, and the replacement backplane.

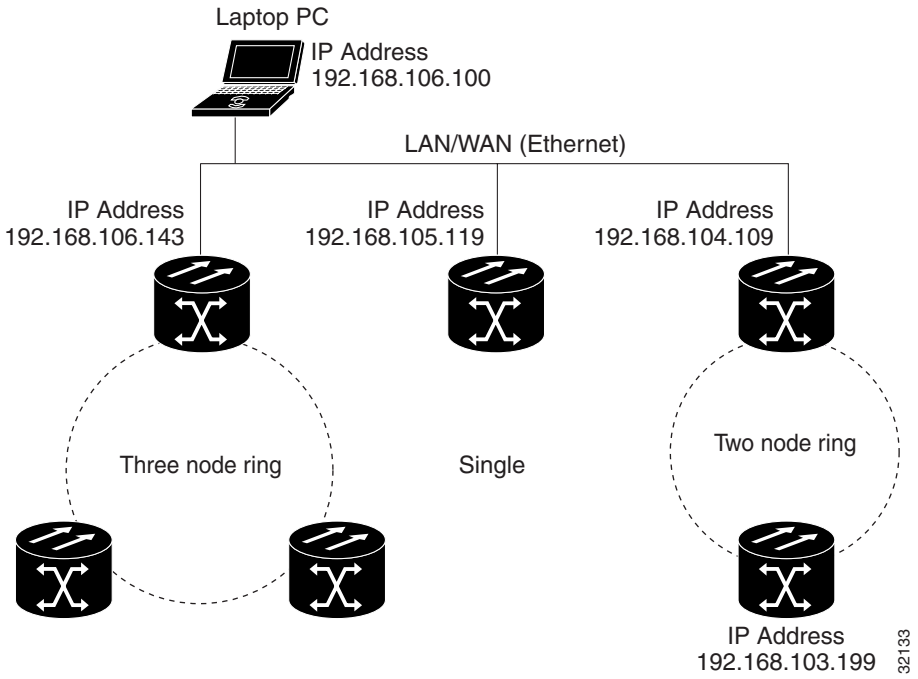
(g) If the circuit is now good, the problem was probably the defective backplane.

Step 15 The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

4.9 Managing Multiple ONS 15454 Rings

A small modification to the CMS.INI file enables CTC to manage multiple rings or nodes that are connected only by Ethernet and not interconnected by fiber or the DCC. Figure 4-52 shows a multiple ONS 15454 ring. An ONS 15454 with an unmodified CMS.INI file can only manage the ONS 15454 that the PC dialed directly into and the three node ring attached to that ONS 15454. The file cannot manage the single node and two-node ring that are not optically connected to the dialed into ONS 15454. However, you can modify the CMS.INI file to manage the additional single node and two node ring.

Figure 4-52 CTC Multiple Ring Management



Procedure: Enable Multiple Ring Management

The following procedure shows how to enable CTC for multiple ring management. To enable multiple ring management, the CTC software must be installed and launched.

Caution Close all CTC sessions before modifying the CMS.INI file.

Step 1 from the Windows Start menu, select **Find>Files or Folder**.

Step 2 In the **Find** dialog, type CMS.INI in the *Named* field. Click **Find Now**.

Step 3 Double-click the located file to bring up Microsoft Notepad or a similar text-editing program. Example text from an unmodified CMS.INI file is shown below:

#CTC Preferences File

#Tue Aug 8 15:00:27 PDT 2000

CMS_LAUNCHER.CmsJarPath=C\:\\TEMP\\CMS51877.jar

CMS.LastHost=192.168.106.143

Step 4 Record on paper the IP addresses for the rings and nodes that connect directly to the Ethernet. Do not record IP addresses that connect to the Ethernet through another node on the ring.

Note All nodes in a ring can connect directly to the Ethernet; in this case any node IP address in the ring can be used.

In this example, record IP addresses 192.168.105.119 and 192.168.104.109 because they connect directly to the Ethernet. Do not record the IP address 192.168.103.199 because it does not connect directly to the Ethernet. The IP address 192.168.103.199 connects via the ring to 192.168.104.109, which connects to the Ethernet.

Step 5 After recording the IP addresses, close any open CTC sessions and edit the CMS.INI file text by adding an additional line below the next line that contains the date.

The added line reads **Topology.Hosts=**(first IP address to manage through Ethernet)**\n**(second IP address to manage through Ethernet)**\n**(third IP address to manage through Ethernet), etc. In the example, the additional line reads: **Topology.Hosts=192.168.106.143\n192.168.105.119\n192.168.104.109.** The modified CMS.INI text is:

#CTC Preferences File

#Tue Aug 8 15:00:27 PDT 2000

Topology.Hosts=192.168.106.143\n192.168.105.119\n192.168.104.109

CMS_LAUNCHER.CmsJarPath=C\:\\TEMP\\CMS51877.jar

CMS.LastHost=192.168.106.143

Note The IP address used for the node ring directly connected to the PC does not need to be entered in the added line. This IP address is already present in the bottom line of the CMS.INI file.

Step 6 Save and close the modified CMS.INI. file.

Step 7 Launch CTC and view the separate configurations in one CTC network view.

4.10 Creating Diagnostic Files

When working with ONS 15454 customer support, you might need to record system information to a file for diagnosis by technical personnel.

Procedure: Create a Diagnostic File

Step 1 Select the **Maintenance>Diagnostic** tabs.

Step 2 Click **Diagnostic**.

Step 3 In the Save dialog, type a file name. Do not add an extension to the file name; the CTC extension is added automatically.

Step 4 Choose a directory where you want to save the file.

Step 5 Click **Save**. A dialog confirms a successful file transfer. (The dialog can take 20-30 seconds to display.)

Step 6 E-mail the diagnostic file to the address given to you by customer support.

Provisioning Cards

This chapter provides procedures to configure ONS 15454 electrical cards, optical cards, and the Alarm Interface Controller card. The chapter also tells you how to upgrade the XC card to an XCVT card and convert the DS1-14 and DS3-12 cards from 1:1 to 1:N protection.

5.1 Provisioning Electrical Cards

The DS1-14, DS1N-14, DS3-12, DS3N-12, DS3XM-6, and EC1-12 cards are pre-provisioned with settings that you can modify to manage transmission quality. To provision electrical card settings, open the card in CTC and select the **Provisioning** tab. Use the subtabs to provision the line, line threshold, line electrical path, and SONET thresholds.

5.1.1 Card Settings

The Line subtab is where you set transmission line settings, including line type, coding, length, and status. Figure 5-1 shows the Line subtab for the DS1-14 card. Table 5-1 shows the available electrical card line settings.

Figure 5-1 Line Subtab

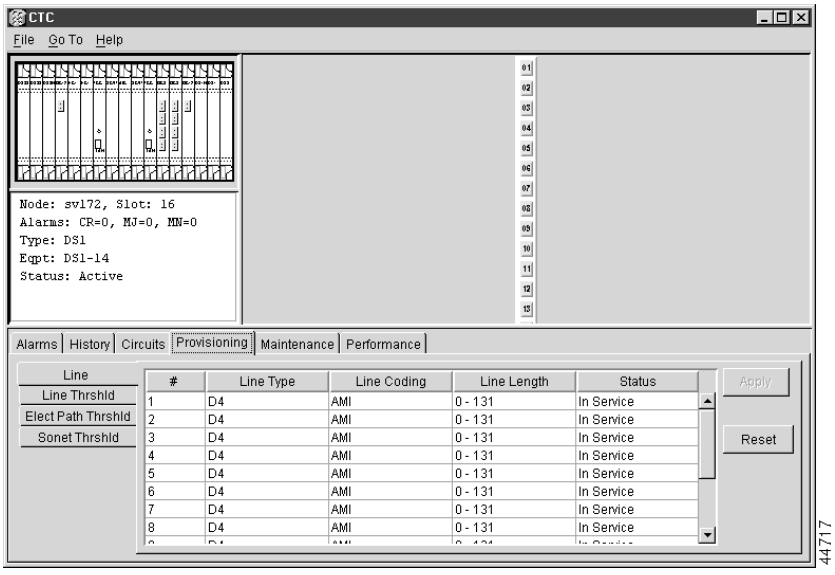


Table 5-1 Line Settings - Electrical

Heading	Description	Options
#	Port number	• 1 - 6 (DS3XM-6) • 1 - 12 (DS3-12, DS3N-12, EC1-12) • 1 - 14 (DS1-14, DS1N-14)
Line Type	Defines the line framing type	• D4 (default) • ESF - Extended Super Frame • Unframed • M13 - DS3XM-6 only • C BIT - DS3XM-6 only; default
Line Coding	Defines the DS-1 transmission coding type that is used	• AMI - Alternate Mark Inversion (default) • B8ZS - Bipolar 8 Zero Substitution • B3ZS - DS3XM-6 only, default
Line Length	Defines the distance (in feet) from backplane connection to the next termination point	DS-1: • 0 - 131 (default) • 132 - 262 • 263 - 393 • 394 - 524 • 525 - 655 DS-3. DS3XM-6 • 0 - 225 (default) • 226 - 450
Status	Places port in or out of service	Out of Service (default) In Service
PJ Sts Mon # (EC1-12 only)	Sets the STS that will be used for pointer justification. If set to zero, no STS is used	0 (default) 1
Line Buildout (EC1-12 only)	Defines the distance (in feet) from backplane to next termination point	• 0 - 225 (default) • 226 - 450
Rx Equalization (EC1-12 only)	For early EC1-12 card versions, equalization can be turned off if the line length is short or the environment is extremely cold; Rx Equalization should normally be set to On	On (checked, default) Off (unchecked)

Table 5-2 shows electrical card threshold settings for all ONS 15454 electrical cards except the DS3XM-6. Table 5-3 shows the DS3XM-6 card thresholds. The default values are based on threshold recommendations in GR-820-CORE, Sections 4.0 (DS-1) and 5.0 (DS-3).

Table 5-2 Threshold Settings - Electrical

Heading	Description	Options
#	Port number	• 1 - 12 (DS3-12, DS3N-12, EC1-12) • 1 - 14 (DS1-14, DS1N-14)

Table 5-2 Threshold Settings - Electrical (continued)

Heading	Description	Options
CV	Coding violations	Numeric. Defaults (15 min/1 day): • 13,340/133,400 (DS-1) • 387/3,865 (DS-3) • 1,312/13,120 (EC-1)
ES	Errored Seconds	Numeric. Defaults (15 min/1 day): • 65/648 (DS-1) • 25/250 (DS-3) • 87/864 (EC-1)
SES	Severely Errored Seconds	Numeric. Defaults (15 min/1 day): • 10/100 (DS-1) • 4/40 (DS-3) • 1/4 (EC-1)
SAS	Severely Errored Frame/Alarm Indication Signal	Numeric. Default (15 min/1 day): • 2/17 (DS-1)
UAS	Unavailable Seconds	Numeric. Default (15 min/1 day): • 3/10 (all cards)
AIS	Alarm Indication Signal	Numeric. Default (15 min/1 day): • 10/10 (DS-1)
Loss	Loss of signal	Numeric. Default (15 min/1 day): • 10/10 (DS-3)
PJ	Pointer Justification	Numeric. Defaults (15 min/1 day): • 60/5,760 (EC-1 Near End) • 0/0 (EC-1 Far End)
SEFS	Severely errored frame seconds	Numeric. Defaults (15min/1 day): • 500/5,000 (EC-1 Near End) • 0/0 (EC-1 Far End)
SF BER Level	Sets the signal fail bit error rate	EC-1 card only: • 1E-3 • 1E-4 (default) • 1E-5
SD BER Level	Sets the signal degrade bit error rate	EC-1 card only: • 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9

Table 5-3 Threshold Settings - DS3XM-6 Card

Heading	Description	Options
#	Port number	• 1 - 6
CV	Coding violations	Numeric. Defaults (15 min/1 day): • 387/3,865 (Line) • 382/3,820 (Electrical Path - DS-3, Near and Far End))
ES	Errored Seconds	Numeric. Defaults (15 min/1 day): • 25/250 (Line) • 25/250 (Electrical Path - DS-3, Near & Far End) • 65/648 (Electrical Path - DS-1 Near End) • 0/0 (Electrical Path - DS-1, Far end)
SES	Severely Errored Seconds	Numeric. Defaults (15 min/1 day): • 4/40 (Line) • 4/40 (Electrical Path - DS-3, Near and Far End) • 10/100 (Electrical Path - DS-1 Near End) • 0/0 (Electrical Path - DS-1, Far end)
SAS	Severely Errored Frame/Alarm indication Signal	Numeric. Defaults (15 min/1 day): • 2/8 (Electrical Path - DS-3, Near & Far End) • 2/17 (Electrical Path - DS-1 Near End) • 0/0 (Electrical Path - DS-1, Far end)
UAS	Unavailable Seconds	Numeric. Defaults (15 min/1 day): • 10/10 Electrical Path, DS-1, Near End; DS-3; Near & Far End • 0/0 Electrical Path, DS-1 Far End
AIS	Alarm Indication Signal	Numeric. Defaults (15 min/1 day): • 10/10 Electrical Path, DS-1, Near End; DS-3; Near & Far End • 0/0 Electrical Path, DS-1 Far End
Loss	Loss of signal	Numeric. Default (15 min/1 day): • 10/10 (Line)

5.1.2 Provisioning DS3XM-6 Cards

The DS3XM-6 transmux card can accept up to six DS-3 signals and convert each to 28 VT1.5s. Conversely, it can take 28 T-1s and multiplex them into a channeled CBIT or M23 framed DS-3. Unlike the DS3-12 and DS3N-12 cards, the DS3XM-6 allows circuit mapping at the VT level. To provision a DS3XM-6 card, perform three basic steps:

- Set up the protection groups
- Set up the circuits
- Provision the ports

Procedure: Set Up DS3XM-6 Protection Groups

Step 1 Click the **Provisioning>Protection** tabs.

Step 2 Click **Create**.

Step 3 In the Create Protection Group dialog, type the name for the protection group in the *Name* field (optional).

Step 4 Click **Type** and choose 1:1 from the pull-down menu. (1:1 is the only type of protection available for the DS3XM-6 card.)

Note For 1:1 protection groups, install the protect card in an odd-numbered slot and the working card in an even-numbered slot that follows the protect slot.

Step 5 Click **Protect Card** and select the protect card from the pull-down menu.

The selected card will appear in the Protect Card field.

Step 6 To select the working card, click the card and click the arrow tab (>>) to move the card from the Available side to the Working side.

Step 7 Click **OK**.

After you set up the protection groups for the DS3XM-6 card, set up the circuits. For circuit provisioning procedures, see the "Creating and Provisioning Circuits" section on page 4-40. Setting up circuits for the DS3XM-6 is identical to other cards.

Procedure: Provision the DS3XM-6 Ports

Step 1 To open the DS3XM-6 card, either double click or right click the card and choose **Open** from the list of options.

Step 2 Click the **Provisioning** tab.

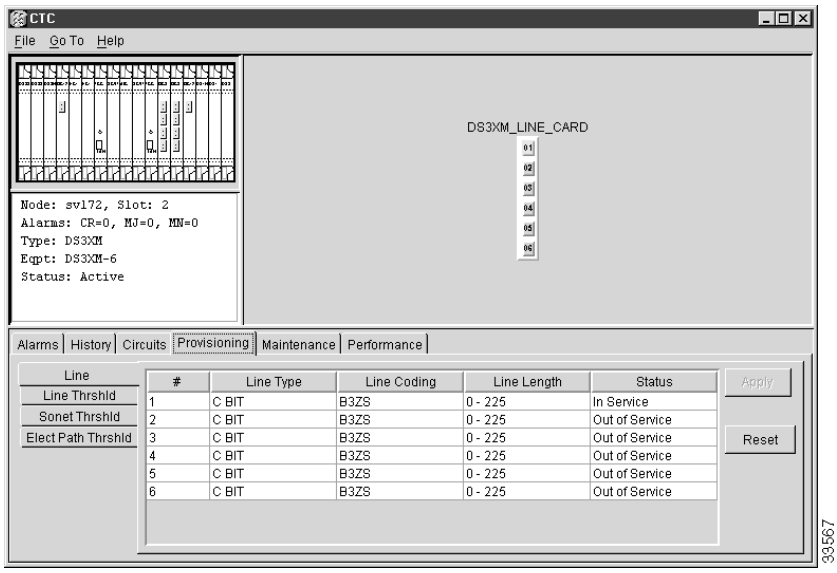
Step 3 In the **Line** subtab, (Figure 5-2) complete the following fields:

- *Line Type*—set framing (either M23 or C BIT)
- *Line coding*—always set to B3ZS
- *Line Length*—set the line length from your equipment to a patch panel. Line length is the same as line build out (LBO).
- *Status*—choose In Service from the pull-down menu.

Step 4 Click **Apply**.

Step 5 Select the **Line Thrshld**, **Sonet Thrshld**, and **Elect Path Thrshld** subtabs to set the card's performance monitoring thresholds.

Figure 5-2 Port Provisioning (DS3XM-6 Card)

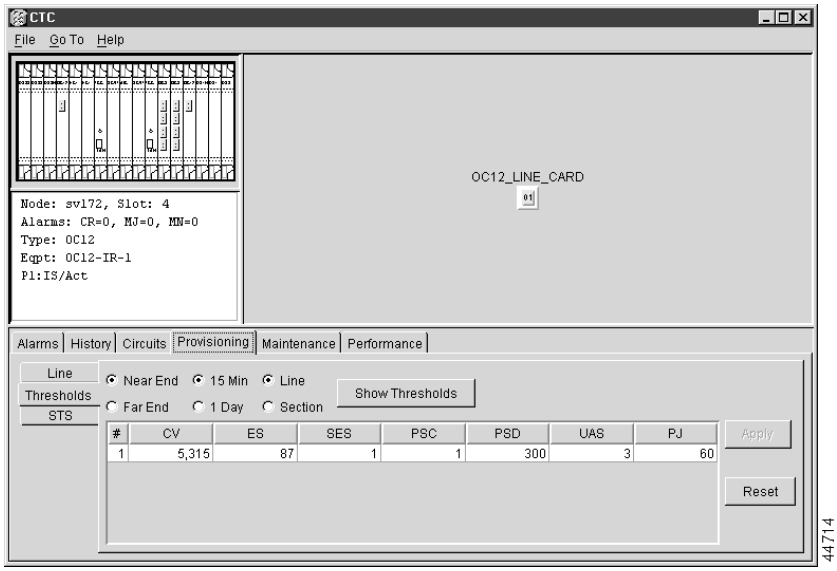


The DS3XM-6 card is now provisioned. Refer to this section whenever you need to install a new DS3XM-6 card.

5.2 Provisioning Optical Cards

The OC-3, OC-12, and OC-48 cards are pre-provisioned with settings that you can modify to manage transmission quality. To provision the optical cards, open the card in CTC and select the **Provisioning** tab. Each optical card provides three subtabs: Line, Thresholds, and STS. Figure 5-3 shows the Thresholds subtab for an OC12 IR 1310 card.

Figure 5-3 Thresholds Subtab - OC12 IR 1310 Card



The Line subtab provisions line transmission quality settings. Line settings are shown in Table 5-4.

Table 5-4 Line Settings - Optical

Heading	Description	Options
#	Port number	• 1 (OC-12, OC-48) • 1-4 (OC-3)
SF Ber Level	Sets the signal fail bit error rate	• 1E-3 • 1E-4 (default) • 1E-5
SD Ber Level	Sets the signal degrade bit error rate	• 1E-5 • 1E-6 • 1E-7 (default) • 1E-8 • 1E-9
Provides Synch	If checked, the card is provisioned as a network element timing reference on CTC Provisioning>Timing tabs	Read-only • Yes (checked) • No (unchecked)
Enable Synch Messages	Enables synchronization status messages (S1 byte), which allows the node to choose the best clocking source	• Yes (checked, default) • No (unchecked)
Send Do Not Use	When checked, sends a DUS (do not use) message on the S1 byte	• Yes (checked) • No (unchecked; default)
PJ Sts Mon #	Sets the STS that will be used for pointer justification. If set to 0, no STS is monitored. (Only one STS per card can be monitored, even on a multiport card such as the OC-3)	• 0 (default) - 3 (OC-3, per port) • 0 (default) - 12 (OC-12) • 0 (default) - 48 (OC-48)

Table 5-5 shows the ONS 15454 optical threshold settings.

Table 5-5 Threshold Settings - Optical

Heading	Description	Options
#	Port number	• 1 (OC-12, OC-48) • 1-4 (OC-3)
CV	Coding violations (Line)	Numeric. Defaults (15 min/1 day): • 1312/13,120 (OC-3 Near and Far End)) • 5,315/53,150 (OC-12 Near and Far End) • 21,260/212,600 (OC-48 Near & Far End)
ES	Errored Seconds (Line)	Numeric. Default (15 min/1 day): • 87/864 (Near and Far End)
SES	Severely Errored Seconds (Line)	Numeric. Defaults (15 min/1 day) • 1/4 (Near and Far End)
PSC	Protection Switching Count (Line)	Numeric. Default (15 min/1 day): • 1/5 (Near End) • 0/0 (Far End)
PSD	Protection Switch Duration (Line)	Numeric. Default (15 min/1 day): • 300/600 (Near End) • 0/0 (all optical cards, Far End
UAS	Unavailable Seconds (Line)	Numeric. Default (15 min/1 day): • 3/10 (Near and Far End)
PJ	Pointer Justification (Path)	Numeric. Default: • 60/5,760 (Near End) • 0/0 (Far End)
SEFS	Severely errored frame seconds	Numeric. Default: • 500/5,000 (Near End) • 0/0 (Far End)

5.3 Provisioning the OC-3 Card for STM-1

You can provision the OC3 IR 4 1310 card to support either OC-3 or STM-1 signals. When provisioned for STM-1, all four ports drop and insert STM-1 traffic in unprotected or 1+1 protected Automatic Protection Switching (APS) mode. Each STM-1 signal is mapped as a 155 Mbps concatenated signal (STS-3c) for transparent transport over a SONET network. The original STM-1 traffic may be handed off as an STM-1 or OC-3.

Because SDH and SONET frame format and size are nearly identical, their line speed meets, starting at 155 Mbps. At the STM-1/OC-3 level, the ONS 15454 performs section and line overhead conversions and maps the 261x9 byte VC-4 into an STS-3c for transparent transport across the SONET domain. At the far end, the STS-3c carrying the original VC-4 is then remapped into an STM-1 for handoff to an SDH network element.

The ONS 15454 performs section, line overheads and pointer conversions between SDH and SONET for an STM-1 to OC-3c circuit. However, to ensure operability, the following requirements must be met:

- The embedded payload must be compatible on both sides and require no conversion of any kind. Examples of such payloads include concatenated ATM or Packet over SONET/SDH signals.
- The path overhead (POH) must be compatible on both sides and require no conversion of any kind. Each overhead byte must be processed identically or simultaneously ignored. Key POH bytes to consider are the J1 (path indicator) and C2 (payload format).

Most SONET and SDH routers and ATM switches can be configured to meet these requirements.

Procedure: Provision the OC3 IR 4 1310 for STM-1

Step 1 Log into the node and double click the OC3 IR 4 1310 card.

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

Step 3 Under **Line Mode** (bottom of window), choose SDH.

Step 4 Click **Apply**.

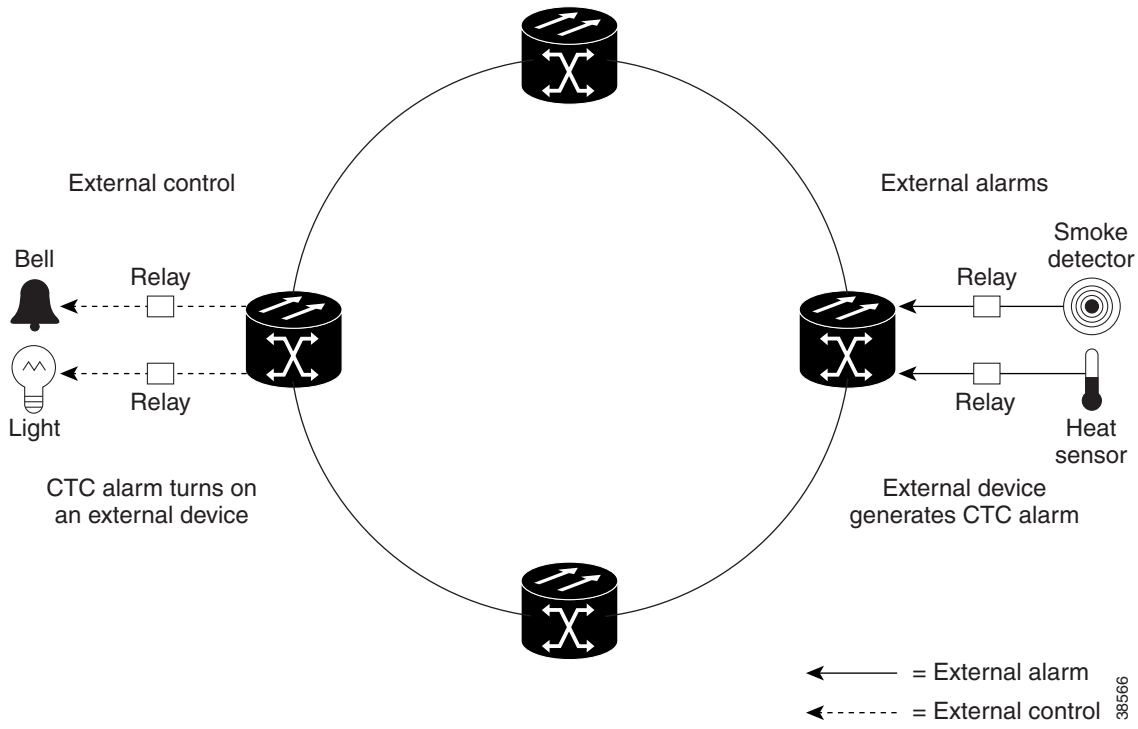
5.4 Provisioning the Alarm Interface Controller

The Alarm Interface Controller (AIC) card can be provisioned to receive input from, or send output to, external devices wired to the ONS 15454 backplane. (For a description of the AIC, see the "Alarm Interface Controller Card" section on page 2-19.) You can provision the AIC to:

- Generate CTC alarms based on events detected by external devices such as heating or cooling equipment failure, fire alarms, smoke detection, and other environmental changes that can damage ONS 15454 equipment.
- Turn external devices on or off based on a CTC alarm. For example, you can provision the AIC to turn on an audio or visual device, such as a bell or light, when a critical ONS 15454 alarm occurs.

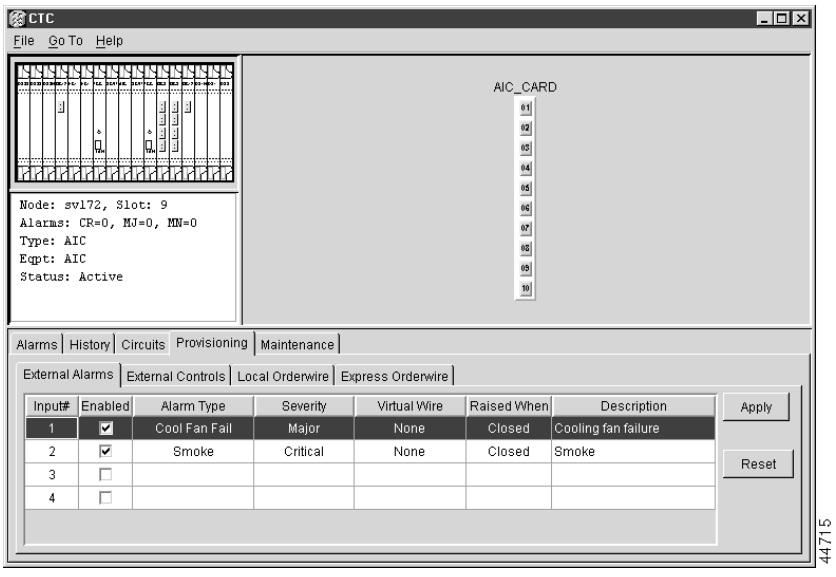
Figure 5-4 shows the flow to and from external devices provisioned through the AIC.

Figure 5-4 AIC Alarm Input and Output



To provision the AIC, open the card in CTC and select the **Provisioning** tab (Figure 5-5). You provision external alarms using the External Alarms subtab and provision external controls using the External Controls subtab.

Figure 5-5 AIC Provisioning Tab - External Alarms Subtab

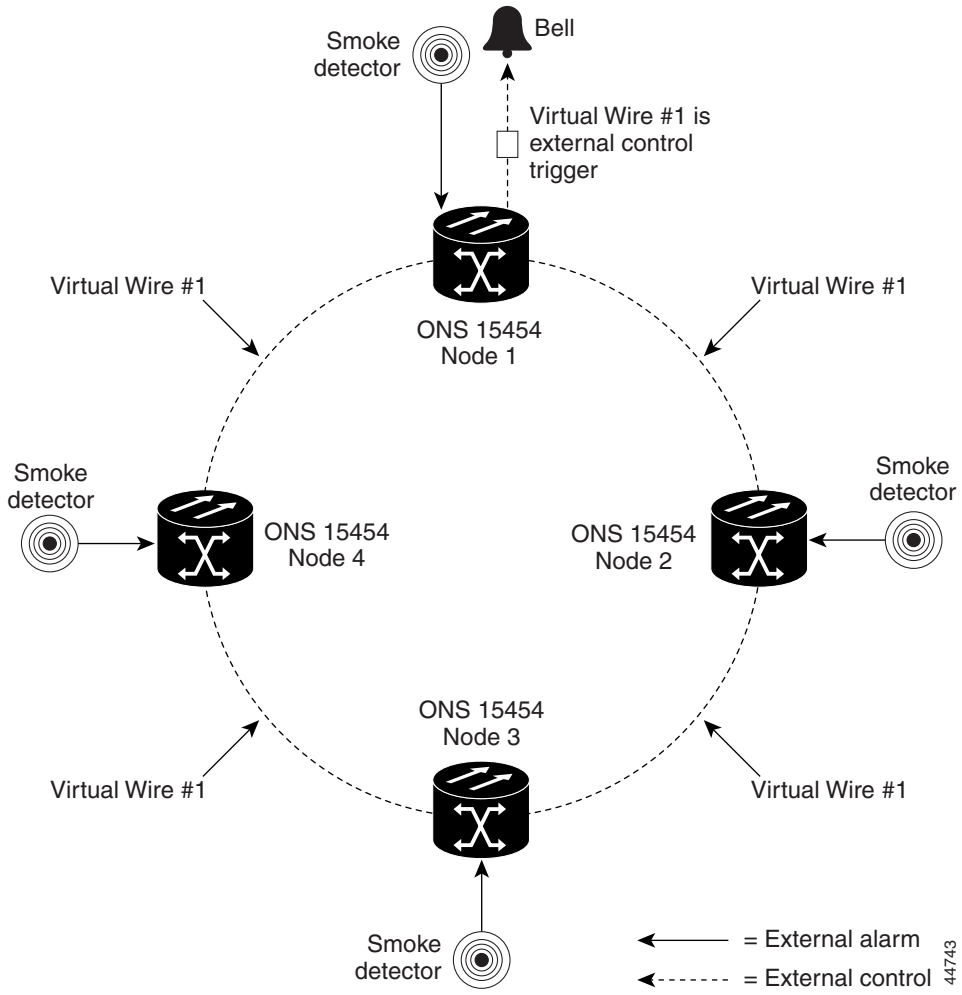


External devices provisioned on the AIC are wired to the Environmental Alarms (ENVIR ALARMS IN and ENVIR ALARMS OUT) backplane pins. See the "Alarm Pin Field Connections" section on page 1-28 for more information.

5.4.1 Using Virtual Wires

Provisioning the AIC card 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. In Figure 5-6, smoke detectors at Nodes 1, 2, 3, and 4 are assigned to Virtual Wire #1, and Virtual Wire #1 is provisioned as the trigger for an external bell at Node 1.

Figure 5-6 AIC Virtual Wire Example



When using AIC virtual wires, you can:

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

Procedure: Provision External Alarms

Step 1 Wire the external-device relays to the ENVIR ALARMS IN backplane pins.

Step 2 Log into the node in CTC and display the AIC in card view.

Step 3 On the **External Alarms** subtab (Figure 5-5), complete the following fields for each external device wired to the ONS 15454 backplane:

- *Enabled*—click to activate the fields for the alarm input number.
- *Alarm Type*—select an alarm type from the provided list.
- *Severity*—select a severity. The severity determines how the alarm is displayed in the CTC Alarms and History tabs and whether the LEDs are activated. Critical, Major, and Minor activate the appropriate LEDs. Not Alarmed and Not Reported do not activate LEDs, but do report the information in CTC.
- *Virtual Wire*—To assign the external device to a virtual wire, select the virtual wire. Otherwise, do not change the None default.
- *Raised When*—select the contact condition (open or closed) that will trigger the alarm in CTC.
- *Description*—default descriptions are provided for each alarm type; change the description as necessary.

Step 4 If you want to provision additional devices, complete Step 3 for each additional device.

Step 5 Click **Apply.**

Procedure: Provision External Controls

Step 1 Wire the external control relays to the ENVIR ALARMS OUT backplane pins.

Step 2 In CTC, log into the node and display the AIC in card view.

Step 3 On the **External Controls** subtab, complete the following fields for each external control wired to the ONS 15454 backplane:

- *Enabled*—click to activate the fields for the alarm input number.
- *Trigger Type*—select a trigger type: a local minor, major, or critical alarm, a remote minor, major, or critical alarm, or a virtual wire activation.
- *Description*—enter a description.

Step 4 If you want to provision additional controls, complete Step 3 for each additional device.

Step 5 Click **Apply.**

5.4.2 Provisioning AIC Orderwire

The AIC provides RJ-11 jacks to allow onsite personnel to communicate with one another using standard phone sets. The AIC Local and Express orderwire channels are carried on the SONET Orderwire overhead:

- Local orderwire is carried on the SONET Section layer E1 byte. Regenerators between ONS 15454 nodes terminate the channel.
- Express orderwire is carried on the E2 byte of the SONET Line layer.

If regenerators are not used between ONS 15454 nodes, local or express AIC orderwire channels can be used. If regenerators exist, use the Express orderwire channel. You can provision up to four ONS 15454 optical carrier ports for each orderwire path.

Caution When provisioning orderwire for ONS 15454s residing in a ring, do not provision a complete orderwire loop. For example, a four-node ring typically has east and west ports provisioned at all four nodes. However, to prevent orderwire loops from occurring, provision two orderwire ports (east and west) at all but one of the ring nodes.

Procedure: Provision AIC Orderwire

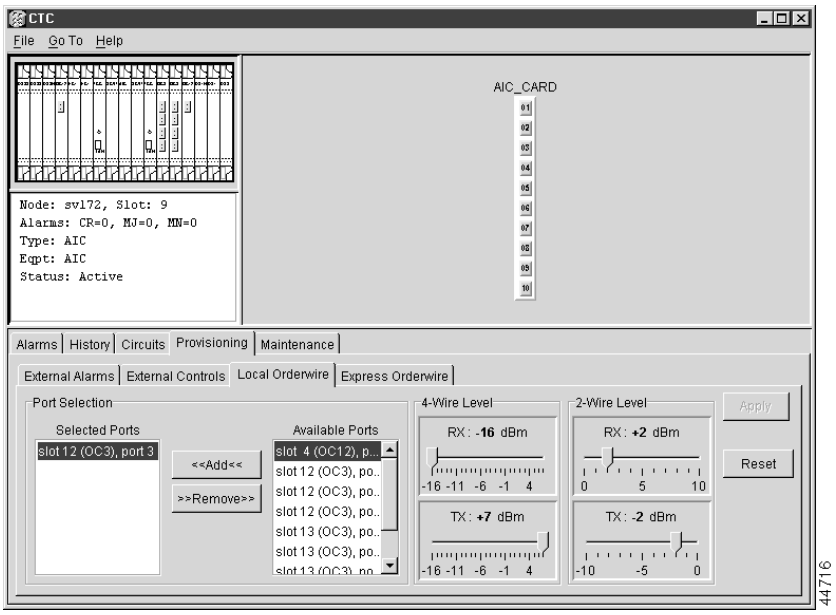
Tip Before you begin, make a list of the ONS 15454 slots and ports that require orderwire communication.

Step 1 In CTC, open the AIC card.

Step 2 Select the orderwire subtab appropriate to the orderwire path (**Local Orderwire** or **Express Orderwire**) that you want to create.

The Local Orderwire subtab is shown in Figure 5-7. Provisioning procedures are the same for both types.

Figure 5-7 AIC - Local Orderwire Subtab



Step 3 Under Available Ports, select each port that you want to use for the orderwire channel and click **Add** to move them to the Selected Ports column.

Step 4 If needed, adjust the Tx and Rx dBm by moving the slider to the right or left for the headset type (four-wire or two-wire) that you will use. (In general, you should not need to adjust the dBm.)

Step 5 Click **Apply.**

5.4.3 Using the AIC Orderwire

The AIC orderwire channels function as a party line. Anyone plugging a phone set into an AIC orderwire channel can communicate with all participants on the connected orderwire. The AIC does not provide private, point-to-point connections. To get the attention of participants, press the AIC Call button to activate a buzzer and illuminate the RING LED on AICs at all connected nodes.

5.5 Converting DS-1 and DS-3 Cards From 1:1 to 1:N Protection

The ONS 15454 provides several protection options for DS1-14 and DS3-12 cards: unprotected, 1:1, and 1:N. Changing protection from 1:1 to 1:N increases the available bandwidth because two of the three cards used for protection in the 1:1 protection group become working cards in the 1:N group.

When setting up 1:N protection, install the DS1N-14 or DS3N-12 card in Slot 3 or 15 on the same side of the ONS 15454 as the cards it protects. Slot 3 protects cards in Slots 1 - 2 and 4 - 6. Slot 15 protects Slots 12 - 14 and 16 - 17. A DS1N-14 or DS3N-12 card installed in Slot 3 or 15 can protect up to five DS1-14 or DS3-12 cards. If you install a DS3N-12 or DS1N-14 card in another slot, it behaves like a normal DS-1 or DS-3 card.

Procedure: Convert DS1-14 Cards From 1:1 to 1:N Protection

Note This procedure assumes DS1-14 cards are installed in Slots 1 through 6 and/or Slots 12 through 17. The DS1-14 cards in Slots 3 and 15, which are the protection slots, will be replaced with DS1N-14 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS1N-14 card and a protection group with DS1-14 cards.

Step 1 Click the **Maintenance>Protection** tabs.

Step 2 Click the protection group that contains Slot 3 or Slot 15 (where the DS1N-14 will be installed).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. Under Selected Group, the protect slot must say Protect/Standby (shown in Figure 5-8) and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to switch traffic to the working card:

(a) Under **Selected Group**, click the protect card.

(b) From **Operation** at the bottom of the screen, select MANUAL.

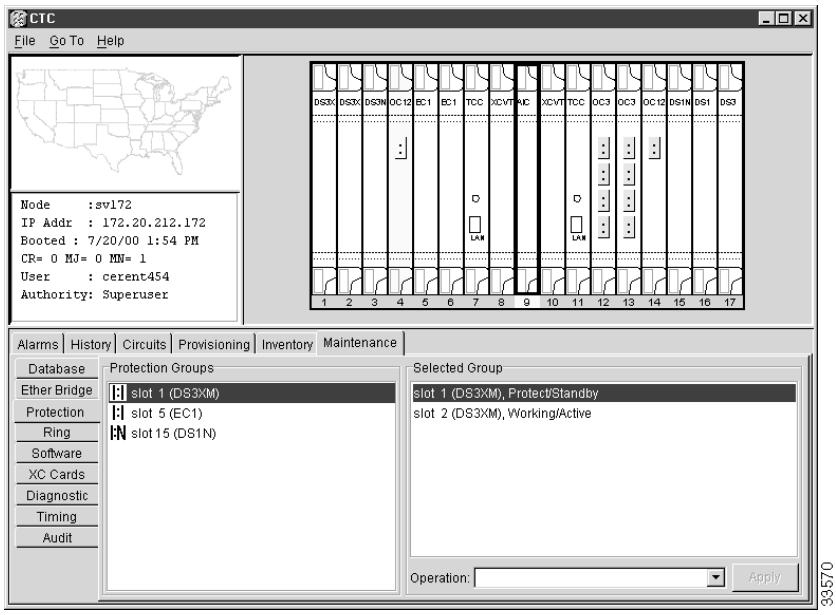
(c) Click **Apply**.

Note The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they do not change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

(d) From **Operation**, select CLEAR.

(e) Click **Apply**.

Figure 5-8 Protection Group Slot Status



Step 4 Repeat Steps 1-3 for each protection group that you need to convert. If you are only converting one protection group, proceed to Step 5.

Step 5 Verify that no standing alarms exist for any of the DS1-14 cards that you are converting.

Step 6 Clear any alarms that may exist on the DS1-14 cards before proceeding. If you have difficulty clearing alarms, contact your next level of support.

Step 7 Click the **Provisioning>Protection** tabs.

Step 8 Click the 1:1 protection group containing cards that will be moved into the new protection group.

Step 9 Click **Delete**.

Step 10 When the confirmation dialog displays, click **Yes**.

Note Deleting the 1:1 protection groups does not disrupt service. However, no protection bandwidth exists for the working circuits until you complete the 1:N protection procedure. Therefore, complete this procedure as quickly as possible.

Step 11 If needed, repeat Steps 8 - 10 for other protection groups.

Step 12 On the node view shelf graphic, right-click the DS1-14 card in Slot 3 or Slot 15 and select **Delete** from the shortcut menu. Wait for the card to disappear from the node view.

Step 13 Physically remove the DS1-14 card from Slot 3 or Slot 15.

Step 14 Physically insert a DS1N-14 card in the same slot.

Step 15 Verify that the card boots up properly.

Step 16 Click the **Inventory** tab and verify that the new card appears as a DS1N-14.

Step 17 Click the **Provisioning>Protection** tabs.

Step 18 Click **Create**. The Create Protection Group dialog opens with the protect card in the *Protect Card* field and the available cards in the *Available Cards* field.

Step 19 Type a name for the protection group in the *Name* field (optional).

Step 20 Click **Type** and choose 1:N (card) from the pull-down menu.

Step 21 Verify that the DS1N-14 card appears in the *Protect Card* field.

Step 22 Under Available Cards, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 23 Click **OK**. The protection group appears under Protection Groups on the Protection subtab.

Procedure: Convert DS3-12 Cards From 1:1 to 1:N Protection

Note This procedure assumes that DS3-12 cards are installed in Slots 1 - 6 and/or Slots 12 - 17. The DS3-12 cards in Slots 3 and 15, which are the protection slots, will be replaced with DS3N-12 cards. The ONS 15454 must run CTC Release 2.0 or later. The procedure also requires at least one DS3N-12 card and a protection group with DS3-12 cards.

Step 1 Click the **Maintenance>Protection** tabs.

Step 2 Click the protection group containing Slot 13 or Slot 15 (where you will install the DS3N-12 card).

Step 3 Make sure the slot you are upgrading is not carrying working traffic. Under Selected Group, the protect slot must say Protect/Standby as shown in Figure 5-8, and not Protect/Active. If the protect slot status is Protect/Active, use the following steps to switch traffic to the working card:

(a) Under Selected Group, click the protect card.

(b) From **Operation** at the bottom of the screen, select MANUAL.

(c) Click **Apply**.

Note The working slot should change to Working/Active and the protect slot should change to Protect/Standby. If they fail to change, do not continue. Troubleshoot the working card and slot to determine why the card cannot carry working traffic.

(d) From **Operation**, select CLEAR.

(e) Click **Apply**.

Step 4 If you are converting more than one protection group, repeat Step 2 for each group that needs conversion. Otherwise, proceed to Step 5.

Step 5 Verify that no standing alarms exist for any of the DS3-12 cards you are converting.

Note Clear any alarms that may exist on the DS3-12 cards before proceeding. If you have difficulty clearing alarms, contact your next level of support.

Step 6 Click the **Provisioning>Protection** tabs.

Step 7 Click a 1:1 protection group containing cards that will be moved into the new protection group.

Step 8 Click **Delete**.

Step 9 When the confirmation dialog displays, click **Yes**.

Note Deleting the 1:1 protection groups will not disrupt service. However, no protection bandwidth exists for the working circuits until the 1:N protection procedure is completed. Do not delay when completing this procedure.

Step 10 If you are deleting more than one protection group, repeat Steps 6 - 8 for each group. Otherwise, proceed to Step 11.

Step 11 On the node view shelf graphic, right-click the DS3-12 card in Slot 3 or Slot 15 and select Delete from the shortcut menu.

Step 12 Physically remove the DS3-12 card from Slot 3 or Slot 15. This raises an improper removal alarm.

Step 13 In node view, right-click the slot that held the removed card and select delete from the pull-down menu. Wait for the card to disappear from the node view.

Step 14 Physically insert a DS3N-12 in the same slot.

Step 15 Verify that the card boots up properly.

Step 16 Click the **Inventory** tab and verify that the new card appears as a DS3N-12.

Step 17 Click the **Provisioning>Protection** tabs.

Step 18 Click **Create**.

The Create Protection Group dialog shows the protect card in the *Protect Card* field and the available cards in the *Available Cards* field.

Step 19 Type a name for the protection group in the *Name* field (optional).

Step 20 Click **Type** and select 1:N (card) from the pull-down menu.

Step 21 Verify that the DS3N-12 card appears in the *Protect Card* field.

Step 22 Under Available Cards, highlight the cards that you want in the protection group. Click the arrow (>>) tab to move the cards to the Working Cards list.

Step 23 Click **OK**.

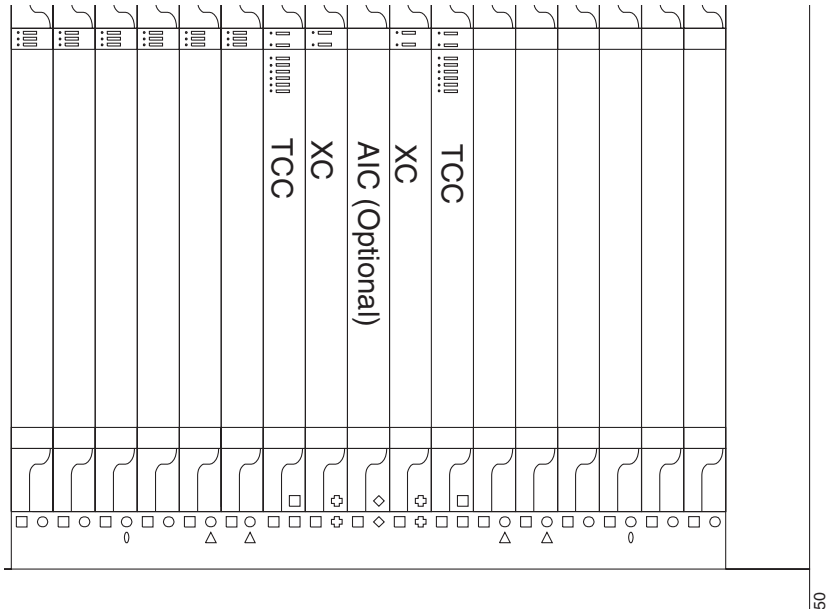
The protection group should appear under Protection Groups on the Protection subtab.

This completes the procedure for converting a DS3N-12 from 1:1 to 1:N protection. Repeat this process for all protection groups or nodes that need upgrading.

5.6 Upgrading XC Cards to XCVT

This section explains how to replace dual XC cards with dual XCVT cards in an ONS 15454 with live traffic. The substitution will not disrupt traffic. Figure 5-9 shows a ONS 15454 with XC cards installed.

Figure 5-9 ONS 15454 with XC Cards



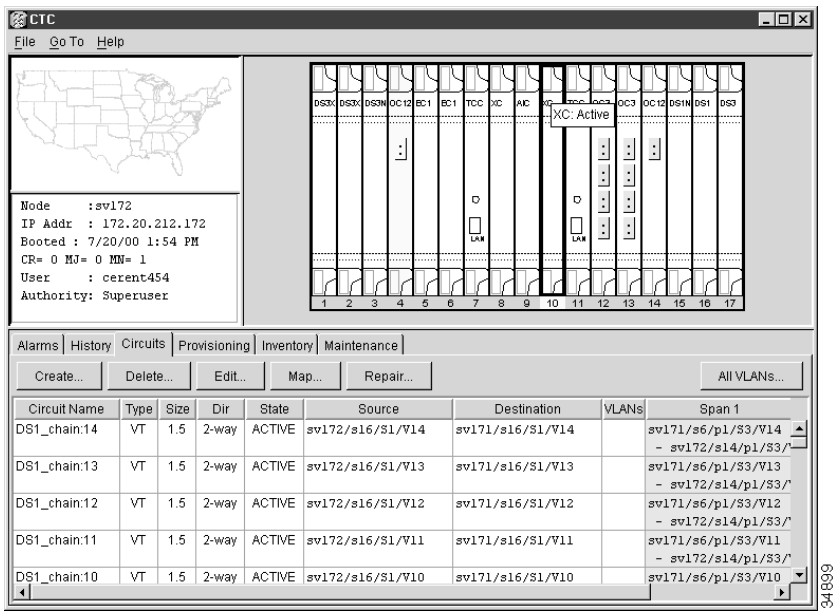
Procedure: Upgrade XC Cards to XCVT

Upgrading XC cards to XCVT requires that the ONS 15454 run CTC Release 2.0 or later. Two XC cards must be installed in the ONS 15454, and two XCVT cards must be available for installation.

Step 1 Determine the standby XC card. The ACT/STBY LED of the standby XC card is yellow, while the ACT/STBY LED of the active XC card is green.

Note You can also place the cursor on top of the card graphic to display a dialog. This display identifies the card as *XC: Active* or *XC: Standby*. Figure 5-10 shows an Active XC dialog.

Figure 5-10 Active XC Card



Step 2 Remove the standby XC card from the ONS 15454. This raises an improper removal alarm.

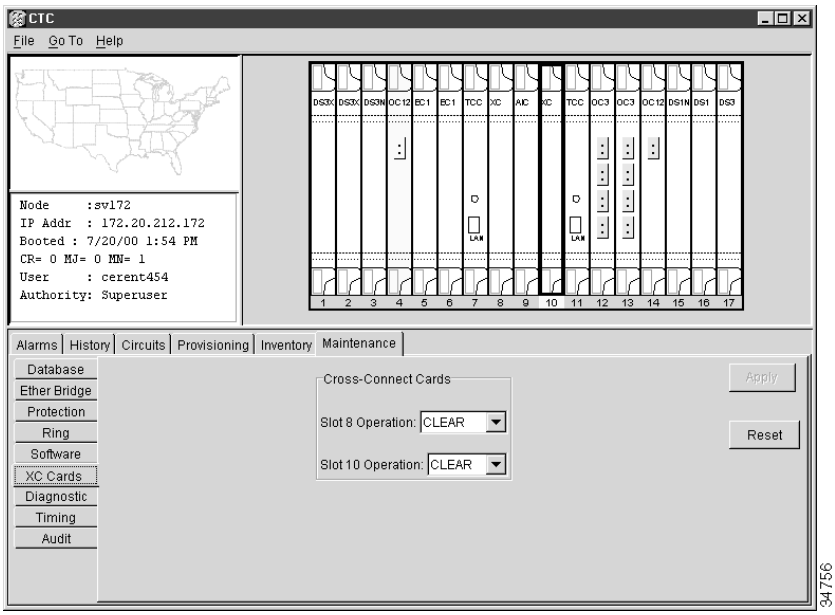
Step 3 Insert the first XCVT card into the empty XC slot and latch the levers.

The fail LED above the ACT/STBY LED becomes red, blinks for several seconds, then turns off.

The ACT/STBY LED turns yellow and stays lit.

Step 4 In node view, select the **Maintenance>XC Cards** tabs (Figure 5-11).

Figure 5-11 XC Cards Subtab



Step 5 Use the Slot Operation menu for the slot of the active card. In this example, **Slot 10 Operation**.

Step 6 Choose MANUAL from the pull-down menu.

Step 7 Click **Apply**.

Note A minor alarm will appear on the manually switched slot. After the active XC disengages, the standby slot or first XCVT card becomes active. This causes the ACT/STBY LED on the first XCVT card to change from yellow to green.

Step 8 Choose CLEAR from the same Slot Operation menu.

Step 9 Click **Apply**.

Step 10 Physically remove the now standby XC card from the ONS 15454.

Step 11 Insert the second XCVT card into the empty XC slot. The second XCVT card boots up and becomes a standby XCVT.

DWDM

This chapter provides a general overview of Dense Wavelength Division Multiplexing (DWDM) technology, components, and applications and describes how the Cisco ONS 15454 implements DWDM solutions.

6.1 DWDM Overview

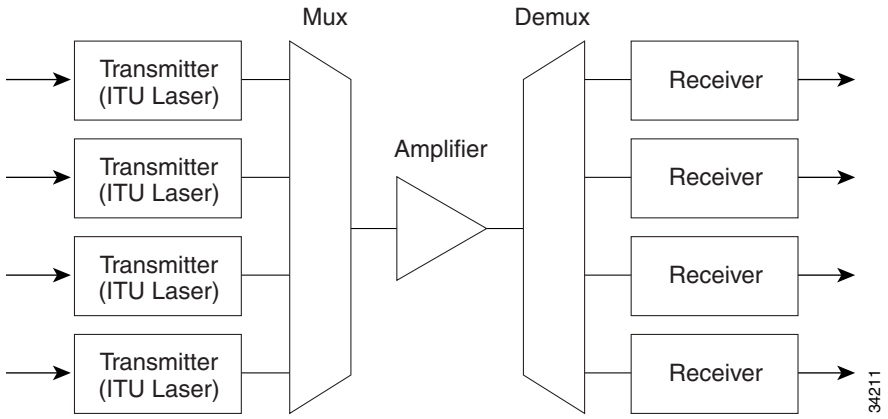
DWDM increases the information-carrying capacity of existing fiber optic infrastructure to eliminate the high cost of installing new fiber optic cable. The majority of the current high-speed backbones used by service providers are comprised of fiber optic links operating at 2.5 Gigabits per second (Gbps) or 10 Gbps. DWDM offers a scalable solution for using existing installed fiber optics to gain increased bandwidth.

DWDM transmits multiple signals simultaneously at different wavelengths. This allows a single fiber to operate as if it were multiple fibers, referred to as “virtual fiber.” Each signal carried can be at a different rate (OC-48 or OC-192 for example) yet use the same physical fiber optic cable.

6.2 DWDM Components

All DWDM systems consist of the following components: precise wavelength optical transmitters (lasers), optical multiplexers (mux) and demultiplexers (demux), and broadband optical receivers. Optional components of a DWDM system are optical add/drop multiplexers (OADM) and optical amplifiers. Figure 6-1 shows the basic concept of a DWDM system with an amplifier.

Figure 6-1 DWDM System



6.2.1 Optical Transmitters and Transponders

The optical transmitters for DWDM systems are high resolution, precision narrow-band lasers. These lasers allow close channel spacing, which increases the number of wavelengths that can be used in the 1500 nm band while minimizing the effects of signal impairments such as dispersion. The optical transmitter minimizes power loss which to allow long transmission distances and a high level of signal integrity. These lasers can use optical amplifiers that boost signal strength for extended distances and eliminate the electronic-amplifier need to regenerate individual optical signals. Most laser systems are designed to wavelength frequencies that follow the ITU-T, which enables simplified interoperability and easier component selection.

A component of some DWDM systems is the transponder, which converts broadband optical signals to specific wavelengths using optical-to-electrical-to-optical (OEO) conversion. Transponders or wavelength converters are optional devices that provide the conversion of one optical wavelength (in other words, 1310 nm or 1550 nm) to a precision narrow-band wavelength. This conversion enables devices that are not equipped with precision narrowband lasers to be multiplexed onto a single fiber, such as routers, ATM switches, or other multiplexers.

6.2.2 Optical Amplifiers

Optical amplifiers boost optical signals to minimize the effects of power loss and attenuation that result from sending light pulses over optical fiber. Optical amplifier technology is the key to enabling the high speed, high-volume transmission of DWDM to take place. Optical amplifier technology was the key to the commercial success of long-haul DWDM systems. However, because of the shorter distances found in metropolitan and regional networks, optical amplifiers are not always deployed in these networks.

Before the advent of optical amplifiers, each signal had to be regenerated electronically. When regenerating an optical signal electronically, the signal must first be converted to an electrical signal, amplified, and then converted back to an optical signal before being retransmitted. Electronic regeneration requires a separate regenerator for each wavelength on each fiber. A single optical amplifier can amplify all of the wavelengths on one fiber.

The most common type of optical amplifier is the erbium doped fiber amplifier (EDFA). Conventional EDFAs operate in the 1530 to 1560 nm range.

6.2.3 Optical Multiplexers and Demultiplexers

Optical multiplexers combine the transmit signals from different wavelengths onto a single optical fiber. Optical demultiplexers separate the combined signals into their component wavelengths at the receiving end. Thin film dielectric filters and optical gratings types of multiplexers and demultiplexers. DWDM multiplexers are typically passive devices, which means they do not require electrical input. These passive multiplexers behave like high-precision prisms to separate the individual colors of the DWDM signal.

6.2.4 Optical Receivers

Optical receivers detect incoming lightwave signals and convert them to an appropriate signal for processing by the receiving device. Optical receivers are usually wideband devices that can detect light over a relatively wide range of wavelengths. The ability to detect this wide range of wavelengths allows a single receiver to accept any wavelength in the 1300 to 1550 nm range.

6.2.5 OADMs

Optical Add/Drop Multiplexers (OADMs) can be deployed into a DWDM system or network for added signal grooming flexibility. OADMs allow you to add or drop channels from a fiber that is dense wave division multiplexed. OADMs are installed in a multi-wavelength fiber span, and allow a specific wavelength on the fiber to be demultiplexed (dropped) and remultiplexed (added) while enabling all other wavelengths to pass. As the result of an OADM filter, the wavelengths that pass through experience only a small amount of signal attenuation.

6.3 DWDM Applications

DWDM offers many benefits over traditional fiber-optic systems. It minimizes fiber usage by creating “virtual fiber” to convert each fiber into multiple fibers. DWDM provides greater scalability and extends the non-regenerated distance limits. It is also bit-rate and protocol independent. These benefits enable many new applications. A few of the possible applications are described in this section.

6.3.1 Long Distance

DWDM technology works well for long distance carriers that use point-to-point or ring topologies. Having 16 new transmission channels instead of one greatly improves a carrier’s ability to expand capacity while setting aside backup bandwidth without deploying new fiber.

DWDM technology has been used extensively by long distance carriers and has allowed the existing fiber plant to keep pace with the growing demand for bandwidth. DWDM systems designed for long-haul networks have the ability to provide more than 32 wavelengths over a single fiber.

6.3.2 Self-Healing Rings

The development of self-healing rings depends on the large amount of capacity provided by DWDM. Self-healing rings are typical in most sophisticated telecommunications networks. Using DWDM, a telecommunications network operator can construct a 40 Gb/s ring with 16 separate fully-protected signals. All of this can be accomplished using just two fibers.

DWDM technology does not hinder the deployment of self-healing ring technology as found in SONET systems, and is transparent to the protocol operating on top of the OC-N signal. DWDM systems provide multiple wavelengths that can be used for the working or protection channels of a SONET system. These wavelengths can also be used for unprotected optical signals, such as those found on many routers or ATM equipment.

6.3.3 Network Expansion

For network operators that are building or expanding their networks, DWDM is an economical way to future-proof existing infrastructure. DWDM allows for incremental capacity increases and ease in implementing new equipment. In some geographic areas where the industrial base is rapidly expanding, DWDM is one way to meet the growing demand without laying new fiber.

6.4 DWDM and the ONS 15454

The Cisco ONS 15454 DWDM solution employs 18 distinct OC48 ITU DWDM cards. Nine of these cards operate in the blue band with spacing of 200 GHz, and the other nine operate in the red band with 200 GHz spacing. The optics have a link budget of 25 dB. The cards are intended to be used for long unregenerated spans of up to 200 km with mid-span amplification, or 80 km without amplification.

6.4.1 ONS 15454 OC48 ELR ITU Optics

The ONS 15454 OC48 ELR ITU optics complement the standard OC-48 optics cards currently offered on the platform. As with all ONS 15454 optics cards, they can be configured for operation in ring networks (UPSR or BLSR), linear networks, point-to-point or ADM configurations, mesh networks, or as a terminal node. The ONS 15454 system can be configured with a combination of ITU and non-ITU cards, depending on the user's application.

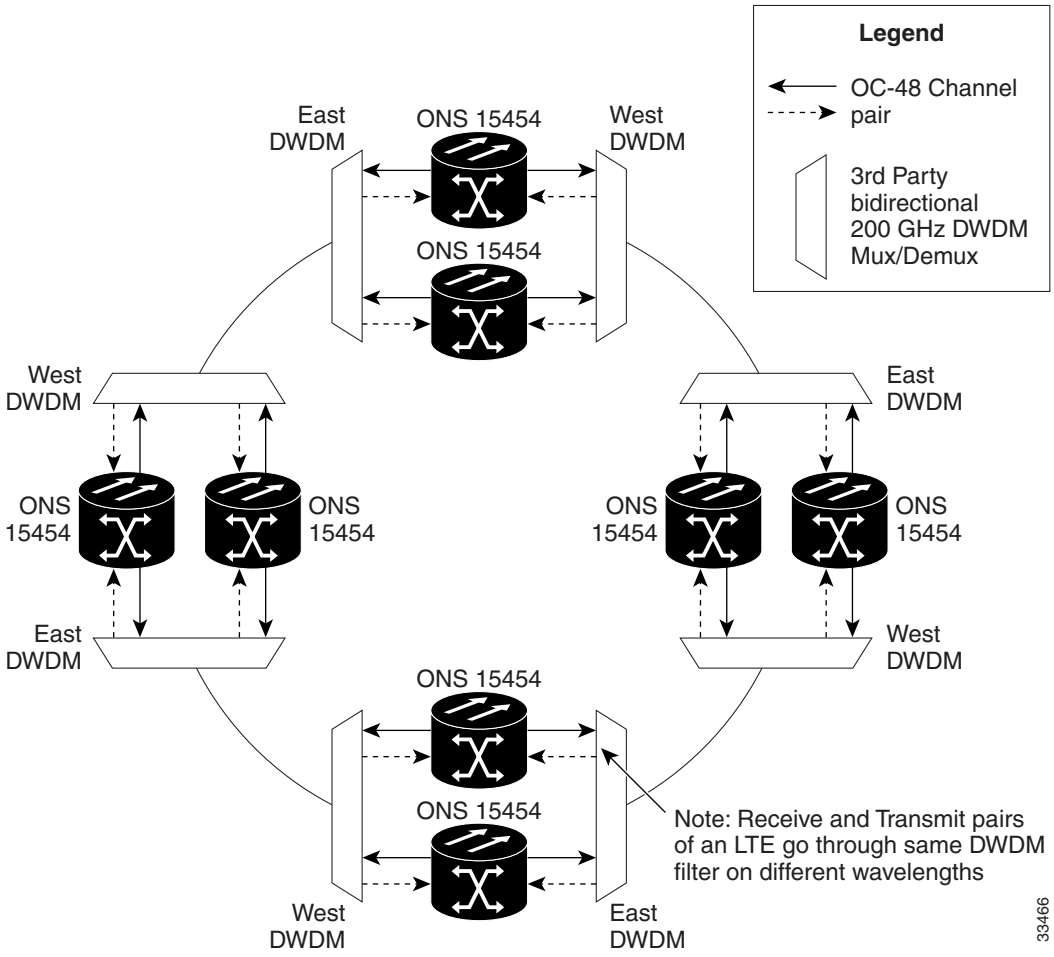
Pairing the ONS 15454 ELR ITU optics with bidirectional DWDM multiplexers and demultiplexers can provide up to 45 Gb/s of bandwidth over a single fiber. Where available fiber is limited, the resulting fiber bandwidth improvement reduces the need to install new fiber. Because the Cisco DWDM solution is standards-based and ITU-compliant, users can deploy products from third-party manufacturers to build multivendor networks that best suit their applications.

Engineering a metropolitan fiber link with DWDM and ITU lasers is similar to using single channel operation. Because the ONS 15454 OC48 ELR ITU optics are designed for single span, non-amplified links, this solution should operate over most types of fiber plant. Fiber non-linear effects including four-wave mixing, stimulated brillouin scattering, self-phase modulation, cross-phase modulation, and stimulated raman scattering are irrelevant because of the low optical transmit power levels and wide frequency spacing of the DWDM system.

6.4.2 Using the ONS 15454 in a DWDM Network

The deployment of DWDM does not limit the type of network topology supported, whether it is a ring, linear, or mesh network. The ability of the ONS 15454 platform to deliver multiple services (DS-1, DS-3, and Ethernet, for example) is unaffected. The DWDM passive multiplexers/demultiplexers are transparent to the data traversing the wavelengths and are used to expand the capacity of the existing fiber. The ONS 15454 can support applications that use both the ITU and standard 1310nm or 1550nm wavelengths depending on the requirements of the particular network. Figure 6-2 shows the Cisco ONS 15454 used in a DWDM ring application.

Figure 6-2 DWDM Ring Application



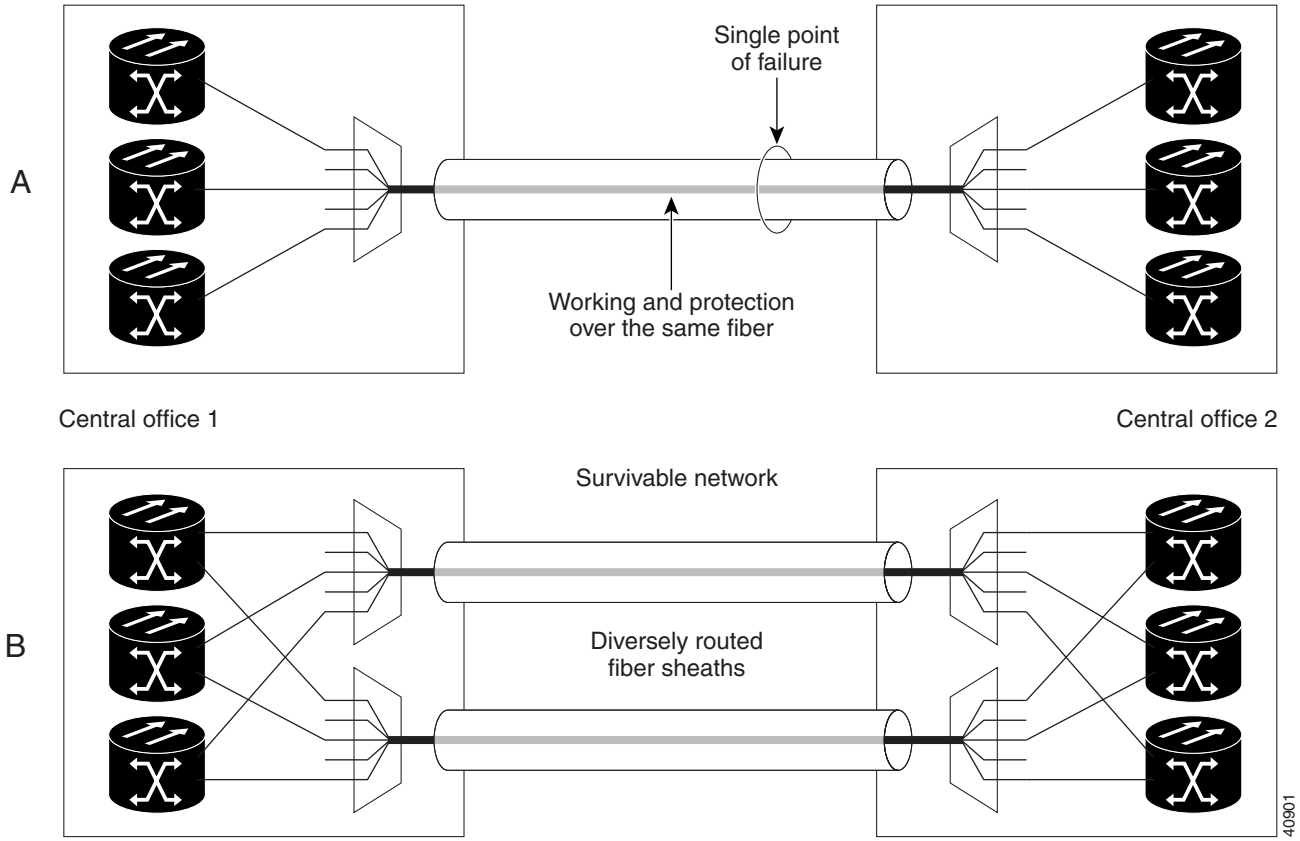
6.4.2.1 ONS 15454 DWDM Network Design

The ONS 15454 DWDM solution expands the available options for designing a high-bandwidth network that uses existing infrastructure. It is important to follow a set of engineering guidelines/practices to be sure that you are maximizing the benefits and efficiency of your DWDM network. This section presents high-level examples of some common network design improvements using DWDM.

6.4.2.2 Survivable Network

Building a survivable network is one of the primary concerns when making network design decisions. At the very least, you should make sure that there is no interruption of traffic because of a fiber cut. Eliminating a single point of failure is one way to create a more survivable network. Figure 6-3 shows two examples of the same network. Example A has working and protection circuits set up on the same fiber to create a single point of failure. Example B is a survivable network with working and protection circuits set up on different fibers taking separate routes.

Figure 6-3 Survivable Network



6.4.2.3 Sparing Practices

Sparing keeps a network up and running after a card failure. The two methods of sparing are 1:1 card sparing and wavelength sparing. Wavelength sparing is the preferred method because it requires only one spare card at each site. With 1:1 card sparing, each card must have an identical card in inventory at the site.

Ethernet Applications

This chapter explains how to use the Ethernet features of the Cisco ONS 15454.

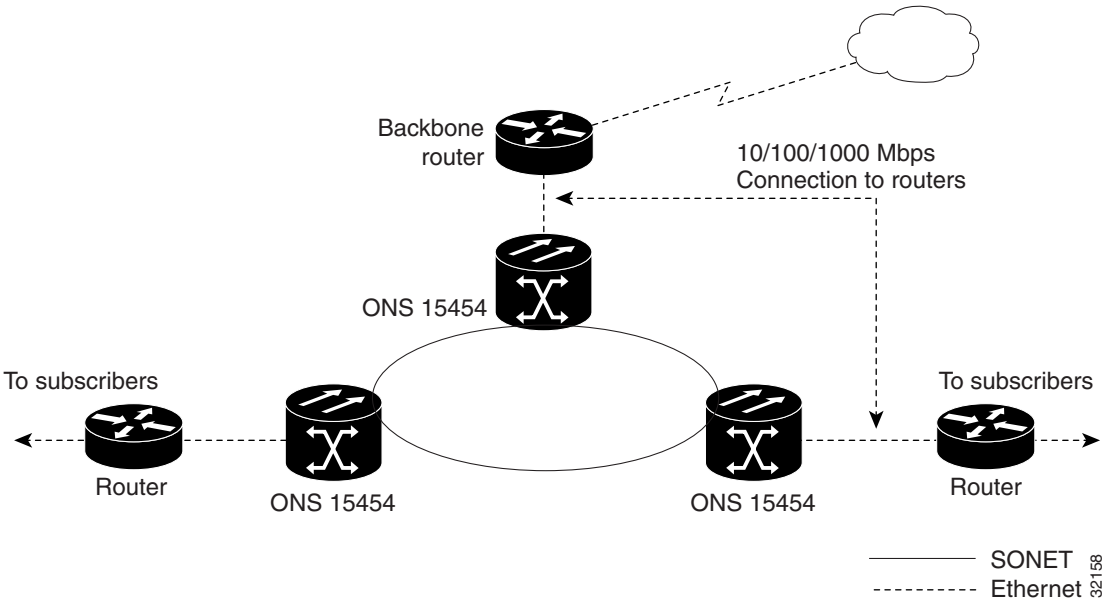
7.1 Ethernet over SONET Application

To maximize Ethernet cost effectiveness, the ONS 15454 integrates Ethernet access into the same SONET platform that transports data and voice traffic. The ONS 15454 supports layer 2 switching and the ability to classify Ethernet traffic as defined in IEEE 802.1 Q. You can switch tagged traffic onto separate SONET STS channels to engineer bandwidth by traffic class. 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 15454 can also concentrate Ethernet ports into one or more STS-n circuits to use bandwidth more efficiently.

7.2 Router Aggregation Application

The ONS 15454 Ethernet solution uses existing SONET infrastructure to transport aggregate traffic from multiple, remote sources. Figure 7-1 illustrates the aggregation and transport.

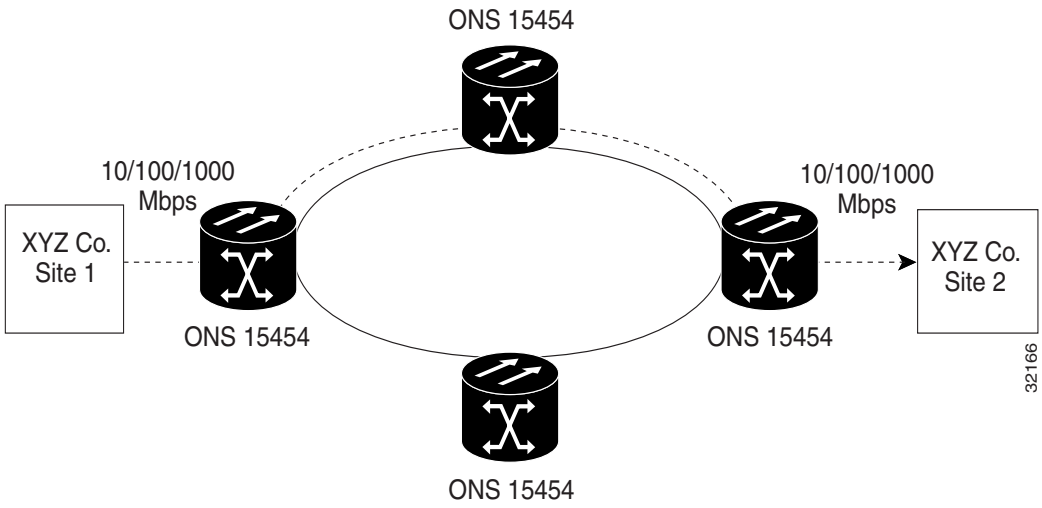
Figure 7-1 Router Aggregation Application



7.3 Transparent LAN Application

The ONS 15454 supports Transparent LAN Service (TLS) that provides private network service across a SONET backbone. Because network subscribers sometimes share the same equipment or even the same STS channels, it is necessary to logically isolate subscriber traffic. Service providers can use the IEEE 802.1Q feature in the ONS 15454 to define multiple, virtual local area networks (VLANs) across the backbone. Specific Ethernet ports and SONET STS channels can be defined as a VLAN group. VLAN groups isolate the subscriber's traffic from users outside the VLAN group and keep "outside" traffic from "leaking" into the VPN. Figure 7-2 illustrates a transparent LAN application.

Figure 7-2 Transparent LAN Application



7.4 ONS 15454 Ethernet Cards

The ONS 15454 supports two separate Ethernet cards, the E100T and the E1000-2. This section describes the characteristics of each card.

7.4.1 E100T

The ONS 15454 uses E100T cards for Ethernet (10 Mbps) and Fast Ethernet (100 Mbps). The E100T enables network operators to provide multiple 10/100 Mbps access drops for high-capacity customer LAN interconnections. The card provides efficient transport and co-existence of traditional TDM traffic with packet switched data traffic. The E100T eliminates the need for external Ethernet aggregation equipment.

Specifications:

- Operating Temperature: 0 to +55 degrees Celsius
- Operating Humidity: 5 - 95% non-condensing
- Power Consumption: 40 Watts

Figure 7-3 E100T Card, Front view

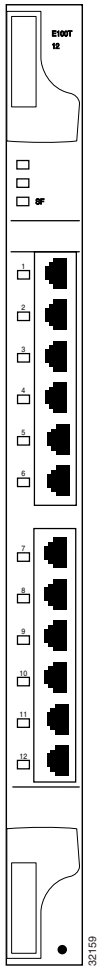


Table 7-1 E100T Ethernet Port LED States

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Flashing Green	Transmitting only or Receiving only
Green Off	Inactive connection or uni-directional traffic.

7.4.2 E1000-2

The ONS 15454 uses the E1000-2 cards for Gigabit Ethernet (1000 Mbps). The E1000-2 enables network operators to provide multiple 1000 Mbps access drops for high-capacity customer LAN interconnections. The E1000-2 provides efficient transport and co-existence of traditional TDM traffic with packet-switched data traffic.

For Cisco Release 2.2.0, two GBIC modules are offered as separate products for flexibility: an IEEE 1000Base-SX compliant 850 nm optical module and an IEEE 1000Base-LX compliant 1300 nm optical module. The 850 nm SX optics are designed for multimode fiber and distances of up to 220 meters on 62.5 micron fiber and up to 550 meters on 50 micron fiber. The 1300 nm LX optics are designed for single-mode fiber and distances of up to 5 kilometers.

Caution IE1000-2 cards lose traffic for approximately 30 seconds when an ONS 15454 database is restored. Traffic is lost during the period of spanning tree reconvergence. The CARLOSS alarm will appear and clear during this period.

Specifications:

- Operating Temperature: 0 to +55 degrees Celsius
- Operating Humidity: 5 - 95% non-condensing
- Power Consumption: 40 Watts

Figure 7-4 E1000-2 Card, Front view

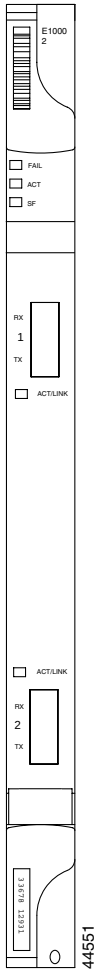


Table 7-2 E1000-2 Ethernet Port LED States

LED State	Description
Amber	Transmitting and Receiving
Solid Green	Idle and Link Integrity
Flashing Green	Transmitting only or Receiving only
Green Off	Inactive connection or uni-directional traffic.

7.5 Virtual Local Area Networks (VLANs)

As Ethernet networks grow, too many hosts transmitting data within a single broadcast domain cause an increase in "broadcast storms." You can create VLANs with the CTC to partition the broadcast domain into several domains and decrease the likelihood of broadcast storms. A VLAN carves out its own single broadcast domain from the larger Ethernet network.

The ONS 15454 supports port-based VLANs that group ports into virtual workgroups. These VLANs ensure that Ethernet ports see only traffic from ports within the same VLAN. These different VLANs communicate with each other through a router that spans multiple VLANs by using router ports in each VLAN, or through a router that understands IEEE 802.1Q.

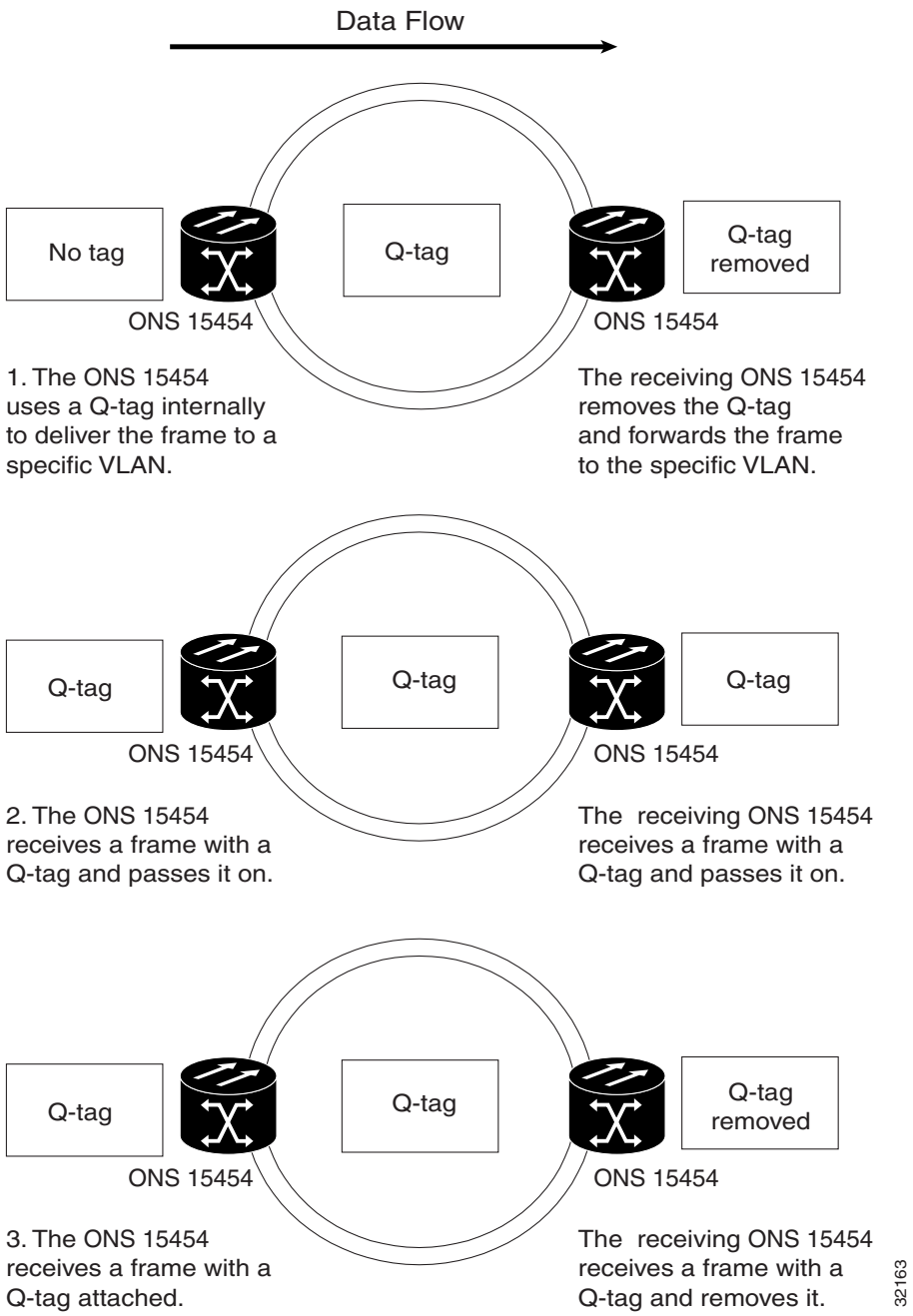
7.5.1 IEEE 802.1Q

IEEE 802.1Q, the VLAN standard, places a Q-tag in the frame header. The 802.1Q-aware devices look at Q-tags to differentiate LANs. Therefore, multiple 802.1Q VLANs representing different logical networks can be transported over the same physical port. If a frame is received without a Q-tag, the frame is given a Q-tag based on the default VLAN assigned to the ingress port. If a frame is received with a Q-tag attached, the port classifies the frame based on the VLAN identifier present in the Q-tag.

Many older Ethernet devices do not understand 802.1Q tagging. Because 802.1Q lengthens the Ethernet header, older (non-802.1Q) devices may incorrectly identify the 802.1Q tagged packets as giants (an Ethernet frame larger than 1518 bytes) and drop them. The ONS 15454 takes non-tagged packets from the ingress port and assigns the frame to the VLAN associated with the ingress port. If packets come into the ONS 15454 network already tagged, the ONS 15454 uses the already-attached tag to forward the packet accordingly. Figure 7-5 illustrates different ways the ONS 15454 performs 802.1Q tagging.

The CTC allows the user to assign specific ports to specific VLANs and prohibit ports from being part of specific VLANs. ONS 15454 ports can also be set to Untag or Tagged. See the "Provision Ethernet Ports for VLAN Membership" section on page 7-59 for more information on these operations.

Figure 7-5 Q-tag



7.5.2 IEEE 802.1Q Priority Queuing (formerly IEEE 802.1P)

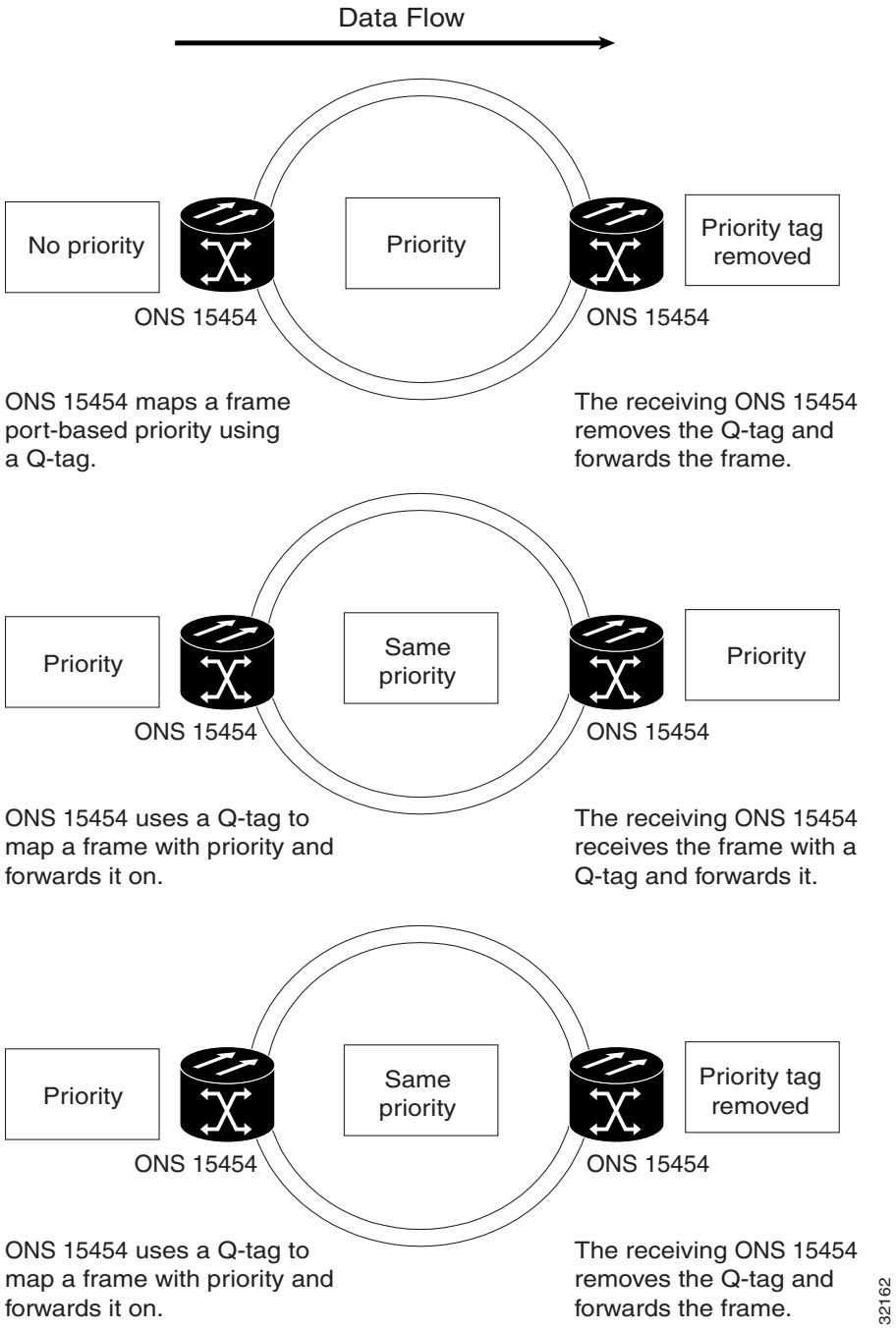
Priority Queuing eases network congestion by mapping Ethernet traffic to different priority levels. Networks without Priority Queing handle all packets on a first-in-first-out basis. Priority Queuing assigns priorities to data packets. The ONS 15454 uses a “leaky bucket” algorithm to establish a weighted priority (not a strict priority). A weighted priority gives high-priority packets greater access to bandwidth, but does not totally preempt low priority packets. 70% of bandwidth goes to the high priority que and the remaining 30% goes to the low priority que. Low priority packets can also be dropped when the network is congested. The ONS 15454 takes the eight priorities specified in IEEE 802.1Q and maps them to two queues (shown in Table 7-3). Priority Queuing information is carried through the network via IEEE 802.1Q tags

.

Table 7-3 Priority Queuing

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

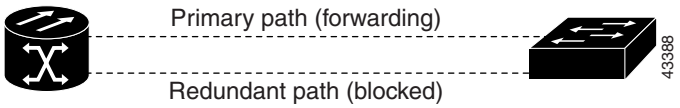
Figure 7-6 Priority Queuing



7.6 Spanning Tree

STP detects and eliminates network loops. By default, the ONS 15454 uses IEEE 802.1D STP on the optical line interfaces. When STP detects multiple paths between any two network hosts, STP blocks ports until only one path exists between any two network hosts (Figure 7-7). The single path eliminates possible bridge loops.

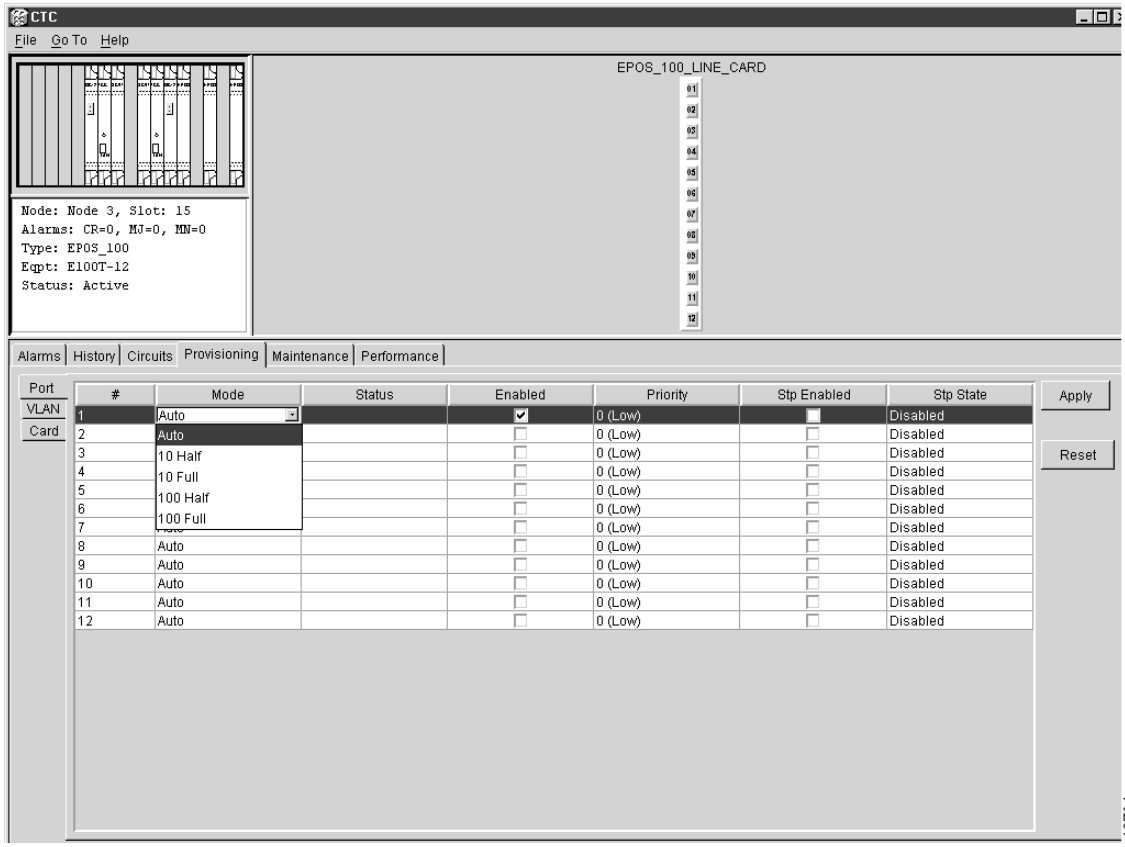
Figure 7-7 Spanning Tree Blocked Path



When loops occur, some Ethernet switches see the same stations transmitting data on more than one interface. This condition disables the forwarding algorithm and allows duplicate frames to be forwarded. 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 re-establish the link. STP operation is transparent to end stations, which do not discriminate between connections to a single LAN segment or a switched LAN with multiple segments. The ONS 15454 supports one STP instance per circuit up to a maximum of eight instances per shelf.

Starting with Release 2.2.0, users have the ability to enable STP on the Ethernet ports of the E100 and E1000 cards. This allows redundant circuit paths to be available for additional fault tolerance, but not cause a loop, as they are blocked by STP.

Figure 7-8 Enabling Spanning Tree



Procedure: Enable Spanning Tree on Ethernet Ports

Step 1 At the card-level view, click the **Provisioning** tab and the **Port** subtab.

Step 2 In the left-hand column, find the applicable port number and check the **Stp Enabled** box to enable STP for that port (see Figure 7-8).

Step 3 Click **Apply**.

7.6.1 Spanning Tree Parameters

Default spanning tree parameters are appropriate for most situations. Contact the Technical Assistance Center (TAC) at 1-877-323-7368 *before* you change the default STP parameters.

At the node view click the **Maintenance**>**Spanning Trees> Etherbridge** tabs to view spanning tree parameters.

Figure 7-9 Spanning Tree Parameters

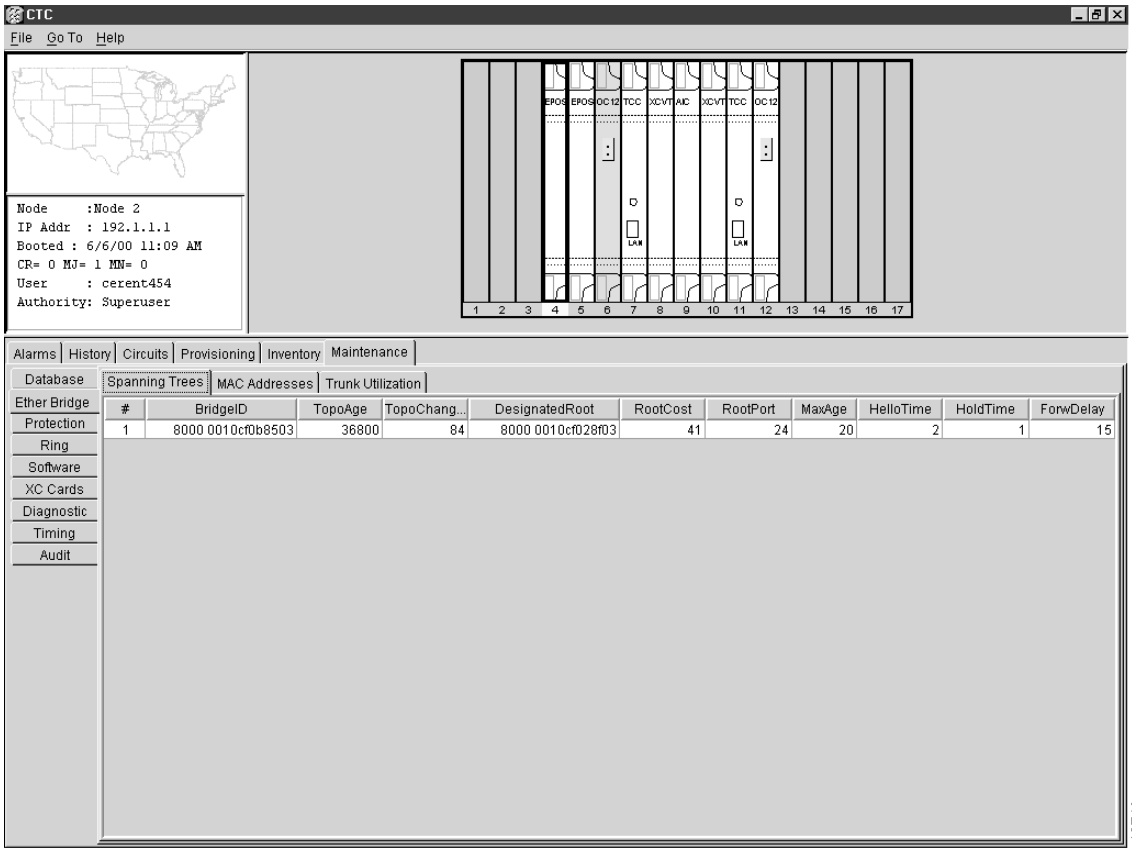


Table 7-4 Spanning Tree Parameters

BridgeID	The unique identifier of the ONS 15454 that is transmitting the configuration bridge protocol data unit (BPDU). The bridge ID combines ONS 15454's MAC address and Priority.
TopoAge	The amount of time in seconds since the last topology change.
TopoChanges	Number of times the spanning tree topology has been changed since the shelf was booted.
DesignatedRoot	Identifies the spanning tree's designated root for a particular spanning tree instance.
RootCost	Identifies the total path cost to the designated root.
RootPort	The port used to reach the root.
MaxAge	The maximum time that received-protocol information is retained before it is discarded.
HelloTime	The time interval, in seconds, of the transmission of configuration BPDUs by a bridge attempting to become the spanning tree root or a bridge that is the spanning tree root.
HoldTime	The minimum time period, in seconds, that elapses during the transmission of configuration information on a given port.
ForwardDelay	The time spent by a port in the listening state and the learning state.

7.6.2 Spanning Tree Configuration

To view the spanning tree configuration, at the node view click the **Provisioning** tab and **Etherbridge** subtab.

Figure 7-10 Spanning Tree Configuration

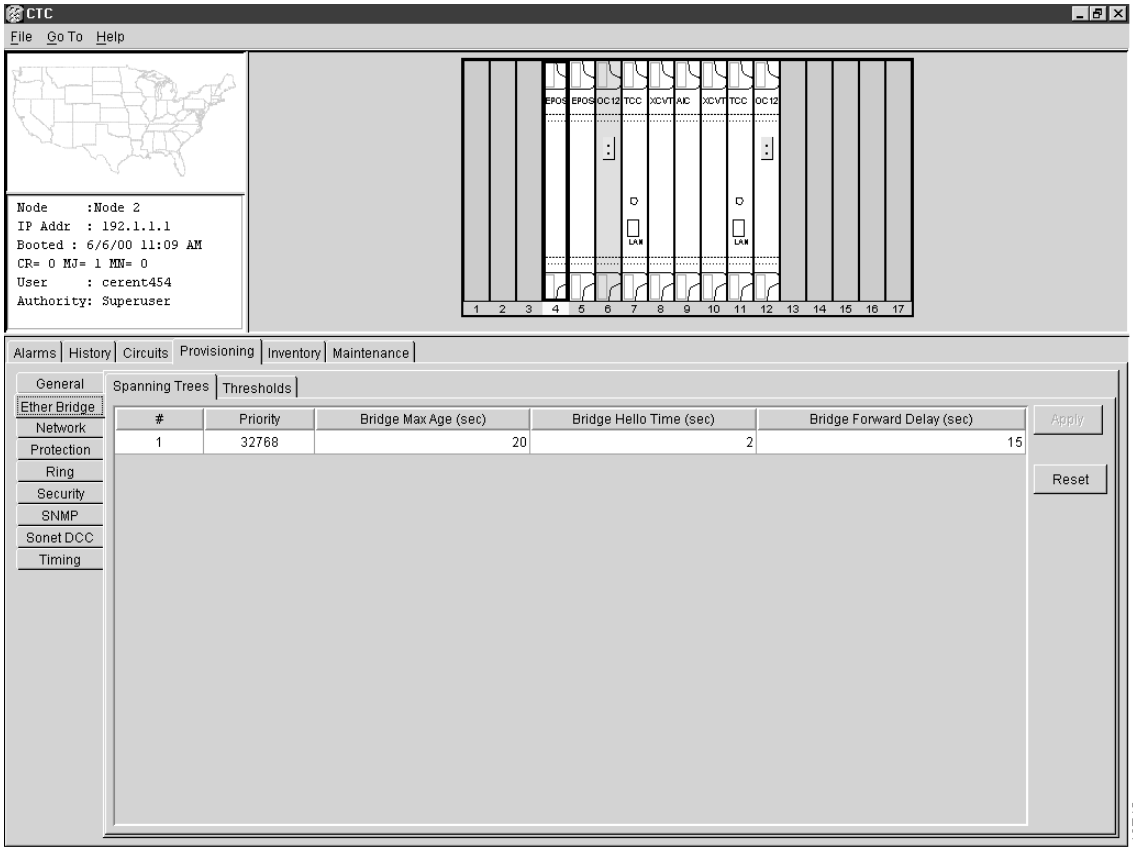
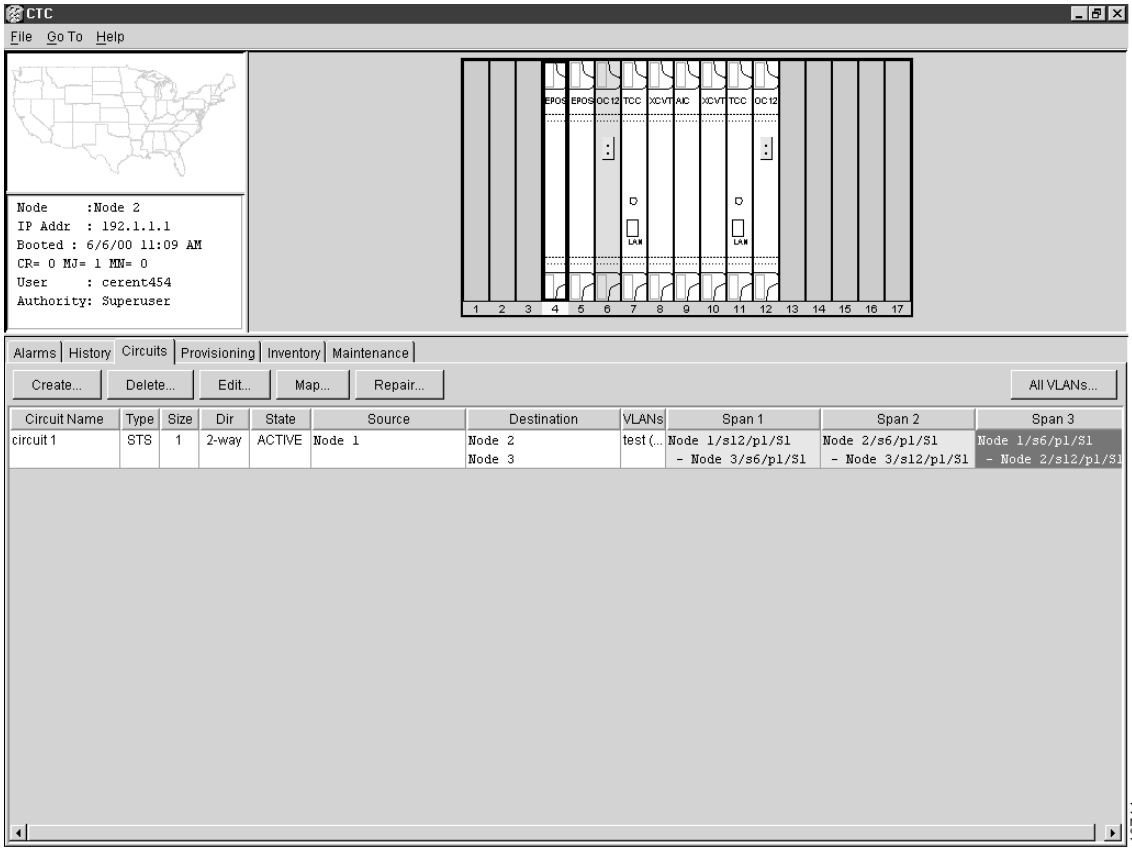


Table 7-5 Spanning Tree Configuration

Column	Default Value	Value Range
Priority	32768	0-65535
Bridge max age	20 seconds	6-40 seconds
Bridge Hello Time	2 seconds	1-10 seconds
Bridge Forward Delay	15 seconds	4-30 seconds

7.6.3 Viewing Spanning Tree

Figure 7-11 Circuit Screen



Procedure: View Spanning Tree

Step 1 On the circuit screen (Figure 7-11), highlight an Ethernet circuit.

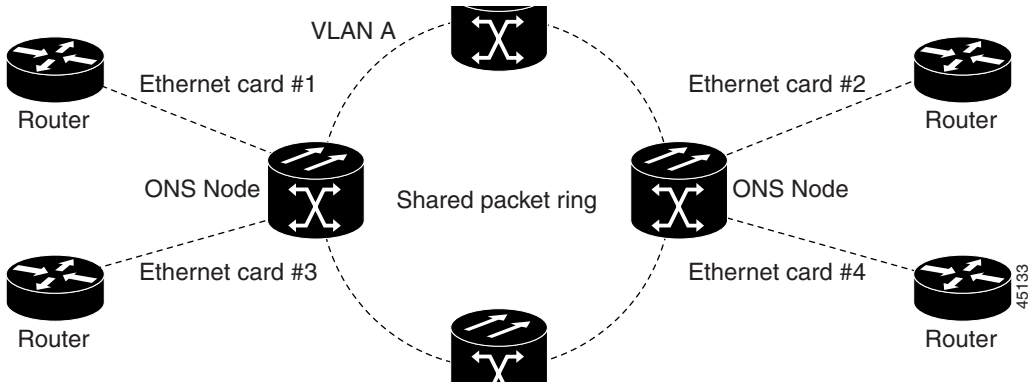
Step 2 Click the **Map** button.

Note On the spanning tree map, green represents forwarding spans and purple represents blocked (protect) spans. If you have a packet ring configuration, at least one span should be purple.

7.7 Multicard and Single-card EtherSwitch

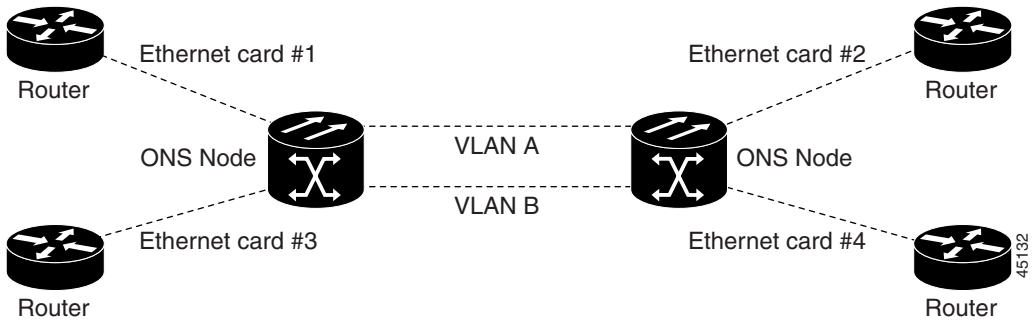
Release 2.0 of the ONS 15454 used multicard EtherSwitch exclusively. As Ethernet cards were added within a shelf, they would combine to form a single layer 2 switch. The bandwidth of the single switch formed by the Ethernet cards matches the bandwidth of the provisioned Ethernet circuit up to STS-6C worth of bandwidth. Figure 7-12 illustrates a multicard EtherSwitch configuration.

Figure 7-12 Multicard EtherSwitch



In Release 2.2.0 and later, single-card EtherSwitch Ethernet is an additional option that allows each Ethernet card to remain a single switching entity within the ONS 15454 shelf. Both E100 and E1000 cards allow either multicard EtherSwitch or single-card EtherSwitch operation. Single-card EtherSwitch allows a full STS-12C worth of bandwidth between two Ethernet circuit points. Figure 7-13 illustrates a single-card EtherSwitch configuration.

Figure 7-13 Single-card EtherSwitch



Seven scenarios for provisioning single-card EtherSwitch bandwidth are possible:

1. 12c
2. 6c 6c
3. 6c 3c 3c
4. 6c 6 STS-1s
5. 3c 3c 3c 3c
6. 3c 3c 6 STS-1s

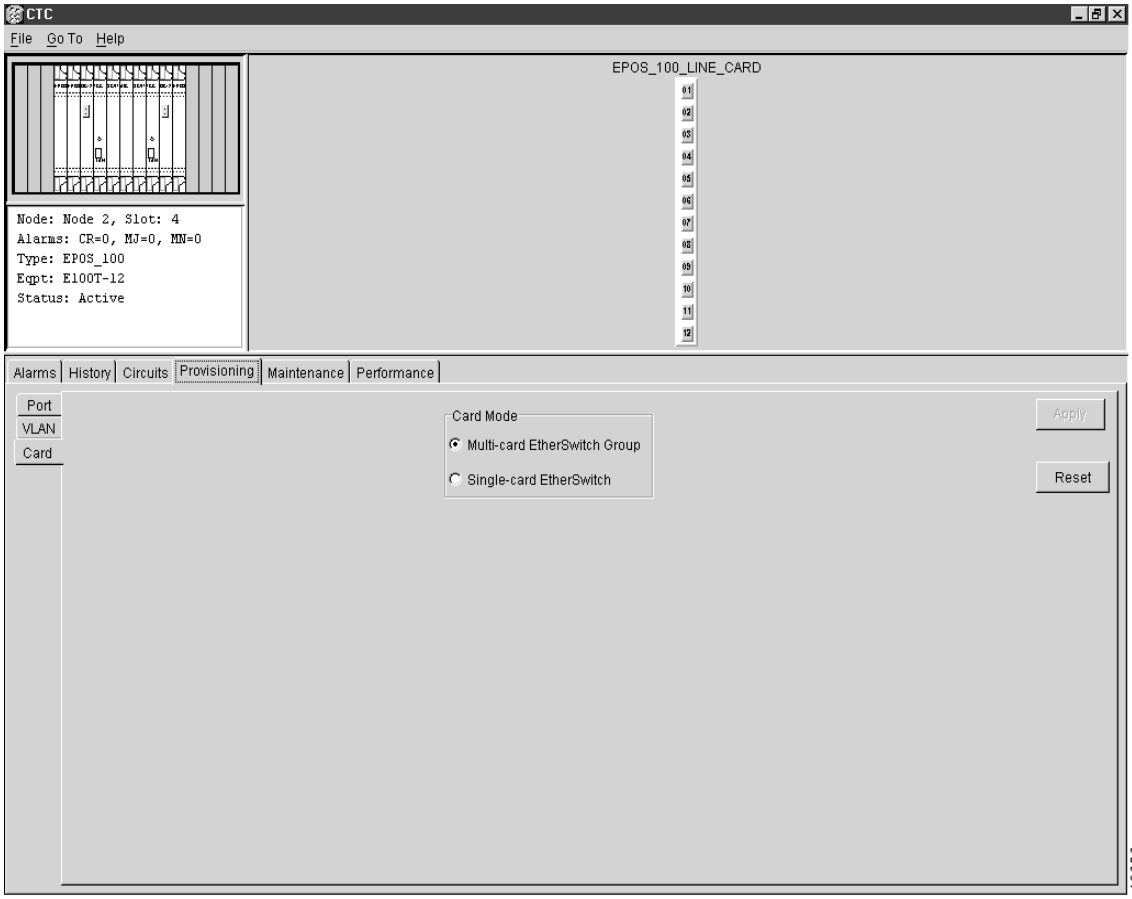
7 12 STS-1s

Note When configuring scenario 3, the STS 6c must be provisioned before either of the STS 3c circuits. A future software release will resolve this issue.

Note When deleting and recreating Ethernet circuits that have different sizes, all STS circuits provisioned to the EtherSwitch must be deleted before the new circuit scenario is created. A future software release will resolve this issue.

Figure 7-14 illustrates the Card Mode screen where the EtherSwitch option is provisioned.

Figure 7-14 Card Mode



7.8 ONS 15454 Ethernet Circuit Configurations

There are three common methods for configuring Ethernet circuits between ONS 15454 nodes: a straight circuit configuration, a shared packet ring configuration, and a hub and spoke configuration. Two nodes usually connect with a straight circuit configuration. More than two nodes usually connect with a shared packet ring configuration or a hub and spoke configuration.

Figure 7-15 shows a straight circuit configuration, Figure 7-16 shows a shared packet ring configuration, and Figure 7-17 shows a hub and spoke configuration.

Figure 7-15 Straight Circuit Configuration

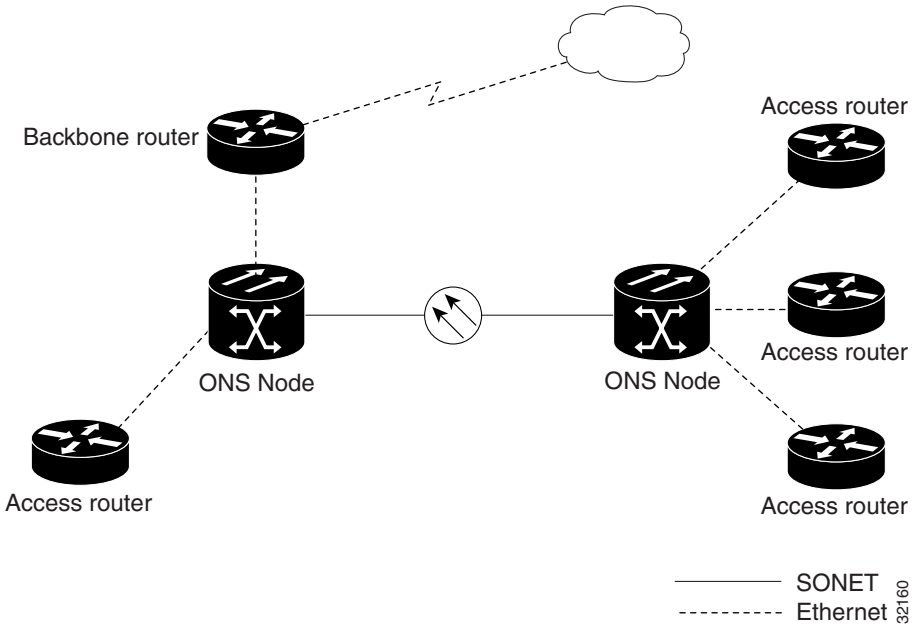


Figure 7-16 Shared Packet Ring Ethernet Circuit Configuration

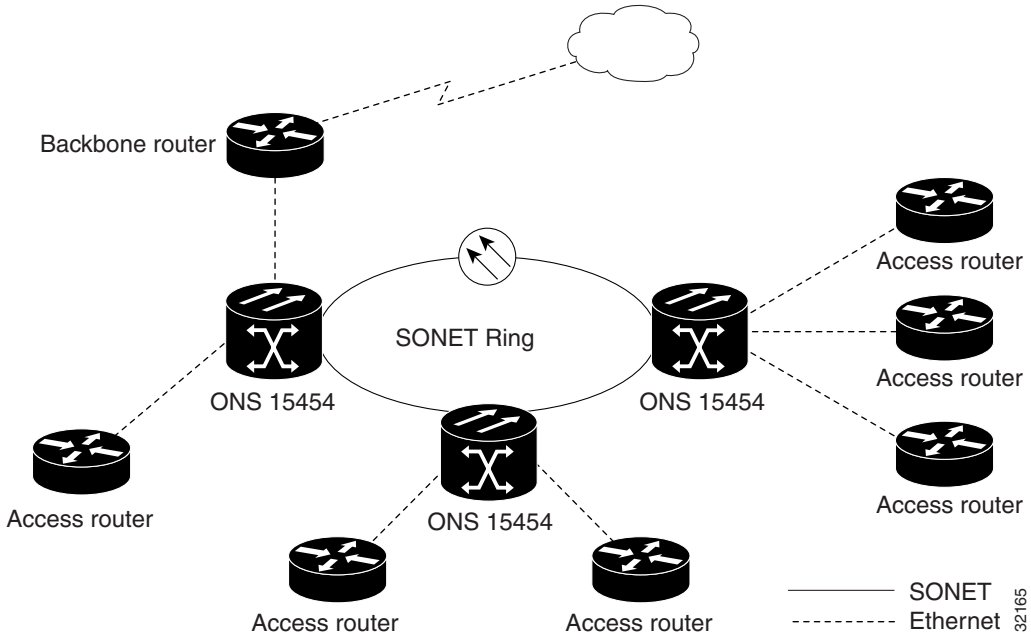
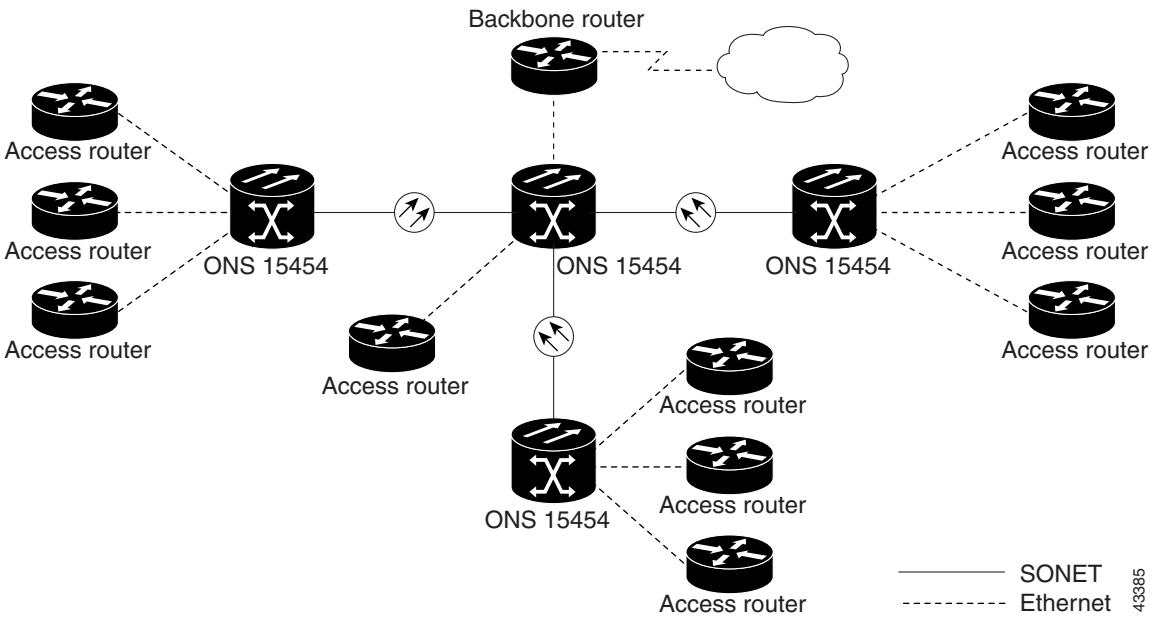


Figure 7-17 Hub and Spoke Ethernet Circuit Configuration



Note Before making Ethernet connections, choose a circuit size from STS-1, STS-3C, STS-6C, or STS-12C.

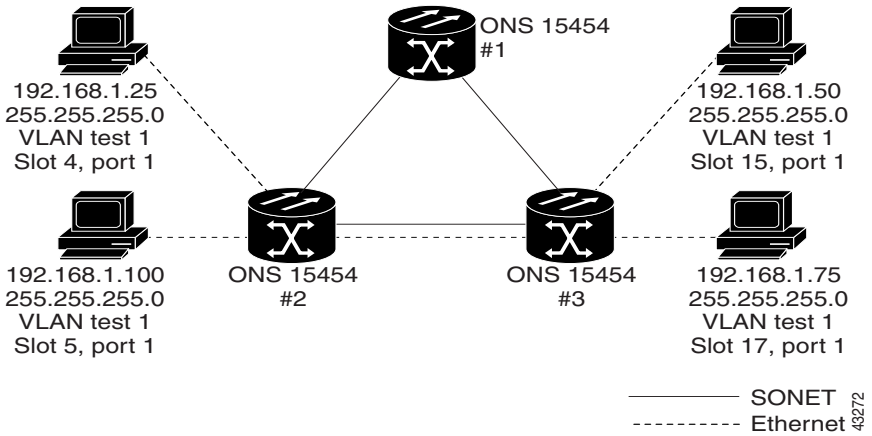
Note When making an STS-12C Ethernet circuit, the E100 and the E1000 cards must be configured as single-card EtherSwitch.

7.8.1 Multicard EtherSwitch Ethernet Circuit Provisioning

Procedure: Provision a Multicard Straight Ethernet Circuit

Note Single-card EtherSwitch allows a full STS-12C worth of bandwidth between two Ethernet circuit points. Multicard EtherSwitch limits bandwidth to STS-6C worth of bandwidth between two Ethernet circuit points.

Figure 7-18 Multicard Straight Circuit

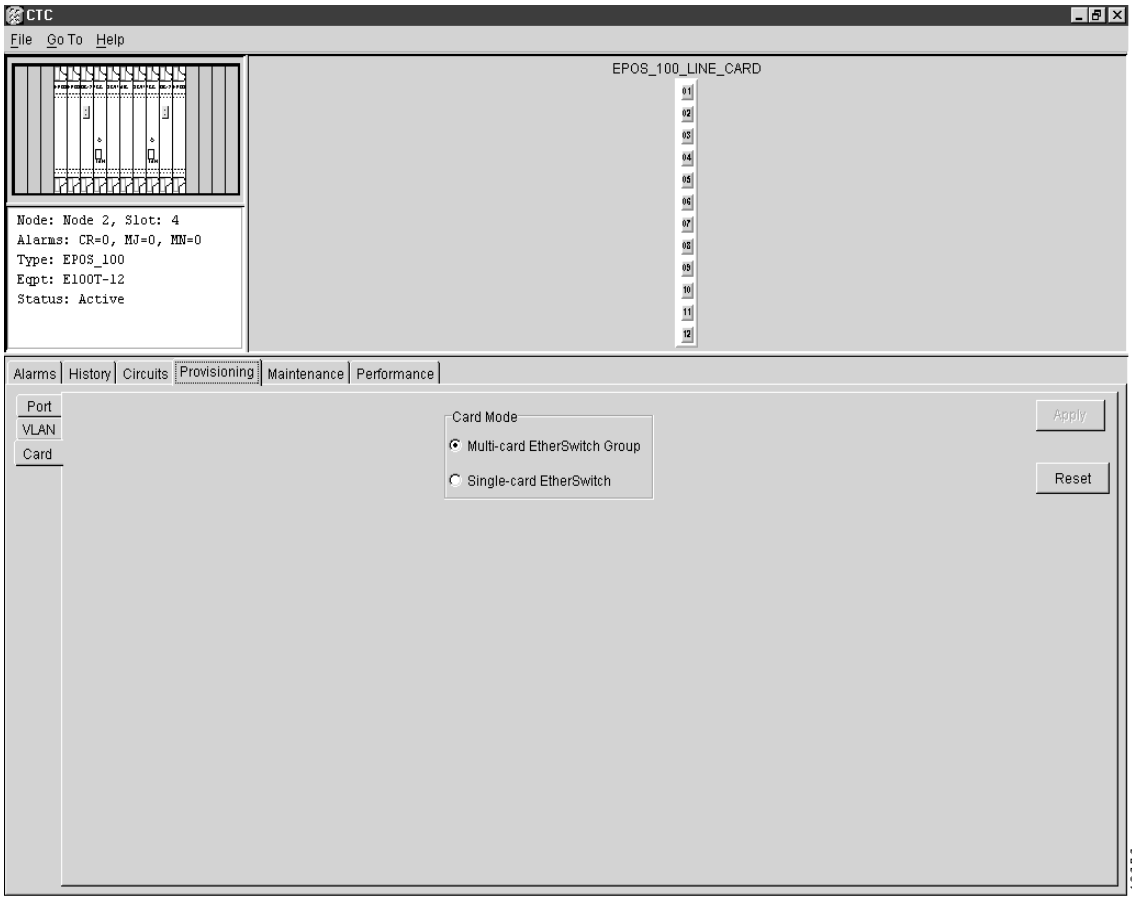


Step 1 Log into one of the ONS 15454 Ethernet circuit endpoints.

Step 2 Double click one of the Ethernet cards included in the circuit.

Step 3 Click the **Provisioning** tab and the **Card** subtab.

Figure 7-19 Card Mode Window



Step 4 Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.

Step 5 Display the node view.

Step 6 Repeat Steps 2-4 for all other Ethernet cards in the ONS 15454 that will make up the circuit.

Step 7 Log into the other ONS 15454 endpoint.

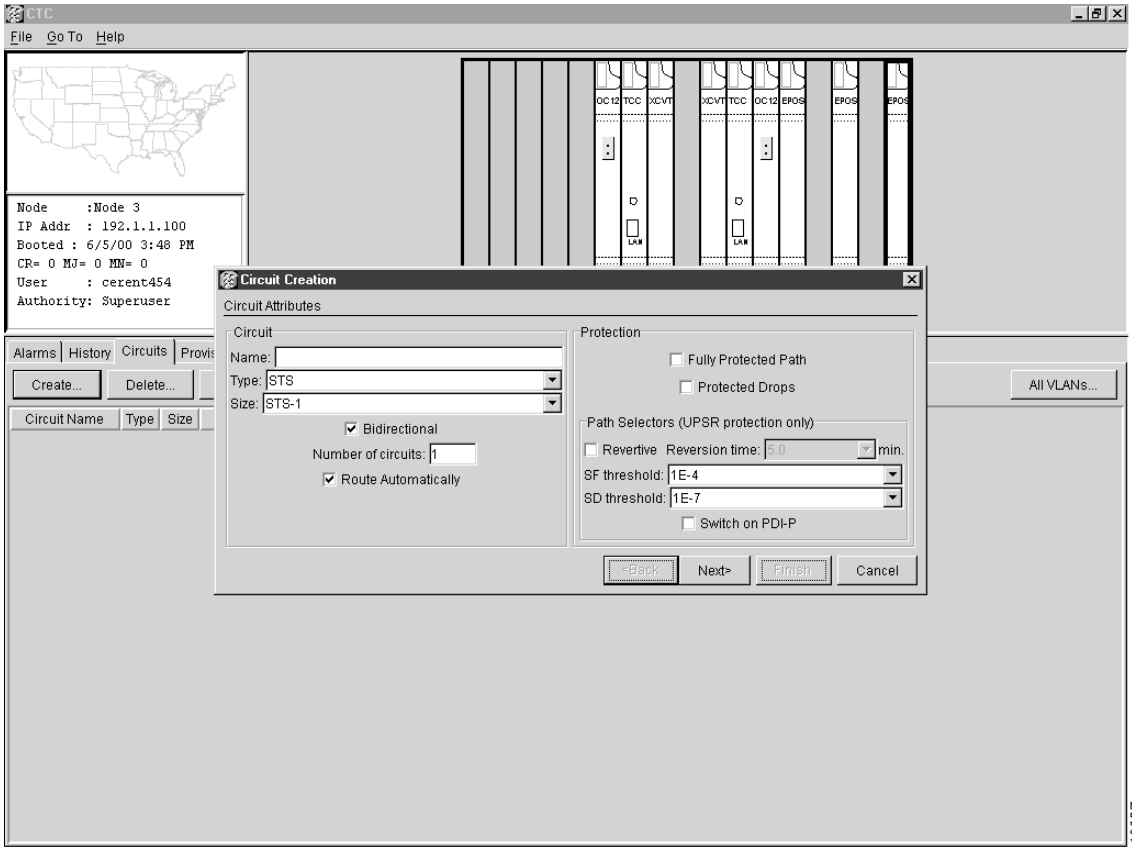
Step 8 Repeat Steps 2-6.

Step 9 Click the **Circuits** tab.

Step 10 Click **Create**.

The Circuit Attributes dialog opens (see Figure 7-20).

Figure 7-20 Circuit Attributes Dialog



Step 11 In the *Name* field, type a name for the circuit.

Step 12 From the Type menu, choose **STS**.

Note VT and VT Tunnel **Type:** do not apply to Ethernet circuits.

Step 13 Choose the size of the circuit from the Size menu.

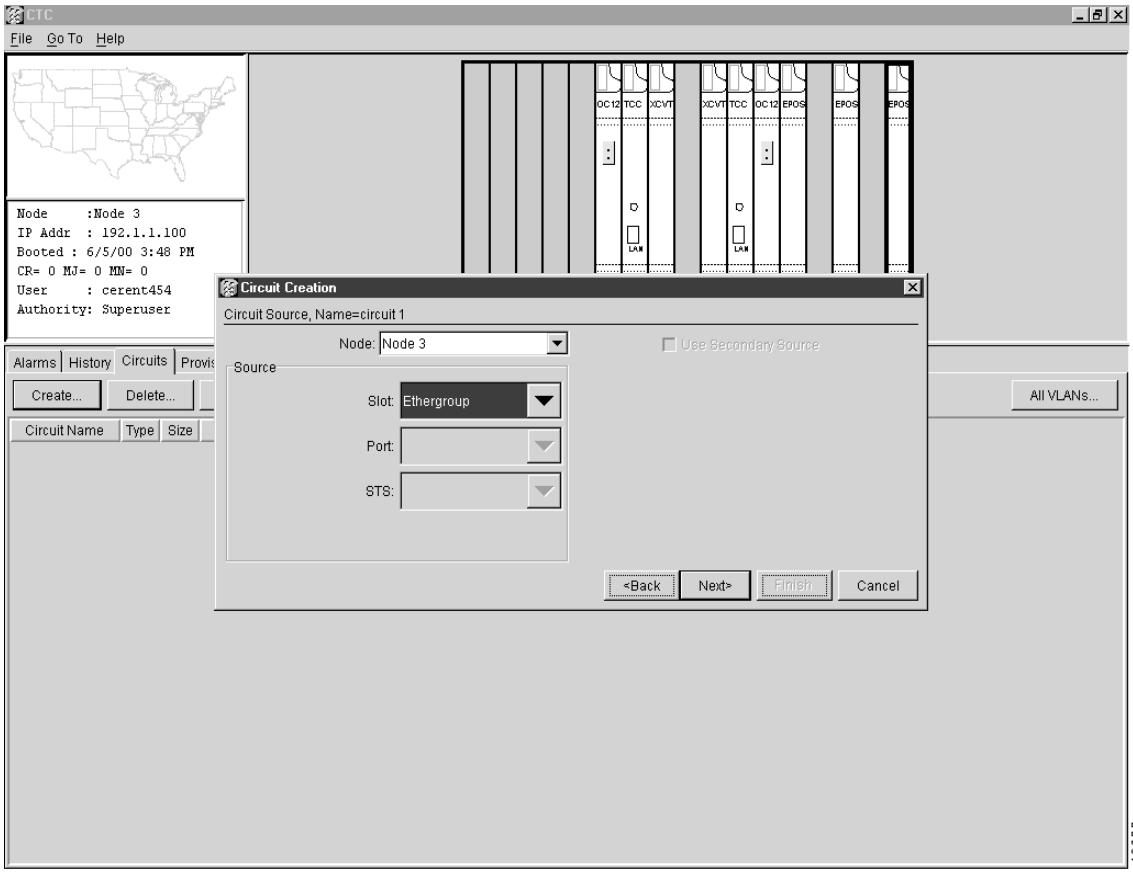
Note The valid circuit sizes for an Ethernet Multicard circuit are STS-1, STS-3C, and STS-6C.

Step 14 Verify that the Route Automatically box is checked.

Step 15 Verify that the Bidirectional box is checked.

Step 16 Click **Next**.

Figure 7-21 Circuit Source



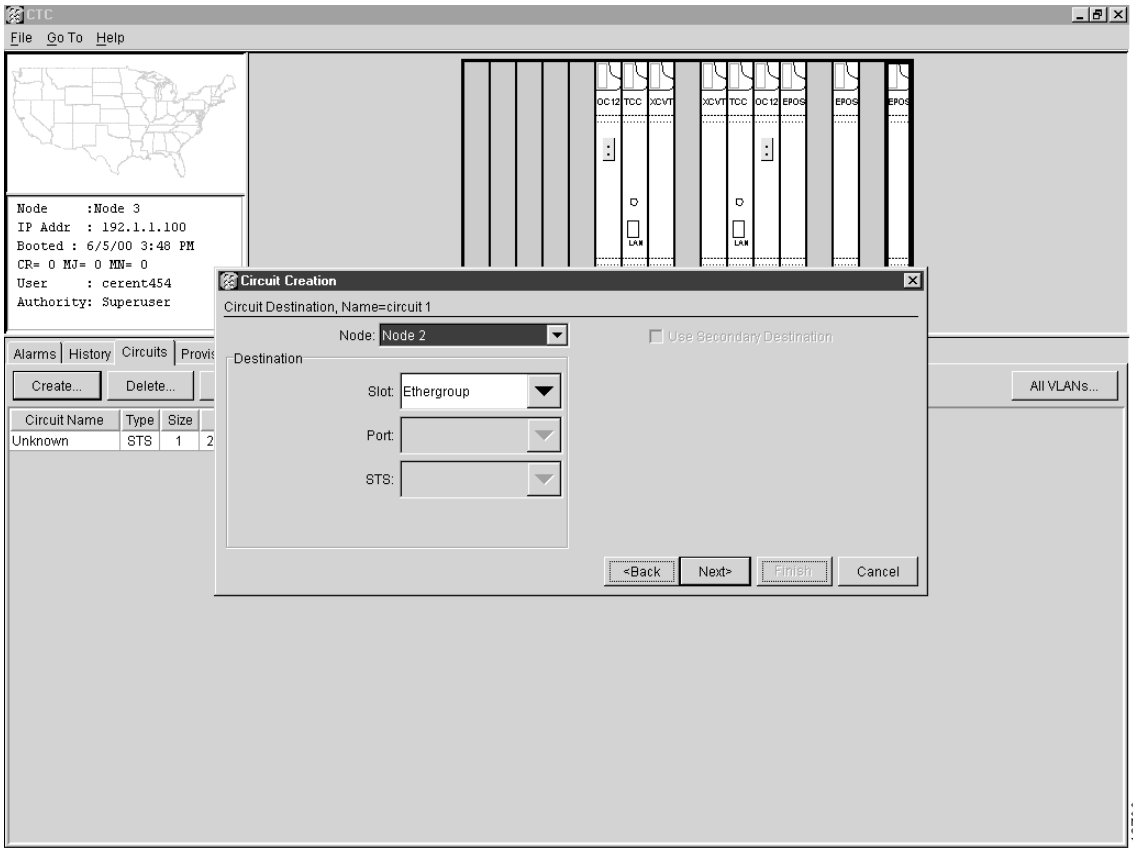
Step 17 Choose the circuit source from the Node menu (see Figure 7-21) in the circuit creation dialog box.

Note Either end node can be the circuit source.

Step 18 Choose Ethergroup from the Slot menu.

Step 19 Click **Next**.

Figure 7-22 Circuit Destination



Step 20 Choose a circuit destination from the **Node** menu (see Figure 7-22). Choose the node that is *not* the source.

Step 21 Choose **Ethergroup** from the Slot menu.

Step 22 Click **Next**.

The Circuit VLAN Selection window displays (see Figure 7-23).

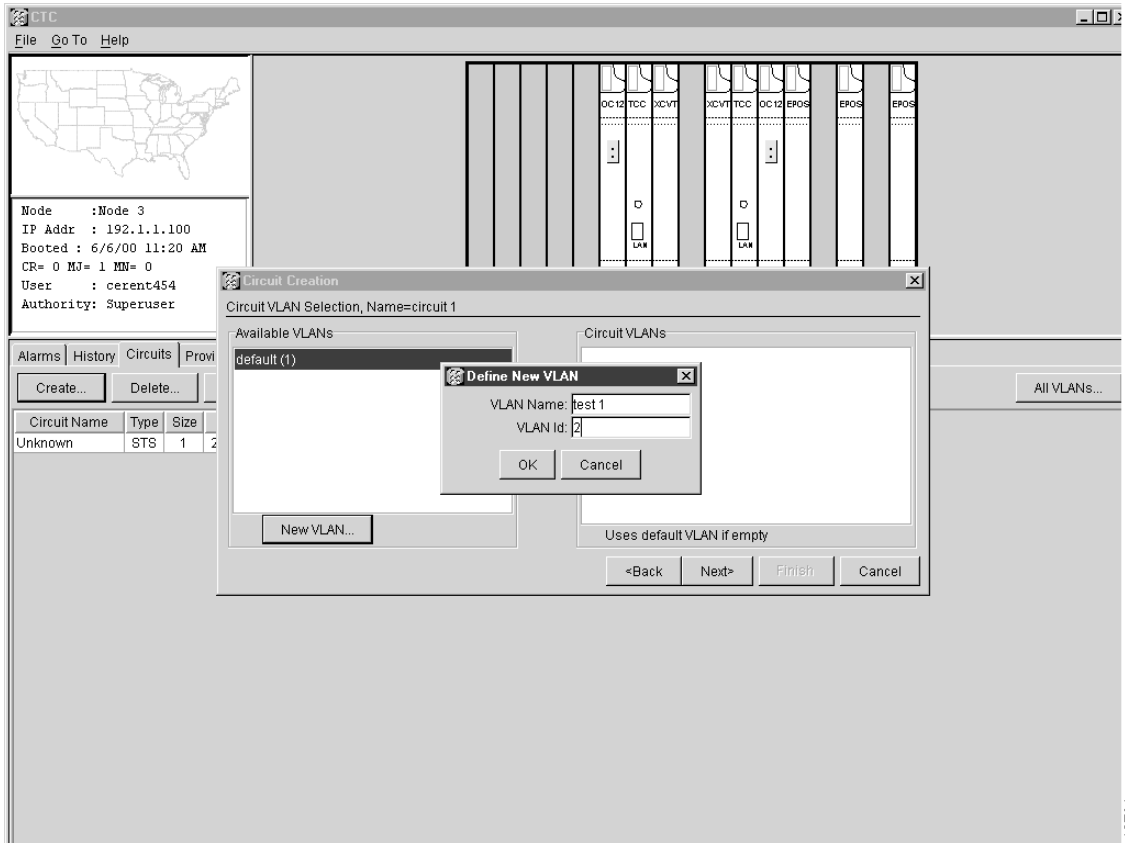
Note Do not use the default VLAN to pass traffic between nodes.

Step 23 Create the VLAN:

(a) Click the **New VLAN** tab.

The Define New VLAN dialog opens (see Figure 7-23).

Figure 7-23 Define New VLAN Dialog



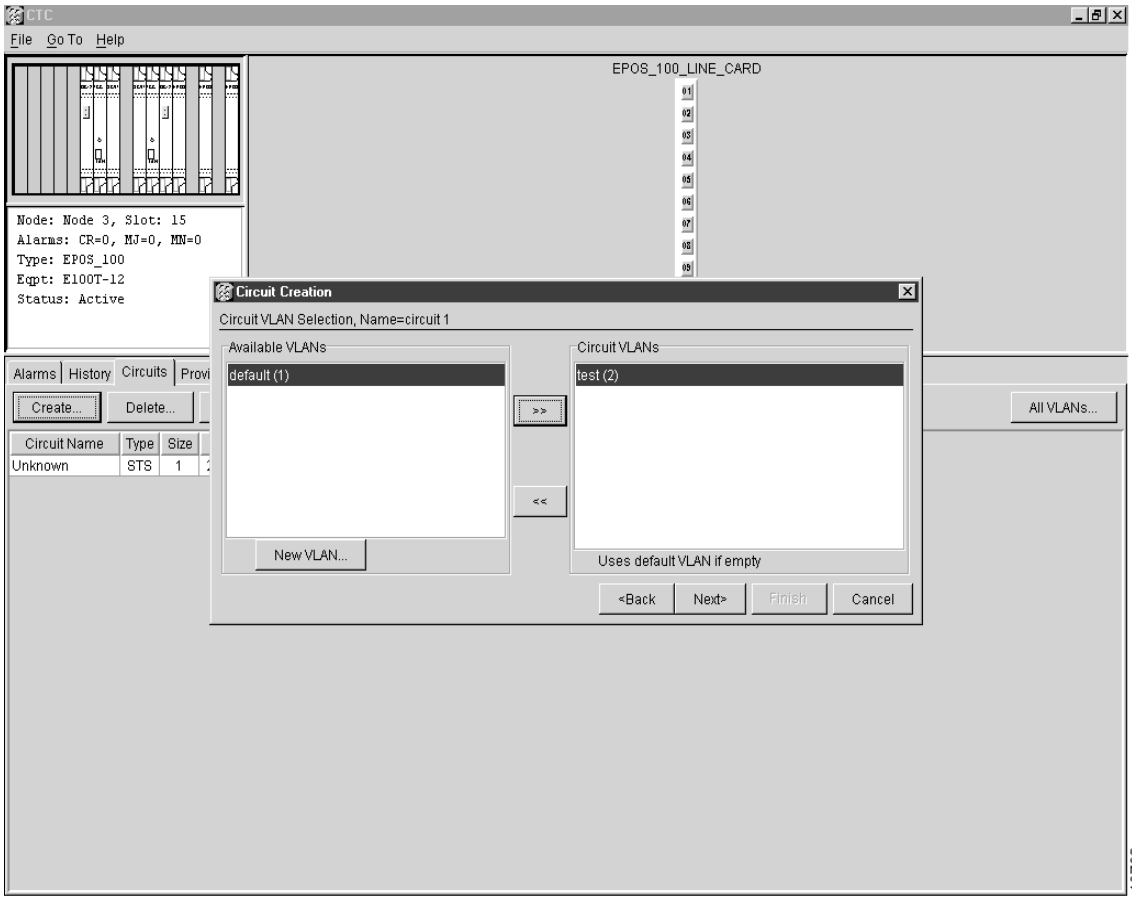
(b) Assign a name to your VLAN that will allow you to easily identify a particular network.

(c) Assign a VLAN ID.

This should be the next available number between 2 and 4093 that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user provisionable VLANs.

(d) Click **OK**.

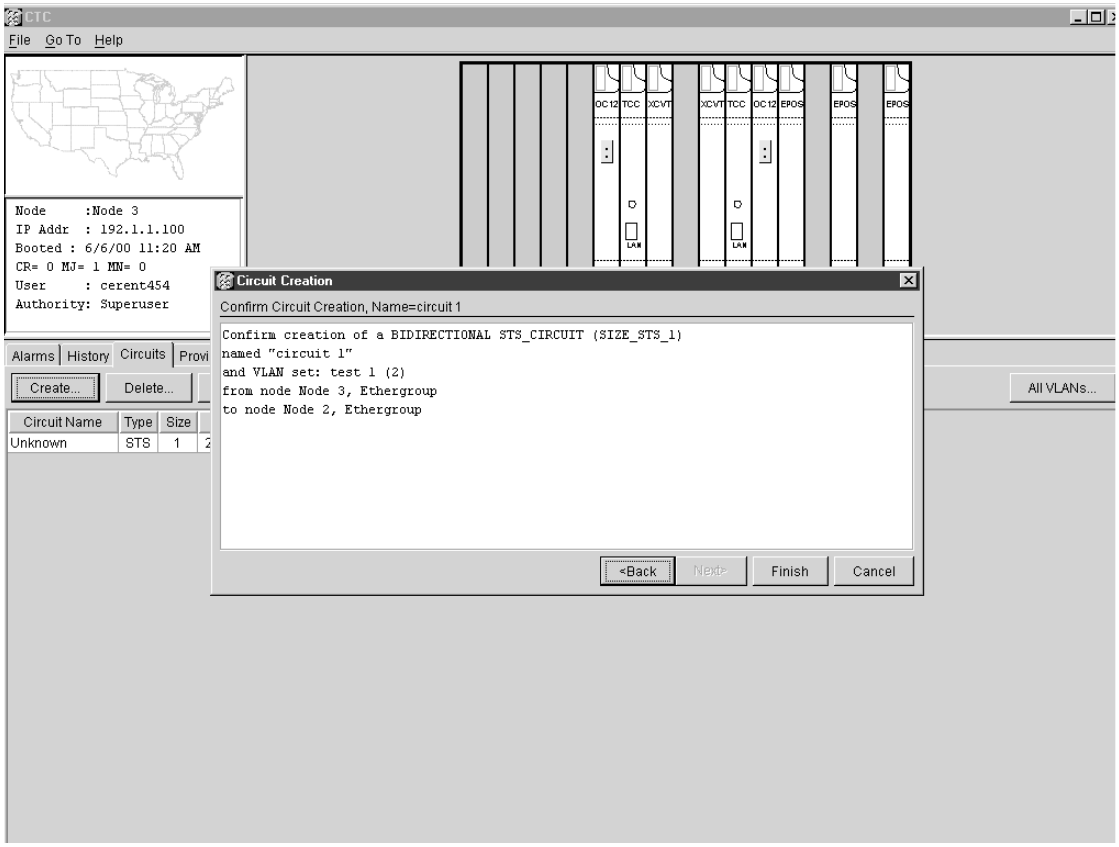
Figure 7-24 Circuit VLAN Selection



(e) Highlight the VLAN name and click the arrow **>>** tab to move the available VLAN(s) to the Circuit VLANs column.

Step 24 Click **Next**.

Figure 7-25 Circuit Confirmation



Step 25 The Confirm Circuit Creation dialog opens and displays the following information about the point-to-point circuit:

- Circuit is bidirectional Ethernet
- Circuit size
- Circuit name
- VLANs that will be transported across this circuit
- ONS 15454 nodes included in the circuit

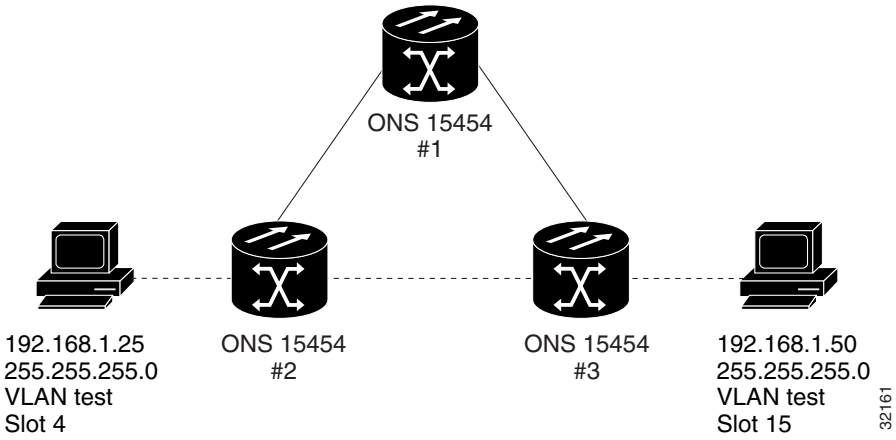
Note If the circuit information is not correct, use the <Back button to correct the information.

Step 26 Click **Finish**.

You now need to provision the Ethernet ports and assign these ports to VLANs. For port provisioning instructions, see the "VLAN Membership and Ethernet Port Provisioning" section on page 7-59. For information about manually provisioning circuits, see the "Ethernet Manual Cross-Connects" section on page 7-54.

Procedure: Provision a Single Card Ethernet Straight Circuit

Figure 7-26 Single-card Straight Circuit

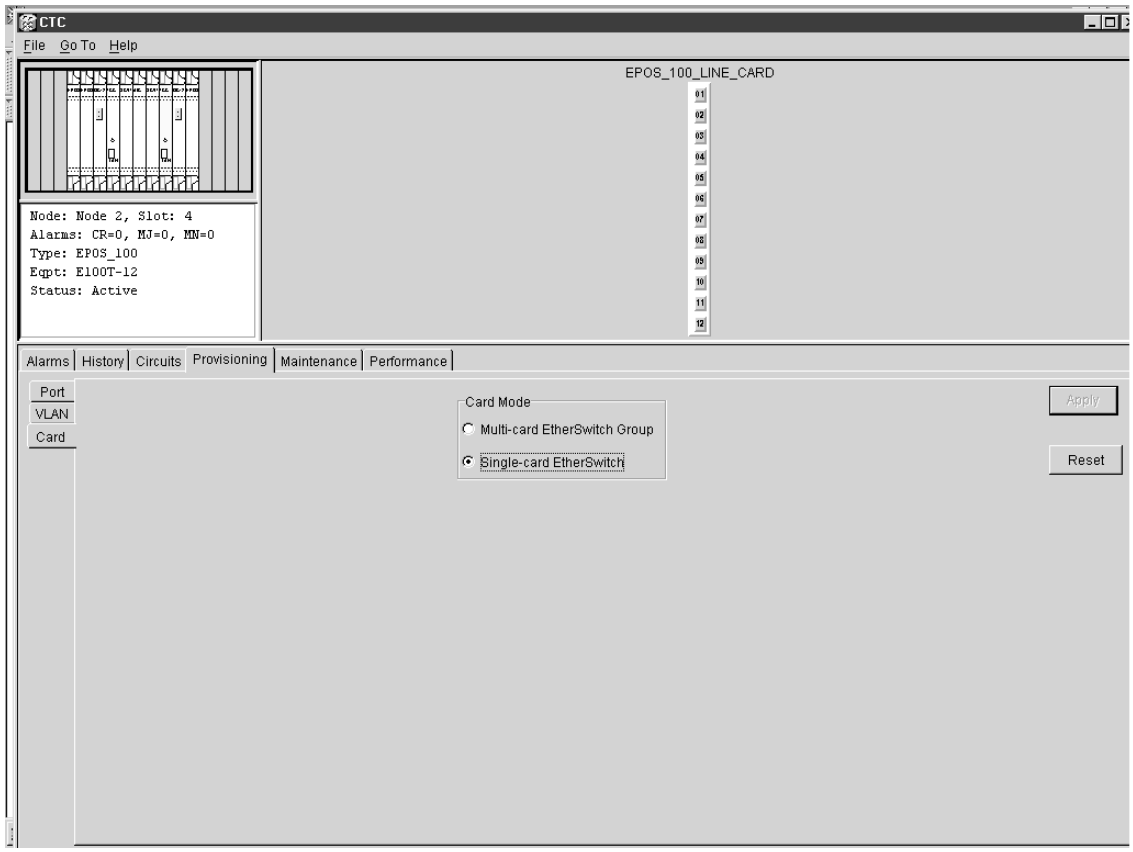


Step 1 Log into one of the ONS 15454 Ethernet circuit endpoints.

Step 2 Double click the Ethernet card that will make the circuit.

Step 3 Click the **Provisioning** tab and the **Card** subtab.

Figure 7-27 Single-card EtherSwitch Screen



Step 4 Under Card Mode, check the **Single-card EtherSwitch**.

Step 5 Click **Apply**.

Step 6 Log into the other ONS 15454 endpoint and repeat Steps 2-5.

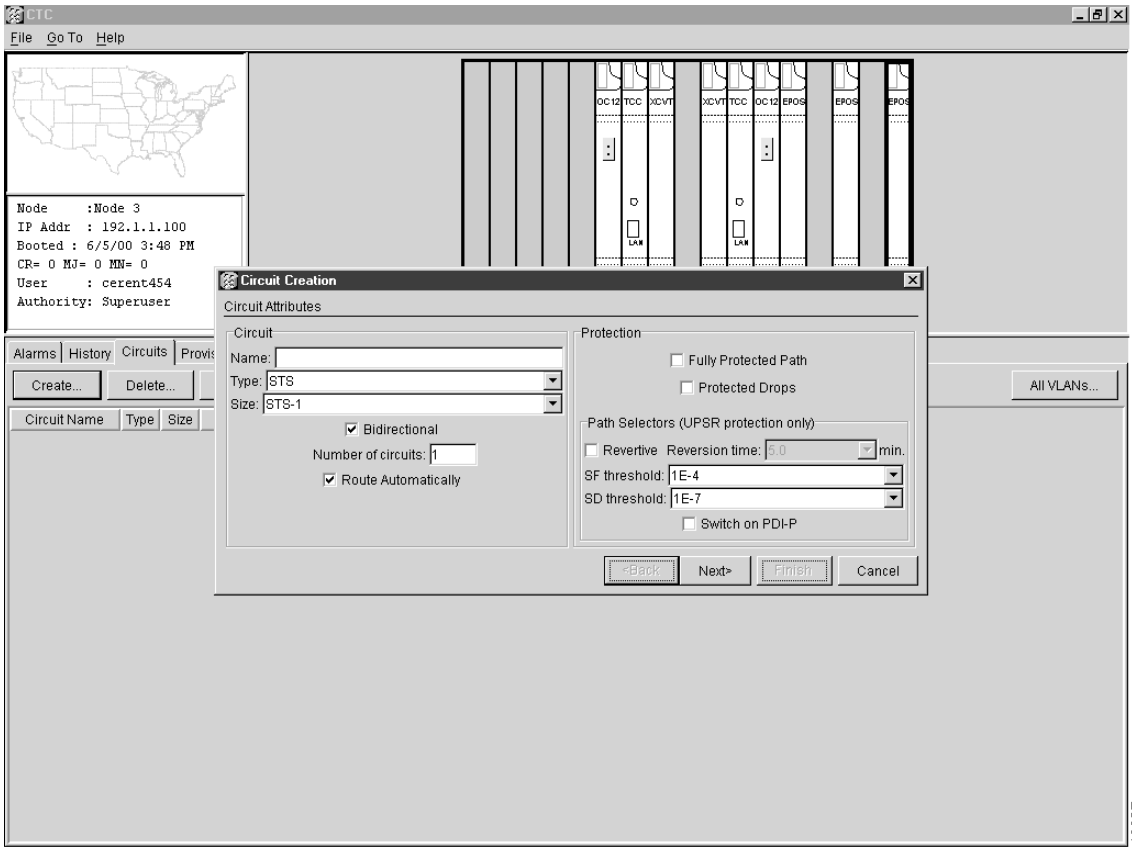
Step 7 Display the node view.

Step 8 Click the **Circuits** tab.

Step 9 Click **Create**.

The Circuit Attributes window opens.

Figure 7-28 Circuit AttributesDialog



Step 10 In the *Name* field, type a name for the circuit.

Step 11 From the Type menu, choose **STS**.

Note VT and VT Tunnel **Type:** do not apply to Ethernet circuits.

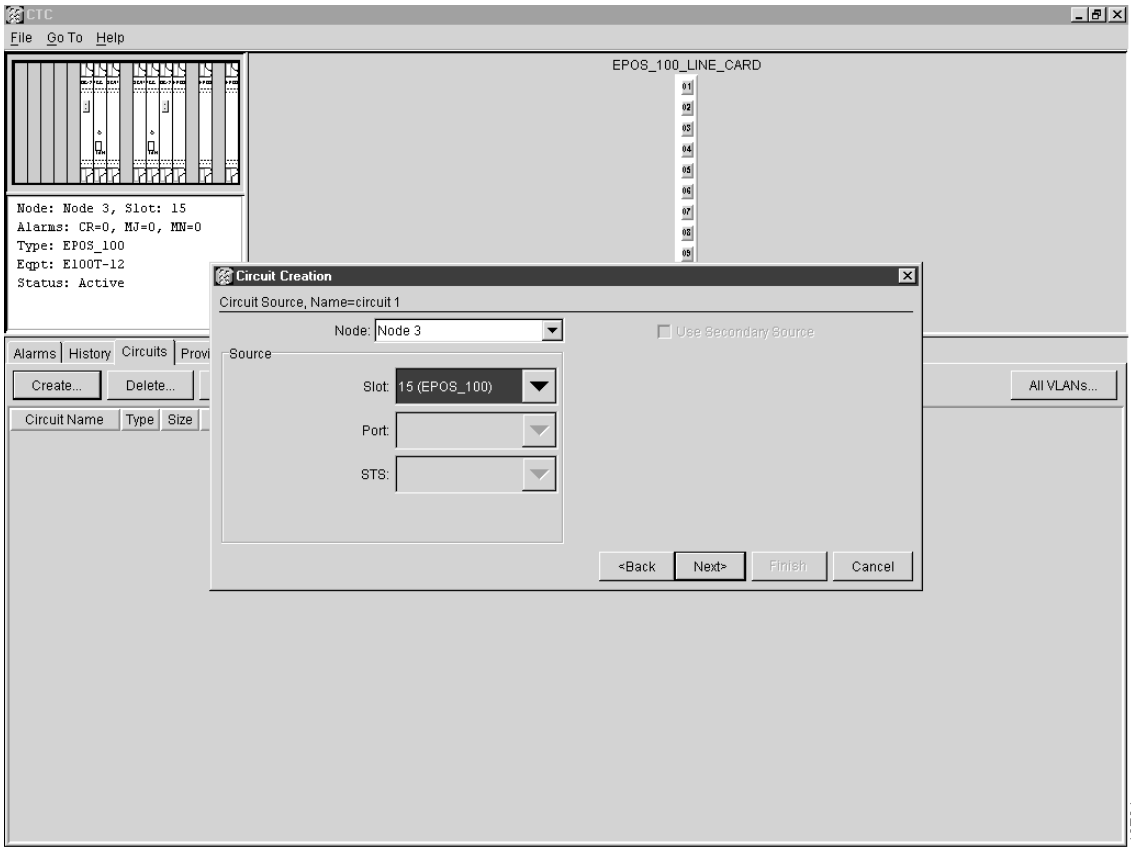
Step 12 Choose the size of the circuit from the Size menu.

Step 13 Verify that the Route Automatically box is checked.

Step 14 Verify that the Bidirectional box is checked.

Step 15 Click **Next**.

Figure 7-29 Circuit Source



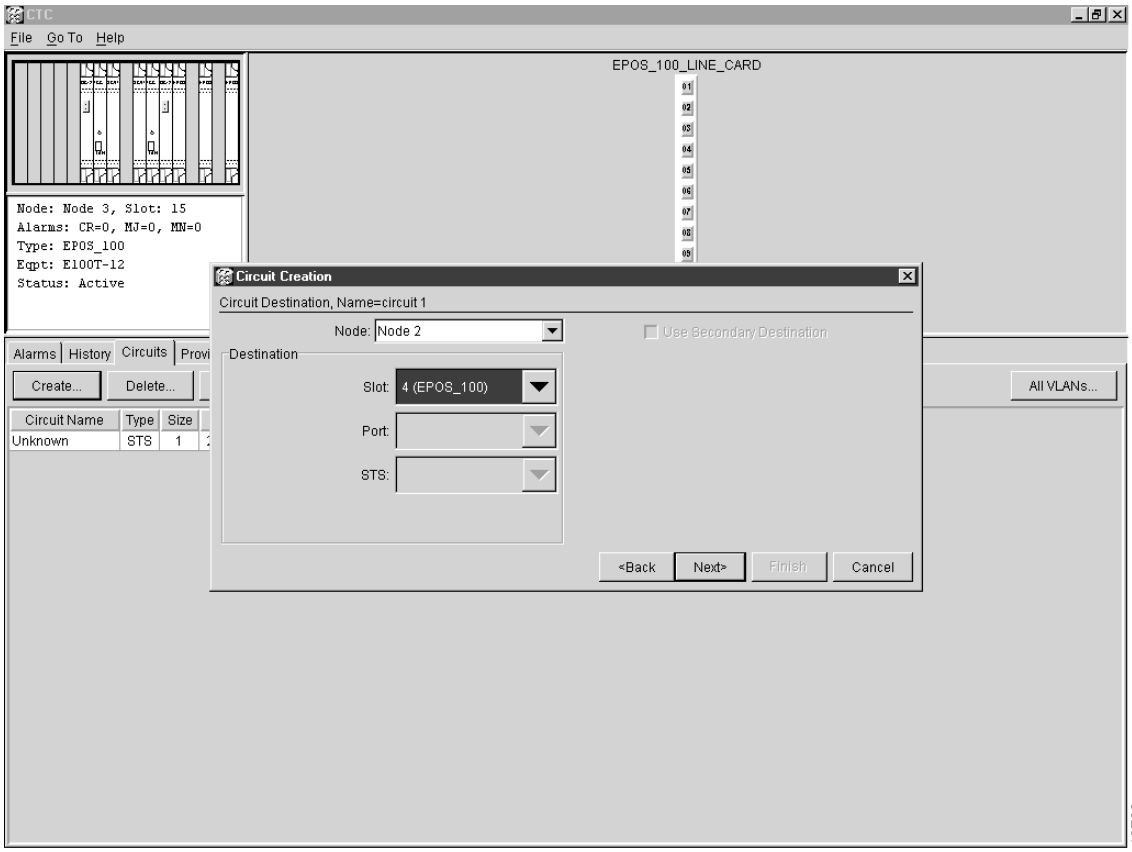
Step 16 Choose the circuit source from the Node menu.

Note Either end node can be the circuit source.

Step 17 From the Slot menu, choose the Ethernet card for which you enabled the single-card EtherSwitch.

Step 18 Click **Next**.

Figure 7-30 Circuit Destination



Step 19 Choose the circuit destination from the Node menu.

Note Choose the node that is *not* the source.

Step 20 From the slot menu, choose the Ethernet card for which you enabled the single-card EtherSwitch.

Step 21 Click **Next**.

The Circuit VLAN Selection window displays. See Figure 7-31.

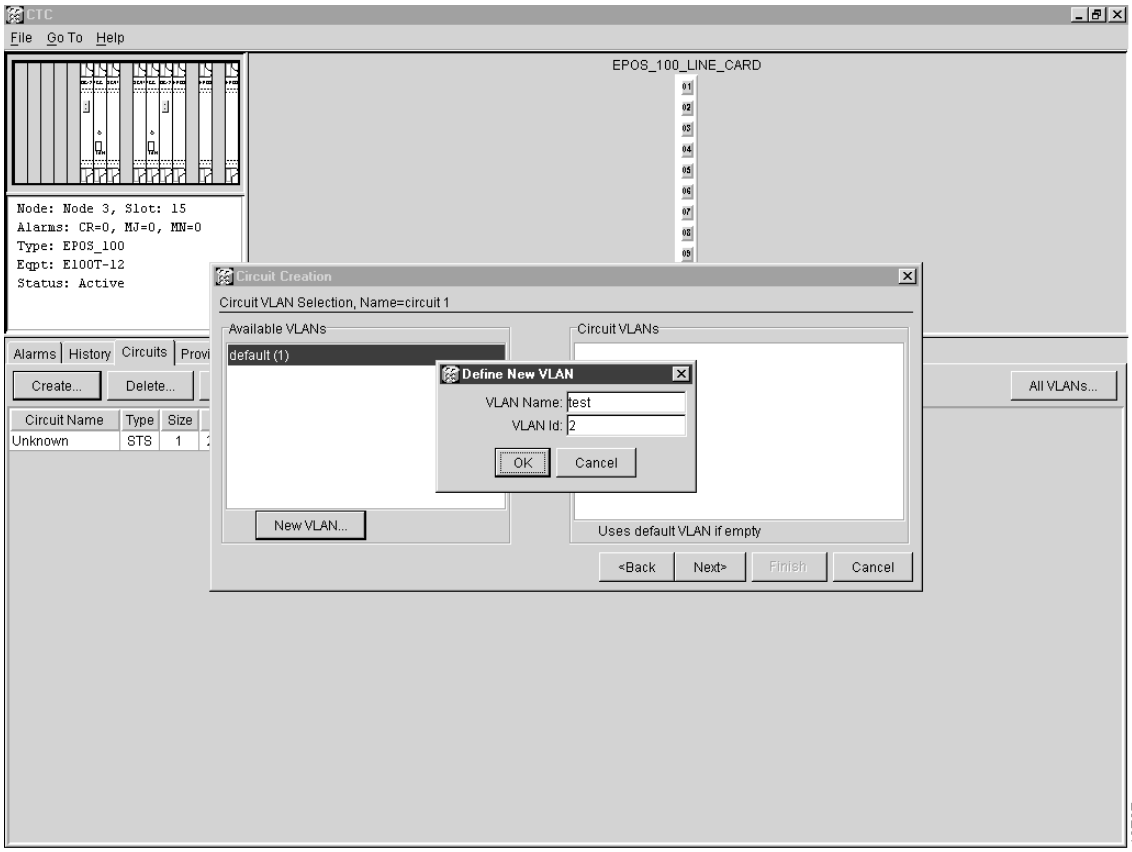
Note Do not use the default VLAN to pass traffic between nodes.

Step 22 Create the VLAN:

(a) Click the **New VLAN** tab.

The Define New VLAN dialog opens.

Figure 7-31 Define New VLAN Dialog



(b) Assign a name to your VLAN to help you easily identify a particular network.

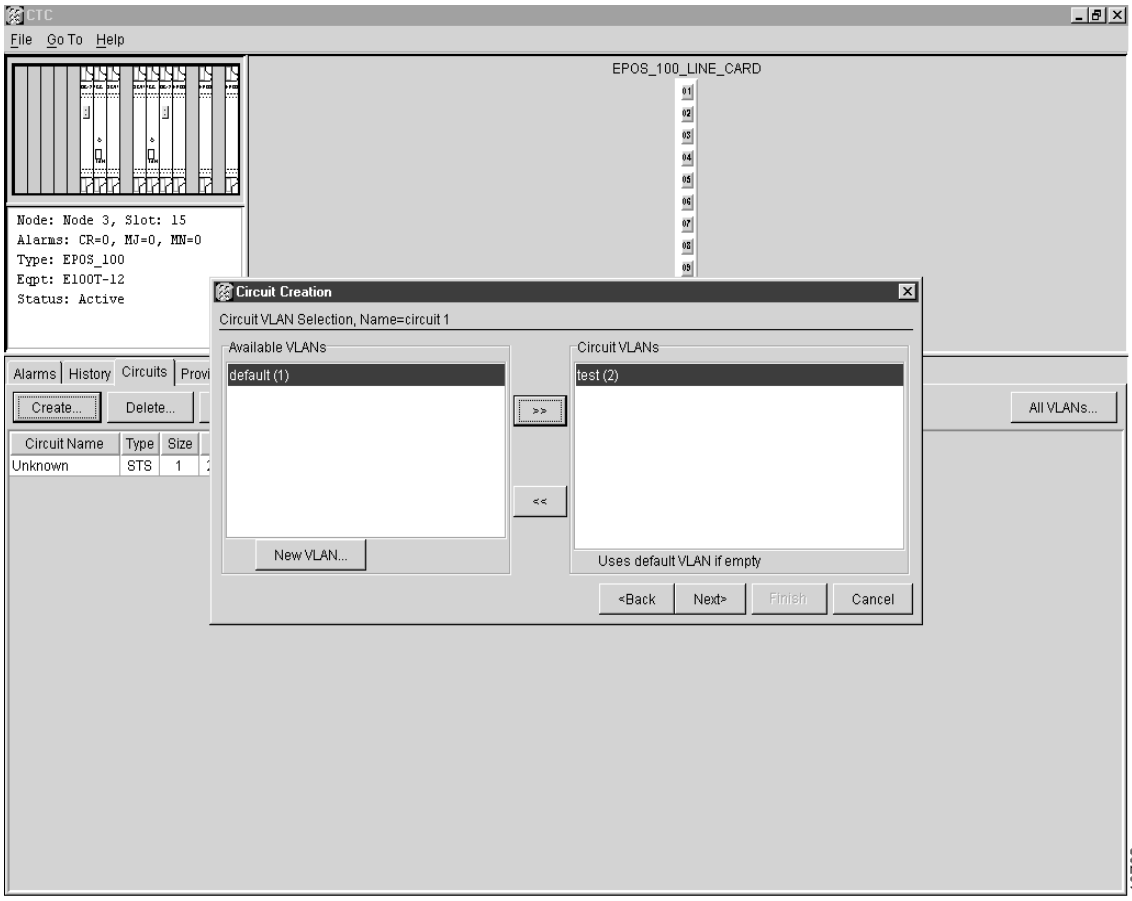
(c) Assign a VLAN ID.

This should be the next available number (between 2 and 4093) not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user provisionable VLANs.

(d) Click **OK**.

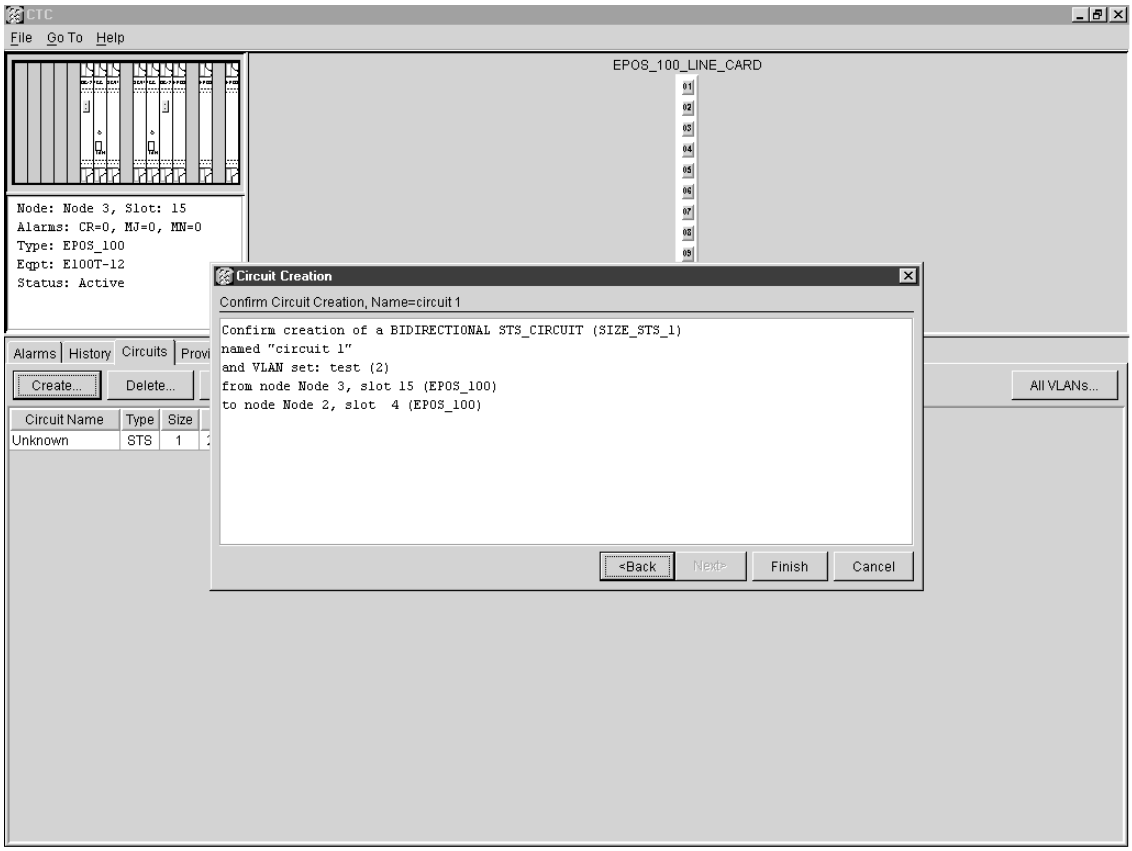
(e) Highlight the VLAN name and click the arrow **>>** tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (see Figure 7-32).

Figure 7-32 Circuit VLAN Selection



Step 23 Click **Next**.

Figure 7-33 Circuit Confirmation



The Confirm Circuit Creation dialog opens and displays the following information about the point-to-point circuit (see Figure 7-33):

- Circuit is bidirectional Ethernet
- Circuit size
- Circuit name
- VLANs that will be transported across this circuit
- ONS 15454 nodes included in the circuit

Note If the circuit information is not correct, use the <Back button to correct the information.

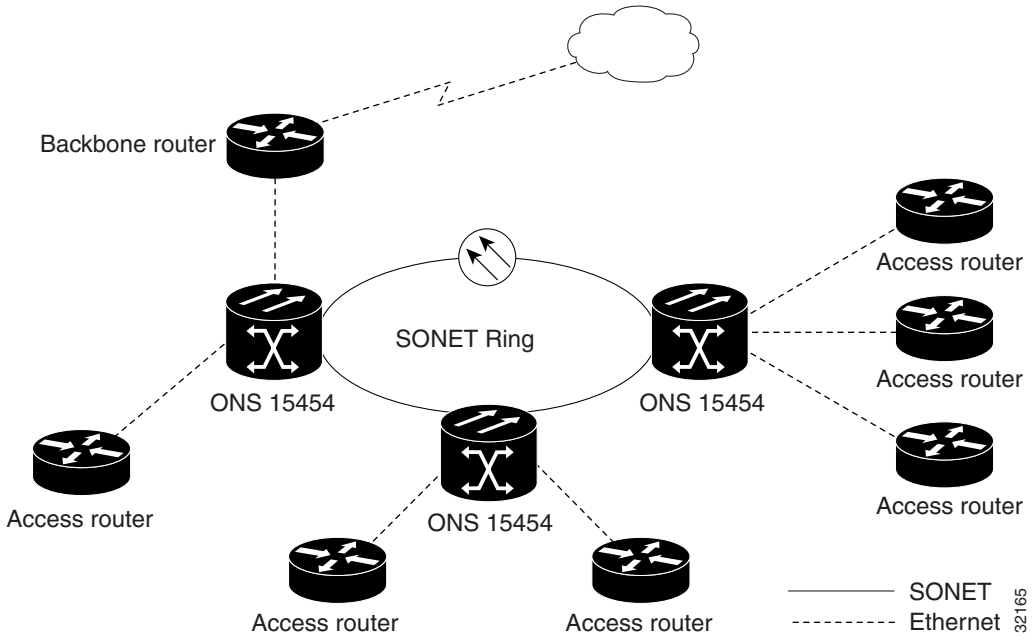
Step 24 Click **Finish**.

You now need to provision the Ethernet ports and assign these ports to VLANs. For port provisioning instructions, see the "VLAN Membership and Ethernet Port Provisioning" section on page 7-59. For information about manually provisioning circuits, see the "Ethernet Manual Cross-Connects" section on page 7-54.

7.8.2 Shared Packet Ring Ethernet Circuit Provisioning

This section provides steps for creating a shared packet ring. Figure 7-34 illustrates a sample shared packet ring. (Your network architecture may differ from the example.)

Figure 7-34 Shared Packet Ring



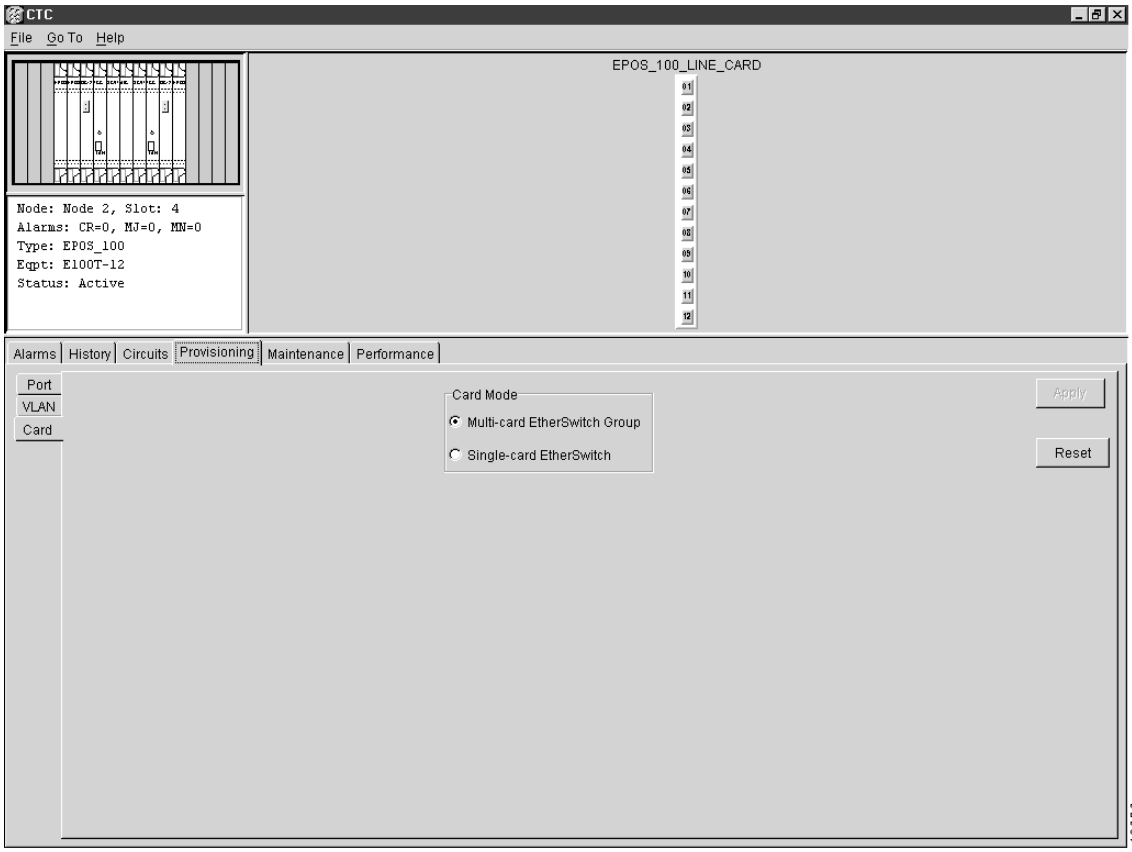
Procedure: Provision a Shared Packet Ring

Step 1 Log into one of the ONS 15454 Ethernet circuit endpoints.

Step 2 Double click one of the Ethernet cards that will make up the circuit.

Step 3 Click the **Provisioning** tab and the **Card** subtab.

Figure 7-35 Multicard EtherSwitch Group



Step 4 Under Card Mode, verify that **Multi-card EtherSwitch Group** is checked.

Step 5 Display the node view.

Step 6 Repeat Steps 2-4 for all other Ethernet cards in the ONS 15454 that will make up the shared packet ring.

Step 7 Log into the other ONS 15454 endpoint.

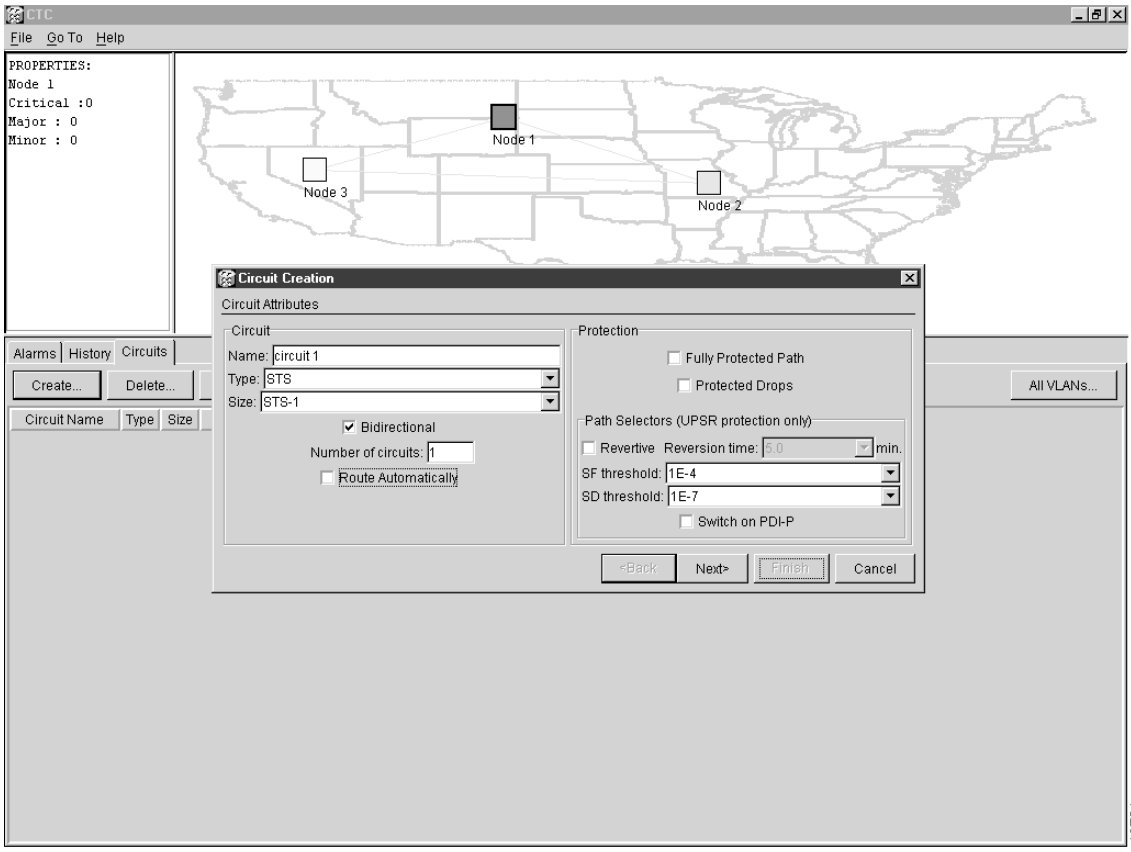
Step 8 Repeat Steps 2-6.

Step 9 Click the **Circuits** tab.

Step 10 Click **Create**.

The Circuit Creation dialog opens (see Figure 7-36).

Figure 7-36 Circuit Attributes Dialog



Step 11 In the *Name* field, type a name for the circuit.

Step 12 From the Type menu, choose **STS**.

Step 13 From the Size menu, choose the size of the circuit.

Note For shared packet ring Ethernet, valid circuit sizes are STS-1, STS-3C, and STS-6C.

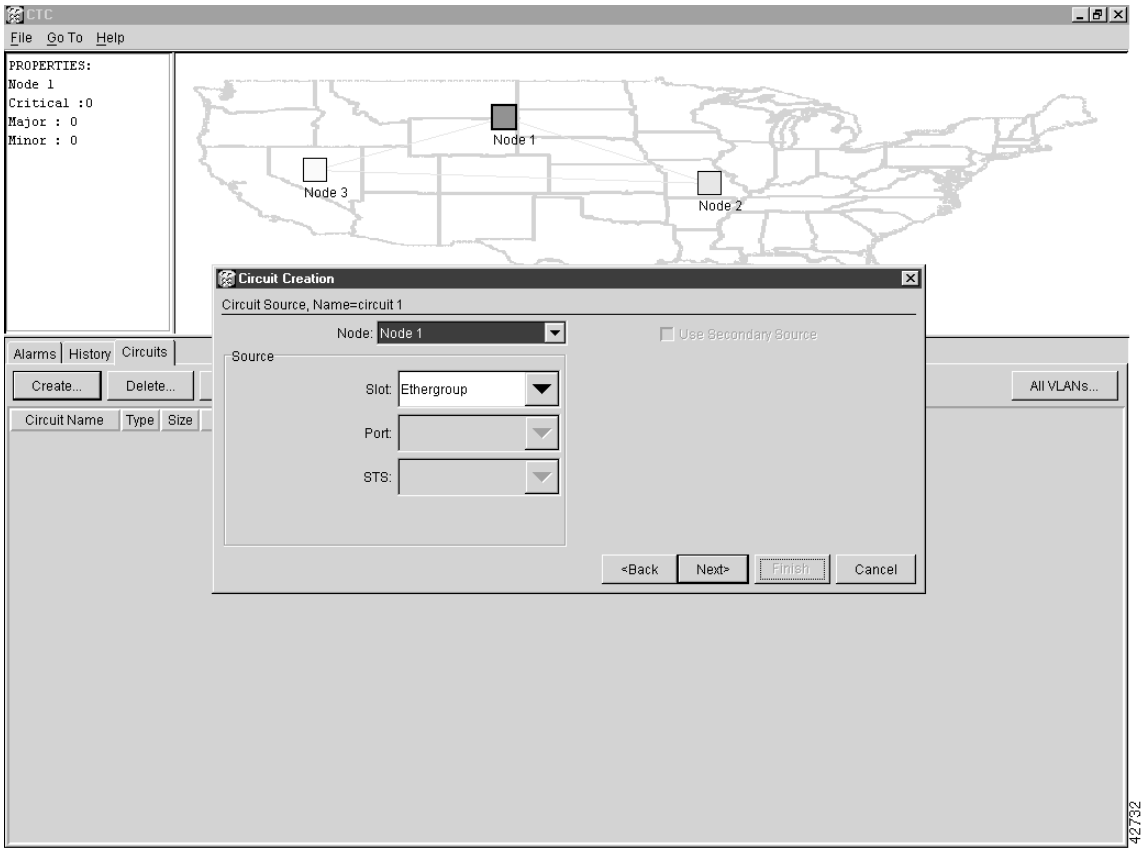
Step 14 Verify that Route Automatically is *not* selected.

Step 15 Verify that Bidirectional is selected.

Note You must manually provision the circuits if you are building a shared packet ring configuration.

Step 16 Click **Next**.

Figure 7-37 Circuit Source Dialog



Step 17 Choose the circuit source from the Node menu.

Note Any shared packet ring node can serve as the circuit source.

Step 18 Choose **Ethergroup** from the Slot menu.

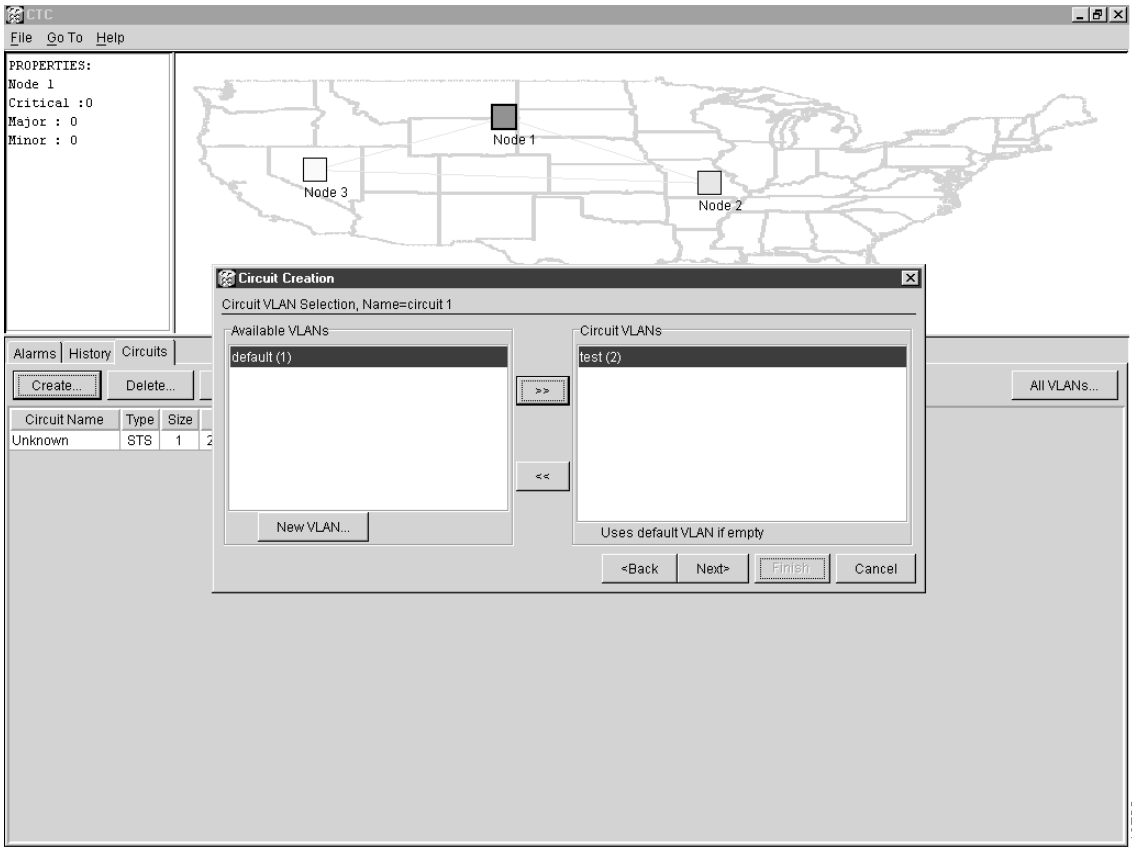
Step 19 Click **Next**.

Step 20 Choose the circuit destination in the Node menu.

Note Except for the source node, any shared packet ring node can serve as the circuit destination.

Step 21 Choose **Ethergroup** from the Slot menu.

Figure 7-38 Circuit VLAN Selection



Step 22 Click **Next**.

The Circuit VLAN Selection window opens (see Figure 7-38).

Note Do not use the default VLAN to pass traffic between nodes.

Step 23 Create the VLAN:

(a) Click the **New VLAN** tab.

The Define New VLAN dialog opens.

(b) Assign a name to your VLAN. The name should be one that allows you to easily identify a particular network.

(c) Assign a VLAN ID.

This VLAN ID number must be unique. It is usually the next available number not already assigned to an existing VLAN (between 2 and 4093). Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

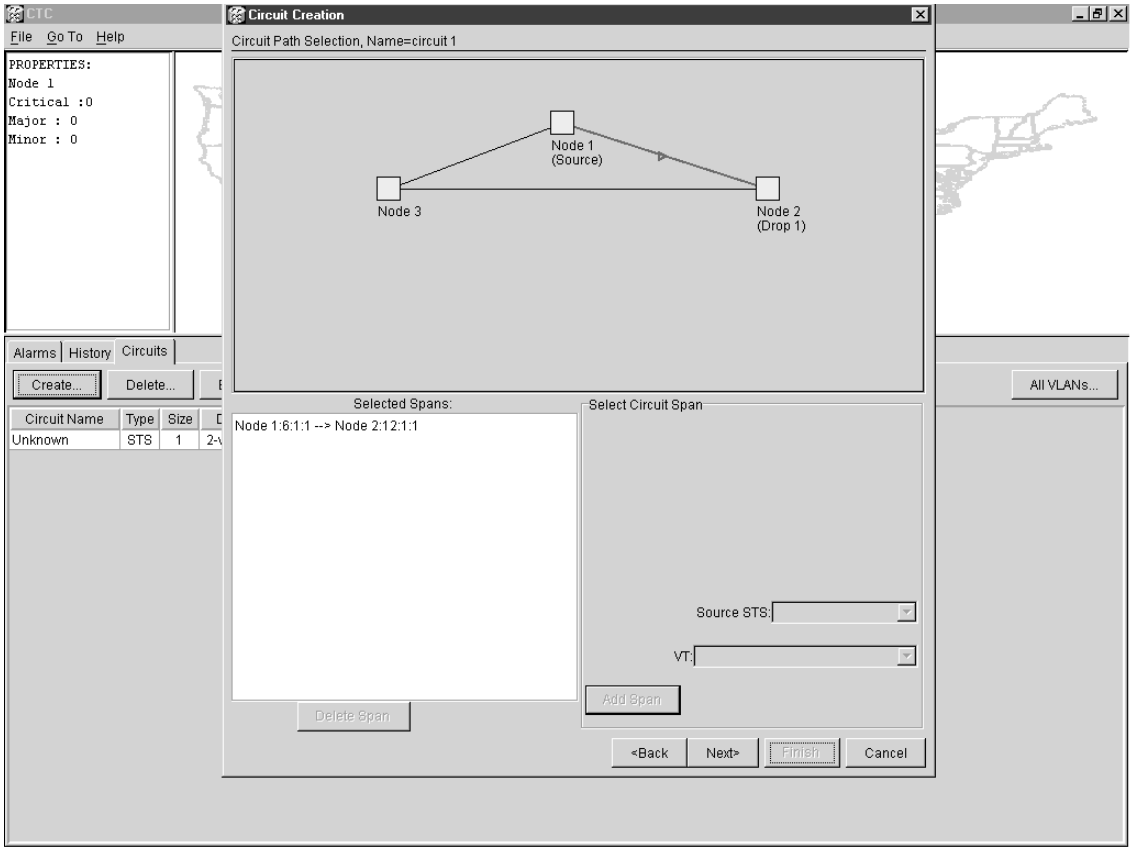
(d) Click **OK**.

(e) Highlight the VLAN name and click the arrow **>>** tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column.

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 24 Click **Next**.

Figure 7-39 Circuit Path Selection



Step 25 Click the line representing the span between Node 1 (Source) and Node 2 (Drop 1). Click the line again until the arrow points from the source (in this case, Node 1) to the destination (Node 2).

Step 26 Click the Source STS menu and choose a source STS.

The menu shows the STSs available to carry the shared packet ring circuit.

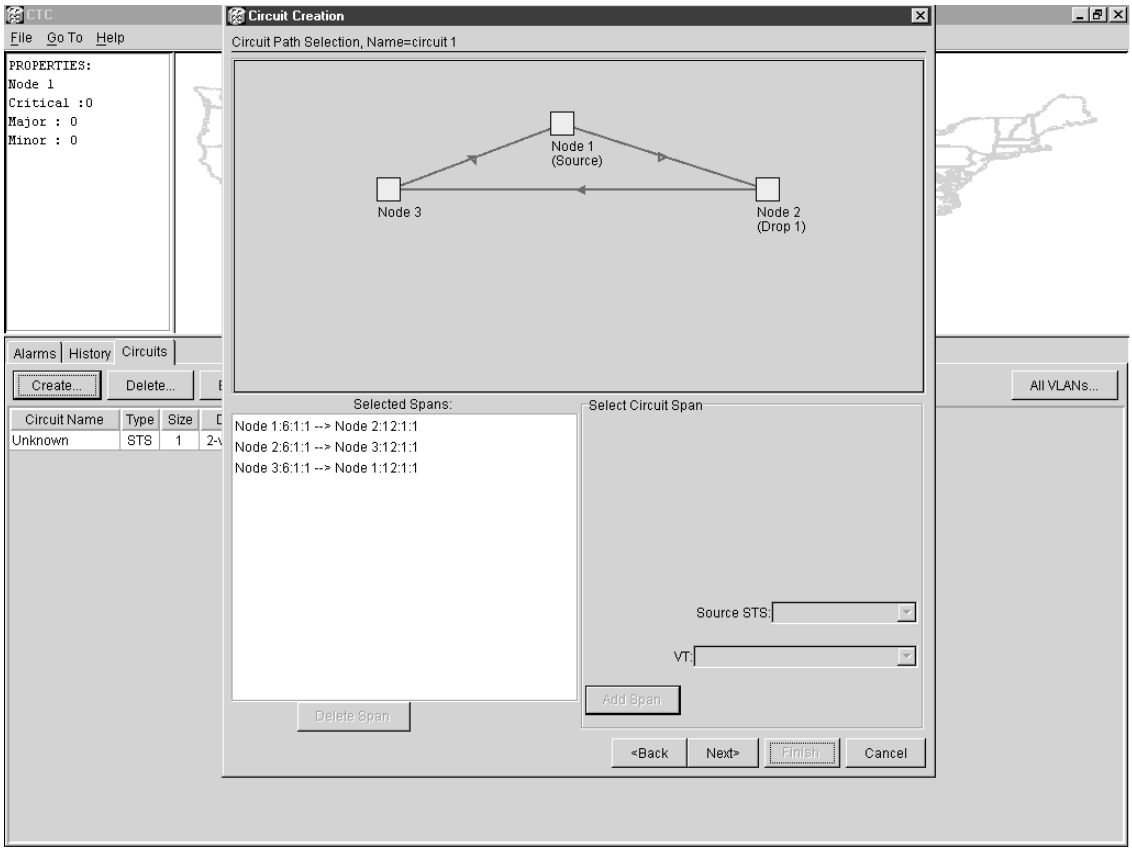
Step 27 Click **Add Span**.

Step 28 Repeat Steps 25, 26, and 27 for the next span (between nodes 2 and 3 in this example).

Step 29 Repeat Steps 25, 26, and 27 for the span between nodes 3 and 1. Figure 7-40 shows the Circuit Path Selection dialog with all the spans selected.

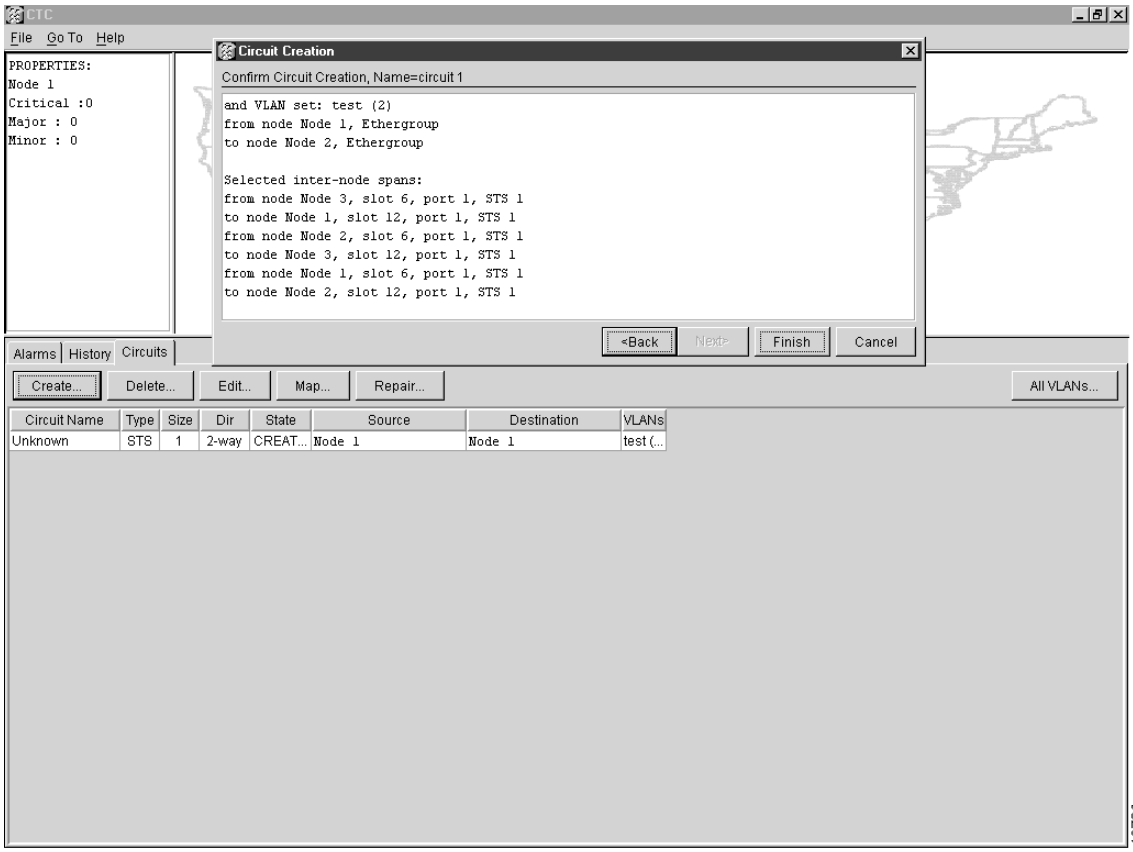
Note As each new span is selected, make sure the direction arrow on each span continues along a continuous path of travel. The arrows should connect head-to-tail in a circle (see Figure 7-40).

Figure 7-40 Circuit Path Selection (all spans)



Step 30 Click **Next**.

Figure 7-41 Circuit Creation



Step 31 Verify that the new circuit is correctly configured.

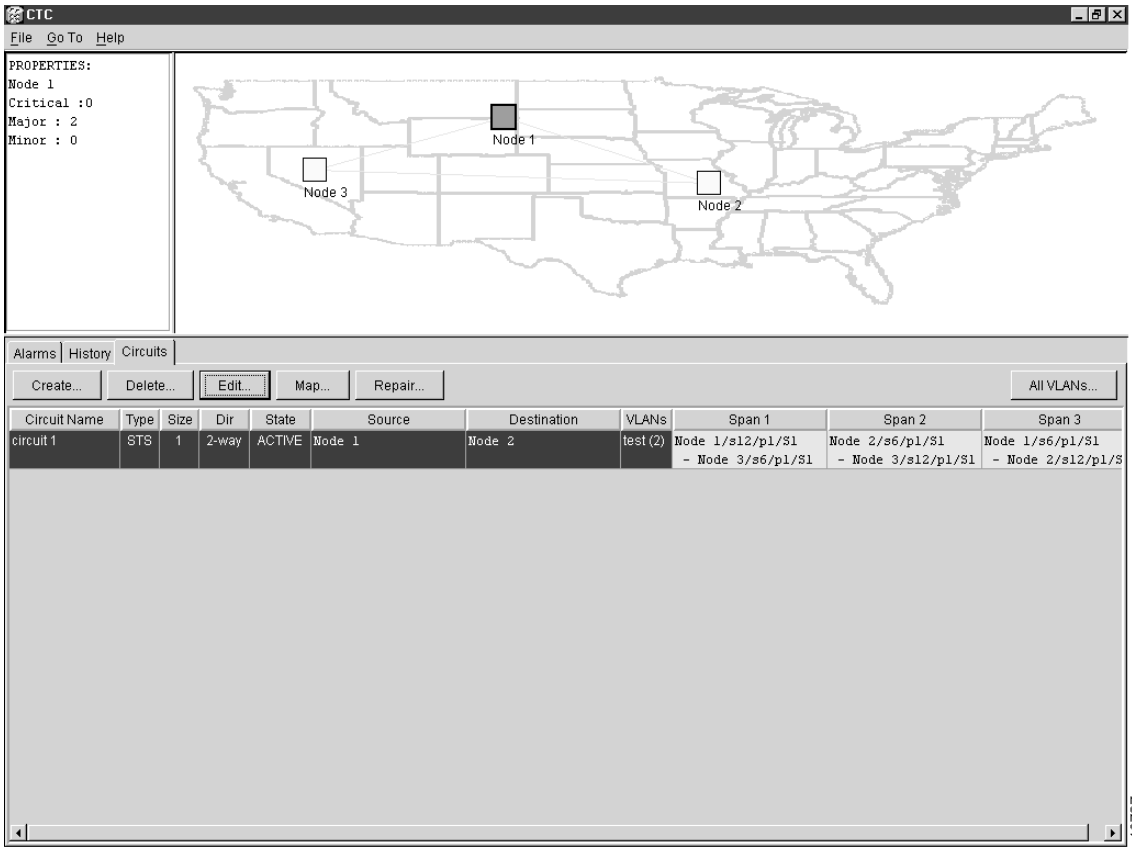
Note If the circuit information is not correct, use the <Back button to correct the information.

Step 32 Click **Finish.**

Step 33 Add the remaining packet ring drops:

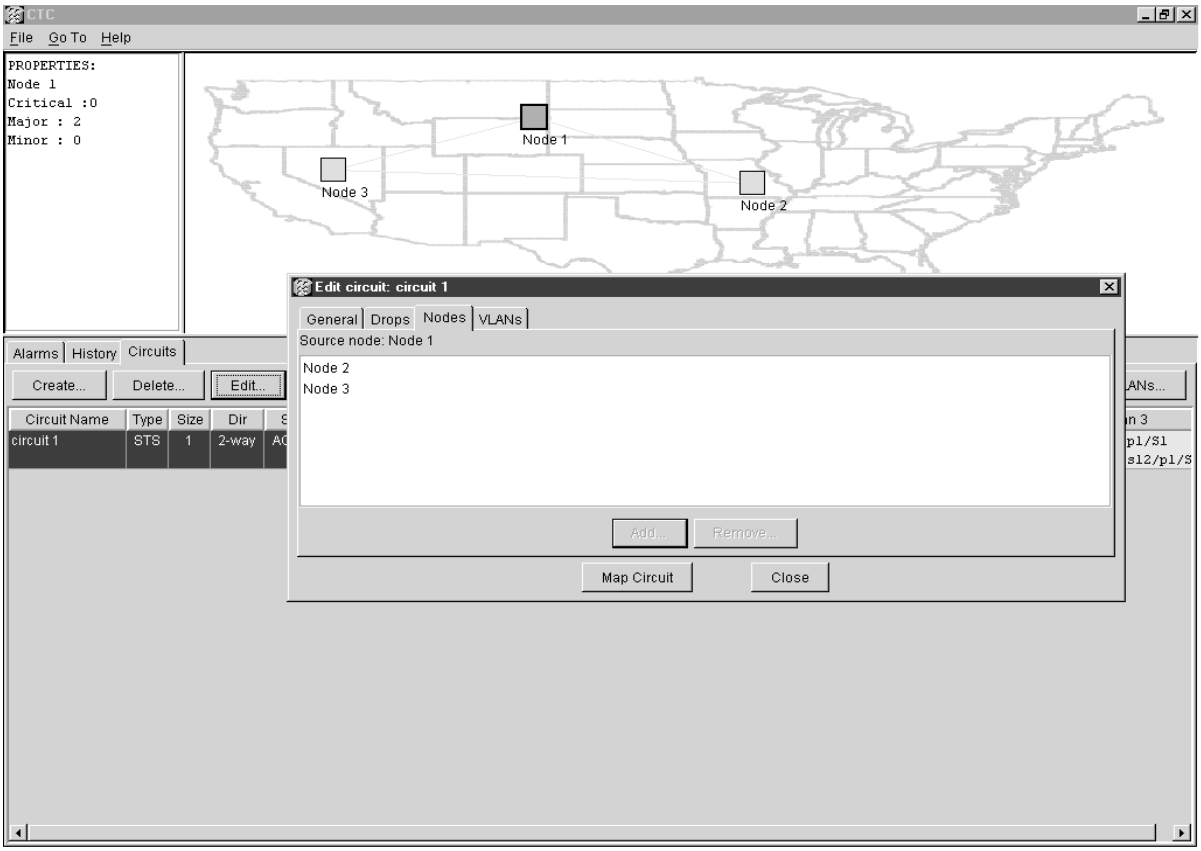
(a) Highlight the shared packet ring circuit (see Figure 7-42).

Figure 7-42 Highlighted Circuit Path



(b) Click **Edit**.

Figure 7-43 Edit Circuit Dialog Box



(c) Click the **Nodes** tab.

(d) Click the **Add** button to add additional drops.

(e) Choose **Node 3** from the Node menu.

(f) Choose **Ethergroup** from the Slot menu.

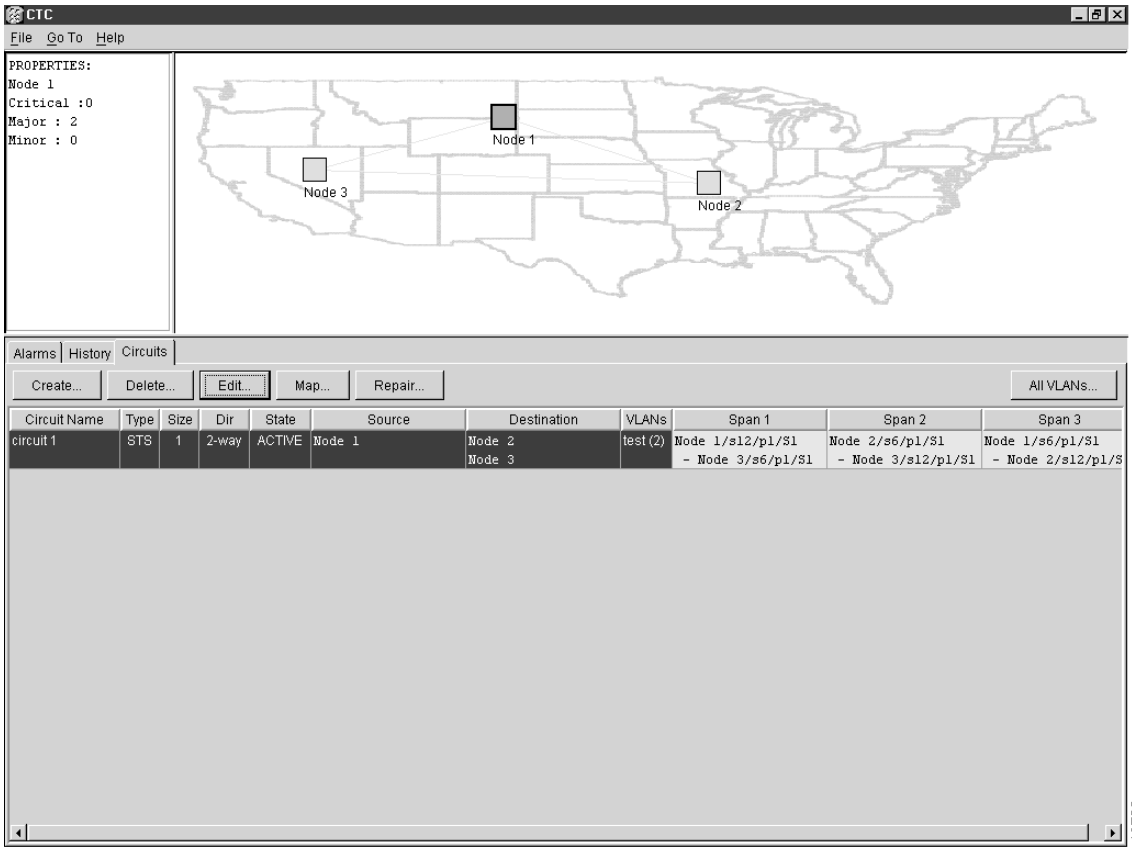
(g) Click **OK**.

(h) Click **Close**.

You now need to provision the Ethernet ports and assign ports to VLANs. For instructions on port provisioning, see the "VLAN Membership and Ethernet Port Provisioning" section on page 7-59. For information about manually provisioning Ethernet circuits, see the "Ethernet Manual Cross-Connects" section on page 7-54.

Figure 7-44 shows a completed shared packet ring circuit.

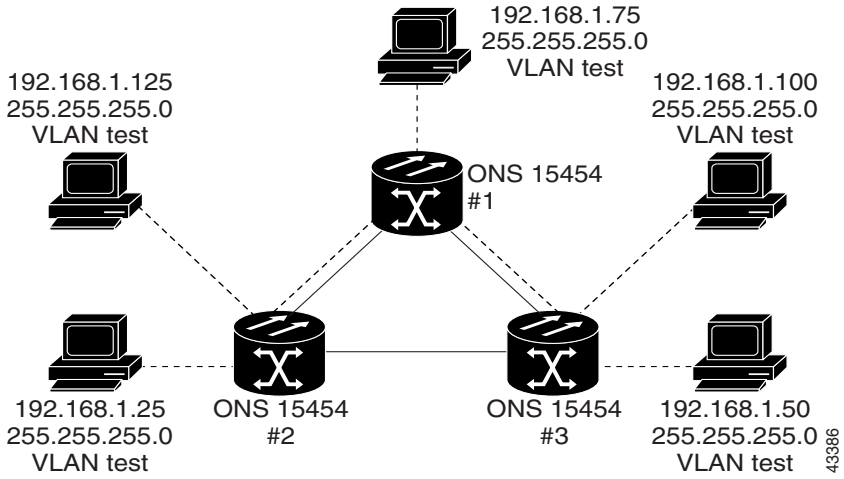
Figure 7-44 Completed Shared Packet Ring Circuit



7.8.3 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 is an E1000-2 card that links to a high-speed connection and the spokes are E100T cards. Figure 7-45 illustrates a sample hub spoke ring. (Your network architecture may differ from the example.)

Figure 7-45 Hub and Spoke Ethernet Circuit



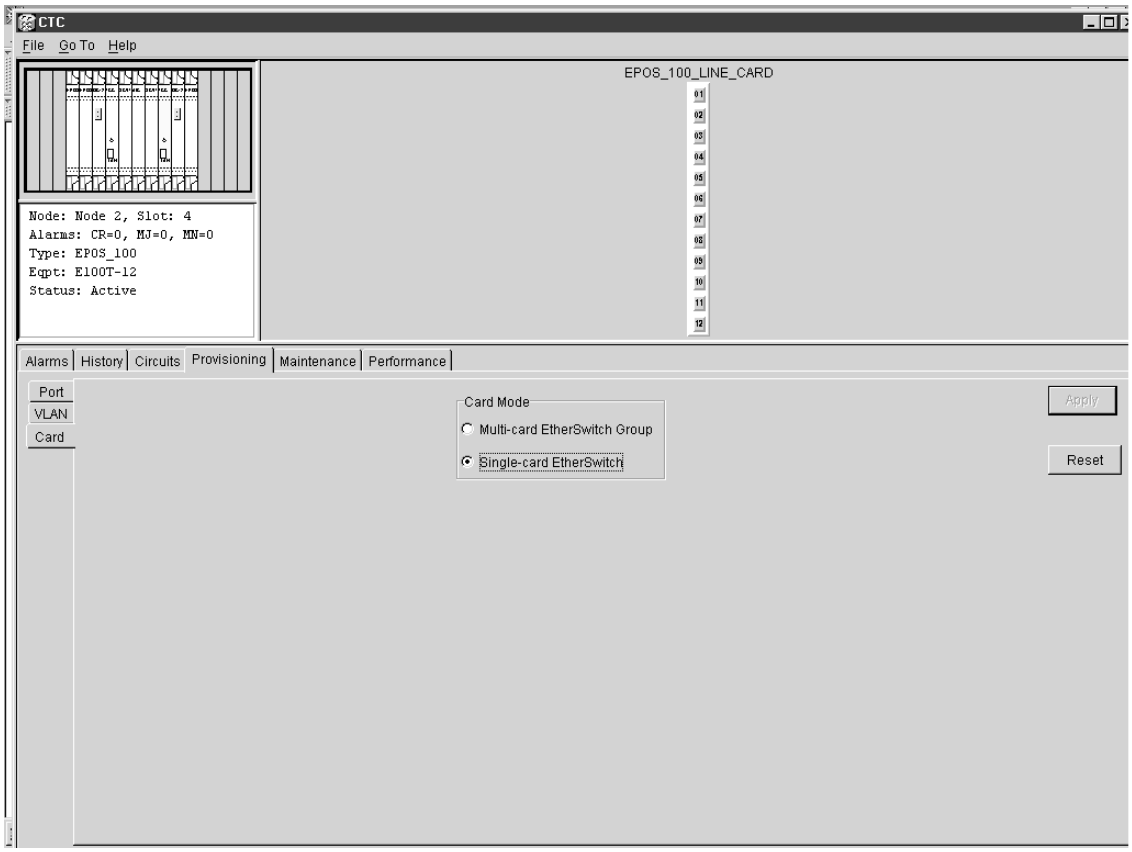
Procedure: Provision a Hub and Spoke Ethernet Circuit

Step 1 Log into one of the ONS 15454 Ethernet circuit endpoints.

Step 2 Double-click the Ethernet card that will create the circuit.

Step 3 Click the **Provisioning** tab and the **Card** subtab.

Figure 7-46 Single-card EtherSwitch Screen



Step 4 Under Card Mode, check the **Single-card EtherSwitch**.

Step 5 Click **Apply**.

Step 6 Log into the other ONS 15454 endpoint and repeat Steps 2-5.

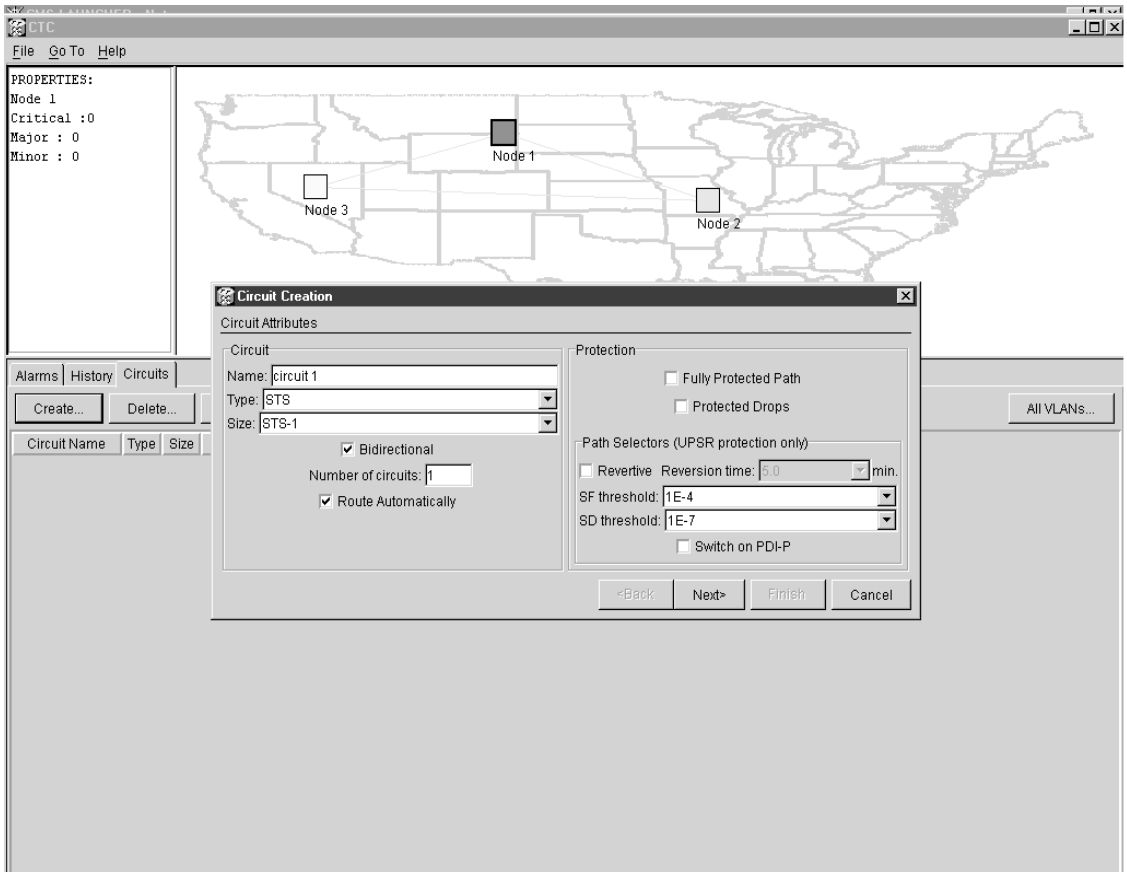
Step 7 Display the network view.

Step 8 Click the **Circuits** tab.

Step 9 Click **Create**.

The Circuit Attributes dialog opens (shown in Figure 7-47).

Figure 7-47 Circuit Attributes Dialog



Step 10 In the *Name* field, type a name for the circuit.

Step 11 From the Type menu, choose **STS**.

Note VT and VT Tunnel **Type:** do not apply to Ethernet circuits.

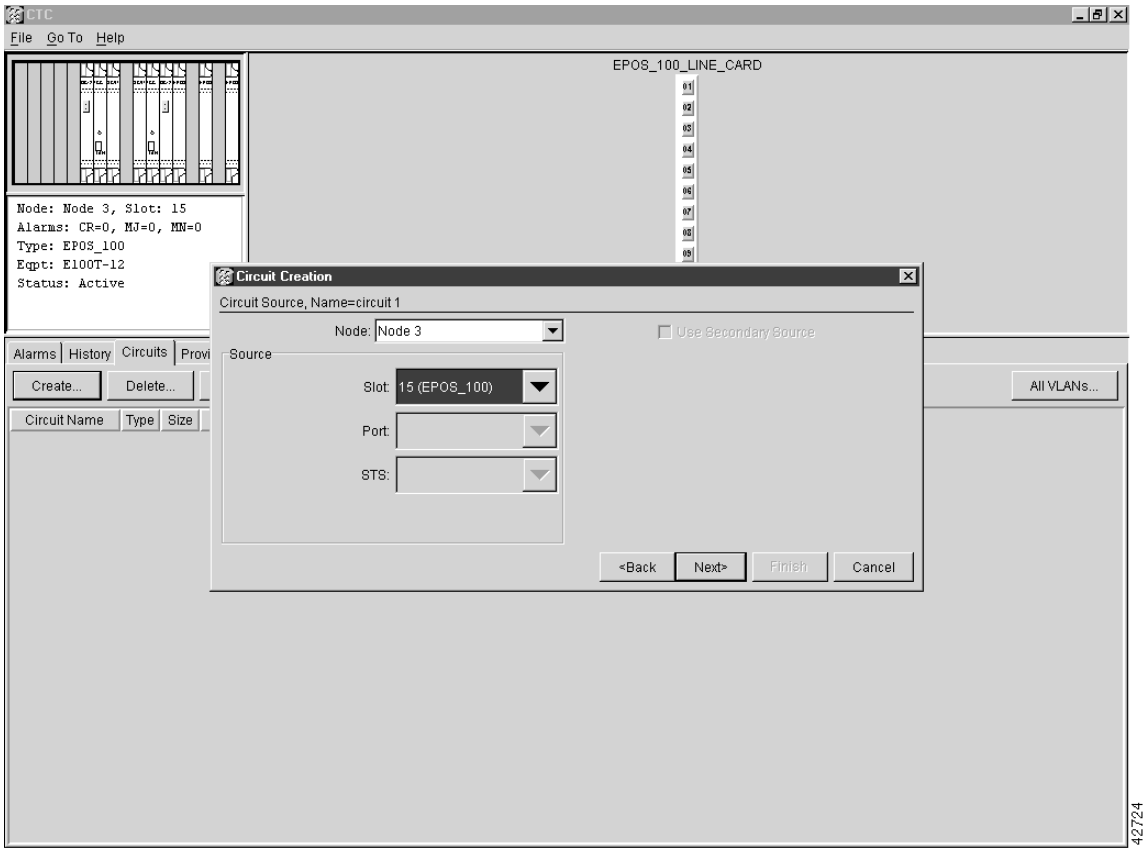
Step 12 Choose the size of the circuit from the Size menu.

Step 13 Verify that the Route Automatically box is checked.

Step 14 Verify that the Bidirectional box is checked.

Step 15 Click **Next**.

Figure 7-48 Circuit Source



Step 16 Choose the circuit source from the Node menu.

Note Either end node can be the circuit source.

Step 17 From the Slot menu, choose the Ethernet card for which you enabled the single-card EtherSwitch.

Step 18 Click **Next**.

Step 19 Choose the circuit destination from the Node menu.

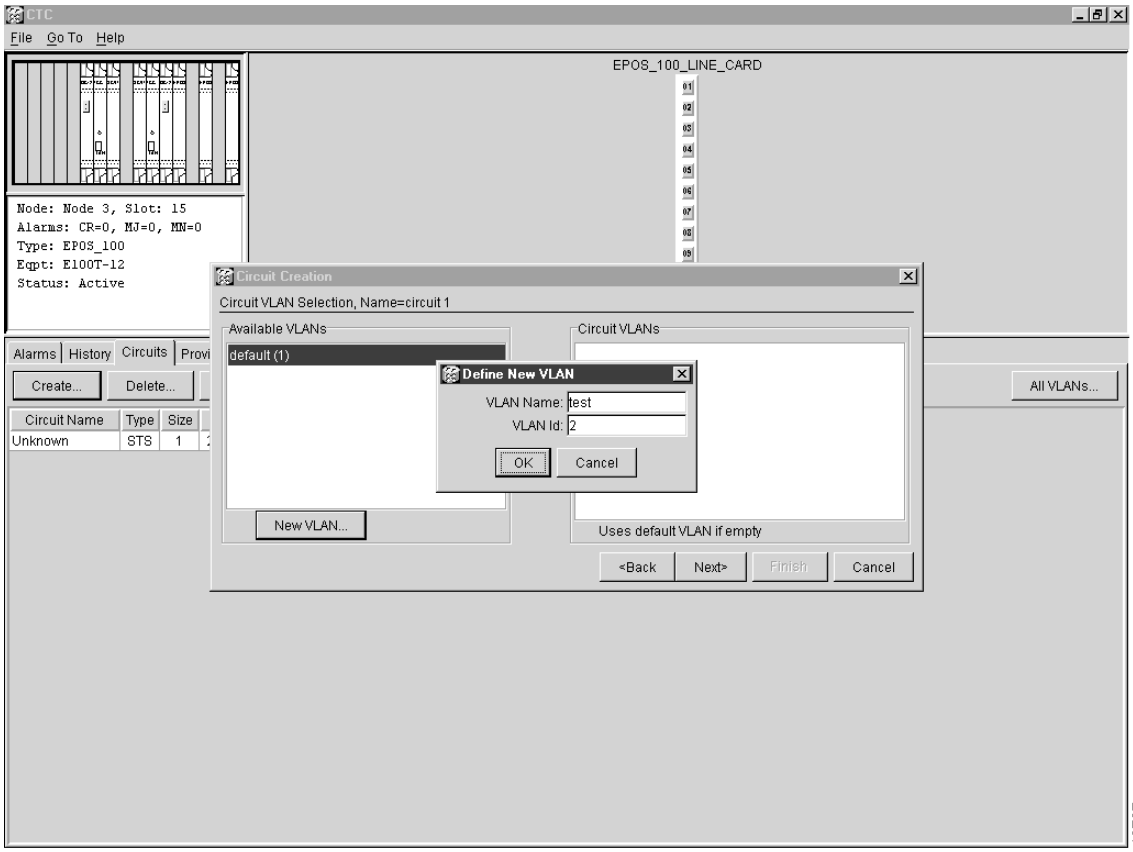
Note Choose the node that is *not* the source.

Step 20 From the Slot menu, choose the Ethernet card for which you enabled the single-card EtherSwitch.

Step 21 Click **Next**.

The Circuit VLAN Selection dialog displays.

Figure 7-49 Circuit VLAN Selection



Note Do not use the default VLAN to pass traffic between nodes.

Step 22 Create the VLAN:

(a) Click the **New VLAN** tab.

The Define New VLAN dialog opens (see Figure 7-49).

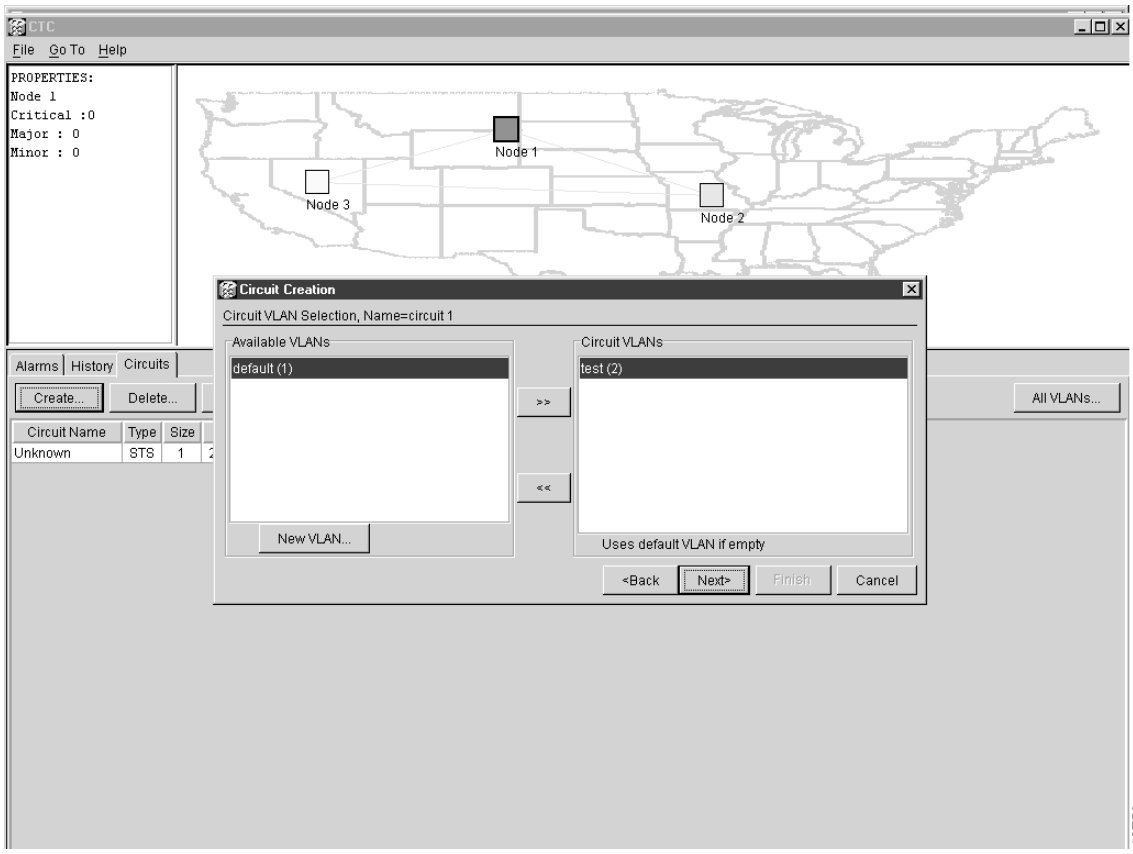
(b) Assign a name to your VLAN that will allow you to easily identify a particular network.

(c) Assign a VLAN ID.

This should be the next available number (between 2 and 4093) not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

(d) Click **OK**.

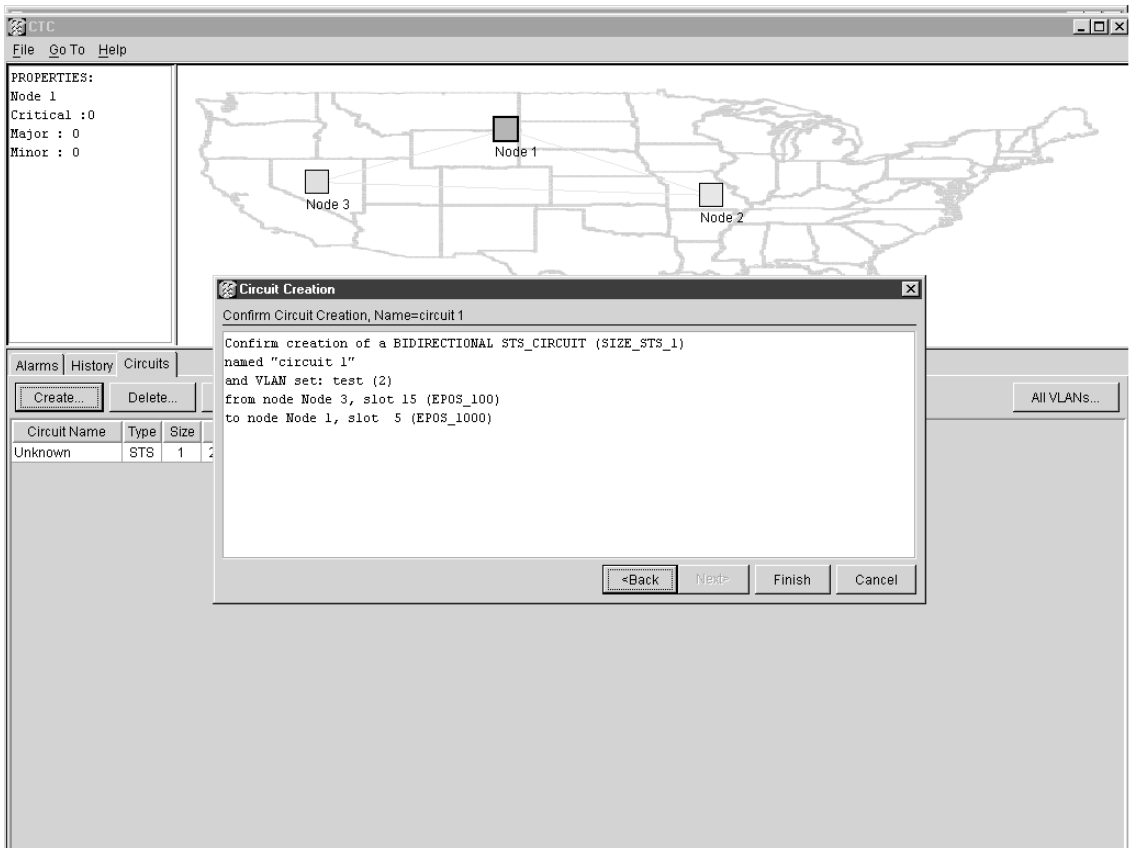
Figure 7-50 Selected VLANs



(e) Highlight the VLAN name and click the arrow **>>** tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column.

Step 23 Click **Next**.

Figure 7-51 Circuit Confirmation



The Confirm Circuit Creation dialog opens and displays the following information about the point-to-point circuit (see Figure 7-51):

- Circuit is bidirectional Ethernet
- Circuit size
- Circuit name
- VLANs that will be transported across this circuit
- ONS 15454 nodes that are part of this circuit

Note If the circuit information is not correct, use the <Back button to correct the information.

Step 24 Click **Finish**.

You must now provision the second circuit and attach it to the already-created VLAN.

Step 25 Log into the ONS 15454 Ethernet circuit endpoint for the second circuit.

Step 26 Double-click the Ethernet card that will create the circuit and go to the card view.

Step 27 Click the **Provisioning** tab and the **Card** subtab.

Step 28 Under Card Mode, check **Single-card EtherSwitch**.

Step 29 Click **Apply**.

Step 30 Log into the other ONS 15454 endpoint and repeat Steps 26-30.

Step 31 Go to the node view.

Step 32 Click the **Circuits** tab.

Step 33 Click **Create**.

Step 34 Choose **STS** from the Type menu.

Note VT and VT Tunnel **Type:** do not apply to Ethernet circuits.

Step 35 Choose the size of the circuit from the Size menu.

Step 36 Verify that the Route Automatically box is checked.

Step 37 Verify that the Bidirectional box is checked.

Step 38 Click **Next**.

Step 39 Choose the circuit source from the Node menu.

Note Either end node can be the circuit source.

Step 40 Click **Next**.

Step 41 Choose the circuit destination from the Node menu.

Note Choose the node that is *not* the source.

Step 42 From the Slot menu, choose the Ethernet card for which you enabled the single-card EtherSwitch.

Step 43 Click **Next**.

The Circuit VLAN Selection dialog is displayed.

Note Do not use the default VLAN to pass traffic between nodes.

Step 44 Highlight the VLAN that you created for the first circuit and click the arrow **>>** tab to move the VLAN(s) from the Available VLANs column to the Selected VLANs column.

Step 45 Click **Next**.

Step 46 Click **Finish**.

You now need to provision the Ethernet ports and assign the ports to VLANs. For instructions about port provisioning, see the "VLAN Membership and Ethernet Port Provisioning" section on page 7-59. For information about assigning Ethernet ports to VLANs, see the "Provision Ethernet Ports for VLAN Membership" section on page 7-59.

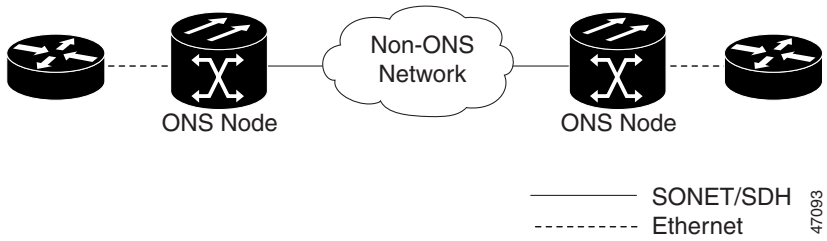
7.8.4 Ethernet Manual Cross-Connects

ONS 15454s require end-to-end CTC visibility between nodes for normal provisioning of Ethernet circuits. When other vendors' equipment sits between ONS 15454s, OSI/TARP- based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent this lack of continuous DCC, the Ethernet circuit must be manually cross-connected to an STS channel riding through the non-ONS network. This allows an Ethernet circuit to run from ONS node to ONS node utilizing the non-ONS network.

Note Provisioning manual cross-connects for *multi-card* Etherswitch circuits is a separate procedure from provisioning manual cross-connects for *single-card* Etherswitch circuits. Both procedures are listed below.

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 was configured on the first ONS 15454 and circuit size of STS-12c was configured on the second ONS 15454. To troubleshoot this occurrence of the CARLOSS alarm, refer to the CARLOSS alarm troubleshooting procedure in the Alarm Troubleshooting chapter of the *Cisco ONS 15454 Troubleshooting and Maintenance Guide*.

Figure 7-52 Ethernet manual cross-connects



Procedure: Provision a Single-card Etherswitch Manual Cross-Connect

Step 1 Log into one of the ONS 15454 Ethernet circuit endpoints.

Step 2 Double-click one of the Ethernet cards that will comprise the circuit.

Step 3 Click the **Provisioning > Card** tabs.

Step 4 Under Card Mode, verify that **Single-card EtherSwitch** is checked.

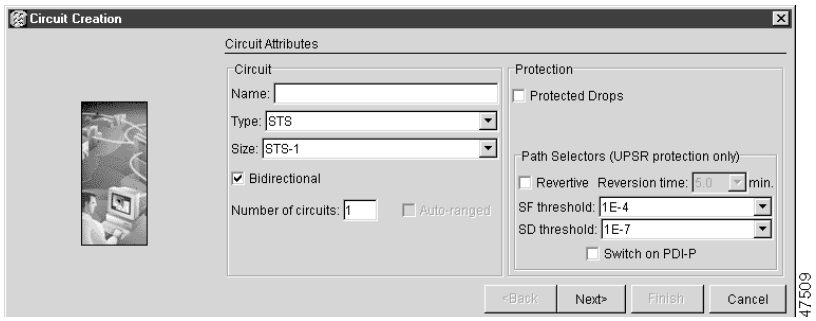
If the **Single-card EtherSwitch** is not checked, check it and click **Apply**.

Step 5 Display the node view.

Step 6 Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens (Figure 7-53).

Figure 7-53 Creating an Ethernet circuit



Step 7 In the Name field, type a name for the circuit.

Step 8 From the Type menu, choose **STS**.

The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 9 Choose the size of the circuit from the Size menu.

The valid circuit sizes for an Ethernet Multicard circuit are STS-1, STS-3c and STS-6c.

Step 10 Verify that the **Bidirectional** checkbox is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box opens.

Step 11 From the Node menu, choose the current node as the circuit source.

Step 12 Choose the Ethernet card that will comprise the circuit from the Slot menu and click **Next**.

The Circuit Creation (Circuit Destination) dialog box opens.

Step 13 From the Node menu, choose the current node as the circuit destination.

Step 14 Choose the optical card that will comprise the circuit from the Slot menu.

Step 15 Choose the STS that will comprise the circuit from the STS menu and click **Next**.

Note For the Ethernet manual cross-connect, the destination and source should be the same node.

The Circuit Creation (Circuit VLAN Selection) dialog box opens (Figure 7-49).

Note As a general rule, do not use the default VLAN to pass traffic between nodes.

Step 16 Create the VLAN:

(a) Click the **New VLAN** tab.

The Circuit Creation (Define New VLAN) dialog box opens (Figure 7-54).

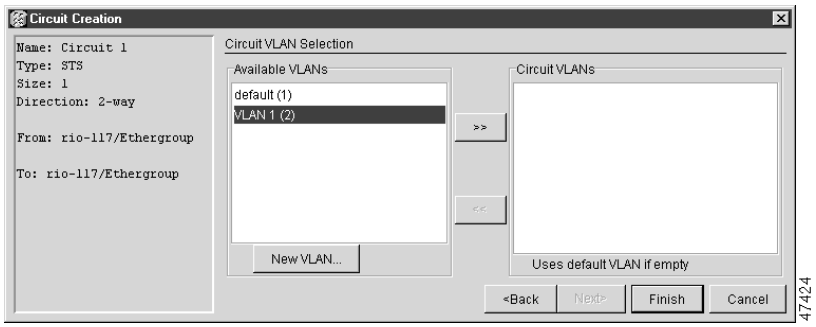
(b) Assign an easily-identifiable name to your VLAN.

(c) Assign a VLAN ID.

The VLAN ID should be the next available number (between 2 and 4093) that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

(d) Click **OK**.

Figure 7-54 Selecting VLANs



(e) Highlight the VLAN name and click the arrow >> tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 7-56).

Step 17 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 18 Confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs that will be transported across this circuit
- ONS 15454 nodes included in this circuit

Note If the circuit information is not correct use the **Back** button, then redo the procedure with the correct information. Alternately, you can click **Finish**, then delete the completed circuit and start the procedure from the beginning.

Step 19 Click **Finish**.

You now need to provision the Ethernet ports and assign these ports to VLANs. For port provisioning instructions, see the "VLAN Membership and Ethernet Port Provisioning" section on page 7-59. Return to the following step after assigning the ports to VLANs.

Step 20 Repeat Steps 1 – 19 at the second ONS 15454 Ethernet manual cross-connect endpoint.

Note The appropriate STS circuit must exist in the non-ONS 15454 equipment to connect the two STSs from the ONS 15454 Ethernet manual cross-connect endpoints.

Procedure: Provision a Multi-card Etherswitch Manual Cross-Connect

Step 1 Log into one of the ONS 15454 Ethernet circuit endpoints.

Step 2 Double-click one of the Ethernet cards that will comprise the circuit.

Step 3 Click the **Provisioning > Card** tabs.

Step 4 Under Card Mode, verify that **Multi-card EtherSwitch** is checked.

If the **Multicard-card EtherSwitch** is not checked, check it and click **Apply**.

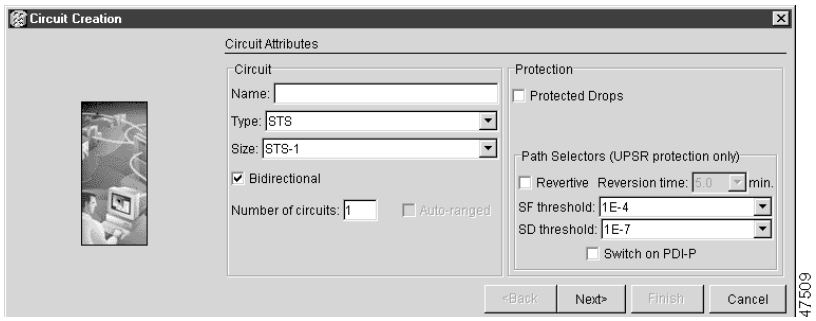
Step 5 Display the node view.

Step 6 Repeat Steps 2 – 5 for any other Ethernet cards in the ONS 15454 that will comprise the circuit.

Step 7 Click the **Circuits** tab and click **Create**.

The Circuit Creation (Circuit Attributes) dialog box opens (Figure 7-55).

Figure 7-55 Creating an Ethernet circuit



Step 8 In the Name field, type a name for the circuit.

Step 9 From the Type menu, choose **STS**.

The types VT and VT Tunnel do not apply to Ethernet circuits.

Step 10 Choose the size of the circuit from the Size menu.

The valid circuit sizes for an Ethernet Multicard circuit are STS-1, STS-3c and STS-6c.

Step 11 Verify that the **Bidirectional** checkbox is checked and click **Next**.

The Circuit Creation (Circuit Source) dialog box opens.

Step 12 From the Node menu, choose the current node as the circuit source.

Step 13 Choose **Ethergroup** from the Slot menu and click **Next**.

The Circuit Creation (Circuit Destination) dialog box opens.

Step 14 From the Node menu, choose the current node as the circuit destination.

Step 15 Choose **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 opens (Figure 7-56).

Note Do not use the default VLAN to pass traffic between nodes.

Step 16 Create the VLAN:

(a) Click the **New VLAN** tab.

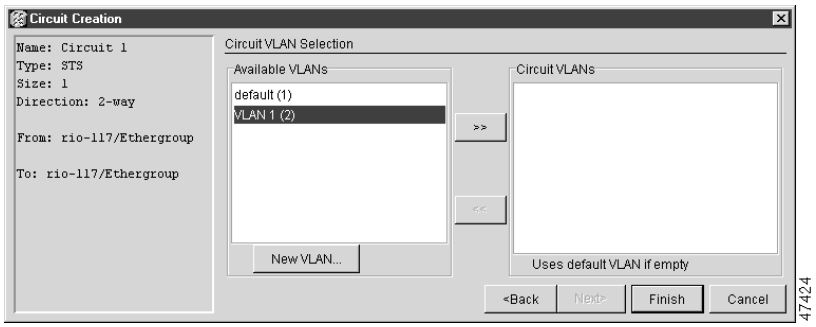
(b) Assign an easily-identifiable name to your VLAN.

(c) Assign a VLAN ID.

The VLAN ID should be the next available number (between 2 and 4093) that is not already assigned to an existing VLAN. Each ONS 15454 network supports a maximum of 509 user-provisionable VLANs.

(d) Click **OK**.

Figure 7-56 Selecting VLANs



(e) Highlight the VLAN name and click the arrow >> tab to move the VLAN(s) from the Available VLANs column to the Circuit VLANs column (Figure 7-56).

Step 17 Click **Next**.

The Circuit Creation (Circuit Routing Preferences) dialog box opens.

Step 18 Confirm that the following information is correct:

- Circuit name
- Circuit type
- Circuit size
- VLANs that will be transported across this circuit
- ONS 15454 nodes included in this circuit

Note If the circuit information is not correct use the **Back** button, then redo the procedure with the correct information. Alternately, you can click **Finish**, then delete the completed circuit and start the procedure from the beginning.

Step 19 Click **Finish**.

You now need to provision the Ethernet ports and assign these ports to VLANs. For port provisioning instructions, see the "VLAN Membership and Ethernet Port Provisioning" section on page 7-59. Return to the following step after assigning the ports to VLANs.

Step 20 Highlight the circuit and click **Edit**.

The Edit Circuit dialog box opens.

Step 21 Click **Drops** and click **Create**.

The Define New Drop dialog box opens.

Step 22 From the **Slot** menu, choose the optical card that links the ONS 15454 to the non-ONS 15454 equipment.

Step 23 From the **Port** menu, choose the appropriate port.

Step 24 From the **STS** menu, choose the STS that matches the STS of the connecting non-ONS 15454 equipment.

Step 25 Click **OK**.

The Edit Circuit dialog box opens.

Step 26 Confirm the circuit information that displays in the Circuit Information dialog box and click **Close**.

Step 27 Repeat Steps 1 – 26 at the second ONS 15454 Ethernet manual cross-connect endpoint.

Note The appropriate STS circuit must exist in the non-ONS 15454 equipment to connect the two ONS 15454 Ethernet manual cross-connect endpoints.

7.9 VLAN Membership and Ethernet Port Provisioning

This section explains how to provision Ethernet ports, including provisioning Ethernet ports for VLAN membership.

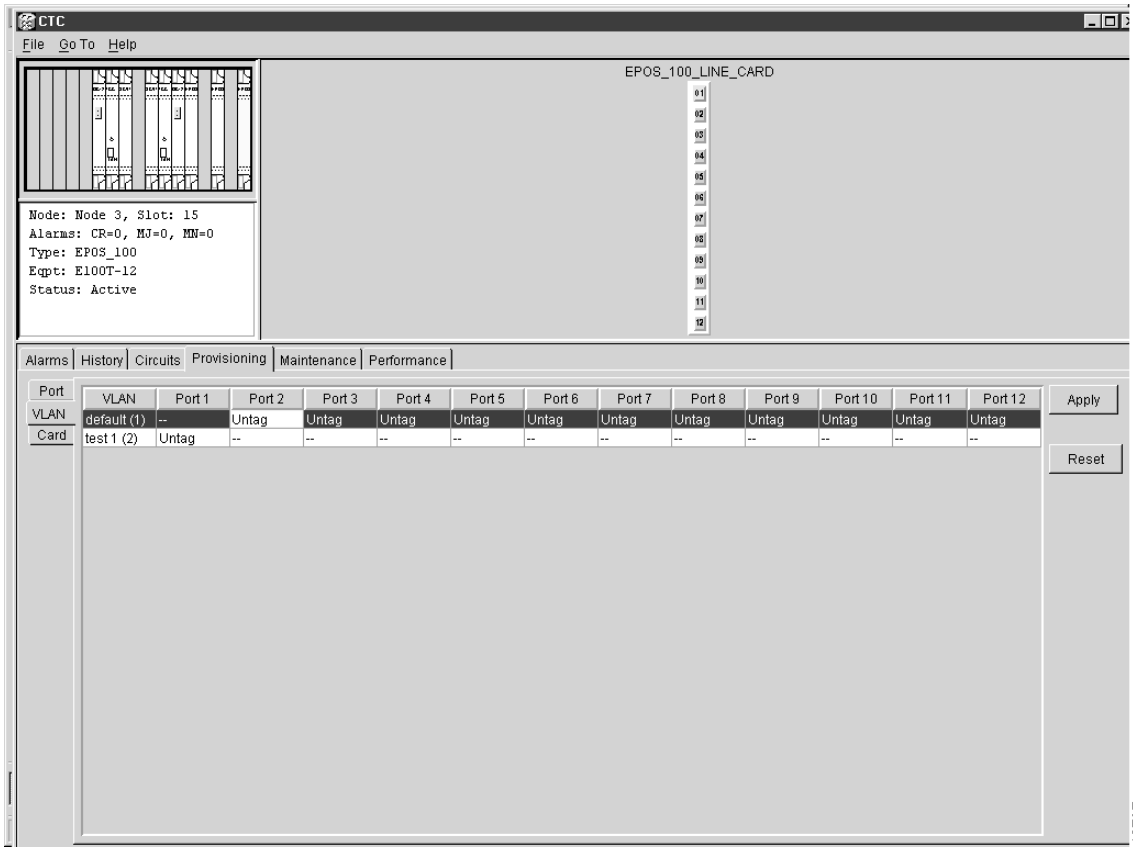
Procedure: Provision Ethernet Ports for VLAN Membership

Note The same basic procedure configures E100T-12 and E1000-2 Ethernet ports for VLAN membership. The VLAN port provisioning screen shown in this example is for an E100T-12 card.

The ONS 15454 allows you to configure the VLAN membership and the Q-tag handling of individual Ethernet ports.

Step 1 With the **Provisioning** menu tab selected, click the **VLAN** subtab (see Figure 7-57).

Figure 7-57 VLAN Port Provisioning Screen



Step 2 To place a port in a VLAN, click the port and choose either Tagged or Untag. Figure 7-57 shows Port 1 placed in the test 1 VLAN and Port 2-Port 12 in the default VLAN. Table 7-6 shows valid port settings.

If a port belongs to only one VLAN, go to that VLAN's row and choose **Untag** from that port's column. Choose **--** for all the other VLAN rows under that port. This allows the VLAN with **Untag** selected to access that port and prohibits the other VLANS with **--** selected to access the port.

If a port is a trunk port, it connects multiple VLANs to an external device, such as a router. This port must have tagging (8021.Q) enabled for all the VLANs that connect to the external device. Choose **Tagged** at each VLAN row in the trunk port column. Choose **Untag** in the default VLAN row in the column under the trunk port's heading.

Table 7-6 Port Settings

Setting	Description
--	A port marked with this symbol does not belong to the VLAN.
Untag	The ONS 15454 will tag ingress frames and strip tags from egress frames.
Tagged	The ONS 15454 will handle ingress frames according to VLAN ID, egress frames will not have their tags removed.

Note If Tagged is chosen, the attached devices must be IEEE 802.1Q VLAN aware.

Step 3 After each port is placed in the appropriate VLAN, click **Apply**.

Note Both ports on an individual E1000-2 card cannot be members of the same VLAN.

Procedure: Provision E1000-2 Ethernet Ports

Step 1 Double-click the card graphic to open the Ethernet card.

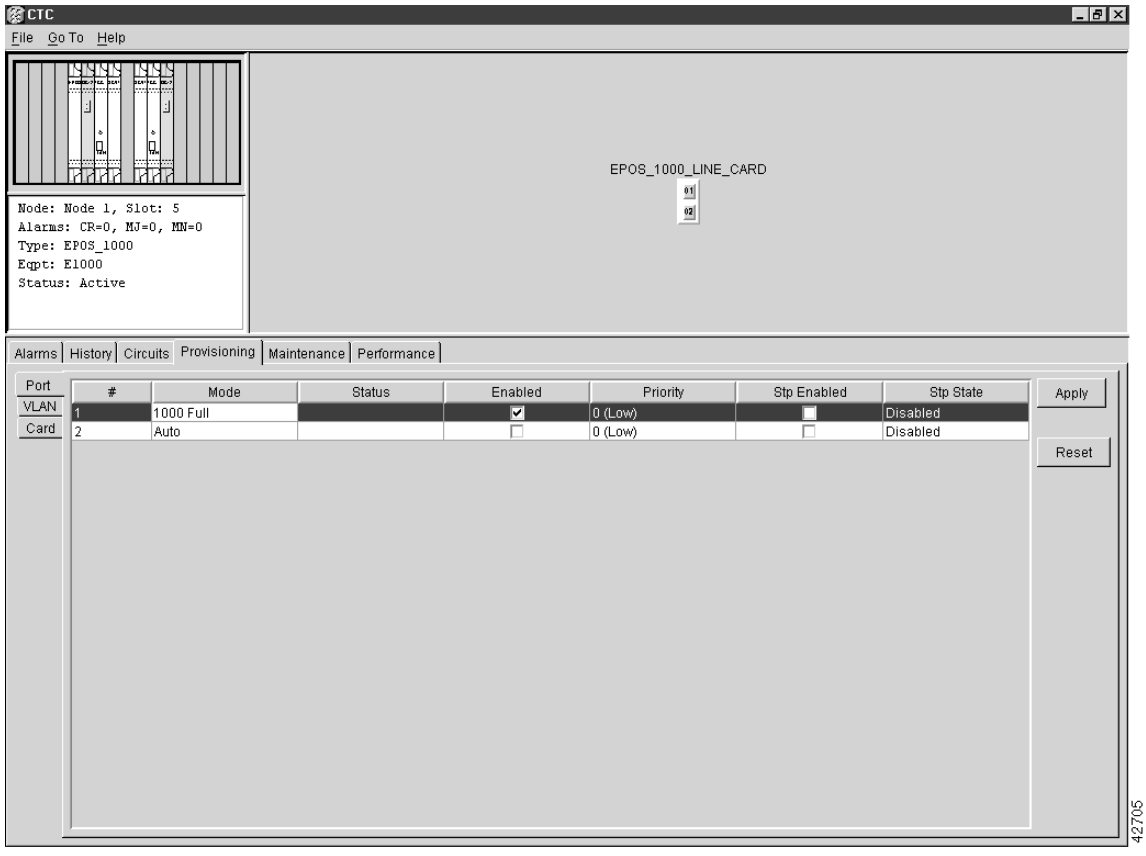
Step 2 From the Ethernet card view, choose the **Provisioning** menu tab.

Step 3 Choose the **Port** subtab.

Note Most provisioning requires only two fields: Enabled and Mode.

Figure 7-59 shows the Provisioning menu screen with the **Port** subtab selected.

Figure 7-58 Port Provisioning Screen



Step 4 From the Port Provisioning screen, choose the appropriate mode for each Ethernet port. The valid choices for the E1000-2 card are 1000 Full or Auto.

Step 5 Click the **Enabled** box to activate the desired Ethernet ports.

Note The Status column displays information about the port's current operating mode.

Step 6 Click **Apply**.

Your Ethernet ports are now provisioned and ready to be configured for VLAN membership (see the "Provision Ethernet Ports for VLAN Membership" section on page 7-59).

Procedure: Provision E100T-12 Ethernet Ports

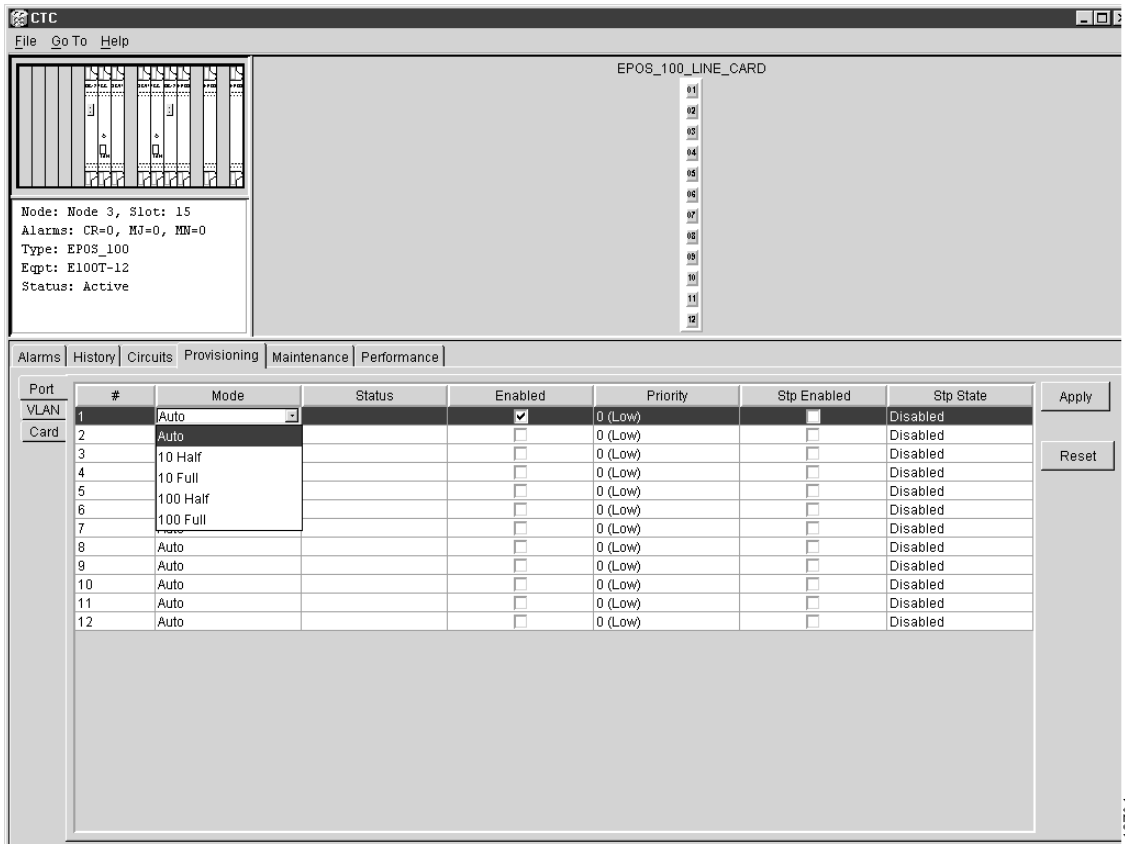
Step 1 Double click the card graphic to open the E100T-12 card.

Step 2 From the Ethernet card view, choose the **Provisioning** menu tab.

Step 3 Choose the **Port** subtab.

Figure 7-59 shows the Provisioning menu screen with the **Port** function subtab selected.

Figure 7-59 Port Provisioning Screen



Step 4 From the Port Provisioning screen, choose the appropriate mode for each Ethernet port. Valid choices for the E100T-12 card are Auto, 10 Half, 10 Full, 100 Half or 100 Full.

Step 5 In the **Enabled** column, click the box to activate the desired Ethernet ports.

Most provisioning requires filling in two fields: Enabled and Mode. However, the user may also map incoming traffic to a low priority or a high priority using the Priority column or enable spanning tree with the Stp Enabled column. The Status column displays information about the port's current operating mode, and the Stp State column gives the current Spanning tree status.

Step 6 Click **Apply**.

Your Ethernet ports are now provisioned and ready to be configured for VLAN membership (see the "Provision Ethernet Ports for VLAN Membership" section on page 7-59).

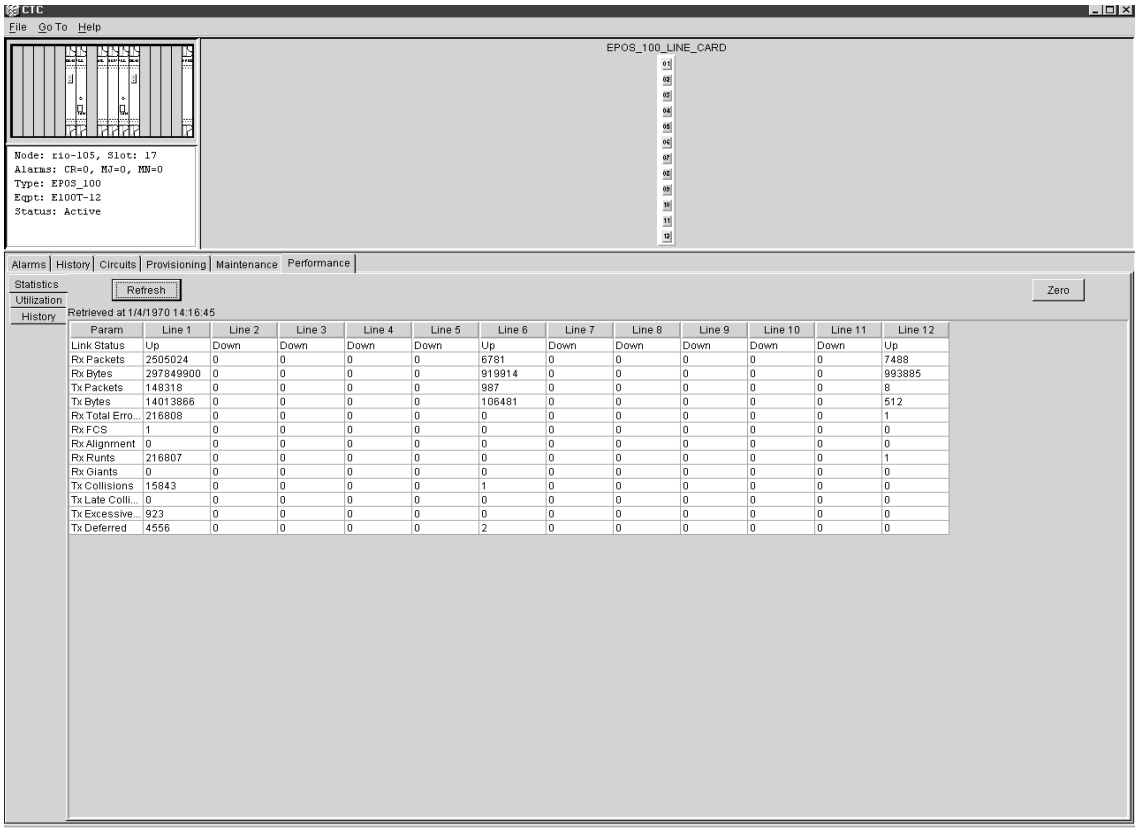
7.10 Ethernet Maintenance and Performance Screens

The CTC provides several screens of information to help manage and maintain Ethernet performance.

7.10.1 Statistics Screen

The Ethernet statistics screen lists Ethernet parameters at the port level. Table 7-7 defines the parameters. Click the Performance and Statistics tabs at the card level view to display the screen (see Figure 7-60).

Figure 7-60 Ethernet Statistics



Param	Line 1	Line 2	Line 3	Line 4	Line 5	Line 6	Line 7	Line 8	Line 9	Line 10	Line 11	Line 12
Link Status	Up	Down	Down	Down	Down	Up	Down	Down	Down	Down	Down	Up
Rx Packets	2505024	0	0	0	0	6781	0	0	0	0	0	7488
Rx Bytes	297849900	0	0	0	0	919914	0	0	0	0	0	993885
Tx Packets	148318	0	0	0	0	987	0	0	0	0	0	8
Tx Bytes	14013866	0	0	0	0	106481	0	0	0	0	0	512
Rx Total Erro...	216808	0	0	0	0	0	0	0	0	0	0	1
Rx FCS	1	0	0	0	0	0	0	0	0	0	0	0
Rx Alignment	0	0	0	0	0	0	0	0	0	0	0	0
Rx Runts	216807	0	0	0	0	0	0	0	0	0	0	1
Rx Giants	0	0	0	0	0	0	0	0	0	0	0	0
Tx Collisions	15843	0	0	0	0	1	0	0	0	0	0	0
Tx Late Colli...	0	0	0	0	0	0	0	0	0	0	0	0
Tx Excessive...	923	0	0	0	0	0	0	0	0	0	0	0
Tx Deferred	4556	0	0	0	0	2	0	0	0	0	0	0

Table 7-7 Ethernet Parameters

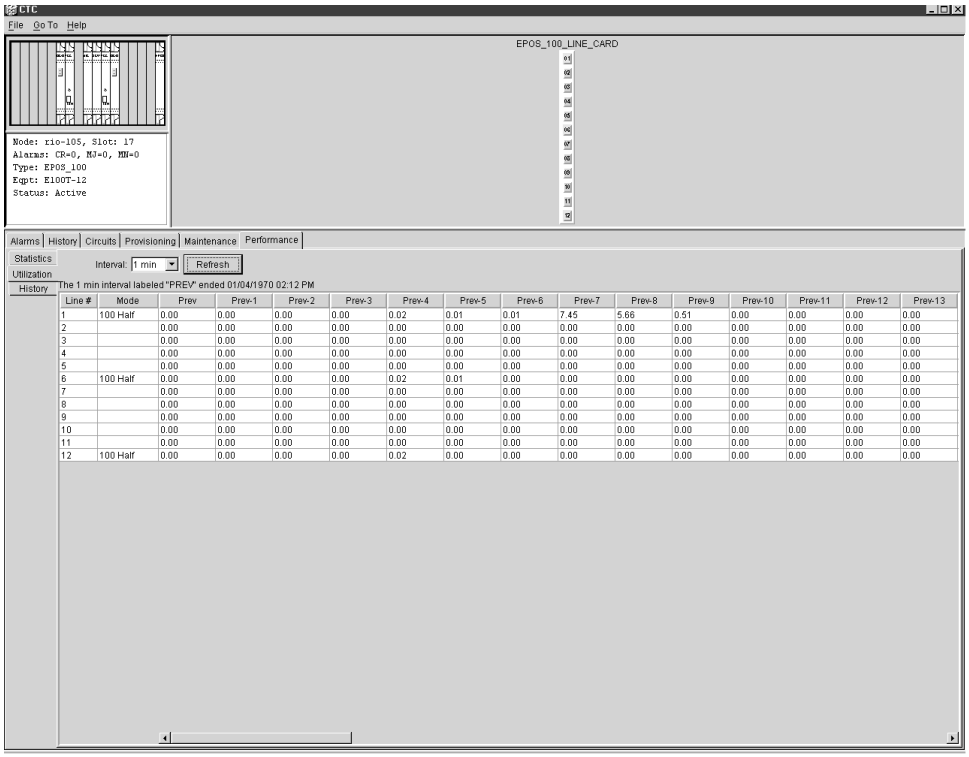
Parameter	Meaning
Link Status	Indicates if link integrity is present; up indicates present, and down indicates not present
RX Packets	Number of packets received since the last counter reset
RX Bytes	Number of bytes received since the last counter reset
TX Packets	Number of packets transmitted since the 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 error; alignment errors are Frames not received whole
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
TX Collisions	Number of transmit packets that are collisions; collisions are caused by the port and attached device transmitting at the same time
TX Excessive	Number of consecutive collisions
TX Deferred	Number of packets deferred

7.10.2 Line Utilization Screen

The Line Utilization screen shows the percentage of line or port bandwidth currently used and the percentage used in the past. Click the **Performance** and **Utilization** tabs at the Ethernet card view to display the screen (see Figure 7-61). At the *Interval* drop-down menu, choose a time segment variable for the intervals. Valid intervals are 1 minute, 15 minutes, 1 hour, and 1 day.

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

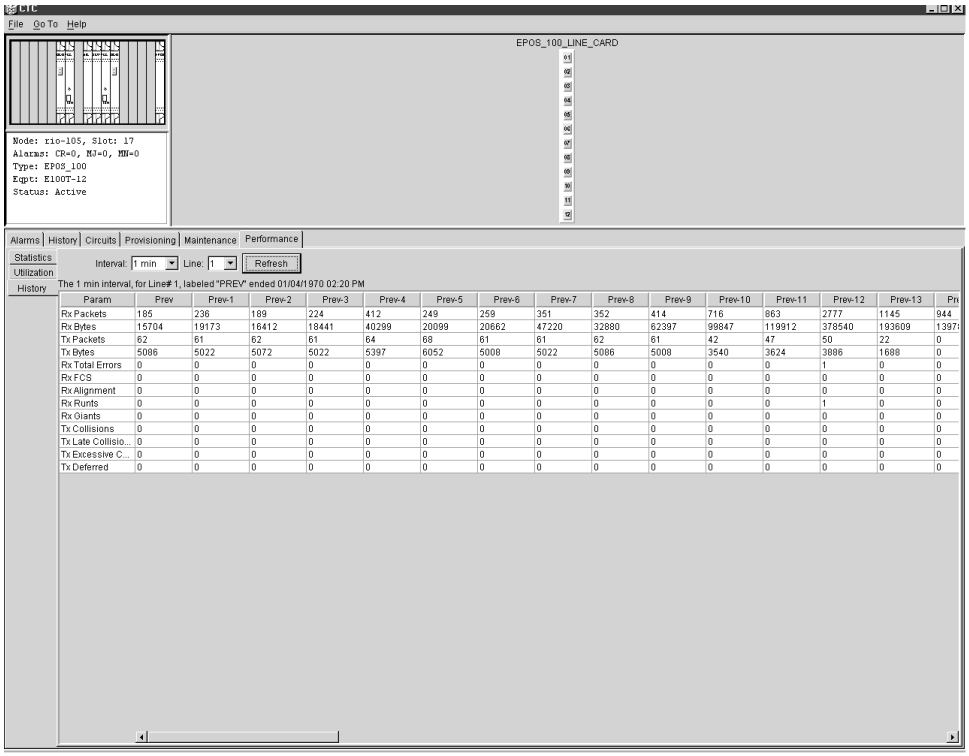
Figure 7-61 Line Utilization



7.10.3 History Screen

The Ethernet History screen lists past Ethernet statistics. Choose the appropriate port from the Line menu. Table 7-7 defines the listed parameters. At the Ethernet card view, click the **Performance** tab and **History** subtab to view the screen (shown in Figure 7-62).

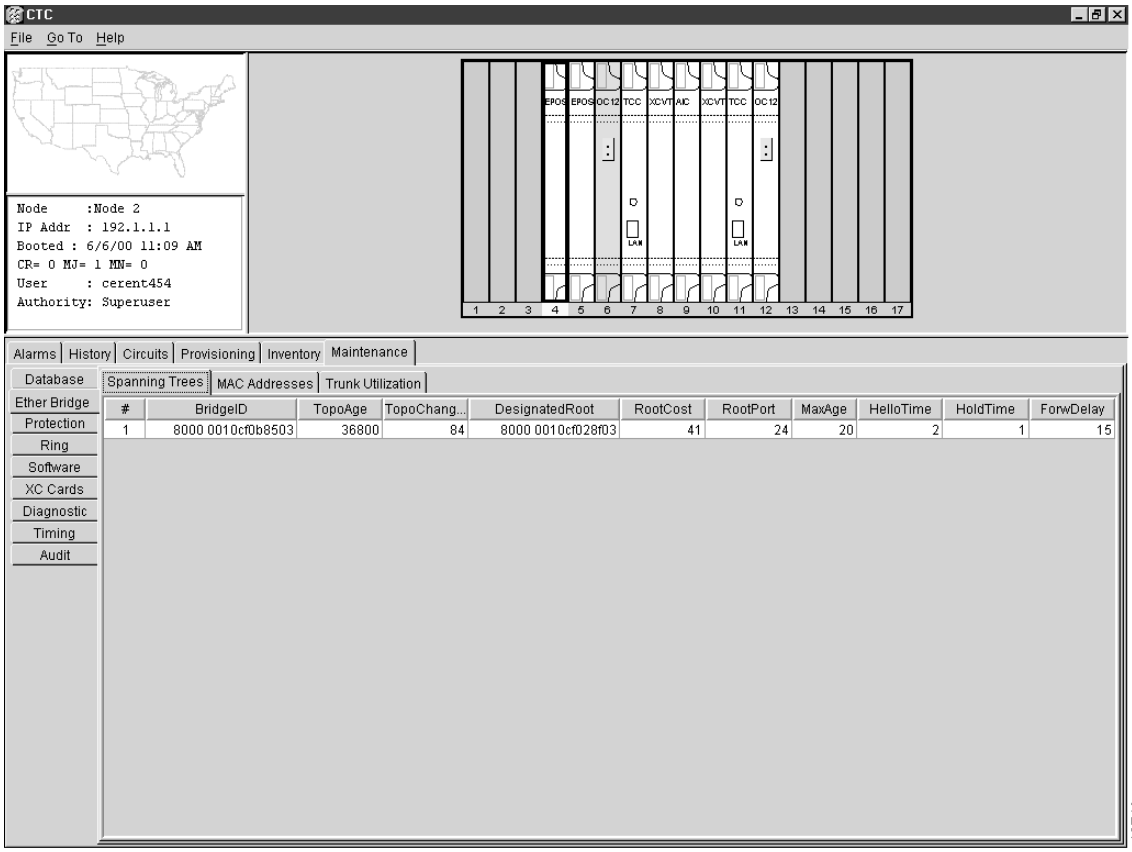
Figure 7-62 Ethernet History



7.10.4 Spanning Trees Screen

The Spanning Trees screen lists information about spanning trees on the ONS 15454. Click the **Maintenance>EtherBridge>Spanning Trees** tabs to view the screen (shown in Figure 7-63). For more information about spanning trees and the ONS 15454, see the "Spanning Tree" section on page 7-10.

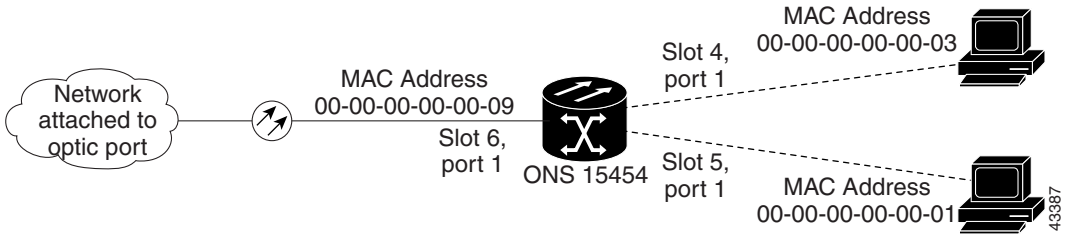
Figure 7-63 Spanning Tree Topology



7.10.5 MAC Addresses Screen

A MAC address is a hardware address that physically identifies the equipment attached to the ONS 15454 port or the network attached to the port. The MAC addresses table (also called the MAC forwarding table) lists the MAC Addresses stored by the ONS 15454 and the VLAN, Slot/Port/STS, and circuit that links the ONS 15454 to each MAC address (see Figure 7-64).

Figure 7-64 MAC Addresses Discovered

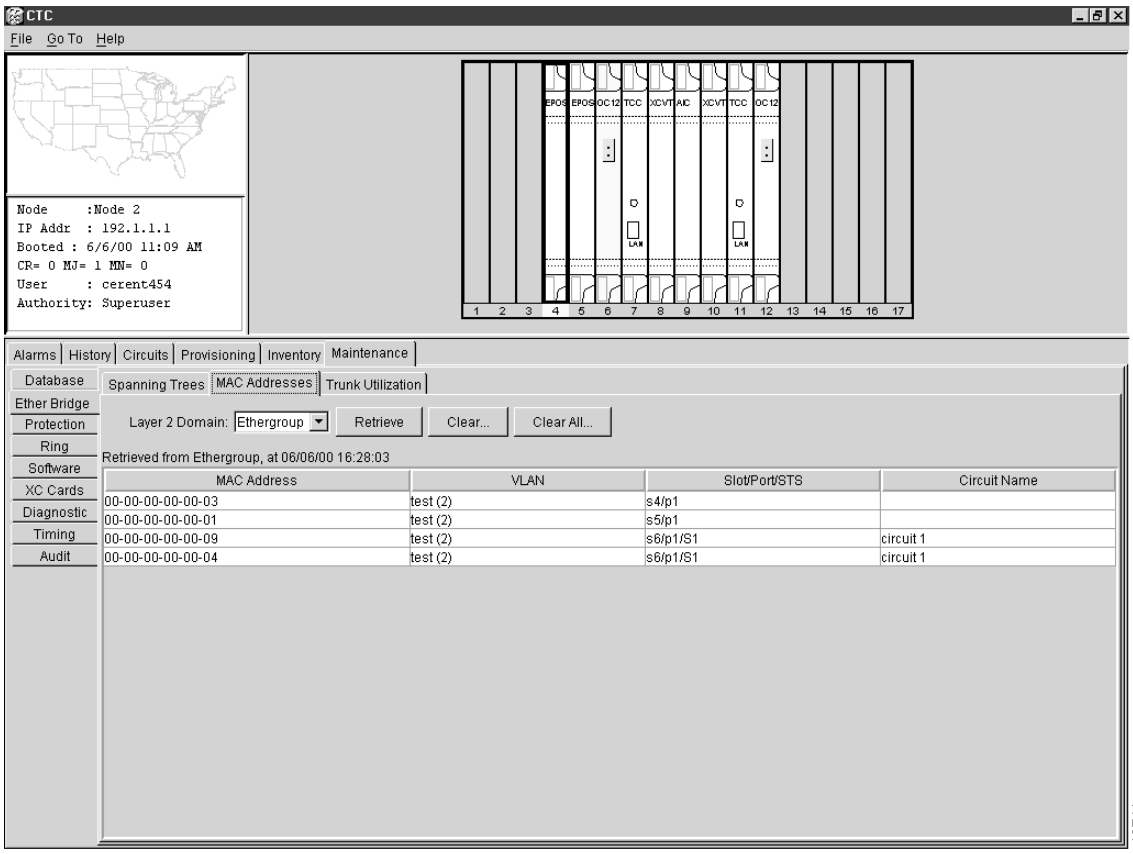


Click the **Maintenance>EtherBridge>MAC Addresses** tabs to view the screen (see Figure 7-65).

- Click **Retrieve** for the ONS 15454 to retrieve and display the current MAC IDs.
- Click **Clear** to clear the highlighted rows.

- Click **Clear All** to clear all displayed rows.

Figure 7-65 MAC Forwarding Table

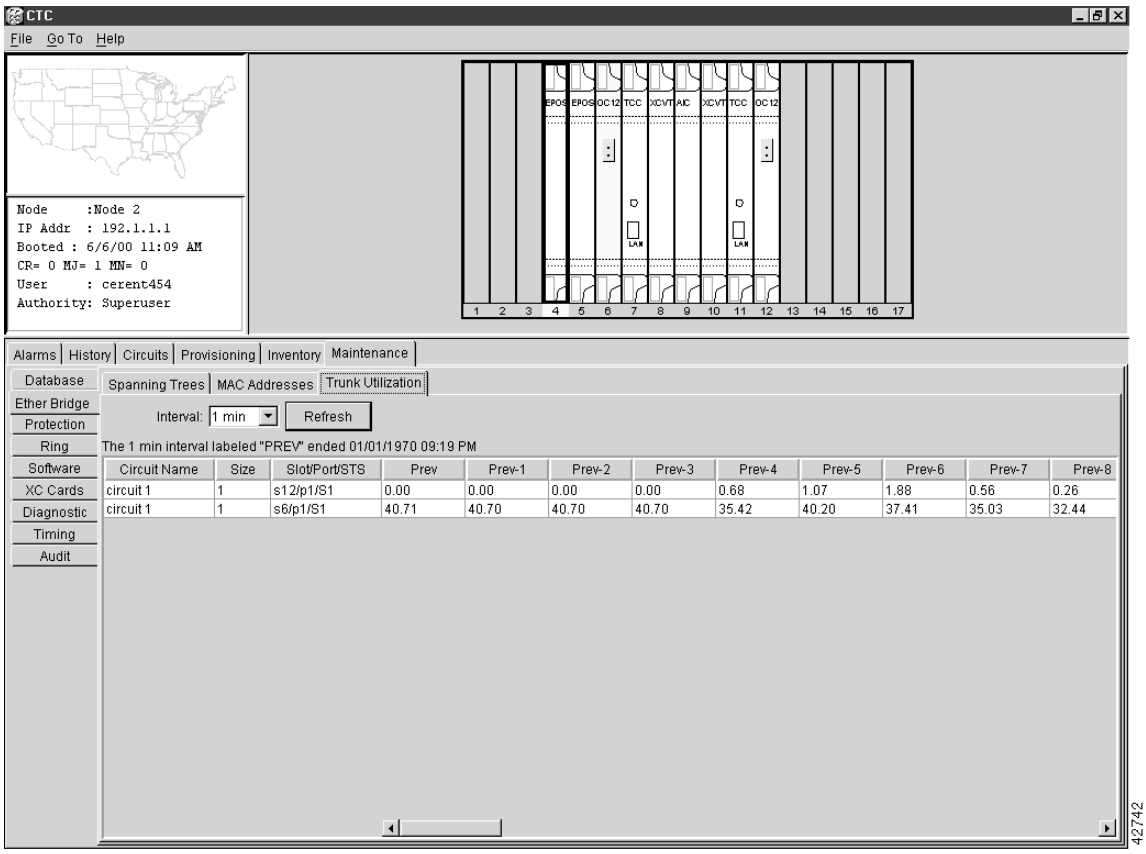


7.10.6 Trunk Utilization Screen

The Trunk Utilization screen is similar to the Line Utilization screen, but the Trunk Utilization screen shows the percentage of circuit bandwidth being used rather than the percentage of line bandwidth being used. Choose a time segment variable for the intervals at the Interval menu. Click the **Maintenance>EtherBridge>Trunk Utilization** tabs to view the screen (shown in Figure 7-66).

Note The percentage shown is the average of ingress and egress traffic.

Figure 7-66 Trunk Utilization



7.11 Remote Monitoring Specification Alarm Thresholds

The ONS 15454 features SNMP Remote Network Monitoring (RMON) that allows network operators to monitor the health of the network with a Network Management System (NMS). For a complete list of the implemented RMON Management Information Bases (MIBs), see the "SNMP Remote Network Monitoring" section on page 8-8.

One of the ONS 15454's RMON MIBs is the Alarm group. The alarm group contains 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. The 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. The following tables define the variables provisioned in the CTC. For example, to set the collision threshold, click **etherStatsCollisions** in the Variable menu.

Table 7-8 Ethernet Threshold Variables (MIBs)

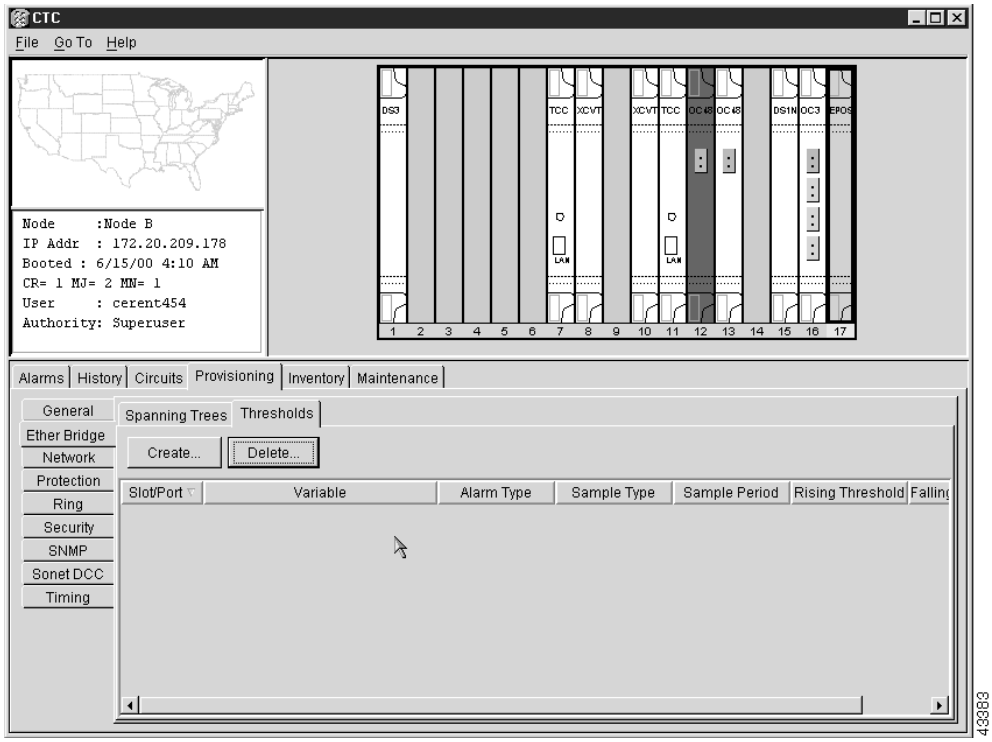
Variable	Definition
iflnOctets	Total number of octets received on the interface, including framing octets.
iflnUcastPkts	Total number of unicast packets delivered to an appropriate protocol.
iflnErrors	Number of inbound packets discarded because they contain errors.
ifOutOctets	Total number of transmitted octets, including framing packets.
ifOutUcastPkts	Total number of unicast packets requested to transmit to a single address.
dot3statsAlignmentErrors	Number of frames with an alignment error, i.e., the length is not an integral number of octets and the frame cannot pass the 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 for which there was exactly one collision.
dot3StatsMutlipleCollisionFrame	Number of successfully transmitted frames for which there were multiple collisions.
dot3StatsDeferredTransmissions	Number of times the first transmission was delayed because the medium was busy.
dot3StatsLateCollision	Number of times that a collision was detected later than 64 octets into the transmission (also added into collision count).
dot3StatsExcessiveCollision	Number of frames for which transmissions failed because of excessive collisions.
dot3StatsFrameTooLong	Number of received frames that were bigger than the maximum size permitted.
etherStatsUndersizePkts	Number of packets received with a length less than 64 octets.
etherStatsFragments	Total number of packets without an integral number of octets or with a bad FCS and less than 64 octets long.
etherStatsPkts64Octets	Total number of packets received (including error packets) that were 64 octets in length.
etherStatsPkts65to127Octets	Total number of packets received (including error packets) that were 65 – 172 octets in length.
etherStatsPkts128to255Octets	Total number of packets received (including error packets) that were 128 – 255 octets in length.
etherStatsPkts256to511Octets	Total number of packets received (including error packets) that were 256 – 511 octets in length.
etherStatsPkts512to1023Octets	Total number of packets received (including error packets) that were 512 – 1023 octets in length.
etherStatsPkts1024to1518Octets	Total number of packets received (including error packets) that were 1024 – 1518 octets in length.
etherStatsBroadcastPkts	Total number of good broadcast packets received.
etherStatsMulticastPkts	Total number of good multicast (non broadcast) packets received.
etherStatsJabbers	Total number of packets longer than 1518 octets without an integral number of octets or 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.

Table 7-8 Ethernet Threshold Variables (MIBs)

Variable	Definition
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 Thresholds

Figure 7-67 Ethernet Alarm Screen



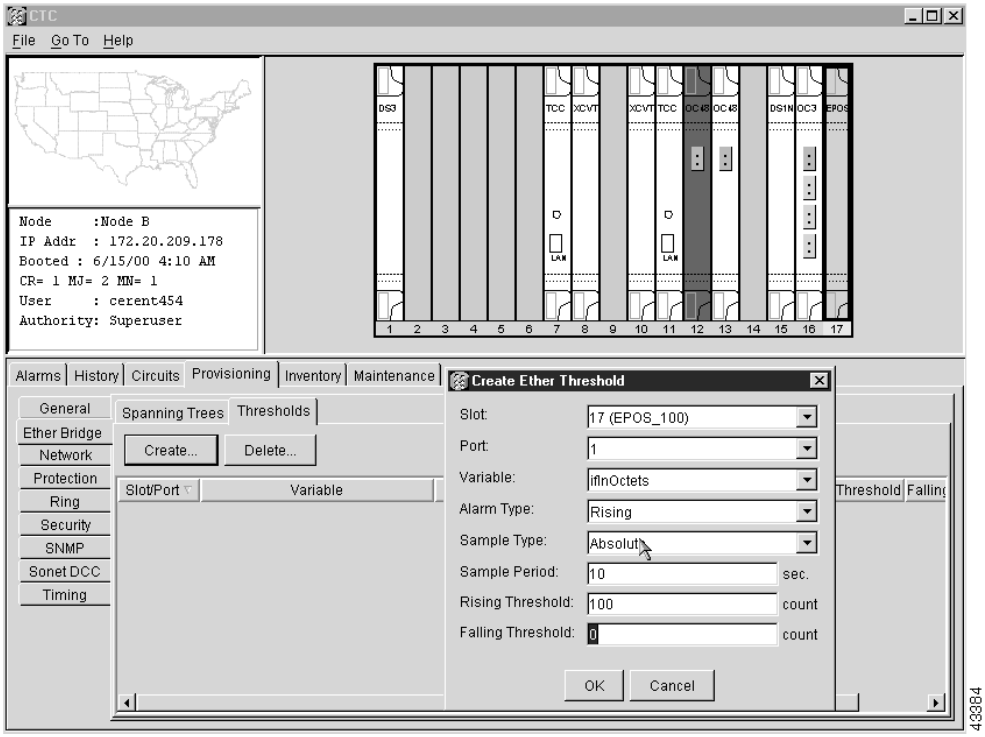
Step 1 From the node view, click the **Provisioning** tab and the **Etherbridge** subtab.

Step 2 Click the **Thresholds** tab.

Step 3 Click **Create**.

The Create Ether Threshold menu appears.

Figure 7-68 Ethernet Alarm Thresholds



Step 4 Click the **Slot** menu to choose the appropriate Ethernet card.

Step 5 Click the **Port** menu to choose the Port on the Ethernet card.

Step 6 Click the **Variable** menu to choose the variable. Table 7-8 lists and defines the Ethernet Threshold Variables available in this field.

Step 7 Click the **Alarm Type** to choose whether the event will be triggered by the rising threshold, falling threshold, or both the rising and falling thresholds.

Step 8 Click the **Sample Type**, 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 The rising threshold is the number of occurrences that must be exceeded to trigger an event. For example, if a network problem causes 1001 collisions in 15 seconds, these occurrences cross a rising threshold set at 1000 collisions in 15 seconds.

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.

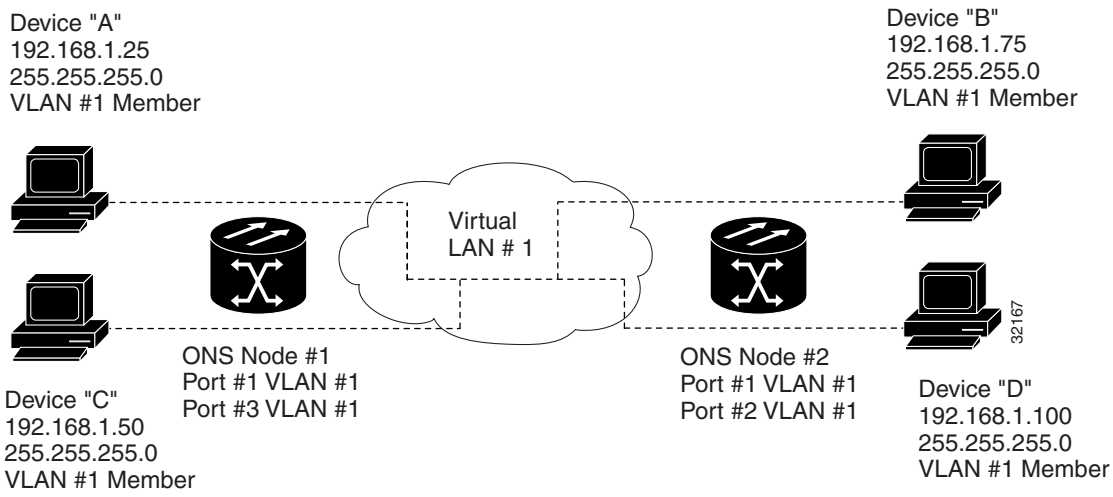
Note A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, it resets the rising threshold. For example, when the network problem that caused 1001 collisions in 15 minutes subsides and creates only 799 collisions in 15 minutes, occurrences fall below a falling threshold of 800 collisions. This resets the rising threshold so that if network collisions again spike over a 1000 per 15- minute period, an event again triggers when the rising threshold is crossed. An event is triggered only the first time a rising threshold is exceeded (otherwise a single network problem might cause a rising threshold to be exceeded multiple times and cause a flood of events).

Step 12 Click the **OK** button to complete the procedure.

7.12 Basic Ethernet Connectivity Testing

Most connectivity problems experienced in an Ethernet network can be fixed by following a few guidelines. Refer to this section if you have problems connecting Ethernet networks. See Figure 7-69 when consulting these guidelines.

Figure 7-69 Ethernet Connectivity Reference



Procedure: Test Ethernet Connectivity

Step 1 Verify that no SONET alarms exist for the STS-N that carries the VLAN #1 Ethernet circuit.

Step 2 Verify that no Ethernet specific alarms exist.

Step 3 Verify that the ACT LED on the Ethernet card is green.

Step 4 Verify that Ports 1 and 3 on ONS 15454 #1 and Port 1 and Port 2 on ONS 15454 #2 have green link-integrity LEDs. If there is no green link-integrity LED for any of these ports:

(a) Verify physical connectivity between the ONS 15454s and the attached device.

(b) Verify that the ports are enabled on the Ethernet cards.

(c) Verify that you are using the proper Ethernet cable and that it is wired correctly.

Step 5 Verify connectivity between device A and device C by performing an ICMP ping between these locally attached devices. If the ping is unsuccessful:

(a) Verify that device A and device C can ping each other.

(b) Verify that device A and device C are on the same IP subnet.

(c) Verify that both Port 1 and Port 3 on the Ethernet card are assigned to the same VLAN.

Step 6 Repeat Steps 4 and 5 for devices B and D.

Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that both ONS 15454 #1 and ONS 15454 #2 are included in the VLAN #1 circuit.

Network Management

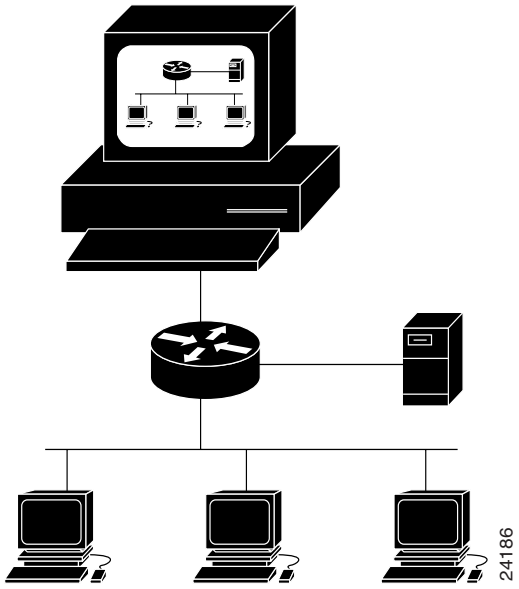
This chapter explains concepts related to network management with the ONS 15454. It includes Simple Network Management Protocol (SNMP), front panel LCD IP entry, Proxy ARP, IP addressing and subnets, IP troubleshooting, and Static Route Provisioning.

8.1 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer Internet Protocol (IP) that allows network devices to exchange management information. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

The Cisco ONS 15454 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both versions share many features, but SNMPv2c offers additional protocol operations. This section describes both versions and explains how to configure SNMP on the ONS 15454. Figure 8-1 illustrates a basic network managed by SNMP.

Figure 8-1 Basic Network Managed by SNMP

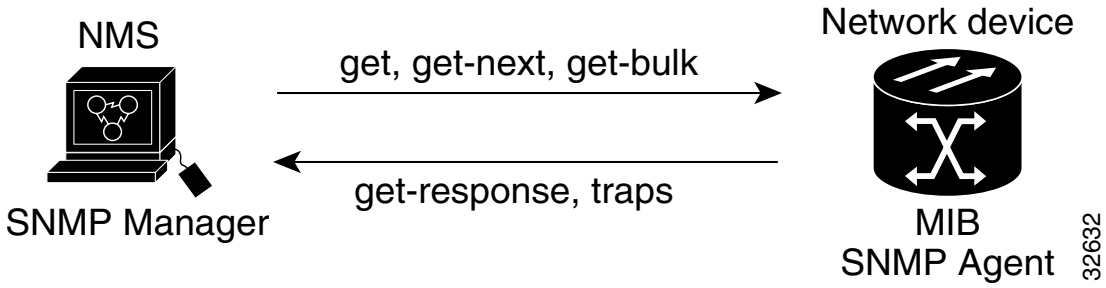


8.1.1 SNMP Basic Components

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 a 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 printers.

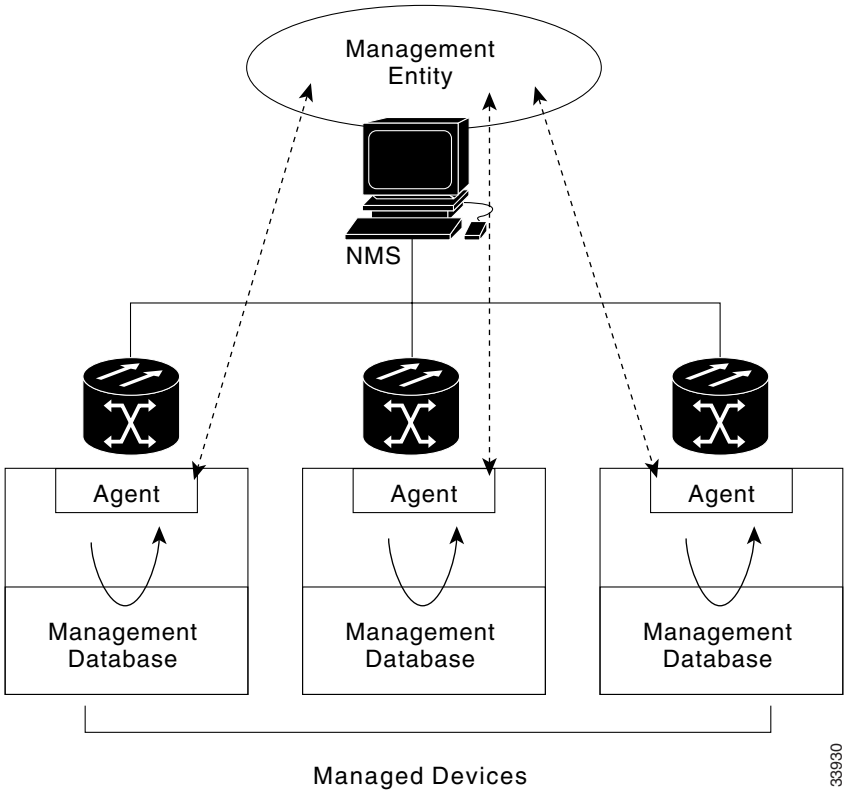
An agent is a software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP. The SNMP agent gathers data from the management information base (MIB), which is the repository for information about device parameters and network data. The agent can also send traps, or notification of certain events, to the manager. Figure 8-2 illustrates these SNMP operations.

Figure 8-2 SNMP Operations



A management system 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 8-3 illustrates the relationship between the three key SNMP components.

Figure 8-3 SNMP Components



8.1.2 SNMP Support

The ONS 15454 supports SNMP v1 and v2c traps and gets. The SNMP MIBs in the ONS 15454 define alarms, traps, and status. Through SNMP, network management system (NMS) applications can query a management agent using a supported MIB. The functional entities include an Ethernet switch, SONET multiplexer, and many others. SNMP can access the ONS 15454 through the Timing Communication and Control (TCC) card Ethernet port, the backplane LAN wire-wrap, or SONET Data Communication Channel (SDCC).

Procedure: Set up SNMP Support

Step 1 On the Cisco Transport Controller (CTC) window, click the **Provisioning** tab.

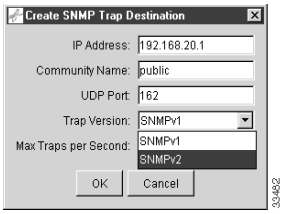
Step 2 From the Provisioning menu, click the **SNMP** function tab.

Step 3 Click **Create**.

The Create SNMP Trap Destination dialog opens (Figure 8-4).

For a description of SNMP traps, see the "SNMP Traps" section on page 8-7.

Figure 8-4 Create SNMP Trap Destination Dialog



Step 4 Type the IP address of your NMS in the *IP Address* field.

Step 5 Type the SNMP community name in the *Community Name* field.

For a description of SNMP community names, see the "SNMP Community Names" section on page 8-8.

Note The community name is a form of authentication and access control. The community name assigned to the ONS 15454 is case-sensitive and must match the community name of the NMS.

Note The default UDP port for SNMP is 162.

Step 6 Set the *Trap Version* field for either SNMPv1 or SNMPv2.

Refer to your NMS documentation to determine whether to use SNMP v1 or v2.

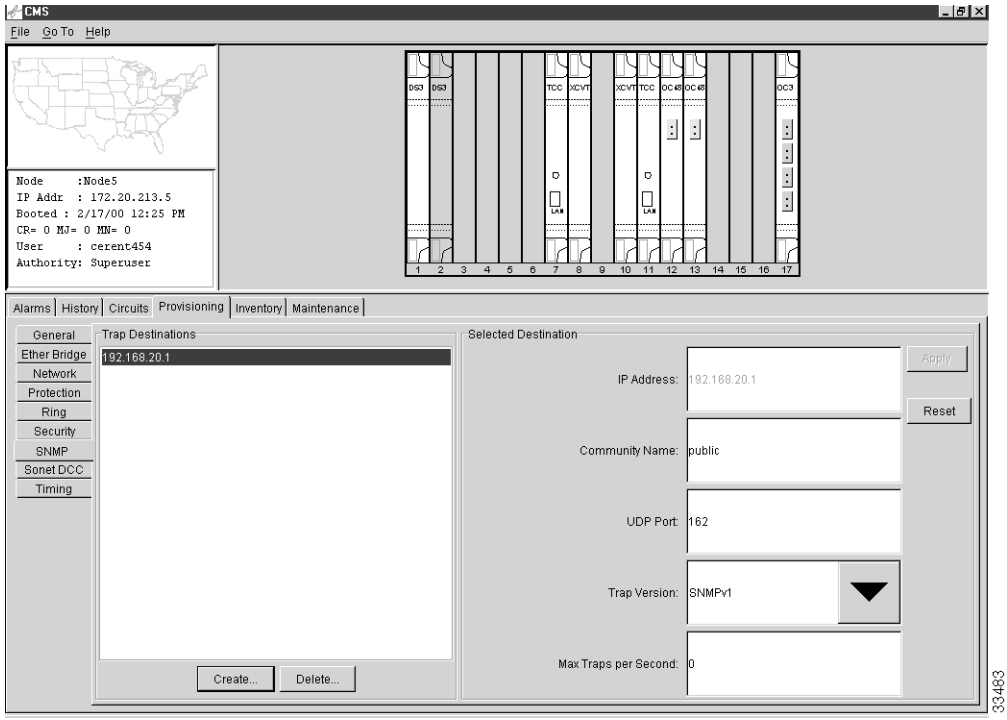
Step 7 Set your maximum traps per second in the *Max Traps per Second* field.

Note The max traps per second is the maximum number of traps per second that you want sent to the SNMP manager. If set to 0, there is no maximum and all traps are sent.

Step 8 Click **OK**.

SNMP settings are now configured. To view SNMP information for each node, click the IP address of a node on the Trap Destinations screen (Figure 8-5).

Figure 8-5 Trap Destinations Screen



8.1.3 SNMP MIBs

A Management Information Base (MIB) is a hierarchically-organized collection of information. MIBs are accessed using a network-management protocol such as SNMP. They are comprised of managed objects and are identified by object identifiers.

The ONS 15454 SNMP manager uses information in the MIB to perform the operations described in Table 8-1

.

Table 8-1 SNMP Manager Operations

Operation	Description
get-request	Retrieve a value from a specific variable
get-next-request	Retrieve the value following the named variable; Often used to retrieve variables from within a table (1)
get-response	The reply to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS
get-bulk-request	Similar to get-next-request, but fill the get-response with up to max-repetition number of get-next interactions
trap	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred

1.With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within the MIB.

A managed object (sometimes called a MIB object) is one of any number of specific characteristics of a managed device. Managed objects are comprised of one or more object instances that are essentially variables.

The ONS 15454 MIBs ship on the accompanying software CD. These MIBs need to be compiled in the following order. If the order is not followed, one or more MIB files may not compile.

1 cerentregistry.mib

2 cerentTC.mib

3 cerent454.mib

If you are unable to compile the ONS 15454 MIBs, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Table 8-2 IETF Standard MIBs Implemented in the ONS 15454 SNMP Agent

RFC#	Module Name	Title/Comments
1213 +1907	RFC1213-MIB, SNMPV2-MIB	MIB-II from RFC1213 with enhancement from RFC1907 for v2
1493	BRIDGE-MIB	Bridge/Spanning Tree (SNMPv1 MIB)
2037	ENTITY-MIB	Entity MIB using SMI v2
2233	IF-MIB	Interface evolution (enhances MIB-II)
2358	Etherlike-MIB	Ethernet-like interface (SNMPv2 MIB)
2495		DS-1/E1
2496		DS-3/E3
2558	SONET-MIB	SONET

Table 8-2 IETF Standard MIBs Implemented in the ONS 15454 SNMP Agent

RFC#	Module Name	Title/Comments
2674		P-Bridge and Q-Bridge MIB

8.1.4 SNMP Traps

The ONS 15454 can receive SNMP requests from a number of SNMP managers and send traps to ten trap receivers. The ONS 15454 generates all alarms and events as SNMP traps.

Traps generated by the ONS 15454 contain an object ID that uniquely identifies the alarm. An entity identifier uniquely identifies which entity generated the alarm (slot, port, STS, VT, BLSR, STP, etc.). The traps give the severity of the alarm (critical, major, minor, event, etc.) and indicate whether the alarm is service affecting or non-service affecting. The traps also contain a date/time stamp that shows the date and time the alarm occurred. The ONS 15454 also generates a trap for each alarm when the alarm condition clears.

Each SNMP trap contains seven variable bindings (Table 8-3).

Table 8-3 SNMP Trap Variable Bindings

Number	Name	Description
1	cerentNodeTime	Indicates current local time as reflected by the ONS 15454
2	cerent454AlarmState	Specifies alarm severity and service affecting status (SA/NSA); only {minor|major|critical}+{NA|NSA} are represented here
3	cerent454AlarmObjectType	Indicates what type of entity raised this alarm (for example, DS-3, etherBridge, VT-TERM, etc); the NMS often uses this value to decide which table to poll for further information about the alarm
4	cerent454AlarmObjectIndex	Every alarm is raised by an object that is an entry in a specific table. This is the index of the object in that table; in other words, if the alarm is interface related, this is the index of the interface in the interface table.
5	cerent454AlarmSlotNumber	This indicates the object slot that raised this alarm; if no slot is relevant to the alarm, the object slot will be zero
6	cerent454AlarmPortNumber	This indicates the object port that raised this alarm; if no object port is relevant to the alarm, the object port will be zero.
7	cerent454AlarmLineNumber	This indicates the object LINE that raised this alarm; If no LINE is relevant to the alarm, the LINE will be zero.

The ONS 15454 supports generic and Internet Engineering Task Force (IETF) traps. The generic traps are listed in Table 8-4. IETF-supported traps are listed in Table 8-5.

Table 8-4 Generic Traps Supported in the ONS 15454

Trap	From RFC#	IETF Standard Objects in Varbind List	Description
ColdStart	RFC1213-MIB	None	Agent up - cold start
WarmStart	RFC1213-MIB	None	Agent up - warm start

Table 8-4 Generic Traps Supported in the ONS 15454

Trap	From RFC#	IETF Standard Objects in Varbind List	Description
AuthenticationFailure	RFC1213-MIB	None	Community string did not match

Table 8-5 IETF Traps Supported by the ONS 15454

Trap	From RFC #	IETF standard objects in varbind list	Description
NewRoot	RFC1493/ BRIDGE-MIB	None	Sending agent is the new root of the spanning tree
TopologyChange	RFC1493/ BRIDGE-MIB	None	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking
EntConfigChange	RFC2037/ ENTITY-MIB	None	entLastChangeTime value has changed

8.1.5 SNMP Community Names

You can provision community names for all SNMP requests from the SNMP Trap Destination window in CTC (see the "Set up SNMP Support" section on page 8-3). In effect, any SNMP request using a community name that matches a community name on the list of provisioned SNMP trap destinations is considered valid. Otherwise, the request is considered invalid and is dropped.

If an SNMP request contains an invalid community name, the request is silently dropped and the MIB variable, snmpInBadCommunityNames, is incremented. All SNMP requests containing a validated community name are granted access to all MIB variables managed by the agent.

8.1.6 SNMP Remote Network Monitoring

The ONS 15454 incorporates Remote Monitoring (RMON) to allow network operators to monitor the ONS 15454's E100 and E1000 cards. This feature is not apparent to the typical CTC user, because RMON interoperates with a network management application. However, with CTC the user can provision the RMON alarm thresholds (see the "Remote Monitoring Specification Alarm Thresholds" section on page 7-69). The CTC also monitors the five RMON groups implemented by the ONS 15454.

The ONS 15454 RMON implementation is based on the IETF standard MIB Request for Comment (RFC)1757. The ONS 15454 implements five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

8.1.6.1 Ethernet Statistics Group

The Statistics group contains the basic statistics for each monitored subnetwork in a single table named etherstats.

8.1.6.2 History Control Group

The History Control group defines sampling functions for one or more monitor interfaces. RFC 1757 defines the historyControlTable.

8.1.6.3 Ethernet History Group

RFC 1757 defines the etherHistoryTable. The etherHistoryTable will be implemented as defined in RFC 1757, within the bounds of the historyControlTable.

8.1.6.4 Alarm Group

The alarm group consists of a single alarm table. This table provides the network performance alarm thresholds for the network management application.You can provision the thresholds in the table with CTC.

8.1.6.5 Event Group

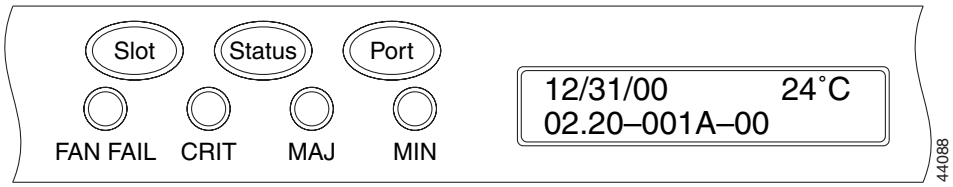
The event group consists of two tables, evenTable and logTable. The evenTable is read-only. The logTable is implemented as specified in RFC 1757.

8.2 IP Address Entry Using Front Panel LCD

Users can set up the IP address, subnet mask, and default router addresses of the ONS 15454 using the slot, status, and port buttons on the front panel LCD (see Figure 8-6). This allows users to accomplish these basic operations without a computer.

Note You can lock out the front panel LCD access to network configuration. Using the CTC at the shelf view, click the **Provisioning** and **Network** tabs. Check **Prevent LCD IP Config** and click **Apply**.

Figure 8-6 Front Panel LCD



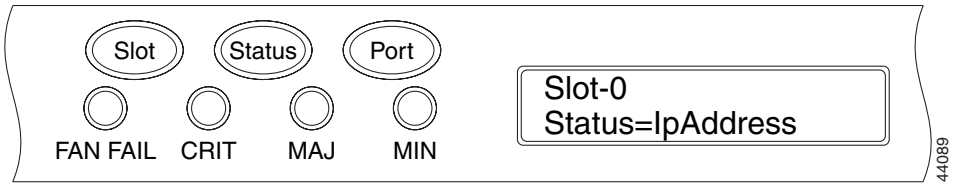
Procedure: Enter IP Address Using Front Panel LCD

Note The LCD reverts to normal display mode after 30 seconds of button inactivity.

Step 1 Repeatedly press the **Slot** button until Slot-0 appears on the LCD panel. This is the Slot-0 menu.

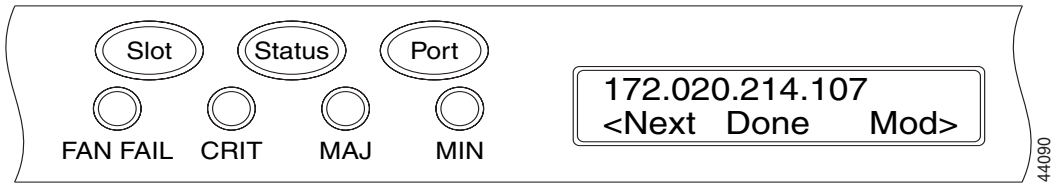
Step 2 Repeatedly press the **Port** button to scroll through the configuration menus.

Figure 8-7 IP Address Option



Step 3 When the IP Address option appears, press the **Status** button (Figure 8-7).

Figure 8-8 IP Address LCD Screen

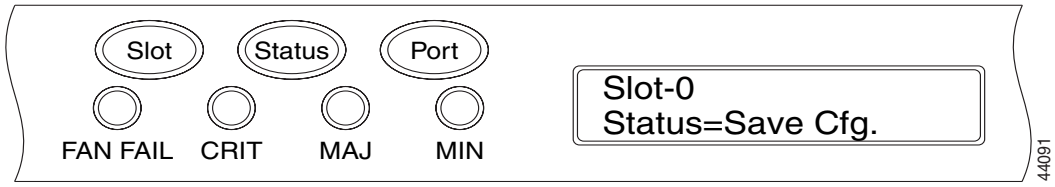


Step 4 Push the **Slot** (Next) button to move to the IP address digit you need to change. The selected digit flashes.

Step 5 Press the **Port** (Modify) button to cycle the IP address digit to the correct digit.

Step 6 When the desired IP address is set, press the **Status** (Done) button to return to the Slot-0 menu.

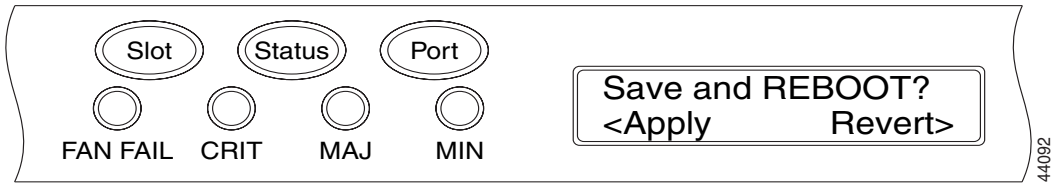
Figure 8-9 Save Configuration Option LCD Screen



Step 7 At the Slot-0 menu, repeatedly press the **Port** button until the Save Configuration option appears (Figure 8-9).

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

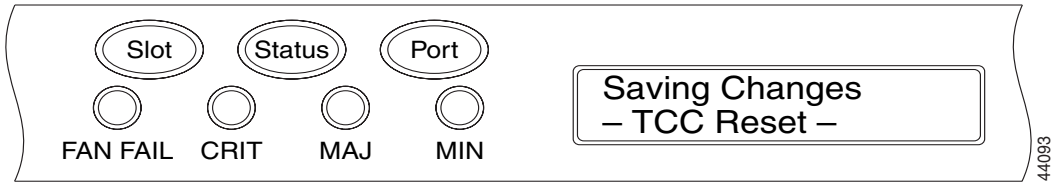
Figure 8-10 Save and REBOOT LCD Screen



The Save and REBOOT screen appears (Figure 8-10).

Step 9 Press the **Slot** (Apply) button to save the new IP address configuration.

Figure 8-11 Saving Changes LCD Screen



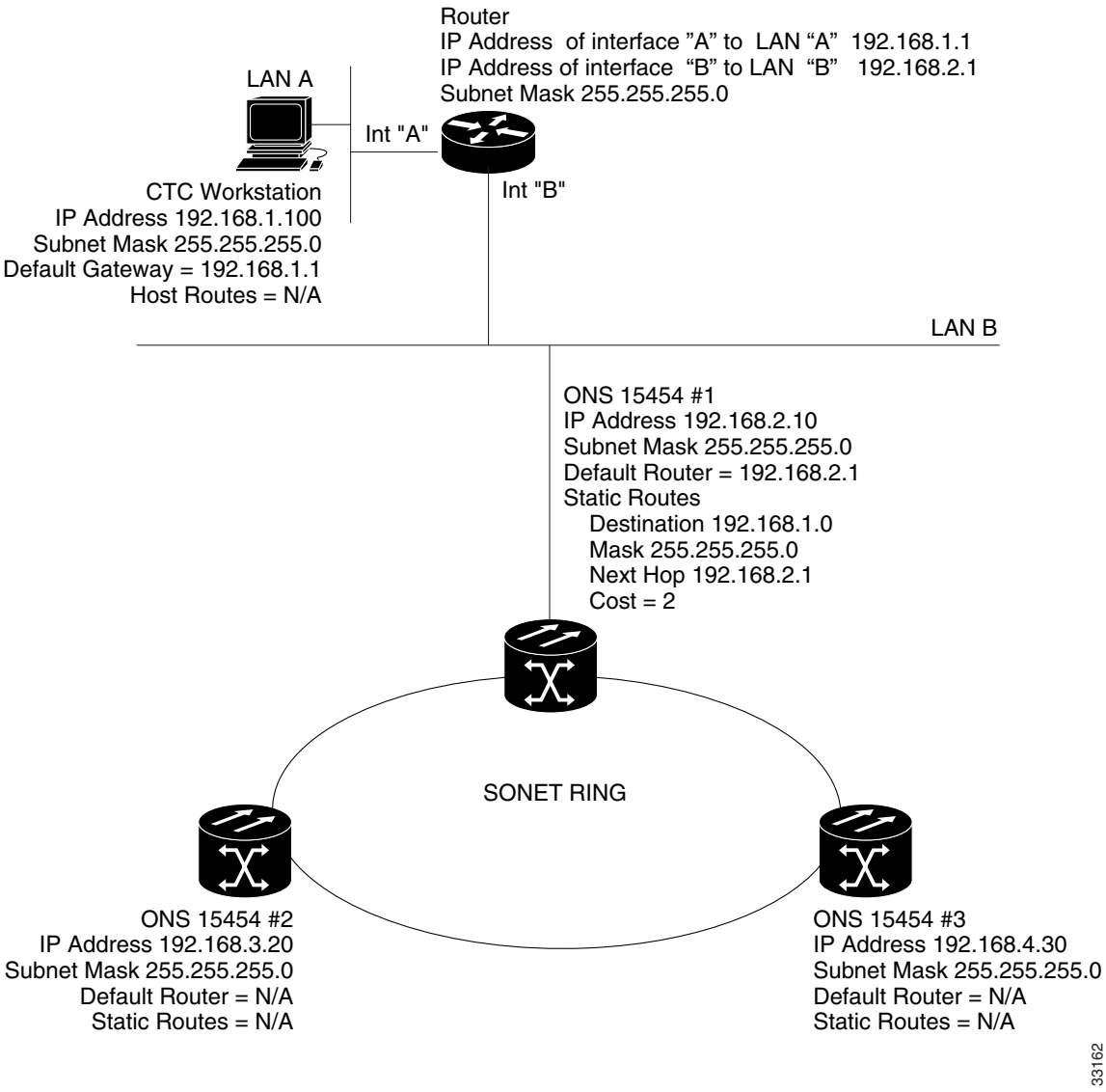
Saving a new configuration reboots the TCC cards. The Saving Changes LCD appears for several minutes while the TCC cards reboot (Figure 8-11). When the LCD screen returns to the normal alternating display mode, the procedure is complete.

8.3 Proxy ARP

Proxy Address Resolution Protocol (ARP) enables a LAN-connected gateway ONS 15454 to automatically handle ARP requests for remote non-LAN ONS 15454s connected via DCC to the gateway ONS 15454. Proxy ARP requires no configuration from the user and eliminates the need for the user to set up static host routes.

Proxy ARP works by having a single LAN-connected ONS 15454 proxy for remote ONS 15454s. If a device on the LAN sends an ARP request intended for one of the DCC-connected ONS 15454s, then the gateway ONS 15454 ONS 15454 returns its own MAC address to the LAN device (proxies). The LAN device then sends the datagram intended for the remote ONS 15454 to the MAC address of the proxy ONS 15454. The proxy ONS 15454 forwards this data to the remote 15454 using its own ARP table. The ARP table matches IP addresses with the MAC IDs of remote ONS 15454s and is built through internal OSPF routing protocol. Figure 8-12 illustrates Proxy ARP.

Figure 8-12 ONS 15454 Network Using Proxy ARP



Note Proxy ARP is automatic and requires no user input.

8.4 IP Addressing and Subnets

This section provides IP addressing guidelines for the ONS 15454. The IP addressing information includes IP addressing classes and IP configuration scenarios.

8.4.1 Types of IP Addresses

IP addresses are categorized as either Class A, B, or C. The different classes refer primarily to how the addresses may be used and how many subnets and hosts will be available for use in the network.

Each network needs its own, unique network number and each host within a network needs a unique host number.

Subnetting is used to maximize the number of networks available within a range (class) of addresses. Each class of address allows a different number of subnets to be configured.

8.4.1.1 Class A Addresses and Subnets

In a class A IP address, the first eight bits are used for the network ID, and the last 24 bits are used for the host ID. The first bit of a network address will be 0 when the number is converted to binary. For example, 5.xxx.xxx.xxx = 00000101 (5). The maximum number of network addresses that can be derived in class A is 126; the maximum number of hosts is 16,777,214. The address 0.0.0.0 is reserved as the default route and 127.xxx.xxx.xxx is reserved as the loopback address. The natural mask is 255.0.0.0 and the available addresses are 1.xxx.xxx.xxx through 126.xxx.xxx.xxx.

8.4.1.2 Class B Addresses and Subnets

In a class B IP address, the first 16 bits are used for the network ID and the last 16 bits are used for the host ID. The first two bits of a network address begin with 10 when the number is converted to binary. For example, 128.x.x.x = 10000000. The maximum number of network addresses that can be derived from class B is 16,384; the maximum number of hosts is 65,534. The natural mask is 255.255.0.0 and the available addresses are 128.0.xxx.xxx through 191.255.0.0.

8.4.1.3 Class C Addresses and Subnets

In a class C IP address, the first 24 bits are used for the network ID and the last eight bits are used for the host ID. The first two bits of a network address begin with 11 when the number is converted to binary. For example, 192.x.x.x = 11000000. The maximum number of network addresses that can be derived from class C is 2,097,152; the maximum number of hosts is 254. The natural mask is 255.255.255.0 and the available addresses are 192.0.0.xxx through 223.255.255.xxx.

8.4.2 Common IP Addressing Scenarios with the ONS 15454

ONS 15454 IP addressing generally has seven common IP addressing scenarios or configurations. Refer to the following illustrations and checklists when setting IP addresses and configuring subnets. You must be able to answer yes to each checklist question to be sure that all IP addressing guidelines are met. The following figures illustrate these seven scenarios and provide an IP checklist for each scenario.

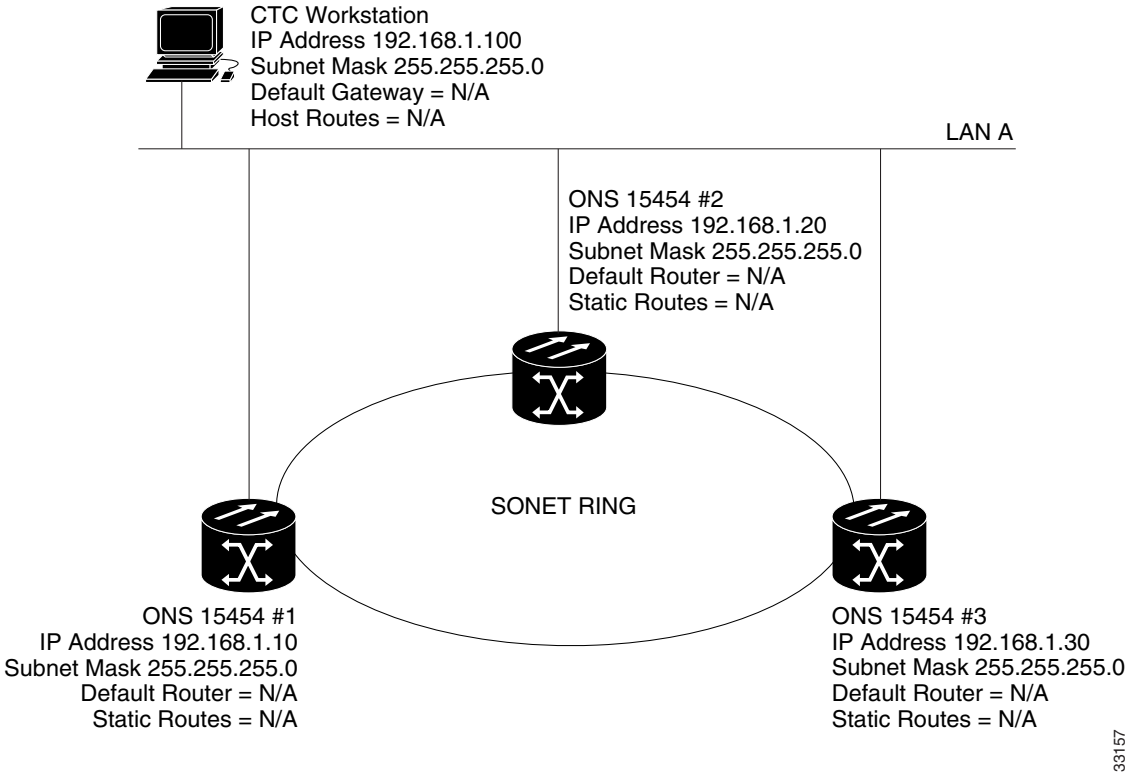
Note Beginning with Release 2.2.0, LAN devices no longer need host routes to communicate with other ONS 15454s on the same subnet that connect through DCC.

8.4.2.1 IP Scenario 1

ONS 15454s and CTC are on the same subnet; all ONS 15454s attach to LAN A.

If you answer No to any of the questions in the checklist see the "IP Troubleshooting" section on page 8-28.

Figure 8-13 IP Addressing Scenario 1



Procedure: IP Checklist for Scenario 1

- Are the IP addresses of ONS 15454s #1, #2 and #3 on the same IP subnet?
- Are all of the IP addresses unique?
- Can the workstation running CTC ping itself?
- Is there link integrity between the CTC workstation and the hub/switch?
- Do the LAN wire-wrap pins on the backplane/TCC's RJ-45 port have link integrity? On all ONS 15454s and the hub/switch?
- Is the hub/switch port for all ONS 15454s set for 10 Mbps half-duplex?
- Can you ping ONS 15454 #1, #2, and #3 from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 or higher)?
- Do you have the Java plug-in installed (version 1.2.2. or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?

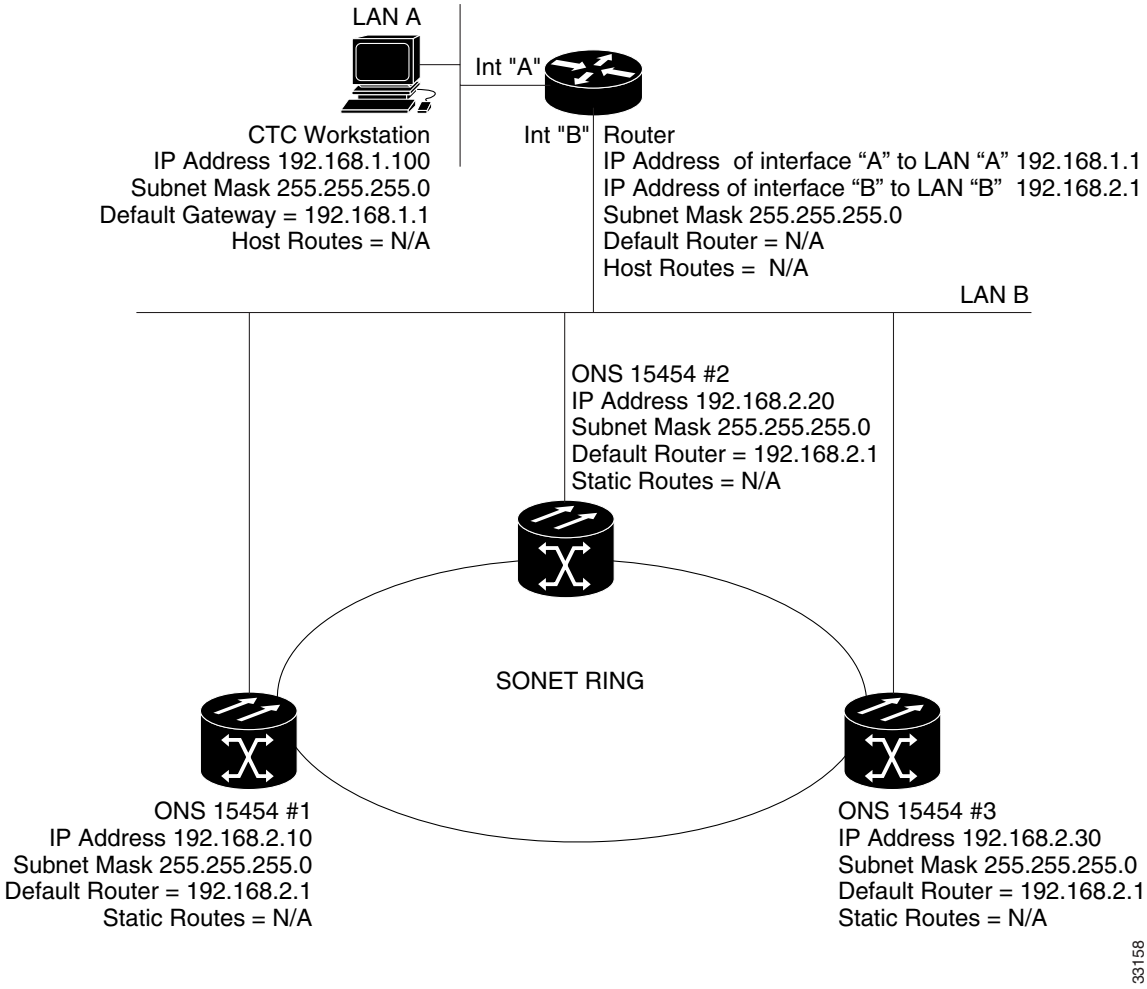
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.4.2.2 IP Scenario 2

ONS 15454s and CTC are on different subnets; all ONS 15454s attach to LAN B.

If you answer No to any of the questions in the checklist see the "IP Troubleshooting" section on page 8-28.

Figure 8-14 IP Addressing Scenario 2



Procedure: IP Checklist for Scenario 2

- Is the IP address of the CTC workstation and the router interface A on the same subnet?
- Can the workstation running CTC ping itself?
- Is the workstation's default gateway set to the same IP address as the router A interface?
- Are the IP addresses of the ONS 15454 #1, #2, and #3 on the same subnet as the router's B interface?

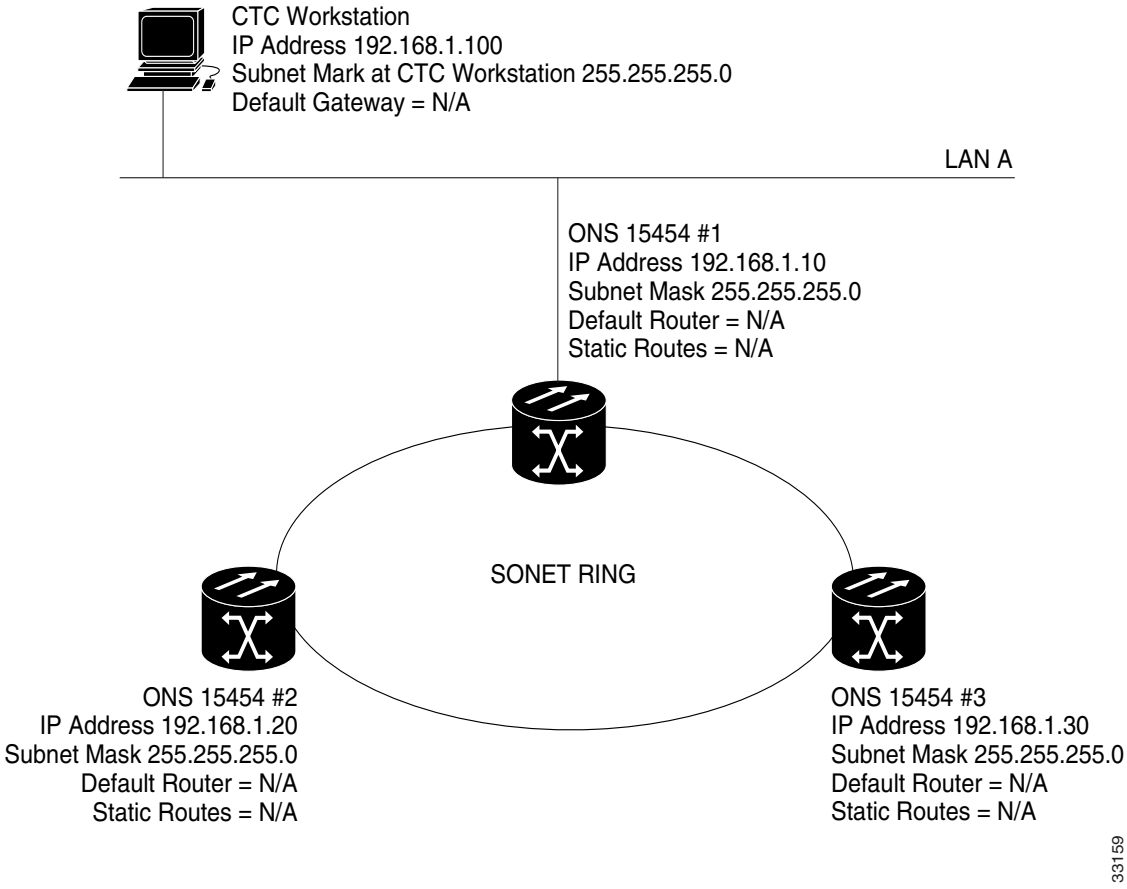
- Are all of the IP addresses unique?
- Is the default router of the ONS 15454 #1, #2, and #3 set to the IP address of the router's B interface?
- Is there link integrity between the workstation and the hub/switch?
- Is there link integrity between the LAN wire-wrap pins on the backplane or the TCC's RJ-45 port of all nodes and the hub/switch(es)?
- Is there link integrity between the router ports and their hubs/switches?
- Are the hub/switch ports on all ONS 15454s set for 10 Mbps half-duplex?
- Can you ping ONS 15454 #1, #2 and #3 from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 or higher)?
- Do you have the Java plug-in installed (version 1.2.2 or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.4.2.3 IP Scenario 3

CTC and all ONS 15454s are on the same subnet; ONS 15454 #1 is attached to LAN A and ONS 15454 #2 and #3 are at remote sites

If you answer No to any of the questions in the checklist, see the "IP Troubleshooting" section on page 8-28.

Figure 8-15 IP Addressing Scenario 3



Procedure: IP Checklist for Scenario 3

- Is the workstation IP address and the IP address of all ONS 15454s on the same IP subnet?
- Are all of the IP addresses unique?
- Can the workstation running CTC ping itself?
- Are host routes configured on the CTC workstation for each remote node (ONS 15454 #2 and #3)?
- Is there link integrity between the CTC workstation and the hub/switch?
- Is there link integrity between the LAN wire-wrap pins on the backplane or the active TCC RJ-45 port and the hub/switch?
- Is the hub/switch port set for 10 Mbps half-duplex?

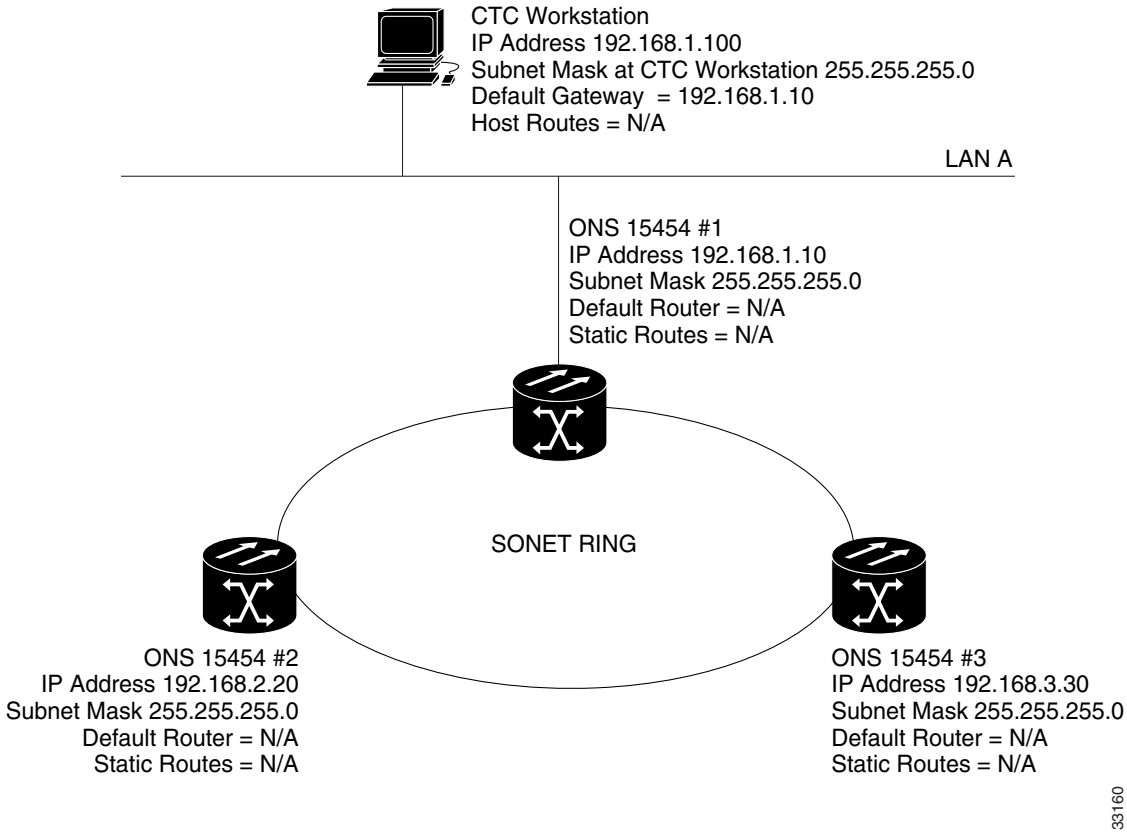
- Can you ping ONS 15454 #1 from the CTC workstation?
- Are the optical trunk ports on all nodes in service?
- Is the DCC enabled for all optical trunk ports that are in service?
- Can you ping the remote nodes (ONS 15454 #2 and #3) from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 or higher)?
- Do you have the Java plug-in installed (version 1.2.2 or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.4.2.4 IP Scenario 4

CTC and ONS 15454 #1 are on the same subnet, while ONS 15454 #2 and # 3 are on different subnets; ONS 15454 #1 is attached to LAN A and ONS 15454 #2 and #3 are at remote sites.

If you answer No to any of the questions in the checklist, see the "IP Troubleshooting" section on page 8-28.

Figure 8-16 IP Addressing Scenario 4



Procedure: IP Checklist for Scenario 4

- Is the CTC workstation IP address and the ONS 15454 #1 IP address on the same subnet?
- Are the IP addresses of ONS 15454 #1, #2, and #3 on different subnets?
- Are all of the IP addresses unique?
- Can the workstation running the CTC ping itself?
- Is the CTC workstation's default gateway set to the same IP address as ONS 15454 #1?
- Is there link integrity between the workstation and the hub/switch?
- Is there link integrity between the LAN wire-wrap pins on the backplane or the active TCC RJ-45 port and the hub/switch?
- Is the hub/switch port set for 10 Mbps half-duplex?
- Can you ping ONS 15454 #1 from the CTC workstation?
- Are the optical trunk ports on all nodes in service?

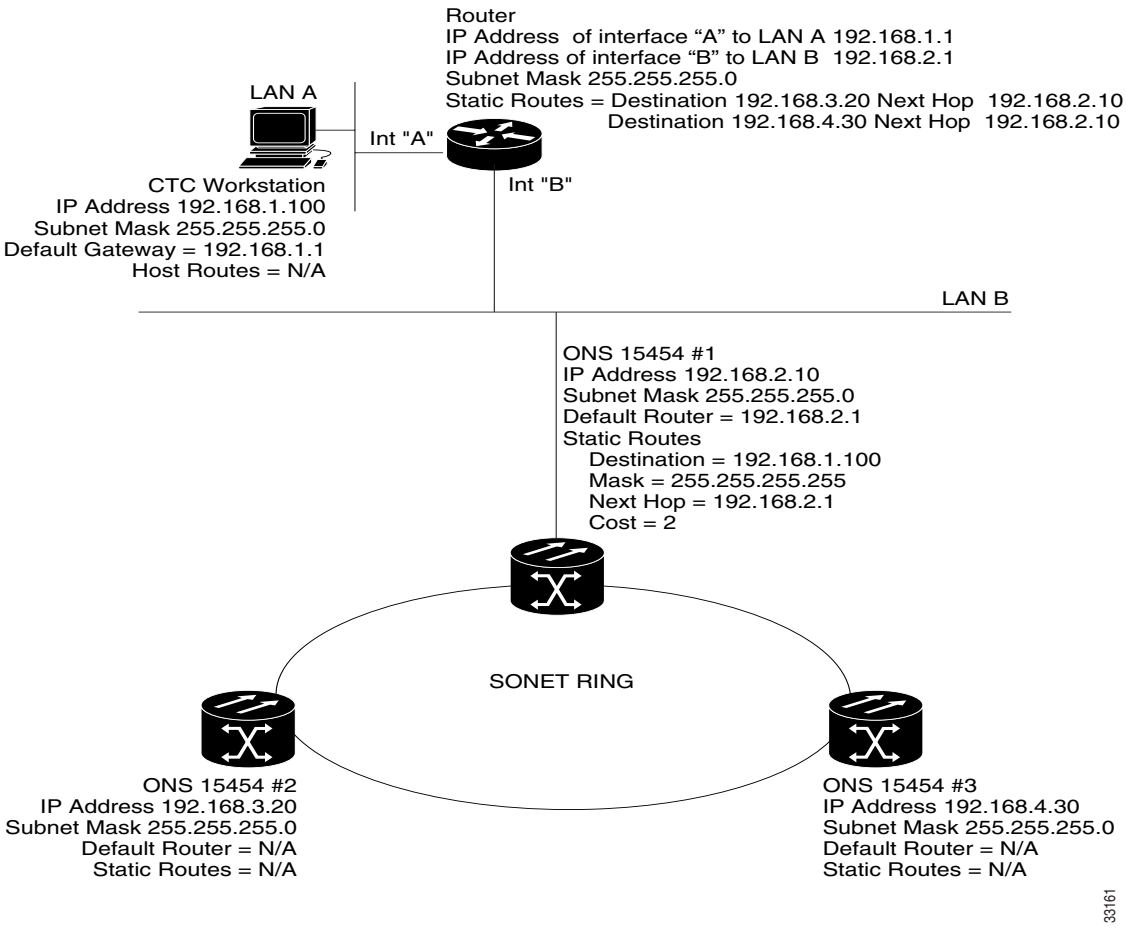
- Is the DCC enabled for all optical trunk ports that are in service?
- Can you ping the remote nodes (ONS 15454 #2 and #3) from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 and higher)?
- Do you have the Java plug-in installed (version 1.2.2 or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.4.2.5 IP Scenario 5

CTC and each of the ONS 15454s are on different subnets; ONS 15454 #1 is attached to LAN A and ONS 15454 #2 and #3 are at remote sites.

If you answer No to any of the questions in the checklist, see the "IP Troubleshooting" section on page 8-28.

Figure 8-17 IP Addressing Scenario 5



Procedure: IP Checklist for Scenario 5

- Is the IP address of the CTC workstation and the router A interface on the same subnet?
- Can the workstation running the CTC ping itself?
- Is the workstation's default gateway set to the IP address of the local router's A interface?
- Are the IP addresses of ONS 15454 #1, #2, and #3 on the different subnets?
- Are all of the IP addresses unique?
- Is the Default Router of ONS 15454 #1 set to the same IP address as the router's B interface?
- Does ONS 15454 #1 have static routes pointing to the CTC workstation?
- Does the router have host routes configured for all the remote ONS 15454s?

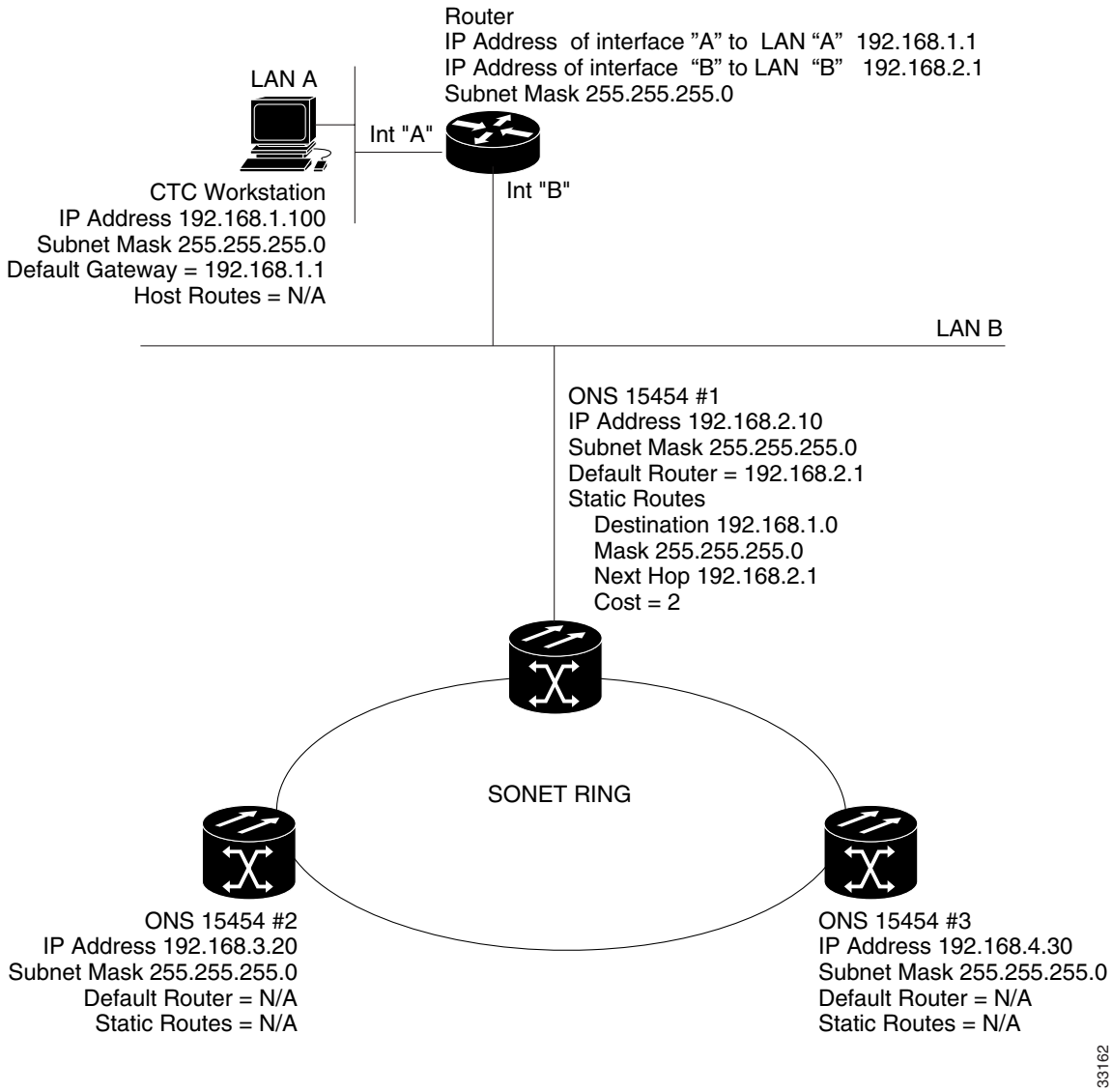
- Is there link integrity between the workstation and the hub/switch?
- Is there link integrity between the LAN wire-wrap pins on the backplane or the TCC RJ-45 ports and the hub/switch?
- Is there link integrity between the router ports and their hubs/switches?
- Is the hub/switch port for ONS 15454 #1 set for 10 Mbps half-duplex?
- Can you ping ONS 15454 #1 from the CTC workstation?
- Are the optical trunk ports on all nodes in service?
- Is the DCC enabled for all optical trunk ports that are in service?
- Can you ping the remote nodes (ONS 15454 #2 and #3) from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 and higher)?
- Do you have the Java plug-in installed (version 1.2.2 or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.4.2.6 IP Scenario 6

CTC is on a different subnet and all ONS 15454s are on the same subnet; ONS 15454 #1 attached to LAN A and ONS 15454 #2 and #3 are at remote sites.

If you answer No to any of the questions in the checklist, see the "IP Troubleshooting" section on page 8-28.

Figure 8-18 IP Addressing Scenario 6



Procedure: IP Checklist for Scenario 6

- Is the IP address of the CTC workstation and the router A interface on the same subnet?
- Can the workstation running the CTC ping itself?
- Is the workstation's default gateway set to the same IP address as the local router's A interface?

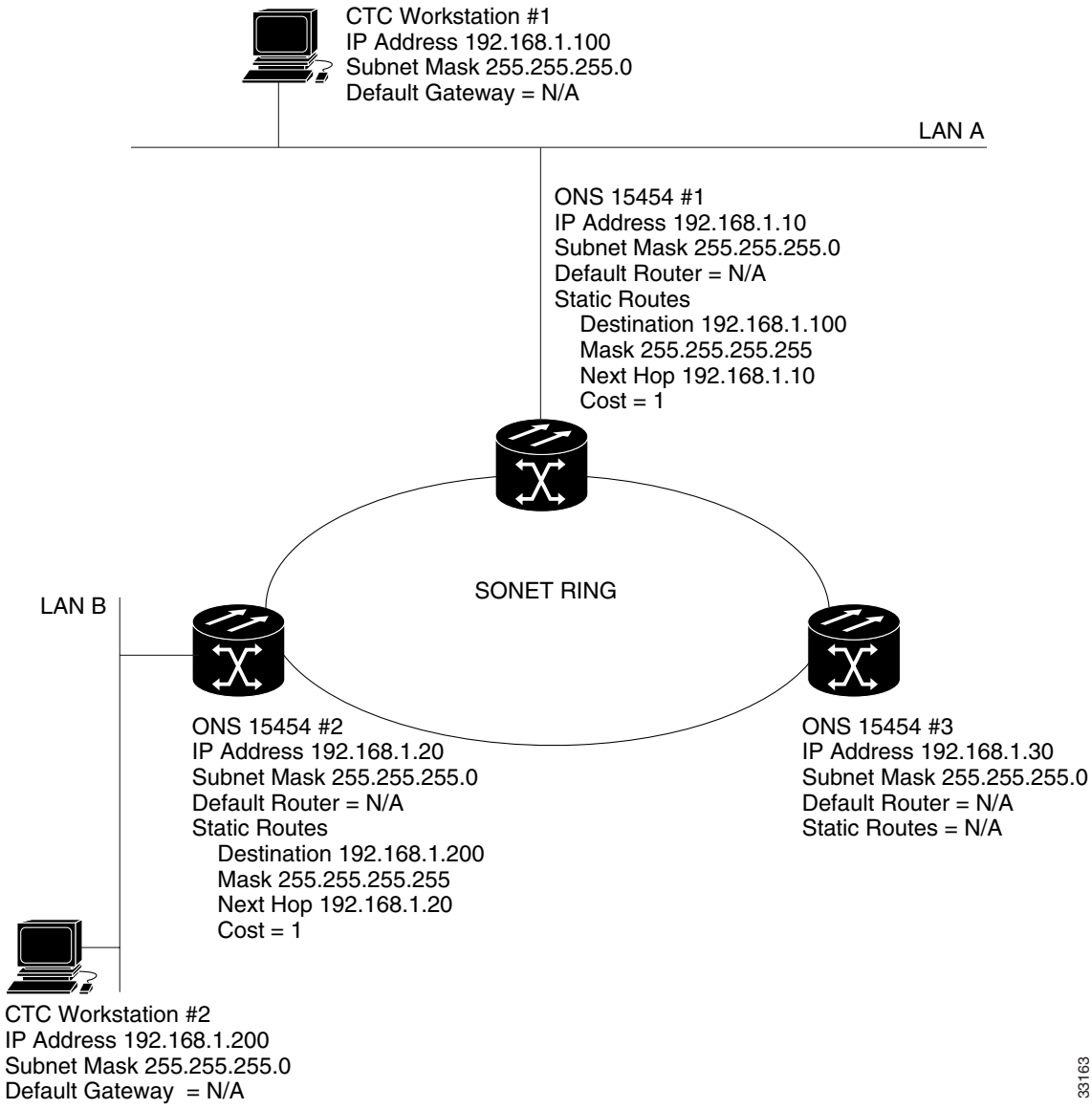
- Are the IP addresses of ONS 15454 #1, #2 and #3 on the same subnet as the local router's B interface?
- Are all of the IP addresses unique?
- Is the Default Router of ONS 15454 #1 set to the IP address of the router's B interface?
- Is there link integrity between the workstation and the hub/switch?
- Is there link integrity between the LAN wire-wrap pins on the backplane or the TCC RJ-45 port and the hub/switch?
- Is there link integrity between the router ports and their hubs/switches?
- Is the hub/switch port for ONS 15454 #1 set for 10 Mbps half-duplex?
- Can you ping ONS 15454 #1 from the CTC workstation?
- Are the optical trunk ports on all nodes in service?
- Is the DCC enabled for all optical trunk ports that are in service?
- Can you ping the remote nodes (ONS 15454 #2 and #3) from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 and higher)?
- Do you have the Java plug-in installed (version 1.2.2 or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.4.2.7 IP Scenario 7

CTC #1 and #2 and all ONS 15454s are on the same IP subnet; ONS 15454 #1 and CTC #1 are attached to LAN A. ONS 15454 #2 and CTC #2 are attached to LAN B.

If you answer No to any of the questions in the checklist, see the "IP Troubleshooting" section on page 8-28.

Figure 8-19 IP Addressing Scenario 7



Procedure: IP Checklist for Scenario 7

- Are the two CTC workstations IP addresses and all the ONS 15454s IP addresses on the same subnet?
- Are all of the IP addresses unique?
- Does ONS 15454 #1 have static routes pointing to CTC workstation #1?

- Does ONS 15454 #2 have static routes pointing to CTC workstation #2?
- Can the workstations running the CTC ping itself?
- Is there link integrity between the workstation and the hub/switch?
- Is there link integrity between the wire-wrap pins on the backplane (or the active TCC) and the hub/switch?
- Is the hub/switch port set for 10 Mbps half-duplex?
- Can you ping ONS 15454 #1 from the CTC workstation?
- Are the optical trunk ports on all nodes in service?
- Is the DCC enabled for all optical trunk ports that are in service?
- Can you ping the remote nodes (ONS 15454 #2 and #3) from the CTC workstation?
- Do you have a web browser installed (either Netscape Navigator version 4.08 or higher or Internet Explorer 4 and higher)?
- Do you have the Java plug-in installed (version 1.2.2 or higher for Microsoft Windows and version 1.2.1_03 for Sun Solaris)?
- Do you have the Java policy file installed?
- Are you using the browser to connect to the IP address of the ONS 15454?
- Can you log into the ONS 15454?

8.5 IP Troubleshooting

Look for solutions in the following section if you answered No to any of the questions in the IP scenarios checklists or encounter any of the listed IP problems.

Table 8-6 IP Troubleshooting Solutions

Problem	Solution
The workstation running the CTC cannot ping itself.	
	• Verify the IP address of your workstation.
	• If unable to ping, there is a problem with your workstation. Contact the network administrator.
There is no link integrity between the workstation and the hub/switch.	
	• Verify that you are using a straight-through Ethernet cable.
	• Verify there is a link-integrity indicator for the port on the hub/switch.
	• Change the Ethernet cable.
	• Verify that the hub/switch port is enabled.
	• Verify wire-wrap connection.
	• Contact the network administrator.
No link integrity exists between the hub/switch and the ONS 15454's LAN wire-wraps or RJ-45 port.	
	• Verify that you are using a cross-over Ethernet cable.
	• Change the Ethernet cable.
	• Verify that the hub/switch port is enabled.
	• Verify wire-wrap connection.
	• Contact the network administrator.
You do not know if the hub/switch port that connects to the ONS 15454(s) is properly set at 10 Mbps half-duplex.	
	• Contact the network administrator.
Although the workstation is capable of pinging other devices sucessfully, it cannot ping a specific ONS 15454.	
	• Verify that the IP address of ONS 15454 entered on the workstation matches the IP address displayed on the ONS 15454 LCD screen.
	• Check the routing of the workstation, router and any CTC static routes.
	• Check that optical card ports are in service and have DCC enabled.
The Java policy file was not installed or it was installed before the Java plug-in.	
	• The policy file and installation instructions are on the software CD that accompanies every ONS 15454.

Table 8-6 IP Troubleshooting Solutions

Problem	Solution
	• Call the Cisco Technical Assistance Center (TAC) at 1-877-323-7368.
You do not know whether the IP addresses of ONS 15454s #X, #Y and #Z lie on the same or different subnets?	
	• Contact the network administrator.
It is not known whether the default router entry for the ONS 15454 is set correctly to match the IP address of the router's B interface.	
	• Using the CTC, verify that the default router configuration entered on the ONS 15454 matches the verified IP address of the router's interface B.
	• See the “Static Route Provisioning” section on page 8-30.
	• Is there link integrity between the ports on the router and the hubs/switches?
	• Contact the network administrator to verify the IP address of the router’s B interface.
No link integrity exists between the router ports and the hub/switches.	
	• Contact the network administrator.
You do not know if the optical trunk ports on the ONS 15454s are in service.	
	• Verify trunk ports are in service through the CTC: Click the **Provisioning** tab. Click the **Line** subtab. Click **Status** column. Verify the ports are set to **In Service**.
You do not know if the DCC is enabled on in-service optical trunk ports.	
	• Verify that DCC is enabled through the CTC: Go to the card level view of the optical card. Click the **Provisioning** tab. Click the **Sonet DCC** subtab. Verify that the optical cards are listed.
The web browser will not connect to the ONS 15454, but connects successfully to other sites.	
	• Verify that the IP address of the ONS 15454 entered on the workstation matches the IP address displayed on the LCD screen of the ONS 15454.
	• Verify that the workstation can ping the ONS 15454.
Unable to ping remote ONS 15454s.	

Table 8-6 IP Troubleshooting Solutions

Problem	Solution
	• Verify that the IP address of ONS 15454 entered on the workstation matches the IP addresses displayed on the LCD screen of the remote ONS 15454s.
	• Check the routing of the ONS 15454 and the workstation.

8.6 Static Route Provisioning

The ONS 15454 provisions static network routes in the ONS 15454 network element through the CTC. This makes it possible to have multiple CTC sessions, with different destination IP addresses, on a network of ONS 15454s that all lie on the same subnet. For example, a Network Operations Center (NOC) may be remotely monitoring an ONS 15454 through CTC, while at the same time an on-site employee is logged into an ONS 15454 on the network with a separate CTC session. It also allows workstations to connect to ONS 15454s through routers.

To achieve CTC connectivity, interconnected ONS 15454 network elements use the SONET DCC (SDCC) for communication. Communication is accomplished using a combination of the Open Shortest Path First (OSPF) routing protocol and manually-entered static routes.

The CTC adds static route entries to the network element's routing table. This routing table information is advertised to the other ONS 15454s connected by DCCs.

Adding static route provisioning on the ONS 15454 requires configuration changes in the network elements and CTC workstations. Only one example is given below. For other typical IP addressing scenarios, see the "Common IP Addressing Scenarios with the ONS 15454" section on page 8-14. These scenarios contain additional details on router and CTC workstation setup that support the configurations described below.

Procedure: Provision Static Routing to a Router Linked Workstation

This procedure provisions a static route to connect an ONS 15454 through a router and to a CTC workstation. All networks in this example use a 24-bit subnet mask. The CTC workstation IP address is 192.168.100.20, the ONS 15454 IP address is 192.168.90.11, and the IP address of the router port on the same segment as the ONS 15454 is 192.168.90.1.

Step 1 Go to the node view of the CTC.

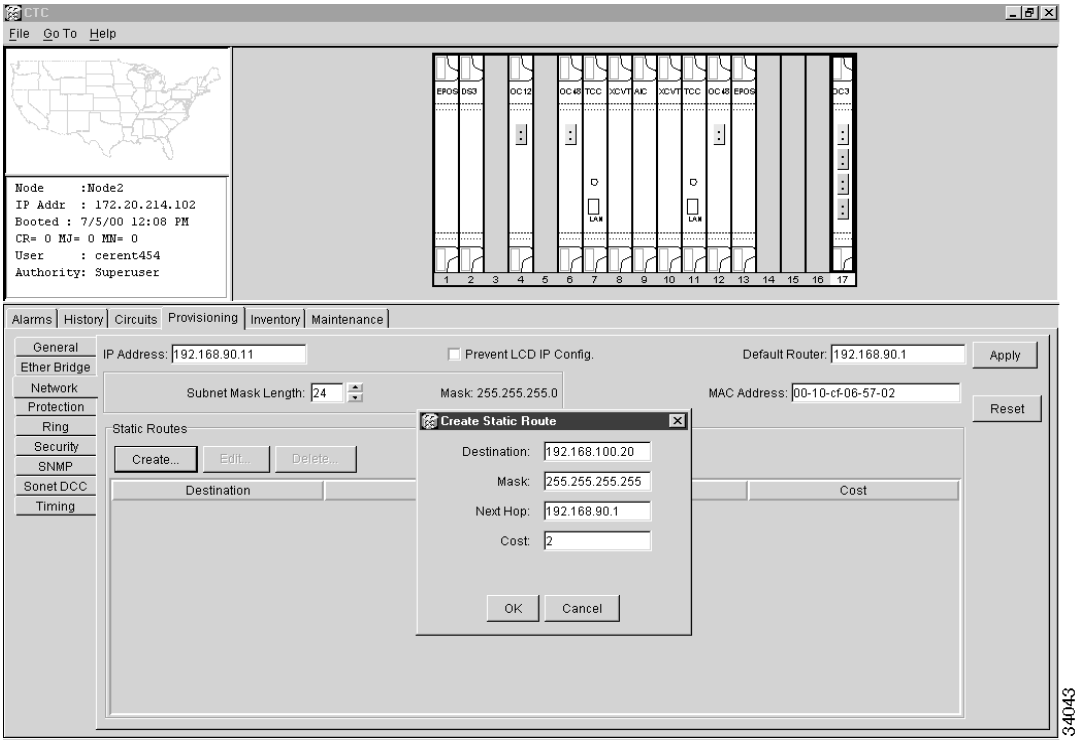
Step 2 Click the **Provisioning** tab.

Step 3 Click the **Network** tab.

Step 4 In the Static Routes pane, click **Create**.

The Create Static Route dialog opens (see Figure 8-20).

Figure 8-20 Create Static Route Window



Step 5 In the *Destination* field, enter the IP address of the workstation running the CTC (in this example, 192.168.100.20.)

Step 6 In the *Mask* field, enter a 32 bit subnet mask to designate that this is a host route (255.255.255.255).

Step 7 In the *Next Hop* field, enter the IP address of the router port (in this example, 192.168.90.1).

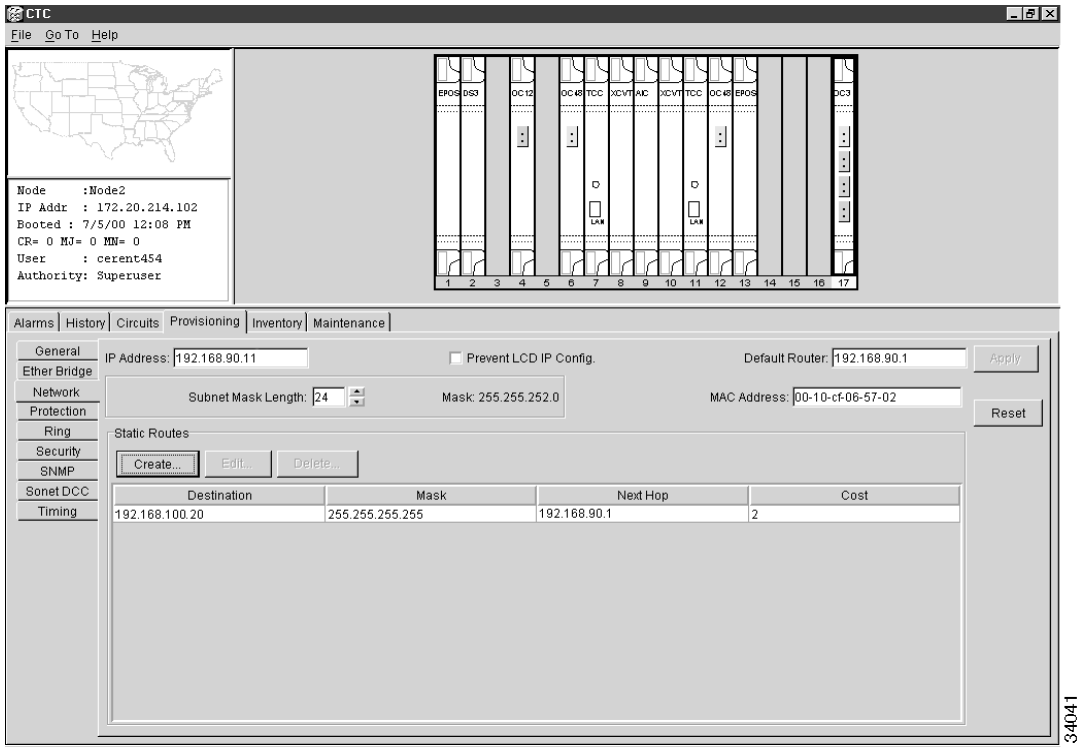
Step 8 In the *Cost* field enter the number of hops (in this example, 2). See the following note for information on determining cost.

Note To determine cost, count the number of hops between the ONS 15454 and the CTC workstation. In this example, the count is two, one hop from the ONS 15454 to the router and a second hop from the router to the CTC workstation.

Step 9 Click **OK.**

Step 10 To confirm that you have successfully completed the procedure, view the static route in the Static Route Window (show in Figure 8-21) or ping the node.

Figure 8-21 Static Route Window



Note The Default Router entry for the ONS 15454 should be the router port (in this example, 192.168.90.1).

CTC Alarms

9.1 Overview

This chapter gives an alphabetical list of Cisco Transport Controller (CTC) alarm messages for the Cisco ONS 15454 and provides procedures to correct the alarms. The same procedures apply to the corresponding TL1 alarms. The chapter also includes a matrix showing the alarms as facility alarms, equipment alarms and common equipment alarms. A list of threshold crossing events (EVTs) is also provided. Call the Technical Assistance Center (TAC) at 1-877-323-7368 for unresolved problems.

Note Some minor differences exist between TL1 error messages and CTC error messages for the ONS 15454, for example, a TL1 error message might contain a hyphen and the CTC error message might not. These discrepancies will be resolved in an upcoming release of the ONS 15454. This chapter is based on the error messages as they appear in the CTC. For a description of the CTC, see Chapter 3, "Using the Cisco Transport Controller."

Note Fan tray Liquid Crystal Displays (LCDs) running on Release 2.1 and later display alarm counts for Critical, Major, and Minor alarms on a slot or port basis. LCDs running on earlier software releases display alarm error messages on a slot or port basis, but do not provide alarm counts.

Table 9-1 Alarm Index

To clear this alarm	Go to page
AIS-L	9-5
AIS-P	9-6
AISV	9-6
APSB	9-7
APSCIMP	9-7
APSCM	9-8
APSMM	9-9
AUTORESET	9-9
BKUPMEMP	9-10
BLSROOSYNC	9-11
CARLOSS	9-12
CONCAT	9-14
CONNLOS	9-14
CONTBUS-A-X	9-15
CONTBUS-A-18	9-16
CONTBUS-B-X	9-17
CONTBUS-B-18	9-19
CTNEQPT-PBXPROT	9-20
CTNEQPT-PBXWORK	9-21
DATAFLT	9-23
DFLTK	9-24
DISCONNECTED	9-25
EOC	9-26
EQPT	9-27
EXTERNAL	9-27
FAILTOSW-PATH	9-28
FAN	9-29
FE-AIS	9-30
FE-DS1-MULTLOS	9-31
FE-DS1-SNGLLOS	9-31
FE-EQPT-FAIL-SA	9-32
FE-EQPT-NSA	9-32
FE-IDLE	9-33
FE-LOF	9-33
FE-LOS	9-34
FORCED-REQ	9-34
FRNGSYNC	9-35

Table 9-1 Alarm Index

To clear this alarm	Go to page
HITEMP	9-35
HLDOVERSYNC	9-36
IMPROPRMVL	9-36
INCOMPATIBLE-SW	9-38
INCON	9-38
LBKFACILITY	9-39
LPBKTERMINAL	9-40
LOCKOUTOFPR-RING	9-40
LOF	9-41
LOP	9-46
LOP-V	9-47
LOS	9-48
LPBKDS1FEAC	9-51
LPBKDS3FEAC	9-51
LPBKFACILITY	9-52
LPBKTERMINAL	9-53
MANRESET	9-54
MANUAL-REQ	9-55
MEA	9-56
MEM-GONE	9-57
MEM-LOW	9-58
NODEMIS	9-58
PDI-P	9-59
PLM-P	9-62
PLM-V	9-62
PWRRESTART	9-62
RAI	9-63
RCVRMISS	9-63
RFI-L	9-64
RFI-P	9-64
RFI-V	9-65
SDBER	9-66
SFBER	9-67
SQUELCH	9-68
STU	9-68
SWTOPRI	9-69
SWTOSEC	9-69
SWTOTHIRD	9-69

Table 9-1 Alarm Index

To clear this alarm	Go to page
SWTRANSFER	9-70
SYNCPRI	9-70
SYNCSEC	9-71
SYNCTHIRD	9-71
SYSBOOT	9-72
TRMTMISS	9-73
UNEQ-P	9-73
UNEQ-V	9-74

9.2 AIS-L

9.2.1 OCN

The ONS 15454 detects an Alarm Indication Signal (AIS) in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. The AIS can be caused by an incomplete circuit path, for example, when the port on the reporting node is in service but a node upstream on the circuit does not have its port inservice. The upstream node often reports a loss of signal (LOS) or has an OCN port out of service. The AIS-L clears when the primary alarm on the upstream node is cleared. However, the upstream node might not report anything to 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.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Check upstream nodes and equipment for alarms, especially for LOS and an out-of-service port.

Step 2 Clear the upstream alarms.

Step 3 The AIS-L clears.

9.2.2 EC-1 (AIS-L)

The ONS 15454 detects an Alarm Indication Signal (AIS) in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. The AIS can be caused by an incomplete circuit path, for example, 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 OCN port out of service. The AIS-L clears when the primary alarm on the upstream node is cleared. However, the upstream node might not report anything to 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.

- Active: Minor, Service affecting
- Standby: Minor, Service affecting

Recommended Action

Step 1 Check upstream nodes and equipment for alarms, especially LOS or an out-of-service port.

Step 2 Clear the upstream alarms.

The AIS-L clears.

9.3 AIS-P

9.3.1 I/O

The ONS 15454 detects an Alarm Indication Signal (AIS) in the SONET overhead. This alarm is secondary to another alarm occurring simultaneously in an upstream node. The AIS can be caused by an incomplete circuit path, for example, 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 OCN port out of service. The AIS-P clears when the primary alarm on the upstream node is cleared. However, the upstream node might not report anything to indicate it is at fault.

AIS-P occurs in the node that terminates a path. The path layer is 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. 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 15454, often perform the origination and termination tasks of the SONET payload.

An AIS-P error message on the ONS 15454 indicates that the node reporting the AIS-P is the terminating node on that path segment. If there is a node between the failing node and the terminating node, the middle node reports an AIS-L.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Check upstream nodes and equipment for alarms, especially LOS and out of service port.

Step 2 Clear the upstream alarms.

The AIS-P clears.

9.4 AISV

9.4.1 DS1, DS3XM-6

The ONS 15454 detects an Alarm Indication Signal (AIS) in the SONET overhead. This alarm is secondary to another alarm occurring in an upstream node. The AIS can be caused by an incomplete circuit path, for example, 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 is commonly reporting a loss of signal (LOS) or has an OCN port out of service. The AIS-V clears when the primary alarm is cleared. The upstream node with the port out of service might not report anything to indicate it is at fault.

An AIS-V indicates that an upstream failure has occurred at the VT layer. The VT, or electrical layer, occurs when the SONET signal is broken down into an electrical signal, for example when an OC-48 signal comes into an OC-48 optical card contained in the ONS 15454. If this OC-48 signal is demultiplexed by the ONS 15454, and one of the channels separated from the OC-48 is then cross-connected into the DS-1 card in the ONS 15454, the DS-1 card 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 optical card.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Check upstream nodes and equipment for alarms, especially for LOS or an out-of-service port.

Step 2 Correct the upstream alarms.

The AIS-V clears.

9.5 APSB

9.5.1 OCN

Explanation Line terminating equipment detects protection switching byte failure in the incoming Automatic Protection Switching (APS) signal. A protection switching byte defect occurs when an inconsistent APS byte or invalid code is detected.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Verify the APS setting on the upstream equipment.

9.6 APSCIMP

9.6.1 OC-12 and OC-48 in BLSR

Explanation An Improper SONET Automatic Protect Switch code alarm indicates invalid K bytes. 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.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

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 15454. 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:

(a) Using CTC, log into a node on the ring.

(b) Click the **Provisioning** tab and the **Ring** subtab.

(c) Record the ring ID number.

(d) 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**.

9.7 APSCM

9.7.1 OCN in linear mode

Explanation The Automatic Protection Switching channel mismatch alarm occurs when the ONS 15454 expects a working channel but receives a protection channel, or vice versa. In many cases, the working and protection channels are crossed. For example, the protection and working receivers are crossed but the protection and working transmitters are not crossed. APSCM does not occur when both channels switch over, and it only occurs in a linear configuration.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 Verify that the working-card channel fibers connect directly to the working-card channel fibers of the adjoining node's.

Step 2 Verify that the protection-card channel fibers connect directly to the working-card channel fibers of the adjoining node.

9.8 APSMM

9.8.1 OCN in linear mode

Explanation An Automatic Protection Switching Mode Mismatch failure occurs when there is a mismatch of the protection switching schemes at the two ends of the span. If one end is provisioned for bidirectional switching, 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 results. This alarm occurs in a linear configuration.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 For the reporting ONS 15454, display CTC and click the **Provisioning** tab and the **Protection** subtab.

Step 2 Select the 1+1 protection group configured for the OCn cards.

This is the protection group optically connected to the far-end.

Step 3 Record whether the Bidirectional switching box is checked.

Step 4 Log into the far-end node and verify the OCn 1+1 protection group.

This is the protection group optically connected to the near end.

Step 5 Verify that the Bidirectional switching box matches the condition of the box recorded in Step 3. If not, change it to match.

Step 6 Click **Apply**.

9.9 AUTORESET

9.9.1 Any Card

Explanation The card is warm rebooting automatically. An AUTORESET can occur when you change an IP address or perform any other operation that causes an automatic card-level reboot.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

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

Step 1 Check for additional alarms that might have triggered an automatic reset.

Step 2 If the card automatically resets often with no apparent cause, replace it with a new card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the database.

9.10 BKUPMEMP

9.10.1 TCC+

Explanation The BKUPMEMP alarm refers to a problem with the TCC+ card's flash memory. The alarm occurs when the TCC 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 cylic redundancy checking (CRC), which is a method to check for errors in data transmitted to the TCC+.

The BLKUPMEMP alarm will also raise the alarm EQPT alarm. In this instance of an EQPT alarm, following the Reccomended Action for the BKUPMEM alarm, which will also clear the EQPT alarm.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Verify that both TCC+ cards are powered and enabled by confirming a lighted green ACT/STBY LED on the TCC+ card.

Step 2 Reset the Active TCC+ card to make the standby TCC+ card active.

(a) In CTC go to the node view of the node.

(b) Position the cursor over the active TCC+ card slot.

(c) Right click and choose **RESET CARD**.

Step 3 If the alarm clears, reseat the old TCC+ and allow it to boot up completely.

Step 4 Do a second reset, this time on the newly active TCC+ card to make the recently reseated standby TCC+ card active.

(a) In CTC go to the node view of the node.

(b) Position the cursor over the active TCC+ card slot.

(c) Right click and choose **RESET CARD**.

Step 5 If the alarm reappears after you perform the switch, replace the TCC+.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.11 BLSROOSYNC

Explanation The BLSR Out Of Sync alarm occurs when the mapping table needs updating. To clear the alarm, a new ring map must be created and accepted. Before you create a new ring map, complete Steps 1–4.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Prior to accepting a new mapping table, verify that each node has a unique node ID number:

(a) Log into a node on the ring.

(b) Click the **Provisioning** tab and the **Ring** subtab.

(c) Record the Node ID number.

(d) Repeat Steps a – c for all nodes in the ring.

(e) If two nodes have the same node ID number, change one node's ID number.

(f) Click **Apply**.

Step 2 Verify that each node has a ring ID that matches the other node ring IDs:

(a) Log into a node on the ring.

(b) Click the **Provisioning** tab and the **Ring** subtab.

(c) Record the Ring ID number.

(d) Repeat Steps a – b for all nodes in the ring.

(e) If a node has a ring ID number that does not match the other nodes, change one node's ID.

(f) Click **Apply**.

Step 3 Verify correct configuration of the east port and west port optical fibers:

(a) Click the **Provisioning** tab and the **Ring** subtab.

(b) Verify the east port and west port pattern for all network elements.

Clockwise ring fiber should be optically connected starting east to west.
Counter-clockwise ring fiber should be optically connected starting west to east.

Step 4 If items have been changed, click **Apply**.

The BLSR Ring Map Change screen appears.

Step 5 Click **Yes** to accept the Ring Map.

Step 6 If the alarm does not clear, check the ring map for each ONS 15454 in the network and verify that each node is visible to the other nodes.

(a) Under the node view, click the **Provisioning** tab and the **SONET DCC** subtab.

(b) Click **Create**.

(c) Click the optical card that links to the adjacent network element.

(d) Click **OK**.

Step 7 If alarms are raised when the Data Communications Channels (DCCs) are turned on, follow the troubleshooting procedure for the EOC alarm on page 9-26.

Step 8 If the alarm still does not clear, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Step 9

9.12 CARLOSS

9.12.1 E100T-12, E1000-2

Explanation A carrier loss on the LAN is the data equivalent of an optical LOS (loss of signal). The Ethernet card has lost its link and is not receiving any signal, even an invalid one. The most common causes of this alarm are a disconnected cable or an improperly installed Ethernet card.

CARLOSS also occurs after the restoration of a node's database. In this instance, the alarm will clear in approximately 30 seconds after spanning tree protection is reestablished.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify that the cable is properly connected and attached to the correct port.

Step 1 Check that the transmitting device is operational. If not, troubleshoot the device.

Step 2 Using a test set, determine that a valid signal is coming into the Ethernet port.

Step 3 If a valid Ethernet signal is not present and the transmitting device is operational, check that the Ethernet wiring is intact and correct.

Step 4 If a valid Ethernet signal is present, physically reseat the Ethernet card.

Step 5 If the alarm does not clear, replace the Ethernet card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Step 6 If a CARLOSS alarm repeatedly appears and clears, examine the layout of your particular network to determine whether 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 set up 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 another vendors' equipment sits between ONS 15454s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 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 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 15454 and card that host the Ethernet circuit at the other end of the Ethernet manual cross connect.

(e) Log into the ONS 15454 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 will connect the Ethernet card to an OC-N card on the same node.

(i) Determine whether 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. Refer to the Cisco Installation and Operations Guide for procedures to provision Ethernet manual cross connects.

9.13 CONCAT

9.13.1 OCN

Explanation The STS Concatenation error alarm occurs when the transmitted STSc circuit is smaller than the provisioned STSc and causes a mismatch of the circuit type on the concatenation facility. For example, an STS-3c or STS-1 is sent across a circuit provisioned for STS-12c.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Using the CTC, log into the network element.

Step 2 Check that the circuit is correctly provisioned.

Step 3 Check that the circuit source is correctly provisioned.

9.14 CONNLOS

9.14.1 OC-12 and OC-48 in BLSR

Explanation An APS channel connection loss is occurring in the BLSR.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify that both TCC cards are powered and enabled by confirming a lighted green ACT/STBY LED on the TCC card.

Step 2 Verify that both OCN cards are powered and enabled by confirming a lighted green ACT/STBY LED on the OCN card.

Step 3 Reset the Active TCC card to make the standby TCC card active.

(a) In CTC go to the node view of the node.

(b) Position the cursor over the active TCC card slot.

(c) Right click and choose **RESET CARD**.

Step 4 If the alarm clears, reseat the old TCC and allow it to boot up completely.

Step 5 Do a second Reset, this time on the newly active TCC card to make the recently reseated standby TCC card active.

(a) In CTC go to the node view of the node.

(b) Position the cursor over the active TCC card slot.

(c) Right click and choose **RESET CARD**.

Step 6 If the alarm reappears after you perform the switch, replace the TCC.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.15 CONTBUS-A-*X*

9.15.1 Any Card

Explanation The TCC card in Slot 7 has lost communication with the card in Slot *X*. Cards require frequent communication with the TCC because the TCC performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET DCC termination, and system fault detection for the ONS 15454. The TCC also ensures that the system maintains Telcordia timing requirements.

This alarm might appear briefly when the ONS 15454 switches to the standby TCC card. In this instance, the alarm clears after the cards establish communication with the new primary TCC card. In cases where the alarm persists, the problem lies in the physical communication path from the TCC card to the reporting card. The physical communication path includes the TCC card, the card in Slot *X,* and the ONS 15454 backplane.

- Active: Major, Non-service affecting
- Standby: Minor, Non-service affecting

Note If *X* equals 18, then see CONTBUS-A-18 listed below.

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

Recommended Action

Step 1 Make sure the slot *X* card is physically present and note the card type.

Step 2 Click the **Inventory** tab to reveal the provisioned card type.

If the actual card type and the provisioned card type do not match, follow the procedure for the MEA alarm on page 9-56.

Step 3 If this slot is the only one reporting the alarm, perform a software reset of the I/O card.

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm (slot *X*).

(c) Right click and choose **RESET CARD**.

Step 4 If the software reset does not clear the alarm, physically reseat the reporting card.

Step 5 If all I/O cards report this alarm, perform a software reset of the active TCC.

(a) Go to the node view.

(b) Position the CTC cursor over the active TCC card slot.

(c) Right click to **RESET CARD**.

Step 6 If the software reset does not clear the alarm, physically reseat the TCC card.

Step 7 If the alarm still does not clear, replace the TCC card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.16 CONTBUS-A-18

9.16.1 TCC, TCC+

Explanation The main processor on the TCC/TCC+ card in Slot 7 has lost communication with the coprocessor on the second TCC card in Slot 11. The problem lies in the physical path of communication from the TCC card to the reporting card. The physical path of communication includes the two TCC cards and the ONS 15454 backplane.

The Timing Communications and Control (TCC) card ensures that the system maintains Telcordia timing requirements.

- Active: Major, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Position the CTC cursor over the TCC card in Slot 7.

Step 2 Right click the mouse to reveal a menu.

Step 3 Click **RESET CARD** from the menu to make the standby TCC in Slot 11 the active TCC and clear the alarm.

Step 4 Wait approximately 2 minutes for the TCC in Slot 7 to reset as the standby TCC.

Step 5 Position the CTC cursor over the TCC card in Slot 7.

Step 6 Right click the mouse to reveal a menu.

Step 7 Click **RESET CARD** from the menu to make the standby TCC in Slot 7 the active TCC.

Step 8 If the alarm reappears when the TCC in slot 7 reestablishes as the active TCC, the TCC card in Slot 7 is defective and must be replaced.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.17 CONTBUS-B-*X*

9.17.1 Any Card

Explanation The TCC card in Slot 11 has lost communication with the card in Slot *X*. Cards require frequent communication with the TCC because the TCC performs system initialization, provisioning, alarm reporting, maintenance, diagnostics, IP address detection/resolution, SONET DCC termination, and system fault detection for the ONS 15454. The TCC also ensures that the system maintains Telcordia timing requirements.

This alarm might appear briefly when the ONS 15454 switches over to the second TCC card. In this instance, the alarm clears after the cards establish communication with the new primary TCC card. In cases where the alarm persists, the problem lies in the physical communication path from the TCC card to the reporting card. The physical communication path includes the TCC card. The card in Slot *X* and the ONS 15454 backplane.

- Active: Major, Non-service affecting
- Standby: Minor, Non-service affecting

Note If *X* equals 18, then see CONTBUS-B-18 listed below.

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

Recommended Action

Step 1 Make sure the Slot *X* card is physically present and that it matches the type of card identified in that slot on the CTC.

Step 2 If this is the only slot reporting the alarm, perform a software reset of the I/O card:

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm (Slot *X)*.

(c) Right click the mouse and select **RESET CARD** to do a software reset.

Step 3 If the software reset does not clear the alarm, physically reseat the reporting card.

Step 4 If all cards, with the possible exception of the active TCC, report this alarm, perform a software reset of the active TCC.

(a) Go to the node view.

(b) Position the CTC cursor over the active TCC card slot.

(c) Select **RESET CARD**.

Step 5 If the software reset does not clear the card, then physically reseat the TCC card.

Step 6 If the alarm still does not clear, then replace the TCC card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.18 CONTBUS-B-18

9.18.1 TCC/TCC+

Explanation The processor on the TCC/TCC+ card in Slot 11 has lost communication with the processor on the TCC card in Slot 7. The problem lies in the physical communication path from the TCC card to the reporting card. The physical communication path includes the two cards and the ONS 15454 backplane.

The Timing Communications and Control (TCC) card also ensures that the system maintains Telcordia timing requirements.

- Active: Major, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Position the CTC cursor over the TCC card in Slot 11.

Step 2 Click the right button on the mouse to reveal a menu.

Step 3 Click **RESET CARD** from the menu to make the TCC in Slot 11 the active TCC and clear the alarm.

Step 4 Wait approximately 2 minutes for the TCC in Slot 7 to reset as the standby TCC.

Step 5 Position the CTC cursor over the TCC card in Slot 7.

Step 6 Select **RESET CARD** to again make the TCC in Slot 11 the active TCC.

Step 7 If the alarm reappears when the TCC in Slot 11 is reestablished as the active TCC, the TCC card in Slot 11 is defective and must be replaced.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

the CTC database.

9.19 CTNEQPT-PB*X*PROT

9.19.1 I/O, XC/XCVT

Explanation This alarm indicates a failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot *X*. The XC/XCVT card and the reporting card are no longer communicating through the backplane. The problem lies in either the XC/XCVT card, the reporting I/O card, or the backplane.

Note *X* is equal to the number of the card slot for numbers 1–6. If *X* is 7 or greater, then add 5 to *X* to determine the actual card slot. For example, CTNEQPT-PB7PROT signifies Slot 12, not Slot 7.

Note If all I/O cards show this alarm, physically reseat the standby XC/XCVT card. If this fails to clear the alarm, replace the standby XC/XCVT card. Do not physically reseat an active XC/XCVT card. This might disrupt traffic.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Perform a software reset on the standby XC/XCVT card.

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm.

(c) Right click to select **RESET CARD**.

Step 2 If the alarm persists, physically reseat the standby XC/XCVT card.

Step 3 If the reporting I/O card is active:

(a) Do a manual switch to move traffic away from the card.

At the node view, click the **Maintenance** tab.

Click the **Protection** tab.

Double-click the protection group that contains the reporting card.

Click the Protect/Standby card of that protection group.

At **Operation** click the drop-down arrow.

Click **FORCE_SWITCH_TO_PROTECT**.

Click **APPLY**.

Click **YES** at the confirmation dialog.

(b) Perform a software reset on the reporting card.

Go to the node view.

Position the CTC cursor over the slot reporting the alarm.

Right click to select **RESET CARD**.

(c) If the alarm persists, physically reseat the reporting card.

Step 4 If the reporting I/O card is protect:

(a) Perform a software reset on the reporting card.

Go to the node view.

Position the CTC cursor over the slot reporting the alarm.

Right click to select **RESET CARD**.

(b) If the alarm persists, physically reseat the reporting card.

Step 5 If the alarm persists, replace the standby XC/XCVT card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Step 6 If the alarm persists, replace the reporting I/O card.

9.20 CTNEQPT-PB*X*WORK

9.20.1 I/O, XC/XCVT

Explanation The main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot *X* failed. The XC/XCVT card and the reporting card are no longer communicating through the backplane. The problem lies in the XC/XCVT card, the reporting I/O card, or the backplane.

Note *X* is equal to the number of the card slot for numbers 1–6. If *X* is 7 or greater, add 5 to *X* to determine the actual card slot. For example, CTNEQPT-PB7WORK signifies Slot 12, not Slot 7.

Note If all I/O cards show this alarm, do a side-switch on the active XC/XCVT card (shown in Step 1) and physically reseat this XC/XCVT card. If this fails to clear the alarm, replace the XC/XCVT card. Do not physically reseat an active XC/XCVT card; this might disrupt traffic.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Do a side-switch from the active XC/XCVT card to the protect XC/XCVT card.

(a) From the node view, click the **Maintenance** tab.

(b) Click the **XC Cards** subtab.

(c) At **Slot Operation** for the active card, click the drop-down arrow.

(d) Click **FORCE**.

(e) Click **Apply**.

Step 2 Perform a software reset on the reporting card.

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm.

(c) Right click to select **RESET CARD**.

Step 3 If the alarm persists, physically reseat the standby XC/XCVT card to perform a hard reset.

Step 4 If the reporting I/O card is active:

(a) Do a manual switch to move traffic away from the card.

At the node view, click the **Maintenance** tab.

Click the **Protection** subtab.

Double-click the protection group that contains the reporting card.

Click the Protect/Standby card of that protection group.

At **Operation** click the drop-down arrow.

Click **FORCE_SWITCH_TO_PROTECT**.

Click **APPLY**.

Click **YES** at the confirmation dialog.

(b) Perform a software reset on the reporting card.

Go to the node view.

Position the CTC cursor over the slot reporting the alarm.

Right click to select **RESET CARD**.

(c) If the alarm persists, physically reseat the reporting card.

Step 5 If the reporting I/O card is protect:

(a) Perform a software reset on the reporting card.

Go to the node view.

Position the CTC cursor over the slot reporting the alarm.

Right click to select **RESET CARD**.

(b) If the alarm persists, physically reseat the reporting card.

Step 6 If the alarm persists, replace the XC/XCVT card. Make sure the card has been side-switched from active to standby (Step 1) before replacement.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Step 7 If the alarm persists, replace the reporting I/O card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.21 DATAFLT

9.21.1 TCC/TCC+

Explanation The database has exceeded the capacity of the flash memory on the TCC/TCC+.

- Active: Critical, Non-service affecting
- Standby: Minor, Non-service affecting

Caution When the system reboots, the last configuration entered is not saved.

Recommended Action

Call the Technical Assistance Center (TAC) at 1-877-323-7368.

9.22 DFLTK

9.22.1 OCN

Explanation The Default K Byte Received alarm occurs when a BLSR is not properly configured, for example, when a four-node BLSR has one node configured as UPSR. A node in a UPSR or linear 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 DFLTK is often similar to troubleshooting for BLSROOSYNC.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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.

Recommended Action

Step 1 Prior to accepting a new mapping table, verify that each node has a unique node ID number.

(a) Log into a node on the ring.

(b) Click the **Provisioning** tab and the **Ring** subtab.

(c) Record the node ID number.

(d) Repeat Steps a – c for all nodes in the ring.

(e) If two nodes have the same node ID number, change one node's ID number so that each node has a unique node ID.

(f) Click **Apply**.

Step 2 Verify that each node has a ring ID that matches the other node ring IDs.

(a) Log into a node on the ring.

(b) Click the **Provisioning** tab and the **Ring** subtab.

(c) Record the Ring ID number.

(d) Repeat Steps a – c for all nodes in the ring.

(e) If a node has a ring ID number that does not match, change the node ID number of that node so that all nodes have the same *Ring ID*.

(f) Click **Apply**.

Step 3 Verify correct configuration of east port and west port optical fibers.

(a) Click the **Provisioning** tab and the **Ring** subtab.

(b) Verify the east port and west port pattern for all network elements (see Note).

Note Clockwise ring fiber should be optically connected starting east to west. Counter-clockwise ring fiber should be optically connected starting west to east.

Step 4 If items have changed, click **Apply.** The BLSR Ring Map Change screen appears.

Step 5 Click **Yes** to accept the Ring Map.

Step 6 If the alarm does not clear, check the ring map for each ONS 15454 in the network and verify that each node is visible to the other nodes.

(a) At the node view, click the **Provisioning** tab and the **SONET DCC** subtab.

(b) Click **Create**.

(c) Select the optical card that links to the adjacent network element.

(d) Click **OK**.

Step 7 If alarms are raised when the DCCs are turned on, follow the troubleshooting procedure for the EOC alarm on page 9-26.

Step 8 If the alarm still does not clear, call the Technical Assistance Center (TAC) at 1-877-323-7368.

9.23 DISCONNECTED

Explanation The ONS 15454 and the CTC do not have a TCP/IP connection. The problem lies in this connection, usually a LAN problem, and not the CTC or the ONS 15454.

Recommended Action

Step 1 Check the LAN connection to your PC.

Step 2 Verify connectivity by performing a Ping to the ONS 15454 reporting the alarm.

(a) If you are using a Microsoft Windows operating system, from the Start Menu select Command Prompt.

(b) If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and select Terminal.

(c) For both the Sun and Microsoft operating systems, at the prompt type ping [ONS 15454 IP address] for example, `ping 192.1.0.2`.

If the workstation has connectivity to the ONS 15454, it displays a `reply from [IP Address]` after the ping. If the workstation does not have connectivity, a `Request timed out` message displays.

Step 3 If the ping is successful, an active TCP/IP connection exists. Restart the CTC.

Step 4 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.

9.24 EOC

9.24.1 OCN

Explanation The ONS 15454 has lost its Data Communications Channel (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 15454 uses the DCC on the SONET section layer (SDCC) to communicate network management information.

- Active: Major, Non-service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 If there is also a LOS alarm reported, first resolve the LOS alarm by following the troubleshooting procedure given for that alarm.

Step 1 On the node reporting the alarm, check the physical connections of the optic fibers configured to carry DCC traffic.

Step 2 Verify that both ends of the fiber span have in-service ports.

Step 3 Verify that both ends of the fibers have DCC provisioned.

(a) Under the node view, click the **Provisioning** tab and the **SONET DCC** subtab.

(b) If the slot and port are listed under **SDCC Terminations**, the DCC is provisioned.

(c) If the slot and port are not listed under the SDCC Terminations, click **Create**.

(d) Click the optical card that links to the adjacent network element.

(e) Click **OK**.

(f) Repeat Steps a – e at the adjacent nodes.

Step 4 Verify that the OCN port is active and in service.

Step 5 With a test set, check for signal failure on fiber terminations.

Step 6 Measure power levels to verify that the budget loss is within the parameters of the receiver.

Step 7 Make sure fiber connectors are securely fastened and properly terminated.

Step 8 Restart the active TCC.

Step 9 Select the **Provisioning** tab and the **SONET DCC** subtab.

Step 10 Delete and recreate the offending SDCC termination.

Step 11 Verify that both ends of the SDCC have been recreated at the optical ports.

9.25 EQPT

9.25.1 Any Card

Explanation An equipment failure (EQPT) alarm indicates that a hardware failure has occurred on the reporting card.

If the EQPT alarm occurs with a BLKUPMEMP alarm, follow the Reccomended Action for the BKUPMEM alarm on the "BKUPMEMP" section on page 9-10. This procedure will also clear the EQPT alarm.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Perform a software reset on the reporting card.

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm.

(c) Right click **RESET CARD**.

Step 2 If the software reset fails to clear the alarm, physically reseat the card.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.26 EXTERNAL

9.26.1 AIC

Explanation A facility alarm is detected external to the node because an environmental alarm is present; for example, a door is open or flooding has occurred.

- Active: Major, Service affecting

- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Open the AIC maintenance screen to gather further information about this alarm.

Step 2 Perform your standard operating procedure for this environmental condition.

9.27 FAILTOSW-PATH

9.27.1 UPSR

Explanation There is a switch failure between the working path and 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.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Check that a lockout is not set on the UPSR.

(a) Go to the network view.

(b) Right click the span (the line between the nodes).

(c) Click **Circuits**.

(d) Under Switch State, confirm that Clear appears.

(e) If Clear appears perform Steps a–d at the next span.

(f) If Clear does not appear, click the arrow next to Switch all UPSR-circuits away.

(g) Click **Clear**.

(h) Click **Apply**.

(i) Click **Yes** at the Confirm UPSR Switch Are You Sure? dialog.

(j) Click **OK** at the next dialog box.

Step 2 Check fiber connections to make sure they are securely fastened and intact.

Step 3 Make sure OCN cards are active and in service.

Step 4 Verify that the Protect OCN card paired with the reporting Active OCN card is the same type and inservice.

Step 5 Do a manual switch to move traffic away from the reporting active card.

(a) At the node view, click the **Maintenance** tab.

(b) Click the **Protection** subtab.

(c) Double-click the protection group that contains the reporting card.

(d) Click the Protect/Standby card of that protection group.

(e) At **Operation** click the drop-down arrow.

(f) Click **MANUAL_SWITCH_TO_PROTECT**.

(g) Click **APPLY**.

(h) Click **YES** at the confirmation dialog.

Step 6 If the traffic does not switch over, try restarting the protect cards through the Maintenance tab.

Step 7 Attempt another manual switch after the protect cards have booted up completely.

Step 8 If you are still unable to perform a switch, try reseating the protect card.

Step 9 Attempt another manual switch.

Step 10 If the alarm persists, replace the protect card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Step 11 Call the Technical Assistance Center (TAC) at 1-877-323-7368 for unresolved problems.

9.28 FAN

Explanation The fan alarm indicates a problem with the fan tray assembly. When the fan is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range. The ONS 15454 fan tray contains six fans, and the unit is designed to cool properly with only five of the six fans operating. However, when only five of the six fans are operational, the fan tray still needs replacement. Six operational fans give the ONS 15454 additional protection against overheating.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Check the condition of the filter to see if it needs replacement. See the "Air Filter Inspection" section on page 10-1 for instructions on locating and accessing the filter.

Step 2 If the filter is clean, take the fan tray assembly out of the ONS 15454.

Step 3 Reinsert the fan tray making sure the back of the fan tray connects to the rear of the ONS 15454.

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, call the Technical Assistance Center (TAC) at 1-877-323-7368. The Alarm Interface Board (AIP) might have blown a fuse. If the fuse did blow, TAC will determine if the board needs replacement.

9.29 FE-AIS

9.29.1 DS3XM-6

Explanation The far-end DS-3 node is reporting an Alarm Indication Signal (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 the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both the alarms clear when the main alarm clears.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot an FE alarm determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from an DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.30 FE-DS1-MULTLOS

9.30.1 DS3XM-6

Explanation Multiple inputs detect a loss on the far end. The prefix FE in an alarm message 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 alarms clear when the main alarm clears.

Explanation

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from an DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Troubleshoot the main alarm.

This clears the FE alarm.

9.31 FE-DS1-SNGLLOS

9.31.1 DS3XM-6

Explanation One of the DS-1 inputs on the far end detects a LOS. The prefix FE in an alarm message 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 alarms clear when the main alarm clears.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of node 1 might link to the main AIS alarm from a DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.32 FE-EQPT-FAIL-SA

9.32.1 DS3XM-6

Explanation A far-end DS-3 equipment failure is occurring. The prefix FE in an alarm message 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 alarms clear when the main alarm clears.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from a DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.33 FE-EQPT-NSA

9.33.1 DS3XM-6

Explanation A non-service affecting equipment failure is detected in the far-end DS-3. The prefix FE in an alarm message means that the main alarm is occurring at the far-end node, not the node reporting the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from a DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.34 FE-IDLE

9.34.1 DS3XM-6

Explanation A far-end node detects an idle DS-3 signal. The prefix FE in an alarm message means that the main alarm is occurring at the far-end node, not the node reporting the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarms will clear when the main alarm clears.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from a DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.35 FE-LOF

9.35.1 DS3XM-6

Explanation A far-end node reports a DS-3 loss of frame (LOF). The prefix FE in an alarm message means that the main alarm is occurring at the far-end node, not the node reporting the FE alarm. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Explanation

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot an FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from a DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.36 FE-LOS

9.36.1 DS3XM-6

Explanation The far-end node reports a DS-3 loss of signal (LOS). The prefix FE in an alarm message means that 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 alarms clear when the main alarm clears.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS alarm from the DS3XM-6 card in Slot 12 of Node 1 might link to the main AIS alarm from a DS3XM-6 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE alarm.

Step 3 Clear the main alarm.

This clears the FE alarm.

9.37 FORCED-REQ

9.37.1 OCN in linear mode

Explanation This alarm means that 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. 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.

- Active: Minor, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

To clear the force command:

Step 1 Click the **Maintenance** tab.

Step 2 Click the **Protection** tab for a card or span switch. Click the **Ring** tab to clear a ring switch.

Step 3 Click the drop-down arrow at **Operation**.

Step 4 Click **Clear**.

Step 5 Click **Apply**.

9.38 FRNGSYNC

Explanation The reporting ONS 15454 is in free run synchronization mode. Either external timing sources have been disabled so the node is using its internal clock, or the ONS 15454 has lost its designated BITS timing source.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 If the ONS 15454 is configured to operate from its own internal clock, disregard this alarm.

Step 2 If the ONS 15454 is configured to operate from 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.

9.39 HITEMP

Explanation The temperature of the ONS 15454 is above 50 degrees Celsius.

- Active: Critical, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Check the temperature of the ONS 15454 (shown on the front panel LCD).

Step 2 Check that the temperature of the room is not abnormally high.

Step 3 Make sure that nothing prevents the fan tray assembly from passing air through the ONS 15454.

Step 4 Make sure blank faceplates fill the ONS 15454 empty slots. Blank faceplates aid airflow.

Step 5 Check the condition of the filter to see if it needs replacement.

Step 6 If the filter is clean, take the fan tray assembly out of the ONS 15454.

Step 7 Reinsert the fan tray, making sure the back of the fan tray connects to the rear of the ONS 15454.

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.

9.40 HLDOVERSYNC

Explanation The Holdover Synchronization alarm occurs when primary/secondary reference timing is lost. This might occur when line coding on the timing input is different than the configuration on the ONS 15454. It also occurs after the selection of a new node reference clock.This alarm indicates that the ONS 15454 has gone into holdover and is using the ONS 15454 internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Check for additional alarms that relate to timing.

Step 2 Reestablish a primary and secondary timing source according to local site practice.

9.41 IMPROPRMVL

9.41.1 Any Card

Explanation A card was physically removed from its slot before the card was deleted in the CTC. The card does not have to be in service to cause this alarm, it only has to be recognized by the CTC and the TCC card. This alarm will not appear if you delete the card from the CTC before you physically remove it from the node.

Note The CTC gives the user approximately 15 seconds to physically remove the card before the CTC begins a card reboot.

Caution Do not pull a rebooting card. If the CTC begins to reboot a card before you can remove it, allow the card to finish rebooting. After the card reboots, delete the card in the CTC again and physically remove it before the card begins to reboot.

- Active: Critical, Service affecting

- Standby: Minor, Non-service affecting

Recommended Action

Step 1 At the node view, right click the card reporting the IMPROPRMVL.

Step 2 Choose **Delete**.

Step 3 If the card is in service, has a circuit mapped to it, is paired in a working protection scheme, and has DCC communications turned on or is used as a timing reference, the CTC will not allow the card to be deleted.

Step 4 If the card is in service, then take the facility out of service.

Caution Prior to taking the facility out of service, ensure that there is no live traffic on the facility.

(a) Double click the reporting card to display a card level view.

(b) Click the **Provisioning** tab.

(c) Click the **Status** of any in-service ports.

(d) Choose **Out of Service** to take the ports out of service.

Step 5 If a circuit has been mapped to the card, delete the circuit.

Caution Prior to deleting the circuit, ensure that there is no live traffic on the circuit.

(a) On the node view, click the **Circuits** tab.

(b) Select the applicable circuit. (The circuit that connects to the reporting card.)

(c) Click **Delete**.

Step 6 If the card is paired in a protection scheme, delete the protection group.

(a) Click the **Provisioning** tab and the **Protection** subtab.

(b) Select the protection group of the reporting card.

(c) Click **Delete.**

Step 7 If the card is provisioned for DCC, delete the DCC provisioning.

(a) Click the **Provisioning** tab and the **SONET DCC** subtab.

(b) Click the slots and ports listed in **SDCC Terminations**.

(c) Click **Delete**.

(d) Click **Yes** when a dialog appears.

Step 8 If the card is used as a timing reference, change the timing reference.

(a) Click the **Provisioning** tab and the **Timing** subtab.

(b) Click the arrow next to the *Ref-1* field.

(c) Change the field from the listed OCn card to Internal Clock.

(d) Click **Apply**.

Step 9 Right click the card reporting the IMPROPRMVL.

Step 10 Choose **Delete**.

9.42 INCOMPATIBLE-SW

Explanation The CTC software and the TCC software are incompatible. This can happen when the TCC software is upgraded but the PC has not yet upgraded the compatible CTC.jar file. It can also happen when the CTC logs into a node with compatible software, but encounters another node in the network that has a newer version of TCC software.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Exit the current CTC session and completely close down the browser.

Step 2 Start the browser.

Step 3 Type the ONS 15454 IP address of the node that reported the alarm. This might be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into the CTC. (The browser will download the.jar file from the CTC.)

9.43 INCON

9.43.1 OC-12 and OC-48 in BLSR

Explanation An inconsistent automatic protection switching (APS) code is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454, 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.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Look for other alarms, especially LOS, LOF or AIS. Clearing these alarms clears the INCON alarm.

Step 2 If an INCON alarm occurs with no other alarms, call the Technical Assistance Center (TAC) at 1-877-323-7368.

9.44 LANOVERFLOW

9.44.1 TCC/TCC+

Explanation The LAN overflow alarm indicates that there is a broadcast storm on the network management LAN. The network management LAN connects to the TCC/TCC+ card, and this connection is temporarily disabled to prevent data packets from flooding the port of the TCC/TCC+ card. When the connection is disabled, the ONS periodically checks the LAN to determine when the broadcast storm clears. When the broadcast storm clears, the TCC connection is reinstated.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

This problem is external to the ONS node. Troubleshoot the TCC/TCC+ connected network management LAN for a broadcast storm.

9.45 LBKFACILITY

9.45.1 OCN

Explanation 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 narrow down the source of the problem.

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. Users provision loopbacks through the CTC.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To remove the loopback alarm, open the reporting card by double clicking on the card or right clicking on the card in the CTC and selecting **Open** from the list of options.

Step 2 Click the **Maintenance** tab.

Step 3 Select the Loopback Type column and select **None** from the menu.

Step 4 Click **Apply**.

9.46 LPBKTERMINAL

9.46.1 OCN

Explanation A software terminal loopback is active for a port on the reporting card.

Loopback is a commonly used troubleshooting technique. A signal is sent 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.

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 can provision loopbacks through the CTC.

Caution The CTC permits loopbacks on an in-service circuit. This operation is service affecting.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To remove the loopback alarm, open the reporting card by double clicking on the card in the CTC or right clicking on the card in the CTC and selecting **Open** from the list of options.

Step 2 Click the **Maintenance** menu tab.

Step 3 Select the Loopback Type column and select **None** from the menu.

Step 4 Click **Apply**.

9.47 LOCKOUTOFPR-RING

9.47.1 OC-12 and OC-48 in BLSR

Explanation The BLSR will not allow a protection channel switch. One of the BLSR nodes has a LOCKOUT SPAN set. Clearing this LOCKOUT SPAN allows the protection channel switch.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Remove the lockout set on the BLSR.

(a) Log into one of the BLSR nodes.

(b) Click the **Maintenance** tab.

(c) Click the **Ring** tab.

(d) Click the arrow next to **East Operation**.

(e) Click **Clear**.

(f) Click the arrow next to **West Operation**.

(g) Click **Clear**.

(h) Click **Apply**.

(i) Click **Yes** at the Confirm BLSR Switch Are You Sure? dialog.

(j) Click **OK** at the next dialog box.

Step 2 Repeat Step 1 at each node in the BLSR until the alarm clears.

9.48 LOF

9.48.1 DS3XM-6

Explanation A port on the DS3XM-6 card has a loss of frame (LOF) condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the data being received.

When a LOF appears on the DS3XM-6 card, the transmitting equipment might have framing set to a format different from the receiving ONS 15454, or there might be no framing contained in the signal.

Explanation

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Verify that the line framing and line coding match between the DS3XM-6 port reporting the alarm and the signal source:

Step 1 In CTC, note the slot and port reporting the alarm.

Step 2 Find the coding and framing formats of the signal source for the port reporting the alarm. You might need to contact your Network Administrator for this information.

Step 3 Go to the card-level view of the reporting card.

Step 4 Click the **Provisioning** tab.

Step 5 Verify that the reporting port's Line Type matches the signal source's Line Type.

Step 6 If the signal source line type does not match the reporting port, click the Line Type to reveal a menu.

Step 7 Choose the matching type.

Step 8 Click **Apply**.

Step 9 Verify that the reporting port's Line Coding matches the signal source's Line Type.

Step 10 Slide the replacement card into the slot along the guide rails.

9.48.2 TCC/TCC+ (LOF)

Explanation A port on the TCC BITS input detects a loss of frame (LOF) on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 has lost frame delineation in the data being received.

Note The procedure assumes that the BITS timing reference signal has been functioning properly. It also assumes the alarm is not appearing during system turn-up.

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

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Verify that the BITS input and the TCC have matching line framing and line coding.

(a) In the CTC, note the slot and port reporting the alarm.

(b) 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 unit itself.

(c) Click the **Provisioning** tab and the **Timing** tab to display the General Timing Screen.

(d) Verify that Coding matches the coding of the BITS timing source (either B8ZS or AMI).

(e) If the coding does not match, click **Coding** to reveal the menu. Choose the appropriate coding.

(f) Verify that Framing matches the framing of the BITS timing source (either ESF or SF[D4]).

(g) If the Framing does not match, click **Framing** to reveal the menu. Choose the appropriate framing.

Note 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 coding and framing of the ONS 15454 match the coding and framing of the external BITS timing source, replace the TCC card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.48.3 DS1 (LOF)

Explanation A port on the DS-1 card has a loss of frame (LOF) condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the data being received.

When a LOF appears on the DS-1 card, the transmitting equipment might have its framing set to a format different from the receiving ONS 15454.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify that the line framing and line coding match between the DS-1 card and the signal source.

(a) In the CTC, note the slot and port reporting the alarm.

(b) Find the coding and framing formats of the DS-1 signal source for the card reporting the alarm. You might need to contact your Network Administrator for this information.

(c) Go to the card level view of the reporting card.

(d) Click the **Provisioning** tab.

(e) Verify that the reporting port's Line Type matches the signal source's Line Type.

(f) If the signal source line type does not match the reporting port, click **Line Type** to reveal the menu and choose the matching type.

(g) Verify that the reporting port's Line Coding matches the signal source's Line Type.

(h) If the signal source line coding does not match the reporting port, click **Port Line Coding** to reveal the menu. Choose the matching type.

Note 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.

Step 2 If the alarm does not clear when the coding and framing of the ONS 15454 match the coding and framing of the DS-1 source, replace the DS-1 card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.48.4 OCN (LOF)

Explanation A port on the reporting card has a loss of frame (LOF) condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the data being received. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

LOF on an OCN card is sometimes an indication that the OCN card reporting the alarm might be expecting a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

Explanation

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Do a manual switch to move traffic away from the card.

(a) At the node view, click the **Maintenance** tab.

(b) Click the **Protection** tab.

(c) Click the protection group that contains the reporting card.

(d) Click the Protect/Standby card of that protection group.

(e) At **Operation** click the drop-down arrow.

(f) Click **FORCE_SWITCH_TO_PROTECT**.

(g) Click **APPLY**.

(h) Click **YES** at the confirmation dialog.

Step 2 If you still receive the LOF alarm, ensure that the source of the input line rate matches the input line rate of the optical receiver.

(a) Verify that the reporting optical card matches the originating optical card, for example, an OC-3 card matches an OC-3 card.

(b) If the optical cards match, use a test set to measure the input line rate to verify that the input line rate of the source matches the input line rate of the optical receiver.

Step 3 Verify physical connections between the optical ports.

Step 4 Verify that the optical connectors are clean.

Step 5 Verify that the receive levels are in the specified range.

Step 6 If the receive levels are not in the specified range, go to the receive side and attenuate the receive input.

Step 7 Verify that the optical port of the upstream node is inservice.

9.48.5 EC-1 (LOF)

Explanation This alarm occurs when a port on the reporting card has a Loss of Frame (LOF) condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the data being received. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Do a manual switch to move traffic away from the card.

(a) At the node view, click the **Maintenance** tab.

(b) Click the **Protection** tab.

(c) Double-click the protection group that contains the reporting card.

(d) Click the Protect/Standby card of that protection group.

(e) At **Operation** click the drop-down arrow.

(f) Click **FORCE_SWITCH_TO_PROTECT**.

(g) Click **APPLY**.

Step 2 Click **YES** at the confirmation dialog.

Note If you do not have a protect card for the reporting card, on the reporting card create a new port and a new circuit to achieve the same effect.

Step 3 If you still receive the LOF alarm, check to make sure the input line rate source matches the input line rate of the optical receiver.

(a) Verify that the reporting optical card line rate matches the originating optical card line rate, for example, an EC-1 line rate matches an EC-1 line rate.

(b) If the optical card line rates are still in question, use an optical test set to measure the input line rate.

(c) If the received dbm levels are not in the specified range, go to the receive side and attenuate the receive input.

Step 4 Verify physical connections for the ports.

9.49 LOP

9.49.1 I/O

Explanation This alarm indicates a Loss of Pointer (LOP) condition. LOP occurs when valid H1/H2 pointer bytes are missing from the SONET overhead. The H1/H2 pointer bytes are monitored by receiving equipment to locate the SONET payload. The LOP alarm indicates that invalid pointer values came in on eight, nine, or ten frames. The alarm clears when three consecutive valid pointers are received.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Do a manual switch to move traffic away from the card.

(a) At the node view, click the **Maintenance** tab.

(b) Click the **Protection** tab.

(c) Double-click the protection group that contains the reporting card.

(d) Click the Protect/Standby card of that protection group.

(e) At **Operation** click the drop-down arrow.

(f) Click **FORCE_SWITCH_TO_PROTECT**.

(g) Click **APPLY**.

Step 2 Click **YES** at the confirmation dialog.

Step 3 Perform a software reset on the reporting card.

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm.

(c) Right click to select **RESET CARD**.

Step 4 If the alarm persists, the problem is at the far-end node. Verify the cabling and physical connections at the far-end card.

Step 5 Switch from the far-end working card to the far-end protect card:

(a) At the node view, click the **Maintenance** tab.

(b) Click the **Protection** tab.

(c) Double-click the protection group that contains the far-end working card.

(d) Click the Protect/Standby card of that protection group.

(e) At **Operation** click the drop-down arrow.

(f) Click **FORCE_SWITCH_TO_PROTECT**.

(g) Click **APPLY**.

Step 6 If the alarm persists, replace the far-end card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Step 7 Do a soft reset on the far-end card.

Step 8 Verify the cabling and physical connections on the reporting card.

9.50 LOP-V

9.50.1 DS3XM-6, DS1

Explanation This alarm indicates a loss of pointer (LOP) condition. LOP occurs when valid H1/H2 pointer bytes are missing from the SONET overhead. The H1/H2 pointer bytes are monitored by receiving equipment to locate the SONET payload. The LOP alarm indicates that invalid pointer values came in on eight, nine, or ten frames. The alarm clears when three consecutive valid pointers are received.

LOP-V indicates a loss of pointer at the VT level. The VT layer, or electrical layer, occurs when the SONET signal is broken down into an electrical signal, for example, when an OC-48 signal comes into an OC-48 optical card. This OC-48 signal is demultiplexed by the ONS 15454 and one of the channels separated from the OC-48 is cross connected into the DS3XM-6 card. This DS3XM-6 card reports the LOS-V alarm.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify the cabling and physical connections on the reporting card.

Step 2 Do a manual switch to move traffic away from the card.

(a) At the node view, click the **Maintenance** tab.

(b) Click the **Protection** tab.

(c) Double-click the protection group that contains the reporting card.

(d) Click the Protect/Standby card of that protection group.

(e) At **Operation** click the drop-down arrow.

(f) Click **FORCE_SWITCH_TO_PROTECT**.

(g) Click **APPLY**.

(h) Click **YES** at the confirmation dialog.

Step 3 Perform a software reset on the reporting card.

(a) Go to the node view.

(b) Position the CTC cursor over the slot reporting the alarm.

(c) Right click to select **RESET CARD**.

Step 4 If the alarm persists, the problem is at the far-end node. Verify the cabling and physical connections at the far-end card.

Step 5 Do a soft reset on the far-end card.

Step 6 Switch from the far-end working card to the far-end protect card.

9.51 LOS

9.51.1 DS3, DS3XM-6, DS1

Explanation This alarm indicates a loss of signal (LOS) for a DS-3, DS-1 or DS3XM-6 card.

Loss of signal occurs when the port on the card is inservice but no signal is being received. The cabling might not be hooked up correctly to the card or a signal might not be present on the line.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify cabling continuity to the port.

Step 2 Verify that the proper port is inservice.

Step 3 Use a test set to verify that a valid signal is 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 Look for another alarm that might identify the source of the problem.

Step 6 Replace the reporting card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Step 7 If there is a valid signal, replace the connector on the Backplane Interface Connector (BIC).

9.51.2 OCN (LOS)

Explanation A port on the reporting OCN card has a loss of signal (LOS) condition. A LOS occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. The loss of signal indicates that the upstream transmitter has failed. If an OCN LOS alarm is not accompanied by additional alarms, a fiber break is often the cause of the alarm.The condition clears when two consecutive valid frames are received.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 Verify fiber continuity to the port.

Step 2 Verify that the proper 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 Verify that the power level of the optical signal is within the optical card's receiver specifications. Each individual card section in Chapter 2 lists the receiver specifications for that card.

Step 5 Ensure that the optical transmits and receives are connected properly.

Step 6 Replace the OCN card.

9.51.3 EC-1 (LOS)

Explanation A port on the reporting card has a loss of signal (LOS) condition. A loss of signal occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. The loss of signal indicates that the upstream transmitter has failed. The condition clears when two consecutive valid frames are received.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify cabling continuity to the port.

Step 2 Verify that the proper port is in service.

Step 3 Use a test set to verify that there is a valid signal on the line.

Test the line as close to the receiving card as possible.

Step 4 Ensure that the transmit and receive cables from the DSX panel to your equipment are properly connected.

Step 5 If there is a valid signal, replace the connector on the backplane.

Step 6 Try another port on the card.

Step 7 Replace the EC-1 card.

9.52 LPBKDS1FEAC

9.52.1 DS3XM-6

Explanation A DS-1 loopback signal is received from the far-end node due to a Far-End Alarm and Control (FEAC) command. A FEAC command is often used when troubleshooting 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.

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 can provision loopbacks through the CTC.

Caution The CTC permits loopbacks on an in-service circuit. This operation is service affecting.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Note This is an informational alarm.

9.53 LPBKDS3FEAC

9.53.1 DS3XM-6

Explanation A DS-3 loopback signal is received from the far-end node due to a Far-End Alarm and Control (FEAC) command. A FEAC command is often used when troubleshooting 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 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.

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 can provision loopbacks through the CTC.

Caution The CTC permits loopbacks on an in-service circuit. This operation is service affecting.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Note This is an informational alarm.

9.54 LPBKFACILITY

9.54.1 DS3, DS3XM-6

Explanation A software facility loopback is active for a DS3/DS3XM-6 port.

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 isolate the source of the problem.

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 can provision loopbacks through the CTC.

Caution The CTC permits loopbacks to be performed on an in-service circuit. This operation is service affecting.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To remove the loopback alarm, double-click the reporting card.

Step 2 Click the **Maintenance** tab.

Step 3 Select the Loopback Type column.

Step 4 Select **None**.

Step 5 Click **Apply**.

9.54.2 DS1 (LPBKFACILITY)

Explanation A software facility loopback is active for a DS-1 port.

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 isolate the source of the problem.

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 can provision loopbacks through the CTC.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To remove the loopback alarm, double click the reporting card.

Step 2 Click the **Maintenance** tab.

Step 3 Select the Loopback Type column.

Step 4 Select **None**.

Step 5 Click **Apply**.

9.55 LPBKTERMINAL

9.55.1 DS3, DS3XM-6

Explanation A terminal loopback is active for a DS3/DS3XM-6 port.

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.

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 can provision loopbacks through the CTC.

Caution The CTC permits loopbacks on an in-service circuit. This operation is service affecting.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To remove the loopback alarm, double click or right click the card in the CTC and select **Open** to open the reporting card.

Step 2 Click the **Maintenance** tab.

Step 3 Select the Loopback Type column.

Step 4 Select **None**.

Step 5 Click **Apply**.

9.55.2 DS1 (LPBKTERMINAL)

Explanation A software terminal loopback is active for a DS-1 port.

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 isolate the source of the problem.

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 can provision loopbacks through the CTC.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 To remove the loopback alarm, double click the reporting card.

The reporting card opens.

Step 2 Click the **Maintenance** tab.

Step 3 Select the Loopback Type column.

Step 4 Select **None** from the menu.

Step 5 Click **Apply**.

9.56 MANRESET

9.56.1 Any Card

Explanation The user performed a manual system reset. This alarm appears when a user right clicks on a card and chooses **Reset**. Resets performed during a software upgrade also prompt the alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Note This is an informational alarm.

9.57 MANUAL-REQ

9.57.1 OCN (Not OC3)

Explanation The Manual Switch Request on Facility/Equipment alarm occurs when a user initiates a manual switch request on a BLSR. BLSR reverts to the original working path if the manual switch is cleared. Clearing the manual switch also clears the MANUAL-REQ alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Note This is an informational alarm.

Recommended Action

Step 1 To clear the manual switch and the MANUAL-REQ alarm on the BLSR:

(a) Log into one of the BLSR nodes.

(b) Click the **Maintenance** tab.

(c) Click the **Ring** tab.

(d) Click the arrow next to **East Operation**.

(e) Click **Clear**.

(f) Click the arrow next to **West Operation**.

(g) Click **Clear**.

(h) Click **Apply**.

(i) Click **Yes** at the Confirm BLSR Switch Are You Sure? dialog box.

(j) Click **OK** at the next dialog box.

Step 2 Repeat Step 1 at each node in the BLSR until the alarm clears.

9.57.2 XC/XCVT (MANUAL-REQ)

Explanation The Manual Switch Request on Facility/Equipment alarm occurs when a user initiates a manual switch request on an XC/XCVT. Clearing the manual switch will not cause the XC/XCVT card to revert back to the pre-switch card. Clearing the manual switch clears the MANUAL-REQ alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Note This is an informational alarm.

Recommended Action

Clear the manual switch and the MANUAL-REQ alarm on the XC/XCVT.

Step 1 Click the **Maintenance** tab.

Step 2 Click the **XC Cards** tab.

Step 3 Click the arrow next to **Slot 8 Operation**.

Step 4 Click **Clear**.

Step 5 Click the arrow next to **Slot 10 Operation**.

Step 6 Click **Clear**.

Step 7 Click **Apply**.

9.58 MEA

9.58.1 XC, I/O

Explanation The Mismatch Between Entity/Equipment Type and Provisioned Attributes alarm occurs when the physical card inserted in a slot does not match the card type provisioned for that slot through the CTC. The alarm clears when the provisioned card type and the actual card type match.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Physically verify the type of card that sits in the reported slot.

Step 2 Click the **Inventory** tab to reveal the provisioned card type.

Step 3 Determine which card the CTC identifies as residing in the reported slot.

Step 4 If the card depicted by the CTC is the card type desired, physically insert the type of card provisioned for that slot.

Step 5 If the card that physically occupies the slot is correct card type, put the cursor over the card in the CTC.

Step 6 Right click and select **Delete Card**.

The card that physically occupies the slot reboots and CTC automatically provisions the card type into that slot.

Step 7 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 the CTC will not allow the card to be deleted.

Step 8 If the card is in-service, take the facility out of service.

Caution Prior to taking the facility out of service, ensure that no live traffic exists on the facility.

(a) Double-click the reporting card to display a card level view.

(b) Click the **Provisioning** tab.

(c) Click the Status of any in service ports.

(d) Select Out of Service to take the ports out of service.

Step 9 If a circuit has been mapped to the card, delete the circuit.

Caution Prior to deleting the circuit, ensure that no live traffic exists on the circuit.

(a) On the node view, click the **Circuits** tab.

(b) Select the applicable circuit. (The one that connects to the reporting card.)

(c) Click **Delete**.

Step 10 If the card is paired in a protection scheme, delete the protection group.

(a) Click the **Provisioning** tab and the **Protection** tab.

(b) Select the protection group of the reporting card.

(c) Click **Delete.**

Step 11 Right click the card reporting the IMPROPRMVL.

Step 12 Choose **Delete**.

9.59 MEM-GONE

9.59.1 TCC/TCC+

Explanation The Memory Gone alarm occurs when software operations exceed the memory capacity of the TCC/TCC+ card. The CTC will not function properly until this alarm clears. The alarm clears when additional memory becomes available.

- Active: Critical, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 If the card reporting the alarm is a TCC, replace the TCC with a TCC+, see the "TCC Card to TCC+ Card Upgrade" section on page 10-11.

Step 2 If the card reporting the alarm is a TCC+, call the Technical Assistance Center (TAC) at 1-877-323-7368.

9.60 MEM-LOW

9.60.1 TCC/TCC+

Explanation The Memory Low alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC/TCC+ card. The CTC still functions, but will cease to function if additional CTC operations further tax the memory. The alarm clears when additional memory becomes available.

- Active: Major, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 If the card reporting the alarm is a TCC, replace the TCC with a TCC+, see the "TCC Card to TCC+ Card Upgrade" section on page 10-11.

Step 2 If the card reporting the alarm is a TCC+, call the Technical Assistance Center (TAC) at 1-877-323-7368.

9.61 NODEMIS

9.61.1 OC-12 and OC-48 in BLSR

Explanation The Node Id Mismatch failure alarm indicates two identical node IDs in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Find the nodes with identical node IDs.

(a) Log into a node on the ring.

(b) Click the **Provisioning** tab and the **Ring** tab.

(c) Record the Node ID number.

(d) Repeat Steps a – c for all nodes in the ring.

Step 2 If two nodes have the identical node ID number, change the node ID number of one node.

(a) Log into a node that has an identical node ID number.

(b) Click the **Provisioning** tab and the **Ring** tab.

(c) Change the number in *Node ID* to a unique number between 0 and 15.

(d) Click **Apply**.

9.62 NOT-AUTHENTICATED

Explanation This alarm indicates that the username and password entered do not match the information stored in the TCC. All ONS 15454s must have the same username and password created in order to access every ONS 15454 in the network. Users can also be locked out of certain ONS 15454s on a network if their username and password is not created on that specific ONS 15454.

Recommended Action For initial logon to the ONS 15454, type the user name `CISCO15` and click **Login** (no password is required).

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Ensure that you are using a correct username and password.

Step 2 Ensure that an account exists on the TCC.

9.63 PDI-P

9.63.1 DS3, DS3XM-6, DS1

Explanation A Payload Defect Indication Path alarm means that a signal label mismatch failure is occurring. A signal label mismatch failure (SLMF) is caused when an invalid C2 byte occurs in the SONET path overhead. 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. For example, ATM cells and fiber distributed data interface (FDDI) data frames can be interwoven and carried together.

The ONS 15454 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, clearing the PDI-P alarm clears the AIS alarm. PDI-P might also occur during an upgrade, but usually clears itself and is not a valid alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

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 up to 10 minutes for the ONS 15454 to fully initialize.

Step 2 Verify that the signal source to the DSN card is reporting the alarm.

Step 3 If traffic is being affected, delete and recreate the circuit.

Caution Deleting a circuit might affect traffic.

Step 4 Check the far-end OCN card that provides STS payload to the DSN card.

Step 5 Verify the cross-connect between the OCN card and the DSN card.

Step 6 Clean the far-end OCN 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 7 Replace OCN/DSN cards.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.64 PLM-P

9.64.1 DS3, DS3XM-6, DS1

Explanation A Payload Label Mismatch Path means that a signal label mismatch failure is occurring. A signal label mismatch failure (SLMF) occurs when an invalid C2 byte occurs in the SONET path overhead. 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. For example, ATM cells and fiber distributed data interface (FDDI) data frames can be interwoven and carried together.

The ONS 15454 encounters a SLMF when the payload, such as an ATM, 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. PDI-P might also occur during an upgrade, but usually clears itself and is not a valid alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 Verify that all circuits terminating in the reporting card are active.

(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 up to 10 minutes for the ONS 15454 to fully initialize.

Step 2 Verify that the signal source to the DSN card is reporting the alarm.

Step 3 If traffic is being affected, delete and recreate the circuit.

Caution Deleting a circuit might affect traffic.

Step 4 Check the far-end OCN card that provides STS payload to the DSN card.

Step 5 Verify the cross-connect between the OCN card and the DSN card.

Step 6 Clean the far-end OCN 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 OCN/DSN cards.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.65 PLM-V

9.65.1 DS1, DS3XM-6

Explanation A VT Payload Label Mismatch indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Verify that your signal source matches the signal allowed by the I/O card, for example, the I/O card does not allow VT6 or VT9 mapping.

Step 2 Verify that the SONET VT path originator, which can be found through circuit provisioning, is sending the correct VT label value.

9.66 PWRRESTART

Explanation A power fail restart is a cold boot of the reporting card. This alarm might occur when you hard reset (physically remove and insert) a card, power up an ONS 15454, or replace a card.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Note This is an informational alarm.

Step 1 If the alarm does not clear after the card reboots, physically reseat the card.

Step 2 If the alarm still fails to clear, replace the card.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.67 RAI

9.67.1 DS3XM-6

Explanation Remote Alarm Indication signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other.

RAI on the DS3XM-6 card indicates that far-end signalling is receiving a DS-3 AIS.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Troubleshoot the far-end DS-3 node for AIS.

9.68 RCVRMISS

9.68.1 DS1

Explanation Facility termination equipment detects a missing receive cable on the DS-1 port or a possible mismatch of backplane equipment, for example, an SMB connector or a BNC connector is connected to a DS-1 card.

Note DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Check that the device attached to the DS-1 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.

9.69 RFI-L

9.69.1 OCN, EC-1

Explanation The ONS 15454 detects a remote fault indication (RFI) in the SONET overhead because a fault exists in another network element. 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 and its functions include multiplexing and synchronization.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Log into the far-end node from the reporting ONS 15454.

Step 2 Check for alarms in the far-end node, especially UNEQ-P or UNEQ-V.

Step 3 Resolve alarms in the far-end node.

9.70 RFI-P

9.70.1 DS3, DS3XM-6, DS1, E100-T12, E1000-2

Explanation A Remote Failure Indication Path alarm occurs when the ONS 15454 detects a remote fault indication (RFI) in the SONET overhead because a fault exists in another network element. 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 might 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 15454, often perform the origination and termination tasks of the SONET payload.

An RFI-P error message on the ONS 15454 indicates that the node reporting the RFI-P is the terminating node on that path segment. If there is a node between the failing node and the terminating node, this node reports an RFI-L.

- Active: Minor, Non-service affecting

- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Verify that the ports are enabled and in service on the reporting ONS 15454.

Step 2 To find the path failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3 Log into the far-end node from the reporting ONS 15454.

Step 4 Check for alarms in the far-end node, especially UNEQ-P or UNEQ-V.

Step 5 Resolve alarms in the far-end node.

9.71 RFI-V

9.71.1 DS3XM-6, DS1

Explanation The ONS 15454 detects a remote fault indication (RFI) because a fault exists in another network element. 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 occurs when the SONET signal is broken down into an electrical signal, for example when an OC-48 signal comes into an OC-48 optical card contained in the ONS 15454. If this OC-48 signal is demultiplexed and one of the channels separated from the OC-48 is cross connected into the DS-1 card in the ONS 15454, the DS-1 card reports an RFI-V alarm.

An AIS-V error message on the electrical card is accompanied by an AIS-P error message on the cross-connected optical card.

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

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Check connectors on the Electrical Interface Assembly (EIA) or balun and make sure they are securely fastened and connected to the proper slot/port.

Step 2 Verify that the DS1/DS3XM-6 card is active and in service.

Step 3 Check the signal source for errors.

Step 4 Log into the far-end node from the reporting ONS 15454.

Step 5 Check for alarms in the far-end node, especially UNEQ-P or UNEQ-V.

Step 6 Resolve alarms in the far-end node.

9.72 SDBER

9.72.1 OCN

Explanation The SDBER alarm indicates that the quality of the signal is so poor that the bit error rate (BER) on the incoming OCN line has passed the signal degrade threshold. The ONS 15454 sets the BER threshold for SDBER from 10^{-9} to 10^{-5}. Signal degrade is defined by Telcordia as a "soft failure" condition. SDBER and SFBER (Signal Fail Bit Error Rate) both monitor the incoming bit error rate and are similar alarms, but SDBER is triggered at a lower bit error rate than SFBER. SDBER causes the card to switch from working to protect. The ONS 15454 detects SDBER on the STS level, not the VT level.

SDBER causes a switch from the working card to the protect card at either the path or line level. The SDBER 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.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 With an optical test set, measure the power level of the line to ensure it is within guidelines.

Step 2 Verify that optical receive levels are within the acceptable range.

Step 3 Clean the fibers at both ends for a line signal degrade, but not for a path signal degrade. (If you do not know whether the signal degrade is path or line, clean the fibers.)

(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 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 OCN line might be failing and require replacement.

9.73 SFBER

9.73.1 OCN

Explanation The quality of the signal is so poor that the bit error rate (BER) on the incoming OCN line passed the signal failure threshold. The ONS 15454 sets the BER threshold for SFBER from 10^{-5} to 10^{-3}. Signal failure is defined by Telcordia as a "hard failure" condition. SDBER and SFBER both monitor the incoming bit error rate and are similar alarms, but SFBER is triggered at a higher bit error rate than SDBER. The ONS 15454 detects SFBER on the STS level, not the VT level.

SFBER causes a switchover from working to protect at either the path or line level. The SFBER 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.

- Active: Critical, Service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 Using an optical test set, measure the power level of the line and ensure it is within the guidelines.

Step 2 Verify that optical receive levels are within the acceptable range.

Step 3 Clean the fibers at both ends for a line signal degrade, but not for a path signal degrade. (If you do not know whether the signal degrade is path or line, clean the fibers.)

(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 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 OCN line might be failing and need replacement.

9.74 SQUELCH

Explanation The Squelch alarm occurs in a BLSR when a a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts. The isolation or failure of the node will disable 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 will also appear on all nodes in the ring, except the isolated node.

- Active: Major, Service affecting

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

Warning 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.

Recommended Action

Step 1 Determine the isolated node:

(a) Go to Network View.

(b) The grayed out node with red spans will be 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's receiver specifications. Each individual card section in Chapter 2 lists the receiver specifications for that card.

Step 6 Ensure that the optical transmits and receives are connected properly.

Step 7 Replace the OCN card.

9.75 STU

Explanation The Synchronization Traceability Unknown alarm means the reporting node is timed to a reference that does not support Sync Status Messaging (SSM). 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 select the highest quality timing reference and to avoid timing loops. The ONS 15454 supports SSM.

This alarm indicates that the reporting node has SSM enabled but the timing source does not support SSM, or the reporting node does not have SSM enabled but the timing source supports SSM.

- Active: Minor, Non-service affecting

- Standby: Minor, Non-service affecting

Recommended Action

Step 1 From the node view, click the **Provisioning** tab and the **Timing** tab.

Step 2 If **Sync Messaging** is checked, uncheck the box.

Step 3 If **Sync Messaging** is unchecked, check the box.

Step 4 Click **Apply**.

9.76 SWTOPRI

Explanation The ONS 15454 has switched to the primary timing source (reference 1). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

- Active: Not reportable, Non-service affecting
- Standby: Not reportable, Non-service affecting

Note This is an informational alarm.

9.77 SWTOSEC

Explanation The ONS 15454 has switched to the secondary timing source (reference 2). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

- Active: Not reportable, Non-service affecting
- Standby: Not reportable, Non-service affecting

Recommended Action

Troubleshoot alarms related to failures of the primary timing source, such as SYNCPRI.

9.78 SWTOTHIRD

Explanation The ONS 15454 has switched to the third timing source (reference 3). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

- Active: Not reportable, Non-service affecting
- Standby: Not reportable, Non-service affecting

Recommended Action

Troubleshoot alarms related to failures of the primary and secondary reference source, such as SYNCPRI and SYNCSEC.

9.79 SWTRANSFER

9.79.1 TCC/TCC+

Explanation TCC/TCC+ is downloading or transferring software. This operation takes approximately 20 to 30 minutes.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

No action is necessary. Wait for the transfer to complete or the software to download.

9.80 SYNCPRI

9.80.1 TCC/TCC+

Explanation A Loss of Timing on Primary Reference alarm means that the ONS 15454 lost the primary timing source (reference 1). The ONS 15454 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 15454 should switch to secondary timing (reference 2) to obtain valid timing for the ONS 15454. This switch also triggers the SWTOSEC alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 From the card level screen for the reporting TCC card, click the **Provisioning** tab and **Timing** tab.

Step 2 Check the current configuration for the REF-1 for the NE Reference.

Step 3 If the primary reference clock is an incoming port on the ONS 15454, check the timing source for this port to make sure the current configuration of REF-1 matches the configuration of the timing source.

9.81 SYNCSEC

9.81.1 TCC/TCC+

Explanation A Loss of Timing on Secondary Reference alarm means that the ONS 15454 lost the secondary timing source (reference 2). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should automatically switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. This switch also triggers the SWTOTHIRD alarm.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 From the card-level screen for the reporting TCC card, click the **Provisioning** tab and **Timing** tab.

Step 2 Check the current configuration for the REF-2 for the NE Reference.

Step 3 If the secondary timing source is an incoming port on the ONS 15454, check the timing source for this port to make sure the current configuration of REF-2 matches the configuration of the timing source.

9.82 SYNCTHIRD

9.82.1 TCC/TCC+

Explanation The Loss of Timing on Third Reference alarm means that the ONS 15454 lost the third timing source (reference 3). The ONS 15454 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 15454 uses an internal reference for source three, then the TCC card might have failed. The ONS 15454 often reports either FRNSYNC or HLDOVERSYNC after SYNCTHIRD.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 From the card-level screen for the reporting TCC card, click the **Provisioning** tab and **Timing** tab.

Step 2 Check the current configuration for the REF-3 of the NE Reference.

Step 3 If the third timing source is an incoming port on the ONS 15454, check the timing source for this port to make sure the current configuration of REF-3 matches the configuration of the timing source.

Step 4 If the third timing source uses the internal ONS 15454 timing:

(a) Perform a software reset on the XC/XCVT card.

Go to the node view.

Position the CTC cursor over the slot reporting the alarm.

Right click to select **RESET CARD**.

(b) If this fails to clear the alarm, physically reseat the TCC card.

(c) If this fails to clear the alarm, replace the TCC 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.

When replacing a card with an identical type of card, you do not need to change the CTC database.

9.83 SYSBOOT

9.83.1 TCC/TCC+

Explanation This alarm indicates new software is activating.

- Active: Minor, Non-service affecting
- Standby: Minor, Non-service affecting

No action is required. The alarm clears when all cards finish rebooting the new software. (The reboot might take up to thirty minutes.)

9.84 TRMTMISS

9.84.1 DS1

Explanation The facility termination equipment detects a missing transmit cable on the DS-1 port. A transmit cable connector may have come off or the wrong backplane may be installed on an ONS 15454. For example, an ONS 15454 with DS1-14 cards may have a BNC backplane installed, when an AMP Champ backplane is the correct backplane for these cards.

Note DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

Recommended Action

Step 1 Check that the device attached to the DS-1 port is operational.

Step 2 Verify that the cabling is securely connected.

Step 3 Verify that the pinouts are correct.

Step 4 Replace the transmit cable, if steps 1–3 do not clear the alarm.

9.85 UNEQ-P

9.85.1 I/O

Explanation An Unequipped Path Alarm means the path does not have a valid sender or receiver. This message is carried in the C2 signal path byte in the SONET overhead. The message informs the system that the SONET payload envelope (SPE) is invalid.

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 might 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 15454, often perform the origination and termination tasks of the SONET payload.

A UNEQ-P error message on the ONS 15454 indicates that the node reporting the RFI-P is the terminating node on that path segment.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Recommended Action

Step 1 Verify that all circuits terminating in the reporting card are active.

(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, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Step 2 Verify the signal source to the DSN card reporting the alarm.

Step 3 If traffic is being affected, delete and recreate the circuit.

Caution Deleting a circuit might affect traffic.

Step 4 Check the far-end OCN card that provides STS payload to the DSN card.

Step 5 Verify cross connect between the OCN card and the DSN card.

Step 6 Clean the far-end OCN 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.

9.86 UNEQ-V

9.86.1 DS1, DS3XM-6

Explanation The VT is receiving an unequipped signal.

- Active: Major, Service affecting
- Standby: Minor, Non-service affecting

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

Warning 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.

Recommended Action

Step 1 Verify that all circuits terminating in the reporting card are active.

(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, call the Technical Assistance Center (TAC) at 1-877-323-7368.

Step 2 Verify the signal source to the DSN card reporting the alarm.

Step 3 If traffic is being affected, delete and recreate the circuit.

Caution Deleting a circuit might affect traffic.

Step 4 Check the far-end OCN card that provides STS payload to the DSN card.

Step 5 Verify cross connect between the OCN card and the DSN card.

Step 6 Clean the far-end OCN 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 OCN/DSN cards.

(a) Open the card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the replacement card.

(d) Slide the replacement card into the slot along the guide rails.

(e) Close the ejectors.

When replacing a card with an identical type of card, you do not need to change the CTC database.

Table 9-2 Entity Alarms, Equipment Alarms and Common Equipment Alarms

	Facility Alarms							Equipment	Common Equipment
	OCN	DS3	DS3XM	DS1	EC1	E100	STS		
AIS		X		X					X
AIS-L	X				X				
AIS-P							X		
AIS-V							X		
APSB	X								
APSC-DFLTK	X								
APSCIMP	X								
APSCM	X								
APSMM	X								
AUTORESET								X	
BKUPMEMP								X	
BLSROOSYNC									X
CARLOSS						X		X	
CONCAT								X	
CONNLOS	X								
CONTBUS-A-FAIL18								X	
CONTBUS-A-FAILx								X	
CONTBUS-B-FAIL18								X	
CONTBUS-B-FAILx								X	
CTNEQPT-PB*x*PROT								X	
CTNEQPT-PBxWORK								X	
DFLTK	X								
DISCONNECTED									
DS3FEEQPTFAILSA			X						
DS3FE-LOF									
EOC									
EQPT								X	X
EXTERNAL									
FAILTOSW							X		
FAILTOSW-RNG	X								
FAILTOSW-SPAN	X								
FAN								X	X

Table 9-2 Entity Alarms, Equipment Alarms and Common Equipment Alarms

	Facility Alarms							Equipment	Common Equipment
	OCN	DS3	DS3XM	DS1	EC1	E100	STS		
FE-AIS			X						
FE-DS1-MULTLOS			X						
FE-DS1-SNGLLOS			X						
FE-EQPT-NSA			X						
FE-IDLE			X						
FE-LOF			X						
FE-LOS			X						
FORCED-REQ	X								
FRNGSYNC									X
HITEMP								X	X
HLDOVERSYNC									X
IMPROPRMVL								X	
INCON	X								
LBKFACILITY									
LOCKOUTOFPR-RING	X								
LOF	X	X		X	X				X
LOP							X	X	
LOP-V							X	X	
LOS	X	X		X	X				X
LPBKDS1FEAC			X	X					
LPBKDS1FEAC-CMD				X					
LPBKDS3FEAC			X						
LPBKDS3FEAC-CMD			X						
LPBKFACILITY	X	X		X	X				
LPBKTERMINAL	X	X		X	X				
MACFAIL									X
MANRESET								X	
MANUAL							X	X	
MANUAL-REQ	X								
MEA								X	
NODEMIS	X								
PDI-P							X		
PLM-P							X		
PLM-V							X		
PRCDERR									X

Table 9-2 Entity Alarms, Equipment Alarms and Common Equipment Alarms

	Facility Alarms							Equipment	Common Equipment
	OCN	DS3	DS3XM	DS1	EC1	E100	STS		
PWRESTART								X	
RAI				X					
RCVRMISS				X					
RFI-L	X				X				
RFI-P							X		
RFI-V							X		
SD	X						X		
SFBER	X						X		
SLMF							X		
SQUELCH	X								
STU	X								X
SWTOPRI									X
SWTOSEC									X
SWTOTHIRD									X
SWTRANSFER								X	
SYNCPRI									X
SYNCSEC									X
SYNCTHIRD									X
SYSBOOT									X
TRMTMISS				X					
UNEQ-P							X		
UNEQ-V							X		

Table 9-3 and Table 9-4 list system-issued EVTs. The tables do not indicate which cards issue which EVTs or suggest that all of the EVTs on a table row are issued at the same time. For example, the transmux performs DS1, DS3, and SONET path monitoring.

Table 9-3 Threshold Crossing Events (EVTs)

		DS1	DS3	SONET Section	SONET Line	SONET Path	SONET VT
T-CVL	Coding Violations-Line	X	X		X		
T-CVP	Coding Violations-Path	X	X			X	
T-CVS	Coding Violations-Section						
T-CVV	Errored Seconds-Line						X
T-ESL	Errored Seconds-Path	X	X		X		
T-ESP	Errored Seconds-Section	X	X			X	
T-ESS	Failure Count-Path						
T-ESV	Failure Count-Line						X
T-FCP	Failure Count-Path						
T-FCL	Failure Count-Line				X		
T-PJNEG	PPJC-PDET: Negative Pointer Justification				X		
T-PJPOS	PPJC-PDET: Positive Pointer Justification				X		
T-PSC	Protection Switching Count				X		
T-PSD	Protection Switching Duration				X		
T-SASP		X	X				
T-SEFS	Severely Errored Framing Seconds			X			
T-SESL	Severely Errored Second Line	X	X		X		
T-SESP	Severely Errored Second-Path	X	X			X	
T-SESS	Severely Errored Section-Section						
T-SESV							X
T-UASL	Unavailable Second-Line				X		
T-UASP	Unavailable Second-Path	X	X			X	
T-UASV							X
T-AISSP		X	X				

Table 9-3 Threshold Crossing Events (EVTs) (continued)

	DS1	DS3	SONET Section	SONET Line	SONET Path	SONET VT
T-CVCPP		X				
T-ESCPP		X				
T-LOSSL		X				
T-SASCPP		X				
T-SESCPP		X				
T-UASCPP		X				

Table 9-4 Additional Events (EVTs)

		Etherbridge	System
TOP-CHANGE	Ethernet bridge topology change	X	
NEW-ROOT	Ethernet bridge is New Root of spanning tree	X	
CLDRESTART	Cold Restart		X
WRMRESTART	Warm Restart		X
BLSR-RESYNC	BLSR tables resynchronized		X
WKSWPR	Working unit switched to protection unit		
WKSWBK	Protection unit switched back to working unit		

Maintenance

This chapter describes procedures needed to maintain the ONS 15454, including:

- Air filter inspection
- Hard and soft system resets
- Card replacement
- Database backup and restoration
- Revert to earlier software load
- Electrical Interface Assembly (EIAs) replacement

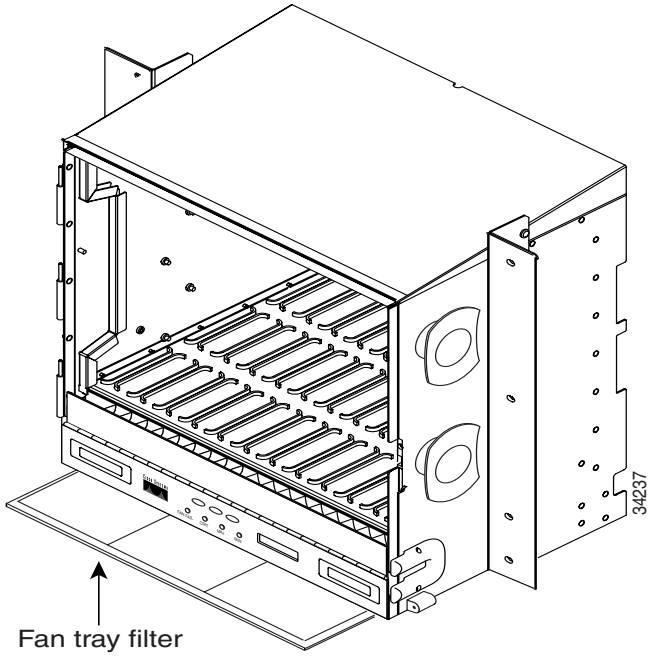
10.1 Air Filter Inspection

The Cisco ONS 15454 contains an air filter that should be removed and visually inspected approximately every 90 days, depending on the cleanliness of the operating environment. NEBS 3E and later versions of the ONS 15454 use a reusable air filter that is installed either beneath the fan tray assembly or in the optional external filter brackets. For more information on filter brackets, see the "Fan Tray Assembly" section on page 1-13. Earlier versions of the ONS 15454 use a disposable air filter that is installed beneath the fan tray assembly only. For more information on installing filters, see the "Fan Tray Assembly" section on page 1-13.

10.1.1 Reusable Air Filter

The reusable filter is made of a gray open cell polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter. Figure 10-1 illustrates a reusable fan tray filter in an external filter bracket.

Figure 10-1 Reusable Fan Tray Filter in an External Filter Bracket



Procedure: Inspecting and Cleaning the Reusable Air Filter

Step 1 If the filter is installed in the external filter brackets, slide the filter out of the bracket while being careful not to dislodge any dust that may have collected on the filter. Proceed to Step 3. If the filter is not installed in the external filter brackets but under the fan tray, open the ONS 15454 door and fold out the retractable handles at each outside edge of the fan tray.

Step 2 Slide the fan tray out of the shelf by gently pulling the handles.

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 or wash the filter under a faucet with a light detergent.

Note If possible, 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 air dry.

Warning Do not put a damp filter back in the ONS 15454.

Step 6 If the filter is installed in the external filter brackets, slide the filter all the way to the back of the bracket to complete the procedure.

Step 7 If the filter is not installed in the external filter brackets but under the fan tray, place the filter in the recessed compartment at the bottom of the ONS 15454 shelf assembly with the front edge of the filter flush against the front edge of the recessed compartment.

Step 8 Push the fan tray back into the shelf.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

Note On a powered-up ONS 15454, the fans start immediately after the fan tray is correctly inserted.

Step 9 Rotate the retractable handles back into their compartments and close the ONS 15454 front door.

10.1.2 Disposable Air Filter

The disposable filter is made of spun white polyester that is flame retardant. This disposable filter is *not* designed to be cleaned. Versions of the ONS 15454 prior to the NEBS 3E version use a disposable air filter. You can order air filter replacements from Cisco (Cisco P/N 47-01-00001) or from Universal Air Filter as model PE-5 (Universal Air Filter Co., 1624 Sauget Ind. Parkway, Sauget, IL 62206.)

Note You must remove the fan tray assembly to inspect and replace the disposable air filter.

Procedure: Inspecting and Replacing the Disposable Air Filter

The fan tray assembly is located at the bottom of the front ONS 15454 compartment. The fan tray assembly is a removable drawer that holds fans and fan control circuitry for the ONS 15454. The fan tray has an electronic plug in the back. It must plug into a corresponding receptacle on the shelf assembly backplane.

Note After you route cables in the tray, make sure the tray can swing forward on its hinges without disrupting cable routing. A hinged panel protects the cable management tray.

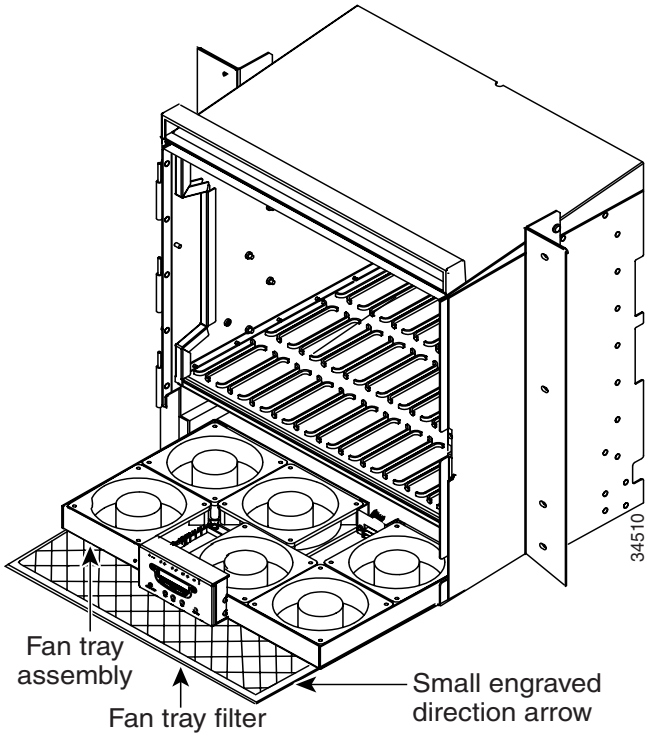
Step 1 Remove the front door of the shelf assembly.

Step 2 Open the front covers of the fiber management area.

Step 3 Lower the hinged panels in front of the cable management tray.

Step 4 Slide the fan tray out of the shelf (see Figure 10-2).

Figure 10-2 Fan Tray Assembly



Step 5 Carefully slide the air filter out of the shelf assembly (see Figure 10-3). Be careful not to dislodge any dust that may have collected on the filter.

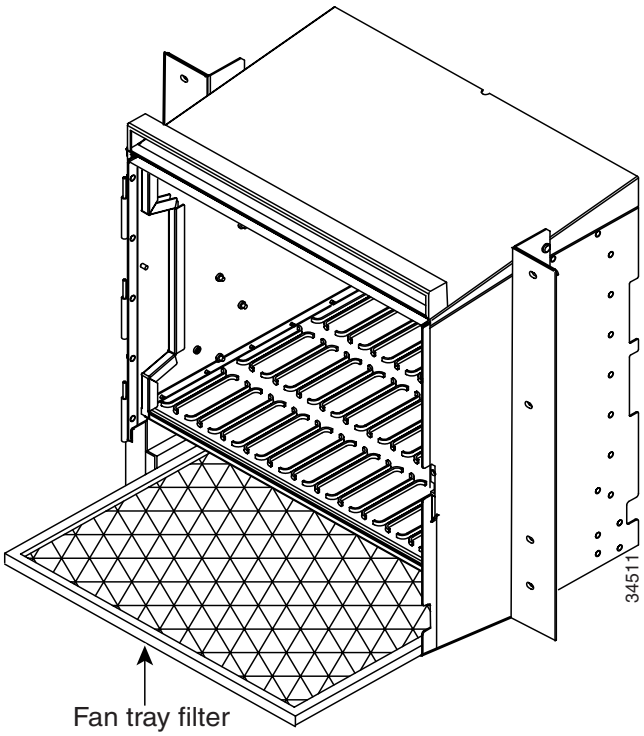
Step 6 Visually inspect the white filter material for dirt and dust.

Step 7 If the air filter shows a heavy concentration of dirt and dust, replace it with a new filter.

Step 8 To be sure you are installing the fan tray assembly correctly, make sure the air flow indications on the filter point upwards.

Step 9 Slide the filter into the bottom of the shelf assembly, making sure that the front of the filter is flush with the front of the shelf assembly.

Figure 10-3 Air Filter



Step 10 Slide the fan tray into the shelf until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane of the shelf unit.

Step 11 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan tray is activated.

Step 12 Close the cable management tray.

Step 13 Raise the hinged panel at the front of the cable management tray.

Step 14 Close the front covers of the fiber management area.

Step 15 Replace the front door of the shelf assembly.

10.2 System Reset

The ONS 15454 TCC/TCC+ may be reset using the Cisco Transport Controller (CTC) (a soft reset) or by physically reseating a TCC/TCC+ card (a hard reset). A soft reset reloads the operating system, and application software and reboots the TCC/TCC+. A hard reset also temporarily removes power from the TCC/TCC+ and clears all buffer memory.

A soft reset can be applied to either an active or standby TCC/TCC+ without affecting traffic. A hard reset should only be applied to a standby TCC/TCC+. If you need to perform a hard reset on an active TCC/TCC+, put the TCC/TCC+ into standby mode first by performing a soft reset on the card.

Procedure: Performing a Soft Reset

Step 1 Go to the node level view of the CTC.

Step 2 Right click on the TCC/TCC+ card to reveal a pull-down menu.

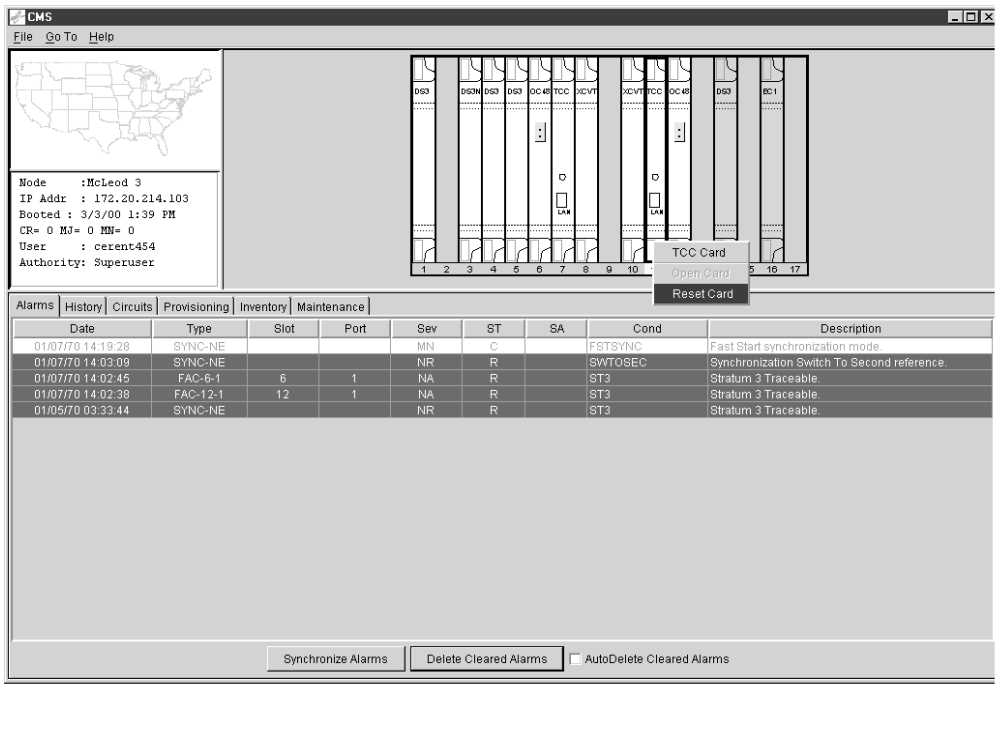
Step 3 Click **Reset Card** (see Figure 10-4).

Step 4 Click **YES** when the "Are You Sure?" dialog appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog appears.

Step 6 Confirm that the TCC comes back up in standby mode after the reset.

Figure 10-4 Soft Reset



Procedure: Performing a Hard Reset

Note To determine whether you have an active or standby TCC/TCC+, position the cursor over the TCC/TCC+ card graphic to display the status.

Step 1 If you need to perform a hard reset on an active TCC/TCC+ card, first perform a soft reset on the active TCC/TCC+ (see the "Performing a Soft Reset" section on page 10-6).

Step 2 When the TCC /TCC+ is in standby mode, unlatch both the top and bottom ejector levers on the TCC/TCC+ 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.

Note The TCC/TCC+ will take several minutes to reboot and will display the yellow standby LED after rebooting.

10.3 Database Backup and Restore

When dual TCC/TCC+ cards are installed in the ONS 15454, each TCC/TCC+ card hosts a separate database, therefore, the protect card's database is available if the database on the working TCC/TCC+ fails. A user can also store a back-up of the database on the workstation running the CTC. This operation should be part of a regular ONS 15454 maintenance program at approximately weekly intervals, and should also be completed when preparing an ONS 15454 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.

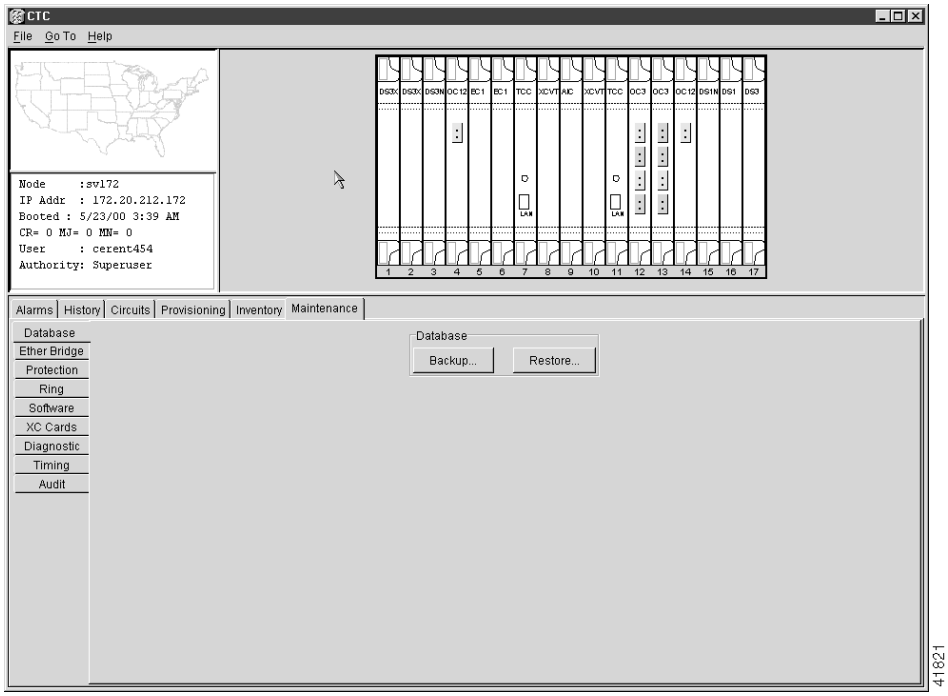
Caution IE1000-2 cards lose traffic for approximately 30 seconds when a database is restored. Traffic is lost during this period while the spanning tree reconverges. The CARLOSS alarm will appear and clear during this period.

Procedure: Backup the Database

Step 1 Log into the CTC.

Step 2 Click the **Maintenance** tab and the **Database** subtab.

Figure 10-5 Database Backup Screen



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**.

Figure 10-6 File Received Dialog

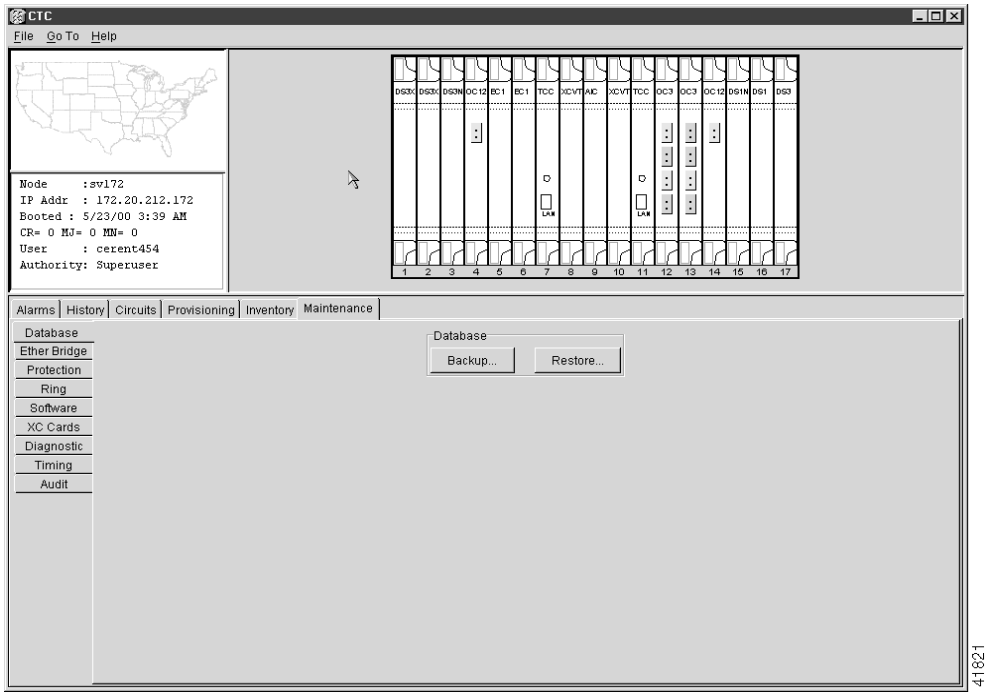
Step 6 Click **OK** on the File Received dialog.

Procedure: Restoring the Database

Step 1 Log into the CTC.

Step 2 Click the **Maintenance** tab and the **Database** subtab.

Figure 10-7 Database Backup Screen



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.**

Figure 10-8 File Transfer Dialog

Step 7 Wait for the selected file to complete the transfer to the TCC.

Step 8 Click **OK** on the **File Transfer** dialog to reboot the TCC and load the recovered database file.

10.4 Revert To Earlier Software Load

Prior to Release 2.2.1, the ONS 15454 could not revert to an earlier software database without deleting the current database and losing both cross-connect and DCC connectivity. This would result in a loss of traffic until the user manually restored the previous database or recreated the existing circuits.

Revert allows the system to switch to another software load and its attendant database without affecting traffic or DCC connectivity. This feature requires dual TCC+ cards and CTC software Release 2.2.1.

When you click the Activate button after a software upgrade, the TCC+ copies the current working database and saves it in a reserved location in the TCC+ flash memory. If later a user needs to switch back to the original working software load from the protect software load, the saved database installs automatically. The user does not need to restore the database manually or recreate circuits, and traffic runs without disruption.

The revert feature is useful when a maintenance window closes on a user upgrading CTC software. The user can revert to the standby software load without losing traffic. When the next maintenance window opens, the user completes the upgrade and activates the new software load.

Note Circuits created after clicking the Activate button will not reinstate with a revert. Only changes made prior to clicking the Activate button will be saved and reinstated.

Procedure: Revert To Earlier Software Load

Step 1 Log into the CTC.

Step 2 Record the IP address of that node.

Step 3 Go to the node view of the CTC.

Step 4 Right click on the standby TCC+ card to reveal a pull-down menu.

Step 5 Click **Reset Card**.

Step 6 Click **YES** when the “Are You Sure?” dialog appears.

Step 7 Click **OK** when the “Lost connection to node, changing to Network View” dialog appears.

Step 8 Confirm that the TCC+ comes back up in standby mode after the reset.

Step 9 Click the **Maintenance** tab and the **Software** tab.

Step 10 Verify that the protect software is Version 2.2.0 or later.

Step 11 Click **Revert**.

The Revert button activates the protect software load. The ONS node will reboot and lose the connection to the CTC.

Step 12 Wait until the software upgrade finishes. This may take as long as 30 minutes.

Step 13 Completely close the browser.

Step 14 Restart the browser and log back into the node using the IP address recorded in Step 2.

The browser downloads the CTC applet for the standby software load.

10.5 Card Replacement

To replace an ONS 15454 card with another card of the same type, you do not need to make any changes to the database; remove the old card and replace it with a new card.

To replace a card with a card of a different type, the database must be updated to reflect the change. After physically removing the card and replacing it with the new card, delete the original card from CTC and add the replacement card to CTC using the provisioning commands. See Chapter 5, "Provisioning Cards," for instructions.

To upgrade a TCC card to a TCC+ card, see the "TCC Card to TCC+ Card Upgrade" section on page 10-11. To upgrade an XC card to an XCVT card, see the "Upgrading XC Cards to XCVT" section on page 5-18.

10.6 TCC Card to TCC+ Card Upgrade

Caution An ONS 15454 must operate with a matching pair of either TCC cards or TCC+ cards.

Caution The TCC card supports ONS 15454 Release 2.2 and earlier software versions. The TCC+ card supports ONS 15454 Release 2.2 and later software versions.

Verify that the ONS 15454 is running Release 2.2 software before starting the upgrade procedure. The TCC to TCC+ upgrade process requires Release 2.2 to support the TCC/TCC+ mismatch that occurs briefly during the TCC to TCC+ upgrade process.

The ACT/STBY LED on the faceplate of the TCC/TCC+ card indicates whether the card is in active or standby mode. A green ACT/STBY LED indicates an active card and an amber light indicates a card in standby. See the "Timing Communication and Control (TCC/TCC+) Card" section on page 2-7 for more information about the TCC/TCC+ card.

Procedure: Upgrade the TCC Card to the TCC+ Card

Step 1 Physically replace the standby TCC card on the ONS 15454 with a TCC+ card.

(a) Open the TCC card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the TCC+ card.

(d) Slide the TCC+ card into the slot along the guide rails.

(e) Close the ejectors.

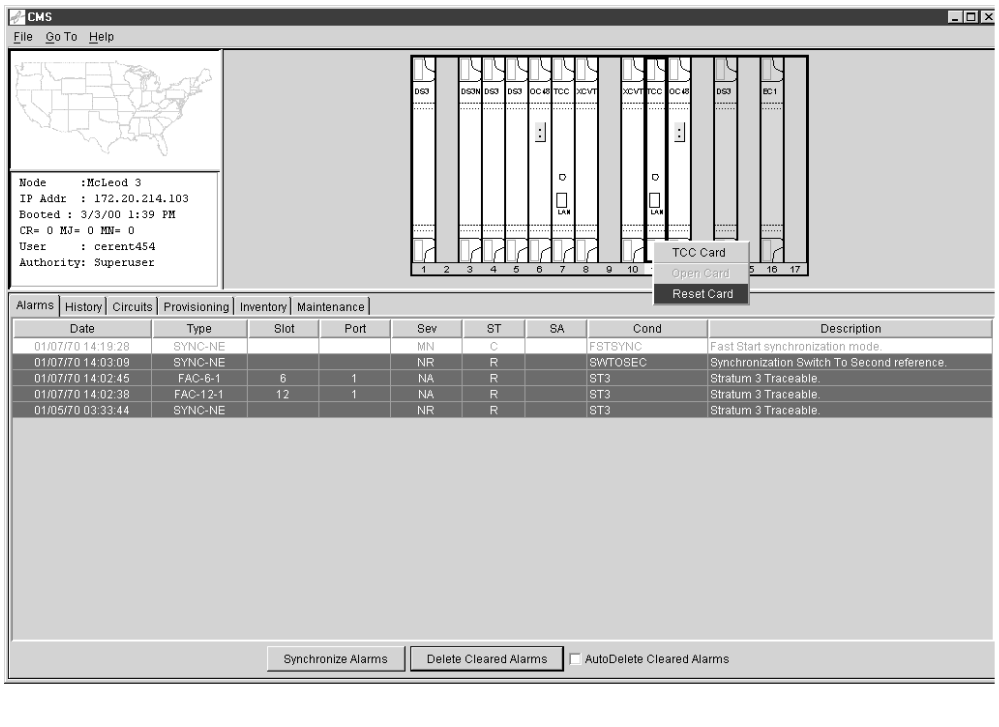
Note The MEA (card mismatch) alarm appears because the CTC recognizes a mismatch between TCC card types. Disregard this alarm; it clears by the end of the procedure.

Caution It takes approximately 20 minutes for the active TCC to transfer the system software to the newly installed TCC+. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the LEDs on the TCC+ flash Fail and then the Active/Standby LED flashes. When the transfer completes, the TCC+ reboots and goes into Standby mode after approximately three minutes.

Step 2 Right click the active TCC card to reveal a pull-down menu.

Step 3 Click **Reset Card** (see Figure 10-9).

Figure 10-9 Soft Reset



Wait for the TCC to reboot. The ONS 15454 switches the standby TCC+ card to active mode.

Step 4 Verify that the remaining TCC card is now in standby mode (the ACT/STBY LED changes to amber).

Step 5 Physically replace the remaining TCC card with the second TCC+ card.

(a) Open the TCC card ejectors.

(b) Slide the card out of the slot.

(c) Open the ejectors on the TCC+ card.

(d) Slide the TCC+ card into the slot along the guide rails.

(e) Close the ejectors.

The ONS 15454 boots up the second TCC+ card. The second TCC+ must also copy the system software, which may take up to twenty minutes. The MEA alarm clears when the ONS 15454 recognizes the matching TCC+s.

10.7 Electrical Interface Assembly Replacement

Electrical Interface Assemblies (EIAs) provide cable connection points on the back of the ONS 15454 and come in several configurations that work with different cards and connections (see Table 10-1). For more information on EIAs, see the "Backplane Covers" section on page 1-18.

EIAs have two sides. As you face the rear of the ONS 15454 shelf assembly, the right-hand side is the A side and the left-hand side is the B side. EIAs install on one or both sides of the ONS 15454 backplane in any combination. For example, you can use an AMP CHAMP EIA on side A and a BNC EIA on side B. EIAs come pre-installed on the ONS 15454 when ordered with the system.

10.7.1 EIA Types

Table 10-1 gives the product numbers and common names for EIAs.

Table 10-1 EIA Configurations

EIA Type	Cards Supported	Side A Hosts	A Side Columns Map to	A Side Product Number	Side B Hosts	B Side Columns Map to	B Side Product Number
BNC	DS-3 DS3XM-6 EC-1	24 pairs of BNC connectors	• Slot 2 • Slot 4	15454-EIA-BNC-A24	24 pairs of BNC connectors	Slot 14 Slot 16	15454-EIA-BNC-B24
High Density BNC	DS-3 DS3XM-6 EC-1	48 pairs of BNC connectors	• Slot 1 • Slot 2 • Slot 4 • Slot 5	15454-EIA-BNC-A48	24 pairs of BNC connectors	• Slot 13 • Slot 14 • Slot 16 • Slot 17	15454-EIA-BNC-B48
SMB	DS-1 DS-3 EC-1 DS3XM-6	84 pairs of SMB connectors	• Slot 1 • Slot 2 • Slot 3 • Slot 4 • Slot 5 • Slot 6	15454-EIA-SMB-A84	84 pairs of SMB connectors	• Slot 12 • Slot 13 • Slot 14 • Slot 15 • Slot 16 • Slot 17	15454-EIA-SMB-B84
AMP CHAMP	DS-1	6 AMP CHAMP connectors	• Slot 1 • Slot 2 • Slot 3 • Slot 4 • Slot 5 • Slot 6	15454-EIA-AMP-A84	6 AMP CHAMP connectors	• Slot 12 • Slot 13 • Slot 14 • Slot 15 • Slot 16 • Slot 17	15454-EIA-AMP-B84

Note The top of the EIA connector columns are labelled with the corresponding slot number.

Note EIA connector pairs are marked Tx and Rx to correspond to transmit and receive cables.

Note SMB EIAs support 14 ports per slot when used with a DS-1 card, 12 ports per slot when used with a DS-3 or EC-1 card, and 6 ports per slot when used with a DS3XM-6.

10.7.2 Replacement Procedures

The replacement procedure is the same for all the EIA types. However, installing the AMP CHAMP EIA requires the additional step of attaching the fastening plate to the bottom of the connector row. Before you attach a new EIA, you must remove the backplane cover or EIA already attached to the ONS 15454.

Procedure: Remove the Backplane Cover or EIA

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

Step 2 Loosen the nine perimeter screws that hold the backplane sheet metal cover in place.

Note Do not remove the interior screws.

Note If you are removing an AMP CHAMP EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

Step 3 If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.

Step 4 If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull the EIA panel away from the backplane.

Note Attach backplane sheet metal cover(s) whenever EIA(s) are not installed.

Procedure: Install the BNC EIAs

Step 1 Line up the connectors on the EIA with the mating connectors on the backplane.

Step 2 Gently push the EIA until both sets of connectors fit together snugly.

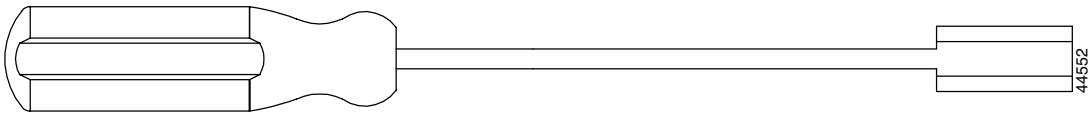
Step 3 Replace the nine perimeter screws that you removed while removing the backplane cover.

Step 4 If you are installing an AMP CHAMP EIA, attach the fastening plate with the two thumbscrews.

Step 5 Reattach the lower backplane cover.

Due to the large number of BNC connectors on the High-density BNC EIA, you might require a special tool for BNC insertion and removal (see Figure 10-10). This tool also helps with ONS 15454 patch panel connections.

Figure 10-10 BNC Insertion and Removal Tool



This tool can be obtained with P/N 227-T1000 from:

Amphenol USA (www.amphenol.com)

One Kennedy Drive

Danbury, CT 06810

Phone: 203-743-9272 Fax: 203-796-2032

This tool can be obtained with P/N RT-1L from:

Trompeter Electronics Inc. (www.trompeter.com)

31186 La Baya Drive

Westlake Village, CA 91362-4047

Phone: (800) 982-2629 Fax: (818) 706-1040

10.8 Fiber Cleaning

No special instructions apply to cleaning a fiber connected to an ONS node. 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.

TL1 Reference

11.1 Overview

This section lists TL1 alarms, commands, and autonomous messages supported by the Cisco ONS 15454. For more information about TL1, refer to Telcordia document GR833-CORE, *Network Maintenance: Network Element and Transport Surveillance Messages*.

11.2 Craft Interface

The TCC/TCC+ has two built-in interface ports for accessing the ONS 15454. With one RJ-45 craft interface browser LAN connection you can access the system using a standard browser interface. While using the browser interface, you can perform local and remote Operations, Administration, Maintenance and Provisioning (OAM&P) functions and open a VT100 emulation window to enter TL1 commands. If a browser is not available, you can access the system using a nine- pin RS-232 port. The RS-232 port supports VT100 emulation such that TL1 commands may be entered directly without a browser.

Refer to the "Craft Interface Installation" section on page 1-31 for detailed installation procedures. Refer to the "Connecting to the ONS 15454 with TL1 Terminals" section on page 3-9 for information on terminal setup.

11.3 TL1 Access using Telnet

To access the ONS 15454 TL1 commands using a Telnet session over a craft interface or a Local Access Network (LAN) connection (TCC/TCC+ front panel or backplane pins), you must use port number 2361. At a command prompt, start the Telnet session by typing:

```
telnet <Node IP Address> 2361 [Enter]
```

11.4 Alarms

This section lists TL1 alarms supported by the ONS 15454. Each alarm list includes a description, service affect criteria, and severity. Refer to Chapter 9, "CTC Alarms," for fault recovery procedures. The following alarm types are listed:

- Equipment Alarms
- SONET Optical Carrier, level n (OC-N) Alarms

- Digital Signal, level 1 (DS-1) Alarms
- Digital Signal, level 3 (DS-3) Alarms
- Synchronous Transport Signal (STS) Alarms
- Virtual Tributary (VT) Termination Alarms
- Building Integrated Timing Supply (BITS) Alarms
- Network Element (NE) Synchronous Reference Alarms

11.4.1 Equipment Alarms

Table 11-1 Equipment Alarms

EQPT alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
INT	all any mode	CR/MN	SA/NSA	Internal board Failure
IMPROPRMVL	all any mode	CR/MN	SA/NSA	Board is provisioned and has been unplugged
MEA	all any mode	MN/MN	NSA/NSA	Mismatch in between the physical equipment type and the provisioned equipment type
FAILTOSW-PATH	TCC,TCC+, XC,DS-3 any mode	MJ/MN	SA/NSA	Failure to perform an equipment protection switch
POWERFAIL	all any mode	CR/MN	NSA/NSA	Power Failure on the node
MANUAL	TCC,TCC+, XC,DS-3 any mode	MN/MN	NSA/NSA	Operator Manual switch severity active
FORCED	TCC,TCC+, XC,DS-3 any mode	MN/MN	NSA/NSA	Operator Force switch severity active
DIAGFAIL	all any mode	CR/MN	NSA/NSA	Equipment diagnostic failure
HITEMP	TCC,TCC+ Any mode	CR/CR	NSA/NSA	Excessive temperature - operating still maintaining normal operations
FAN	all any mode	CR/MI	NSA/NSA	Fan operation failure
PWRRESTART	all any mode	MI/MI	NSA/NSA	Power restart
AUTORESET	all any mode	MI/MI	NSA/NSA	Automatic reset

Table 11-1 Equipment Alarms (continued)

EQPT alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
MANRESET	TCC,TCC+ any mode	MI/MI	NSA/NSA	Manual reset
INIT	TCC,TCC+ any mod	MI/MI	NSA/NSA	Initialization initiated
SWTRANSFER	TCC,TCC+ any mod	MI/MI	NSA/NSA	Software download in progress
CONTBUS-A-*X*	IO,XC any mode	MJ/MN	NSA/NSA	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot *X*
CONTBUS-A-8	IO,XC any mode	MJ/MN	NSA/NSA	Main processor on the TCC/TCC+ card in Slot 7 has lost communication with the coprocessor on the second TCC/TCC+ card in Slot 11
CONTBUS-B-*X*	IO,XC any mode	MJ/MN	NSA/NSA	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot *X*
CONTBUS-B-8	IO,XC any mode	MJ/MN	NSA/NSA	Main processor on the TCC/TCC+ card in Slot 11 has lost communication with the processor on the second TCC/TCC+ card in Slot 7
CTNEQPT-PB*X* PROT	I/O, XC/XCVT	CR/MN	SA/NSA	Failure of the main payload between the XC/XCVT card in Slot 10 and the reporting I/O card in Slot *X*
CTNEQPT-PB*X* WORK	I/O, XC/XCVT	CR/MN	SA/NSA	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot *X*

11.4.2 OC-N Alarms

Table 11-2 OC-N Alarms

OC-n alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
LOS	OC-3, OC-12, OC-48 any mode	CR/MN	SA/NSA	Loss of Signal alarm
LOF	OC-3,OC-12, OC-48 any mode	CR/MN	SA/NSA	Loss of Frame alarm
AIS-L	OC-3,OC-12, OC-48 any mode	MN/MN	SA/NSA	Alarm Indication Signal Line alarm
RFI-L	OC-3,OC-12, OC-48 any mode	MN/MN	NSA/NSA	Remote Failure Indication Line alarm
SFBER	OC-3,OC-12, OC-48, any mode	CR/MN	SA/NSA	Signal fail error rate alarm
SDBER	OC-3,OC-12, OC-48 any mode	MN/MN	SA/NSA	Signal degrade error rate alarm
FAILTOSW-RNG	OC-3,OC-12, OC-48 2F BLSR mode	MJ/MN	SA/NSA	Failure to perform a two-fiber BLSR ring switch
FAILTOSW-SPAN	OC-3,OC-12, OC-48 linear mode	MJ/MN	SA/NSA	Failure to perform a Linear APS 1+1 switch
MANUAL-REQ	OC-3,OC-12, OC-482 2F BLSR mode	MN/MN	NSA/NSA	Manual Ring Switch Severity active
FORCED-REQ	OC-3,OC-12, OC-48 2F BLSR mode	MN/MN	SA/NSA	Force Ring Switch Severity active
LOCKOUTOFPR-RING	OC-3,OC-12, OC-482 2F BLSR mode	MN/MN	SA/NSA	Lockout of Protection Channel Switch Severity active
MANUAL-SPAN	OC-3,OC-12, OC-48 linear mode	MN/MN	NSA/NSA	Manual Span Switch Severity active
FORCED-SPAN	OC-3,OC-12, OC-482 linear mode	MN/MN	SA/NSA	Force Span switch Severity active

Table 11-2 OC-N Alarms (continued)

OC-n alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
LOCKOUT-SPAN	OC-3,OC-12, OC-48 linear mode	MN/MN	SA/NSA	Lockout Span Switch Severity active
APSB	OC-3,OC-12, OC-48 linear mode	MJ/MN	SA/NSA	Automatic Protection Switching (APS) byte failure
APSCM	OC-3,OC-12, OC-48 linear mode	MJ/MN	SA/NSA	APS Channel Mismatch failure
APSMM	OC-3,OC-12, OC-48 linear mode	MJ/MN	SA/NSA	APS Mode Mismatch failure
APSFERPFAIL		MN/MN	NSA/NSA	APS channel far-end protection line failure
EOC		MJ/MN	NSA/NSA	Data communication channel failure
SQUELCH	OC-12,OC-48 2F BLSR mode	MJ/MN	SA/NSA	Squelching in progress
INCON	OC-12,OC-48 2F BLSR mode	MJ/MN	SA/NSA	Inconsistent APS code
APSCIMP	OC-12,OC-48 2F BLSR mode	MJ/MN	SA/NSA	Improper SONET Automatic Protect Switch code
NODEMIS	OC-12,OC-48 2F BLSR mode	MJ/MN	SA/NSA	Node Id mismatch failure
DFLTK	OC-12,OC-48 2F BLSR mode	MN/MN	NSA/NSA	Default K byte transmitted
CONNLOS	TCC/TCC+ 2F BLSR mode	MJ/MN	NSA/NSA	Inter-node connectivity lost in two-fiber BLSR configuration
ALS		CR/MN	NSA/NSA	Automatic laser shut down
LPBKTERMIN	OC-3,OC-12, OC-48 any mode	MJ/MI	SA/NSA	Terminal loopback active
LPBKFACILITY	OC-3, OC-12, OC-48 any mode	MJ/MI	SA/NSA	Facility loopback active

11.4.3 DS-3 Alarms

Table 11-3 DS-3 Alarms

DS-3 alarm	Card/Mode	Severity (Active)	SA/NSA (Active)	Description
PEERMISSM	DS-3 any mode	MJ	SA	Peer state mismatch
LOS	DS-3 any mode	CR	SA	Loss of signal alarm
LPBK	DS-3 any mode	MJ	SA	Loopback active
IDLE	DS-3 any mode	MJ	SA	DS-3 idle condition
RAI	DS-3 any mode	MN	SA	Remote alarm indication
DS3MANTERM-LPBK	DS-3 any mode	MJ	SA	Loopback terminal
DS3MANFAC LPBK	DS-3 any mode	MJ	SA	Loopback facility
DS3FELPBK	DS-3 any mode	MJ	SA	Loopback due to Far-End Alarm Condition (FEAC) command
DS2FELPBK	DS-3 any mode	MJ	SA	DS-2 loopback command sent to far-end
DS1FELPBK	DS-3 any mode	MJ	SA	DS- 1 loopback due to FEAC command
DS3FELPBK	DS-3 any mode	MJ	SA	DS-3 loopback due to FEAC command
DS3FELPBKCMD	DS-3 any mode	MJ	SA	DS-3 loopback command sent to far-end
FE-EQPT-FAIL-SA	DS-3 any mode	MJ	SA	Far-end DS-3 equipment fail service-affecting
FE-LOS	DS-3 any mode	MJ	SA	Far-end loss of signal
FE-LOF	DS-3 any mode	MJ	SA	Far-end loss of frame
FE-AIS	DS-3 any mode	MJ	SA	Far-end alarm indication signal
FE-IDLE	DS-3 any mode	MJ	SA	Far-end idle
FE-EQPT-NSA	DS-3 any mode	MJ	SA	Far-end DS-3 equipment fail non-service affecting

Table 11-3 DS-3 Alarms (continued)

DS3FECMNEQPT FAIL	DS-3 any mode	MJ	SA	Far-end common equipment fail non-service affecting
FE-DS1-MULTI LOS	DS3XM any mode	MJ	SA	Far-end multiple DS-1 LOS detected on DS-3
DS1FEEQPTFAIL SA	DS3XM any mode	MJ	SA	Far-end DS-1 equipment fail service-affecting
FE-SD1-SNGLLOS	DS3XM any mode	MJ	SA	DS-1 far-end single DS-1 LOS
DS1FEEQPT	DS3XM any mode	MJ	SA	Far-end DS-1 equipment failure service-affecting

11.4.4 DS-1 Alarms

Table 11-4 DS-1 Alarms

DS-1 alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
LOS	DS-1 any mode	MJ/None	SA/None	Loss of signal alarm
AIS	DS-1 any mode	MJ/None	SA/None	Alarm indication signal alarm
LOF	DS-1 any mode	MJ/None	SA/None	Loss of frame alarm
RAI	DS-1 any mode	MN/None	SA/None	Remote alarm indication alarm
TERMLPBK	DS-1 any mode	MJ/None	SA/None	Terminal loopback active
FACLPBK	DS-1 any mode	MJ/None	SA/None	Facility loopback active
ELECTRICAL INTERFACE MISSING - TX	DS-1 any mode	MJ/MN	NSA/NSA	Facility Termination equipment - Transmitter missing
ELECTRICAL INTERFACE MISSING - RX	DS-1 any mode	MJ/MN	NSA/NSA	Facility Termination equipment - Receiver missing
ELECTRICAL INTERFACE FAILURE - TX	DS-1 any mode	MJ/MN	NSA/NSA	Transmit Failure
FELPBK	DS-1 any mode	MJ/None	SA/None	DS-1 loopback due to FEAC command
FELPBKCMD	DS-1 any mode	MJ/None	SA/None	DS-1 loopback command sent to far-end

11.4.5 STS Alarms

Table 11-5 STS Alarms

STS Mon alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
AIS-P	STS Monitor any mode	MJ/MN	SA/NSA	Alarm Indication Signal alarm
LOP	STS Monitor any mode	MJ/MN	SA/NSA	Loss of Pointer alarm
CONCAT	STS Monitor any mode	MJ/MN	SA/NSA	STS concatenation alarm
UNEQ-P	STS Termination on DS-3 card any mode	MJ/MN	SA/NSA	Path Unequipped alarm
SFBER	STS Termination on DS-3 card any mode	MJ/MN	SA/NSA	Path Signal Fail bit error rate alarm
SDBER	STS Termination on DS-3 card any mode	MN/MN	SA/NSA	Path Signal Degrade bit error rate alarm
RFI	STS Termination on DS-3 card any mode	MN/MN	SA/NSA	Path Remote Failure Indication alarm
SLMF	STS Termination on DS-3 card any mode	MN/MN	SA/NSA	Signal Label Mismatch alarm
PDI-P		MN/MN	SA/NSA	Payload Defect Indication Path
PLM-P		MN/MN	SA/NSA	Payload Label Mismatch Path
FAILTOSW	STS Termination on DS-3 card any mode	MJ/MN	NSA/NSA	Fail to switch to protection
MANUAL	STS Termination on DS-3 card any mode	MN/MN	NSA/NSA	Manual switch of working facility equipment to protection
FORCED	STS Termination on DS-3 card any mode	MN/MN	NSA/NSA	Working facility/equipment forced to switch to protection

11.4.6 VT Termination Alarms

Table 11-6 VT Termination Alarms

VT Term alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
LOP	STS Monitor any mode	MJ/MN	SA/NSA	Loss of pointer alarm
AIS	VT Termination on DS-1 card any mode	MJ/MN	SA/NSA	VT Alarm Indication Signal alarm
UNEQP	VT Termination on DS-1 card any mode	MJ/MN	SA/NSA	VT Unequipped alarm
RFI	VT Termination on DS-1 card any mode	MN/MN	SA/NSA	VT Remote Failure Indication alarm
PLM	VT Termination on DS-1 card any mode	MN/MN	SA/NSA	VT Payload Label Mismatch alarm
SFBER		MJ/MN	SA/NSA	BER threshold passed for signal failure
SDBER		MJ/MN	SA/NSA	BER threshold passed for signal degrade

11.4.7 BITS Alarms

Table 11-7 Bits Alarms

BITS alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA (Active/ Standby)	Description
LOS	Bits on TCC/TCC+ card any mode	MJ/MN	SA/NSA	Loss of Signal alarm
LOF	Bits on TCC/TCC+ card any mode	MJ/MN	SA/NSA	Loss of Frame alarm
AIS	Bits on TCC/TCC+ card any mode	MJ/MN	SA/NSA	Alarm Indication Signal alarm

11.4.8 Network Element Synch Ref Alarms

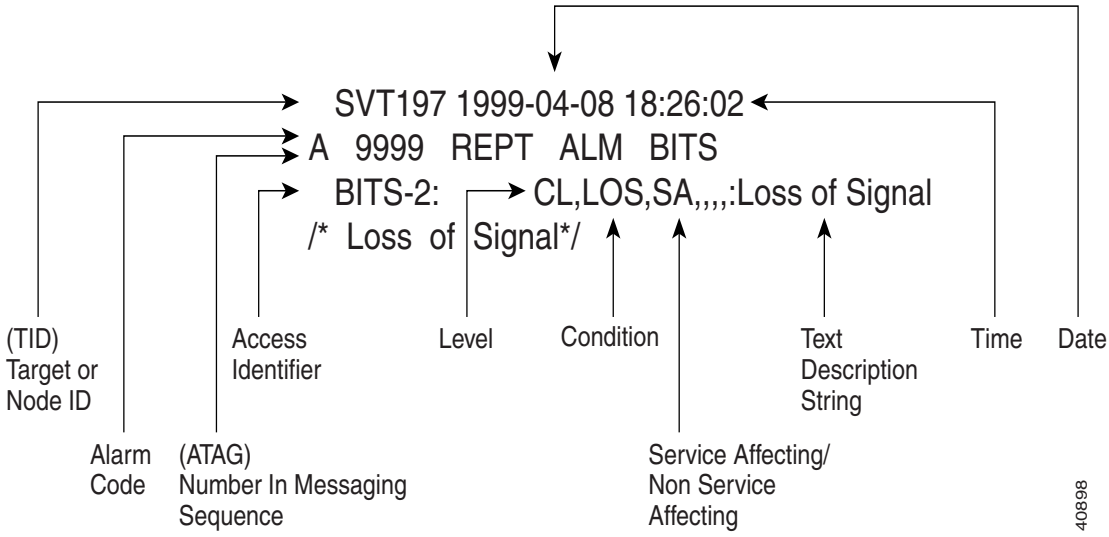
Table 11-8 Synch Ref Alarms

neSynchRef alarm	Card/Mode	Severity (Active/ Standby)	SA/NSA	Description
SYNCPRI	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Primary Synchronization reference failure alarm
SYNCSEC	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Secondary Synchronization reference failure alarm
SYNCTHIRD	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Third Synchronization reference failure alarm
HLDOVRSYNC	neSynchRef on TCC/TCC+ card any mode	MJ/MN	SA/NSA	Holdover Synchronization alarm
FRNGSYNC	neSynchRef on TCC/TCC+ card any mode	MJ/MN	SA/NSA	Free Run Synchronization alarm
MANUAL	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Operator-initiated synchronization switch
FASTSTART	Fast start Synch node	No	No Alarm	Fast Start Synchronization alarm
MANSWTOPRI	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Synchronization switch to primary reference
MANSWTOSEC	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Synchronization switch to second reference
MANSWTOTHID	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Synchronization switch to third reference
SWTOPRI	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Synchronization switch to primary reference
SWTOSEC	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Synchronization switch to second reference
SWTOTHIRD	neSynchRef on TCC/TCC+ card any mode	MN/MN	NSA/NSA	Synchronization switch to third reference

11.5 Autonomous Messages

The autonomous TL1 messages are included in the TL1 Command Description section, and the messages are listed alphabetically. Figure 11-1 shows the autonomous alarm message format. Autonomous Message Tag (ATAG) is used for message sequencing. The number is incremented by one for each autonomous message sent by the ONS 15454. The ONS 15454 uses whole numbers 0000 to 9999.

Figure 11-1 Autonomous Alarm Message Format



11.6 Performance Monitoring

Performance information is continuously monitored and stored in individual Performance Monitoring (PM) registers. This information can be retrieved upon request or when a preset threshold is exceeded. Table 11-9 lists PM Statistics by board.

11.6.1 Performance Monitoring Statistics

Table 11-9 PM Statistics

PM Statistics by Board	Special Qualifications	Source	DS-1	DS-3	DS-3 XM	OC-3/ 12/48	EC-1
Sonet Section Stats							
CV-S	(not supported yet)	B1					
ES-S	(not supported yet)	B1					
SES-S	(not supported yet)	B1					
SEFS-S		B1				X	X
Sonet Line Stats							

Table 11-9 PM Statistics (continued)

PM Statistics by Board	Special Qualifications	Source	DS-1	DS-3	DS-3 XM	OC-3/ 12/48	EC-1
CV-L		B2				X	X
ES-L		B2				X	X
SES-L						X	X
UAS-L						X	X
FC-L						X	X
PSC						X	
PSD						X	
STS PJ	Non-terminated STS only	H1, H2					
PPJC-PDET	Positive detected at input					X	X
NPJC-PDET	Negative detected at input					X	X
PPJC-PGEN	Positive generated					X	X
NPJC-PGEN	Negative generated					X	X
Far End							
CV-L FE		K2				X	X
ES-L FE		K2				X	X
SES-L FE		K2				X	X
UAS-L FE		K2				X	X
FC-L FE		K2				X	X
Sonet Path Stats							
CV-P		B3	X	X	X		
ES-P			X	X	X		
SES-P			X	X	X		
UAS-P			X	X	X		
FC-P							
VT PJ							
Far End	Supplied by XCON						
CV-P FE	From XCON					X	
ES-P FE	From XCON					X	
SES-P FE	From XCON					X	
UAS-P FE	From XCON					X	
FC-P FE							
VT Path Stats	VT terminated circuits only						
CV-V			X		X		
ES-V			X		X		
SES-V			X		X		
UAS-V			X		X		
FC-V							

Table 11-9 PM Statistics (continued)

PM Statistics by Board	Special Qualifications	Source	DS-1	DS-3	DS-3 XM	OC-3/ 12/48	EC-1
Far End							
CV-V FE			X		X		
ES-V FE			X		X		
SES-V FE			X		X		
UAS-V FE			X		X		
FC-V FE							
DS-n Stats							
DS-n Line							
CV-L		X	X	X	X		
ES-L		X	X	X	X		
LOSS-L					X		
SES-L		X	X	X	X		
DS-3 Path							
P Bit Stats	M13 & C Bit Framing						
AISS-P					X		
CVP-0					X		
ESP-P					X		
SASP-P					X		
SESP-P					X		
UASP-P					X		
CP Bit Stats	C Bit Framing ONLY						
CVCP-P					X		
ESCP-P					X		
SASCP-P					X		
SESCP-P					X		
UASCP-P					X		
Far End							
CVCP-P FE					X		
ESCP-P FE					X		
SASCP-P FE					X		
SESCP-P FE					X		
UASCP-P FE					X		
DS-1 Path							
CV-P RX			X				
AISS-P RX			X		X		
ES-P RX			X		X		
SAS-P RX			X		X		

Table 11-9 PM Statistics (continued)

PM Statistics by Board	Special Qualifications	Source	DS-1	DS-3	DS-3 XM	OC-3/ 12/48	EC-1
SES-P RX			X		X		
UAS-P RX			X		X		
CV-P TX			X		X		
AISS-P TX			X		X		
ES-P TX			X		X		
SAS-P TX			X		X		
SES-P TX			X		X		
UAS-P TX			X		X		

11.7 TL1 Command Syntax

TL1 commands conform to the following syntax:

a:b:c::d:e: ... z;

where:

“a” is the Command Code

“b” is the Target Identifier (TID)

“c” is the Access Identifier (AID) or the User Identifier (UID)

“d” is the Correlation Tag (CTAG)

“e: ... z;” are the other positions required for various commands

The TID, AID, and CTAG route and control the TL1 command. Other parameters provide additional messages required to complete the action requested by the command.

The TID is a unique name given to each system when it is installed. The name identifies the particular NE (in this case, the ONS 15454), to which each command is directed. Each TID can have a maximum of 20 alpha-numeric characters. To establish the TID for a ONS 15454 node, use the Network Element Name option of the Network Element Configuration menu.

The AID is an access code used to identify and address specific objects within the ONS 15454. These objects include individual pieces of equipment, transport spans, access tributaries, and other objects.

The CTAG is a unique identifier given to each input command by the operator. When the ONS 15454 system responds to a specific command, it includes the command’s CTAG in the reply. This eliminates discrepancies about what response corresponds to what command. Valid CTAG values include strings of up to six characters comprised of identifiers (alphanumeric, beginning with a letter) or decimal numerals (a string of decimal digits with an optional non-trailing “.”).

11.8 TL1 Command Privilege Map

The following table specifies command access privileges.

Table 11-10 Command Access

Command	Superuser	Provision	Maintenance	Retrieve
DLT-USER-SECU	X			
ED-DAT	X			
ED-USER-SECU	X			
ENT-USER-SECU	X			
SET-TOD	X	X		
DLT-*-*	X	X		
ED-*-*	X	X		
ENT-*-*	X	X		
SET-*-*	X	X		
INIT-*-*	X	X	X	
OPR-*-*	X	X	X	
RLS-*-*	X	X	X	
RMV-*-*	X	X	X	
RST-*-*	X	X	X	
SW-*-*	X	X	X	
ALW-*-*	X	X	X	X
INH-*-*	X	X	X	X
REPT * *	X	X	X	X
RTRV-*-*	X	X	X	X
CANC-*-*	X	X	X	X
ACT-*-*	X	X	X	X
ED-PD	X	X	X	X

User security levels also limit the amount of time a user can leave the system idle before the TL1 session is locked to prevent unauthorized users from making changes. Higher security levels have shorter idle times. Table 11-11 shows security levels and their idle times

Table 11-11 Security Idle Times

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

11.9 TL1 Command List

11.9.1 Cross Connect

DLT-CRS-<STS_PATH>

DLT-CRS-VT1

ED-CRS-<STS_PATH>

ED-CRS-VT1

ENT-CRS-<STS_PATH>

ENT-CRS-VT1

RTRV-CRS-<STS_PATH>

RTRV-CRS-VT1

11.9.2 Environment

REPT ALM ENV

RTRV-ALM-ENV

11.9.3 Equipment

DLT-EQPT

DLT-FFP-EQPT

ED-FFP-EQPT

ENT-EQPT

ENT-FFP-EQPT

OPR-PROTNSW-EQPT

REPT ALM EQPT

REPT EVT EQPT

RLS-PROTNSW-EQPT

RTRV-ALM-EQPT

RTRV-COND-EQPT

RTRV-EQPT

RTRV-FFP-EQPT

SW-DX-EQPT

11.9.4 Facility

RMV-<MOD2>

RST-<MOD2>

11.9.5 Facility Protection

DLT-FFP-<OCN_TYPE>

ED-FFP-<OCN_TYPE>

ENT-FFP-<OCN_TYPE>

RTRV-FFP-<OCN_TYPE>

11.9.6 Fault

REPT ALM <MOD2ALM>

REPT ALM BITS

REPT EVT <MOD2ALM>

RTRV-ALM-<MOD2ALM>

RTRV-ALM-ALL

RTRV-ALM-BITS

RTRV-COND-<MOD2ALM>

RTRV-COND-ALL

RTRV-COND-BITS

11.9.7 Log

RTRV-LOG

11.9.8 Performance

INIT-REG-<MOD2>

RTRV-PM-<MOD2>

RTRV-TH-<MOD2>

SET-TH-<MOD2>

11.9.9 Security

DLT-USER-SECU

ED-PID

ED-USER-SECU

ENT-USER-SECU

11.9.10 Switch

OPR-PROTNSW-<OCN_TYPE>

RLS-PROTNSW-<OCN_TYPE>

11.9.11 Synchronization

ED-SYNCN

REPT ALM SYNCN

REPT EVT SYNCN

RTRV-ALM-SYNCN

RTRV-COND-SYNCN

RTRV-SYNCN

11.9.12 System

ACT-USER

ALW-MSG-ALL

CANC-USER

ED-DAT

INH-MSG-ALL

INIT-SYS

RTRV-HDR

11.9.13 Testing

OPR-LPBK-<OCN_TYPE>

OPR-LPBK-DS1

OPR-LPBK-EC1

OPR-LPBK-T1

OPR-LPBK-T3

RLS-LPBK-<OCN_TYPE>

RLS-LPBK-DS1

RLS-LPBK-EC1

RLS-LPBK-T1

RLS-LPBK-T3

11.9.14 Other

DLT-<MODE2>

ED-<OCN_TYPE>

ED-<STS_PATH>

ED-BITS

ED-EC1

ED-NE

ED-T1

ED-T3

ENT-<MOD2>

OPR-UPGRADE

RTRV-<OCN_TYPE>

RTRV-<STS_PATH>

RTRV-BITS

RTRV-EC1

RTRV-INV

RTRV-NE

RTRV-T1

RTRV-T3

RTRV-TOD

SET-TOD

11.10 TL1 Command Index

Table 11-12 Command Index

Command	Group	Page Number
ACT-USER	System	22
ALW-MSG-ALL	System	23
CANC-USER	System	23
DLT-<MODE2>	Other	24
DLT-CRS-<STS_PATH>	Cross Connect	24
DLT-CRS-VT1	Cross Connect	25
DLT-EQPT	Equipment	25
DLT-FFP-<OCN_TYPE>	Facility Protection	26
DLT-FFP-EQPT	Equipment	26
DLT-USER-SECU	Security	27
ED-<OCN_TYPE>	Other	27
ED-<STS_PATH>	Other	28
ED-BITS	Other	29
ED-CRS-<STS_PATH>	Cross Connect	29
ED-CRS-VT1	Cross Connect	30
ED-DAT	System	30
ED-EC1	Other	31
ED-FFP-<OCN_TYPE>	Facility Protection	31
ED-FFP-EQPT	Equipment	32
ED-NE	Other	33
ED-PID	Security	33
ED-SYNCN	Synchronization	34
ED-T1	Other	35

Table 11-12 Command Index (continued)

Command	Group	Page Number
ED-T3	Other	35
ED-USER-SECU	Security	36
ENT-<MOD2>	Other	37
ENT-CRS-<STS_PATH>	Other	37
ENT-CRS-VT1	Other	38
ENT-EQPT	Equipment	38
ENT-FFP-<OCN_TYPE>	Facility Protection	39
ENT-FFP-EQPT	Equipment	40
ENT-USER-SECU	Security	40
INH-MSG-ALL	System	41
INIT-REG-<MOD2>	Performance	42
INIT-SYS	System	42
OPR-LPBK-<OCN_TYPE>	Testing	43
OPR-LPBK-DS1	Testing	44
OPR-LPBK-EC1	Testing	44
OPR-LPBK-T1	Testing	45
OPR-LPBK-T3	Testing	46
OPR-PROTNSW-<OCN_TYPE>	Switch	46
OPR-PROTNSW-EQPT	Equipment	47
OPR-UPGRADE	Other	47
REPT ALM <MOD2ALM>	Fault	48
REPT ALM BITS	Fault	49
REPT ALM ENV	Environment	50
REPT ALM EQPT	Equipment	50
REPT ALM SYNCN	Synchronization	51
REPT EVT <MOD2ALM>	Fault	52
REPT EVT EQPT	Equipment	53
REPT EVT SYNCN	Synchronization	54
RLS-LPBK-<OCN_TYPE>	Testing	55
RLS-LPBK-DS1	Testing	56
RLS-LPBK-EC1	Testing	56
RLS-LPBK-T1	Testing	57
RLS-LPBK-T3	Testing	58
RLS-PROTNSW-<OCN_TYPE>	Switch	59
RLS-PROTNSW-EQPT	Equipment	59
RMV-<MOD2>	Facility	60
RST-<MOD2>	Facility	60
RTRV-<OCN_TYPE>	Other	61

Table 11-12 Command Index (continued)

Command	Group	Page Number
RTRV-<STS_PATH>	Other	62
RTRV-ALM-<MOD2ALM>	Fault	62
RTRV-ALM-ALL	Fault	63
RTRV-ALM-BITS	Fault	69
RTRV-ALM-ENV	Environment	66
RTRV-ALM-EQPT	Equipment	67
RTRV-ALM-SYNCN	Synchronization	68
RTRV-BITS	Other	69
RTRV-COND-<MOD2ALM>	Fault	70
RTRV-COND-ALL	Fault	71
RTRV-COND-BITS	Fault	72
RTRV-COND-EQPT	Equipment	73
RTRV-COND-SYNCN	Synchronization	74
RTRV-CRS-<STS_PATH>	Cross Connect	75
RTRV-CRS-VT1	Cross Connect	76
RTRV-EC1	Other	77
RTRV-EQPT	Equipment	78
RTRV-FFP-<OCN_TYPE>	Facility Protection	79
RTRV-FFP-EQPT	Equipment	80
RTRV-HDR	System	81
RTRV-INV	Other	81
RTRV-LOG	Log	82
RTRV-NE	Other	83
RTRV-PM-<MOD2>	Performance	85
RTRV-SYNCN	Synchronization	86
RTRV-T1	Other	87
RTRV-T3	Other	88
RTRV-TH-<MOD2>	Performance	89
RTRV-TOD	Other	90
SET-TH-<MOD2>	Performance	90
SET-TOD	Other	91
SW-DX-EQPT	Equipment	92

11.11 TL1 Command Description

This section lists TL1 commands supported by the ONS 15454. Each listing includes a description, input format, input parameters (instructions within a command), and input example. The descriptions are alphabetical according to the first alpha character of the command string.

Note The TL1 input command string size should equal and less than 1023 characters from either a TL1 telnet session or CTC. Any TL1 input string larger than 1023 characters will cause the active TCC to reset.

Note TL1 commands not entered correctly are not completed.

11.11.1 ACT-USER: Activate User

This command allows you to log in to the Network Element (NE).

Section	Description
Category	System
Security	Read Only
Related Messages	ALW-MSG-ALL CANC-USER DLT-USER-SECU ED-DAT ED-PID ED-USER-SECU ENT-USER-SECU INH-MSG-ALL INIT-SYS RTRV-HDR
Input Format	ACT-USER:[TID]:<userid>:[CTAG]::<passwd>; where: • userid identifies the user to the system and is a String • passwd is the user's private password and is a String
Example	Input ACT-USER:PETALUMA:TERRI:100::MYPASSWD;
Errors	This message generates all the default errors

11.11.2 ALW-MSG-ALL: Allow Message All

This command instructs the NE to enter a mode in which all automatic messages are transmitted.

Section	Description
Category	System
Security	N/A
Related Messages	ACT-USER CANC-USER ED-DAT INH-MSG-ALL INIT-SYS RTRV-HDR
Input Format	ALW-MSG-ALL:[TID]::[CTAG]::,,;
Example	Input ALW-MSG-ALL:PETALUMA::549::,,;
Errors	This message generates all the default errors

11.11.3 CANC-USER: Cancel User

This command logs a user off of the NE.

Section	Description
Category	System
Security	Read Only
Related Messages	ACT-USER ALW-MSG-ALL DLT-USER-SECU ED-DAT ED-PID ED-USER-SECU ENT-USER-SECU INH-MSG-ALL INIT-SYS RTRV-HDR
Input Format	CANC-USER:[TID]:[<userid>]:[CTAG]; where: • userid identifies the user to the system and is a String
Example	Input CANC-USER:PETALUMA:TERRI:101;
Errors	This message generates all the default errors

11.11.4 DLT-<MOD2>: Delete (DS-1, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command deletes the line or facility by putting it out of service.

Note The DLT- does not support STS1, STS3C, STS12C, STS48C, VT1, and DS1 modifiers in Release 2.2.1.

Section	Description
Category	Other
Security	N/A
Related Messages	N/A
Input Format	DLT-<MOD2>:[TID]:<aid>:[CTAG]; where: • aid is the AID ALL
Example	Input DLT-EC1:CISCO:FAC-1-1:123;
Errors	This message generates all the default errors

11.11.5 DLT-CRS-<STS_PATH>: Delete Cross Connect (STS1, STS3C, STS12C)

This command deletes a cross-connect between STS paths. STS paths are specified using their STS AID.

Section	Description
Category	Cross Connect
Security	N/A
Related Messages	DLT-CRS-VT1 ED-CRS-<STS_PATH> ED-CRS-VT1 ENT-CRS-<STS_PATH> ENT-CRS-VT1 RTRV-CRS-<STS_PATH> RTRV-CRS-VT1
Input Format	DLT-CRS-<STS_PATH>:[TID]:<from>,<to>:[CTAG]:::; where: • from is the source aid of the cross sts connection and is the AID sts • to is the destination aid of the crs sts connection and is the AID sts
Example	Input DLT-CRS-STS12C:VINBURG:STS-1-1, STS-12-1:102:::;

Section	Description (continued)
Errors	This message generates all the default errors

11.11.6 DLT-CRS-VT1: Delete Cross Connect Virtual Tributary

This command deletes the VT1 cross connects.

Section	Description
Category	Cross Connect
Security	N/A
Related Messages	DLT-CRS-<STS_PATH> ED-CRS-<STS_PATH> ED-CRS-VT1 ENT-CRS-<STS_PATH> ENT-CRS-VT1 RTRV-CRS-<STS_PATH> RTRV-CRS-VT1
Input Format	DLT-CRS-VT1:[TID]:<from>,<to>:[CTAG]:::; where: • from is the source aid of the vt connection and is the AID vt1_5 • to is the destination aid of the crs vt connection and is the AID vt1_5
Example	Input DLT-CRS-VT1:CISCO:VT1-2-3-1,VT1-4-4-1:1234:::;
Errors	This message generates all the default errors

11.11.7 DLT-EQPT: Delete Equipment

This command deletes a card from the NE. It removes the card type and attributes that were entered for a particular slot. If any facilities are assigned, they are also deleted as long as they do not contain any cross-connect end-points, the cards are not in a protection group and they are not in SDCC termination. If any of the above descriptions exist, the command will be denied.

Section	Description	
Category	Equipment	
Security	N/A	
Related Messages	DLT-FFP-EQPT	RLS-PROTNSW-EQPT
	ED-FFP-EQPT	RTRV-ALM-EQPT
	ENT-EQPT	RTRV-COND-EQPT
	ENT-FFP-EQPT	RTRV-EQPT
	OPR-PROTNSW-EQPT	RTRV-FFP-EQPT
	REPT ALM EQPT	SW-DX-EQPT
	REPT EVT EQPT	

Section	Description (continued)
Input Format	DLT-EQPT:[TID]:<eqpt_aid>:[CTAG]; where: • equip_aid is the AID eqpt
Example	Input DLT-EQPT:SONOMA:SLOT-1:104;
Errors	This message generates all the default errors

11.11.8 DLT-FFP-<OCN_TYPE>: Delete Facilities Protection Group (OC3, OC12, OC48)

This command deletes a linear protected group on optical cards.

Section	Description
Category	Facility Protection
Security	N/A
Related Messages	N/A
Input Format	DLT-FFP-<OCN_TYPE>:[TID]:<work>,<protect>:[CTAG]; where: • work is the working equipment and the AID facility • protect is the protection equipment and the AID facility
Example	Input DLT-FFP-OC3:PETALUMA:FAC-2-1,FAC-1-1:1;
Errors	This message generates all the default errors

11.11.9 DLT-FFP-EQPT: Delete Facilities Protection Equipment

This command deletes an equipment protection group.

Section	Description	
Category	Equipment	
Security	N/A	
Related Messages	DLT-EQPT	RLS-PROTNSW-EQPT
	ED-FFP-EQPT	RTRV-ALM-EQPT
	ENT-EQPT	RTRV-COND-EQPT
	ENT-FFP-EQPT	RTRV-EQPT
	OPR-PROTNSW-EQPT	RTRV-FFP-EQPT
	REPT ALM EQPT	SW-DX-EQPT
	REPT EVT EQPT	

Section	Description (continued)
Input Format	DLT-FFP-EQPT:[TID]:<work>,<protect>:[CTAG]; where: • work is the AID eqpt • protect is the AID eqpt
Example	Input DLT-FFP-EQPT:PETALUMA:SLOT-2,SLOT-1:1;
Errors	This message generates all the default errors

11.11.10 DLT-USER-SECU: Delete User Security

This command removes a user and can only be used by an administrator. The AID block contains the user identifier. If this command is executed while the user is logged on, the current session for that user continues. Once the user logs out, the same userid cannot be used to log in again. This command is defined in TR-835.

Section	Description
Category	Security
Security	Admin
Related Messages	ACT-USER CANC-USER ED-PID ED-USER-SECU ENT-USER-SECU
Input Format	DLT-USER-SECU:[TID]:<username>:[CTAG]; where: • username is a String
Example	Input DLT-USER-SECU:CISCO:UID:123;
Errors	This message generates all the default errors

11.11.11 ED-<OCN_TYPE>: Edit (OC3, OC12, OC48)

This command modifies the attributes (i.e. service parameters) and state of an OC-N facility. Allowable states for a facility are Out of Service (OOS) and In Service (IS).

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A

Section	Description (continued)
Input Format	ED-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]::[SDCC=<sdcc>], [PJMON=<pjmon>],[SFBER=<sfber>],[SDBER=<sdber>], [MODE=<opticalMode>]:[<pst>]:; **Note** If changing the pst field only, use the following Input Format: ED-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]::[<pst>]:; where: • fac_aid is the AID facility • sdcc enables the Section DCC for this facility and is of type SDCC_MODE • pjmon is the number of the STS facility to monitor for pointer justifications pjmon is an Integer • sfber is of type SF_BER • sdber is of type SD_BER • opticalMode is of type OPTICAL_MODE • pst is the card primary state and is of type PST
Example	Input ED-OC48:PENNGROVE:FAC-6-1:114::SDCC=Y,PJMON=48,SFBER=1E-4, SDBER=1E-6, MODE=SONET:IS:;
Errors	This message generates all the default errors

11.11.12 ED-<STS_PATH>: Edit (STS1, STS3C, STS12C)

This command is used to modify the attributes associated with an STS path.

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A
Input Format	ED-<STS_PATH>:[TID]:<sts_aid>:[CTAG]::[SFBER=[<sfber>], [SDBER=<sdber>]::; where: • sts_aid is the AID sts • sfber is of type SF_BER • sdber is of type SD_BER
Example	Input ED-STS1:FERNDALE:STS-2-4:115::SFBER=1E-3,SDBER=1E-5::;
Errors	This message generates all the default errors

11.11.13 ED-BITS: Edit Building Integrated Timing Supply

This command modifies BITS reference attributes.

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A
Input Format	ED-BITS:[TID]:<bits_aid>:[CTAG]::[LNCDE=<line_code>], [FRMF=<frame_format>]:<pst>:; where: • bits_aid is the AID bits • line_code is the BITS line code and is of type LINE_CODE • frame_format is the BITS frame format and is of type FRAME_FORMAT • pst is the BITS state and is of type PST
Example	Input ED-BITS:SONOMA:BITS-2:779::LNCDE=AMI,FRMF=ESF:IS;
Errors	This message generates all the default errors

11.11.14 ED-CRS-<STS_PATH>: Edit Cross Connect (STS1, STS3C, STS12C)

This command modifies attributes of an STS-level cross-connect. Under certain circumstances, you may change the cross-connect type (e.g. from 1WAY to 2WAY).

Section	Description
Category	Cross Connect
Security	Read/Write
Related Messages	DLT-CRS-<STS_PATH> DLT-CRS-VT1 ED-CRS-VT1 ENT-CRS-<STS_PATH> ENT-CRS-VT1 RTRV-CRS-<STS_PATH> RTRV-CRS-VT1
Input Format	ED-CRS-<STS_PATH>:[TID]:<from>,<dst>:[CTAG]::<cct>::: where: • from is the source aid of the cross sts connection and is the AID sts • dst is the AID sts • cct is the cross connection type and is of type CCT
Example	Input ED-CRS-STS3C:KENWOOD:STS-6-4,STS-12-7:108::2WAY:::;

Section	Description (continued)
Errors	This message generates all the default errors

11.11.15 ED-CRS-VT1: Edit Cross Connect Virtual Tributary

This command edits the VT1.5 cross-connect.

Section	Description
Category	Cross Connect
Security	Read/Write
Related Messages	DLT-CRS-<STS_PATH> DLT-CRS-VT1 ED-CRS-<STS_PATH> ENT-CRS-<STS_PATH> ENT-CRS-VT1 RTRV-CRS-<STS_PATH> RTRV-CRS-VT1
Input Format	ED-CRS-VT1:[TID]:<from>,<to>:[CTAG]::<cct>:::; where: • from is the AID vtl_5 • to is the AID vtl_5 • cct is the cross connection type and is of type CCT
Example	Input ED-CRS-VT1:CISCO:VT1-2-1-1,VT1-4-1-1:1234::1WAY:::;
Errors	This message generates all the default errors

11.11.16 ED-DAT: Edit Date and Time

This command edits the date and time.

Section	Description
Category	System
Security	Read/Write
Related Messages	ACT-USER ALW-MSG-ALL CANC-USER INH-MSG-ALL INIT-SYS RTRV-HDR

Section	Description (continued)
Input Format	ED-DAT:[TID]::[CTAG]::[<date>],[<time>]; where: • date is the date field YYYY-MM-DD or YY-MM-DD; date is a String • time is the time field HH-MM-SS, the hours 0..24; time is a String
Example	Input ED-DAT:TID::1234::99-12-21,14-35-15;
Errors	This message generates all the default errors

11.11.17 ED-EC1: Edit Electrical Carrier Level 1

This command edits EC-1 facilities. This command will edit the properties of an EC-1 card port.

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A
Input Format	ED-EC1:[TID]:<fac>:[CTAG]::[PJMON=<pjmon>][,][LBO=<lbo>]:<pst>:; where: • fac is the facility aid. fac is the AID facility • pjmon is the SONET pointer number 0 or 1 and is an Integer • lbo is the line buildout and is of type E_LBO • pst is the port state and is of type PST
Example	Input ED-EC1:CISCO:FAC-1-1:123::PJMON=0,LBO=0-225:IS:;
Errors	This message generates all the default errors

11.11.18 ED-FFP-<OCN_TYPE>: Edit Facilities Protection Group (OC3, OC12, OC48)

This command edits the optical facility protection.

Section	Description
Category	Facility Protection
Security	Read/Write
Related Messages	N/A

Section	Description (continued)
Input Format	ED-FFP-<OCN_TYPE>:[TID]:<facility>:[CTAG]::[NAME=<name>],[RVTT=<revertiveType>],[RVTM=<revertiveTime>],[BSWM=<bswMode>]; where: • facility is the facility aid and is the AID facility • name is the protection name and is a String • revertiveType is of type REVERTIVE_TYPE • revertiveTime is of type REVERTIVE_TIME • bswMode specifies if it is a bidirectional switch mode and is of type ON_OFF
Example	Input ED-FFP-OC3:PETALUMA:FAC-1-1:1::NAME=PROT_NAME,RVTT=R,RVTM=1.0,BSWM=OFF;
Errors	This message generates all the default errors

11.11.19 ED-FFP-EQPT: Edit Equipment Protection

This command edits an equipment protection group.

Section	Description	
Category	Equipment	
Security	Read/Write	
Related Messages	DLT-EQPT DLT-FFP-EQPT ENT-EQPT ENT-FFP-EQPT OPR-PROTNSW-EQPT REPT ALM EQPT REPT EVT EQPT	RLS-PROTNSW-EQPT RTRV-ALM-EQPT RTRV-COND-EQPT RTRV-EQPT RTRV-FFP-EQPT SW-DX-EQPT
Input Format	ED-FFP-EQPT:[TID]:<eqpt>:[CTAG]::[NAME=<name>],[RVTT=<revertiveType>],[RVTM=<revertiveTime>]; where: • eqpt is the equipment aid and is the AID eqpt • name is the name of the group and is a String • revertiveType is of type REVERTIVE_TYPE • revertiveTime is of type REVERTIVE_TIME	
Example	Input ED-FFP-EQPT:PETALUMA:SLOT-1:1::NAME=PROT_NAME,RVTT=R,RVTM=1.0;	
Errors	This message generates all the default errors	

11.11.20 ED-NE: Edit Network Element

This command modifies the attributes of the NE system such as changing the node's identity (e.g. IP address), external interfaces (e.g. LAN ports), and major modes of operation (e.g. SONET vs. SDH).

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A
Input Format	ED-NE:[TID]::[CTAG]:::[NAME=<name>],[IPADDR=<ipaddr>], [IPMASK=<ipmask>],[DEFRTR=<defrtr>],[TMMD=<timing_mode>], [SSMG=<sync_gen>],[NSQL=<sync_quality_level>]; where: • name is the System Identifier (SID/TID) of the NE and must be 20 characters or less; name is a String • ipaddr is the IP address of the NE on the local LAN and is a String • ipmask is the IP Mask used to identify the sub-net on which the NE resides; ipmask is a String • defrtr is the IP address of the default router and is a String • timing_mode is of type TIMING_MODE • sync_gen is of type SYNC_GENERATION • sync_quality_level is of type SYNC_QUALITY_LEVEL
Example	Input ED-NE:LKVLL::111:::NAME=LAKEVILLE,IPADDR=192.168.100.52, IPMASK=255.255.255.0,DEFRTR=192.168.100.1,TMMD=LINE, SSMG=GEN1,NSQL=ABOVE-PRS;
Errors	This message generates all the default errors

11.11.21 ED-PID: Edit Private Identifier

This command allows a user to change their own password. Other user identification and access changes may only be made by a superuser. This command is defined in TR-835.

Note The password cannot be null. It will be echoed as clear text as the message is parsed and only after the complete message is entered and terminated.

Note The password should not appear in the TL1 log on the NE.

Section	Description
Category	Security
Security	Read/Write

Section	Description (continued)
Related Messages	ACT-USER CANC-USER DLT-USER-SECU ED-USER-SECU ENT-USER-SECU
Input Format	ED-PID:[TID]:<username>:[CTAG]::<oldPassword>,<newPassword>; where: • username is a String • oldPassword is a String • newPassword is a String
Example	Input ED-PID:CISCO:UID:123::OLD_PASSWORD,NEW_PASSWORD;
Errors	This message generates all the default errors

11.11.22 ED-SYNCN: Edit Synchronization

This command modifies the synchronization reference list used to determine the sources for the NE's reference clock and the BITS output clock. For each clock, up to three synchronization sources may be specified (for example, PRIMARY, SECOND, THIRD).

Section	Description
Category	Synchronization
Security	Read/Write
Related Messages	REPT ALM SYNCN REPT EVT SYNCN RTRV-ALM-SYNCN RTRV-COND-SYNCN RTRV-SYNCN
Input Format	ED-SYNCN:[TID]:<sync_aid>:[CTAG]:::[PRIMARY=<primary>],[SECOND=<second>],[THIRD=<third>]:; where: • sync_aid is the synchronization reference to be modified; sync_aid is the AID sync_ref and is listable • primary is the AID syn_src • second is the AID syn_src • third is the AID syn_src
Example	Input ED-SYNCN:BOYES:SYNC-NE:112:::PRIMARY=INTERNAL,SECOND=INTERNAL,THIRD=INTERNAL:;
Errors	This message generates all the default errors

11.11.23 ED-T1: Edit T1

This command modifies the attributes related to a DS-1 port.

Section	Description
Category	Other
Security	Read/Write
Related Messages	ED-T3 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-T1 RLS-LPBK-T3 RTRV-T1 RTRV-T3
Input Format	ED-T1:[TID]:<tl1_aid>:[CTAG]::[ID=<id>],[LNCDE=<line_code>],[FRMF=<frame_format>],[LBO=<line_buildout>]:[<pst>]:; where: • t1_aid is the AID facility • id is a String • line_code is the port line code and is of type LINE_CODE • frame_format is of type FRAME_FORMAT • line_buildout is the port line buildout and is of type LINE_BUILDOUT • pst is of type PST
Example	Input ED-T1:CISCO:FAC-1-1:1223::ID=CISCO,LNCDE=AMI,FRMF=ESF,LBO=0-131:IS:;
Errors	This message generates all the default errors

11.11.24 ED-T3: Edit T3

This command edits a DS-3 and DS-3 transmux card.

Section	Description
Category	Other
Security	Read/Write
Related Messages	ED-T1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-T1 RLS-LPBK-T3 RTRV-T1 RTRV-T3

Section	Description (continued)
Input Format	ED-T3:[TID]:<facility>:[CTAG]::[LNTYPE=<lineType>], [LNCODE=<lineCode>],[LB0=<lbo>][<pst>]; where: • facility is the AID facility • lineType is the port line type and is of type DS_LINE_TYPE • lineCode is the line code and is the lineCode of the DS3XM card; lineCode is of type DS_LINE_CODE • lbo is the circuit line buildout and is of type E_LBO • pst is of type PST
Example	Input ED-T3:CISCO:FAC-1-2:123::LNTYPE=C-BIT,LNCODE=B3ZS,LBO=0-225: IS:;
Errors	This message generates all the default errors

11.11.25 ED-USER-SECU: Edit User Security

This command edits a user's privileges, password, or ID. Only a user with R/W admin privileges may perform this operation. Privilege levels are described in the ENT-USER-SECU: Enter User Security command. This command is defined in TR-835.

Note If the password is changed with this command, the password should be blanked out in the TL1 log.

Section	Description
Category	Security
Security	Admin
Related Messages	ACT-USER CANC-USER DLT-USER-SECU ED-PID ENT-USER-SECU
Input Format	ED-USER-SECU:[TID]:<username>:[CTAG]::[PASSWORD=<password>], [PRIVILEGE=<privilege>]; where: • username is a String • password is a String • privilege is of type PRIVILEGE
Example	Input ED-USER-SECU:CISCO:UID:123::PASSWORD=PASSWORD, PRIVILEGE=MAINT;
Errors	This message generates all the default errors

11.11.26 ENT-<MOD2>: Enter (DS1, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command puts a facility or an aid in service.

Note ENT-DS1/STS1/STS3C/STS12C/STS48C/VT1 are not supported in Release 2.2.1.

Section	Description
Category	Other
Security	Admin
Related Messages	N/A
Input Format	ENT-<MOD2>:[TID]:<aid>:[CTAG]; where: • aid is the aid to be put in service and is the AID ALL
Example	Input ENT-OC3:CISCO:FAC-1-1:1243;
Errors	This message generates all the default errors

11.11.27 ENT-CRS-<STS_PATH>: Enter Cross Connect (STS1, STS3C, STS12C)

This command creates an STS cross-connect between two or more STS paths. Rather than create each individual unidirectional connection singularly, this command accepts cross-connection types (CCT) that identify aggregate cross-connects based on their function in the network. To enter a cross-connect, the facilities that support the STS paths must be either in service or out of service assigned. If a cross-connect (XC) card is not present in the system or if the paths have incompatible payload types, the request is denied.

Section	Description
Category	Cross Connect
Security	Admin
Related Messages	DLT-CRS-<STS_PATH> DLT-CRS-VT1 ED-CRS-<STS_PATH> ED-CRS-VT1 ENT-CRS-VT1 RTRV-CRS-<STS_PATH> RTRV-CRS-VT1

Section	Description (continued)
Input Format	ENT-CRS-<STS_PATH>:[TID]:<from>,<to>:[CTAG]::<cct>::: where: • from is the source aid of the cross sts connection and is the AID sts • to is the destination aid of the crs sts connection and is the AID sts • cct is the cross connection type and is of type CCT
Example	Input ENT-CRS-STS1:BODEGA:STS-1-5,STS-2-5:116::2WAY:::;
Errors	This message generates all the default errors

11.11.28 ENT-CRS-VT1: Enter Cross Connect Virtual Tributary

This command creates a VT1 cross connect.

Section	Description
Category	Cross Connect
Security	Admin
Related Messages	DLT-CRS-<STS_PATH> DLT-CRS-VT1 ED-CRS-<STS_PATH> ED-CRS-VT1 ENT-CRS-<STS_PATH> RTRV-CRS-<STS_PATH}> RTRV-CRS-VT1
Input Format	ENT-CRS-VT1:[TID]:<from>,<to>:[CTAG]::<cct>::: where: • from is the source aid of the cross vt connection and is the AID vt1_5 • to is the destination aid of the crs vt connection and is the AID vt1_5 • cct is the cross connection type and is of type CCT
Example	Input ENT-CRS-VT1:CISCO:VT1-2-3-14,VT1-4-4-12:1234::1WAY:::;
Errors	This message generates all the default errors

11.11.29 ENT-EQPT: Enter Equipment

This command enters the card type and attributes for a given equipment slot in the NE. It also automatically enters all facilities supported by the card, assigning default values to all facility and path attributes.

Section	Description
Category	Equipment
Security	Admin

Section	Description (continued)	
Related Messages	DLT-EQPT	RLS-PROTNSW-EQPT
	DLT-FFP-EQPT	RTRV-ALM-EQPT
	ED-FFP-EQPT	RTRV-COND-EQPT
	ENT-FFP-EQPT	RTRV-EQPT
	OPR-PROTNSW-EQPT	RTRV-FFP-EQPT
	REPT ALM EQPT	SW-DX-EQPT
	REPT EVT EQPT	
Input Format	ENT-EQPT:[TID]:<eqpt>:[CTAG]::<eqpt_type>; where: • eqpt is the AID eqpt • eqpt_type is of type EQUIPMENT_TYPE	
Example	Input ENT-EQPT:PETALUMA:SLOT-12:118::OC12;	
Errors	This message generates all the default errors	

11.11.30 ENT-FFP-<OCN_TYPE>: Enter Facilities Protection Group (OC3, OC12, OC48)

This command creates an optical protection.

Section	Description
Category	Facility Protection
Security	Admin
Related Messages	N/A
Input Format	ENT-FFP-<OCN_TYPE>:[TID]:<work>,<protect>:[CTAG]::[NAME=<name>],[RVTM=<rvtm>],[RVTT=<rvtt>],[BSWM=<bswMode>]; where: • work is the working unit aid and is the AID facility • protect is the protection unit aid and is the AID facility • name is the protection name and is a String • rvtm is the revertive mode and is of type REVERTIVE_TYPE • rvtt is the revertive time and of type REVERTIVE_TIME • bswMode specifies if it is bidirectional switch mode and is of type ON_OFF
Example	Input ENT-FFP-OC3:PETALUMA:FAC-2-1,FAC-1-1:1::NAME=PROT_NAME,RVTM=R,RVTT=1.0,BSWM=OFF;
Errors	This message generates all the default errors

11.11.31 ENT-FFP-EQPT: Enter Equipment Protection

This command creates an equipment protection.

Section	Description	
Category	Equipment	
Security	Admin	
Related Messages	DLT-EQPT	RLS-PROTNSW-EQPT
	DLT-FFP-EQPT	RTRV-ALM-EQPT
	ED-FFP-EQPT	RTRV-COND-EQPT
	ENT-EQPT	RTRV-EQPT
	OPR-PROTNSW-EQPT	RTRV-FFP-EQPT
	REPT ALM EQPT	SW-DX-EQPT
	REPT EVT EQPT	
Input Format	ENT-FFP-EQPT:[TID]:<work>,<protect>:[CTAG]::PRT=<protectionGroup>, [NAME=<name>],[RVTM=<rvtm>],[RVTT=<rvtt>]; where: • work is the AID eqpt • protect is the AID eqpt • protectionGroup is the protection group 1-1 or 1-N and is of type PROTECTION_GROUP • name is the protection name and is a String • rvtm is the revertive mode and is of type REVERTIVE_TYPE • rvtt is the revertive time and is of type REVERTIVE_TIME	
Example	Input ENT-FFP-EQPT:PETALUMA:SLOT-2,SLOT-1:1::PRT=1-1, NAME=PROT_NAME,RVTM=R,RVTT=1.0;	
Errors	This message generates all the default errors	

11.11.32 ENT-USER-SECU: Enter User Security

This command adds a user account. Only administrators may do this. The AID block contains the user identifier. See Table 11-10 on page 11-15.

There are seven security levels defined for the TalonMX. Each user may be configured as possessing 1or more of these seven privileges.

1 Read-Only Alarms: Users possessing this security level can retrieve and receive autonomous alarms.

2 Read-Write Alarms: Users possessing this security level can manage as well as receive/retrieve alarm information.

3 Read-Only Provisioning: Users possessing this security level can retrieve TalonMX provisioning values.

4 Read-Write Provisioning: Users possessing this security level can set/retrieve TalonMX provisioning values.

5 Read-Only Administrative: Users possessing this security level can retrieve TalonMX security settings.

6 Read-Write Administrative: Users possessing this security level can set/retrieve TalonMX security settings.

7 Read-Write Maintenance: Users possessing this security level can perform maintenance functions such as operating/releasing loopbacks.

A superuser will have all privileges shown above.

This command is defined in TR-835.

Section	Description
Category	Security
Security	Admin
Related Messages	ACT-USER CANC-USER DLT-USER-SECU ED-PID ED-USER-SECU
Input Format	ENT-USER-SECU:[TID]:<username>:[CTAG]::<password>,<privilege>; where: • username is a String • password is the user login password and is a String • privilege is the user security level and is of type PRIVILEGE; Superuser=super, Provision=prov, Maintenance=maint, Retrieve=rtrv
Example	Input ENT-USER-SECU:CISCO:UID:123::PSWD,MAINT;
Errors	This message generates all the default errors

11.11.33 INH-MSG-ALL: Inhibit Message All

This command instructs the NE to enter a mode that prevents all automatic messages from being transmitted.

Section	Description
Category	System
Security	N/A
Related Messages	ACT-USER ALW-MSG-ALL CANC-USER ED-DAT INIT-SYS RTRV-HDR
Input Format	INH-MSG-ALL:[TID]::[CTAG]::,,;

Section	Description (continued)
Example	Input INH-MSG-ALL:PETALUMA::550::,,;
Errors	This message generates all the default errors

11.11.34 INIT-REG-<MOD2>: Initialize Register (DS1, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command initializes the performance monitoring registers.

Section	Description
Category	Performance
Security	Read/Write
Related Messages	RTRV-PM-<MOD2> RTRV-TH-<MOD2> SET-TH-<MOD2>
Input Format	INIT-REG-<MOD2>:[TID]:<aid>:[CTAG]::,,,,<tmpr>,,; where: • aid is the AID facility • tmpr is of type TMPR
Example	Input INIT-REG-OC3:TID:FAC-1-1:1234::,,,,15MIN,,;
Errors	This message generates all the default errors

11.11.35 INIT-SYS: Initialize System

This command instructs the NE to initialize the specified card and its associated subsystem(s). The command supports various levels of restart, called phases, ranging from a warm start to a cold start.

Note In Release 2.2.1 this command only resets equipment. The phase parameter is not supported in this release.

Section	Description
Category	System
Security	Read/Write
Related Messages	ACT-USER ALW-MSG-ALL CANC-USER ED-DAT INH-MSG-ALL RTRV-HDR

Section	Description (continued)
Input Format	INIT-SYS:[TID]:<eqpt_aid>:[CTAG]::[<phase>]; where: • eqpt-aid is the AID eqpt • phase is the level of initialization to take place; the higher the number the stronger the reset, A phase=1 is a warm start and A phase=10 is a cold start; phase is an Integer
Example	Input INIT-SYS:HOTWATER:SLOT-1:201::3;
Errors	This message generates all the default errors

11.11.36 OPR-LPBK-<OCN_TYPE>: Operate Loopback (OC3, OC12, OC48)

This command instructs the NE to operate a loopback on a specified OC-N facility.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T1 RLS-LPBK-T3
Input Format	OPR-LPBK-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]::,,,,<lpbktype>; where: • fac_aid is the AID facility • lpbktype identifies the type of loopback (Terminal or Facility) to be established and is of type LPBK_TYPE
Example	Input OPR-LPBK-OC3:PTREYES:FAC-5-12:203::,,,FACILITY;
Errors	This message generates all the default errors

11.11.37 OPR-LPBK-DS1: Operate Loopback Digital Signal Level 1

This command operates a DS-1 signal loopback on a DS3XM-6 card.

Note The TERMINAL loopback type is not supported for this command.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	OPR-LPBK-<OCN_TYPE> OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T1 RLS-LPBK-T3
Input Format	OPR-LPBK-DS1:[TID]:<ds>:[CTAG]::,,,<lpbkType>; where: • ds is the aid for the DS3XM card on the ds-1 and is the AID ds-1 • lpbkType is the loop back type **Note** The terminal loop back type is not supported for the DS3XM in Release 2.2.1. lpbkType is of type LPBK_TYPE
Example	Input OPR-LPBK-DS1:PTREYES:DS1-4-2-13:203::,,,FACILITY;
Errors	This message generates all the default errors

11.11.38 OPR-LPBK-EC1: Operate Loopback Electrical Carrier Level 1

This command operates the loopback on an EC-1 facility.

Section	Description
Category	Testing
Security	Read/Write

Section	Description (continued)
Related Messages	OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T1 RLS-LPBK-T3
Input Format	OPR-LPBK-EC1:[TID]:<facility>:[CTAG]::,,,<lpbkType>; where: • facility is the facility aid for the EC-1 and is the AID facility • lpbkType is the loop back type and is of type LPBK_TYPE
Example	Input OPR-LPBK-EC1:PTREYES:FAC-4-2:203::,,,FACILITY;
Errors	This message generates all the default errors

11.11.39 OPR-LPBK-T1: Operate Loopback T1

This command operates the loopback for a DS-1 facility.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	ED-T1 ED-T3 OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T1 RLS-LPBK-T3 RTRV-T1 RTRV-T3
Input Format	OPR-LPBK-T1:[TID]:<fac>:[CTAG]::,,,<lpbk_type>; where: • fac is the AID facility • lpbk_type is the loop back type for the DS-1 cards and is of type LPBK_TYPE

Section	Description (continued)
Example	Input OPR-LPBK-T1:PTREYES:FAC-4-12:203::,,,FACILITY;
Errors	This message generates all the default errors

11.11.40 OPR-LPBK-T3: Operate Loopback T3

This command instructs the NE to operate a loopback on a specified T3 facility.

Section	Description	
Category	Testing	
Security	Read/Write	
Related Messages	ED-T1	RLS-LPBK-DS1
	ED-T3	RLS-LPBK-EC1
	OPR-LPBK-<OCN_TYPE>	RLS-LPBK-T1
	OPR-LPBK-DS1	RLS-LPBK-T3
	OPR-LPBK-EC1	RTRV-T1
	OPR-LPBK-T1	RTRV-T3
	RLS-LPBK-<OCN_TYPE>	
Input Format	OPR-LPBK-T3:[TID]:<fac_aid>:[CTAG]::,,,<lpbktype>; where: • fac_aid is the AID facility • lpbktype identifies the loopback type (Terminal or Facility) to be established and is of type LPBK_TYPE	
Example	Input OPR-LPBK-T3:SCHELLVILLE:FAC-2-11:202::,,,TERMINAL;	
Errors	This message generates all the default errors	

11.11.41 OPR-PROTNSW-<OCN_TYPE>: Operate Protection Switch (OC3, OC12, OC48)

This command instructs the NE to initiate a SONET line protection switch request. User switch requests initiated with this command remain active until they are released via the RLS-PROTNSW-OCN command or are overridden by a higher priority protection switch request.

Section	Description
Category	Switch
Security	Read/Write
Related Messages	N/A

Section	Description (continued)
Input Format	OPR-PROTNSW-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]::<dnField>; where: • fac_aid is the AID facility and is listable • dnField is the switch mode and is of type SWITCH
Example	Input OPR-PROTNSW-OC48:CHICKALUMA:FAC-2-1:204::LOCKOUT;
Errors	This message generates all the default errors

11.11.42 OPR-PROTNSW-EQPT: Operate Protection Switch Equipment

This command initiates a protection switch. The RLS-PROTNSW-EQPT command can be used to release a switch condition.

Section	Description	
Category	Equipment	
Security	Read/Write	
Related Messages	DLT-EQPT DLT-FFP-EQPT ED-FFP-EQPT ENT-EQPT ENT-FFP-EQPT REPT ALM EQPT REPT EVT EQPT	RLS-PROTNSW-EQPT RTRV-ALM-EQPT RTRV-COND-EQPT RTRV-EQPT RTRV-FFP-EQPT SW-DX-EQPT
Input Format	OPR-PROTNSW-EQPT:[TID]:<eqpt_aid>:[CTAG]::<sc>; where: • eqpt_aid is the equipment aid and is the AID eqpt • sc is the protection switch mode and is of type PROT_MOD_OP	
Example	Input OPR-PROTNSW-EQPT:LASLOMAS:SLOT-1:205::FRCD;	
Errors	This message generates all the default errors	

11.11.43 OPR-UPGRADE: Operate Upgrade

This command operates upgrades.

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A

Section	Description (continued)
Input Format	OPR-UPGRADE:[TID]:<eqpt_aid>:[CTAG]; where: • eqpt_aid is the AID eqpt
Example	Input OPR-UPGRADE:FOUNTAINGROVE:SLOT-1:204;
Errors	This message generates all the default errors

11.11.44 REPT ALM <MOD2>: Report Alarm (DS1, E100, E1000, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

Reports an alarm condition against a facility or a line.

Note The STS alarms are reported as STS1 alarms.

Section	Description	
Category	Fault	
Security	Read Only	
Related Messages	REPT ALM BITS	RTRV-ALM-BITS
	REPT ALM ENV	RTRV-ALM-ENV
	REPT ALM EQPT	RTRV-ALM-EQPT
	REPT ALM SYNCN	RTRV-ALM-SYNCN
	REPT EVT <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT EVT EQPT	RTRV-COND-ALL
	REPT EVT SYNCN	RTRV-COND-BITS
	RTRV-ALM-<MOD2ALM>	RTRV-COND-EQPT
	RTRV-ALM-ALL	RTRV-COND-SYNCN
Output Format	SID DATE TIME ** ATAG REPT ALM <MOD2ALM> "<ds1Aid>:<ntfcncde>,<condition>,<srveff>,,,,:[<desc>],<eqptType>" ; where: • ds1aid is the AID ds1 • ntfcncde is the 2-letter notification code and is of type NOTIF_CODE • condition is of type CONDITION • srveff is the effect on service caused by the alarm condition; srveff is of type SERV_EFF. • desc is a String • eqptType is of type EQPT_TYPE	

Section	Description (continued)
Example	Output TID-000 98-06-20 14-30-00 ** 001 REPT ALM DS1 "DS1-14-3-5:MJ,LPBKFACILITY,SA,,,,:\"LOOP BACK ACTIVE\", DS3XM-6" ;

11.11.45 REPT ALM BITS: Report Alarm Building Integrated Timing Supply

Reports an alarm condition on a BITS facility.

Section	Description	
Category	Fault	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-BITS
	REPT ALM ENV	RTRV-ALM-ENV
	REPT ALM EQPT	RTRV-ALM-EQPT
	REPT ALM SYNCN	RTRV-ALM-SYNCN
	REPT EVT <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT EVT EQPT	RTRV-COND-ALL
	REPT EVT SYNCN	RTRV-COND-BITS
	RTRV-ALM-<MOD2ALM>	RTRV-COND-EQPT
	RTRV-ALM-ALL	RTRV-COND-SYNCN
Output Format	SID DATE TIME ** ATAG REPT ALM BITS "<bits_aid>:<ntfcncde>,<condition>,<srveff>,,,,:[<desc>]" ; where: • bits_aid is the AID bits • ntfcncde is the 2-letter notification code and is of type NOTIF_CODE • condition is a type of alarm condition and is of type CONDITION • srveff is the effect on service caused by the alarm condition; srveff is of type SERV_EFF • desc is a String	
Example	Output TID-000 98-06-20 14-30-00 ** 001 REPT ALM BITS "BITS-1:MJ,SYNC,SA,,,,:\"LOSS OF TIMING\"," ;	

11.11.46 REPT ALM ENV: Report Alarm Environment

Reports a customer-defined condition on an environmental alarm input.

Section	Description	
Category	Environment	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-BITS
	REPT ALM BITS	RTRV-ALM-EQPT
	REPT ALM EQPT	RTRV-ALM-SYNCN
	REPT ALM SYNCN	RTRV-COND-<MOD2ALM>
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
	RTRV-ALM-ALL	
Output Format	SID DATE TIME ** ATAG REPT ALM ENV "<env_aid>:<ntfcnnde>,<almtype>,,,<desc>" ; where: • env_aid is AID env • ntfcncde is of type NOTIF_CODE • almtype is of type ENV_ALM • desc is a String	
Example	Output TID-000 98-06-20 14-30-00 ** 001 REPT ALM ENV "ENV-IN-1:MJ,OPENDR,,,\"OPEN DOOR\"" ;	
Errors	This message generates all the default errors	

11.11.47 REPT ALM EQPT: Report Alarm Equipment

Reports an alarm condition against an equipment unit or slot.

Section	Description
Category	Equipment
Security	Read Only

Section	Description (continued)	
Related Messages	DLT-EQPT	RTRV-ALM-<MOD2ALM>
	DLT-FFP-EQPT	RTRV-ALM-ALL
	ED-FFP-EQPT	RTRV-ALM-BITS
	ENT-EQPT	RTRV-ALM-ENV
	ENT-FFP-EQPT	RTRV-ALM-EQPT
	OPR-PROTNSW-EQPT	RTRV-ALM-SYNCN
	REPT ALM <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT ALM BITS	RTRV-COND-ALL
	REPT ALM ENV	RTRV-COND-BITS
	REPT ALM SYNCN	RTRV-COND-EQPT
	REPT EVT <MOD2ALM>	RTRV-COND-SYNCN
	REPT EVT EQPT	RTRV-EQPT
	REPT EVT SYNCN	RTRV-FFP-EQPT
	RLS-PROTNSW-EQPT	SW-DX-EQPT
Output Format	SID DATE TIME ** ATAG REPT ALM EQPT “<eqpt>:<ntfcncde>,<condition>,<srveff>,,,,,<desc>,<eqptType>” ; where: • eqpt is the equipment aid SLOT-{1-17} and is the AID eqpt • ntfcncde is the 2-letter notification code and is of type NOTIF_CODE • condition is the type of alarm condition and is of type CONDITION • srveff is the effect on service caused by the alarm condition and is of type SERV_EFF • desc is a String • eqptType is of type EQPT_TYPE	
Example	Output TID-000 98-06-20 14-30-00 ** 001 REPT ALM EQPT “SLOT-7:MN,CONTR,NSA,,,,:\”CONTROLLER FAILURE\”,TCC” ;	

11.11.48 REPT ALM SYNCN: Report Alarm Synchronization

Reports an alarm condition against a synchronization reference.

Section	Description
Category	Synchronization
Security	Read Only

Section	Description (continued)	
Related Messages	ED-SYNCN	RTRV-ALM-BITS
	REPT ALM <MOD2ALM>	RTRV-ALM-ENV
	REPT ALM BITS	RTRV-ALM-EQPT
	REPT ALM ENV	RTRV-ALM-SYNCN
	REPT ALM EQPT	RTRV-COND-<MOD2ALM>
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
	RTRV-ALM-ALL	RTRV-SYNCN
Output Format	SID DATE TIME ** ATAG REPT ALM SYNCN "<sync_aid>:<ntfcncde>,<condition>,<srveff>,,,,:<desc>" ; where: • sync_aid is the identifier of Synchronization Reference with alarm condition; sync_aid is the AID sync_ref • ntfcncde is the 2-letter notification code and is of type NOTIF_CODE • condition is the type of alarm condition and is of type CONDITION • srveff is the effect on service caused by the alarm condition and is of type SERV_EFF • desc is a String	
Example	Output TID-000 98-06-20 14-30-00 ** 001 REPT ALM SYNCN "SYNC-NE:MJ,MAN,SA,,,,:\"MANUAL SWITCH\"," ;	

11.11.49 REPT EVT <MOD2ALM>: Report Event (DS1, E100, E1000, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

Reports the occurrence of a non-alarmed event.

Section	Description
Category	Fault
Security	Read Only

Section	Description (continued)	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-BITS
	REPT ALM BITS	RTRV-ALM-ENV
	REPT ALM ENV	RTRV-ALM-EQPT
	REPT ALM EQPT	RTRV-ALM-SYNCN
	REPT ALM SYNCN	RTRV-COND-<MOD2ALM>
	REPT EVT EQPT	RTRV-COND-ALL
	REPT EVT SYNCN	RTRV-COND-BITS
	RTRV-ALM-<MOD2ALM>	RTRV-COND-EQPT
	RTRV-ALM-ALL	RTRV-COND-SYNCN
Output Format	SID DATE TIME A ATAG REPT EVT <MOD2ALM> "<fac_aid>:<condition>,[<condeff>],,,[<location>],,[<monval>], [<th_val>],[<tmpr>]:<desc>,<eqptType>" ; where: • fac_aid is the identifier of the OC-N facility with the condition and is the AID facility • condition is of type CONDITION • condeff is the effect of the condition on the NE; condeff is of type COND_EFF and is optional • location is of type LOCATION and is optional • monval is the monitored value and is optional • th_val is the threshold value; th_val is an Integer and is optional • tmpr is the time period; tmpr is of type TMPR and is optional • desc is a String • eqptType is of type EQPT_TYPE	
Example	Output TID-000 98-06-20 14-30-00 A 001 REPT EVT T3 "FAC-4-1:WKSWPR,TC,,,FEND,,12,13,15MIN:\"WORKING SWITCH TO PROTECTION\",DS3-12" ;	

11.11.50 REPT EVT EQPT: Report Event Equipment

Reports the occurrence of a non-alarmed event against an equipment unit or slot.

Section	Description
Category	Equipment
Security	Read Only

Section	Description (continued)	
Related Messages	DLT-EQPT	RTRV-ALM-<MOD2ALM>
	DLT-FFP-EQPT	RTRV-ALM-ALL
	ED-FFP-EQPT	RTRV-ALM-BITS
	ENT-EQPT	RTRV-ALM-ENV
	ENT-FFP-EQPT	RTRV-ALM-EQPT
	OPR-PROTNSW-EQPT	RTRV-ALM-SYNCN
	REPT ALM <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT ALM BITS	RTRV-COND-ALL
	REPT ALM ENV	RTRV-COND-BITS
	REPT ALM EQPT	RTRV-COND-EQPT
	REPT ALM SYNCN	RTRV-COND-SYNCN
	REPT EVT <MOD2ALM>	RTRV-EQPT
	REPT EVT SYNCN	RTRV-FFP-EQPT
	RLS-PROTNSW-EQPT	SW-DX-EQPT
Output Format	SID DATE TIME A ATAG REPT EVT EQPT "<eqpt>:<condition>,<condeff>,<eqptType>,,,,,:[<desc>]" ; where: • eqpt is the slot number of the equipment and is the AID eqpt • condition is the type of event and is of type CONDITION • condeff is the effect of the condition on the NE; condeff is of type COND_EFF • eqptType is the equipment type and is of type EQPT_TYPE • desc is a String	
Example	Output TID-000 98-06-20 14-30-00 A 001 REPT EVT EQPT "SLOT-7:,PLUGIN,TC,TCC,,,,,:\"EQUIPMENT PLUG-IN\"," ;	

11.11.51 REPT EVT SYNCN: Report Event Synchronization

Reports the occurrence of a non-alarmed event against a synchronization entity.

Section	Description
Category	Synchronization
Security	Read Only

Section	Description (continued)	
Related Messages	ED-SYNCN	RTRV-ALM-BITS
	REPT ALM <MOD2ALM>	RTRV-ALM-ENV
	REPT ALM BITS	RTRV-ALM-EQPT
	REPT ALM ENV	RTRV-ALM-SYNCN
	REPT ALM EQPT	RTRV-COND-<MOD2ALM>
	REPT ALM SYNCN	RTRV-COND-ALL
	REPT EVT <MOD2ALM>	RTRV-COND-BITS
	REPT EVT EQPT	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
	RTRV-ALM-ALL	RTRV-SYNCN
Output Format	SID DATE TIME A ATAG REPT EVT SYNCN "<sync_aid>:<condition>,<condeff>,,,,,,:[<desc>]" ; where: • sync_aid is the identifier of the synchronization entity with the condition; sync_aid is the AID sync_ref • condition is of type CONDITION • condeff is of type COND_EFF • desc is a String	
Example	Output TID-000 98-06-20 14-30-00 A 001 REPT EVT SYNCN "SYNC-NE:SWTOINT,SC,,,,,,:\"SWITCH TO INTERNAL CLOCK\"," ;	

11.11.52 RLS-LPBK-<OCN_TYPE>: Release Loopback (OC3, OC12, OC48)

This command instructs the NE to release a loopback on the specified OC-N facility.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T1 RLS-LPBK-T3

Section	Description (continued)
Input Format	RLS-LPBK-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]::,,,[<lpbktype>]; where: • fac_aid is the AID facility • lpbktype is the type of loopback to be released and is of type LPBK_TYPE
Example	Input RLS-LPBK-OC3:PTREYES:FAC-12-1:208::,,,FACILITY;
Errors	This message generates all the default errors

11.11.53 RLS-LPBK-DS1: Release Loopback Digital Signal Level 1

This command releases a DS-1 signal loopback for the DS3XM-6 card.

Note The TERMINAL loopback is not supported.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-EC1 RLS-LPBK-T1 RLS-LPBK-T3
Input Format	RLS-LPBK-DS1:[TID]:<ds1Aid>:[CTAG]::,,,[<lpbkType>]; where: • ds1Aid is the AID ds1 • lpbkType is of type LPBK_TYPE
Example	Input RLS-LPBK-DS1:PTREYES:DS1-4-2-13:203::,,,FACILITY;
Errors	This message generates all the default errors

11.11.54 RLS-LPBK-EC1: Release Loopback Electrical Carrier Level 1

This command releases loopback for an EC-1 facility.

Section	Description
Category	Testing

Section	Description (continued)
Security	Read/Write
Related Messages	OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-T1 RLS-LPBK-T3
Input Format	RLS-LPBK-EC1:[TID]:<facility>:[CTAG]::,,,<lpbkType>; where: • facility is the AID facility • lpbkType is of type LPBK_TYPE
Example	Input RLS-LPBK-EC1:PTREYES:FAC-3-12:203::,,,FACILITY;
Errors	This message generates all the default errors

11.11.55 RLS-LPBK-T1: Release Loopback T1 Facility

This command instructs the NE to release the loopback for the T1 facility.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	ED-T1 ED-T3 OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T3 RTRV-T1 RTRV-T3

Section	Description (continued)
Input Format	RLS-LPBK-T1:[TID]:<fac>:[CTAG]::,,,[<lpbk_type>]; where: • fac releases the loopback for a T1 facility. fac is the AID facility. • lpbk_type is of type LPBK_TYPE.
Example	Input RLS-LPBK-T1:PTREYES:FAC-1-12:203::,,,FACILITY;
Errors	This message generates all of the Default Errors.

11.11.56 RLS-LPBK-T3: Release Loopback T3 Facility

This command instructs the NE to release a loopback on the specified T3 facility.

Section	Description
Category	Testing
Security	Read/Write
Related Messages	ED-T1 ED-T3 OPR-LPBK-<OCN_TYPE> OPR-LPBK-DS1 OPR-LPBK-EC1 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-<OCN_TYPE> RLS-LPBK-DS1 RLS-LPBK-EC1 RLS-LPBK-T1 RTRV-T1 RTRV-T3
Input Format	RLS-LPBK-T3:[TID]:<fac_aid>:[CTAG]::,,,[<lpbk_type>]; where: • fac_aid is the AID facility • lpbktype is the type of loopback to be released; lpbktype is of type LPBK_TYPE.
Example	Input RLS-LPBK-T3:SCHELLVILLE:FAC-6-11:207::,,,TERMINAL;
Errors	This message generates all the default errors

11.11.57 RLS-PROTNSW-<OCN_TYPE>: Release Protection Switch (OC3, OC12, OC48)

Instructs the NE to release a line protection switch request between a working line and a protection line.

Section	Description
Category	Switch
Security	Read/Write
Related Messages	N/A
Input Format	RLS-PROTNSW-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]; where: • fac_aid is the AID facility
Example	Input RLS-PROTNSW-OC48:CHICKALUMA:FAC-6-1:209;
Errors	This message generates all the default errors

11.11.58 RLS-PROTNSW-EQPT: Release Protection Switch Equipment

This command instructs the NE to release a protection switch on an equipment unit.

Section	Description	
Category	Equipment	
Security	Read/Write	
Related Messages	DLT-EQPT	REPT EVT EQPT
	DLT-FFP-EQPT	RTRV-ALM-EQPT
	ED-FFP-EQPT	RTRV-COND-EQPT
	ENT-EQPT	RTRV-EQPT
	ENT-FFP-EQPT	RTRV-FFP-EQPT
	OPR-PROTNSW-EQPT	SW-DX-EQPT
	REPT ALM EQPT	
Input Format	RLS-PROTNSW-EQPT:[TID]:<eqpt_aid>:[CTAG]; where: • eqpt_aid is the AID eqpt	
Example	Input RLS-PROTNSW-EQPT:LASLOMAS:SLOT-3:401;	
Errors	This message generates all the default errors	

11.11.59 RMV-<MOD2>: Remove (DS1, EC1,OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command removes a facility from an in service state to out of service.

Note RMV-DS1/STS1/STS3C/STS12C/STS48C/VT1 are not supported in Release 2.2.1.

Section	Description
Category	Facility
Security	N/A
Related Messages	N/A
Input Format	RMV-<MOD2>:[TID]:<facility>:[CTAG]; where: • facility is the AID facility
Example	Input RMV-EC1:CISCO:FAC-1-1:1234;
Errors	This message generates all the default errors

11.11.60 RST-<MOD2>: Restore (DS1, EC1,OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command provisions a facility in service.

Section	Description
Category	Facility
Security	N/A
Related Messages	N/A
Input Format	RST-<MOD2>:[TID]:<facility>:[CTAG]; where: • facility is the AID facility
Example	Input RST-EC1:CISCO:FAC-1-1:1234;
Errors	This message generates all the default errors

11.11.61 RTRV-<OCN_TYPE>: Retrieve (OC3, OC12, OC48)

This command retrieves the parameters of an OC-N facility.

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-<OCN_TYPE>:[TID]:<fac_aid>:[CTAG]::::; where: • fac_aid is the AID facility and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<fac_aid>:[SDCC=<sdcc>],[TMERGF=<tmgref>],[SPNWTR=<spnwtr>], [PJMON=<pjmon>],[SFBER=<sfber>],[SDBER=<sdber>], [MODE=<mode>],[WVLEN=<wvlen>]:<pst>,,<role>,<status>" ; where: • fac_aid is the AID facility • sdcc is of type SDCC_MODE and is optional • tmgref is of type TMG_REF and is optional • spnwtr is of type REVERTIVE_TIME and is optional • pjmon is an Integer and is optional • sfber is of type SF_BER and is optional • sdber is of type SD_BER and is optional • mode is of type OPTICAL-MODE. mode is optional • wvlen is the optical signal wavelength in nanometers; it is a Float and is optional • pst is of type PST • role is of type SIDE • status is of type STATUS
Example	Input RTRV-OC3:CISCO:FAC-15-2:123::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-15-2:SDCC=N, TMGREF=N, SPNWTR=8.5, PJMON=0, SFBER=1E-4, SDBER=1E-7, MODE=SONET, WVLEN=1310.00:OOS,, WORK,STBY" ;
Errors	This message generates all the default errors

11.11.62 RTRV-<STS_PATH>: Retrieve (STS1, STS3C, STS12C)

This command retrieves the attributes associated with an STS path.

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-<STS_PATH>:[TID]:<sts_aid>:[CTAG]::::; where: • sts_aid is the AID sts and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<sts_aid>:RATE=<stsrate>,[SFBER=<sfber>],[SDBER=<sdber>]" ; where: • sts_aid is the AID sts • stsrate is the STS Rate and is of type STS_PATH • sfber is of type SF_BER and is optional • sdber is of type SD_BER and is optional
Example	Input RTRV-STS1:FERNDALE:STS-2-4:238::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "STS-2-4:RATE=STS1,SFBER=1E-3,SDBER=1E-5" ;
Errors	This message generates all the default errors

11.11.63 RTRV-ALM-<MOD2ALM>:Retrieve Alarm (DS1, E100, E1000, EC1, OC12, OC3, OC48, STS1, STS12C, STS3C, STS48C, T1, T3, VT1)

Instructs the network to retrieve and send the current status of its alarm conditions. The alarm condition or severity to be retrieved can be specified by using the input parameters as a filter.

Section	Description
Category	Fault
Security	Read Only

Section	Description (continued)	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-BITS
	REPT ALM BITS	RTRV-ALM-ENV
	REPT ALM ENV	RTRV-ALM-EQPT
	REPT ALM EQPT	RTRV-ALM-SYNCN
	REPT ALM SYNCN	RTRV-COND-<MOD2ALM>
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-ALL	RTRV-COND-SYNCN
Input Format	RTRV-ALM-<MOD2ALM>:[TID]:<aid>:[CTAG]::[<ntfcncde>],[<condition>],[<serv_eff>],,,; where: • aid is the AID facility and must not be null • ntfcnde is the 2-letter notification code and is of type NOTIF_CODE; a null value is equivalent to “ALL” • condition is a type of alarm condition and is of type CONDITION; condition is listable and a null value is equivalent to “ALL” • serveff of type SERV_EFF and a null value is equivalent to “ALL”	
Output Format	SID DATE TIME M CTAG COMPLD “<aid>,<type>:<ntfcnde>,<condition>,<srveff>,,,,:<desc>” ; where: • aid is the AID facility • type specifies the type of OC-N facility associated with the facility AID; type is of type MOD2ALM • ntfcnde is the 2-letter notification code and is of type NOTIF_CODE • condition is a type of alarm condition and is of type CONDITION • srveff is the type of effect on service caused by the alarm condition and is of type SERV_EFF • desc is a String	
Example	Input RTRV-ALM-OC12:ELDRIDGE:FAC-6-1:255::MN,SD,SA,,,; Output TID-000 98-06-20 14-30-00 M 001 COMPLD “FAC-6-1,OC12:MJ,SD,SA,,,,:\”BER AT SIGNAL DEGRADE LEVEL\”,” ;	
Errors	This message generates all the default errors	

11.11.64 RTRV-ALM-ALL: Retrieve Alarm All

This command instructs the NE to retrieve and send the current status of all active alarm conditions. The alarm condition or severity retrieved is specified using the input parameters as a filter.

Section	Description
Category	Fault
Security	Read Only
Related Messages	REPT ALM <MOD2ALM> REPT ALM BITS REPT ALM ENV REPT ALM EQPT REPT ALM SYNCN REPT EVT <MOD2ALM> REPT EVT EQPT REPT EVT SYNCN RTRV-ALM-<MOD2ALM> RTRV-ALM-BITS RTRV-ALM-ENV RTRV-ALM-EQPT RTRV-ALM-SYNCN RTRV-COND-<MOD2ALM> RTRV-COND-ALL RTRV-COND-BITS RTRV-COND-EQPT RTRV-COND-SYNCN
Input Format	RTRV-ALM-ALL:[TID]::[CTAG]::,,,,,;
Output Format	SID DATE TIME M CTAG COMPLD "<aid>,<aid_type>:<notifCode>,<condition1>,<servEff>,,,,,:<dnField>" ; where: • aid is the aid where the alarm took place and d is the AID ALL • aid_type is of type MOD2 • notifCode is of type NOTIF_CODE • condition1 is of type CONDITION • servEff is a service-affecting alarm and is of type SERV_EFF • dsField is a String
Example	Input RTRV-ALM-ALL:COTATI::229::,,,,,; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "SLOT-2,EQPT:MN,PWRRESTART,NSA,,,,,:\"POWERFAIL RESTART\"," ;
Errors	This message generates all the default errors

11.11.65 RTRV-ALM-BITS: Retrieve Alarm Building Integrated Timing Supply

This command instructs the NE to retrieve and send the current status of its alarm conditions associated with the BITS facility. The alarm condition or severity retrieved is specified using the input parameters as a filter.

Section	Description	
Category	Fault	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-ALL
	REPT ALM BITS	RTRV-ALM-ENV
	REPT ALM ENV	RTRV-ALM-EQPT
	REPT ALM EQPT	RTRV-ALM-SYNCN
	REPT ALM SYNCN	RTRV-COND-<MOD2ALM>
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
Input Format	RTRV-ALM-BITS:[TID]:<bits_aid>:[CTAG]::[<ntfcncde>],[<condition>],[<serv_eff>]; where: • bits_aid is the AID bits and must not be null. • ntfcncde is a 2-letter notification code and is of type NOTIF_CODE; a null value is equivalent to “ALL” • condition is a type of alarm condition and is of type CONDITION; condition is listable and a null value is equivalent to “ALL” • serv_eff is a type of effect on service caused by the alarm condition and is of type SERV_EFF; a null value is equivalent to “ALL”	
Output Format	SID DATE TIME M CTAG COMPLD “<bits_aid>:<ntfcncde>,<condition>,<srveff>,,,,:<desc>” ; where: • bits_aid is the AID bits • ntfcncde is a 2-letter notification code and is of type NOTIF_CODE • condition is a type of alarm condition and is of type CONDITION • srveff is a type of effect on service caused by the alarm condition and is of type SERV_EFF • desc is a String	

Section	Description (continued)
Example	Input RTRV-ALM-BITS:ELVERANO:BITS-1:288::CR,LOS,SA; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "BITS-1:CR,LOS,SA,,,,:\"LOSS OF SIGNAL\"," ;
Errors	This message generates all the default errors

11.11.66 RTRV-ALM-ENV: Retrieve Alarm Environment

This command instructs the NE to retrieve outstanding environmental alarms.

Section	Description	
Category	Environment	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-ALL
	REPT ALM BITS	RTRV-ALM-BITS
	REPT ALM ENV	RTRV-ALM-EQPT
	REPT ALM EQPT	RTRV-ALM-SYNCN
	REPT ALM SYNCN	RTRV-COND-<MOD2ALM>
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
Input Format	RTRV-ALM-ENV:[TID]:[<env>]:[CTAG]::[<notifCode>],[<envAlm>]; where: • env is the AID env and is listable; a null value is equivalent to "ALL" • notifCode is of type NOTIF_CODE and a null value is equivalent to "ALL" • envAlm is of type ENV_ALM and a null value is equivalent to "ALL"	
Output Format	SID DATE TIME M CTAG COMPLD "<env>:<notifCode>,<envAlm>,,,[<desc>]" ; where: • env is the AID env • notifCode is of type NOTIF_CODE • envAlm is of type ENV_ALM • desc is a String	

Section	Description (continued)
Example	Input RTRV-ALM-ENV:CISCO-1:ENV-IN-1:123::MJ,OPENDR; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "ENV-IN-1:MJ,OPENDR,,,\"OPEN DOOR\"" ;
Errors	This message generates all the default errors

11.11.67 RTRV-ALM-EQPT: Retrieve Alarm Equipment

This command instructs the NE to retrieve and send the current status of its equipment-unit alarm conditions. The alarm condition or severity retrieved is specified using the input parameters as a filter.

Section	Description	
Category	Equipment	
Security	Read Only	
Related Messages	DLT-EQPT	RLS-PROTNSW-EQPT
	DLT-FFP-EQPT	RTRV-ALM-<MOD2ALM>
	ED-FFP-EQPT	RTRV-ALM-ALL
	ENT-EQPT	RTRV-ALM-BITS
	ENT-FFP-EQPT	RTRV-ALM-ENV
	OPR-PROTNSW-EQPT	RTRV-ALM-SYNCN
	REPT ALM <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT ALM BITS	RTRV-COND-ALL
	REPT ALM ENV	RTRV-COND-BITS
	REPT ALM EQPT	RTRV-COND-EQPT
	REPT ALM SYNCN	RTRV-COND-SYNCN
	REPT EVT <MOD2ALM>	RTRV-EQPT
	REPT EVT EQPT	RTRV-FFP-EQPT
	REPT EVT SYNCN	SW-DX-EQPT
Input Format	RTRV-ALM-EQPT:[TID]:<eqpt_aid>:[CTAG]::[<ntfcncde>],[<condition>],[<serv_eff>],,,; where: • eqpt_aid is the AID eqpt and must not be null • ntfcncde is a 2-letter notification code and is of type NOTIF_CODE; a null value is equivalent to "ALL" • condition is a type of alarm condition and is of type CONDITION; condition is listable and a null value is equivalent to "ALL" • serv_eff is of type SERV_EFF and is null value is equivalent to "ALL"	

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<eqpt>,<eqpt_type>:<ntfcncde>,<condition>,<srveff>,,,,:<desc>" ; where: • eqpt is the AID eqpt • eqpt_type specifies the type of card associated with the slot AID for equipment units; eqpt_type is of type EQPT_TYPE • ntfcncde is a 2-letter notification code and is of type NOTIF_CODE • condition is a type of alarm condition and is of type CONDITION • srveff is a type of effect on service caused by the alarm condition; srveff is of type SERV_EFF • desc is a String
Example	Input RTRV-ALM-EQPT:TWOROCK:SLOT-7:227::MJ,HITEMP,NSA,,,; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "SLOT-7,TCC:MJ,HITEMP,NSA,,,,:\"HIGH TEMPERATURE\"," ;
Errors	This message generates all the default errors

11.11.68 RTRV-ALM-SYNCN: Retrieve Alarm Synchronization

Instructs the NE to retrieve and send the current status of its alarm conditions associated with a synchronization facility. The alarm condition or severity to be retrieved can be specified by using the input parameters as a filter.

Section	Description	
Category	Synchronization	
Security	Read Only	
Related Messages	ED-SYNCN	RTRV-ALM-ALL
	OPR-SYNCNSW	RTRV-ALM-BITS
	REPT ALM <MOD2ALM>	RTRV-ALM-ENV
	REPT ALM BITS	RTRV-ALM-EQPT
	REPT ALM ENV	RTRV-COND-<MOD2ALM>
	REPT ALM EQPT	RTRV-COND-ALL
	REPT ALM SYNCN	RTRV-COND-BITS
	REPT EVT <MOD2ALM>	RTRV-COND-EQPT
	REPT EVT EQPT	RTRV-COND-SYNCN
	REPT EVT SYNCN	RTRV-SYNCN
	RTRV-ALM-<MOD2ALM>	

Section	Description (continued)
Input Format	RTRV-ALM-SYNCN:[TID]:[<sync_aid>]:[CTAG]::[<ntfcncde>],[<condition>],[<serv_eff>]; where: • sync_aid is the AID sync_ref and is listable; a null value is equivalent to “ALL” • ntfcncde is a 2-letter notification code and is of type NOTIF_CODE; a null value is equivalent to “ALL” • condition is a type of alarm condition and is of type CONDITION; condition is listable and a null value is equivalent to “ALL” • serv_eff is a type of effect on service caused by the alarm condition; serv_eff is of type SERV_EFF and a null value is equivalent to “ALL”
Output Format	SID DATE TIME M CTAG COMPLD “<sync_aid>:<ntfcncde>,<condition>,<srveff>,,,,:<desc>” ; where: • sync_aid identifies the facility queried and is the AID sync_ref • ntfcncde is a 2-letter notification code and is of type NOTIF_CODE • condition is a type of alarm condition and is of type CONDITION • srveff is a type of effect on service caused by the alarm condition; serveff is of type SERV_EFF • desc is a String
Example	Input RTRV-ALM-SYNCN:FULTON:SYNC-NE:226::CR,FAILTOSW,SA; Output TID-000 98-06-20 14-30-00 M 001 COMPLD “SYNC-NE:CR,FAILTOSW,SA,,,,:\”FAILURE TO SWITCH TO PROTECTION\”,” ;
Errors	This message generates all the default errors

11.11.69 RTRV-BITS: Retrieve Building Integrated Timing Supply

This command retrieves the BITS configuration command.

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-BITS:[TID]:<bits_aid>:[CTAG]::::; where: • bits_aid is the AID bits and must not be null

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<bits_aid>:LNCDE=<line_code>,FMT=<frame_format>:<pst>" ; where: • bits_aid is the AID bits • line_code is of type LINE_CODE • frame_format is of type FRAME_FORMAT • pst is of type PST
Example	Input RTRV-BITS:SONOMA:BITS-1:782::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "BITS-1:LNCDE=AMI,FMT=ESF:IS" ;
Errors	This message generates all the default errors

11.11.70 RTRV-COND-<MOD2ALM>: Retrieve Condition (DS1, E100, E1000, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command instructs the NE to retrieve the current standing condition and/or state associated with an entity.

Section	Description	
Category	Fault	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-ALL
	REPT ALM BITS	RTRV-ALM-BITS
	REPT ALM ENV	RTRV-ALM-ENV
	REPT ALM EQPT	RTRV-ALM-EQPT
	REPT ALM SYNCN	RTRV-ALM-SYNCN
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
Input Format	RTRV-COND-<MOD2ALM>:[TID]:[<facility>]:[CTAG]::[<condition>],,,;	
	where: • facility is the facility aid and is the AID facility; a null value is equivalent to "ALL" • condition is the requested condition, if not set=> we want all the conditions for the specified facility; condition is of type CONDITION and a null value is equivalent to "ALL"	

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<facility>,<eqptType>:[<notifcode>],<condition>,[<servEff>],,,,,, [<desc>]" ; where: • facility is the facility aid and is the AID facility • eqptType is of type EQPT_TYPE • notifCode is the notification code; notifCode is of type NOTIF_CODE and is optional • condition is the condition itself and is of type CONDITION • servEff is of type SERV_EFF and is optional • desc is the condition description; desc is a String and is optional
Example	Input RTRV-COND-T3:TID:FAC-2-1:229::LOS,,,; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-2-1,DS3-12:CR,LOS,SA,,,,,,\"LOS OF SIGNAL\"" ;
Errors	This message generates all the default errors

11.11.71 RTRV-COND-ALL: Retrieve Condition All

This command instructs the NE to retrieve the current standing condition for all entities.

Section	Description	
Category	Fault	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-ALL
	REPT ALM BITS	RTRV-ALM-BITS
	REPT ALM ENV	RTRV-ALM-ENV
	REPT ALM EQPT	RTRV-ALM-EQPT
	REPT ALM SYNCN	RTRV-ALM-SYNCN
	REPT EVT <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
Input Format	RTRV-COND-ALL:[TID]::[CTAG]::[<condition>],:::; where: • condition is of type CONDITION and a null value is equivalent to "ALL"	

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<facility>,[<aid_type>]:[<notifCode>],<condition>,[<servEff>],,,,,, [<desc>]" ; where: • facility is the AID facility • aid_type is of type MOD2B and is optional • notifCode is of type NOTIF_CODE and is optional • condition is of type CONDITION • servEff is of type SERV_EFF and is optional • desc is a String and is optional
Example	Input RTRV-COND-ALL::TID::229::LOS,,,: Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-2-1,OC3:CR,LOS,SA,,,,,,\"LOS OF SIGNAL\"" ;
Errors	This message generates all the default errors

11.11.72 RTRV-COND-BITS: Retrieve Condition Building Integrated Timing Supply

This command instructs the NE to retrieve the standing conditions on BITS.

Section	Description	
Category	Fault	
Security	Read Only	
Related Messages	REPT ALM <MOD2ALM>	RTRV-ALM-ALL
	REPT ALM BITS	RTRV-ALM-BITS
	REPT ALM ENV	RTRV-ALM-ENV
	REPT ALM EQPT	RTRV-ALM-EQPT
	REPT ALM SYNCN	RTRV-ALM-SYNCN
	REPT EVT <MOD2ALM>	RTRV-COND-<MOD2ALM>
	REPT EVT EQPT	RTRV-COND-ALL
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2ALM>	RTRV-COND-SYNCN
Input Format	RTRV-COND-BITS:[TID]:<facility>:[CTAG]::[<condition>],,,; where: • facility is the AID bits and must not be null • condition is of type CONDITION and a null value is equivalent to "ALL"	

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<facility>,<eqptType>:[<notifCode>],<condition>,[<servEff>],,,,,, [<desc>]" ; where: • facility is the AID bits • eqptType is of type EQPT_TYPE • notifCode is of type NOTIF_CODE and is optional • condition is of type CONDITION • servEff is of type SERV_EFF and is optional • desc is a String and is optional
Example	Input RTRV-COND-BITS:TID:BITS-1:229::LOS,,,: Output TID-000 98-06-20 14-30-00 M 001 COMPLD "BITS-1,TCC:CR,LOS,SA,,,,,,\"LOS OF SIGNAL\"" ;
Errors	This message generates all the default errors

11.11.73 RTRV-COND-EQPT: Retrieve Condition Equipment

This command instructs the NE to retrieve current equipment conditions.

Section	Description	
Category	Equipment	
Security	Read Only	
Related Messages	DLT-EQPT	RLS-PROTNSW-EQPT
	DLT-FFP-EQPT	RTRV-ALM-<MOD2ALM>
	ED-FFP-EQPT	RTRV-ALM-ALL
	ENT-EQPT	RTRV-ALM-BITS
	ENT-FFP-EQPT	RTRV-ALM-ENV
	OPR-PROTNSW-EQPT	RTRV-ALM-EQPT
	REPT ALM <MOD2ALM>	RTRV-ALM-SYNCN
	REPT ALM BITS	RTRV-COND-<MOD2ALM>
	REPT ALM ENV	RTRV-COND-ALL
	REPT ALM EQPT	RTRV-COND-BITS
	REPT ALM SYNCN	RTRV-COND-SYNCN
	REPT EVT <MOD2ALM>	RTRV-EQPT
	REPT EVT EQPT	RTRV-FFP-EQPT
	REPT EVT SYNCN	SW-DX-EQPT

Section	Description (continued)
Input Format	RTRV-COND-EQPT:[TID]:<facility>:[CTAG]::[<condition>],,,; where: • facility is the AID and must not be null. • condition is of type CONDITION and a null value is equivalent to “ALL”
Output Format	SID DATE TIME M CTAG COMPLD “<facility>,<eqptType>:[<notifCode>],<condition>,[<servEff>],,,,,,[<desc>]” ; where: • facility is the AID facility • eqptType is of type EQPT_TYPE • notifCode is of type NOTIF_CODE and is optional • condition is of type CONDITION • servEff is of type SERV_EFF and is optional • desc is a String and is optional
Example	Input RTRV-COND-EQPT:TID:SLOT-1:229::LOS,,,: Output TID-000 98-06-20 14-30-00 M 001 COMPLD “SLOT-1,DS3-12:CR,LOS,SA,,,,,,,\”LOS OF SIGNAL\”” ;
Errors	This message generates all the default errors

11.11.74 RTRV-COND-SYNCN: Retrieve Condition Synchronization

This command retrieves the synchronization condition.

Section	Description	
Category	Synchronization	
Security	Read Only	
Related Messages	ED-SYNCN	RTRV-ALM-ALL
	REPT ALM <MOD2ALM>	RTRV-ALM-BITS
	REPT ALM BITS	RTRV-ALM-ENV
	REPT ALM ENV	RTRV-ALM-EQPT
	REPT ALM EQPT	RTRV-ALM-SYNCN
	REPT ALM SYNCN	RTRV-COND-<MOD2ALM>
	REPT EVT <MOD2ALM>	RTRV-COND-ALL
	REPT EVT EQPT	RTRV-COND-BITS
	REPT EVT SYNCN	RTRV-COND-EQPT
	RTRV-ALM-<MOD2>	RTRV-SYNCN

Section	Description (continued)
Input Format	RTRV-COND-SYNCN:[TID]:<facility>:[CTAG]::[<condition>],,,; where: • facility is the AID sync_ref and must not be null • condition is of type CONDITION and a null value is equivalent to “ALL”
Output Format	SID DATE TIME M CTAG COMPLD “<facility>,[<eqptType>]:[<notifCode>],<condition>,[<servEff>],,,,,, [<desc>]” ; where: • facility is the AID sync_ref • eqptType is of type EQPT_TYPE and is optional • notifCode is of type NOTIF_CODE and is optional • condition is of type CONDITION • servEff is of type SERV_EFF and is optional • desc is a String and is optional
Example	Input RTRV-COND-SYNCN:TID:SYNC-NE:229::LOS,,,: Output TID-000 98-06-20 14-30-00 M 001 COMPLD “SYNC-NE,TCC:MJ,FRNGSYNC,SA,,,,,,\”FREE RUNNING SYNCHRONIZAION MODE\”” ;
Errors	This message generates all the default errors

11.11.75 RTRV-CRS-<STS_PATH>: Retrieve Cross Connect (STS1, STS3C STS12C)

This command retrieves any connections associated with the Access Identifiers entered. FROM and TO information is returned along with the type of connection.

Section	Description
Category	Cross Connect
Security	Read Only
Related Messages	DLT-CRS-<STS_PATH> DLT-CRS-VT1 ED-CRS-<STS_PATH> ED-CRS-VT1 ENT-CRS-<STS_PATH> ENT-CRS-VT1 RTRV-CRS-VT1

Section	Description (continued)
Input Format	RTRV-CRS-<STS_PATH>:[TID]:<sts_ep>:[CTAG]::,,,; where: • sts_ep is the AID sts and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<crs_ep>,<crs_ep1>:<cct>" ; where: • crs_ep is the AID sts • crs_ep1 is the AID sts • cct is the cross connect type and is of type CCT
Example	Input RTRV-CRS-STS3C:KENWOOD:STS-6-1:223::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "STS-6-1,STS-12-4:2WAY" ;
Errors	This message generates all the default errors

11.11.76 RTRV-CRS-VT1: Retrieve Cross Connect Virtual Tributary

This command retrieves the VT cross-connection information.

Section	Description
Category	Cross Connect
Security	Read Only
Related Messages	DLT-CRS-<STS_PATH> DLT-CRS-VT1 ED-CRS-<STS_PATH> ED-CRS-VT1 ENT-CRS-<STS_PATH> ENT-CRS-VT1 RTRV-CRS-<STS_PATH>
Input Format	RTRV-CRS-VT1:[TID]:<vt>:[CTAG]::::; where: • vt is the AID vt1_5 and must not be null

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<from>,<to>:<cct>" ; where: • from is the first (FROM) VT in cross-connection and is the AID vt1_5 • to is the second (TO) VT in cross-connection and is the AID vt1_5 • cct is the cross connect type and is of type CCT
Example	Input RTRV-CRS-VT1:CISCO:VT1-2-3-1:1234::::: Output TID-000 98-06-20 14-30-00 M 001 COMPLD "VT1-2-3-1,VT1-4-4-1:1WAY" ;
Errors	This message generates all the default errors

11.11.77 RTRV-EC1: Retrieve Electrical Carrier Level 1

This command retrieves the facility status of an EC-1 card.

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-EC1:[TID]:<fac>:[CTAG]:::::; where: • fac is the facility aid and is the AID facility; fac must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<fac>:PJMON=<pjmon>,LBO=<lbo>:PST=<pst>" ; where: • fac is the facility aid and is the AID facility • pjmon is the SONET pointer monitor and is an Integer • lbo is line buildout and is of type E_LBO • pst is the primary service state and is of type PST

Section	Description (continued)
Example	Input RTRV-EC1:CISCO:FAC-1-1:1234::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-1-1:PJMON=0,LBO=0-225:PST=IS" ;
Errors	This message generates all the default errors

11.11.78 RTRV-EQPT: Retrieve Equipment

This command retrieves the data and state parameters associated with an equipment unit.

Section	Description	
Category	Equipment	
Security	Read Only	
Related Messages	DLT-EQPT	REPT EVT EQPT
	DLT-FFP-EQPT	RLS-PROTNSW-EQPT
	ED-FFP-EQPT	RTRV-ALM-EQPT
	ENT-EQPT	RTRV-COND-EQPT
	ENT-FFP-EQPT	RTRV-FFP-EQPT
	OPR-PROTNSW-EQPT	SW-DX-EQPT
	REPT ALM EQPT	
Input Format	RTRV-EQPT:[TID]:<eqpt_aid>:[CTAG]::::; where: • eqpt_aid is the AID eqpt and must not be null	
Output Format	SID DATE TIME M CTAG COMPLD "<eqpt_aid>:[<eqpt_type>]:[WTR=<wtr>],[NAME=<name>]:<state>,<equip>,[<role>],[<status>]" ; where: • eqpt_aid is the AID eqpt • eqpt_type is the type of card in the slot; eqpt_type is of type EQPT_TYPE and is optional • wtr is an Integer and is optional • name is a String and is optional • state is of type PST • equip indicates if the equipment unit is physically present and is of type EQUIP. • role indicates if the card is a working unit or the protecting unit; role is of type SIDE and is optional • status is of type STATUS and is optional	

Section	Description (continued)
Example	Input RTRV-EQPT:MIRABEL:SLOT-12:230::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "SLOT-12:OC12:WTR=99,NAME=DESCRIPTION:IS,EQUIP,,ACT" ;
Errors	This message generates all the default errors

11.11.79 RTRV-FFP-<OCN_TYPE>: Retrieve Facilities Protection Group (OC3, OC12, OC48)

This command retrieves the optical facility protection information.

Section	Description
Category	Facility Protection
Security	Read Only
Related Messages	N/A
Input Format	RTRV-FFP-<OCN_TYPE>:[TID]:<facility>:[CTAG]; where: • facility is the AID facility and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<work>,<protect>:NAME=<name>,RVTT=<revertiveType>, RVTM=<revertiveTime>,BSWM=<bswMode>" ; where: • work is the AID facility • protect is the AID facility • name is the protection name and is a String • revertiveType is the revertive type and e is of type REVERTIVE_TYPE • revertiveTime is the revertive time and is of type REVERTIVE_TIME • bswMode specifies if it is a bidirectional switch mode and is of type ON_OFF
Example	Input RTRV-FFP-OC3:PETALUMA:FAC-3-1:1; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-3-1,FAC-4-1:NAME=PROT_NAME,RVTT=R,RVTM=1.0, BSWM=OFF" ;

Section	Description (continued)
Errors	This message generates all the default errors

11.11.80 RTRV-FFP-EQPT: Retrieve Facilities Protection Group Equipment

This command retrieves the equipment protection information.

Section	Description	
Category	Equipment	
Security	Read Only	
Related Messages	DLT-EQPT	REPT EVT EQPT
	DLT-FFP-EQPT	RLS-PROTNSW-EQPT
	ED-FFP-EQPT	RTRV-ALM-EQPT
	ENT-EQPT	RTRV-COND-EQPT
	ENT-FFP-EQPT	RTRV-EQPT
	OPR-PROTNSW-EQPT	SW-DX-EQPT
	REPT ALM EQPT	
Input Format	RTRV-FFP-EQPT:[TID]:<eqpt>:[CTAG]; where: • eqpt is the AID eqpt and must not be null	
Output Format	SID DATE TIME M CTAG COMPLD "<work>,<protect>:PRT=<protectionGroup>,NAME=<name>, RVTT=<revertiveType>,RVTM=<revertiveTime>,BSWM=<bswMode>" ; where: • work is the working slot aid and is the AID eqpt • protect is the protection slot aid and is the AID eqpt • protectionGroup is the protection group and is of type PROTECTION_GROUP • name is the protection name and is a String • revertiveType is of type REVERTIVE_TYPE • revertiveTime is of type REVERTIVE_TIME	
Example	Input RTRV-FFP-EQPT:PETALUMA:SLOT-16:1; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "SLOT-16,SLOT-17:PRT=1-1,NAME=PROT_NAME,RVTT=R,RVTM=1.0" ;	
Errors	This message generates all the default errors	

11.11.81 RTRV-HDR: Retrieve Header

This command instructs the NE to return the header of a TL1 response message. Used by TL1 clients to determine if the link to the NE is still active and if the NE is responding to commands.

Section	Description
Category	System
Security	Read Only
Related Messages	ACT-USER ALW-MSG-ALL CANC-USER ED-DAT INH-MSG-ALL INIT-SYS
Input Format	RTRV-HDR:[TID]::[CTAG];
Example	Input RTRV-HDR:SONOMA::232;
Errors	This message generates all the default errors

11.11.82 RTRV-INV: Retrieve Inventory

This command queries the NE and returns a listing of the equipment inventory. For each unit in the system, it identifies the unit's hardware version and revision numbers, firmware version, and the unit's CLEI code.

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-INV:[TID]:<eqpt_aid>:[CTAG]::,,; where: eqpt_aid is the AID eqpt and must not be null

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<eqpt_aid>,<eqptType>:[PN=<pn>],[HWVER=<hwver>], [FWVER=<fwver>],[SN=<sn>],[CLEI=<clei>]" ; where: • eqpt_aid is the AID eqpt • eqpt_type is of type EQPT_TYPE • pn is a String and is optional • hwver is a String and is optional • fwver is a String and is optional • sn is an integer and is optional • clei is a String and is optional
Example	Input RTRV-INV:OCCIDENTAL:SLOT-15:301:::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "SLOT-15,OC3-IR-4:PN=87-00002,HWVER=004K, FWVER=76-99-00009-004A,SN=013510,CLEI=NOCLEI" ;
Errors	This message generates all the default errors

11.11.83 RTRV-LOG: Retrieve Log

This command retrieves the alarm log of the NE.

Section	Description
Category	Log
Security	Read Only
Related Messages	N/A
Input Format	RTRV-LOG:[TID]::[CTAG];

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "<aid>,<seq>:CURRENT=<current>,[PREVIOUS=<previous>], <condition>,servEff>,[TIME=<time>],DATE=<date>:<desc>" ; where: • aid is the AID ALL • seq is an Integer • current is of type NOTIF_CODE • previous is of type COND_EFF and is optional • condition is of type CONDITION • servEff is of type SERV_EFF • time is a Date and is optional • date is a String • desc is a String
Example	Input RTRV-LOG:CISCO::123; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-3-1,12:CURRENT=MJ,PREVIOUS=CL,EOC,NSA,TIME=16-33-04, DATE=1971-02-03:\"SDCC TERMINATION FAILURE\"" ;
Errors	This message generates all the default errors

11.11.84 RTRV-NE: Retrieve Network Element

This command retrieves the attributes of the NE system such as the node identity (e.g. IP address), external interfaces (e.g. LAN ports), and major modes of operation (e.g. SONET vs. SDH).

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-NE:[TID]::[CTAG]::::;

Section	Description (continued)
Output Format	SID DATE TIME M CTAG COMPLD "IPADDR=<ipaddr>,IPMASK=<ipmask>,DEFRTR=<defrtr>, EXTLAN=<extlan>,INTLAN=<intlan>,RTRMDE=<rtrmode>, STM=<stm>,NODEID=<nodeid>,EXTRNG=<ext_ring>, RNGWTR=<rngwtr>,TMMD=<timing_mode>,SSMG=<sync_gen>, NSQL=<sync_quality_level>" ; where: • ipaddr is the IP address of the NE on the local LAN and is a String • ipmask is the IP Mask used to identify the sub-net on which the NE resides; ipmask is a String • defrtr is the IP address of the default router and is a String • extlan is of type EXT_LAN • intlan is of type EXT_LAN • rtrmode is of type EXT_LAN • stm is of type OPTICAL_MODE • nodeid is the Node ID of the NE in the BLSR and is an Integer • ext_ring is the node/ring that supports the extended K1/K2/K3 protocol for more than 16 nodes per BLSR; ext_ring is of type EXT_RING • rngwtr is an Integer • timing_mode is of type TIMING_MODE • sync_gen is of type SYNC_GENERATION • sync_quality_level is of type SYNC_QUALITY_LEVEL
Example	Input RTRV-NE:LAKEVILLE::233:::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "IPADDR=192.168.100.52,IPMASK=255.255.255.0, DEFRTR=192.168.100.1,EXTLAN=OFF,INTLAN=OFF, RTRMDE=OFF,STM=SONET,NODEID=3,EXTRNG=N,RNGWTR=99, TMMD=LINE,SSMG=GEN1,NSQL=ABOVE-PRS" ;
Errors	This message generates all the default errors

11.11.85 RTRV-PM-<MOD2>: Retrieve Performance (DS1, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command retrieves the performance monitoring for specified card type.

Note Release 2.2.1 does not support the 48C value.

Section	Description
Category	Performance
Security	Read Only
Related Messages	INIT-REG-<MOD2> RTRV-TH-<MOD2> SET-TH-<MOD2>
Input Format	RTRV-PM-<MOD2>:[TID]:<aid>:[CTAG]::,,,,<tmpr>,,; where: • aid is the AID ALL and must not be null • tmpr is of type TMPR and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<aid>:<montype>,<monval>,<validity>,<location>,<tmpr>,<direction>" ; where: • aid is the AID ALL • montype is the monitored type ex CVL, ESL and is of type ALL_MONTYPE • monval is the monitored value and l is an Integer • validity is of type VALIDITY • location is the location far-end, near-end or both; location is of type LOCATION • tmpr is the time period 15 min, 1 hour or 1 day; tmpr is of type TMPR • direction is the direction receive, transmit or both; direction is of type DIRECTION
Example	Input RTRV-PM-T1:TID:AID:123::,,,,15MIN,,; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "AID:CVL,21,COMPL,FEND,15MIN,RCV,," ;
Errors	This message generates all the default errors

11.11.86 RTRV-SYNCN: Retrieve SYNCN

This command retrieves the synchronization reference list used to determine the sources for the NE's reference clock and the BITS output clock. For each clock, up to three synchronization sources may be specified (e.g. PRIMARY, SECOND,THIRD).

Section	Description
Category	Synchronization
Security	Read Only
Related Messages	ED-SYNCN OPR-SYNCNCSW REPT ALM SYNCN REPT EVT SYNCN RTRV-ALM-SYNCN RTRV-COND-SYNCN
Input Format	RTRV-SYNCN:[TID]:<sync_aid>:[CTAG]::::; where: • sync_aid identifies the synchronization reference to retrieve and is the AID sync_ref; sync_ref is listable and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<sync_aid>:PRIMARY=<primary>,SECOND=<second>,THIRD=<third>" ; where: • sync_aid is the synchronization reference to be modified and is the AID sync_ref • primary is the AID syn_src • second is the AID syn_src • third is the AID syn_src
Example	Input RTRV-SYNCN:BOYES:SYNC-NE:234::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "SYNC-NE:PRIMARY=FAC-1-2,SECOND=FAC-2-2,THIRD=FAC-3-2;" ;
Errors	This message generates all the default errors

11.11.87 RTRV-T1: Retrieve T1

This command retrieves the DS-1 facilities configuration.

Section	Description
Category	Other
Security	Read Only
Related Messages	ED-T1 ED-T3 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-T1 RLS-LPBK-T3 RTRV-T3
Input Format	RTRV-T1:[TID]:<aid>:[CTAG]::::; where: • aid is the AID facility and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<aid>:STATE=<pst>,ID=<id>,LNCDE=<line_code>, FRMF=<fame_format>,LBO=<line_buildout>" ; where: • aid is the AID facility • pst is of type PST • id is a String • line_code is of type LINE_CODE • frame_format is of type FRAME_FORMAT • line_buildout is of type LINE_BUILDOUT
Example	Input RTRV-T1:TID:AID:1223::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "AID:STATE=OOS,ID=CISCO,LNCDE=AMI,FRMF=ESF,LBO=0-131" ;
Errors	This message generates all the default errors

11.11.88 RTRV-T3: Retrieve T3

This command retrieves the facilities properties of a DS-3 and a DS-3 transmux card.

Section	Description
Category	Other
Security	Read Only
Related Messages	ED-T1 ED-T3 OPR-LPBK-T1 OPR-LPBK-T3 RLS-LPBK-T1 RLS-LPBK-T3 RTRV-T1
Input Format	RTRV-T3:[TID]:<facility>:[CTAG]::::; where: • facility is the facility aid FAC-[SLOT]-[1..6] or FAC-[SLOT]-[1..12]; facility is the AID facility and must not be null
Output Format	SID DATE TIME M CTAG COMPLD "<facility>:LNTYPE=<lineType>,[LNCODE=<lineCode>],LBO=<lbo>: PST=<pst>" ; where: • facility is the facility aid FAC-[SLOT]-[1..6] or FAC-[SLOT]-[1..12] and is the AID facility. • lineType is the port line type and is of type DS_LINE_TYPE • lineCode is the port one code; lineCode is of type DS_LINE_CODE and is optional • lbo is the circuit line buildout and is of type E_LBO • pst is of type PST
Example	Input RTRV-T3:CISCO:FAC-1-2:123::::; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-1-2:LNTYPE=C-BIT,LNCODE=B3ZS,LBO=0-225:PST=IS" ;
Errors	This message generates all the default errors

11.11.89 RTRV-TH-<MOD2>: Retrieve Threshold (DS1, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command retrieves the threshold level.

Note Release 2.2.1 does not support STS48C and VT1.

Section	Description
Category	Performance
Security	Read Only
Related Messages	INIT-REG-<MOD2> RTRV-PM-<MOD2> SET-TH-<MOD2>
Input Format	RTRV-TH-<MOD2>:[TID]:<facility>:[CTAG]::<allMontype>,[<location>],[<tmpr>]; where: • facility is the aid type and is the AID ALL; facility must not be null • allMontype is the monitored type and is of type ALL_MONTYPE; allMontype must not be null • location is the location and is of type LOCATION; a null value is equivalent to "ALL" • tmpr is the time period and is of type TMPR; a null value is equivalent to "ALL"
Output Format	SID DATE TIME M CTAG COMPLD "<facility>,[<eqptType>]:<allMontype>,[<location>],,<thval>,[<tmpr>]" ; where: • facility is the aid and is the AID ALL • eqptType is of type EQPT_TYPE and is optional • allMontype is the monitored type and is of type ALL_MONTYPE • location is the location and is of type location; location is optional • thVal is the threshold value and is an Integer • tmpr is the time period and is of type TMPR; tmpr is optional
Example	Input RTRV-TH-T3:CISCO:FAC-1-3:1234::CVL,FEND,15MIN; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "FAC-1-3,DS3-12:CVL,FEND,,1,15MIN" ;
Errors	This message generates all the default errors

11.11.90 RTRV-TOD: Retrieve Time of Day

This command queries the NE and displays the system date and time at the instant when the command was executed. The time returned is in Coordinated Universal Time (UTC).

Section	Description
Category	Other
Security	Read Only
Related Messages	N/A
Input Format	RTRV-TOD:[TID]::[CTAG];
Output Format	SID DATE TIME M CTAG COMPLD "<year>,<month>,<day>,<hour>,<minute>,<second>,,<tmtype>" ; where: • year is an Integer • month is an Integer • day is an Integer • hour is an Integer • minute is an Integer • second is an Integer • tmtype is a String
Example	Input RTRV-TOD:CAZADERO::230; Output TID-000 98-06-20 14-30-00 M 001 COMPLD "1998,05,08,17,01,33,,UTC" ;
Errors	This message generates all the default errors

11.11.91 SET-TH-<MOD2>: Set Threshold (DS1, EC1, OC3, OC12, OC48, STS1, STS3C, STS12C, STS48C, T1, T3, VT1)

This command sets the threshold level.

Note Release 2.2.1 does not support STS48C.

Section	Description
Category	Performance
Security	Read/Write

Section	Description (continued)
Related Messages	INIT-REG-<MOD2> RTRV-TH-<MOD2> RTRV-PM-<MOD2>
Input Format	SET-TH-<MOD2>:[TID]:<facility>:[CTAG]::<allMontype>,<thVal>, [<location>],,[<tmpr>]; where: • facility is the aid and is the AID ALL • allMontype is the monitored value and is of type ALL_MONTYPE • thVal is the threshold value and is an Integer • location is the location and is of type LOCATION • tmpr is the time period and is of type TMPR
Example	Input SET-TH-T3:CISCO:FAC-1-1:123::CVL,12,NEND,,15MIN;
Errors	This message generates all the default errors

11.11.92 SET-TOD: Set Time of Day

This command sets the system date and time for the NE. The year should be entered using four digits while the hour should be entered using a 24-hour time period (i.e. military time).

Section	Description
Category	Other
Security	Read/Write
Related Messages	N/A
Input Format	SET-TOD:[TID]::[CTAG]::<year>,<month>,<day>,<hour>,<minute>,<second>, [<difference>]:[USEDST=<usedst>]; where: • year is the current calendar year and is an Integer • month is the month of the year and ranges from 01 to 12; month is an Integer • day is the day of the month and ranges from 01 to 31; day is an Integer • hour is the hour of the day and ranges from 00 to 59; hour is an Integer • minute is the minute of the hour and ranges from 00 to 59; minute is an Integer • second is the second of the minute and ranges from 00 to 59; second is an Integer • difference is the number of minutes behind UTC and is an Integer • usedst indicates if Daylight Saving Time is used and is of type USE_DST
Example	Input SET-TOD:CAZADERO::240::1998,05,08,13,18,55,480:USEDST=Y;
Errors	This message generates all the default errors

11.11.93 SW-DX-EQPT: Switch DX Equipment

This command instructs the NE to switch duplex equipment.

Section	Description	
Category	Equipment	
Security	N/A	
Related Messages	DLT-EQPT	REPT EVT EQPT
	DLT-FFP-EQPT	RLS-PROTNSW-EQPT
	ED-FFP-EQPT	RTRV-ALM-EQPT
	ENT-EQPT	RTRV-COND-EQPT
	ENT-FFP-EQPT	RTRV-EQPT
	OPR-PROTNSW-EQPT	RTRV-FFP-EQPT
	REPT ALM EQPT	
Input Format	SW-DX-EQPT:[TID]:<eqpt>:[CTAG]::[<dxModeOp>],; where: • eqpt is the AID eqpt • dxModeOp is of type DX_MODE_OP	
Example	Input SW-DX-EQPT:CISCO:SLOT-1:123::FRCD,;	
Errors	This message generates all the default errors	

11.12 Access Identifiers

The Access Identification code (AID) directs an input command to its intended physical or data entity inside the NE. Equipment Modules and facilities are typical examples of entities addressed by the access code.

Table 11-13 Access Identifiers

AID	Patterns
bits	BITS-ALL
	BITS-{1,2}
ds-1	DS1-{1-6,12-17}-{1-6}-{1-28}
env	ENV-IN-{1-4}
eqpt	SLOT-{1-17}
	SLOT-{1-6,12-17}
facility	FAC-{1-6,12-17}-1
	FAC-{1-6,12-17}-{1-12}
	FAC-{1-6,12-17}-{1-14}
	FAC-{1-6,12-17}-{1-4}
	FAC-{1-6,12-17}-{1-6}
	FAC-{5,6,12,13}-1

Table 11-13 Access Identifiers

sts	STS-{1-6,12-17}-1 STS-{1-6,12-17}-{1,4,7,10-46} STS-{1-6,12-17}-{1-12} STS-{1-6,12-17}-{1-6} STS-{5,6,12,13}-{1,13,25,37} STS-{5,6,12,13}-{1,4,7,10-46} STS-{5,6,12,13}-{1-48} STS-{5,6,12,13}-{1}
syn_src	FAC-{1-6,12-17}-1 FAC-{1-6,12-17}-{1-4} FAC-{5,6,12,13}-1 INTERNAL SYNC-NE SYNC-{BITS1,BITS2}
sync_ref	SYNC-NE SYNC-{BITS1,BITS2}
vt1_5	VT1-{1-6,12-17}-1-{1-14} VT1-{1-6,12-17}-{1-12}-{1-28} VT1-{1-6,12-17}-{1-6}-{1-28} VT1-{5,6,12,13}-{1-48}-{1-28}

11.12.1 bits

Table 11-14 bits

Pattern	Description
BITS-ALL	BITS-1 and BITS-2
BITS-{1,2}	Individual BITS AID

11.12.2 ds-1

Used to access the DS-1 frame layer of the DS3XM-6

Table 11-15 ds-1

Pattern	Description
DS1-{1-6,12-17}-{1-6}-{1-28}	DS-1 aid for a DX3Xm card

11.12.3 env

The AIC card environmental AIDs

Table 11-16 env

Pattern	Description
ENV-{IN}-{1-4}	Environmental alarm aid

11.12.4 eqpt

Table 11-17 eqpt

Pattern	Description
SLOT-{1-17}	Equipment aid for the whole NE
SLOT-{1-6,12-17}	Equipment aid for the I/O slots

11.12.5 facility

Used to access specific ports

Table 11-18 facility

Pattern	Description
FAC-{1-6,12-17}-1	Facility aid for the OC-12
FAC-{1-6,12-17}-{1-12}	Facility aid for the EC-1 and DS-3 cards
FAC-{1-6,12-17}-{1-14}	Facilities for the DS-1 card
FAC-{1-6,12-17}-{1-4}	Facility aid for the OC-3 card
FAC-{1-6,12-17}-{1-6}	Facility aid for the DS3XM card
FAC-{5,6,12,13}-1	Facility aid for the OC-48 card

11.12.6 sts

SONET frame-level AID set

Table 11-19 sts

AID	Description
STS-{1-6,12-17}-1	STS-1 aid for DS-1 cards STS-3C aid for OC-3 cards STS-12C aid for OC-12 cards
STS-{1-6,12-17}-{1,4,7,10}	STS-3C aid for OC-3 and OC-12 cards
STS-{1-6,12-17}-{1-12}	STS-1 aid for OC-12, EC-1, DS-3 and OC-3 cards
STS-{1-6,12-17}-{1-6}	STS-1 aid for DS3XM cards
STS-{5,6,12,13}-{1,13,25,37}	STS-12C for OC-48
STS-{5,6,12,13}-{1,4,7,10,13,16,19,22, 25,28,31,34,37,40,43,46}	STS-3C for OC-48
STS-{5,6,12,13}-{1-48}	STS-1 for OC-48
STS-{5,6,12,13}-{1}	STS-48C for OC-48

11.12.7 syn_src

Synchronization source

Table 11-20 sync_src

Pattern	Description
FAC-{1-6,12-17}-1	Sync source is the optical card (OC-12) facility
FAC-{1-6,12-17}-{1-4}	Sync source is the optical card (OC-3) facility
FAC-{5,6,12,13}-1	Sync source is the optical card (OC-48) facility
INTERNAL	Set the syn_src to be the system default value
SYNC-NE	Sync-NE source
SYNC-{BITS1,BITS2}	SYNC-BITS1 or SYNC-BITS2 sync source

11.12.8 sync_ref

Synchronization aids

Table 11-21 sync_ref

Pattern	Description
SYNC-NE	NE sync aid
SYNC-{BITS1,BITS2}	BITS1 and BITS2 sync aids

11.12.9 vt1_5

Virtual termination aids

Table 11-22 vt1_5

Pattern	Description
VT1-{1-6,12-17}-1-{1-14}	DS-1 vts
VT1-{1-6,12-17}-{1-12}-{1-28}	OC-12, OC-3, EC-1 vts
VT1-{1-6,12-17}-{1-6}-{1-28}	DS3XM vts
VT1-{5,6,12,13}-{1-48}-{1-28}	OC-48 vts

11.13 Parameter Types

This section provides a description of all message parameter types defined for the TL1 messages used in the ONS 15454. The TL1 message descriptions frequently refer to this section.

11.13.1 ATAG Description

The Autonomous Message Tag (ATAG) is used for message sequencing. The number is incremented by one for each autonomous message sent by the ONS 15454. The ONS 15454 uses whole numbers 0000 to 9999.

11.13.2 CTAG Description

The Correlation tag is included in each command by the user and is repeated by the ONS 15454 in the response to allow the user to associate the command and response messages.

Note The valid values for a ctag are decimal numbers with a maximum of 6 digits in Release 2.2.1.

11.13.3 TID Description

The Target Identifier is the name of the NE where the command is addressed. TID is the Telcordia name for the system.

11.13.4 ALL_MONTYPE

Monitoring type list

Table 11-23 ALL_MONTYPE Values

ALL_MONTYPE Values	Description
AISSP	Alarm Indication Signal Seconds-Path
CVCPP	Coding Violations - CP-Bit Path
CVL	Coding Violations - Line
CVP	Coding Violations - Path
CVV	Coding Violations - Section
ESCPP	Errored Seconds - CP-Bit Path
ESL	Errored Seconds - Line
ESP	Errored Seconds - Path
ESV	Errored Seconds - VT Path
FCL	Failure Count - Line
FCP	Failure Count - Path
LOSSL	Loss of Signal Seconds - Line
NPJC-PDET	PPJC-PDET:Negative Pointer Justification
NPJC-PGEN	PPJC-PDEN:Negative Pointer Justification
PPJC-PDET	PPJC-PDET:Positive Pointer Justification
PPJC-PGEN	PPJC-PDEN:Positive Pointer Justification
PSC	Protection Switching Count
PSD	Protection Switching Duration
SASCPP	Severely Errored Framing/AIS Second - CP-Bit Path
SASP	Severely Errored Framing/AIS Seconds
SEFS	Severely Errored Framing Seconds
SESCPP	Severely Errored Second - CP-Bit Path
SESL	Severely Errored Second - Line
SESP	Severely Errored Second - Path
SESV	Severely Errored Second - VT Path
UASCPP	Unavailable Second - CP-Bit Path
UASL	Unavailable Second - Line
UASP	Unavailable Second - Path
UASV	Unavailable Second - VT Path

11.13.5 ALL_THR

Threshold list

Table 11-24 ALL_THR Value

ALL_THR Values	Description
T-AISSP	Alarm Indication Signal Seconds-Path
T-CVCPP	Coding Violations - CP-Bit Path
T-CVL	Coding Violations - Line
T-CVP	Coding Violations - Path
T-CVS	Coding Violations - Section
T-CVV	Coding Violations - VT Path
T-ESCPP	Errored Seconds - CP-Bit Path
T-ESL	Errored Seconds - Line
T-ESP	Errored Seconds - Path
T-ESS	Errored Seconds - Section
T-ESV	Errored Seconds - VT Path
T-FCL	Failure Count - Line
T-FCP	Failure Count - Path
T-LOSSL	Loss of Signal Seconds - Line
T-PJNEG	PPJC-PDET:Negative Pointer Justification
T-PJNEG-GEN	PPJC-PGEN:Negative Pointer Justification
T-PJPOS	PPJC-PDET:Positive Pointer Justification
T-PJPOS-GEN	PPJC-PGEN:Positive Pointer Justification
T-PSC	Protection Switching Count
T-PSD	Protection Switching Duration
T-SASCPP	Severely Errored Framing/AIS Second - CP-Bit Path
T-SASP	Severely Errored Framing/AIS Seconds
T-SEFS	Severely Errored Framing Seconds
T-SESCPP	Severely Errored Second - CP-Bit Path
T-SESL	Severely Errored Second - Line
T-SESP	Severely Errored Second - Path
T-SESS	Severely Errored Second - Section
T-SESV	Severely Errored Second - VT Path
T-UASCPP	Unavailable Second - CP-Bit Path
T-UASL	Unavailable Second - Line
T-UASP	Unavailable Second - Path
T-UASV	Unavailable Second - VT Path

11.13.6 CCT

Defines the type of cross-connect to be created.

Table 11-25 CCT Values

CCT Values	Description
1WAY	A unidirectional connection from a source tributary to a destination tributary
2WAY	A bidirectional connection between the two tributaries
MON	Monitored cross connection

11.13.7 COND_EFF

The affected unit's condition

Table 11-26 COND_EFF Values

COND_EFF Values	Description
CL	Standing condition cleared
SC	Standing condition raised
TC	Transient condition

11.13.8 CONDITION

The condition type of the alarm indication

Table 11-27 CONDITION Values

CONDITION Values	Description
ACOMAN	Alarm cutoff is in manual mode
AIS	External failure - Incoming - Alarm Indication Signal
AIS-L	External failure - Incoming - Alarm Indication Signal - Line
AIS-P	External failure - Incoming - Alarm Indication Signal - Path
AIS-V	External failure - Incoming - Alarm Indication Signal - VT layer
APSB	External failure - Incoming - Automatic Protection Switching Channel - Byte failure
APSC	External failure - Incoming - Automatic Protection Switching Channel failure
APSC-IMP	External failure - Incoming - Automatic Protection Switching - Invalid K bytes
APSCCONNL	External failure - Incoming - Automatic Protection Switching - Connection Loss
APSCDFLTK	External failure - Incoming - Automatic Protection Switching - Default K byte
APSCINCON	External failure - Incoming - Automatic Protection Switching - Inconsistent
APSCM	External failure - Incoming - Automatic Protection Switching Channel - Protection Switching Channel Match failure
APSCNMIS	APS Channel - BLSR - Node ID Mismatch
APSMM	External failure - Incoming - Automatic Protection Switching Channel - Automatic Protection Switch Mode Mismatch
AUTOLSROFF	Internal hardware - Facility Termination Equipment - Automatic Laser Shutdown

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
AUTORESET	Recovery action - Automatic System Reset
AUTOSW-AIS	Automatic Switch - Alarm Indication Signal
AUTOSW-LOP	Automatic Switch - Loss of Pointer
AUTOSW-PDI	Automatic Switch - Payload Defect Indication
AUTOSW-SDBER	Automatic Switch - Signal Degrade Bit Error Rate
AUTOSW-SFBER	Automatic Switch - Signal Fail Bit Error Rate
AUTOSW-UNEQ	Automatic Switch - Unequipped
BKUPMEMP	Internal hardware - Control Equipment - Primary Non-Volatile Backup Memory Failure
BKUPMEMS	Internal hardware - Control Equipment - Secondary Non-Volatile Backup Memory Failure
BLSR-RESYNC	Bidirectional Line Switched Ring - Tables Resynchronized
BLSROOSYNC	Bidirectional Line Switched Ring - Out of Sync
BPV	External failure - Incoming - Bipolar Violation
CARLOSS	External failure - Incoming - Carrier Loss on the LAN
CLDRESTART	Recovery action - Cold Restart
CONCAT	STS Concatenation Error
CONTBUS	Control Bus Failure
CONTBUS-1	Control Bus Failure - 1
CONTBUS-2	Control Bus Failure - 2
CONTBUS-A-1	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 1
CONTBUS-A-2	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 2
CONTBUS-A-3	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 3
CONTBUS-A-4	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 4
CONTBUS-A-5	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 5
CONTBUS-A-6	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 6
CONTBUS-A-7	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 7
CONTBUS-A-8	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 8
CONTBUS-A-9	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 9
CONTBUS-A-10	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 10
CONTBUS-A-11	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 11
CONTBUS-A-12	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 12
CONTBUS-A-13	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 13
CONTBUS-A-14	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 14
CONTBUS-A-15	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 15
CONTBUS-A-16	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 16
CONTBUS-A-17	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 17
CONTBUS-A-18	TCC/TCC+ card in Slot 7 has lost communication with the card in Slot 18
CONTBUS-B-1	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 1

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
CONTBUS-B-2	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 2
CONTBUS-B-3	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 3
CONTBUS-B-4	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 4
CONTBUS-B-5	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 5
CONTBUS-B-6	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 6
CONTBUS-B-7	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 7
CONTBUS-B-8	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 8
CONTBUS-B-9	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 9
CONTBUS-B-10	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 10
CONTBUS-B-11	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 11
CONTBUS-B-12	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 12
CONTBUS-B-13	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 13
CONTBUS-B-14	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 14
CONTBUS-B-15	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 15
CONTBUS-B-16	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 16
CONTBUS-B-17	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 17
CONTBUS-B-18	TCC/TCC+ card in Slot 11 has lost communication with the card in Slot 18
CONTCOM	Internal hardware - Control Equipment - Control Communications equipment failure
CONTEQPT	Internal hardware - Control Equipment failure
CONTR	Internal hardware - Control Equipment - Control processor failure
CTNEQPT	Internal hardware - Interconnection Equipment failure
CTNEQPT-PB1PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 1
CTNEQPT-PB1WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 1
CTNEQPT-PB2PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 2
CTNEQPT-PB2WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 2
CTNEQPT-PB3PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 3
CTNEQPT-PB3WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 3
CTNEQPT-PB4PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 4
CTNEQPT-PB4WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 4
CTNEQPT-PB5PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 5
CTNEQPT-PB5WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 5

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
CTNEQPT-PB6PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 6
CTNEQPT-PB6WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 6
CTNEQPT-PB12PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 12
CTNEQPT-PB12WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 12
CTNEQPT-PB13PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 13
CTNEQPT-PB13WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 13
CTNEQPT-PB14PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 14
CTNEQPT-PB14WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 14
CTNEQPT-PB15PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 15
CTNEQPT-PB15WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 15
CTNEQPT-PB16PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 16
CTNEQPT-PB16WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 16
CTNEQPT-PB17PROT	Failure of the main payload between the protect XC/XCVT card in Slot 10 and the reporting I/O card in Slot 17
CTNEQPT-PB17WORK	Failure of the main payload bus between the active XC/XCVT card in Slot 8 and the reporting I/O card in Slot 17
DATAFLT	Internal Error - Software Fault - Data integrity fault
EOC	Embedded Operations Channel (Section DCC) failure
EOC-DOWN	Embedded Operation Channel Fail
EQPT	Internal hardware - Critical alarm caused by equipment failure
EQPT-DIAG	Equipment failure - Diagnostics Failure
EQPT-FAIL	Equipment Failure - Board Failure
EQPT-MAC	Equipment Failure - Medium Access Control
ESW	External Error - Excessive Switching
EXCCOL	External Failure - Incoming - Excess collisions on the LAN
EXT	Failure Detected External to the NE
EXTERR	External Error
FA	Internal Hardware - Power Failure - Fuse Alarm
FAC	External failure - Incoming - Facility, critical alarm caused by DS-3 facility failure
FACTERM	Internal hardware - Facility Termination equipment failure

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
FAILTORLS	Internal hardware - Failure To Release from protection
FAILTOSW	Internal hardware - Failure To Switch to protection
FAILTOSW-PATH	Failure to switch from the working path to the protection path on a UPSR
FAILTOSWR	Failure to Switch to Protection in a Ring
FAILTOSWS	Failure to Switch to Protection in a Span
FAN	Fan Tray Failure
FE-AIS	Far-end DS-3 node is reporting an AIS
FE-DS1-MULTLOS	Multiple inputs detect a loss on the far-end
FE-DS1-NSA	Non-service affecting failure detected from the far-end DS-1
FE-DS1-SA	Service affecting failure detected from the far-end DS-1
FE-DS1-SNGLLOS	One of the DS-1 inputs on the far-end detects a LOS
FE-DS3-NSA	Non-service affecting failure detected from the far-end DS-3
FE-DS3-SA	Service affecting failure detected from the far-end DS-3
FE-EQPT-NSA	Non-service affecting equipment failure is detected from the far-end DS-3
FE-IDLE	Far-end node detects an idle DS-3 signal
FE-LOF	Far-end node reports a DS-3 loss of frame
FE-LOS	Far-end node reports a DS-3 loss of signal
FEBE	External failure - Incoming - Far End Block Error
FEPRLF	External failure - Incoming - Automatic Protection Switching Channel - Far End Protection Line Failure
FORCED-REQ	Forced switch request on facility/equipment
FRCDWKSWBK	Recovery action - Working facility/equipment forced to switch back to working
FRCDWKSWPR	Recovery action - Working facility/equipment forced to switch to protection unit
FRCDWKSWPR-PATH	Recovery action - Working facility/equipment forced to switch to protection unit - Path
FRCWKBK-R	Recovery action - Working facility/equipment forced to switch back to working - Ring
FRCWKBK-S	Recovery action - Working facility/equipment forced to switch back to working - Span
FRCWKPR-R	Recovery action - Working facility/equipment forced to switch to protection unit- Ring
FRCWKPR-S	Recovery action - Working facility/equipment forced to switch to protection unit- Span
FRNGSYNC	Free Running Synchronization mode
FSTSYNC	Fast Start Synchronization Mode
HITEMP	Internal hardware - Equipment failure - High temperature
HLDOVRSYNC	Holdover synchronization mode
IMPROPRMVL	Procedural Error - Improper Removal
INC	Incoming failure condition
INC-ISD	Incoming failure condition - Idle Signal Path
INIT	Recovery action - Initialization initiated
INT	Internal hardware fault or failure
INTERR	Error Internal to the NE Detected

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
INTMSGERR	Internal Error - Internal Message Error
INTSFT	Internal Error - Software Fault or failure
INVMACADR	Equipment Failure - Invalid MAC address
LKOUTPR-R	Lockout or Protection - Ring
LKOUTPR-S	Lockout or Protection - Span
LKOUTWK-R	Lockout of Working - Ring
LKOUTWK-S	Lockout of Working - Span
LOCKOUT-REQ	Lockout switch request on facility/equipment
LOCKOUTOFPR	Recovery action - Lockout of Protection
LOCKOUTOFPR-PATH	Recovery action - Lockout of Protection - Path
LOCKOUTOFWK	Recovery action - Lockout of working
LOF	External failure - Incoming - Loss of Frame
LOP	External failure - Incoming - Loss of Pointer
LOP-P	External failure - Incoming - Loss of Pointer - Path
LOP-V	Loss of pointer at the VT level
LOS	External failure - Incoming - Loss of Signal
LPBK	Loopback
LPBKDS1FEAC	DS-1 loopback signal is received from the far-end due to a Far-End Alarm and Control (FEAC) command
LPBKDS1FEAC-CMD	DS-1 loopback command sent by the ONS 15454 to the far-end equipment
LPBKDS3FEAC	DS-3 loopback signal is received from the far-end due to a Far-End Alarm and Control (FEAC) command
LPBKDS3FEAC-CMD	DS-3 loopback command sent by the ONS 15454 to the far-end equipment
LPBKFACILITY	Loopback, Facility
LPBKM23	DS-2 Loopback due to Far End Command
LPBKM23-CMD	DS-2 Loopback Command sent to Far End
LPBKNETWORK	Loopback, Network
LPBKTERMINAL	Loopback, Terminal
MAN	Manually caused abnormal condition
MAN-REQ	Manual Switch Request
MANRESET	Recovery action - Manual system Reset
MANSWTOINT	Recovery action - Manual synchronization switch to internal clock
MANSWTOPRI	Recovery action - Manual synchronization Switch To Primary reference
MANSWTOSEC	Recovery action - Manual synchronization Switch To Second reference
MANSWTOTHIRD	Recovery action - Manual synchronization Switch To Third reference
MANSWTOFOURTH	Recovery action - Manual synchronization Switch To Fourth reference
MANSWTOFIFTH	Recovery action - Manual synchronization Switch To Fifth reference
MANSWTOSIXTH	Recovery action - Manual synchronization Switch To Sixth reference
MANWKBK-R	Manual Switch of working facility/equipment to protection - Ring

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
MANWKBK-S	Manual Switch of working facility/equipment to protection - Span
MANWKPR-R	Manual Switch of working facility/equipment to protection unit - Ring
MANWKPR-S	Manual Switch of working facility/equipment to protection unit - Span
MANWKSWBK	Recovery action - Manual Switch or working facility/equipment to protection
MANWKSWPR	Recovery action - Manual Switch of Working facility/equipment to protection unit
MANWKSWPR-PATH	Recovery action - Manual Switch of Working facility/equipment to protection - Path
MEA	Internal error - Mismatch of Equipment and Attributes
MEM-GONE	Software operations exceed the memory capacity of the TCC/TCC+ card
MEM-LOW	Data generated by software operations is close to exceeding the memory capacity of the TCC/TCC+ card
NEW-ROOT	New root trap in BRIDGE-MIB
NORMAL	Normal condition - This condition type is used by the NE to report the returning to normal from a previous off-normal condition
OG	External failure - Outgoing failure condition
OOF	External failure - Incoming - Out of Frame
PATHSEL	External failure - Incoming - Path Selector inability to switch to a valid signal
PDI	External failure - Incoming - Signal Label Mismatch Failure - Payload Defect Indication
PDI-P	External failure - Incoming - Signal Label Mismatch Failure - Payload Defect Indication - Path
PEERMISSM	Peer state mismatch
PLM-P	External failure - Incoming - Signal Label Mismatch Failure - Payload Label Mismatch - Path
PLM-V	Content of the V5 byte in the SONET overhead is inconsistent or invalid
PLUG-IN	Internal hardware - Equipment unit plug-in
PM-TCA	Performance Monitoring - Threshold Crossing Alert
PRC-DUPID	Procedural Error - Duplicate Node ID
PRCDRERR	Procedural Error
PROGFLT	Internal Error - Software Fault - Program failure
PROTNA	Protection unit not available
PS	Occurrence of a protection switching event
PWR	Internal hardware - Power failure (detected internal to NE)
PWRRESTART	Recovery action - Powerfail Restart
RAI	External failure - Incoming - Remote Alarm Indication
RCVR	Internal hardware - Facility Termination equipment - Receiver failure
RCVR-MISS	Facility termination equipment detects a missing receive cable on the DS-1 port or a possible mismatch of backplane equipment
RCVRY	Recovery or service protection action has been initiated
RDI-L	External failure - Outgoing - Remote Defect Indication - Line
RDI-P	External failure - Outgoing - Remote Defect Indication - Path

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
RFI	External failure - Incoming - Remote Failure Indication
RFI-L	External failure - Incoming - Remote Failure Indication - Line
RFI-P	External failure - Incoming - Remote Failure Indication - Path
RFI-V	Upstream failure has occurred at the VT layer
RMON-ALARM	An RMON Alarm
RMON-RESET	RMON histories and alarms have been reset due to chipset reboot
SD	Facility has passed BER Threshold for Signal Degrade
SEF	External failure - Incoming - Severely Errored Frame
SF	Facility has passed BER threshold for Signal Failure
SLMF	External failure - Incoming - Signal Label Mismatch Failures - SONET
SQUELCH	Ring is isolated into two or more segments
SSM-DUS	Synchronization Status Messaging - Don’t use for timing synchronization
SSM-FAIL	Synchronization Status Messaging - Failed
SSM-OFF	Synchronization Status Messaging - Off
SSM-PRS	Synchronization Status Messaging - Primary reference source - Stratum 1
SSM-RES	Synchronization Status Messaging - Reserved - quality level set by user
SSM-SMC	Synchronization Status Messaging - SONET minimum clock
SSM-ST2	Synchronization Status Messaging - Stratum 2
SSM-ST3	Synchronization Status Messaging - Stratum 3
SSM-ST3E	Synchronization Status Messaging - Stratum 3E
SSM-ST4	Synchronization Status Messaging - Stratum 4
SSM-STU	Synchronization Status Messaging - Sync traceability unknown
SSM-TNC	Synchronization Status Messaging - Transit node clock
SWFTDWN	Recovery action - Software download in progress
SWTOINT	Recovery action - Synchronization Switch To Internal clock
SWTOPRI	Recovery action - Synchronization Switch To Primary reference
SWTOSEC	Recovery action - Synchronization Switch To Second reference
SWTOTHIRD	Recovery action - Synchronization Switch To Third reference
SWTOFOURTH	Recovery action - Synchronization Switch To Fourth reference
SWTOFIFTH	Recovery action - Synchronization Switch To Fifth reference
SWTOSIXTH	Recovery action - Synchronization Switch To Sixth reference
SYNC	External failure - Incoming - Loss of timing on Synchronization link.
SYNCCLK	Internal hardware - Synchronization unit failure
SYNCEQPT	Internal hardware - Synchronization switching Equipment failure
SYNCOOS	External failure - Incoming - Loss of timing on all specified synchronization links
SYNCPRI	External failure - Incoming - Loss of timing on primary synchronization link
SYNCSEC	External failure - Incoming - Loss of timing on secondary synchronization link
SYNCTHIRD	External failure - Incoming - Loss of timing on third synchronization link

Table 11-27 CONDITION Values (continued)

CONDITION Values	Description
SYNCFOURTH	External failure - Incoming - Loss of timing on fourth synchronization link
SYNCFIFTH	External failure - Incoming - Loss of timing on fifth synchronization link
SYNCSIXTH	External failure - Incoming - Loss of timing on sixth synchronization link
SYSBOOT	Activation of new software
TOP-CHANGE	Topology Change trap in BRIDGE-MIB
TRMT	Internal hardware - Facility Termination equipment - Transmit failure
TRMT-MISS	Facility termination equipment detects a missing transmit cable on the DS-1 port or a possible mismatch of backplane equipment
TSI	Internal hardware - Interconnection Equipment - Time slot interchange equipment failure
UNEQ-P	External failure - Incoming - Signal Label Mismatch Failure - Unequipped - Path
UNEQ-V	VT is receiving an unequipped signal
UNPLUG	Internal hardware - Equipment unit un-plug
WATM-TO	Internal Error - Watchdog Timer Timeout
WKGMEM	Internal hardware - Control Equipment -Working memory failure
WKSWBK	Recovery action - Working facility/equipment switched back to working
WKSWPR	Recovery action - Working facility/equipment switched to protection unit
WRMRESTART	Recovery action - Warm Restart
WTR	Recovery action - SONET line is in Wait To Restore state

11.13.9 DIRECTION

Transmit and receive directions

Table 11-28 DIRECTION Values

DIRECTION Values	Description
BTH	Both transmit and receive directions
RCV	Receive direction only
TRMT	Transmit direction only

11.13.10 DS3_FMT

Indicates a DS-3 digital signal format

Table 11-29 DS3_FMT Values

DS3_FMT Values	Description
ASYNC	The DS-3 digital signal format is ASYNC
CBIT	The DS-3 digital signal format is C-BIT
SYNC	The DS-3 digital signal format is SYNC
UNFR	The DS-3 digital signal format is unframed

11.13.11 DS_LINE_CODE

DS-123 Line Code

Table 11-30 DS_LINE_CODE Values

DS_LINE_CODE Values	Description
B3ZS	Bipolar with Three-Zero Substitution

11.13.12 DS_LINE_TYPE

DS-123 Line type

Table 11-31 DS_LINE_TYPE Values

DS_LINE_TYPE Values	Description
C-BIT	C-BIT line type applies to DS3XM card
M23	M23 line type applies to DS3XM card
UNFRAMED	Line Type is Unframed

11.13.13 DX_MODE_OP

Duplex switch operation mode

Table 11-32 DX_MODE_OP Values

DX_MODE_OP Values	Description
FRCD	Forced Switch
MAN	Manual Switch

11.13.14 E_LBO

Electrical signal line buildout

Table 11-33 E_LBO Values

E_LBO Values	Description
0-225	Electrical signal buildout range is 0-255
226-450	Electrical signal buildout range is 255-450

11.13.15 ENV_ALM

Environmental alarm types as defined by Telcordia GR-833-CORE, Issue 2, November 1996, Appendix F.

Table 11-34 ENV_ALM Values

ENV_ALM Values	Description
AIRCOMPR	Air compressor failure
AIRCOND	Air conditioning failure
AIRDRYR	Air dryer failure
BATDSCHRG	Battery discharging
BATTERY	Battery failure
CLFAN	Cooling fan failure
CPMAJOR	Centralized power major failure
CPMINOR	Centralized power minor failure
ENGINE	Engine failure
ENGOPRG	Engine operating
EXPLGS	Explosive gas
FIRDETR	Fire detector failure
FIRE	Fire
FLOOD	Flood
FUSE	Fuse failure
GEN	Generator failure
HIAIR	High airflow
HIHUM	High humidity
HITEMP	High temperature
HIWTR	High water
INTRUDER	Intrusion
LWBATVG	Low battery voltage
LWFUEL	Low fuel
LWHUM	Low humidity
LWPRES	Low cable pressure
LWTEMP	Low temperature
LWWTR	Low water
MISC	Miscellaneous
OPENDR	Open door
POWER	Commercial power failure
PUMP	Pump failure
PWR-48	48 Volt power supply failure
RECT	Rectifier failure
RECTHI	Rectifier high voltage

Table 11-34 ENV_ALM Values (continued)

ENV_ALM Values	Description
RECTLO	Rectifier low voltage
SMOKE	Smoke
TOXICGAS	Toxic gas
VENTN	Ventilation system failure

11.13.16 ENV_CTL

Environmental control types as defined by Telcordia GR-833-CORE, Issue 2, November 1996, Appendix G.

Table 11-35 ENV_CTL Values

ENV_CTL Values	Description
AIRCOND	Air conditioning
ENGINE	Engine
FAN	Fan
GEN	Generator
HEAT	Heat
LIGHT	Light
MISC	Miscellaneous
SPKLR	Sprinkler

11.13.17 EQPT_TYPE

Identifies the type of equipment being provisioned into a slot.

Table 11-36 EQPT_TYPE Values

EQPT_TYPE Values	Description
AIC	The Alarm Interface Controller Card is an optional card which expands system management capabilities for the customer defined alarm I/O and orderwire functionality
DCC	The Data Communications Channel communicates network management information
DS1-14	A 14 port interface card supporting DS-1 facilities
DS1N-14	A 14 port interface card supporting DS-1 facilities
DS3-12	A 12 port interface card supporting DS-3 facilities
DS3CR-12	Cost reduced DS-3
DS3N-12	A 12 port interface card supporting DS-3 facilities
DS3XM-6	An interface card that converts six framed DS-3 network connections to 28x6 or 168 VT1.5s
E1000T-2	A two port interface card supporting 1000 Base T ethernet facilities
E100T-12	A 12 port interface card supporting 100 Base T ethernet facilities

Table 11-36 EQPT_TYPE Values (continued)

EQPT_TYPE Values	Description
EC1-12	A 12 port interface card supporting EC-1 facilities
EC1N-12	A 12 port interface card supporting EC-1 facilities
OC-12	An interface card that supports one or more OC-12 (622Mbs) optical facilities
OC12-IR-1	An interface card that supports one intermediate range OC-12 (622Mbs) optical facilities
OC12-LR-1	An interface card that supports one long range OC-12 (622Mbs) optical facilities
OC12-SR-1	An interface card that supports one short range OC-12 (622Mbs) optical facilities
OC192-LR-1	An interface card that supports one or more long range OC-192 optical facilities
OC-3	An interface card that supports multiple OC-3 (155Mbs) optical facilities
OC3-IR-4	An interface card that supports four intermediate range OC-3 (155Mbs) optical facilities
OC3-SR-4	An interface card that supports four short range OC-3 (155Mbs) optical facilities
OC-48	An interface card that supports one or more OC-48 (10Gbs) optical facilities
OC48-IR-1	An interface card that supports one intermediate range OC-48 (10Gbs) optical facilities
OC48-LR-1	An interface card that supports one long range OC-48 (10Gbs) optical facilities
OC48-SR-1	An interface card that supports one short range OC-48 (10Gbs) optical facilities
TCC	The Timing, Communication and Control card
TCC+	The Timing, Communication and Control+ card
XC	A Cross-Connect card
XC-192	A Cross-Connect card
XC-VT	A Cross-Connect card

11.13.18 EQUIP

Indicates the presence of a plug-in unit

Table 11-37 EQUIP Values

EQUIP Values	Description
EQUIP	The unit is Equipped - present
UNEQUIP	The unit is Unequipped - absent

11.13.19 EQUIPMENT_TYPE

Table 11-38 EQUIPMENT_TYPE Values

EQUIPMENT_TYPE Values	Description
AIC	AIC card
DS-1	DS-1 card
DS-1N	DS-1N card
DS-3	DS-3 card
DS-3N	DS-3N card
DS3XM	DS3XM card
E-100T	E-100T card
E-1000T	E-1000T card
EC-1	EC-1 card
EC-1N	EC-1N card
OC-12	OC-12 card
OC-3	OC-3 card
OC-48	OC-48 card
TCC	TCC card
TCC+	TCC+ card
XC-STS	XC-STS card
XC-VT	XC-VT card

11.13.20 EXT_RING

Indicates if the ring supports the extended K1/K2/K3 protocol.

Table 11-39 EXT_RING Values

EXT_RING Values	Description
N	Indicates the Ring does not support the extended K1/K2/K3 protocol
Y	Indicates the Ring does support the extended K1/K2/K3 protocol

11.13.21 FRAME_FORMAT

The frame format for a T1 port

Table 11-40 FRAME_FORMAT Values

FRAME_FORMAT Values	Description
D4	Frame format is D4
ESF	Frame format is ESF
UNFRAMED	Frame format is unframed

11.13.22 LINE_BUILDOUT

Table 11-41 LINE_BUILDOUT Values

LINE_BUILDOUT Values	Description
0-131	Line buildout range is 0-131
132-262	Line buildout range is 132-262
263-393	Line buildout range is 263-393
394-524	Line buildout range is 394-524
525-655	Line buildout range is 525-655

11.13.23 LINE_CODE

Table 11-42 LINE_CODE Values

LINE_CODE Values	Description
AMI	Line code value is AMI
B8ZS	Line code value is B8ZS (Bipolar with Eight-Zero Substitution)

11.13.24 LOCATION

Identifies the location where the action is to take place

Table 11-43 LOCATION Values

LOCATION Values	Description
FEND	Action occurs on the Far End of the facility
NEND	Action occurs on the Near End of the facility

11.13.25 LPBK_TYPE

Indicates the type of loopback that is to be operated or released

Table 11-44 LPBK_TYPE Values

LPBK_TYPE Values	Description
FACILITY	A type of loopback that connects the incoming received signal immediately following the optical-to-electrical conversion (before descrambling) to the associated transmitter in the return direction
TERMINAL	A loopback that connects the signal that is about to be transmitted (after scrambling but before the electrical-to-optical conversion) is connected to the associated, incoming receiver

11.13.26 MOD2

A generic object type

Table 11-45 MOD2 Values

MOD2 Values	Description
DS-1	DS-1 facility on DS3XM
EC-1	EC-1 facility
OC-12	OC-12 facility
OC-3	OC-3 facility
OC-48	OC-48 facility
STS-1	STS path
STS-12C	STS path
STS-3C	STS path
STS-48C	STS path
T1	DS-1 facility
T3	DS-3 facility
VT1	VT1 path

11.13.27 MOD2ALM

Alarm type for certain generic TL1 commands

Table 11-46 MOD2ALM Values

MOD2ALM Values	Description
DS-1	DS-1 alarm
E-100	E-100 alarm
E-1000	E-1000 alarm
EC-1	EC-1 alarm
OC-12	OC-12 alarm
OC-3	OC-3 alarm
OC-48	OC-48 alarm
STS-1	STS-1 alarm
STS-12C	STS-12C alarm
STS-3C	STS-3C alarm
STS-48C	STS-48C alarm
T1	T1 alarm
T3	T3 alarm
VT1	VT1 alarm

11.13.28 MOD2B

Alarm type for certain generic TL1 commands

Table 11-47 MOD2B Values

MOD2B Values	Description
BITS	BITS alarm
COMM	COMM alarm
DS-1	DS-1 alarm
E-100	E-100 alarm
E-1000	E-1000 alarm
EC-1	EC-1 alarm
ENV	ENV alarm
EQPT	EQPT alarm
OC-12	OC-12 alarm
OC-3	OC-3 alarm
OC-48	OC-48 alarm
STS-1	STS alarm
STS-12C	STS alarm
STS-3C	STS alarm
STS-48C	STS alarm
SYNCN	SYNCN alarm
T1	T1 alarm
T3	T3 alarm
TCC	TCC alarm
TCC+	TCC+ alarm
VT1	VT alarm

11.13.29 MODIFIER

Modifier for certain TL1 commands that are generic in their syntax

Table 11-48 MODIFIER Values

MODIFIER Values	Description
BITS	BITS command modifier
EQPT	Equipment command modifier
OC-12	OC-12 command modifier
OC-3	OC-3 command modifier
OC-48	OC-48 command modifier
STS-1	STS-1 command modifier
STS-12C	STS-12c command modifier
STS-3C	STS-3c command modifier

Table 11-48 MODIFIER Values (continued)

MODIFIER Values	Description
SYNCN	Synchronization command modifier
T3	T3/DS-3 command modifier

11.13.30 NOTIF_CODE

The 2-character Notification Code associated with an autonomous message

Table 11-49 NOTIF_CODE Values

NOTIF_CODE Values	Description
CL	The condition causing the alarm has Cleared
CR	A Critical alarm
MJ	A Major alarm
MN	A Minor alarm
NA	The condition is Not Alarmed
NR	The alarm is not reported

11.13.31 OCN_MONTYPE

OCN monitor type

Table 11-50 OCN_MONTYPE Values

OCN_MONTYPE Values	Description
CVL	Coding Violation - Line
ESL	Errored Second - Line
PJNEG	PPJC-PDET:Negative Pointer Justification
PJPOS	PPJC-PGEN:Negative Pointer Justification
PSC	Protection Switching Count
PSD	Protection Switching Duration
SEFS	Severely Errored Framing Seconds
UASL	Unavailable Second - Line

11.13.32 OCN_TYPE

Modifier used to differentiate the various levels of OC-N in the ENT/ED/DLT commands

Table 11-51 OCN_TYPE Values

OCN_TYPE Values	Description
OC-12	Optical Carrier level-12 (622Mbs)
OC-3	Optical Carrier level-3 (155Mbs)
OC-48	Optical Carrier level-48 (2.4Gbs)

11.13.33 ON_OFF

Disable or Enable Mode

Table 11-52 ON_OFF Values

ON_OFF Values	Description
OFF	Mode is disabled
ON	Mode is enabled

11.13.34 OPTICAL_MODE

Table 11-53 OPTICAL_MODE Values

OPTICAL_MODE Values	Description
SDH	The SDH optical mode the European format
SONET	The SONET optical mode the American format

11.13.35 PRIVILEGE

Security level

Table 11-54 PRIVILEGE Values

PRIVILEGE Values	Description
MAINT	Maintenance Security Level
PROV	Provision Security Level
RTRV	Retrieve Security Level
SUPER	Superuser Security Level

11.13.36 PROT_MOD_OP

Protection switch operation mode

Table 11-55 PROT_MOD_OP Values

PROT_MOD_OP Values	Description
FRCD	Force switch operation mode
MAN	Manual switch operation mode

11.13.37 PROTECTION_GROUP

Table 11-56 PROTECTION_GROUP Values

PROTECTION_GROUP Values	Description
1-1	1 to 1 protection group
1-N	1 to N protection group

11.13.38 PST

Primary State of the entity (e.g. facility)

Table 11-57 PST Values

PST Values	Description
IS	In-service
OOS	Out-of-Service

11.13.39 REVERTIVE_TIME

Table 11-58 REVERTIVE_TIME Values

REVERTIVE_TIME Values	Description
0.0 - 12.0	Revertive time is 0.0 to 12.0 minutes

11.13.40 REVERTIVE_TYPE

Table 11-59 REVERTIVE_TYPE Values

REVERTIVE_TYPE Values	Description
NR	Revertive type is disabled
R	Revertive type is enabled

11.13.41 RNG_TYPE

Defines the type of ring that is to be deployed for this path

Table 11-60 RNG_TYPE Values

RNG_TYPE Values	Description
BLSR2	2-Fiber Bidirectional Line Switched Ring
BLSR4	4-Fiber Bidirectional Line Switched Ring
UPSR	Unidirectional Path Switched Ring

11.13.42 SD_BER

The threshold for declaring Signal Degrade on a facility or path

Table 11-61 SD_BER Values

SD_BER Values	Description
1E-5 - 1E-9	SDBER is the 1E-5 to 1E-9

11.13.43 SDCC_MODE

Enables or disables the Section Data Communications Channel (SDCC) for the specified facility

Table 11-62 SDCC_MODE Values

SDCC_MODE Values	Description
N	Section Data Communications Channel is disabled for this facility
Y	Section Data Communications Channel is enabled for this facility

11.13.44 SERV_EFF

Indicates the effect of the alarm on service

Table 11-63 SERV_EFF Values

SERV_EFF Values	Description
NSA	The condition is Non-Service Affecting
SA	The condition is Service Affecting

11.13.45 SF_BER

The threshold for declaring Signal Failure on a facility or path

Table 11-64 SF_BER Values

SF_BER Values	Description
1E-3 - 1E-5	SFBER is the 1E-3 to 1E-5

11.13.46 SIDE

The role the unit is playing in the protection group

Table 11-65 SIDE Values

SIDE Values	Description
PROT	The entity is the protection unit in the protection group
WORK	The entity is a working unit in the protection group

11.13.47 STATE

The provisioned state of the equipment unit or facility

Table 11-66 STATE Values

STATE Values	Description
IS	The entity is InService
OOS-AS	The entity is Out-Of-Service and Assigned
OOS-UAS	The entity is Out-Of-Service and UnAssigned

11.13.48 STATUS

Indicates whether the unit in the pair is Active or Standby

Table 11-67 Status Values

STATUS Values	Description
ACT	The entity is the Active unit in the protection group
NA	Status is unavailable
STBY	The entity is the standby unit in the protection group

11.13.49 STM_TYPE

The Synchronous Transport Mode of the NE

Table 11-68 STM_TYPE Values

STM_TYPE Values	Description
SDH	The NE is operating in Synchronous Digital Hierarchy mode
SONET	The NE is operating in Synchronous Optical NETwork mode

11.13.50 STS_MONTYPE

Table 11-69 STS_MONOTYPE Values

STS_MONTYPE Values	Description
CVP	Coding Violation - P
ESP	Errored Second - Path
SESP	Severely Errored Second - Path
UASP	Unavailable Second - Path

11.13.51 STS_PATH

Modifier for some of the STS commands

Table 11-70 STS_PATH Values

STS_PATH Values	Description
STS-1	Synchronous Transport Signal level-1 (51Mbs)
STS-12C	Synchronous Transport Signal level-12 Concatenated (622Mbs)
STS-3C	Synchronous Transport Signal level-3 Concatenated (155Mbs)

11.13.52 SWITCH

The type of switch to be initiated

Table 11-71 SWITCH Values

SWITCH Values	Description
FRCD	Force a switch unless another FRCD or LOCKOUT is in effect
LOCKOUT	Locks the facility out of switching. The system cannot switch to the protect facility to carry service
MAN	Requests a manual switch of the facility

11.13.53 SYNC_GENERATION

Synchronization status message set generation

Table 11-72 SYNC_GENERATION Values

SYNC_GENERATION Values	Description
GEN1	First generation SSM set
GEN2	Second generation SSM set

11.13.54 SYNC_MODE

Table 11-73 SYNC_MODE Values

SYNC_MODE Values	Description
FRNG	Reset operation mode
FST	Reset operation mode
HLDOVR	Reset operation mode
NORM	Reset operation mode

11.13.55 SYNC_QUALITY_LEVEL

Reserved for network synchronization quality level

Table 11-74 SYNC_QUALITY_LEVEL Values

SYNC_QUALITY_LEVEL Values	Description
ABOVE-PRS	Better than Primary Reference Source
ABOVE-SMC	Between SMC and ST3
ABOVE-ST2	Between ST2 and STU
ABOVE-ST3	Between ST3 and ST2
ABOVE-ST3E	Between ST3E and TNC
ABOVE-ST4	Between ST4 and ST3
ABOVE-STU	Between STU and PRS
ABOVE-TNC	Between TNC and PRS
BELOW-ST4	Below ST4 but still usable
SAME-AS-DUS	Disable the RES message by equating it to DUS

11.13.56 TIMING_MODE

Timing mode for the current node

Table 11-75 TIMING_MODE Values

TIMING_MODE Values	Description
EXTERNAL	The node derives its clock from the BITS input
LINE	The node derives its clock from the SONET lines

11.13.57 TMG_REF

Identifies whether or not this entity is the Timing Reference for its group. For equipment, it identifies the facility that is supplying the timing reference. For interface groups, it identifies the card that is supplying the main timing reference.

Table 11-76 TMG_REF Values

TMG_REF Values	Description
N	This facility or card is not a timing reference
Y	This facility or card is a timing reference

11.13.58 TMPR

Performance parameter

Table 11-77 TMPR Values

TMPR Values	Description
15MIN	Performance Parameter Accumulation Interval Length - Every 15 Minutes
1DAY	Performance Parameter Accumulation Interval Length - Every 24 Hours

11.13.59 USE_DST

Identifies whether Daylight Saving Time is recognized in the area where this NE is deployed

Table 11-78 USE_DST Values

USE_DST Values	Description
N	Daylight Saving Time is not recognized
Y	Daylight Saving Time is recognized

11.13.60 VALIDITY

Response validity

Table 11-79 VALIDITY Values

VALIDITY Values	Description
COMPL	Complete Response
PRTL	Partial Response

11.13.61 Performance Monitoring Parameters by Line Type

Table 11-80 Performance Monitoring Parameters by Line Type

	OC-n	T1	T3	STS	VT1.5
CVL	Y	Y	Y		
CVP		Y	Y	Y	
CVS	Y				
CVV					Y
ESL	Y	Y	Y		
ESP		Y	Y	Y	
ESS	Y				
ESV					Y
FCP				Y	
FCL	Y				
PJNEG	Y				
PJPOS	Y				
PSC	Y				
PSD	Y				
SASP		Y	Y		
SEFS	Y				
SESL	Y	Y	Y		
SESP		Y	Y	Y	
SESS	Y				
SESV					Y
UASL	Y				
UASP		Y	Y	Y	
UASV					Y
AISSP		Y	Y		
CVCPP			Y		
ESCPP			Y		
LOSSL			Y		
SASCPP			Y		
SESCPP			Y		
UASCPP			Y		

11.14 Errors

Errors may be generated by any command or command response message. The format of an error message is as follows:

```
    sid date time
M  ctag DENY
    <errcde>
    /* <errmsg> */
;
```

Table 11-81 Error Codes

Error Code (errcde)	Error Type	Error Message (errmsg)
EANS	EQUIPAGE	Access Not Supported
EATN	EQUIPAGE	Not Valid for Access Type
EFON	EQUIPAGE	Feature Option Not Provided
EN2T	EQUIPAGE	Not 2-Wire Terminate and Leave
ENAC	EQUIPAGE	Not Equipped with Alarm Cutoff
ENAD	EQUIPAGE	Not Equipped with Audit Capability
ENAR	EQUIPAGE	Not Equipped with Automatic Reconfiguration
ENAT	EQUIPAGE	Request Not Valid for Access Type
ENDG	EQUIPAGE	Not Equipped with Diagnostic Capability
ENDS	EQUIPAGE	Not Equipped with Duplex Switching
ENEA	EQUIPAGE	Not Equipped with Error Analysis Capability
ENEQ	EQUIPAGE	Not Equipped
ENEX	EQUIPAGE	Not Equipped with Exercise Capability
ENFE	EQUIPAGE	Feature Not Provided
ENFL	EQUIPAGE	Not Equipped for Fault Locating
ENHN	EQUIPAGE	Not Hybrid Network
ENMB	EQUIPAGE	Not Multipoint Bridge
ENMD	EQUIPAGE	Not Equipped with Memory Device
ENPM	EQUIPAGE	Not Equipped for Performance Monitoring
ENPS	EQUIPAGE	Not Equipped with Protection Switching
ENRE	EQUIPAGE	Not Recognized Equipage
ENRI	EQUIPAGE	Not Equipped for Retrieving Specified Information
ENRS	EQUIPAGE	Not Equipped for Restoration
ENSA	EQUIPAGE	Not Equipped for Scheduling Audit
ENSG	EQUIPAGE	Not Software Generic
ENSI	EQUIPAGE	Not Equipped for Setting Specified Information
ENSS	EQUIPAGE	Not Equipped with Synchronization Switching
ENTL	EQUIPAGE	Not Terminate and Leave
ERLC	EQUIPAGE	Red-Lined Circuit
ERNS	EQUIPAGE	RTU Does Not Support Command
ESPG	EQUIPAGE	Software Program
ETNS	EQUIPAGE	TSC Does Not Support Command

Table 11-81 Error Codes (continued)

Error Code (errcde)	Error Type	Error Message (errmsg)
FNCR	FAULT	NE Failure - Circuit Restored to Last Condition - Monitor or Terminate
FNDT	FAULT	No Dial Tone Detected
FNEC	FAULT	NTE Has Lost 8-KHZ Byte Clock
FNSC	FAULT	NTE Has Lost 16-KHZ Byte Clock
FRCE	FAULT	RTU Component or Configuration Error
FRDA	FAULT	RTU Does Not Answer the Call
FREC	FAULT	RTU Eight KHZ Byte Clock Lost
FRNR	FAULT	RTU Does Not Reply
IBEX	INPUT	Block Extra
IBMS	INPUT	Block Missing
IBNC	INPUT	Block Not Consistent
ICNV	INPUT	Command Not Valid
IDMS	INPUT	Data Missing
IDNC	INPUT	Data Not Consistent
IDNV	INPUT	Data Not Valid
IDRG	INPUT	Data Range Error
IIAC	INPUT	Invalid Access Identifier (AID)
IICM	INPUT	Invalid Command
IICT	INPUT	Invalid Correlation Tag
IIDT	INPUT	Invalid Data Parameter
IIFM	INPUT	Invalid Data Format
IIPG	INPUT	Invalid Parameter Grouping
IISP	INPUT	Invalid Syntax or Punctuation
IITA	INPUT	Invalid Target Identifier
INAC	INPUT	Access Number Not Correct
INUP	INPUT	Non-Null Unimplemented Parameter
IPEX	INPUT	Parameter Extra
IPMS	INPUT	Parameter Missing
IPNC	INPUT	Parameter Not Consistent
IPNV	INPUT	Parameter Not Valid
ISCH	INPUT	Syntax Invalid Character
ISPC	INPUT	Syntax Punctuation
ITSN	INPUT	Invalid/Inactive Test Session Number
PICC	PRIVILEGE	Illegal Command Code
PIMA	PRIVILEGE	Invalid Memory Address
PIMF	PRIVILEGE	Invalid Memory File
PIUC	PRIVILEGE	Illegal Privilege Code

Table 11-81 Error Codes (continued)

Error Code (errcde)	Error Type	Error Message (errmsg)
PLNA	PRIVILEGE	Login Not Active
RABY	RESOURCE	All Taps Busy
RALB	RESOURCE	All Units of Requested Type are Busy
RANB	RESOURCE	Access Network Busy
RCBY	RESOURCE	Circuit Busy
RCIN	RESOURCE	Requested Circuit ID Does Not Exist
RNAN	RESOURCE	Requested NE Access Number Does Not Exist
RNAU	RESOURCE	Requested NE Access Number Unassigned
RNBY	RESOURCE	NE is Busy
RRCP	RESOURCE	Unit Specified by Routing Code Busy
RRNG	RESOURCE	Requested Changes Exceeds Range
RTBY	RESOURCE	Requested Tap Busy
RTEN	RESOURCE	Requested Tab Does Not Exist
RTUB	RESOURCE	Test Unit Busy
SAAL	STATUS	Already Allowed
SAAS	STATUS	Already Assigned
SABT	STATUS	Aborted
SACS	STATUS	Access Unit Cannot Sync on Facility Signal
SADC	STATUS	Already Disconnected
SADS	STATUS	Access Unit in Diagnostic State
SAIN	STATUS	Already Inhibited
SAIS	STATUS	Already In-Service
SAMS	STATUS	Already in Maintenance State
SAOP	STATUS	Already Operated
SAOS	STATUS	Already Out-of-Service
SAPF	STATUS	Access Path Continuity Check Failed
SAPR	STATUS	Already in Protection State
SARB	STATUS	All Resources Busy
SATF	STATUS	Automatic Test Failed
SCAT	STATUS	Circuit is Already Connected to Another Tap
SCBS	STATUS	Channel Busy
SCIS	STATUS	Circuit in Split Condition
SCNA	STATUS	Command Not Able to be Aborted
SCNF	STATUS	Command Not Found
SCNS	STATUS	Circuit Not in Split Condition
SCOS	STATUS	Channel Out-of-Service
SCSD	STATUS	Can't Split DS0B Circuit

Table 11-81 Error Codes (continued)

Error Code (errcde)	Error Type	Error Message (errmsg)
SCSN	STATUS	Invalid Command Sequence
SDAS	STATUS	Diagnosis Already Started
SDBE	STATUS	Internal Data Base Error
SDFA	STATUS	Duplex Unit Failed
SDLD	STATUS	Duplex Unit Locked
SDNA	STATUS	Dumple Unit Not Available
SDNC	STATUS	Input Data is Not Consistent With NE Data
SDNR	STATUS	Data Not Ready
SDNS	STATUS	Diagnosis Not Started Yet
SEOS	STATUS	NTE is Out-of-Service
SFAS	STATUS	Fault Locating Already Started
SFNS	STATUS	Fault Locating Not Started yet
SFYA	STATUS	Facility Reports Yellow Alarm
SLNS	STATUS	Log Not Started Yet
SLOS	STATUS	TSC to RTU Link Out-of-Service
SNCC	STATUS	Not Cross-Connected
SNCN	STATUS	NTE Unable to Execute Command
SNDS	STATUS	NTE is in a Diagnostic State
SNIM	STATUS	NTE Access Complete, Circuit was in Monitor State
SNIS	STATUS	Not in Service
SNML	STATUS	No Monitor Line Established
SNNB	STATUS	NTE Could Not Sync on DS0B Signal
SNNS	STATUS	NTE Could Not Sync on DS-1 Signal
SNOS	STATUS	NTE is Out-of-Service
SNPR	STATUS	Not in Protection State
SNRM	STATUS	System Not in Restoration Mode
SNRS	STATUS	Not Reserved
SNSR	STATUS	No Switch Request Outstanding
SNVS	STATUS	Not in Valid State
SNYA	STATUS	NTE has Detected a Yellow Alarm
SOSE	STATUS	Operating System Error
SOST	STATUS	Out-of-Service, Testing
SPFA	STATUS	Protection Unit Failed
SPLD	STATUS	Protection Unit Locked
SPNA	STATUS	Process Not Able to be Aborted
SPNF	STATUS	Process Not Found
SRAC	STATUS	Requested Access Configuration is Invalid

Table 11-81 Error Codes (continued)

Error Code (errcde)	Error Type	Error Message (errmsg)
SRAN	STATUS	Unable to Release Access System
SRCI	STATUS	Requested Command(s) Inhibited
SRCN	STATUS	Requested Condition Already Exists
SROF	STATUS	Requested Operation Failed
SROS	STATUS	Required RTU Out of Service
SRQN	STATUS	Invalid Request
SRTN	STATUS	Unable to Release Tap
SRTO	STATUS	Reply Timeout Occurred
SSCE	STATUS	Systemic (SNIDER) Communications Error
SSNG	STATUS	Subrate Selected is Incorrect
SSNP	STATUS	Speed Selected is Incorrect
SSNQ	STATUS	Test Signal Not QRS
SSRD	STATUS	Switch Request Denied
SSRE	STATUS	System Resources Exceeded
STAB	STATUS	Test Aborted
STLC	STATUS	Tap Unable to Locate Channel
STNO	STATUS	TSC/RTU to TAU Link Out of service
STOS	STATUS	Test Access Unit Out of Service
STTI	STATUS	Tap Idle
SWFA	STATUS	Working Unit Failed
SWLD	STATUS	Working Unit Locked

11.15 Echo

In order to improve telnet functionality for automated systems, the echo function was been turned off in Release 2.1.0. This change is transparent to users running standard UNIX-compliant telnet clients; however, PC users may need to change their client setup to enable “local echo.” This is normally accomplished by a pull-down menu or a preference attribute.

To test the local echo on your PC client, use the RTRV-HDR command. If you receive a response but no data, set local echo ON.

Regulatory and Compliance Requirements

A.1 Overview

This appendix lists customer, industry, and government requirements met by the Cisco ONS 15454.

A.1.1 Emissions/Immunity

The ONS 15454 meets the following regulatory requirements:

- FCC Part 15 Class A- for the United States
- ICES-003 Class A- for Canada
- EN55022 Class A-readiness for the EU and Asia.

The ONS 15454 meets the following customer and industry requirements:

- Telcordia GR-1089-CORE
- WorldCom Electrostatic Discharge immunity
- EN61000-4-2 Electrostatic Discharge immunity
- EN61000-4-3 Radiated immunity
- EN61000-4-4 Electrical fast transient/burst immunity
- EN61000-4-6 Conducted immunity

A.1.2 Safety

The ONS 15454 meets the following regulatory requirements:

- UL1950/CSA950- for the United States and Canada
- EN60950-readiness for the EU and Asia

The ONS 15454 meets the following customer and industry requirements:

- Telcordia GR-1089-CORE

A.1.3 Environmental/Mechanical

The ONS 15454 meets the following customer and industry requirements:

- Telcordia GR-63-CORE

- Bell Atlantic NEBS Requirements, RNSA-NEB-95-0003, Rev 8
- SBC Local Exchange Carriers, Network Equipment Power, Grounding, Environmental, and Physical Design Requirements, TP76200MP.
- Pacific Bell/Nevada Bell, Detailed Method of Procedure Number 1 (13.01), Section 8
- AT&T Network Equipment Development Standards (NEDS) Generic Requirements, AT&T 801-900-160

Glossary

Numerics

1:1 protection A card protection scheme that pairs a working card with a protect card of the same type in an adjacent slot. If the working card fails, the traffic from the working card switches to the protect card. When the failure on the working card is resolved, traffic reverts back to the working card if this option is set. This protection scheme is specific to electrical cards.

1:N protection A card protection scheme that allows a single card to protect several working cards. When the failure on the working card is resolved, traffic reverts back to the working card. A term specific to electrical cards.

1+1 protection A card protection scheme that pairs a single working card with a single dedicated protect card. A term specific to optical cards.

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 the ONS 15454. These objects include individual pieces of equipment, transport spans, access tributaries, and others.

AMI Alternate Mark Inversion. Line-code format used on T1 circuits that transmits ones by alternate positive and negative pulses. Zeroes are represented by 01 during each bit cell and ones are represented by 11 or 00, alternately, during each bit cell. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called binary-coded alternate mark inversion.

APS Automatic Protection Switching. SONET switching mechanism that routes traffic from working lines to protect lines in case a line card failure or fiber cut occurs.

ATAG Autonomous Message Tag. ATAG is used for TL1 message sequencing.

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.

Bit rate Speed at which bits are transmitted, usually expressed in bits per second.

BITS Building Integrated Timing Supply. A single building master timing supply that minimizes the number of synchronization links entering an office. Sometimes referred to as a Synchronization Supply Unit.

BLSR Bidirectional Line Switch Ring. SONET ring architecture that provides working and protection fibers between nodes. If the working fiber between nodes is cut, traffic is automatically routed onto the protection fiber.

Blue band Dense Wavelength Division Multiplexing (DWDM) wavelengths are broken into two distinct bands: red and blue. DWDM cards for the ONS 15454 operate on wavelengths between 1530.33nm and 1542.94nm in the blue band. The blue band is the lower frequency band.

Bridge Device that connects and passes packets between two network segments that use the same communications protocol. In general, a bridge will filter, forward, or flood an incoming frame based on the MAC address of that frame.

Broadcast Data packet that will be sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*. See also *Broadcast address*.

Broadcast address Special address reserved for sending a message to all stations. Generally, a broadcast address is a MAC destination address of all ones.

Broadcast storm Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

Bus Common physical signal path composed of wires or other media across which signals can be sent from one part of a computer to another.

C

C2 byte The C2 byte is the signal label byte in the STS path overhead. This byte tells the equipment what the SONET payload envelope contains and how it is constructed.

Cell Basic Unit of ATM switching and multiplexing. Cells contain identifiers that specify the data stream to which 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 the ONS 15454 system responds to a specific command, it includes the command's CTAG in the reply. This eliminates discrepancies about which response corresponds to which command.

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 the ONS 15454 using an Internet browser.

CTM Cisco Transport Manager. A Java-based network management tool used to support large networks of Cisco 15000-class equipment.

D

DCC Data Communications Channel. Used to transport information about operation, administration, maintenance, and provisioning (OAM&P) over a SONET interface. DCC can be located in section DCC (SDCC) or line overhead (LDCC.)

Demultiplex To separate multiple multiplexed input streams from a common physical signal back into multiple output streams. See also *Multiplexing.*

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.

EIA Electrical Interface Assemblies. Provides connection points for the ONS 15454 and DS-1, DS-3, or EC-1 units.

EMI Electromagnetic Interference. Interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

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 provide the capability to increase the aggregate LAN bandwidth by allowing simultaneous switching of packets between switch ports. Ethernet switches subdivide previously-shared LAN segments into multiple networks with fewer stations per network.

External timing reference A timing reference obtained from a source external to the communications system, such as one of the navigation systems. Many external timing references are referenced to Coordinated Universal Time (UTC).

F

Falling threshold — A falling threshold is the counterpart to a rising threshold. When the number of occurrences drops below a falling threshold, this triggers an event to reset the rising threshold. See also *rising threshold*.

FDDI — Fiber Distributed Data Interface. LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.

Frame — Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control that surrounds the user data contained in the unit.

Free run synchronization mode — Occurs when the external timing sources have been disabled and the ONS 15454 is receiving timing from its Stratum 3 level internal timing source.

G

GBIC — Gigabit Interface Converter. A hot-swappable input/output device that plugs into a Gigabit Ethernet port to link the port with the fiber optic network.

H

Hard reset — The physical removal and insertion of a card.

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, 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 15454.

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, resisters, and coils.

Path Layer The segment between the originating equipment and the terminating equipment. This path segment may encompass several consecutive line segments or segments between two SONET devices.

Payload Portion of a cell, frame, or packet that contains upper-layer information (data).

PCM Pulse Code Modulation. 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 reachability of 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 security level that allows the user to access only provisioning and maintenance options in CTC. See also *Superuser*, *Maintenance user,* and *Retrieve user.*

Q

Queue In routing, a backlog of packets waiting to be forwarded over a router interface.

R

Red band DWDM wavelengths are broken into two distinct bands: red and blue. The red band is the higher frequency band. The red band DWDM cards for the ONS 15454 operate on wavelengths between 1547.72nm and 1560.61nm.

Retrieve user A security level that allows the user to retrieve and view CTC information but not set or modify parameters. See also *Superuser*, *Maintenance user*, and *Provisioning user*.

Revertive switching A process that sends electrical interfaces back to the original working card after the card comes back online.

Rising threshold The number of occurrences (collisions) that must be exceeded to trigger an event.

RMON Remote Network Monitoring. Allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

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 15454 network nodes use the same date and time reference. The server synchronizes alarm timing during power outages or software upgrades.

Soft reset A soft reset reloads the operating system, application software, etc., and reboots the card. It does not initialize the ONS 15454 ASIC hardware.

SONET Synchronous Optical Network. High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

Spanning tree Loop-free subset of a network topology. See also *STA* and *STP*.

SPE Synchronous Payload Envelope. A SONET term describing the envelope that carries the user data or payload.

SSM Sync Status Messaging. A SONET protocol that communicates information about the quality of the timing source using the S1 byte of the line overhead.

STA Spanning-Tree Algorithm. An algorithm used by the spanning tree protocol to create a spanning tree. See also *Spanning tree* and *STP.*

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 uses the spanning-tree algorithm to enable a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. See also *Spanning tree, STA,* and *Learning bridge.*

STS-1 Synchronous Transport Signal 1. Basic building block signal of SONET, operating at 51.84 Mbps for transmission over OC-1 fiber. Faster SONET rates are defined as STS-*n*, where *n* is a multiple of 51.84 Mbps. See also *SONET.*

Subnet mask 32-bit address mask used in IP to indicate the bits of an IP address that are used for the subnet address. Sometimes referred to simply as mask. See also *IP address mask* and *IP address*.

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.

TCC Timing Communications and Control card. A common control card is the main processing center of the ONS 15454. A TCC card provides system initialization, provisioning, alarm reporting, maintenance, and diagnostics.

TDM Time Division Multiplexing. Allocates bandwidth on a single wire for information from multiple channels based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.

Telcordia Telcordia Technologies, Inc., formerly named Bellcore. Eighty percent of the U.S. telecommunications network depends on software invented, developed, implemented, or maintained by Telcordia.

TID Target Identifier. Identifies the particular network element (in this case, the ONS 15454) where each TL1 command is directed. The TID is a unique name given to each system at installation.

TLS Transparent LAN Service. Provides private network service across a SONET backbone.

Transponder Optional devices of a DWDM system providing the conversion of one optical wavelength to a precision narrow band wavelength.

Trap Message sent by an SNMP agent to an NMS (CTM), console, or terminal to indicate the occurrence of a significant event, such as an exceeded threshold.

Tributary The lower-rate signal directed into a multiplexer for combination (multiplexing) with other low rate signals to form an aggregate higher rate level.

Trunk Network traffic travels across this physical and logical connection between two switches. A backbone is composed of a number of trunks. See also *Backbone*.

Tunneling Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. See also *encapsulation*.

U

Unicast The communication of a single source to a single destination.

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.

X

XC STS Cross-connect card. A common control card that acts as the central element for switching. The XC card establishes connections and performs time division switching (TDS).

XCVT Cross-connect card with virtual tributary capability.

Acronyms

Numerics

10BaseT standard 10 megabit per second local area network over unshielded twisted pair copper wire

100BaseT standard 100 megabit per second ethernet network

100BaseTX specification of 100BaseT that supports full duplex operation

A

ACO Alarm Cutoff

ACT/STBY Active/Standby

ADM Add-Drop Multiplex

AIC Alarm Interface Controller

AID Access Identifier

AIP Alarm Interface Panel

AIS Alarm Indication Signal

AIS-L Line Alarm Indication Signal

AMI Alternate Mark Inversion

ANSI American National Standards Institute

APS Automatic Protection Switching

ARP Address Resolution Protocol

ATAG Autonomous Message Tag

ATM Asynchronous Transfer Mode

AWG American Wire Gauge

B

B8ZS	Bipolar 8 Zero Substitution
BER	Bit Error Rate
BIC	Backplane Interface Connector
BIP	Bit Interleaved Parity
BITS	Building Integrated Timing Supply
BLSR	Bidirectional Line Switched Ring
BNC	Bayonet Neill-Concelman (coaxial cable bayonet locking connector)
BPDU	Bridge Protocol Data Unit

C

CAT 5	Category 5 (cabling)
CCITT	Consultative Committee International Telegraph and Telephone (France)
CEO	Central Office Environment
CEV	Controlled Environment Vaults
CLEI	Common Language Equipment Identifier code
CLNP	Correctionless Network Protocol
CMIP	Common Management Information Protocol
CMS	Cerent Management System
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

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
GBIC	Gigabit Interface Converter
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
IEC	InterExchange Carrier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
I/O	Input/Output

ITU-T	The International Telecommunication Union- Telecommunication Standards Sector

J

JRE	Java Runtime Environment

K

K	One Thousand

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
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
POP	Point of Presence
PPMN	Path Protected Mesh Network

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
SDDC	Section Data Communications Channel
SDH/SONET	Synchronous Digital Hierarchy/Synchronous Optical Network
SELV	Safety Extra Low Voltage
SF	Super Frame
SML	Service Management Layer
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SONET	Synchronous Optical Network

SPE	Synchronous Payload Envelope
SSM	Synchronous Status Messaging
STA	Spanning Tree Algorithm
STP	Shielded Twisted Pair
STS-1	Synchronous Transport Signal Level 1
SWS	SONET WAN Switch
SXC	SONET Cross Connect ASIC

T

TAC	Technical Assistance Center
TBOS	Telemetry Byte Oriented Serial protocol
TCC	Timing Communications and Control Card
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
X.25	Protocol providing devices with direct connection to a packet switched network

A

Add Drop Multiplexer *See* ADM
ADM
  Description 4-30
  Converting to UPSR 4-32, 4-35
  Setting up 4-31
AIC card
  Description 2-19
  Input/output alarm contacts 2-19
  Orderwire
    description 2-20
    provisioning 5-12
  Provisioning 5-9
  Specifications 2-22
  Virtual wires 5-11
AIP
  Description 1-25
  Accessing 1-25
  Replacing 1-25
Alarm Interface Controller card *See* AIC card
Alarm Interface Panel *See* AIP
Alarm Pin Field
  Description 1-28
  Access 1-25
Alarms, CTC 9-1
  AIS-L
    EC-1 9-5
    OCN 9-5
  AIS-P, I/O 9-6
  AIS-V, DS1 and DS3XM-6 9-6
  APSB, OCN 9-7
  APSCIMP, OC-12 and OC-48 in BLSR 9-7
  APSCM, OCN in linear mode 9-8
  APSMM, OCN in linear mode 9-9
  AUTORESET 9-9
  BKUPMEMP 9-10
  BLSROOSYNC 9-11
  CARLOSS, E100T-12 and E1000-2 9-12
  CONCAT, OCN 9-13
  CONNLOS, OC12 and OC-48 in BLSR 9-14
  CONTBUS-A 9-15
  CONTBUS-A-18, TCC and TCC+ 9-16
  CONTBUS-B 9-17
  CONTBUS-B-18, TCC 9-18
  CTNEQPT-PBXPROT 9-19
  CTNEQPT-PBXWORK 9-21
  DATAFLT, TCC 9-23
  DFLTK, OCN 9-23
  DISCONNECTED 9-24
  EOC, OCN 9-25
  EQPT 9-26
  EXTERNAL, AIC 9-27
  FAILTOSW-PATH, UPSR 9-27
  FAN 9-29
  FE-AIS, DS3XM-6 9-29
  FE-DS1-MULTLOS, DS3XM-6 9-30
  FE-DS1-SNGLLOS, DS3XM-6 9-31
  FE-EQPT-FAIL-SA, DS3XM-6 9-31
  FE-EQPT-NSA, DS3XM-6 9-32
  FE-IDLE, DS3XM-6 9-32
  FE-LOF, DS3XM-6 9-33
  FE-LOS, DS3XM-6 9-33
  FORCED-REQ, OCN in linear mode 9-34
  FRNGSYNC 9-34
  HITEMP 9-35
  HLDOVERSYNC 9-35
  IMPROPRMVL 9-36
  INCOMPATIBLE-SW 9-37
  INCON, OC-12 and OC-48 in BLSR 9-38
  Index of Alarms 9-2
  LBKFACILITY, OCN 9-38, 9-39
  LOCKOUTOFPR-RING 9-40
  LOF
    DS1 9-43
    DS3XM-6 9-41
    EC-1 9-45
    OCN 9-44
    TCC 9-41
  LOP, I/O 9-46
  LOP-V, DS3XM-6 and DS1 9-47
  LOS
    DS3, DS3XM-6, DS1 9-48
    EC-1 9-50
    OCN 9-49
  LPBKDS1FEAC, DS3XM-6 9-50
  LPBKDS3FEAC 9-51
  LPBKFACILITY
    DS1 9-52
    DS3 and DS3XM6 9-51
  LPBKTERMINAL
    DS1 9-53
    DS3 and DS3XM-6 9-53
  LPBKTERMINAL, OCN 9-39
  MANRESET 9-54
  MANUAL-REQ
    OCN 9-54
    XC and XCVT 9-55
  MEA, XC and I/O 9-56
  MEM-GONE, TCC and TCC+ 9-57
  MEM-LOW, TCC and TCC+ 9-57

NODEMIS, OC-12 and OC-48 in BLSR 9-58
NOT-AUTHENTICATED 9-59
PDI-P 9-59
PLM-P 9-60
PLM-V 9-62
PWRRESTART 9-62
RAI, DS3XM-6 9-63
RCVRMISS, DS1 9-63
RFI-L, OCN and EC-1 9-64
RFI-P 9-64
RFI-V 9-65
SDBER, OCN 9-66
SFBER, OCN 9-67
SQUELCH 9-68
STU 9-68
SWTOPRI 9-69
SWTOSEC 9-69
SWTOTHIRD 9-69
SWTRANSFER, TCC 9-70
SYNCPRI, TCC 9-70
SYNCSEC, TCC 9-71
SYNCTHIRD, TCC 9-71
SYSBOOT, TCC 9-72
Threshold Crossing Events 9-79
TRMTMISS, DS1 9-73
UNEQ-P, I/O 9-73
UNEQ-V, DS1 and DS3XM-6 9-74
Alarms, TL1 11-1
AMP CHAMP *See* EIA, *See* Cable Management

B

Backplane
BIC 1-53
Lower backplane cover 1-24
Sheet metal covers 1-18
Bay Assembly *See* Shelf Assembly
BIC Rear Cover 1-53
Bidirectional Line Switched Ring *See* BLSR
BITS 1-30, 11-9
BLSR
Description 4-1
Adding a node 4-10
Dropping a node 4-13
Moving trunk cards 4-14
Sample application 4-3
Setting up 4-6
Subtending 4-27
Testing 4-10
Timing 4-8

C

Cable Management
Description 1-12
Alarm 1-53
AMP CHAMP 1-53
Coaxial 1-51
Optical 1-50
Twisted pair 1-52
Cables *See* Cable Management, *See* Installing the ONS 15454
Card Protection
Converting DS from 1 for 1 to 1 for N 5-14
Creating a protection group 3-26
Deleting a protection group 3-28
Editing a protection group 3-28
Electrical 2-2
1 for 1 2-2
1 for N 2-3
and AMP CHAMP connectors 2-5
and BNC connectors 2-4
and High-density BNC connectors 2-4
and SMB connectors 2-5
backplane differences 2-4
Multiport 2-5
Optical 2-5
Unprotected 2-6
Card Provisioning 5-1 to 5-20
Alarm Interface Controller *See* AIC card
Electrical cards 5-1
Optical cards 5-6
Supporting STM-1 signals 5-8
Card Replacement 10-11
Card Slots 1-36
Cards
Individual cards are indexed by name
Common control, overview 2-1
Electrical, overview 2-1
Ethernet, overview 2-2
Installing 1-35
Optical, overview 2-1
Replacement 10-11
Slots 1-36
Turn-up 1-35, 1-37
Circuits
Creating 4-40
DCC tunneling 4-47

Editing 4-46
Hub and spoke Ethernet circuit 7-45
Manual Ethernet cross-connects 7-54
Monitoring 4-45
Shared packet ring Ethernet circuit 7-35
Cisco Transport Controller *See* CTC
CMS *See* CTC 3-1
CMS.INI file *See*Networks, Managing multiple rings
Cross Connect card
Description 2-11
Capacities 4-40
Card-level LEDs 2-12
Specifications 2-13
Turn-up 1-38
Upgrading to XCVT 5-18
Cross Connect VT card
Capacities 4-40
Card-level LEDs 2-16
Compatibility with XC card 2-16
Description 2-14
Specifications 2-18
Turn-up 1-38
VT mapping 2-15
with DS3XM-6 cards 2-16
CTC
Alarms
See Also Alarms, CTC
colors 3-19
history 3-19
using the alarms tab 3-19
viewing 3-18
and Solaris workstations 3-2
Backup the database 10-7
Card inventory 3-33
Changing format of data 3-34
Computer requirements 3-1
Connecting PCs to the ONS 15454 3-5
LAN connections 3-8
Logging in 3-9
Navigation 3-14
Network view procedures 3-13
Printing 3-34
Remote access 3-9
Setup
card protection 3-26
network 3-22
node 3-21
security levels 3-24
timing parameters 3-29
TL1 access 3-9
Views
card 3-14
description 3-11
network 3-12
node 3-12
parent view 3-11

D

DCC
and Ethernet manual cross-connects 7-54
DCC Tunneling
Creating 4-48
Description 4-47
Dense Wavelength Division Multiplexing *See* DWDM
Diagnostic files, creating 4-65
Documentation
CD-ROM xxxvii
Obtaining xxxvii
DS1-14 Card
in a Facility loopback 4-50
DS1-14 card
Description 2-26
Card-level LEDs 2-27
Port-level indicators 2-27
Specifications 2-27
DS1N-14 card
Description 2-29
Card-level LEDs 2-30
Port-level indicators 2-30
Specifications 2-30
DS3-12 card
Description 2-32
Card-level LEDs 2-33
Port-level indicators 2-33
specifications 2-33
DS3N-12 card
Description 2-35
Card-level LEDs 2-36
Port-level indicators 2-36
Specifications 2-36
DS3XM-6 card
Description 2-38
Card-level LEDs 2-39
Port-level indicators 2-39
Provisioning 5-4
Specifications 2-39
with XCVT 2-38
DWDM
Description 6-1

and ONS 15454 networks 6-4
Benefits 6-3
ONS 15454 cards 6-4
System illustration 6-2

E

E1000-2 card
Description 7-4
Card-level LEDs 2-66
Illustration 7-4
Overview 2-65
Port-level indicators 2-66
Specifications 2-67
E100T-12 card
Description 7-3
Card-level LEDs 2-63
Illustration 7-3
Overview 2-62
Port-level indicators 2-63
Specifications 2-64
EC1-12 card
Card-level LEDs 2-24
Description 2-23
Port-level indicators 2-24
Specifications 2-24
EIA
Description 1-2
AMP CHAMP EIA
and card protection 2-5
cable management 1-53
description 1-22
installation 1-48
Backplane cover 1-19
BNC EIA
and card protection 2-4
description 1-19
installation 1-43
High-density BNC EIA
and card protection 2-4
description 1-20
insertion and removal tool 10-15
installation 1-45
Install 1-24
Remove 1-23
Replacement, all types 10-13
SMB EIA
and card protection 2-5
description 1-21
installation 1-45
Specifications 1-56
Electrical Interface Adapters
Install 1-47
Install DS-1 cables 1-48
Electrical Interface Assemblies *See* EIA
Ethernet 7-1 to 7-74
and Spanning Tree Protocol 7-10
Cards *See Also* E100-12 Card and E1000-2 Card 7-3
Circuits
manual cross-connects 7-54
Connectivity testing 7-73
Multicard and single-card EtherSwitch 7-15

F

Facility Loopbacks *See* Loopbacks
Fan Tray Assembly
Description 1-13
Fan speed 1-16
Fan tray filter 1-14
Fiber Boot 1-42
Front Door 1-10

G

GBIC
Description 1-39
Installing 1-40
Removing 1-41
Types 1-39

H

Hairpin Circuits 4-50, 4-56

I

Installing the ONS 15454
Alarms 1-29
Coaxial cable 1-43
Craft interface 1-31

Description 1-2
DS-1 cables 1-46
Equipment 1-2
Fiber optic cables 1-41
LAN 1-30
Power supply 1-25
Timing 1-30
Using ferrites 1-31
IP Address
Changing the default 3-22
Common scenarios 8-14
Description 3-5
Setup 8-10
Types 8-14

L

LAN
Accessing the ONS 15454 3-8
Installation 1-30
Modem 3-9
Pin field 1-30
Transparent LAN 7-2
LCD Screen
Description 1-17
Alarm indication 1-18
IP address entry 8-10
Liquid Crystal Display *See* LCD Screen
Loopback 4-51 to 4-63
Description 4-50
Facility 4-50
Terminal 4-50
Loopbacks
Description 4-50

M

MAC Addresses 7-67
Manual Cross-Connects *see* Ethernet
MIB
and Ethernet 7-70
Description 8-5

N

Netscape Communicator (using CTC) 3-2
Network Management 8-1 to 8-32
Network Testing
see also Hairpin Circuits
see also Loopbacks
Networks
Configuring 4-1
Management 8-1
Managing multiple rings 4-63

O

OC12 IR 1310 card
Card-level LEDs 2-45
Description 2-44
Port-level indicators 2-45
Specifications 2-45
OC12 LR 1310 card
Card-level LEDs 2-48
Description 2-47
Port-level indicators 2-48
Specifications 2-48
OC12 LR 1550 card
Card-level LEDs 2-51
Description 2-50
Port-level indicators 2-51
Specifications 2-51
OC3 IR 4 1310 card
Card-level LEDs 2-42
Description 2-41
Port-level indicators 2-42
Specifications 2-43
OC48 ELR DWDM cards
Card-level LEDs 2-60
Description 2-59
Port-level indicators 2-60
Specifications 2-61
OC48 IR 1310 card
Card-level LEDs 2-54
Description 2-53
Port-level indicators 2-54
Specifications 2-54
OC48 LR 1550 card
Card-level LEDs 2-57
Description 2-56
Port-level indicators 2-57

Specifications 2-57
ONS 15454
Cards *See* Cards
Installation *See* Installing the ONS 15454
Maintenance 10-1 to 10-15
Software, *see* CTC

P

PPMN 4-38
Protocols
IP *See* IP Address
Proxy ARP 8-12
SNMP 8-1
Spanning Tree 7-10, 7-66
SSM 3-30
Provisioning
Cards *See* Card Provisioning
Circuits 4-40
for BLSRs 4-6
for UPSRs 4-21
Proxy ARP 8-12

R

Rack Installation *See* Shelf Assembly
Regulatory requirements A-1
Remote Network Monitoring *See*RMON
Rings
Multiple 4-63
See BLSR
See UPSR
RMON
Alarm thresholds 7-69
Description 8-8

S

Shared Packet Ring 7-35
Shelf Assembly
Description 1-3
Bay Assembly 1-8
Installing 1-5
SNMP
Description 8-1
and the ONS 15454 8-3
Traps 8-7
SONET
and DWDM 6-4
and Ethernet 7-1
Data communications channel 2-7, 4-8
Line layer (maintenance span) 9-5
Synchronization status messaging 3-30
Timing parameters 3-29
Spanning Tree Protocol
Configuration 7-13
Description 7-10
Parameters 7-11
Spanning trees screen 7-66
Static Route Provisioning 8-30
Subtending Rings 4-27
Switching
and Ethernet 7-1
Multicard and Single-card EtherSwitch 7-15
Non-revertive 2-5
Revertive, in 1 to N card protection 2-3
Time division switching 2-11

T

TCC and TCC+ Cards
and TL1 11-1
Database backup 10-7
Description 2-7
LEDs
card level 2-8
system level 2-8
TCC specifications 2-9
TCC+ functions overview 2-8
Turn-up 1-38
Upgrading from TCC to TCC+ 10-11
Uploading 1-38
Technical Assistance Center xxxviii
Terminal Loopbacks *See* Loopbacks
Timing
Installation 1-30
Parameters 3-29
Setting up 3-31
Specifications 1-57
Timing Communications and Control Card *See* TCC and TCC+
TL1 11-1 to 11-129
TL1 Commands
Descriptions 11-21 to 11-92

Index 11-19
Troubleshooting
See Also Alarms
See Also Diagnostic files
See Also Loopbacks
see also Loopbacks
Turn-up *See* Cards, Turn-up

U

Unidirectional Path Switched Rings *See* UPSR
UPSR
Adding a node 4-25
Converting from ADM 4-32, 4-35
Description 4-17
Dropping nodes 4-26
Removing nodes 4-23
Sample application 4-19
Setting up 4-21
Subtending 4-27

V

VLAN
Description 7-6
and Ethernet 7-2
Provisioning ports 7-59
Tagging 7-6
VT Mapping 2-15

X

XC Card *See* Cross Connect Card
XCVT Card *See* Cross Connect VT card